


UNIVERSIDAD CATÓLICA DE CUENCA

**UNIVERSIDAD CATÓLICA DE CUENCA**

*Comunidad Educativa al Servicio del Pueblo*

**FACULTAD INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA**

**CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN**

**PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN**

# EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA MEDIANTE PENTESTING EN LOS SISTEMAS DE INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO YUYAY LTDA.

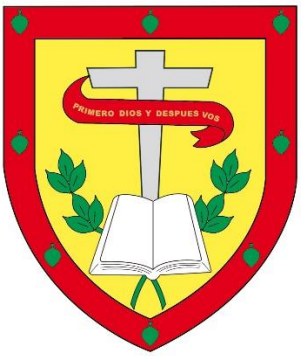
**AUTOR: CARLOS ISRAEL AVALOS GOMESCOELLO**

**DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES, MGS.**

**CAÑAR - ECUADOR**

**2026**

**DIOS, PATRIA, CULTURA Y DESARROLLO**




**UNIVERSIDAD CATÓLICA DE CUENCA**

*Comunidad Educativa al Servicio del Pueblo*

**FACULTAD INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA**

**CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN**

**PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN**

# EVALUACIÓN DE LA SEGURIDAD INFORMÁTICA MEDIANTE PENTESTING EN LOS SISTEMAS DE INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO YUYAY LTDA.

AUTOR: CARLOS ISRAEL AVALOS GOMESCOELLO

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILES, MGS.

**CAÑAR – ECUADOR**

2026

**DIOS, PATRIA, CULTURA Y DESARROLLO**

# DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

**CARLOS ISRAEL AVALOS GOMESCOELLO**, portador de la cédula de ciudadanía Nº **0302546635**. Declaro ser el autor de la obra: **"Evaluación de la seguridad informática mediante pentesting en los sistemas de información de la Cooperativa de Ahorro y Crédito Yuyay Ltda."**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.



CARLOS ISRAEL AVALOS GOMESCOELLO

C.I. 0302546635

# CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el est. CARLOS ISRAEL AVALOS GOMESCOELLO, bajo mi supervisión.



ING. CRISTHIAN HUMBERTO FLORES URGILES, MGS.

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

# DEDICATORIA

Con profundo cariño y gratitud, dedico este trabajo a las personas que han sido fundamentales en mi vida y en el proceso que me ha llevado hasta este momento.

Dedico este trabajo a mi padre Carlos Avalos, a mi madre Ipatya Gomescoello, a mi hermano Toño, mi abuelita Balvina, a mi Abuelito Jaime, a mi Tata, quienes con su paciencia, apoyo constante y sabios consejos han sido el pilar fundamental en mi vida. Gracias por sus enseñanzas recibidas, he logrado llegar hasta aquí. Extiendo mi gratitud a todos mis profesores que me han guiado en este camino.

# AGRADECIMIENTO

Al haber terminado esta etapa significativa de mi vida, quiero agradecer a mis seres queridos por ser un apoyo incondicional en mi vida y ayudarme a alcanzar este logro importante.

Agradezco por la Sinceridad, Paciencia, Generosidad y Nobleza a todos los que me acompañaron en este largo y arduo proceso.

Agradezco también a mi tutor de Tesis, cuyo apoyo y enseñanza me han guiado durante este trabajo significativo. De la misma manera a los docentes universitarios quien con su sabiduría me han enriquecido de conocimientos, inspirándome a seguir avanzando día a día.

# RESUMEN

La creciente sofisticación de las amenazas cibernéticas expone a las cooperativas de ahorro y crédito, que custodian información financiera y datos personales de sus socios. Este trabajo tuvo como objetivo evaluar la seguridad de la información de los sistemas de la Cooperativa de Ahorro y Crédito Yuyay Ltda. mediante técnicas de prueba de penetración (pentesting) para identificar debilidades, valorar los riesgos y proponer medidas de mejora. Se aplicó un enfoque mixto, de nivel descriptivo-aplicado y diseño no experimental, transversal y de campo, como estudio de caso. La ejecución técnica siguió NIST SP 800-115, OWASP y PTES; la valoración del riesgo, ISO/IEC 27005:2022 y MAGERIT; y la severidad se clasificó con CVSS v4.0. Las pruebas se realizaron en modalidad de caja gris sobre un servidor de réplica del entorno de producción y abarcaron el servidor web institucional, la aplicación de marcación y los servicios de red. Se documentaron siete hallazgos validados con evidencia: dos de severidad alta, relacionados con la exposición del servicio MySQL en todas las interfaces de red y con el uso de HTTP sin cifrado, cuatro de severidad media y uno de severidad baja, asociados con debilidades de configuración y con una superficie de ataque innecesariamente amplia. Para cada hallazgo se formuló un plan de tratamiento alineado con ISO/IEC 27002:2022, el NIST Cybersecurity Framework 2.0 y la normativa de la SEPS, con responsables y plazos definidos. Se concluye que el esquema integrado permite a la cooperativa priorizar la mitigación y sostener evaluaciones periódicas de seguridad.

***Palabras clave:*** *pentesting, ciberseguridad, vulnerabilidades, CVSS, cooperativas*

## ABSTRACT

The increasing sophistication of cyber threats exposes credit unions that safeguard members' financial information and personal data. This study aimed to evaluate the information security of the systems at Cooperativa de Ahorro y Crédito Yuyay Ltda. using penetration testing (pentesting) techniques to identify vulnerabilities, assess risks, and propose improvement measures. The study used a mixed-methods approach, combining descriptive and applied scopes with a non-experimental, cross-sectional, field-based case study design. The technical assessment followed NIST SP 800-115, OWASP, and PTES; the risk assessment followed ISO/IEC 27005:2022 and MAGERIT; and severity was classified using Common Vulnerability Scoring System (CVSS) v4.0. The tests were conducted in a gray-box configuration on a replica server of the production environment and covered the institutional web server, the attendance-tracking application, and network services. Seven findings supported by evidence were documented: two of high severity, related to the exposure of the MySQL service on all network interfaces and the use of unencrypted HTTP; four of medium severity; and one of low severity, associated with configuration weaknesses and an unnecessarily broad attack surface. For each finding, a treatment plan was developed in accordance with ISO/IEC 27002:2022, the NIST Cybersecurity Framework 2.0, and SEPS regulations, with defined responsible parties and deadlines. It concludes that the integrated framework enables the cooperative to prioritize mitigation and conduct periodic security assessments.

***Keywords***: *pentesting, cybersecurity, vulnerabilities, CVSS, cooperatives*

# ÍNDICE

Contenido

Declaratoria de autoría y responsabilidad ..... iii

CERTIFICACIÓN ..... iv

DEDICATORIA ..... v

AGRADECIMIENTO ..... vi

Resumen ..... vii

ABSTRACT ..... **¡Error! Marcador no definido.**

ÍNDICE ..... viii

ÍNDICE DE TABLAS ..... xv

ÍNDICE DE FIGURAS ..... xvi

Introducción ..... 1

CAPÍTULO I ..... 4

1.1 Planteamiento del problema ..... 4

1.1.1 Formulación del problema ..... 6

1.2 Antecedentes de la Investigación (Trabajos Relacionados) ..... 6

1.3 Justificación de la investigación ..... 8

1.3.1 Objetivo General ..... 9

1.3.2 Objetivos Específicos ..... 10

1.3.3 Limitaciones ..... 10

1.3.4 Delimitaciones ..... 10

CAPÍTULO II ..... 12

MARCO TEÓRICO ..... 12

2.1 Seguridad informática en sistemas de información financiera.....12
2.1.1 Sistemas de información en cooperativas de ahorro y crédito ..... 13
2.1.2 Canales electrónicos y superficie de ataque ..... 13
2.1.3 Activos de información críticos..... 14
2.2 Seguridad de la información y ciberseguridad.....15
2.2.1 Principios de confidencialidad, integridad y disponibilidad ..... 15
2.2.2 Ciberseguridad como gestión institucional del riesgo ..... 16
2.3 Pentesting o pruebas de penetración .....17
2.3.1 Definición e importancia del pentesting..... 18
2.3.2 Tipos de pruebas de penetración ..... 18
2.3.3 Fases generales del pentesting..... 19
2.3.4 Reglas de compromiso, autorización y ética ..... 20
2.3.5 Producto esperado de una prueba de penetración..... 21
2.3.6 Selección metodológica para la tesis..... 22
2.4 Vulnerabilidades y amenazas en sistemas de información .....22
2.4.1 Vulnerabilidades en aplicaciones web..... 23
2.4.2 Vulnerabilidades en APIs ..... 24
2.4.3 Vulnerabilidades en infraestructura de red..... 24
2.4.4 Ingeniería social y factor humano ..... 25
2.4.5 Priorización de vulnerabilidades ..... 26
2.5 Gestión de vulnerabilidades y valoración del riesgo.....26
2.5.1 CVSS v4.0 como criterio de severidad técnica ..... 27
2.5.2 CISA KEV, CWE y MITRE ATT&CK como criterios de complementarios..... 27

2.5.3 ISO/IEC 27005:2022 para valoración del riesgo ..... 28
2.5.4 Riesgo inherente, controles y riesgo residual ..... 29
2.5.5 Articulación con MAGERIT para el tratamiento del riesgo ..... 29
2.6 Normativa y estándares aplicables ..... 30
2.6.1 Ley Orgánica de Protección de Datos Personales y su Reglamento ..... 30
2.6.2 Normativa SEPS sobre seguridad de la Información ..... 31
2.6.3 Normativa SEPS sobre canales electrónicos ..... 31
2.6.4 Normativa SEPS sobre riesgo operativo ..... 32
2.6.5 Estándares ISO/IEC 27001, 27002, 27005 y 27035 ..... 32
2.6.6 NIST Cybersecurity Framework 2.0 ..... 33
2.6.7 OWASP Top 10 y OWASP API Security Top 10 ..... 33
2.7 Herramientas y técnicas para la evaluación de seguridad ..... 34
2.7.1 Reconocimiento y escaneo ..... 34
2.7.2 Análisis de vulnerabilidades ..... 35
2.7.3 Explotación Controlada ..... 35
2.7.4 Reporte y tratamiento de hallazgos ..... 36
2.8 Comparación de normas, metodologías y marcos aplicables ..... 36
2.9 Síntesis del marco teórico aplicado al estudio ..... 39
CAPÍTULO III ..... 41
MARCO METODOLÓGICO ..... 41
3.1 Enfoque de la investigación ..... 41
3.2 Nivel de la investigación ..... 42
3.3 Diseño de la investigación ..... 42

3.4 Entorno de pruebas y laboratorio ....43
3.4 Métodos de investigación....43
3.5 Población y muestra ....44
3.6 Tipo de muestreo....45
3.7 Criterios de inclusión y exclusión ....45
3.8 Técnicas e instrumentos de recolección de datos....46
3.9 Procedimiento de la investigación....47
3.10 Validación de los instrumentos ....49
3.11 Confiabilidad de los instrumentos....49
3.12 Técnicas de procesamiento y análisis de datos ....50
3.13 Operacionalización de variables....50
3.14 Consideraciones éticas ....51
CAPÍTULO IV.... 53
PROPUESTA.... 53
4.1 Introducción ....53
4.1.1 Objetivo de la propuesta.... 54
4.2 Fase 1. Estudio documental y normativo ....54
4.3 Fase 2. Levantamiento y definición del alcance ....57
4.3.1 Resultados de la entrevista .... 58
4.4 Fase 3. Ejecución del pentesting ....58
4.4.1 Reconocimiento y escaneo (footprinting y scanning) .... 59
4.4.2 Análisis de vulnerabilidades.... 62
4.4.3 Explotación controlada.... 66

4.5 Fase 4. Evaluación de resultados y análisis de riesgos .....68
4.6 Fase 5. Elaboración de la propuesta de mejora .....70
4.6.1 Lineamientos y políticas de seguridad propuestos ..... 71
4.6.2 Verificación posterior (retest)..... 72
Conclusiones..... 72
Recomendaciones ..... 74
Referencias..... 76
Bibliografía ..... 76
Anexos ..... 79
Anexo 1: Protocolo de Investigación .....79
Anexo: Formato del Anteproyecto. .....79
Anexo 2 Guía de entrevista estructurada.....99
Anexo 3 Comandos ejecutados durante el pentesting .....101
Reconocimiento y descubrimiento ..... 102
Escaneo de puertos y servicios ..... 102
Servicio web / IIS (HTTP)..... 102
Enumeración de directorios ..... 103
Análisis con Nikto (sin hallazgos reportados) ..... 103
HTTPS / TLS..... 103
Base de datos (MySQL, 3306) ..... 103
SMB y RDP ..... 104
Anexo 4 Controles y políticas de seguridad propuestos .....104
A4.1 Fichas de control técnico por hallazgo ..... 104

A4.2 Políticas de seguridad propuestas ..... 105

A4.2.1 Política de gestión de vulnerabilidades..... 106

A4.2.2 Política de endurecimiento (hardening) de servidores y servicios ..... 106

A4.2.3 Política de gestión de accesos y credenciales ..... 107

A4.2.4 Política de cifrado y protección del transporte ..... 107

A4.2.5 Política de segmentación de red ..... 108

A4.2.6 Política de capacitación y concienciación en seguridad ..... 109

# ÍNDICE DE TABLAS

Tabla 1 Tipos de pruebas de penetración según el nivel de conocimiento ..... 19

Tabla 2 Relación entre hallazgo técnico, severidad y tratamiento del riesgo ..... 29

Tabla 3 Cuadro comparativo de normas, marcos y referencias aplicables al estudio ..... 37

Tabla 4 Operacionalización de variables ..... 51

Tabla 5 Correspondencia entre las fases del procedimiento (sección 3.9) y las secciones del Capítulo IV ..... 53

Tabla 6 Documentos internos revisados, norma de referencia y brecha principal ..... 55

Tabla 7 Marcos de referencia seleccionados y su función en la evaluación ..... 56

Tabla 8 Configuración del entorno y alcance de las pruebas ..... 57

Tabla 9 Síntesis de los resultados de la entrevista al responsable de tecnología ..... 58

Tabla 10 Matriz de hallazgos ..... 66

Tabla 11 Consolidación de hallazgos técnicos del pentesting ..... 68

Tabla 12 Matriz de nivel de riesgo Probabilidad × Impacto ..... 69

Tabla 13 Valoración del riesgo por hallazgo ..... 69

Tabla 14 Plan de tratamiento del riesgo por hallazgo ..... 70

Tabla A4.1 Fichas de control técnico por hallazgo ..... 105

# ÍNDICE DE FIGURAS

Figura 1 Escaneo de puertos y detección de servicios sobre el objetivo (Nmap -sV) ..... 59

Figura 2 Detección de MySQL 8.0.36 y Apache httpd (8080) con versión expuesta ..... 60

Figura 3 Divulgación del banner del servidor en las cabeceras HTTP (Server: Microsoft-IIS/10.0) ..... 61

Figura 4 Enumeración de directorios finalizada sin hallazgos sensibles (control negativo) ..... 62

Figura 5 Método HTTP TRACE habilitado y divulgación de métodos permitidos vía OPTIONS ..... 63

Figura 6 Cabeceras HTTP del servidor: banner expuesto, método TRACE y ausencia de cabeceras de seguridad..... 64

Figura 7 Servicio de base de datos (3306) enlazado a 0.0.0.0 en todas las interfaces (netstat).... 65

Figura 8 Servicios de Windows expuestos (SMB, NetBIOS, MSRPC, UPnP) y detección de sistema operativo ..... 66

# INTRODUCCIÓN

La transformación digital de los servicios financieros ha ampliado de forma sostenida la superficie de ataque de las instituciones que los prestan. Las entidades de este sector enfrentan amenazas como el phishing, el ransomware, los ataques a aplicaciones y a proveedores externos, el robo de credenciales, el fraude y la denegación de servicio (ENISA, 2025). En el Ecuador, las cooperativas de ahorro y crédito custodian información financiera y datos personales de sus socios y, con frecuencia, operan con limitaciones de infraestructura y de controles de seguridad, lo que incrementa su exposición. En América Latina, las debilidades más recurrentes se relacionan con el uso de software desactualizado, la ausencia de controles de seguridad y la escasa capacitación del personal (Flor-Unda et al., 2023), factores que muestran que el problema es tanto técnico como organizacional.

A este escenario se suma un marco regulatorio cada vez más exigente. La Ley Orgánica de Protección de Datos Personales (Asamblea Nacional, 2021) y las normas de la Superintendencia de Economía Popular y Solidaria sobre seguridad en el uso de canales electrónicos y administración del riesgo operativo (SEPS, 2022, 2024) obligan a estas entidades a proteger la confidencialidad, la integridad y la disponibilidad de la información que gestionan. Cumplir estas disposiciones exige algo más que disponer de políticas documentadas: es necesario verificar que los controles funcionen en la práctica. Las pruebas de penetración, o pentesting, responden a esta necesidad, ya que simulan de manera controlada las técnicas de un atacante para comprobar si las configuraciones, los mecanismos de acceso y los servicios expuestos resisten amenazas reales. El 94 % de las organizaciones considera el pentesting una práctica básica para evaluar su seguridad (Help Net Security, 2025), y la creciente complejidad de los sistemas

tecnológicos hace necesario aplicarlo de forma periódica y no como una acción aislada (ISTARI, 2024).

En este contexto, la Cooperativa de Ahorro y Crédito Yuyay Ltda. podría presentar debilidades en sus sistemas de información derivadas de la falta de evaluaciones periódicas de seguridad. Por ello, la presente investigación se orientó a responder la pregunta: ¿cómo evaluar la seguridad de la información de los sistemas de la Cooperativa de Ahorro y Crédito Yuyay Ltda. mediante metodologías de pentesting? En correspondencia, el objetivo general fue realizar una evaluación de la seguridad de la información de dichos sistemas mediante técnicas de prueba de penetración basadas en modelos ampliamente adoptados, con el fin de identificar debilidades, valorar los riesgos asociados y ofrecer recomendaciones para mejorar su protección.

Para alcanzar este objetivo, se adoptó un enfoque mixto, de nivel descriptivo-aplicado, con un diseño no experimental, transversal y de campo, desarrollado como estudio de caso. El estudio propone un esquema metodológico integrado que articula la ejecución técnica de las pruebas, orientada por la guía NIST SP 800-115 (National Institute of Standards and Technology, 2008), la guía de pruebas de OWASP (OWASP, s. f.) y el estándar PTES; la valoración y el tratamiento del riesgo, conforme a ISO/IEC 27005:2022 (ISO/IEC, 2022c) y a la metodología MAGERIT; y la clasificación de la severidad de las vulnerabilidades mediante CVSS v4.0 (FIRST, 2023). Las pruebas se ejecutaron bajo la modalidad de caja gris sobre un servidor de réplica proporcionado por la cooperativa, que reproduce la configuración del entorno de producción, de modo que la evaluación del servidor web institucional, la aplicación de marcación y los servicios de red asociados no afectara la continuidad de los servicios ni la información de los socios. El procedimiento se organizó en cinco fases: estudio documental y

normativo; levantamiento y definición del alcance; ejecución del pentesting; evaluación de resultados y análisis de riesgos; y elaboración de la propuesta de mejora.

El aporte del trabajo es doble. En el plano práctico, proporciona a la cooperativa un diagnóstico objetivo y basado en evidencia sobre el estado de seguridad de sus sistemas, junto con un plan de tratamiento del riesgo que asigna controles técnicos y administrativos, responsables y plazos a cada hallazgo. En el plano metodológico, ofrece un esquema documentado con trazabilidad de evidencias, que puede replicarse en futuras evaluaciones de la propia institución y adaptarse a otras entidades del sector financiero popular y solidario con características similares.

El documento se estructura en cuatro capítulos. El Capítulo I presenta el planteamiento y la formulación del problema, los antecedentes de la investigación, la justificación, los objetivos, las limitaciones y las delimitaciones del estudio. El Capítulo II desarrolla el marco teórico, que abarca la seguridad informática en los sistemas de información financiera, los fundamentos del pentesting, las vulnerabilidades y amenazas más relevantes, la gestión y valoración del riesgo, la normativa y los estándares aplicables, y las herramientas empleadas en la evaluación de seguridad. El Capítulo III describe el marco metodológico: enfoque, nivel y diseño de la investigación, entorno de pruebas, población y muestra, técnicas e instrumentos, procedimiento, operacionalización de variables y consideraciones éticas. El Capítulo IV expone la propuesta, organizada según las cinco fases del procedimiento, con los hallazgos validados, su valoración de riesgo y el plan de tratamiento correspondiente. Finalmente, se presentan las conclusiones, las recomendaciones, las referencias y los anexos que respaldan el trabajo.

# CAPÍTULO I

## 1.1 Planteamiento del problema

La digitalización de los servicios financieros ha trasladado buena parte de la operación de las instituciones del sector a portales web, aplicaciones y servicios de red, lo que amplía de forma sostenida su superficie de ataque. Entre las amenazas predominantes contra el sector financiero se encuentran el phishing, el ransomware, los ataques a aplicaciones y a proveedores externos, el robo de credenciales, el fraude y la denegación de servicio (ENISA, 2025). Muchas de estas amenazas no dependen de técnicas sofisticadas para tener éxito, sino de debilidades que ya existen en la infraestructura antes del ataque: servicios expuestos innecesariamente, configuraciones por defecto o canales de comunicación sin cifrado.

En América Latina, esta exposición tiene un componente estructural. Flor-Unda et al. (2023) identifican como debilidades recurrentes de la región el uso de software desactualizado, la ausencia de controles de seguridad y la escasa capacitación del personal. Las cooperativas de ahorro y crédito del Ecuador comparten estas condiciones: custodian información financiera y datos personales de sus socios, pero con frecuencia operan con recursos tecnológicos y humanos limitados para gestionar la seguridad de la información.

A esta situación se suma un marco regulatorio cada vez más exigente. La Ley Orgánica de Protección de Datos Personales obliga a adoptar medidas técnicas y organizativas para proteger los datos que se tratan (ASAMBLEA NACIONAL, 2021). La Superintendencia de Economía Popular y Solidaria, por su parte, exige tres cosas:

- gestionar la seguridad de la información mediante políticas, procesos, roles y controles (SEPS, 2022);

- establecer medidas mínimas de seguridad en los canales electrónicos (SEPS, 2023);
- administrar el riesgo operativo de forma integral (SEPS, 2024).

Sin embargo, estas obligaciones pueden cumplirse en el plano documental, con políticas aprobadas y procedimientos escritos, sin que exista evidencia de que los controles funcionan en la configuración real de los sistemas. Esa distancia entre el control documentado y el control efectivo solo puede verificarse mediante pruebas técnicas que examinen los sistemas desde la perspectiva de un atacante (National Institute of Standards and Technology, 2022). Las auditorías de seguridad y las pruebas de penetración resultan fundamentales para descubrir vulnerabilidades antes de que sean explotadas (Restrepo Gomez & Correa Ortiz , 2024).

La Cooperativa de Ahorro y Crédito Yuyay Ltda., entidad supervisada por la SEPS, se encuentra en esta situación. La institución gestiona información financiera y personal de sus socios a través de servicios web y de red, y cuenta con políticas de seguridad formalizadas. No obstante, [no dispone de evaluaciones técnicas periódicas que verifiquen la efectividad de sus controles]. En consecuencia, la cooperativa no cuenta con un diagnóstico basado en evidencia sobre qué servicios están expuestos, qué configuraciones inseguras persisten y qué nivel de riesgo representan para la confidencialidad, la integridad y la disponibilidad de su información.

Si esta situación se mantiene, las debilidades no detectadas podrían aprovecharse para acceder sin autorización a datos de los socios, interceptar credenciales o interrumpir servicios. Esto tendría consecuencias económicas, legales, por incumplimiento de la LOPDP y de la normativa SEPS, y reputacionales, en una entidad cuya continuidad depende de la confianza de sus socios. Además, sin un diagnóstico técnico, la cooperativa no puede priorizar sus inversiones en seguridad según el riesgo real al que está expuesta.

### *1.1.1 Formulación del problema*

La creciente sofisticación de las amenazas cibernéticas, sumada a las limitaciones en infraestructura y en controles de seguridad, convierte a las cooperativas financieras en organizaciones vulnerables a ataques informáticos. En este contexto, la Cooperativa de Ahorro y Crédito Yuyay Ltda. podría presentar debilidades en sus sistemas de información derivadas de la falta de evaluaciones periódicas de seguridad. Por ello, surge la necesidad de aplicar metodologías estructuradas de pentesting que permitan identificar vulnerabilidades, evaluar los riesgos asociados y fortalecer la protección de la información institucional. A partir de esta necesidad, la presente investigación se orienta a responder la siguiente pregunta:

¿Cómo evaluar la seguridad de la información de los sistemas de la Cooperativa de Ahorro y Crédito Yuyay Ltda. mediante metodologías de pentesting?

## 1.2 Antecedentes de la Investigación (Trabajos Relacionados)

Se han realizado diferentes estudios a nivel internacional para abordar el análisis y comparación de herramientas de prueba de penetración con un enfoque en los criterios basados en la experimentación. Un trabajo relevante es el desarrollado por Albahar et al. (2022), en donde llevaron a cabo una evaluación comparativa de herramientas de análisis de vulnerabilidades en entornos controlados y analizaron problemas de precisión, cobertura y generación de falsos positivos (pág. 23) Las herramientas no demostraron una efectividad completa por sí solas, lo que puso de manifiesto la necesidad de integrar varias soluciones para lograr una detección de vulnerabilidades más integral.

Además, investigaciones recientes se han centrado en incorporar técnicas de inteligencia artificial en las pruebas de penetración y proponen métodos automatizados que facilitan la identificación de vulnerabilidades y reducen el tiempo de análisis. En este sentido, Sharma et al.

(2023) observan que la evolución de los métodos hacia esquemas híbridos (manual-automatizado) permite optimizar de forma notable la eficiencia y la reproducibilidad en la ejecución de pruebas de seguridad. Estos trabajos constituyen una base sólida para la evaluación experimental del rendimiento de las herramientas en entornos virtualizados.

En América Latina, la evidencia sugiere que la protección de la información sigue siendo un problema estructural en las organizaciones que gestionan datos sensibles. Un ejemplo es el estudio de Flor-Unda et al. (2023), realizado en Ecuador y publicado en una revista indexada, que analiza las principales vulnerabilidades en la región e identifica problemáticas como el uso de software obsoleto, la ausencia de controles de seguridad y la falta de capacitación del personal, factores que aumentan significativamente el riesgo de exposición de las organizaciones. Esta investigación resulta de especial interés para el presente estudio porque muestra que las debilidades de seguridad pueden ser tanto técnicas como organizacionales, lo que respalda el uso de las pruebas de penetración para constatar el estado real de la seguridad de los sistemas.

Los estudios recientes también han reconocido que las pruebas de penetración pueden servir como la solución principal para detectar vulnerabilidades en las infraestructuras corporativas. Un artículo publicado en América Latina destaca que, para el descubrimiento de vulnerabilidades dentro del sistema antes de que puedan ser explotadas, las auditorías de seguridad y las pruebas de penetración son fundamentales, y además señala que métodos alternativos, como bug bounty, no sustituyen la necesidad de especialistas en pruebas de penetración (Restrepo Gomez & Correa Ortiz , 2024).

También se señalaron estudios que evaluaban herramientas específicas de detección de vulnerabilidades, y medían su capacidad para encontrar fallos de seguridad en sistemas web y

sistemas de red local Albahar et al. (2022). Sin embargo, estos estudios tienden a centrarse en herramientas individuales, en lugar de en comparaciones exhaustivas de herramientas organizadas en torno a una metodología, destacando una brecha en la literatura nacional, que esta investigación busca llenar.

### 1.3 Justificación de la investigación

La presente investigación es pertinente porque la evaluación técnica de la seguridad se ha consolidado como una práctica esencial en la gestión de la ciberseguridad. Investigaciones recientes muestran que el 94 % de las organizaciones considera el pentesting una práctica básica para evaluar su seguridad (Help Net Security, 2025).

Asimismo, la creciente complejidad de los sistemas tecnológicos y la naturaleza cambiante de las amenazas hacen necesario que estas evaluaciones se realicen de forma periódica y no como acciones aisladas (ISTARI, 2024). En el caso de una cooperativa de ahorro y crédito, esta necesidad es mayor, ya que la información que protege pertenece a sus socios y su pérdida afecta directamente la confianza en la institución.

Desde el punto de vista práctico, el estudio proporcionará a la Cooperativa de Ahorro y Crédito Yuyay Ltda. un diagnóstico objetivo, basado en evidencia, del estado de seguridad de sus sistemas de información. Los hallazgos permitirán identificar vulnerabilidades concretas, valorar el riesgo que representan y priorizar su tratamiento mediante un plan de mitigación con controles técnicos y administrativos, responsables y plazos definidos. De este modo, la institución contará con insumos para fortalecer la confidencialidad, integridad y disponibilidad de su información.

Desde el punto de vista teórico y normativo, la investigación aplica y contrasta el marco normativo de seguridad de la información vigente para el sector financiero popular y solidario

(las normas de la SEPS y la Ley Orgánica de Protección de Datos Personales) con los resultados técnicos obtenidos en un entorno real. Esto permite verificar en qué medida los controles exigidos por la normativa se reflejan en la configuración efectiva de los sistemas, y aporta evidencia sobre la aplicación de estándares internacionales en una entidad cooperativa ecuatoriana.

Desde el punto de vista metodológico, el estudio propone un esquema integrado que articula la ejecución técnica de las pruebas (NIST SP 800-115, OWASP y PTES) con la valoración y el tratamiento del riesgo (ISO/IEC 27005:2022 y MAGERIT) y la clasificación de severidad mediante CVSS v4.0. Este esquema, documentado con trazabilidad de evidencias, puede replicarse en futuras evaluaciones de la propia cooperativa y adaptarse a otras entidades del sector con características similares.

Los beneficiarios directos del estudio son la cooperativa y sus socios, cuya información se verá mejor protegida. Como beneficiaria indirecta, la carrera de Ingeniería de Sistemas de Información dispondrá de un caso aplicado de evaluación de seguridad en el sector cooperativo. Finalmente, la investigación es viable porque la cooperativa autorizó la ejecución de las pruebas sobre un servidor de réplica que reproduce el entorno de producción, lo que permite evaluar los sistemas sin afectar la continuidad de sus servicios ni la información de sus socios.

### *1.3.1 Objetivo General*

Realizar una evaluación de la seguridad de la información de los sistemas de la Cooperativa de Ahorro y Crédito Yuyay Ltda, considerando las técnicas de prueba de penetración basadas en modelos universalmente adoptados, para identificar debilidades y evaluar los riesgos, ofreciendo recomendaciones para mejorar y optimizar su protección.

### *1.3.2 Objetivos Específicos*

- Analizar las metodologías de seguridad de la información y pruebas de penetración para evaluar las herramientas de seguridad utilizadas en la evaluación de seguridad de los sistemas en Yuyay Ltda. Cooperativa.
- Seleccionar y justificar las metodologías de pentesting más adecuadas para el contexto de la Cooperativa Yuyay Ltda., evaluando su efectividad y aplicabilidad.
- Evalúe los sistemas de Yuyay Ltda. Cooperativa y lleve a cabo las diferentes fases de pruebas de penetración. Redacte medidas de mitigación de riesgos basadas en sus hallazgos.

### *1.3.3 Limitaciones*

- El tiempo disponible para la ejecución de la investigación podría limitar la profundidad de las pruebas de penetración realizadas.
- El acceso a información sensible y ciertos sistemas de la cooperativa estará restringido por políticas de confidencialidad y seguridad institucional.
- Los recursos tecnológicos y humanos disponibles para la ejecución de pruebas avanzadas de ciberseguridad pueden ser limitados.
- Las pruebas de pentesting deberán realizarse de forma controlada para evitar afectar la continuidad operativa de la cooperativa.

### *1.3.4 Delimitaciones*

- La investigación se centrará únicamente en la evaluación de la seguridad de los sistemas de información y activos tecnológicos de la Cooperativa de Ahorro y Crédito Yuyay Ltda.

- El estudio abarcará exclusivamente las fases de reconocimiento, análisis de vulnerabilidades, explotación controlada y generación de informes de pentesting.
- El presente trabajo se limitará al análisis de los sistemas actualmente implementados y en funcionamiento, sin proponer el desarrollo de nuevos sistemas.
- La investigación estará enfocada principalmente en el área de tecnologías de la información y sistemas de la cooperativa.

# CAPÍTULO II

# MARCO TEÓRICO

## 2.1 Seguridad informática en sistemas de información financiera

La seguridad informática en instituciones financieras constituye un componente esencial para proteger sistemas que procesan información sensible, transacciones económicas y servicios digitales de atención a socios. Los sistemas de información de cooperativas de ahorro y crédito se utilizan para almacenar datos administrativos y ayudar a impulsar operaciones clave para cuentas, préstamos, cobranzas, autenticación, informes regulatorios y comunicaciones internas y externas dentro del sistema y de los canales electrónicos. Esto significa que la seguridad debe ser un proceso continuo que consiste en controles tecnológicos, políticas, gestión de riesgos, capacitación y evaluación regular.

La “transformación digital” ofrece cada vez más oportunidades y eficiencias para los servicios financieros. Sin embargo, también implica una superficie de ataque creciente. El informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) sobre el sector financiero señala que las amenazas dirigidas a las instituciones de servicios financieros incluyen ataques de phishing, ransomware, ataques a proveedores externos, ataques a aplicaciones, robo de credenciales, fraude y denegación de servicios. (ENISA, 2025). Esta situación exige evaluaciones que permitan identificar fallos antes de que puedan ser explotados por terceros no autorizados, sobre todo cuando los sistemas procesan datos personales, información financiera y operaciones transaccionales.

Pruebas de penetración es un ataque controlado que prueba los controles existentes de la misma manera que no puede hacerlo una revisión documental. Para ello, las pruebas de penetración simulan ataques de forma controlada para verificar si las configuraciones, las

técnicas de autenticación, los controles de acceso, las divisiones de red, las políticas de actualización, los registros de eventos y los controles de seguridad funcionan adecuadamente frente a amenazas posibles, reales o percibidas.

### *2.1.1 Sistemas de información en cooperativas de ahorro y crédito*

Las cooperativas financieras dependen de sistemas integrados que recogen y procesan datos para el funcionamiento de la gestión de ahorro y crédito, así como para los sistemas de auditoría y retención de documentos. Los datos procesados y almacenados por estos sistemas integrados deben estar disponibles de inmediato para los miembros de la cooperativa. La falla de los sistemas de integración de datos provoca fallos de servicio que resultan en pérdidas para los miembros de la cooperativa.

Desde la perspectiva de seguridad, cada sistema debe protegerse considerando su función dentro del negocio y su nivel de exposición. Un sistema core financiero tiene una criticidad mayor que una estación administrativa aislada porque una falla de confidencialidad, integridad o disponibilidad puede afectar directamente la continuidad de los servicios, la confianza de los socios y el cumplimiento normativo. Por tanto, el levantamiento de activos constituye una fase previa indispensable para delimitar el alcance del pentesting y priorizar los activos que serán evaluados, en correspondencia con el enfoque de gestión de riesgos de ISO/IEC 27005:2022 (ISO/IEC, 2022c).

### *2.1.2 Canales electrónicos y superficie de ataque*

Los canales electrónicos permiten a los usuarios realizar operaciones mediante dispositivos, aplicaciones, portales web, cajeros automáticos, banca móvil, banca en línea y otros medios tecnológicos. La normativa de la Superintendencia de Economía Popular y Solidaria sobre canales electrónicos define estos canales como vías mediante las cuales los usuarios

pueden efectuar transacciones con entidades financieras utilizando elementos o dispositivos electrónicos y tecnológicos (SEPS, 2023).

La superficie de ataque aumenta cuando la cooperativa utiliza portales transaccionales, aplicaciones móviles, APIs, conexiones remotas, integraciones con proveedores, servicios de correo institucional o plataformas de atención digital. Cada componente expuesto puede convertirse en punto de entrada si presenta configuraciones inseguras, credenciales débiles, falta de cifrado, versiones obsoletas, validaciones incompletas o controles de autorización deficientes. Por ello, el pentesting no debe limitarse a detectar puertos o servicios activos, sino que debe evaluar también la lógica de negocio y los controles de acceso asociados a los servicios financieros.

### *2.1.3 Activos de información críticos*

Los activos de información son todos los recursos que tienen valor para la organización y que deben protegerse frente a amenazas internas o externas. En una cooperativa financiera, pueden considerarse activos críticos las bases de datos de socios, sistemas de crédito, servidores de aplicaciones, redes internas, respaldos, credenciales, bitácoras, documentación técnica, contratos, políticas, equipos de comunicación y servicios tercerizados.

La Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 establece la norma de control respecto a la seguridad de la información en entidades del Sector Financiero Popular y Solidario. Esta norma exige gestionar la seguridad mediante políticas, procesos, roles, responsabilidades, formación, eventos, recursos y controles; por tanto, permite vincular el pentesting con la administración formal de activos de información y no únicamente con la ejecución de herramientas técnicas (SEPS, 2022).

## 2.2 Seguridad de la información y ciberseguridad

La seguridad de la información y la ciberseguridad son complementarias. La seguridad de la información garantiza la protección de la confidencialidad, integridad y disponibilidad de la información en distintos formatos físicos, digitales y lógicos. La ciberseguridad protege sistemas, redes y servicios digitales frente a ataques en el ciberespacio. La seguridad de la información proporciona los servicios protectores holísticos. La ciberseguridad se centra en las amenazas digitales y en las tecnologías necesarias para su remediación (NIST, 2024).

ISO/IEC 27001:2022 establece requisitos para establecer, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en riesgos. En el caso de las cooperativas financieras, esto implicaría integrar la seguridad como una tarea institucional con sus responsabilidades y políticas asociadas, sistemas de control y monitoreo, y mejora (ISO/IEC, 2022a). El Marco de Ciberseguridad NIST 2.0 incluye seis funciones para la gestión de la ciberseguridad: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. Estas funciones permiten que flujos de trabajo de tareas de nivel inferior se conecten con los procesos de toma de decisiones de la alta dirección (NIST, 2024).

### *2.2.1 Principios de confidencialidad, integridad y disponibilidad*

La confidencialidad se refiere a la disponibilidad de la información para usuarios/sistemas/procesos autorizados. En una cooperativa de ahorro y crédito, la confidencialidad consiste en mantener seguros credenciales, datos personales, información financiera, datos de los miembros, archivos de crédito, transacciones y documentos internos. Fallar en esto conduce a la exposición de datos, aumenta la probabilidad de fraude, pérdida de confianza y genera un riesgo de acción legal.

La integridad garantiza que la información permanezca en su estado original y no sea manipulada. En el sistema financiero, modificaciones incorrectas de balances, asientos contables, límites de crédito y registros de auditoría pueden afectar la confiabilidad de los procesos hasta el punto de que se vuelvan disfuncionales. La integridad de un sistema financiero puede protegerse mediante la inclusión de validaciones, huellas de auditoría, registros de actividad y sistemas de cambio controlado.

La disponibilidad significa que los sistemas y los datos estén accesibles cuando los usuarios autorizados los necesiten. Esto se vuelve crítico para canales digitales, cajeros automáticos, aplicaciones móviles y sistemas transaccionales, ya que una interrupción puede afectar el servicio a los miembros, la continuidad operativa y de servicio, así como la imagen de la institución. ISO/IEC 27002:2022 incluye una serie de controles relacionados con la gestión de acceso, la copia de seguridad y la continuidad. También incluye controles para proteger contra malware y para asegurar la red, así como los controles de monitorización y respuesta. (ISO/IEC, 2022).

### *2.2.2 Ciberseguridad como gestión institucional del riesgo*

La ciberseguridad también abarca la gestión. Entre otras cosas, la gestión de la ciberseguridad implica identificar activos clave, amenazas y riesgos. La gestión de la ciberseguridad también implica evaluar los impactos de varias vulnerabilidades y controles existentes, así como el nivel aceptable de riesgo. Una vez que la dirección haya priorizado los recursos de la cooperativa, los esfuerzos de mitigación pueden dirigirse a los activos que respaldan los procesos comerciales clave de la cooperativa.

Esta gobernanza se ve afectada por las pruebas de penetración porque proporcionan evidencia sobre la efectividad real de los controles. La evidencia de servicios expuestos,

credenciales débiles, configuraciones inseguras y controles de autorización deficientes debe salir del ámbito puramente técnico. Debe abordarse como riesgo, control correctivo, parte responsable, plazo de remediación y verificación de la remediación. Este proceso está en línea con lo descrito en ISO/IEC 27005:2022, donde activos, amenazas, vulnerabilidades, impacto potencial y probabilidad de riesgo se relacionan con el control de riesgo (ISO/IEC, 2022c).

### 2.3 Pentesting o pruebas de penetración

Pruebas de penetración, o pentesting en corto, es una metodología estructurada para evaluar la seguridad de un sistema al intentar deliberadamente romperlo como lo haría un atacante real, pero de manera controlada y legal. La intención es identificar vulnerabilidades explotables, entender los activos en riesgo y proporcionar sugerencias para mitigarlas. Esto es más avanzado que un escaneo automatizado de vulnerabilidades, ya que implica análisis de contexto, comprobaciones manuales y documentación de evidencia con una evaluación del impacto.

Recientemente, la literatura sugiere que el pentesting combina herramientas automatizadas con conocimiento técnico. Es importante saber que existen herramientas que automatizarán el análisis y las pruebas, y estas herramientas difieren en cómo manejan la precisión, la cobertura y los falsos positivos, mientras que Altulaihan et al. (2023) Argumentan que las pruebas de penetración se utilizan para evaluar la seguridad dentro de los servicios de aplicaciones web para la autenticación, la autorización, la gestión de sesiones, la validación y otras configuraciones inseguras. Dichas pruebas son necesarias para los sistemas financieros, ya que los hallazgos deben interpretarse de acuerdo con los efectos operativos y regulatorios.

### *2.3.1 Definición e importancia del pentesting*

La prueba de penetración significa intentar explotar una vulnerabilidad bajo circunstancias controladas. Esta prueba es vital debido a que las herramientas automatizadas tienden a generar falsos positivos. También devuelve configuraciones que no tienen impacto real en el mundo real, e incluso pueden no identificar fallos de la lógica de negocio. Esto conduce a una gran lista de vulnerabilidades identificadas. Las pruebas priorizan y evalúan los riesgos en función del impacto potencial que una vulnerabilidad podría tener en la SCA (Confidencialidad, Integridad y Disponibilidad del Sistema) de los sistemas. Es decir, una vez más las pruebas se convierten en la forma segura y protegida de proteger los sistemas y reducir la exposición de las vulnerabilidades.

(Alhogail & Alkahtani, 2024) señalan que la automatización puede apoyar la recolección de información y el análisis inicial de vulnerabilidades, pero la confirmación del impacto requiere validación técnica. Del mismo modo, Lazarov et al. (2025) plantean que los procedimientos de pentesting se fortalecen cuando se documentan mediante listas de verificación adaptables que permiten combinar pruebas manuales y automatizadas. Estos aportes respaldan la necesidad de una ejecución ordenada, documentada y verificable para la Cooperativa Yuyay Ltda.

### *2.3.2 Tipos de pruebas de penetración*

Las pruebas de penetración pueden clasificarse según el nivel de conocimiento que tiene el evaluador sobre el sistema. Esta clasificación permite definir el alcance, el tipo de evidencia esperada y el grado de realismo frente a posibles escenarios de ataque.

**Tabla 1**

*Tipos de pruebas de penetración según el nivel de conocimiento*

| Tipo de prueba | Descripción | Aplicabilidad en la tesis |
|---|---|---|
| Caja negra | El evaluador no cuenta con información interna previa y actúa desde una perspectiva similar a un atacante externo. | Útil para medir la exposición pública de servicios, dominios, direcciones IP, portales y configuraciones visibles. |
| Caja gris | El evaluador posee información parcial, como credenciales de usuario común, arquitectura general o alcance limitado. | Adecuada para simular usuarios internos o socios con privilegios restringidos, especialmente en aplicaciones web y servicios autenticados. |
| Caja blanca | El evaluador cuenta con información amplia del sistema, código, diagramas, credenciales o documentación técnica. | Útil cuando la cooperativa autoriza una revisión profunda de arquitectura, configuración, permisos y controles internos. |

*Nota.* Elaboración propia con base en Altulaihan et al. (2023) , Alhogail et al. (2024) y Lazarov et al. (2025).

Además de esta clasificación, el pentesting puede dividirse por objetivo: infraestructura de red, aplicaciones web, APIs, aplicaciones móviles, servicios en la nube, configuraciones de servidores, dispositivos de red o ingeniería social autorizada. Para esta investigación, el tipo de prueba debe seleccionarse en función del alcance formalmente aprobado por la cooperativa, la criticidad de los activos y las restricciones operativas establecidas para no afectar servicios en producción.

### *2.3.3 Fases generales del pentesting*

Una prueba de penetración debe ejecutarse mediante fases ordenadas que garanticen trazabilidad, control, autorización y utilidad de los resultados. A partir de la literatura reciente, puede estructurarse en siete fases: definición del alcance, reconocimiento, análisis de vulnerabilidades, explotación controlada, análisis de impacto, reporte y reprueba o retest (Alhogail & Alkahtani, 2024).

- Definición de alcance y reglas de compromiso: identifica activos autorizados, límites, horarios, técnicas permitidas, responsables, canales de comunicación y criterios de interrupción.
- Reconocimiento y recolección de información: recopila datos sobre dominios, direcciones IP, tecnologías, servicios, versiones, certificados, cuentas y posibles puntos de entrada.
- Análisis de vulnerabilidades: utiliza herramientas para examinar debilidades técnicas y configura de forma insegura servicios y aplicaciones, expone servicios y fallas de la aplicación.
- Explotación controlada: examina si una vulnerabilidad puede ser explotada para acceder, elevar privilegios, eludir controles o filtrar información. Esto se hace dentro de los límites y permisos de un alcance definido.
- Análisis de impacto: mide el posible impacto de una violación sin modificar la información real. Este análisis no interrumpe las operaciones comerciales.
- El documento debe incluir lo siguiente: descripción de la evidencia, criticidad del hallazgo, impacto, pasos para reproducir, controles recomendados y propietarios sugeridos y prioridad de tratamiento.
- Reprobar o retest: confirmar si las acciones correctivas eliminaron o redujeron el riesgo

### *2.3.4 Reglas de compromiso, autorización y ética*

Las pruebas de penetración en el sector financiero deben incluir una documentación exhaustiva de ética y legalidad. Las pruebas solo pueden realizarse tras la aprobación de los altos ejecutivos de la institución correspondiente, con la provisión de activos, un cronograma claro y personal especificado asignado al seguimiento. Esto es cierto en el sector financiero porque una prueba

descontrolada puede provocar registros alterados o perdidos, interrupciones del servicio, exposición de datos privados o incluso interrupciones del servicio.

Las reglas de compromiso deben describir los límites de la prueba, específicamente qué direcciones IP están dentro del alcance, qué sistemas quedan fuera del alcance, los métodos permitidos de prueba y ataque, y los límites impuestos a la prueba y al ataque. Las pruebas deben estar respaldadas por evidencia controlada, y una definición de hallazgos críticos documentada junto con un procedimiento para terminar las pruebas fuera de alcance debe describirse. Por último, la protección de datos sensibles, las capturas, la eliminación de artefactos y la confidencialidad del informe final deben protegerse. Estos principios reflejan la responsabilidad y seguridad proporcionadas en la Ley Orgánica de Protección de Datos Personales y su Reglamento (ASAMBLEA NACIONAL, 2021).

En la Cooperativa Yuyay Ltda., estas reglas son necesarias para proteger la continuidad del servicio financiero y cumplir obligaciones de confidencialidad. El evaluador debe evitar acciones destructivas, denegación de servicio, modificación de registros reales, extracción innecesaria de datos, persistencia no autorizada o explotación fuera del alcance aprobado. La evidencia debe limitarse a demostrar la existencia del riesgo sin comprometer información de socios o afectar operaciones.

### *2.3.5 Producto esperado de una prueba de penetración*

El resultado de un pentesting debe presentarse mediante un informe con dos niveles de lectura. El primero corresponde al resumen ejecutivo, dirigido a gerencia y órganos de control, donde se explican los riesgos principales, activos afectados, nivel general de exposición y prioridades de mitigación. El segundo corresponde al detalle técnico, dirigido al área de

tecnología, donde se incluyen evidencias, pasos de reproducción, impacto, severidad, referencias técnicas y recomendaciones específicas.

Cada hallazgo debe incluir un identificador, activo afectado, descripción de la vulnerabilidad, evidencia, impacto, probabilidad, severidad según lo descrito por CVSS, confidencialidad, integridad y disponibilidad, mitigación recomendada, control propuesto, propietario del control sugerido, tiempo para responder y criterios de verificación. Usar esta plantilla le ayudaría a proporcionar un informe que pueda convertirse fácilmente en salida para tratamiento del riesgo y mejora de controles institucionales (ISO/IEC, 2022).

### *2.3.6 Selección metodológica para la tesis*

Se utiliza un enfoque metodológico integrado en esta investigación. NIST SP 800-115 en general estructura el marco técnico en fases de planificación, descubrimiento, ataque organizado y reporte. La guía OWASP Web Security Testing Guide y la guía OWASP API Security Top 10 orientan las pruebas para aplicaciones web y API. PTES proporciona apoyo conceptual para redactar reglas de compromiso, explotación de controles concisa y reporte de problemas técnicos.

Esta selección tiene importancia para una cooperativa financiera porque permite pruebas autorizadas, reproducibles y no destructivas. Los hallazgos de esta manera pueden convertirse en insumos de riesgo mediante CVSS v4.0, ISO/IEC 27005:2022 y MAGERIT. En consecuencia, lo que queda del pentesting es el uso de herramientas, mientras que la evaluación y el tratamiento institucional del riesgo se integran con este proceso.

## 2.4 Vulnerabilidades y amenazas en sistemas de información

Las vulnerabilidades se refieren a preocupaciones del sistema, configuración, proceso o prácticas que, cuando son atacadas por una amenaza, resultan en un incidente de seguridad. Las

vulnerabilidades de los sistemas financieros se encuentran en aplicaciones web y APIs, bases de datos, redes, servidores, estaciones de trabajo, claves de API y credenciales de acceso, proveedores de servicios de respaldo, así como servicios ofrecidos y políticas de control de acceso, y procesos comerciales.

Flor-Unda et al. (2023) según ellos, la baja conciencia de ciberseguridad, el software desactualizado, la falta de normas e infraestructura, y la escasez de capacitación especializada, son problemas continuos en los países de América Latina. Estos temas sugieren que la falta de seguridad en un sistema no puede atribuirse a una escasez de tecnología. Más bien, depende de una combinación del proceso, el personal y la cultura de la organización y su disposición a actualizar y supervisar el sistema.

### *2.4.1 Vulnerabilidades en aplicaciones web*

Las aplicaciones web representan un punto de exposición significativo porque permiten la interacción entre los usuarios y los servicios y datos institucionales. Entre las vulnerabilidades más relevantes se encuentran fallos de control de acceso, errores de configuración, inyección, fallas criptográficas, autenticación deficiente, diseño inseguro, integridad deficiente de software o datos, registros insuficientes y manejo inadecuado de excepciones. OWASP Top 10:2025 presenta una actualización de riesgos críticos para aplicaciones web con base en tendencias y datos recientes de seguridad (OWASP Foundation, 2025).

Para una cooperativa financiera, una falla web puede permitir acceso no autorizado a información de socios, manipulación de solicitudes, exposición de datos, secuestro de sesión o alteración de parámetros. Por ello, el análisis web debe considerar autenticación, autorización, gestión de sesiones, validación de entradas, controles de cifrado, manejo de errores,

configuración de cabeceras HTTP, archivos expuestos, lógica de negocio y dependencias vulnerables.

### *2.4.2 Vulnerabilidades en APIs*

Las APIs permiten conectar aplicaciones móviles, portales web, sistemas internos y servicios de terceros. Sin embargo, también amplían la superficie de ataque, especialmente cuando exponen identificadores de objetos, endpoints no documentados, versiones antiguas, mecanismos de autenticación débiles o controles de autorización insuficientes. OWASP API Security Top 10 2023 ubica la autorización rota a nivel de objeto como uno de los riesgos más críticos en APIs, debido a que muchas interfaces permiten acceder a recursos mediante identificadores sin validar adecuadamente el permiso del usuario (OWASP Foundation, 2023).

En un entorno financiero, una vulnerabilidad de API puede permitir consultar datos de otro socio, alterar solicitudes, manipular parámetros, enumerar cuentas, consumir recursos de forma abusiva o acceder a funciones administrativas. Por tanto, si la cooperativa utiliza APIs internas o externas, el pentesting debe evaluar autorización por objeto, autenticación, exposición excesiva de datos, limitación de tasa, inventario de endpoints, controles de roles y validación de entradas.

### *2.4.3 Vulnerabilidades en infraestructura de red*

La infraestructura de red incluye servidores, routers, switches, firewalls, enlaces, servicios, puertos, protocolos, VPN, sistemas de administración remota y mecanismos de monitoreo. Las vulnerabilidades en este entorno pueden estar asociadas con servicios innecesarios, puertos abiertos sin justificación, credenciales predeterminadas, versiones obsoletas, administración remota expuesta, falta de segmentación, protocolos inseguros, ausencia de cifrado o monitoreo insuficiente.

MITRE ATT&CK mantiene una matriz de tácticas y técnicas utilizadas por adversarios en entornos empresariales. Los tipos de comportamiento como reconocimiento, acceso inicial, ejecución, persistencia, escalamiento de privilegios, evasión defensiva, acceso a credenciales, movimiento lateral, exfiltración e impacto son algunos de los comportamientos para los cuales los hallazgos técnicos pueden estar relacionados (MITRE Corporation, 2026). Esta relación mejora la interpretación de los hallazgos de pentesting porque permite vincular una debilidad técnica con escenarios de ataque y controles defensivos.

### *2.4.4 Ingeniería social y factor humano*

El factor humano continúa siendo uno de los elementos más sensibles de la seguridad informática. La ingeniería social busca manipular a usuarios o personal interno para obtener credenciales, información o acceso a sistemas. En entidades financieras, estas técnicas pueden presentarse mediante correos fraudulentos, llamadas falsas, mensajes de suplantación, enlaces maliciosos o solicitudes engañosas relacionadas con servicios institucionales.

Este estudio analiza las pruebas de penetración técnicas específicamente; sin embargo, el elemento humano/usuario debe integrarse en estas recomendaciones, ya que muchas brechas implican tanto fallos técnicos como errores de usuario. Por ello, las medidas de mitigación pueden incluir capacitación, autenticación multifactor, políticas de contraseñas, verificación de solicitudes, bloqueo de dominios maliciosos y procedimientos de reporte de incidentes. La norma ecuatoriana de seguridad de la información para el Sector Financiero Popular y Solidario también contempla responsabilidades, formación y gestión de eventos como parte de la seguridad institucional (SEPS, 2022).

### *2.4.5 Priorización de vulnerabilidades*

No todas las vulnerabilidades tienen el mismo impacto ni requieren el mismo nivel de urgencia. La priorización debe depender del impacto en la confidencialidad, integridad y disponibilidad, la facilidad de explotación, la exposición al público, la asignación de recursos y la criticidad de los activos. Un sistema crítico puede justificar prioridad si una vulnerabilidad de severidad media resulta en la pérdida de control sobre datos financieros o sobre operaciones de procesos críticos del sistema.

CWE ayuda a detallar las debilidades de una aplicación de software, así como la causa raíz de problemas recurrentes. Algunas de estas incluyen inyección, control de acceso insuficiente, validación de entrada inadecuada o inexistente, o manejo inseguro de datos. La lista MITRE 2025 proporciona un buen punto de partida para determinar debilidades persistentes en el software. Ayuda a mejorar un informe de pruebas de penetración al proporcionar recomendaciones más sustanciales para resolver una vulnerabilidad particular, en lugar de simplemente evitar una única instancia (MITRE Corporation, 2025).

## 2.5 Gestión de vulnerabilidades y valoración del riesgo

Las pruebas de penetración deben formar parte de un proceso de gestión de vulnerabilidades. Las vulnerabilidades encontradas deben ser documentadas. Esto también implica evaluar la vulnerabilidad, determinar su prioridad y clasificarla adecuadamente, así como responder para remediar la vulnerabilidad y verificar la respuesta. El objetivo es cerrar el hallazgo y continuar reduciendo la exposición técnica de la cooperativa.

La gestión de vulnerabilidades debe estar estrechamente vinculada a la evaluación de riesgos. Un hallazgo técnico representa una debilidad. CSVE, en combinación con el contexto de

la Cooperativa, se utiliza para evaluar la gravedad del hallazgo técnico. En cuanto a la matriz de riesgo institucional, esto determina el impacto y la probabilidad en el contexto de la Cooperativa, y los controles de seguridad determinan la respuesta. Esta integración permite que la evaluación técnica aporte información valiosa a las decisiones de seguridad y cumplimiento.

### *2.5.1 CVSS v4.0 como criterio de severidad técnica*

CVSS v4.0 ofrece un enfoque sistemático para la expresión del nivel de severidad de una vulnerabilidad mediante un conjunto de métricas base, de amenaza, ambientales y complementarias. (FIRST, 2023) señala que las métricas de amenaza y ambientales permiten ajustar la puntuación según inteligencia de amenazas y condiciones del entorno. Entender cómo afecta una vulnerabilidad a la cooperativa es esencial al analizar la criticidad de un activo, la exposición del sistema y cuánto impactaría una vulnerabilidad a la institución.

CVSS es un punto de partida al considerar la matriz de riesgos de la organización. En relación con el ejemplo, una vulnerabilidad de grado crítico expuesta al servicio de Internet puede requerir una remediación inmediata, mientras que una vulnerabilidad de grado crítico similar en un sistema cerrado puede abordarse en un momento posterior. Por lo tanto, la tesis debería usar CVSS para el dominio técnico de la severidad y ISO/IEC 27005:2022 para la transformación de esa severidad en riesgo institucional.

### *2.5.2 CISA KEV, CWE y MITRE ATT&CK como criterios de complementarios*

La priorización puede mejorarse con fuentes relacionadas con la explotación que ocurre en el mundo real, patrones de debilidades y técnicas de los atacantes. Las vulnerabilidades que han sido explotadas se rastrean en el catálogo de Vulnerabilidades Conocidas Explotadas por CISA, y el catálogo se actualiza. Esto permite encontrar las vulnerabilidades que han sido

explotadas en el mundo real y aumentar la prioridad para corregir un activo expuesto y/o crítico (CISA, 2026).

CWE y ATT&CK usan enfoques diferentes en el análisis y la descripción de debilidades de software. CWE ayuda en la clasificación de debilidades de software y ATT&CK describe cómo una debilidad puede incorporarse en una cadena de ataque. CVSS, KEV, CWE y ATT&CK brindan al informe técnico la opción de ir más allá de la puntuación para describir la causa raíz y describir formas conocidas de explotar una variante y el posible impacto en las operaciones (FIRST, 2023).

### *2.5.3 ISO/IEC 27005:2022 para valoración del riesgo*

ISO/IEC 27005:2022 proporciona información sobre el control de los riesgos de la seguridad de la información y la creación de un sistema de gestión de la seguridad de la información que está de acuerdo con ISO/IEC 27001. En este estudio, ISO/IEC 27005 se utiliza como metodología de evaluación principal, ya que se encuentra dentro del marco temporal requerido y ayuda a relacionar activos, amenazas, vulnerabilidades, impacto, probabilidad y remediación (ISO/IEC, 2022c).

El Capítulo II distingue dos niveles para evitar contradicciones metodológicas. Las pruebas de penetración enumeran y validan vulnerabilidades técnicas. La gestión de riesgos es el paso subsiguiente y ubica esas vulnerabilidades en función del valor de los activos, el impacto, la probabilidad y los controles compensatorios. El resultado no es solo una lista de vulnerabilidades técnicas. Más bien, es una matriz de riesgos que muestra las acciones de remediación que se priorizan.

### *2.5.4 Riesgo inherente, controles y riesgo residual*

El riesgo inherente es lo que queda después de que no se han considerado los controles o salvaguardas. El riesgo residual es el riesgo que permanece después de que se han implementado los controles. Definir estos conceptos ayuda a explicar si las medidas propuestas para la cooperativa serían efectivas.

Para los fines de la tesis, cada hallazgo ha sido mapeado a un activo, amenaza, vulnerabilidad, impacto, probabilidad, control existente, control recomendado y riesgo residual esperado. Esta estructura facilita elaborar una matriz de tratamiento coherente con la gestión institucional de riesgos y con la norma ecuatoriana de administración del riesgo operativo (SEPS, 2024).

**Tabla 2**

*Relación entre hallazgo técnico, severidad y tratamiento del riesgo*

| Elemento | Función dentro del Pentesting | Resultado esperado |
|---|---|---|
| Hallazgo de pentesting | Describe una vulnerabilidad validada sobre un activo específico. | Evidencia técnica y descripción del impacto potencial. |
| CVSS v4.0 | Clasifica la severidad técnica de la vulnerabilidad. | Puntuación, vector y nivel de severidad. |
| CISA KEV / CWE / ATT&CK | Complementan la priorización con explotación activa, causa raíz y técnicas de ataque. | Criterio adicional de urgencia y explicación del escenario de amenaza. |
| ISO/IEC 27005:2022 | Valora el riesgo institucional considerando activos, amenazas, vulnerabilidades, impacto y probabilidad. | Matriz de riesgo inherente y residual. |
| ISO/IEC 27002 / SEPS | Orienta controles, políticas y medidas de tratamiento. | Plan de mitigación, responsables, plazos y verificación. |

*Nota.* Elaboración propia con base en (FIRST, 2023).

### *2.5.5 Articulación con MAGERIT para el tratamiento del riesgo*

MAGERIT se incorpora como metodología operativa para estructurar el análisis y tratamiento de riesgos en los capítulos metodológicos y de propuesta. Su uso permite organizar

activos, amenazas, salvaguardas, impacto, probabilidad y riesgo residual, manteniendo trazabilidad entre los hallazgos técnicos del pentesting y las decisiones de mitigación.

ISO/IEC 27005:2022 es mi marco de referencia para la gestión de riesgos de seguridad de la información, mientras que MAGERIT me ayuda a construir matrices, valorar activos y definir controles. Ambos enfoques son complementarios, ya que ISO/IEC 27005 proporciona orientación y dirección para el análisis, mientras que MAGERIT aporta herramientas y técnicas a un nivel más práctico para asistir en el análisis del estudio de caso.

## 2.6 Normativa y estándares aplicables

Pruebas de penetración, a fin de realizar una evaluación de seguridad, requieren que los estándares y métodos utilizados para el proceso estén organizados para evitar establecer tiempos extremadamente ajustados. Este estudio utiliza normas internacionales para la seguridad de la información, referencias de vulnerabilidad y marcos de gestión de riesgos, así como regulaciones de Ecuador que son aplicables a las cooperativas financieras.

### *2.6.1 Ley Orgánica de Protección de Datos Personales y su Reglamento*

La Ley Orgánica de Protección de Datos Personales del Ecuador, publicada en el Registro Oficial No. 459, Quinto Suplemento, de 26 de mayo de 2021, establece obligaciones relacionadas con el tratamiento de datos personales. Para una cooperativa de ahorro y crédito, esta ley es relevante porque la entidad gestiona información personal, financiera, contractual y transaccional de sus socios (ASAMBLEA NACIONAL, 2021).

El Reglamento General a la Ley Orgánica de Protección de Datos Personales desarrolla medidas técnicas y organizativas relacionadas con seguridad, responsabilidad y tratamiento de datos. En la tesis, esta normativa justifica la necesidad de proteger la confidencialidad de los

datos, restringir accesos no autorizados, documentar controles y evitar que las pruebas de pentesting expongan información real de socios (Presidencia de la Republica, 2023).

### *2.6.2 Normativa SEPS sobre seguridad de la Información*

La Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 expide la norma de control respecto a la seguridad de la información en entidades del Sector Financiero Popular y Solidario. Esta regulación es directamente pertinente porque la Cooperativa Yuyay Ltda. pertenece al ámbito de supervisión de la SEPS (SEPS, 2022).

La norma exige que las entidades gestionen la seguridad de la información mediante políticas, procesos, procedimientos, roles, responsabilidades, asignación de recursos, formación, registro de eventos y controles. Además, contempla responsabilidades del Comité de Seguridad de la Información, del Gerente General, del Oficial de Seguridad de la Información y de Auditoría Interna. Por ello, los hallazgos del pentesting deben vincularse con la administración formal de la seguridad de la información y con el seguimiento de riesgos.

### *2.6.3 Normativa SEPS sobre canales electrónicos*

La norma de control de seguridades en el uso de canales electrónicos para entidades financieras controladas por la SEPS regula medidas mínimas de seguridad para servicios prestados mediante canales electrónicos. Esta norma es relevante cuando la cooperativa utiliza banca móvil, banca en línea, cajeros automáticos, billeteras digitales, tarjetas u otros canales tecnológicos (SEPS, 2023).

Dentro del pentesting, esta normativa permite justificar la evaluación de autenticación, autorización, cifrado, monitoreo, registro de actividad, parches, controles contra suplantación, seguridad de aplicaciones y protección de información transmitida o almacenada en servicios digitales.

### *2.6.4 Normativa SEPS sobre riesgo operativo*

La Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116 establece la norma de control para la administración del riesgo operativo en entidades del Sector Financiero Popular y Solidario. Su objeto es normar la administración de riesgo operativo para una adecuada administración integral de riesgos (SEPS, 2024).

En la tesis, esta normativa permite relacionar los hallazgos de pentesting con riesgos operacionales. Un ejemplo de una vulnerabilidad de disponibilidad puede relacionarse con una amenaza a la continuidad del negocio. Una exposición de credenciales puede relacionarse con riesgo tecnológico o de fraude. Una falta de monitoreo puede relacionarse con un fallo tanto de detección como de respuesta.

### *2.6.5 Estándares ISO/IEC 27001, 27002, 27005 y 27035*

ISO/IEC 27001:2022 establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Tu enfoque permite vincular hallazgos de pentesing a la estructura de gobernanza de una institución en lugar de solo acciones técnicas aisladas a nivel individual (ISO/IEC, 2022a).

ISO/IEC 27002:2022 proporciona controles de seguridad de la información, ciberseguridad y privacidad. En relación con las pruebas de penetración, ayuda a traducir los hallazgos técnicos en controles como gestión de identidad, autenticación, endurecimiento de la configuración, protección contra malware, gestión de registros, gestión de vulnerabilidades, copias de seguridad y aseguramiento de la continuidad operativa (ISO/IEC, 2022).

ISO/IEC 27005:2022 ayuda a la gestión de riesgos de seguridad de la información. Su inclusión también ayuda a evaluar contribuciones en el contexto de activos, amenazas, vulnerabilidades, impactos y probabilidad. ISO/IEC 27035-1:2023 proporciona criterios

estandarizados de gestión de incidentes de seguridad. Este estándar es pertinente cuando uno de los hallazgos críticos de pruebas de penetración requiere procesos de registro, evaluación, respuesta, aprendizaje y mejora (ISO/IEC, 2023).

### *2.6.6 NIST Cybersecurity Framework 2.0*

La versión actualizada del Marco de Ciberseguridad del NIST, Ciberseguridad Marco 2.0, incorpora la visión de gestión de riesgos técnicos y de gobernanza. Sus funciones ayudan a asociar los resultados de pruebas de penetración con las decisiones de control institucional sobre la gobernanza de la seguridad, la identificación de activos y riesgos, la protección de sistemas, la detección de eventos, la respuesta a incidentes y la restauración de la capacidad operativa (NIST, 2024) muestra que el marco permite a las organizaciones comprender, evaluar, clasificar y comunicar las amenazas cibernéticas.

Para Cooperativa Yuyay Ltda., este marco ayudará a que la evaluación técnica vaya más allá del dominio tecnológico. Los hallazgos deben comunicarse a los ejecutivos y deben priorizarse en función del impacto que tendrían. Los hallazgos relevantes también deben utilizarse para mejorar la sincronización de los procesos institucionales, la continuidad de las operaciones y el cumplimiento de la ley.

### *2.6.7 OWASP Top 10 y OWASP API Security Top 10*

OWASP Top 10:2025 sirve como un documento de concienciación sobre riesgos críticos en problemas de aplicaciones web. En esta tesis, permite clasificar los hallazgos por problemas de control de acceso, fallos de inyección, implementación ambigua de operaciones criptográficas, diseño deficiente de la aplicación y de la implementación, configuración insegura de la aplicación, problemas con la identificación y autenticación de usuarios, falta de integridad en el software y problemas de monitoreo (OWASP Foundation, 2025).

El Top 10 de Seguridad de API de OWASP 2023 destaca algunos problemas de seguridad comunes en las API. Estos problemas incluyen autorización a nivel de objeto rota, autenticación débil, sobrecompartir datos y falta de restricción para el consumo de recursos e inventario de API. Puede usar este documento si su cooperativa utiliza servicios API para integrar aplicaciones móviles, portales de usuarios, sistemas internos y/o servicios externos. (OWASP Foundation, 2023).

## 2.7 Herramientas y técnicas para la evaluación de seguridad

Las herramientas de pruebas de penetración simplifican las pruebas de penetración. Tareas como reconocimiento, escaneo, análisis de vulnerabilidades, explotación, examen del tráfico y documentación de informes se vuelven automatizadas. Dado que el objetivo de una prueba de penetración es proporcionar una evaluación general, un marco metodológico debe preceder a la implementación de las herramientas. Los resultados deben ser analizados y las áreas vulnerables deben ser confirmadas. Por último, debe determinarse el orden de importancia de las vulnerabilidades. Esto requiere tanto competencia técnica como el contexto de la institución.

### *2.7.1 Reconocimiento y escaneo*

Reconocimiento es el procedimiento de recopilación de datos realizado antes de las pruebas reales. Esta etapa implica hallar objetivos, que podrían ser subdominios, dominios, direcciones IP, tecnologías utilizadas, certificados, servicios expuestos y datos publicados, y posibles puntos de acceso. En pruebas de penetración autorizadas, el reconocimiento debe cumplir con el marco acordado con el cliente y, por lo tanto, excluir técnicas no aprobadas y ser menos intrusivo.

En el escaneo, usamos herramientas para comprobar si los hosts están activos, si hay puertos abiertos, qué servicios están ejecutándose, qué versiones están instaladas y si existen configuraciones inseguras. En las cooperativas financieras, estos escaneos deben organizarse dentro de marcos de tiempo aprobados y con restricciones para evitar impactos negativos en servicios vitales. La evidencia de Albahar et al. (2022) los niveles de detección y precisión de las herramientas varían. Por lo tanto, deben ser validados antes de que puedan incluirse en el informe final.

### *2.7.2 Análisis de vulnerabilidades*

Varias herramientas, como escáneres de red y escáneres web, pueden ayudar con algunas formas de análisis de vulnerabilidades. Por ejemplo, estas herramientas ayudan a localizar configuraciones inseguras y componentes HTML que carecen de encabezados necesarios. La falta de autenticación y la exposición de datos a espectadores no autenticados también pueden ser identificadas con estas herramientas. Sin embargo, los resultados deben ser examinados con cuidado para filtrar falsos positivos y examinar el efecto real.

Alhogail et al. (2024) afirma que automatizar el proceso de descubrimiento acorta el tiempo que la automatización tarda, pero la evaluación y el análisis de impacto de la explotación requieren criterios técnicos. Por lo tanto, la tesis debe distinguir entre la detección automatizada de vulnerabilidades y las vulnerabilidades verificadas producidas mediante procesos de prueba establecidos.

### *2.7.3 Explotación Controlada*

El propósito de la explotación controlada es determinar si una vulnerabilidad sospechada podría aprovecharse para comprometer un sistema, dentro de los límites permitidos. Este proceso debe ser breve, estar documentado y centrarse exclusivamente en la verificación del impacto. En

una cooperativa financiera, no se deben realizar pruebas destructivas, denegación de servicio, manipulación de datos reales, persistencia no aprobada o extracción de datos innecesarios.

Esta fase se llevará a cabo con las siguientes restricciones adicionales: una copia de seguridad (cuando corresponda) realizada antes de esta fase, supervisión por el área tecnológica, una ventana de pruebas definida, un plan de reversión y un canal de comunicación para detener la prueba si se detecta degradación del servicio. Estas restricciones incorporan la protección de datos personales y la gestión del riesgo operativo y la continuidad de las operaciones. (ASAMBLEA NACIONAL, 2021).

### *2.7.4 Reporte y tratamiento de hallazgos*

El informe debe ser comprensible para múltiples audiencias, verificable y útil para diversas audiencias. La dirección requiere un resumen ejecutivo de riesgos y prioridades. El área técnica requiere evidencia, pasos para reproducir y acciones correctivas. El área de riesgo requiere impacto, probabilidad, controles y riesgo residual. La trazabilidad de cada hallazgo también respalda a la cooperativa en corregir el hallazgo y verificar su solución.

Los hallazgos deben relacionarse con los controles en ISO/IEC 27002:2022 y con los deberes definidos en SEPS. Esto permitiría que tipos de hallazgos, como autenticación débil, sin cifrado, servicios expuestos, sin monitoreo, se traduzcan en acciones definidas con una persona responsable, fecha objetivo, prioridad y evidencia de cierre (ISO/IEC, 2022), (SEPS, 2022).

## 2.8 Comparación de normas, metodologías y marcos aplicables

Esta tabla muestra cómo se relacionan los marcos revisados con la tesis. Muestra cómo evitar contradicciones metodológicas significa que las pruebas de penetración identifican y verifican vulnerabilidades, mientras que CVSS, CISA KEV, CWE, MITRE ATT&CK, ISO/IEC

27005, MAGERIT, ISO/IEC 27002 y la regulación SEPS proporcionan medios para clasificar, contextualizar y abordar los riesgos.

**Tabla 3**

*Cuadro comparativo de normas, marcos y referencias aplicables al estudio*

| Marco, norma o referencia | Enfoque principal | Fases, funciones o componentes aplicables | Uso dentro del Pentesting | Producto esperado |
|---|---|---|---|---|
| NIST CSF 2.0 | Gobernanza y gestión de riesgos de ciberseguridad. | **Gobernar, identificar, proteger, detectar, responder y recuperar.** Estas funciones se desarrollan de manera continua y no constituyen necesariamente una secuencia lineal. | Relacionar los hallazgos técnicos con las funciones de gobernar, identificar, proteger, detectar, responder y recuperar. | Mapa de relación entre hallazgos y decisiones institucionales. |
| ISO/IEC 27001:2022 | Sistema de Gestión de Seguridad de la Información. | **Contexto de la organización, liderazgo, planificación, apoyo, operación, evaluación del desempeño y mejora.** Estos componentes corresponden a las cláusulas 4 a 10 del SGSI. | Ubicar el pentesting como evidencia para la evaluación y mejora continua del SGSI. | Brechas de seguridad y acciones de mejora continua. |
| ISO/IEC 27002:2022 | Controles de seguridad de la información, ciberseguridad y privacidad. | No establece fases. Organiza sus controles en cuatro grupos: **organizacionales, de personas, físicos y tecnológicos**. Para el pentesting se aplican mediante la selección, evaluación, recomendación y verificación de controles. | Traducir los hallazgos en controles técnicos y administrativos. | Controles recomendados para mitigar vulnerabilidades. |
| ISO/IEC 27005:2022 | Gestión de riesgos de seguridad de la información. | **Establecimiento del contexto; identificación, análisis y evaluación del riesgo; tratamiento y aceptación del riesgo; comunicación y consulta; seguimiento y revisión.** | Valorar los hallazgos según activos, amenazas, vulnerabilidades, impacto, probabilidad y controles existentes. | Matriz de riesgo inherente y residual. |
| ISO/IEC 27035-1:2023 | Gestión de incidentes de seguridad de la información. | **Planificar y preparar; detectar y reportar; evaluar y decidir; responder; y aprender lecciones.** | Orientar la preparación, respuesta y aprendizaje institucional ante hallazgos críticos que puedan convertirse en incidentes. | Criterios de registro, escalamiento, respuesta y mejora. |
| OWASP Top 10:2025 | Riesgos críticos en aplicaciones web. | No define fases metodológicas. Se aplica mediante la **identificación y validación de vulnerabilidades, clasificación en las categorías A01–** | Clasificar los hallazgos web y comunicar los | Categorías de riesgo web asociadas con evidencias técnicas. |

| Marco, norma o referencia | Enfoque principal | Fases, funciones o componentes aplicables | Uso dentro del Pentesting | Producto esperado |
|---|---|---|---|---|
| | | **A10, análisis de impacto, recomendación de mitigaciones y revalidación**. | riesgos de seguridad de las aplicaciones. | |
| OWASP API Security Top 10 2023 | Riesgos críticos en interfaces de programación de aplicaciones. | No establece fases. Se emplea mediante el **descubrimiento e inventario de APIs, evaluación de autenticación y autorización, validación de flujos y consumo de recursos, revisión de configuración, mitigación y nueva prueba**. | Evaluar autorización, autenticación, exposición de datos, consumo de recursos, flujos sensibles e inventario de APIs. | Hallazgos de seguridad de APIs clasificados y priorizados. |
| CVSS v4.0 | Puntuación técnica de severidad de vulnerabilidades. | No posee fases. Comprende cuatro grupos de métricas: **Base, Amenaza, Entorno y Suplementarias**. Su aplicación incluye la selección de métricas, generación del vector, cálculo de la puntuación y contextualización del resultado. | Asignar una severidad técnica y contextual a las vulnerabilidades validadas. | Puntuación, vector CVSS y nivel de severidad. |
| CISA KEV | Catálogo de vulnerabilidades explotadas activamente. | No constituye una metodología por fases. Su utilización comprende la **consulta del catálogo, verificación de aplicabilidad, comprobación de exposición, priorización urgente, remediación o mitigación y validación del cierre**. | Aumentar la prioridad de las vulnerabilidades que poseen evidencia confirmada de explotación activa. | Criterio de urgencia y plazo recomendado de remediación. |
| CWE Top 25 | Debilidades de software recurrentes y peligrosas. | No define fases. Se utiliza mediante la **identificación de la debilidad, mapeo al identificador CWE, análisis de la causa raíz, definición de medidas preventivas y verificación de la corrección**. | Identificar la causa raíz de las vulnerabilidades encontradas en aplicaciones y componentes de software. | Recomendaciones preventivas por tipo de debilidad. |
| MITRE ATT&CK | Tácticas y técnicas utilizadas por adversarios. | Sus componentes son las tácticas de **reconocimiento, desarrollo de recursos, acceso inicial, ejecución, persistencia, escalamiento de privilegios, evasión de defensas, acceso a credenciales, descubrimiento, movimiento lateral, recopilación, comando y control, exfiltración e impacto**. No representan obligatoriamente una secuencia lineal. | Vincular los hallazgos con posibles comportamientos, objetivos y técnicas de un atacante. | Escenarios de amenaza, rutas de ataque y controles defensivos. |
| Normativa SEPS y LOPDP | Obligaciones ecuatorianas relacionadas con seguridad de la información, protección de datos personales, canales electrónicos y riesgo operativo. | No conforman una metodología única por fases. Para el estudio pueden organizarse en: **gobernanza y cumplimiento; inventario y clasificación de activos y datos; evaluación de riesgos; implementación de controles; operación segura de canales; gestión y notificación de incidentes; continuidad; auditoría y mejora**. | Contextualizar legal y regulatoriamente el pentesting ejecutado en una cooperativa financiera ecuatoriana. | Recomendaciones compatibles con el marco regulatorio ecuatoriano y las obligaciones de protección de datos. |

| Marco, norma o referencia | Enfoque principal | Fases, funciones o componentes aplicables | Uso dentro del Pentesting | Producto esperado |
|---|---|---|---|---|
| MAGERIT v3 | Metodología de análisis y gestión de riesgos de los sistemas de información. | Se estructura en tres procesos: **P1: planificación del análisis y gestión de riesgos; P2: análisis de riesgos**, incluyendo activos, amenazas, salvaguardas, impactos y estimación del riesgo; y **P3: gestión de riesgos**, que comprende evaluación, tratamiento, aceptación y seguimiento. | Operacionalizar la valoración de activos, amenazas, salvaguardas, impacto, probabilidad y riesgo residual en el caso de estudio. | Matrices de riesgo y plan de tratamiento coherentes con los hallazgos de pentesting. |

Elaboración propia con base en (ASAMBLEA NACIONAL, 2021), (CISA, 2026), (FIRST, 2023)

## 2.9 Síntesis del marco teórico aplicado al estudio

El marco teórico desarrollado permite sustentar la evaluación de la seguridad informática de la Cooperativa de Ahorro y Crédito Yuyay Ltda. desde un enfoque integrado y actualizado.

Esta sección describe las contribuciones recientes en la validación y documentación automatizadas de la recopilación de evidencias para las pruebas de aplicaciones web y APIs. Para la clasificación de vulnerabilidades técnicas, se integra CVSS v4.0 y, en ausencia de CISA KEV, se utiliza como criterio para la trayectoria de la explotación activa de las vulnerabilidades.

La gestión de riesgos se basa en ISO/IEC 27005:2022 y la metodología MAGERIT para estructurar matrices de activos, amenazas, controles, impacto, probabilidad de ocurrencia y el nivel de riesgo residual. Por último, las ISOT y la Ley Orgánica de Protección de Datos Personales, y las normas SEPS sobre seguridad de la información, canales electrónicos y riesgo operacional, proporcionan un marco para formular recomendaciones de controles, políticas y planes de acción para la mejora de una cooperativa financiera ecuatoriana.

De esta forma, el Capítulo II cumple el objetivo general de la tesis, ya que describe cómo el pentesting identifica vulnerabilidades, cómo estas vulnerabilidades se convierten en riesgos y

cómo dichos riesgos pueden abordarse mediante controles técnicos, administrativos y regulatorios. El enfoque en las fuentes en los años 2021 a 2026 fortalece la base teórica del estudio y elimina la necesidad de depender de referencias antiguas en apoyo de la metodología principal.

# CAPÍTULO III

## MARCO METODOLÓGICO

### 3.1 Enfoque de la investigación

Se utilizaron métodos mixtos para analizar la postura de seguridad de los sistemas de información de la Cooperativa de Ahorro y Crédito Yuyay Ltda., y evaluar las vulnerabilidades identificadas mediante pruebas de penetración. El análisis cualitativo proporciona comprensión del estado de los controles y políticas, y la exposición de los activos de la organización, mientras que el análisis cuantitativo permite evaluar la severidad de las vulnerabilidades y una estimación del riesgo.

La combinación de ambos componentes se justifica porque una prueba de penetración no debe limitarse a entregar una lista de fallos técnicos. Al integrar el valor de los activos, el impacto sobre la confidencialidad, integridad y disponibilidad, los controles existentes y los resultados de las herramientas empleadas, el juicio técnico sobre la exposición de cada activo se sustenta en evidencia verificable. De esta forma, la cooperativa obtiene un diagnóstico fundamentado que le permite priorizar el tratamiento de los riesgos y tomar decisiones informadas sobre su seguridad.

El análisis no se realizó en el entorno de producción, sino en un servidor de réplica proporcionado por la cooperativa, lo que garantizó la continuidad del servicio y protegió los datos de los socios frente a cualquier afectación derivada de las pruebas. Además, la evaluación se enmarca en la modalidad de caja gris, ya que se dispuso de información parcial y de permisos de acceso limitados, pero no de un acceso total a los sistemas. Esta condición permite simular tanto un ataque externo como el de un usuario interno con privilegios restringidos.

### 3.2 Nivel de la investigación

La investigación es de nivel descriptivo–aplicado. Es descriptiva porque busca caracterizar el estado actual de la seguridad informática de los sistemas de la Cooperativa de Ahorro y Crédito Yuyay Ltda., identificando activos, servicios expuestos, configuraciones y vulnerabilidades presentes en los sistemas evaluados. Es aplicada porque no se limita a describir el fenómeno, sino que utiliza metodologías estructuradas de pruebas de penetración para intervenir de manera controlada sobre un caso concreto, con el propósito de identificar debilidades reales, evaluar los riesgos derivados y proponer recomendaciones de mejora ajustadas al contexto institucional.

Este nivel es coherente con el objetivo general del estudio, orientado a evaluar la seguridad de la información mediante técnicas de pentesting basadas en modelos ampliamente adoptados, con el fin de identificar debilidades, valorar riesgos y ofrecer recomendaciones para optimizar la protección de los sistemas.

### 3.3 Diseño de la investigación

El estudio corresponde a un diseño no experimental, transversal y de campo, aplicado bajo la modalidad de estudio de caso sobre la Cooperativa de Ahorro y Crédito Yuyay Ltda. Es no experimental porque no se manipulan deliberadamente variables independientes con fines de contraste estadístico; en su lugar, se evalúan los sistemas sobre un servidor de réplica que reproduce fielmente la configuración del entorno de producción, tal como se encuentra instalado y en funcionamiento. Es transversal porque la recolección de datos se realiza en un momento determinado, correspondiente a la ventana autorizada de ejecución de las pruebas. Es de campo porque la información se obtiene directamente de la infraestructura tecnológica facilitada por la institución mediante técnicas controladas de reconocimiento, análisis y explotación.

La modalidad de estudio de caso se justifica porque el pentesting se ejecuta sobre un contexto único y delimitado, cuyos hallazgos deben interpretarse en relación con las características, restricciones y activos específicos de la cooperativa, sin pretender generalizar los resultados a otras entidades.

### 3.4 Entorno de pruebas y laboratorio

Las pruebas se llevan a cabo sobre un entorno de laboratorio controlado y aislado, con el objetivo de evitar cualquier afectación a los sistemas en producción de la cooperativa y a la información de sus socios. El objetivo de evaluación (target) corresponde a un servidor de réplica proporcionado por la institución, que reproduce la configuración, versiones de software y datos representativos del entorno de producción.

Como estación de trabajo del investigador (máquina atacante) se emplea un equipo con sistema operativo Windows 11 Home, procesador de arquitectura de 64 bits, 32 GB de memoria RAM y almacenamiento en unidad de estado sólido (SSD) de 1 Tera, sobre el cual se virtualiza la distribución Kali Linux mediante un hipervisor, por contener está el conjunto de herramientas especializadas de pruebas de penetración. La comunicación entre la máquina atacante y el servidor de réplica se realiza dentro de un segmento de red aislado, definido en las reglas de compromiso, con el fin de garantizar el control y la trazabilidad de todo el tráfico generado durante las pruebas.

### 3.4 Métodos de investigación

Para el desarrollo del estudio se emplean los siguientes métodos, que orientan tanto el tratamiento teórico como la ejecución técnica de la evaluación de seguridad:

- **Método analítico–sintético:** se utiliza para descomponer los sistemas de información en sus componentes (activos, servicios, aplicaciones web, APIs e infraestructura de red) y,

posteriormente, integrar los hallazgos individuales en una valoración global del nivel de exposición de la cooperativa.

- **Método deductivo–inductivo:** permite partir de los marcos y estándares generales de seguridad (NIST SP 800-115, OWASP, PTES, ISO/IEC 27005) para derivar procedimientos y casos de prueba específicos aplicables al contexto de la institución, y a la vez inferir conclusiones generales sobre la postura de seguridad a partir de las evidencias particulares obtenidas.
- **Método bibliográfico-documental**: se utiliza en la fase documental para revisar regulaciones, normas, literatura publicada recientemente y buenas prácticas para ayudar en la selección metodológica e interpretación de los resultados.
- **Método empírico-técnico (aplicado al entorno de prueba controlado):** describe cómo se realizan los pasos de pruebas de penetración mediante la observación del comportamiento del sistema y el registro sistemático de pruebas obtenidas en pruebas controladas realizadas en el entorno réplica sin manipulación del entorno con el fin de hacer inferencias estadísticas.

### 3.5 Población y muestra

La población de estudio está constituida por el conjunto de sistemas de información y activos tecnológicos de la Cooperativa de Ahorro y Crédito Yuyay Ltda. que soportan sus operaciones y servicios digitales, incluidos aplicaciones, servidores, equipos de red, canales electrónicos y servicios expuestos.

Dado el carácter técnico y delimitado de las pruebas de penetración, se aplicó un muestreo no probabilístico intencional. La muestra estuvo constituida específicamente por el servidor de réplica proporcionado por la cooperativa, que reproduce la configuración, las

versiones de software y los datos representativos del entorno de producción. Este servidor aloja los activos autorizados para la evaluación: el sitio web institucional, la aplicación de marcación y los servicios e infraestructura de red asociados. Estos activos fueron seleccionados por su importancia para los procesos de la institución y por su inclusión formal en las reglas de compromiso. Como la selección responde a criterios técnicos y a la autorización de la cooperativa, y no a un procedimiento aleatorio, los resultados deben interpretarse únicamente para el caso estudiado y no pueden generalizarse a otras cooperativas.

Con base al alcance de la autorización otorgada por la cooperativa, la muestra consiste en: la aplicación móvil de la cooperativa y sus servicios API, la aplicación de informes de contabilidad en malla, el sitio institucional y los servicios e infraestructura de red. Todo esto se aloja en el servidor de réplica.

### 3.6 Tipo de muestreo

Se utiliza una muestra juiciosa y la selección de los activos evaluados se realiza intencionalmente (juicio del investigador). No se seleccionan activos al azar. Basado en la importancia crucial del sistema para la cooperativa, el nivel de exposición y dada la autorización de la organización (autorizante) para incluirlos dentro del alcance de la prueba de penetración, se seleccionan estos sistemas.

Este tipo de muestreo es coherente con la naturaleza aplicada del estudio y con las restricciones de confidencialidad y continuidad operativa propias de una entidad financiera.

### 3.7 Criterios de inclusión y exclusión

Para delimitar los activos que forman parte de la evaluación se definen los siguientes criterios:

**Criterios de inclusión:**

- Sistemas de información y activos tecnológicos actualmente instalados y en funcionamiento en la cooperativa.
- Activos autorizados formalmente por la institución dentro de las reglas de compromiso del pentesting.
- Servicios, aplicaciones web, APIs e infraestructura de red relevantes para la seguridad de la información institucional.

**Criterios de exclusión:**

- Sistemas o servicios no autorizados expresamente por la cooperativa para su evaluación.
- Activos de terceros o servicios tercerizados sobre los cuales la institución no tenga autorización para permitir pruebas.
- Sistemas cuya evaluación pueda comprometer la continuidad operativa o la información sensible de los socios sin controles adecuados.
- Propuestas de nuevos sistemas o soluciones, dado que el estudio se limita al análisis de los sistemas existentes.

### 3.8 Técnicas e instrumentos de recolección de datos

La recolección de datos se realiza combinando técnicas documentales, técnicas de campo y observación estructurada, con el fin de obtener información suficiente sobre el estado de la seguridad de los sistemas evaluados. Las técnicas e instrumentos empleados se describen a continuación:

- **Análisis documental:** revisión de normativa, estándares, políticas internas de la cooperativa y documentación técnica de los sistemas, con apoyo de fichas bibliográficas y matrices de análisis.

- **Entrevista:** aplicada al personal responsable del área de tecnología para el levantamiento de información sobre los sistemas, la arquitectura y los controles existentes, mediante una guía de entrevista estructurada.
- **Observación estructurada:** registro sistemático del comportamiento de los sistemas durante la ejecución de las pruebas, apoyado en listas de verificación derivadas de OWASP y NIST SP 800-115 y en el registro de evidencias técnicas.
- **Pruebas de penetración:** ejecución controlada de reconocimiento, análisis de vulnerabilidades y explotación mediante herramientas especializadas, cuyos resultados constituyen la principal fuente de datos cuantitativos del estudio.

Como instrumentos técnicos se utilizan las herramientas Nmap para el reconocimiento y escaneo de red; Nessus Essentials (u OpenVAS/Greenbone como alternativa de código abierto) para el análisis automatizado de vulnerabilidades; y Metasploit Framework para la explotación controlada. Para la evaluación de un sitio web institucional y sus API, se utilizan Burp Suite y OWASP ZAP, así como Nikto y sqlmap para pruebas especializadas, basadas en OWASP Web Security Testing Guide (WSTG) y OWASP Top 10. Para la app, se ha utilizado Mobile Security Framework (MobSF) tanto para el análisis estático como dinámico del APK, con el apoyo de OWASP Mobile Application Security Testing Guide (MASTG). Las pruebas se ejecutan en un host de virtualización y se utiliza Kali Linux como distribución especializada para pruebas de penetración. Los resultados se documentan en logs de brechas, capturas, logs de hallazgos y matrices de registro, que permiten clasificar y evaluar los registros.

### 3.9 Procedimiento de la investigación

Cada fase del enfoque secuencial general para la evaluación integrada de la seguridad se basa en la metodología iterativa. Para la implementación técnica, las metodologías NIST

SP 800-115, OWASP, PTES siguen una secuencia. Para la evaluación y tratamiento de riesgos, las metodologías ISO/IEC 27005:2022 y MAGERIT siguen una secuencia. Las fases son las siguientes:

- **Fase 1. Estudio documental y regulatorio:** revisión del marco regulatorio y normas aplicables, identificación de las políticas de seguridad de la cooperativa y selección justificada del marco metodológico de pentesting más adecuado para el contexto institucional.

  Esta fase del estudio implica una revisión de las regulaciones aplicables a la Superintendencia de Economía Popular y Solidaria (SEPS). Esta fase incluye la revisión de las normas de SEPS sobre controles de seguridad en el uso de canales electrónicos y la normativa de seguridad de la información del sector financiero popular y solidario, así como la Ley Orgánica de Protección de Datos (LOPDP) y su Reglamento. Así, para cada uno de los hallazgos técnicos, se compara una norma internacional y las regulaciones a las que la institución está legalmente obligada a implementar. De este modo, es posible determinar el grado de cumplimiento de la normativa y ofrecer recomendaciones para el estudio.
- **Fase 2. Levantamiento y definición del alcance:** levantamiento de información sobre los sistemas de la cooperativa, identificación de activos y arquitectura, y definición del alcance del pentesting junto con las reglas de compromiso, activos autorizados, horarios y límites de las pruebas.
- **Fase 3. Ejecución del pentesting:** recolección de información mediante footprinting y scanning, análisis de vulnerabilidades con herramientas especializadas y explotación

controlada de las debilidades identificadas, sin afectar la continuidad operativa de la institución.

- **Fase 4. Evaluación de resultados y análisis de riesgos:** clasificación de las vulnerabilidades según su criticidad, evaluación del impacto sobre los sistemas y elaboración de la matriz de riesgos, vinculando los hallazgos técnicos con la valoración de activos, amenazas, impacto y probabilidad.
- **Fase 5. Preparación de la propuesta de mejora:** generar sugerencias de mitigación y diseñar políticas y directrices de seguridad para abordar el riesgo no resuelto de los sistemas evaluados.

### 3.10 Validación de los instrumentos

Metodología de recopilación de datos que debe recoger datos relevantes para el resultado del estudio. La evidencia relevante para los objetivos del estudio se determina mediante la validez de contenido. Esto lo realizan expertos que revisan la relevancia de las guías utilizadas para realizar las entrevistas y de las listas de verificación utilizadas para las pruebas.

Las máquinas utilizadas para realizar el estudio se evalúan para determinar si pueden o no ser utilizadas para recoger datos relevantes del estudio. Las máquinas se evalúan con base en las normas y marcos desarrollados internacionalmente (NIST SP 800-115, OWASP, PTES) y luego se confirma manualmente eliminando falsos positivos para verificar que la vulnerabilidad reportada por las máquinas es una debilidad explotable real y controlada.

### 3.11 Confiabilidad de los instrumentos

La confiabilidad se logra estandarizando los métodos de prueba y rastreando la evidencia. Los resultados serán consistentes y verificables con el uso de listas de verificación uniformes, el registro sistemático de cada hallazgo y la documentación de los pasos para reproducir los

hallazgos. CVSS v4.0 es un marco establecido para calificar la severidad técnica y, por lo tanto, proporciona criterios que contribuyen a la reproducibilidad de esta evaluación también.

La confiabilidad del proceso se mejora al realizar una nueva verificación o retest de las vulnerabilidades abordadas para verificar la consistencia de los resultados y la eficacia de la remediación.

### 3.12 Técnicas de procesamiento y análisis de datos

Los datos cuantitativos de vulnerabilidad se procesan mediante la combinación del análisis de la vulnerabilidad y su impacto en la institución. Cada hallazgo se registra, se valida y se califica en función de su importancia mediante la técnica de criticidad. Para la evaluación cualitativa, el nivel técnico de importancia se aborda a través del marco de CVSS v4.0; cuando es necesario, también se utilizan los criterios de CISA KEV como indicador de la explotación activa actual.

Los hallazgos se incorporan a una matriz de riesgo como recurso de apoyo, utilizando el marco de ISO/IEC 27005:2022, junto con la metodología de MAGERIT. La combinación de los recursos permite evaluar los activos, las amenazas, las vulnerabilidades y su impacto, así como la probabilidad y abordar los riesgos inherentes y los riesgos residuales. Los resultados se comunican a través de tablas de priorización, y matrices, y presentaciones de visualización de riesgos (dibujos) junto con recomendaciones explicadas para las acciones correctivas adecuadas.

### 3.13 Operacionalización de variables

A partir del problema planteado y los objetivos del estudio, la variable independiente se considera la evaluación de la seguridad de la información mediante pruebas de penetración y la variable dependiente es el nivel de seguridad de la información de los sistemas de Cooperativa de Ahorro y Crédito Yuyay Ltda. La siguiente tabla ilustra la operacionalización.

**Tabla 4**

*Operacionalización de variables*

| Variable | Definición conceptual | Dimensiones | Indicadores | Técnica / Instrumento |
|---|---|---|---|---|
| Variable independiente: Evaluación de la seguridad informática mediante pentesting | Proceso técnico que simula ataques controlados para identificar y validar vulnerabilidades en los sistemas de información. | Reconocimiento; Análisis de vulnerabilidades; Explotación controlada; Reporte | N.º de activos y servicios identificados; N.º de vulnerabilidades detectadas; N.º de vulnerabilidades explotadas; N.º de hallazgos documentados | Pruebas de penetración; Nmap. |
| Variable dependiente: Nivel de seguridad de la información de los sistemas | Grado en que los sistemas preservan la confidencialidad, integridad y disponibilidad de la información institucional. | Confidencialidad; Integridad; Disponibilidad; Nivel de riesgo | Severidad CVSS por hallazgo; nivel de criticidad de activos; riesgo inherente; riesgo residual; nivel de cumplimiento de los controles exigidos por la normativa SEPS | Clasificación CVSS v4.0; matriz de riesgos ISO/IEC 27005 – MAGERIT |

*Nota*. Elaboración propia con base en los objetivos de la investigación.

### 3.14 Consideraciones éticas

La investigación cumple con las normas legales y éticas necesarias concernant pruebas de penetración en situaciones del mundo real. No se realizan experimentos sin la aprobación por escrito de las autoridades pertinentes. Los activos incluidos deben estar especificados. Se debe proporcionar un cronograma aprobado y se debe identificar a una persona responsable de supervisar la prueba y acordarlo por las partes cooperantes.

En la fase de pruebas, se pueden ejecutar ataques que resulten en pérdida de datos, denegación de acceso o servicio, o modificación de datos. No se debe extraer datos innecesarios y las pruebas no deben extenderse más allá del alcance acordado. Se recopilan evidencias para demostrar la existencia del riesgo, pero no deben comprometer los datos o servicios de los socios. La Ley 15/2001, la Ley Orgánica de Protección de Datos y su Reglamento, y las normas de la Superintendencia de Economía Popular y Solidaria destinadas a la protección de datos sensibles y a la evidencia, y para garantizar la confidencialidad en el informe final, son aplicables.

En última instancia, los resultados se utilizan únicamente para el objetivo de estudios sin que datos sensibles se hagan públicamente disponibles, y asegurando la eliminación de archivos temporales dejados como resultado de las pruebas.

# CAPÍTULO IV

# PROPUESTA

## 4.1 Introducción

El presente capítulo expone la propuesta de la investigación, entendida como la ejecución del procedimiento definido en la sección 3.9 del Capítulo III y la traducción de sus resultados en una valoración de riesgos y en un plan de tratamiento aplicable a la Cooperativa de Ahorro y Crédito Yuyay Ltda. En coherencia con el enfoque metodológico integrado, la ejecución técnica se ordena mediante NIST SP 800-115, OWASP y PTES, mientras que la valoración y el tratamiento del riesgo se estructuran con ISO/IEC 27005:2022 como marco de referencia y MAGERIT como metodología operativa.

El capítulo se organiza siguiendo las cinco fases secuenciales establecidas en el procedimiento de la investigación: (Fase 1) estudio documental y normativo; (Fase 2) levantamiento y definición del alcance; (Fase 3) ejecución del pentesting; (Fase 4) evaluación de resultados y análisis de riesgos; y (Fase 5) elaboración de la propuesta de mejora. Todas las pruebas se realizaron sobre un servidor de réplica proporcionado por la institución, que reproduce la configuración, versiones de software y datos representativos del entorno de producción, bajo la modalidad de caja gris y respetando las reglas de compromiso y las consideraciones éticas del Capítulo III.

**Tabla 5**

*Correspondencia entre las fases del procedimiento (sección 3.9) y las secciones del Capítulo IV*

| Fase | Descripción (según sección 3.9) | Sección del Capítulo IV |
|---|---|---|
| **Fase 1** | Estudio documental y normativo | 4.2 |
| **Fase 2** | Levantamiento y definición del alcance | 4.3 |
| **Fase 3** | Ejecución del pentesting | 4.4 |
| **Fase 4** | Evaluación de resultados y análisis de riesgos | 4.5 |
| **Fase 5** | Elaboración de la propuesta de mejora | 4.6 |

*Nota.* Elaboración propia.

### *4.1.1 Objetivo de la propuesta*

Identificar, validar y valorar las vulnerabilidades presentes en los sistemas de información autorizados de la Cooperativa de Ahorro y Crédito Yuyay Ltda. mediante la ejecución controlada de las fases de pentesting definidas en el Capítulo III, y formular un plan de tratamiento del riesgo basado en controles técnicos, administrativos y normativos que reduzca el riesgo residual y fortalezca la postura de seguridad institucional.

## 4.2 Fase 1. Estudio documental y normativo

La primera fase consistió en revisar el marco normativo y los estándares aplicables, analizar las políticas de seguridad de la cooperativa y seleccionar de forma justificada el marco metodológico de pentesting más adecuado para el contexto institucional. Esta fase da soporte al primer objetivo específico del estudio y establece los criterios con los que posteriormente se clasifican y contrastan los hallazgos.

La revisión normativa incorporó de manera específica las exigencias de la Superintendencia de Economía Popular y Solidaria (SEPS) aplicables a la cooperativa, en particular la Norma de Control de Seguridades en el Uso de Canales Electrónicos (SEPS, 2023) y la norma de control de seguridad de la información del sector financiero popular y solidario (SEPS, 2022). También incluyó la Ley Orgánica de Protección de Datos Personales (LOPDP) y su Reglamento. De este modo, cada hallazgo técnico puede contrastarse no solo con estándares internacionales, sino también con los controles que la institución está legalmente obligada a implementar.

En cuanto a la documentación interna, la cooperativa entregó diez documentos relacionados con la seguridad de la información: la política general de seguridad de la información; el inventario y la clasificación de activos de información; la metodología de gestión

de riesgos de seguridad; la política de control de accesos y gestión de usuarios; el procedimiento de respaldos y recuperación; el plan de continuidad del negocio o de recuperación ante desastres; el procedimiento de gestión de incidentes de seguridad; la política de protección de datos personales; la designación del oficial o responsable de seguridad de la información; y el plan de capacitación en seguridad. Cada documento se analizó con cuatro criterios: (a) existencia y aprobación formal por la instancia competente; (b) vigencia, según su fecha de emisión o de última actualización; (c) cobertura de los controles exigidos por la norma SEPS de seguridad de la información y por ISO/IEC 27002:2022; y (d) alineación con las obligaciones de la LOPDP. Según estos criterios, cada documento se calificó como *cumple*, *cumple parcialmente* o *no cumple*. La calificación de cada documento por criterio se registra en la Tabla 6 resume la norma de referencia y la brecha principal de cada uno.

**Tabla 6**

*Documentos internos revisados, norma de referencia y brecha principal*

| N.º | Documento interno | Norma de referencia | Brecha principal |
|---|---|---|---|
| 1 | Política general de seguridad de la información | Res. SEPS 2022-002 (políticas de seguridad); ISO/IEC 27002: 5.1 | Configuraciones inseguras por defecto en el servidor web (H-03, H-04, H-05) |
| 2 | Inventario y clasificación de activos de información | Res. SEPS 2022-002 (clasificación de la información); ISO/IEC 27002: 5.9, 5.12 | Servicio web adicional no gestionado en el puerto 8080 (H-06) |
| 3 | Metodología de gestión de riesgos de seguridad | Res. SEPS 2022-002 (gestión de riesgos); ISO/IEC 27005:2022 | Sin evidencia técnica directa |
| 4 | Política de control de accesos y gestión de usuarios | ISO/IEC 27002: 5.15, 5.16, 5.18, 8.2 | Base de datos expuesta en todas las interfaces (H-01) y servicios de Windows accesibles en la red (H-07) |
| 5 | Procedimiento de respaldos y recuperación | Res. SEPS 2022-002 (respaldos); ISO/IEC 27002: 8.13 | Sin evidencia técnica directa |
| 6 | Plan de continuidad del negocio / recuperación ante desastres | Res. SEPS 2022-002 (reporte inmediato de eventos que afecten la continuidad); ISO/IEC 27002: 5.29, 5.30 | Sin evidencia técnica directa |
| 7 | Procedimiento de gestión de incidentes de seguridad | Res. SEPS 2022-002 (reporte inmediato de eventos que afecten la continuidad); ISO/IEC 27002: 5.24 a 5.28 | Sin evidencia técnica directa |

| N.º | Documento interno | Norma de referencia | Brecha principal |
|---|---|---|---|
| 8 | Política de protección de datos personales | LOPDP, art. 47, num. 4; ISO/IEC 27002: 5.34 | Política de privacidad publicada que invoca la LOPDP (Cooperativa de Ahorro y Crédito Yuyay Ltda., s. f.), pero el servicio web opera sin cifrado (H-02) |
| 9 | Designación del oficial o responsable de seguridad de la información | Res. SEPS 2022-002 (Oficial de Seguridad de la Información, régimen general); ISO/IEC 27002: 5.2 | Sin evidencia técnica directa |
| 10 | Plan de capacitación en seguridad | Res. SEPS 2022-002 (concienciación y formación); ISO/IEC 27002: 6.3 | Sin evidencia técnica directa |

*Nota.* Elaboración propia con base en la documentación entregada por la cooperativa. La Cooperativa de Ahorro y Crédito Yuyay Ltda. pertenece al segmento 2 (SEPS, 2026), por lo que le corresponde el régimen general de la Resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002. Los números de control corresponden a ISO/IEC 27002:2022 (ISO/IEC, 2022b). Los códigos H-01 a H-07 remiten a los hallazgos técnicos de la Tabla 10.

Con base en esta revisión, se adoptó un esquema de trabajo que combina NIST SP 800-115, OWASP y PTES para ordenar la ejecución técnica; ISO/IEC 27005:2022 y MAGERIT para la valoración y el tratamiento del riesgo; y CVSS v4.0, complementado con CISA KEV cuando corresponde, para la clasificación de severidad. La Tabla 7 resume los marcos seleccionados y su función en la evaluación.

**Tabla 7**

*Marcos de referencia seleccionados y su función en la evaluación*

| Marco / norma | Función en la evaluación | Producto esperado |
|---|---|---|
| NIST SP 800-115 | Ordenar la ejecución técnica en planificación, descubrimiento, ataque controlado e informe | Secuencia de fases de prueba |
| OWASP (WSTG, Top 10, API Top 10) | Orientar las pruebas específicas sobre aplicaciones web y APIs | Hallazgos web/API clasificados |
| PTES | Documentar reglas de compromiso, explotación controlada y reporte | Trazabilidad del proceso |
| ISO/IEC 27005:2022 – MAGERIT | Valorar activos, amenazas, impacto, probabilidad y riesgo residual | Matriz de riesgos |
| CVSS v4.0 / CISA KEV | Asignar severidad técnica y priorizar por explotación activa | Severidad y prioridad |
| ISO/IEC 27002:2022; SEPS; LOPDP | Traducir los hallazgos en controles y verificar cumplimiento normativo | Controles y recomendaciones |

*Nota.* Elaboración propia.

### 4.3 Fase 2. Levantamiento y definición del alcance

La segunda fase comprendió el levantamiento de información sobre los sistemas de la cooperativa, la identificación de los activos y de la arquitectura, y la definición del alcance del pentesting junto con las reglas de compromiso, los activos autorizados, los horarios y los límites de las pruebas. Esta fase delimita con precisión qué se evalúa y bajo qué condiciones, en correspondencia con el enfoque de gestión de riesgos adoptado.

**Tabla 8**

*Configuración del entorno y alcance de las pruebas*

| Elemento | Descripción |
|---|---|
| **Máquina atacante** | Kali Linux (virtualizada), con Nmap 7.99, Gobuster 3.8.2, WhatWeb, Nikto 2.6.0, Burp Suite, OWASP ZAP, sqlmap, MobSF |
| **Objetivo (target)** | Servidor de réplica: sistema operativo Windows; direcciones observadas: 192.168.163.1 (host de réplica) y 192.168.10.179 (aplicación de marcación) |
| **Activos autorizados** | Página web institucional, aplicación de marcación, y servicios e infraestructura de red asociados, alojados en el servidor de réplica |
| **Segmento de red** | Red aislada de laboratorio; DNS inverso deshabilitado para evitar dependencias externas |
| **Modalidad** | Caja gris (gray box), con información parcial y credenciales limitadas facilitadas por la institución |
| **Reglas de compromiso** | Sin acciones destructivas, denegación de servicio ni extracción innecesaria de datos; ejecución en horario autorizado; evidencia fechada |
| **Repositorio de evidencias** | Directorio ~/yuyay/evidencias/, con salidas de herramientas y capturas para trazabilidad |

*Nota.* Elaboración propia.

Se implementaron límites para que la evaluación examinara el servidor web institucional, la aplicación de marcado y los servicios de red del servidor réplica. Esta evaluación no requería cambios en el entorno de producción ni en activos no autorizados.

### *4.3.1 Resultados de la entrevista*

La entrevista se aplicó el 05 de agosto de 2026 a cargo del Ing. Leonardo Verdugo, siguiendo la guía estructurada del Anexo 2. La información se organizó en cinco categorías, cuyos resultados se sintetizan en la Tabla 9

**Tabla 9**

*Síntesis de los resultados de la entrevista al responsable de tecnología*

| Categoría | Información obtenida | Uso en la evaluación |
|---|---|---|
| Sistemas, arquitectura y alcance | sistemas alojados, equivalencia con producción, segmento de red, modalidad y condiciones | Definición del alcance (Tabla 8); contraste con H-06 y H-07 |
| Gestión de accesos | política de contraseñas y uso de autenticación multifactor | Contraste con H-01 y H-07 |
| Cifrado y exposición de servicios | uso de HTTPS/TLS y restricción de acceso a la base de datos | Contraste con H-01, H-02 y H-04 |
| Actualizaciones y configuración segura | frecuencia de parches y procedimiento de configuración segura | Contraste con H-03, H-05 y H-06 |
| Políticas y cumplimiento | políticas aprobadas y sus fechas; evaluaciones previas | Contraste con el análisis documental (Tabla 6) |

*Nota.* Elaboración propia con base en la entrevista aplicada. Los códigos H-01 a H-07 remiten a los hallazgos técnicos de la Tabla 10.

## 4.4 Fase 3. Ejecución del pentesting

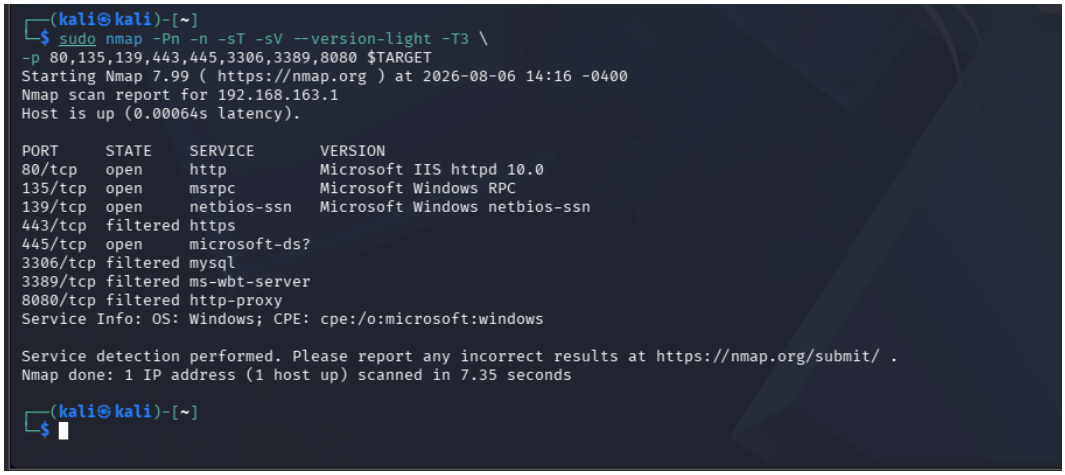
Esta fase del estudio se centró en la actividad técnica de recopilación de información, realizada mediante footprinting y escaneo, junto con el análisis de estos hallazgos para ayudar a identificar vulnerabilidades, y la explotación controlada de las vulnerabilidades encontradas, sin interrumpir las actividades comerciales habituales. Para cada actividad, se proporciona la evidencia y la herramienta utilizada. Esto se hace para garantizar la trazabilidad.

### *4.4.1 Reconocimiento y escaneo (footprinting y scanning)*

El reconocimiento comenzó con un barrido de descubrimiento de hosts en 192.168.10.0/24 con Nmap (nmap -sn). Posteriormente, se realizó un escaneo de puertos y servicios objetivo con detección de versiones en la réplica objetivo. El resultado del escaneo mostró que el objetivo era un sistema Windows con un servidor web Microsoft IIS 10.0 expuesto en el puerto 80. También mostró servicios de Windows, incluyendo MSRPC en el puerto 135, NetBIOS-SSN en el puerto 139 y microsoft-ds/SMB en el puerto 445. Durante el escaneo, se observó que los puertos 443, 3306, 3389 y 8080 estaban cerrados o filtrados en la red.

**Figura 1**

*Escaneo de puertos y detección de servicios sobre el objetivo (Nmap -sV)*



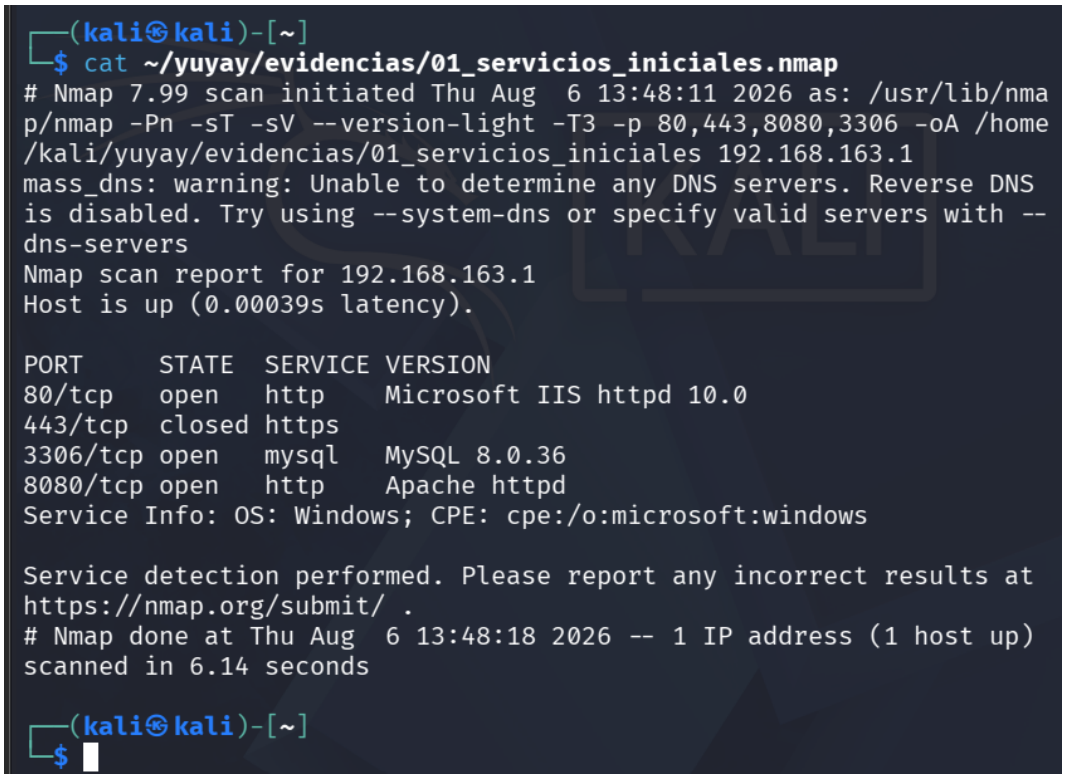

*Nota.* Elaboración propia.

Dentro de una ventana de reconocimiento dirigida previa, el mismo objetivo reportó una gama más amplia de servicios accesibles: además de IIS 10.0, se observaba un servidor MySQL dedicado en el puerto 3306 con la versión expuesta, y una segunda instancia del servidor web

Apache httpd en el puerto 8080. Tener la versión exacta del sistema de gestión de bases de datos en la exposición facilita la búsqueda de vulnerabilidades públicamente conocidas de esa versión.

**Figura 2**

*Detección de MySQL 8.0.36 y Apache httpd (8080) con versión expuesta*

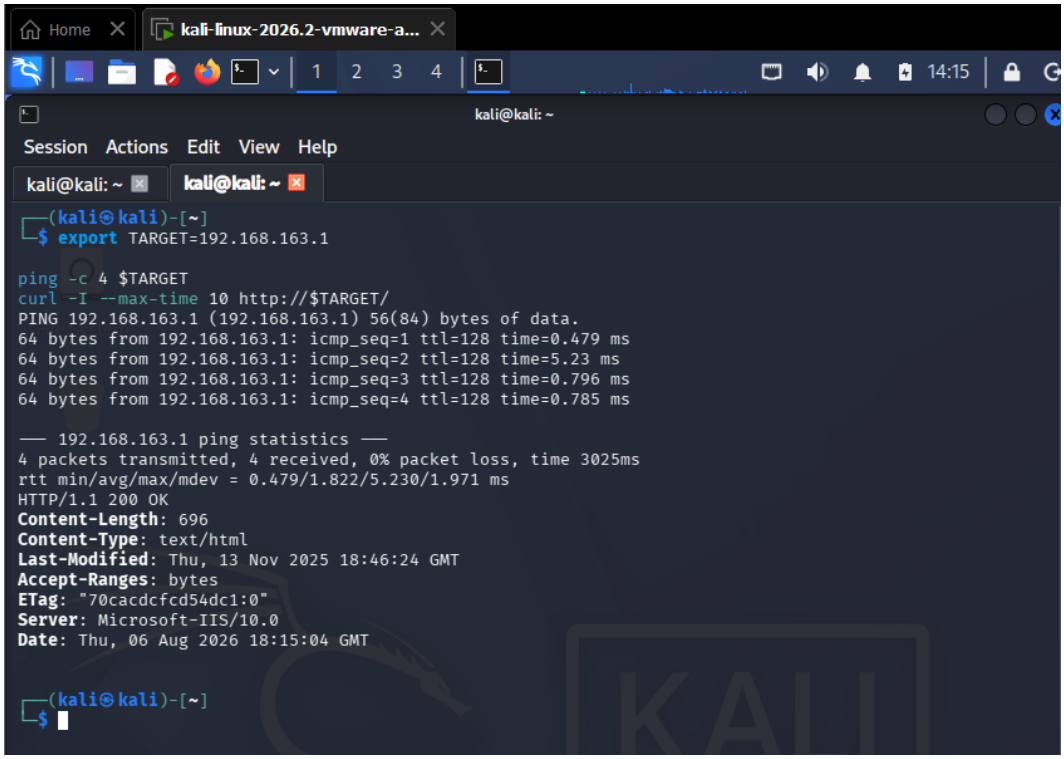



*Nota.* Elaboración propia.

Sobre el servicio HTTP se aplicaron técnicas de identificación de tecnologías y de enumeración de contenidos. La huella del servidor confirmó Microsoft-IIS/10.0 y la página por defecto de IIS, y la cabecera Server reveló de forma innecesaria el producto y la versión, lo que constituye una divulgación de información útil para un atacante.

**Figura 3**

*Divulgación del banner del servidor en las cabeceras HTTP (Server: Microsoft-IIS/10.0)*

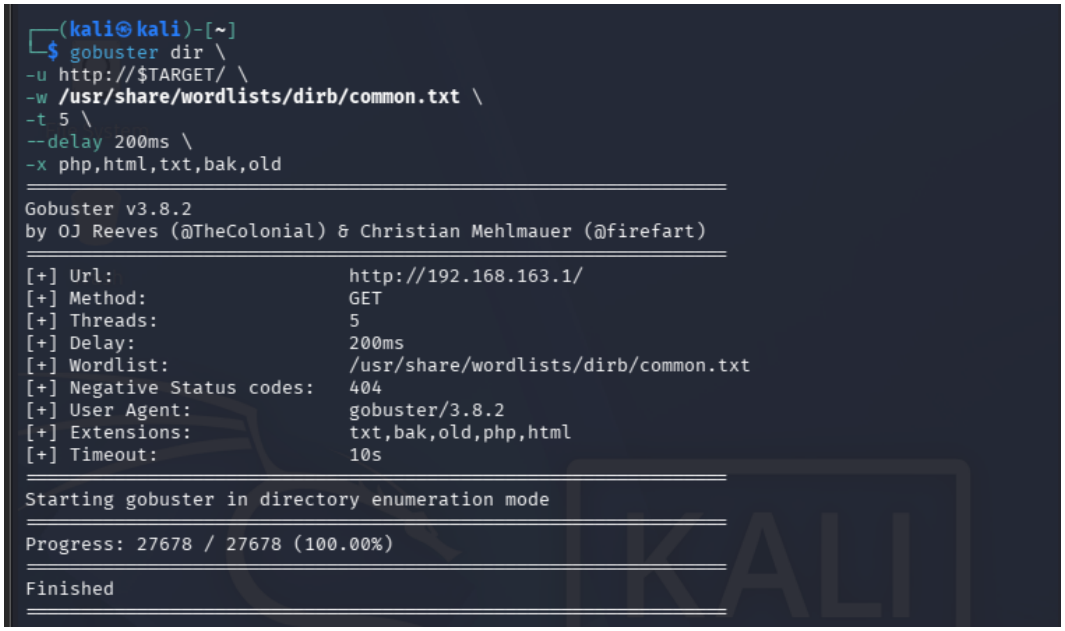



*Nota.* Elaboración propia.

La enumeración de directorios con Gobuster, empleando el diccionario común y las extensiones php, html, txt, bak y old, se ejecutó sobre la raíz del sitio y sobre la ruta /marcacion. El proceso de verificar las 27.678 entradas del diccionario no accedió a otros directorios o archivos sensibles. Esto se señaló como resultado de control.

**Figura 4**

*Enumeración de directorios finalizada sin hallazgos sensibles (control negativo)*



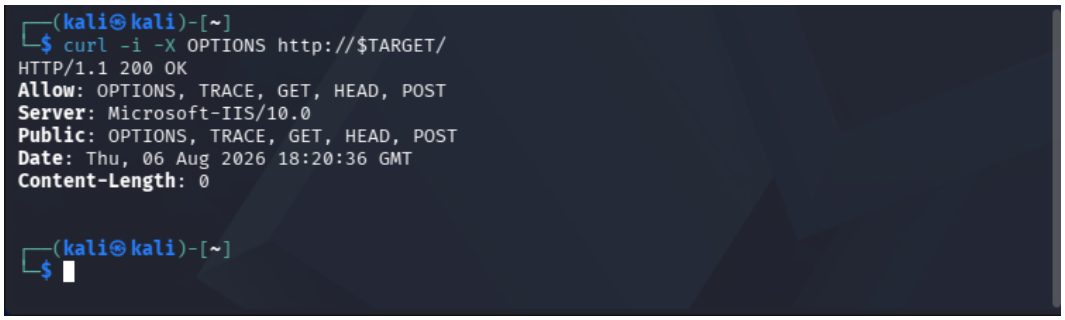

*Nota.* Elaboración propia.

### *4.4.2 Análisis de vulnerabilidades*

El análisis de vulnerabilidades combinó la ejecución de scripts de Nmap que se puede observar en el anexo 3 sobre el servicio HTTP con la verificación manual de configuraciones, diferenciando entre debilidades detectadas automáticamente y debilidades validadas. El método HTTP TRACE, junto con los métodos OPTIONS, GET, HEAD y POST, es motivo de preocupación porque habilitarlos puede permitir ataques de Cross-Site Tracing (XST) y no aporta ningún beneficio en producción.

**Figura 5**

*Método HTTP TRACE habilitado y divulgación de métodos permitidos vía OPTIONS*

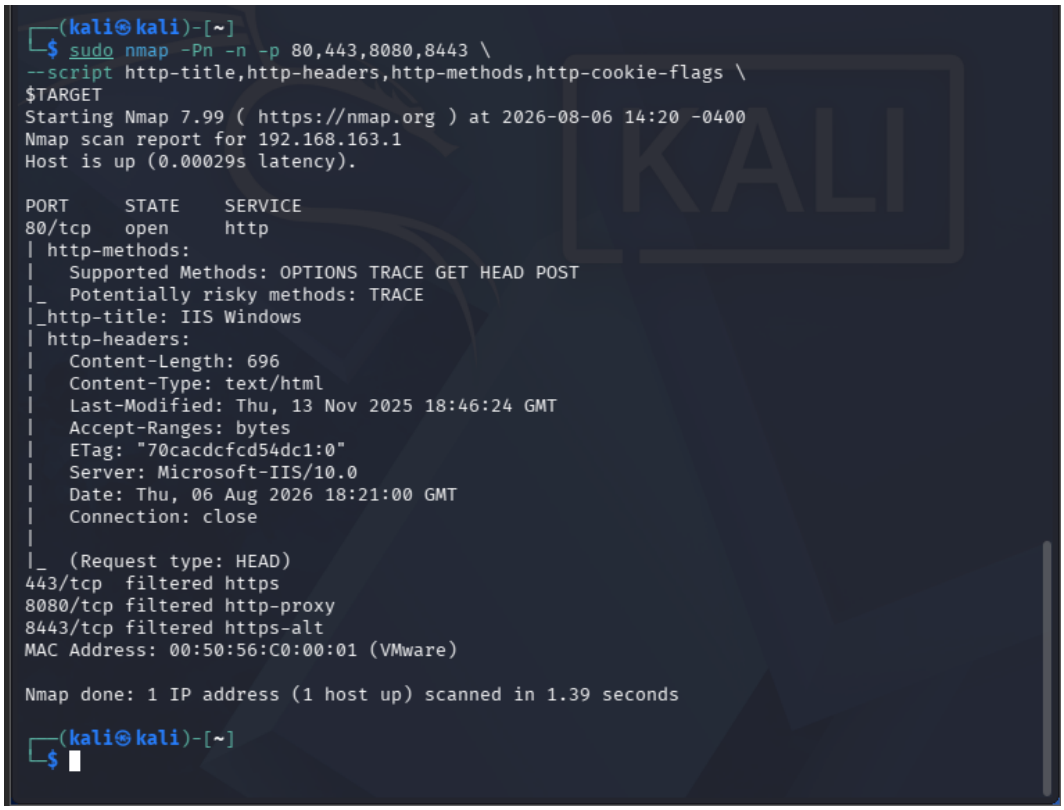



*Nota.* Elaboración propia.

Según el análisis del encabezado, no se observan encabezados de seguridad HTTP (Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options y Referrer-Policy). Esto genera un riesgo de clickjacking, inyección de contenido y degradación del transporte.

**Figura 6**

*Cabeceras HTTP del servidor: banner expuesto, método TRACE y ausencia de cabeceras de seguridad*




*Nota.* Elaboración propia.

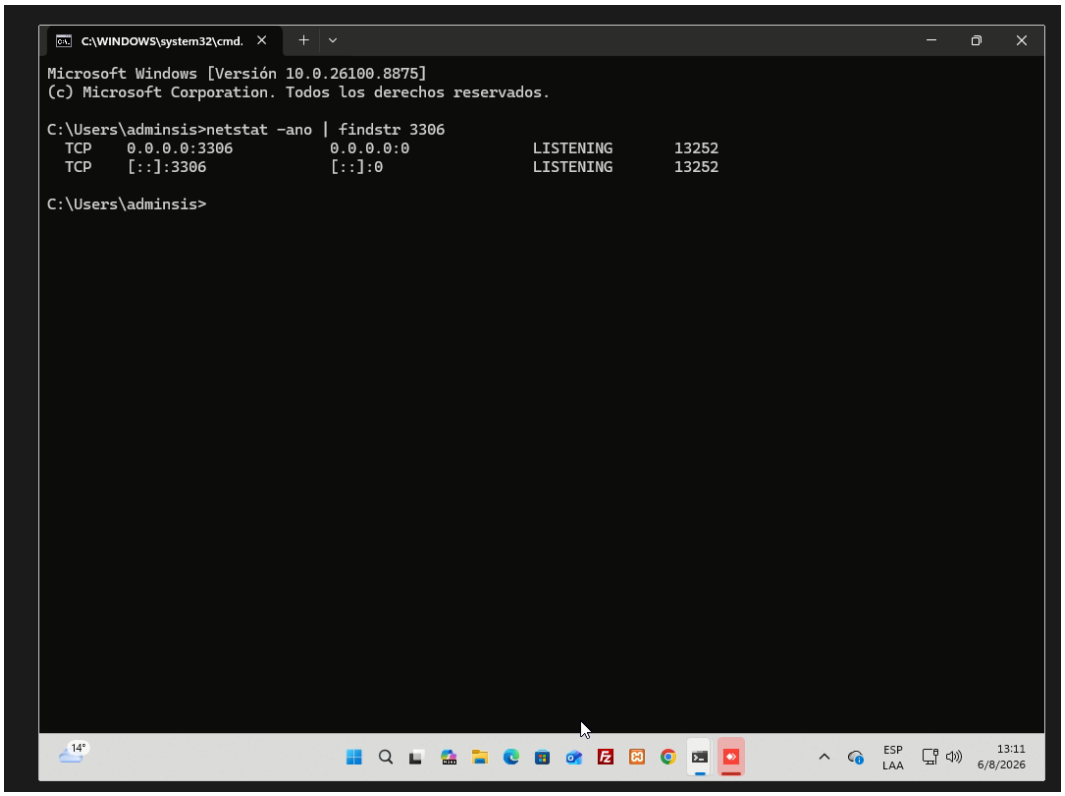
Para el transporte, ningún servicio HTTPS está operando en el objetivo. Los puertos 443 y 8443 estaban cerrados o filtrados. No se estableció ninguna conexión TLS. Esto significa que el servicio web evaluado está funcionando sobre HTTP sin protección. Esto compromete la integridad y la confidencialidad de la información transmitida, especialmente en instituciones financieras, ya que es de particular importancia.

Para la base de datos, la verificación local mediante netstat mostró que el servicio MySQL/MariaDB está escuchando en el puerto 3306 en 0.0.0.0, lo que se traduce en escuchar en todas las interfaces de red y no en la interfaz local. Aunque durante la ventana principal el puerto

se observó filtrado desde la red, el enlace a todas las interfaces mantiene una superficie de exposición que depende exclusivamente de dicho filtrado, sin defensa en profundidad a nivel del propio motor.

**Figura 7**

*Servicio de base de datos (3306) enlazado a 0.0.0.0 en todas las interfaces (netstat)*

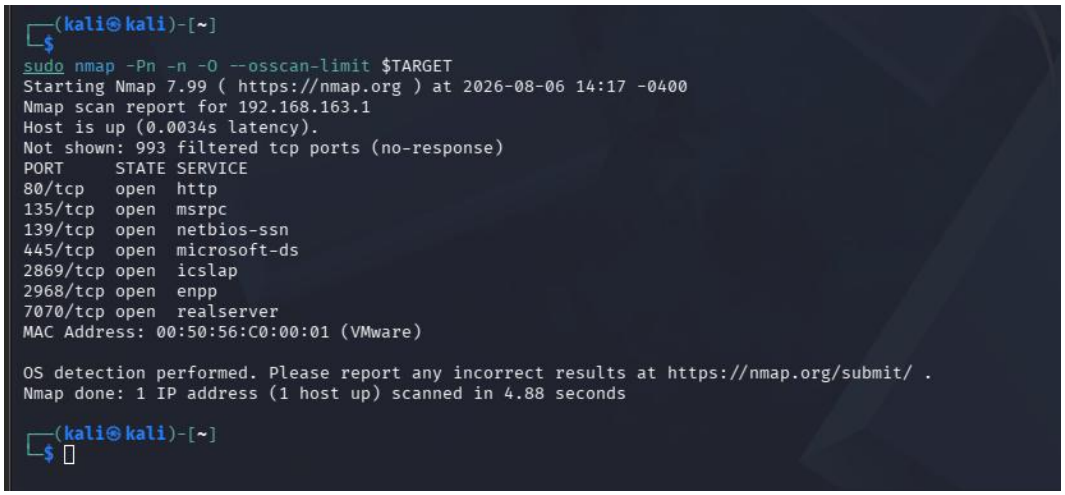



*Nota.* Elaboración propia.

El escaneo con detección de sistema operativo y detección de servicios adicionales ha encontrado servicios del ecosistema de Microsoft expuestos en el segmento (NetBIOS, MSRPC, microsoft-ds/SMB y UPnP/SSDP así como servicios de descubrimiento). Esto ofrece más vectores y debería segmentarse.

**Figura 8**

*Servicios de Windows expuestos (SMB, NetBIOS, MSRPC, UPnP) y detección de sistema operativo*




*Nota.* Elaboración propia.

### *4.4.3 Explotación controlada*

En línea con las normas de participación y consideraciones éticas, el objetivo era limitar la exploración para confirmar la presencia y el alcance de las vulnerabilidades, sin causar daño, denegación de servicio ni alteración de datos. Las pruebas demostraron que los servicios eran accesibles y que las configuraciones evaluadas eran correctas. Los datos recopilados debían mostrar la presencia del riesgo, sin intentar crear ningún impacto en el entorno.

**Tabla 10**

*Matriz de hallazgos*

| ID | Evidencia | Herramienta | Activo afectado | Impacto | Nivel de riesgo | Estado de validación |
|---|---|---|---|---|---|---|
| H-01 | Figuras 2 y 7 | Nmap -sV; netstat -ano | Servidor de base de datos (MySQL 8.0.36, puerto 3306) | Confidencialidad e integridad: acceso no autorizado a la base de datos | Alto | Validado parcialmente: enlace a 0.0.0.0 confirmado localmente; exposición en red |

| ID | Evidencia | Herramienta | Activo afectado | Impacto | Nivel de riesgo | Estado de validación |
|---|---|---|---|---|---|---|
| | | | | | | observada solo en la ventana previa |
| H-02 | Sección 4.4.2 | Nmap ssl-enum-ciphers; curl -k | Servidor web IIS | Confidencialidad e integridad: intercepción de tráfico y robo de credenciales | Alto | Validado: no se estableció conexión TLS (escaneo y verificación manual) |
| H-03 | Figuras 5 y 6 | Nmap http-methods; curl -X OPTIONS | Servidor web IIS | Confidencialidad: Cross-Site Tracing y abuso de métodos HTTP | Bajo | Validado: método TRACE anunciado en la respuesta OPTIONS |
| H-04 | Figura 6 | Nmap http-headers; curl -I | Servidor web IIS | Integridad: clickjacking, inyección de contenido y degradación del transporte | Medio | Validado: ausencia de cabeceras confirmada manualmente |
| H-05 | Figuras 3 y 6 | WhatWeb; curl -I | Servidor web IIS | Confidencialidad: reconocimiento facilitado por divulgación de información | Medio | Validado: banner y página por defecto confirmados manualmente |
| H-06 | Figura 2 | Nmap -sV | Servidor de aplicaciones (Apache httpd, puerto 8080) | Confidencialidad y disponibilidad: explotación de un servicio web no gestionado | Medio | Detectado: observado solo en la ventana previa; no revalidado en la ventana principal |
| H-07 | Figura 8 | Nmap -O; -sU --top-ports | Infraestructura de red (SMB, NetBIOS, MSRPC, UPnP/SSDP) | Confidencialidad y disponibilidad: movimiento lateral y explotación de servicios de Windows | Medio | Detectado: identificado por escaneo, sin verificación manual |

Nota. Elaboración propia

La matriz muestra que cuatro de los siete hallazgos (H-02 a H-05) fueron validados mediante una segunda técnica; H-01 se validó parcialmente, ya que combina una verificación local con una exposición en red observada solo en la ventana de reconocimiento previa; y H-06 y H-07 se sustentan únicamente en el escaneo automatizado. Esta diferencia se considera al priorizar las acciones del plan de tratamiento.

### 4.5 Fase 4. Evaluación de resultados y análisis de riesgos

La cuarta fase clasificó la severidad de las vulnerabilidades y el impacto de cada vulnerabilidad en los sistemas. Construyó la matriz de riesgos asociando los hallazgos técnicos a la valoración del impacto, activos, amenazas y probabilidad de riesgo. Para empezar, los hallazgos se consolidan junto con su identificador, el método, el activo y la severidad técnica de CVSS v4.0.

**Tabla 11**

*Consolidación de hallazgos técnicos del pentesting*

| ID | Hallazgo | Evidencia / técnica | Activo | Severidad |
|---|---|---|---|---|
| **H-01** | Exposición de la versión del gestor de base de datos (MySQL 8.0.36) y enlace del servicio 3306 a todas las interfaces (0.0.0.0) | Nmap -sV; netstat -ano | Servidor de base de datos | **Alta** |
| **H-02** | Servicio web operando sobre HTTP sin cifrado; ausencia de HTTPS/TLS operativo (443/8443 cerrados o filtrados) | Nmap ssl-enum-ciphers; curl -k | Servidor web IIS | **Alta** |
| **H-03** | Método HTTP TRACE habilitado (riesgo de Cross-Site Tracing) | Nmap http-methods; curl -X OPTIONS | Servidor web IIS | **Media** |
| **H-04** | Ausencia de cabeceras de seguridad HTTP (HSTS, CSP, X-Frame-Options, X-Content-Type-Options) | Nmap http-headers; curl -I | Servidor web IIS | **Media** |
| **H-05** | Divulgación del banner del servidor (Server: Microsoft-IIS/10.0) y página por defecto de IIS | WhatWeb; curl -I | Servidor web IIS | **Baja** |
| **H-06** | Segundo servidor web (Apache httpd) expuesto en el puerto 8080, incrementando la superficie de ataque | Nmap -sV | Servidor de aplicaciones | **Media** |
| **H-07** | Servicios de Windows expuestos en la red (SMB/445, NetBIOS/139-137, MSRPC/135, UPnP/SSDP) | Nmap -O; -sU --top-ports | Infraestructura de red | **Media** |

*Nota.* Elaboración propia con base en las evidencias.

A partir de los hallazgos, la valoración del riesgo se realizó con ISO/IEC 27005:2022 y MAGERIT, estimando la probabilidad y el impacto y calculando el riesgo inherente conforme a

la expresión Riesgo = Probabilidad × Impacto, con una escala cualitativa de tres niveles (Bajo = 1, Medio = 2, Alto = 3).

**Tabla 12**

*Matriz de nivel de riesgo Probabilidad × Impacto*

| Probabilidad \ Impacto | Bajo (1) | Medio (2) | Alto (3) |
|---|---|---|---|
| **Alta (3)** | **Medio (3)** | **Alto (6)** | **Crítico (9)** |
| **Media (2)** | **Bajo (2)** | **Medio (4)** | **Alto (6)** |
| **Baja (1)** | **Bajo (1)** | **Bajo (2)** | **Medio (3)** |

*Nota.* Elaboración propia con base en MAGERIT.

**Tabla 13**

*Valoración del riesgo por hallazgo*

| ID | Amenaza asociada | Dimensión CIA | Probabilidad | Impacto | Riesgo inherente | Riesgo residual |
|---|---|---|---|---|---|---|
| **H-01** | Acceso no autorizado a la base de datos / explotación de vulnerabilidad conocida | Confidencialidad, Integridad | Media | Alto | **Alto** | Bajo |
| **H-02** | Intercepción de tráfico / robo de credenciales en tránsito | Confidencialidad, Integridad | Media | Alto | **Alto** | Bajo |
| **H-03** | Cross-Site Tracing / abuso de métodos HTTP | Confidencialidad | Baja | Medio | **Bajo** | Bajo |
| **H-04** | Clickjacking / inyección de contenido / degradación de transporte | Integridad | Media | Medio | **Medio** | Bajo |
| **H-05** | Reconocimiento facilitado por divulgación de información | Confidencialidad | Alta | Bajo | **Medio** | Bajo |
| **H-06** | Explotación de servicio web adicional no gestionado | Confidencialidad, Disponibilidad | Media | Medio | **Medio** | Bajo |

| ID | Amenaza asociada | Dimensión CIA | Probabilidad | Impacto | Riesgo inherente | Riesgo residual |
|---|---|---|---|---|---|---|
| **H-07** | Movimiento lateral / explotación de servicios de Windows expuestos | Confidencialidad, Disponibilidad | Media | Medio | **Medio** | Bajo |

*Nota.* Elaboración propia con base en ISO/IEC 27005:2022 y MAGERIT.

El perfil de riesgo muestra dos hallazgos de nivel alto (H-01 y H-02), asociados a la exposición del servicio de base de datos y a la ausencia de cifrado en el transporte, que deben priorizarse por su impacto sobre la confidencialidad e integridad de la información de los socios. Los hallazgos de nivel medio corresponden a debilidades de configuración y a la ampliación innecesaria de la superficie de ataque. La columna de riesgo residual muestra el nivel de cada riesgo después de aplicar los controles de la Fase 5. El control positivo de la enumeración de directorios no descubrió rutas administrativas ni copias de seguridad dentro del alcance evaluado que fueran accesibles al público en general.

### 4.6 Fase 5. Elaboración de la propuesta de mejora

Las recomendaciones de mitigación y el diseño de políticas y directrices de seguridad durante la fase cinco fueron diseñados para abordar los riesgos residuales de los sistemas evaluados. Cada hallazgo se documenta como un control correctivo específico, identificando a la parte responsable, la fecha objetivo de finalización y la referencia normativa. Esto articula ISO/IEC 27002:2022, el NIST Cybersecurity Framework 2.0, OWASP y las normas SEPS.

**Tabla 14**

*Plan de tratamiento del riesgo por hallazgo*

| ID | Control / medida de mitigación | Referencia normativa | Responsable | Plazo |
|---|---|---|---|---|
| **H-01** | Restringir el servicio de base de datos a la interfaz local (bind-address = | ISO/IEC 27002:2022 (8.20, | Área de TI / DBA | Inmediato (0–1 mes) |

| ID | Control / medida de mitigación | Referencia normativa | Responsable | Plazo |
|---|---|---|---|---|
| | 127.0.0.1) o a la red interna estrictamente necesaria; aplicar firewall de host; actualizar el motor y ocultar su versión; endurecer credenciales y privilegios. | 8.9); NIST CSF PROTECT; SEPS seguridad de la información | | |
| **H-02** | Implementar HTTPS con certificado válido; forzar redirección de HTTP a HTTPS; deshabilitar protocolos y cifradores obsoletos; habilitar HSTS. | OWASP WSTG; ISO/IEC 27002:2022 (8.24); SEPS canales electrónicos | Área de TI | Corto plazo (1–2 meses) |
| **H-03** | Deshabilitar el método HTTP TRACE (y TRACK); limitar los métodos permitidos a los estrictamente necesarios. | OWASP; ISO/IEC 27002:2022 (8.9) | Área de TI | Inmediato (0–1 mes) |
| **H-04** | Configurar cabeceras de seguridad: HSTS, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options y Referrer-Policy. | OWASP Secure Headers; NIST CSF PROTECT | Área de TI | Corto plazo (1–2 meses) |
| **H-05** | Suprimir o enmascarar la cabecera Server y los banners de versión; reemplazar la página por defecto de IIS por una configuración endurecida. | ISO/IEC 27002:2022 (8.9); OWASP | Área de TI | Inmediato (0–1 mes) |
| **H-06** | Inventariar y justificar el segundo servidor web (8080); deshabilitarlo si no es requerido; endurecerlo y restringir su acceso por firewall si lo es. | ISO/IEC 27002:2022 (8.9, 8.20); NIST CSF IDENTIFY | Área de TI | Corto plazo (1–2 meses) |
| **H-07** | Segmentar la red y restringir por firewall los servicios de Windows (SMB, NetBIOS, MSRPC, UPnP) al ámbito estrictamente necesario; deshabilitar los no requeridos. | ISO/IEC 27002:2022 (8.20, 8.22); NIST CSF PROTECT; SEPS riesgo operativo | Área de TI / Redes | Corto plazo (1–3 meses) |

*Nota.* Elaboración propia.

### *4.6.1 Lineamientos y políticas de seguridad propuestos*

Complementando los controles técnicos, se proponen los siguientes lineamientos de carácter administrativo, orientados a sostener la mejora en el tiempo y a alinear la gestión con las exigencias regulatorias del sector:

- Política de gestión de vulnerabilidades: ciclo periódico de identificación, valoración, tratamiento y verificación (retest), con registro documentado y responsables asignados.

- Política de endurecimiento (hardening) de servidores y servicios: configuraciones base seguras verificadas antes de la puesta en producción.
- Política de gestión de accesos y credenciales: principio de mínimo privilegio, credenciales robustas y revisión periódica de permisos.
- Política de protección de cifrado y transporte: HTTPS/TLS debe utilizarse en todos los servicios que transmitan información de socios conforme a las regulaciones SEPS.
- Política de segmentación de red: separación de entornos y restricción del tráfico entre segmentos.
- Entrenar al personal técnico en buenas prácticas de seguridad y comprender los resultados de las evaluaciones de seguridad.

### *4.6.2 Verificación posterior (retest)*

De acuerdo con el criterio de fiabilidad del Capítulo III, una vez implementadas las medidas correctivas, se recomienda volver a probar el hallazgo abordado para determinar la efectividad de las medidas y confirmar el nivel estimado de riesgo residual en la Tabla 10 para cerrar el ciclo de mejora continua de la postura de seguridad de la cooperativa.

## CONCLUSIONES

Para el primer objetivo específico, fuimos capaces de desarrollar tanto la teoría como la legislación, así como un marco de cohesión y una base sólida de concepto. Se identificaron e integraron metodologías de pruebas de penetración y gestión de riesgos con las normas NIST SP 800-115, OWASP y PTES. La ejecución de la metodología fue liderada por las normas ISO/IEC 27005:2022 y MAGERIT para la evaluación de riesgos. Para la clasificación de la severidad del riesgo y el marco de cumplimiento, utilizamos CVSS v4.0 y las normas SEPS y LOPDP,

respectivamente. Estas formaron la base de todas las decisiones metodológicas subsiguientes y proporcionaron un marco de trazabilidad entre la teoría, la ejecución y la evaluación.

Definiciones de alcance de métodos de segunda objective específicos permitidos para identificar las metodologías más adecuadas dentro del contexto de la cooperativa, considerando la situación financiera de la cooperativa, el valor de sus activos y las limitaciones operativas de una entidad típica del sector solidario popular. El uso del método de caja gris en un servidor de réplica con entornos aislados controlados, con una base de evidencia rastreable y técnicas de clasificación mediante CVSS v4.0 y la matriz Probabilidad x Impacto, fue una opción apropiada para una institución que tiene recursos limitados, ya que logró un equilibrio elocuente entre el alcance y la profundidad del análisis, la continuidad del servicio y la protección de la información de los miembros.

La gestión del tercer objetivo específico mostró que se documentaron siete hallazgos verificados con evidencia tras realizar y evaluar las fases de pruebas de penetración. Dos de estos hallazgos fueron de alta gravedad. Estos incluyeron el gestor de base de datos MySQL 8.0.36 expuesto con la versión revelada y el servicio ejecutándose en todas las interfaces de red y el servicio web siendo accesible a través de HTTP sin seguridad. El resto de los hallazgos fueron de gravedad media y baja. Incluyeron problemas de configuración y un aumento innecesario de la superficie de ataque. Entre estos hallazgos, se habilitó el método TRACE, faltaron cabeceras de seguridad, se divulgó la pancarta del servidor y algunos servicios de Windows estuvieron expuestos. A partir de estos hallazgos, desarrollamos acciones de mitigación priorizadas y las asociamos con los controles de ISO/IEC 27002, el Marco de Ciberseguridad de NIST y SEPS. Esto completó el ciclo de identificación, evaluación y respuesta de acuerdo con el estudio.

# RECOMENDACIONES

A partir de los hallazgos y de la valoración del riesgo, se recomienda a la Cooperativa de Ahorro y Crédito Yuyay Ltda.:

En primer lugar, priorizar el tratamiento de los dos hallazgos de severidad alta identificados en la Sección 4.5: restringir el servicio de base de datos MySQL a la interfaz local o a la red estrictamente necesaria, ocultar su versión y endurecer sus credenciales, y habilitar el cifrado del canal web mediante HTTPS con certificado válido, forzando la redirección desde HTTP, dado que ambos concentran el mayor impacto sobre la confidencialidad e integridad de la información de los socios y su corrección es de baja complejidad técnica.

En segundo lugar, se recomienda endurecer la configuración de los servicios web expuestos, deshabilitando el método HTTP TRACE, suprimiendo o enmascarando el banner del servidor, reemplazando la página por defecto de IIS por una configuración segura e incorporando las cabeceras de seguridad ausentes (Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options y Referrer-Policy), medidas que mitigan las debilidades de configuración documentadas en la Sección 4.4 con un esfuerzo mínimo y un beneficio inmediato sobre la postura de seguridad.

En tercer lugar, se recomienda reducir la superficie de ataque mediante la segmentación de la red y la aplicación de reglas de firewall que restrinjan los servicios propios de Windows (SMB, NetBIOS, MSRPC y los servicios de descubrimiento UPnP/SSDP) al ámbito estrictamente requerido, así como inventariar y justificar el segundo servidor web detectado en el puerto 8080, deshabilitándolo si no cumple una función necesaria, con el fin de dificultar el movimiento lateral dentro del segmento que aloja los sistemas financieros.

En cuarto lugar, se recomienda a la dirección de la cooperativa institucionalizar la gestión de la seguridad de la información mediante la formalización de las políticas propuestas en la Sección 4.6, que comprenden la gestión de vulnerabilidades, el endurecimiento de servidores, la gestión de accesos con mínimo privilegio, el cifrado del transporte y la segmentación de red, junto con la programación de evaluaciones de seguridad periódicas, de modo que la seguridad se gestione como un proceso continuo y no como una acción puntual, en concordancia con las obligaciones de la Superintendencia de Economía Popular y Solidaria y de la Ley Orgánica de Protección de Datos Personales.

En quinto lugar, se recomienda ejecutar una verificación posterior (retest) una vez implementados los controles correctivos, repitiendo las pruebas sobre los hallazgos tratados con el fin de comprobar la efectividad de las medidas y confirmar la reducción del riesgo residual al nivel estimado en la Sección 4.5, cerrando de este modo el ciclo de identificación, tratamiento y validación previsto en el estudio.

A partir de los hallazgos y de la valoración del riesgo, se recomienda a la carrera de Sistemas de Información de la extensión Cañar:

Ampliar el alcance de la evaluación a los sistemas que quedaron fuera de la ventana analizada, en particular la aplicación móvil de la cooperativa y sus servicios de backend/API, así como el componente de canales electrónicos, empleando marcos específicos como la OWASP Mobile Application Security Testing Guide y la OWASP API Security Top 10, e incorporando análisis con herramientas complementarias que permitan contrastar la cobertura y precisión de la detección, de modo que la institución disponga de una visión integral y sostenida de su postura de seguridad a lo largo del tiempo.

# REFERENCIAS

# BIBLIOGRAFÍA

Abdullatif Altulaihan, E., Alismail, A., & Frikha, M. (2023). A survey on web application penetration testing. *Electronics*.

Alabbad, M., Mhaskar, N., & Khedri, R. (2024). Hardening of network segmentation using automated referential penetration testing. *Elsevier*.

Albahar, M., Alansari, D., & Jurcut, A. (2022). An empirical comparison of pen-testing tools for detecting web app vulnerabilities. *Electronics*.

Albahar, M., Alansari, Z., & Jurcut, A. D. (2022). Benchmarking vulnerability assessment tools in cybersecurity: Effectiveness and limitations. *Electronics*.

Alhogail, A., & Alkahtani, M. (2024). Automated extension-based penetration testing for web vulnerabilities. *ScienceDirect*.

Almeida, F., & Torres, R. (2023). Cybersecurity challenges in small financial institutions. *Journal of Information Security*, 85–97.

Alqahtani, S. A. (2024). Penetration testing in modern cybersecurity: Techniques, tools, and challenges. *IEEE Access*.

Asamblea Nacional. (2021, 26 de mayo). *Asamblea Nacional*. https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/920-lmoreno/ro-459-5to-sup-26-05-2021.pdf

Behl, A., & Behl, K. (2021). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

CISA. (s. f.). *Known Exploited Vulnerabilities Catalog*. Cybersecurity and Infrastructure Security Agency. Recuperado el 16 de junio de 2026, de https://www.cisa.gov/known-exploited-vulnerabilities-catalog

ENISA. (2025). *ENISA threat landscape: Finance sector*. European Union Agency for Cybersecurity.

Fadhli, M. (2024). Comprehensive analysis of penetration testing frameworks and tools: Trends, challenges, and opportunities. *Indonesian Journal of Electrical Engineering and Renewable Energy*.

FIRST. (2023). *Common Vulnerability Scoring System version 4.0*. FIRST: Improving Security Together.

Flor-Unda, O., Simbaña, F., Larriva-Novo, X., Acuña, A., Tipán, R., & Acosta-Vargas, P. (2023). A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America. *Informatics*, 71.

Hassan, R. K. (2023). Performance evaluation of cybersecurity tools using empirical metrics. *Computers & Security*.

Help Net Security. (2025, 15 de abril). *Help Net Security*. https://www.helpnetsecurity.com/2025/04/15/regular-pentesting-strategy-for-organizations/

ISO/IEC. (2022a). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization/International Electrotechnical Commission.

ISO/IEC. (2022b). *Information security, cybersecurity and privacy protection — Information security controls* (ISO/IEC 27002:2022).

ISO/IEC. (2022c). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO.

ISO/IEC. (2023). *Information technology — Information security incident management*. ISO.

ISTARI. (2024, septiembre). *ISTARI*. https://istari-global.com/insights/spotlight/the-state-of-pentesting-2024/

Lazarov, W., Seda, P., Martinasek, Z., & Kummel, R. (2025). Penterep: Comprehensive penetration testing with adaptable interactive checklists. *ScienceDirect*.

Mahditia Adam, H., Widyawan, W., & Dharma Putra, G. (2023). A review of penetration testing frameworks, tools, and application areas. *ResearchGate*.

MITRE. (2024). *CWE Top 25 most dangerous software weaknesses – 2024*.

MITRE Corporation. (s. f.). *MITRE ATT&CK Enterprise Matrix*. MITRE ATT&CK. Recuperado el 16 de junio de 2026, de https://attack.mitre.org/matrices/enterprise/

MITRE Corporation. (2025). *CWE Top 25 most dangerous software weaknesses*. CWE.

National Institute of Standards and Technology. (2008). *Technical guide to information security testing and assessment* (Special Publication 800-115). https://csrc.nist.gov/pubs/sp/800/115/final

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). National Institute of Standards and Technology.

OWASP. (s. f.). *OWASP Web Security Testing Guide*.

OWASP Foundation. (2023). *OWASP API Security*. OWASP.

OWASP Foundation. (2025). *OWASP Top 10:2025*. OWASP.

Presidencia de la República. (2023). *Reglamento de la Ley Orgánica de*. Lexis.

Restrepo Gomez, J., & Correa Ortiz, L. (2024). Bug-Bounty, ¿el futuro del pentesting? *Ciencia e Ingeniería Neogranadina*, 11–22.

SEPS. (2022). *Norma de control de seguridades en el uso de canales electrónicos para las entidades financieras controladas por la Superintendencia de Economía Popular y Solidaria*. Superintendencia de Economía Popular y Solidaria.

SEPS. (2023). *Norma de control de seguridades en el uso de canales electrónicos para las entidades financieras controladas por la Superintendencia de Economía Popular y Solidaria*. Superintendencia de Economía Popular y Solidaria.

SEPS. (2024). *Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116: Norma de control para la administración del riesgo operativo*. Superintendencia de Economía Popular y Solidaria.

Sharma, P., & Pilli, E. S. (2023). Advancements in penetration testing methodologies using automation and AI. *Cybersecurity*.

# ANEXOS

**Anexo 1: Protocolo de Investigación**

**Anexo: Formato del Anteproyecto.**

| **A. TÍTULO** |
|---|
| Evaluación de la seguridad informática mediante pentesting en los sistemas de información de la Cooperativa de Ahorro y Crédito Yuyay Ltda. |

| **B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN** | | | |
|---|---|---|---|
| | | Inteligencia de Negocios | |
| | | Sistemas de Información | |
| | | Gobierno y administración de tecnologías de información | |
| | | Auditoría Informática | X |
| | | Seguridad Informática | |
| | | Redes y comunicación | |

| | | | |
|---|---|---|---|
| **Tecnologías de Información y Comunicación** | **Ciencias exactas, naturales y tecnológicas** | Arquitectura de Hardware | |
| | | Arquitectura de desarrollo de software | |
| | | Ingeniería de Software | |
| | | Gestión y gobierno de proyectos de tecnología informática | |
| | | Ingeniería de requerimientos | |
| | | Algoritmos y programación | |
| | | Ciencias exactas y naturales (Matemáticas, Física, Química, Biología, etc.) | |
| | | Modelaje y simulación | |
| | | | |

Universidad Católica de Cuenca

**C. PLANTEAMIENTO DEL PROBLEMA**

Dentro del área de evolución digital continua, la creciente dependencia de las instituciones financieras en sus sistemas de información para facilitar sus operaciones, proteger su información sensible y mantener la continuidad de sus servicios, ha aumentado su vulnerabilidad a las amenazas de ciberseguridad. Estas amenazas están aumentando peligrosamente en su intensidad. El Instituto Nacional de Estándares y Tecnología afirma que una de las principales causas de incidentes de seguridad sigue siendo la explotación de debilidades en los sistemas informáticos, lo que demuestra la falla en la ejecución adecuada de controles y medidas de seguridad (National Institute of Standards and Technology, 2022).

Dentro de este contexto, las cooperativas de ahorro y crédito, incluida la Cooperativa de Ahorro y Crédito Yuyay Ltda, serían susceptibles a ciberataques dado su manejo de datos financieros y personales sensibles. Los estudios recientes indican que las instituciones financieras más pequeñas tienden a ser más vulnerables a los ataques debido a su infraestructura tecnológica limitada, recursos especializados y marcos de seguridad deficientes Almeida et al. (2023). Este problema se vuelve aún más problemático cuando realizan pocas o ninguna evaluación periódica para identificar debilidades y rectificarlas en un plazo adecuado.

Los controles de seguridad tradicionales como los cortafuegos y sistemas antivirus están siendo rendered ineficaces por las amenazas avanzadas prevalentes en el entorno cibernético actual. Estas amenazas requieren un enfoque de seguridad más avanzado y dedicado. En este contexto, una de las metodologías más importantes es la prueba de penetración, o “pentesting”. Se trata de

un intento deliberado y controlado de comprometer la seguridad de una organización para evaluar la seguridad de los sistemas y determinar las vulnerabilidades críticas que pueden ser explotadas (Behl & Behl, 2021). Considerando esto, es importante medir el nivel de seguridad de la información de los sistemas de información de la Cooperativa Yuyay Ltda. empleando metodologías estructuradas de pentesting para poder identificar los riesgos y fortalecer la protección de la información de la institución.

**D. OBJETIVO GENERAL**

Realizar una evaluación de la seguridad de la información de los sistemas de la Cooperativa de Ahorro y Crédito Yuyay Ltda, considerando las técnicas de prueba de penetración basadas en modelos universalmente adoptados, para identificar debilidades y evaluar los riesgos, ofreciendo recomendaciones para mejorar y optimizar su protección.

**E. OBJETIVOS ESPECÍFICOS**

1. Analizar las metodologías de seguridad de la información y pruebas de penetración para evaluar las herramientas de seguridad utilizadas en la evaluación de seguridad de los sistemas en Yuyay Ltda. Cooperativa.
2. Seleccionar y justificar las metodologías de pentesting más adecuadas para el contexto de la Cooperativa Yuyay Ltda., evaluando su efectividad y aplicabilidad.
3. Evalúe los sistemas de Yuyay Ltda. Cooperativa y lleve a cabo las diferentes fases de pruebas de penetración. Redacte medidas de mitigación de riesgos basadas en sus hallazgos.

**F. JUSTIFICACIÓN**

La investigación en esta área es necesaria ya que la demanda de marcos de ciberseguridad en el sector financiero está en aumento y adquiriendo prominencia. Se sabe que el pentesting desempeña un papel crucial en cualquier marco de ciberseguridad. En particular, investigaciones recientes muestran que el 94% de las organizaciones consideran el pentesting como una práctica básica para evaluar su seguridad (Help Net Security, 2025).

Desde una perspectiva práctica, la investigación ayudará a descubrir las deficiencias reales en los sistemas de información de la Cooperativa Yuyay Ltda., lo que proporcionará una evaluación sencilla de su condición de seguridad, con sugerencias técnicas elaboradas para abordar sus preocupaciones de seguridad. Además, los hallazgos contribuirán al desarrollo de la seguridad, integridad y accesibilidad de la información en la industria financiera en relación con las necesidades de este campo en particular. Desde una perspectiva científica, esta investigación desarrolla la ley sobre seguridad informática, específicamente el uso de técnicas de pentesting en entornos del mundo real debido a la naturaleza dinámica de las amenazas y las tecnologías. Además, la investigación se ajusta a las tendencias actuales centradas en la necesidad de evaluaciones de seguridad periódicas debido a la creciente vulnerabilidad y a la complejidad creciente de los sistemas tecnológicos (ISTARI, 2024).

Finalmente, esta investigación sentará las bases para las futuras evaluaciones de seguridad de los marcos de seguridad organizacional, promoviendo el uso de protocolos de seguridad preventivos y de gestión de riesgos para los sistemas de información.

| G. ALCANCE |
| --- |
| Este estudio se centra en la evaluación de la seguridad de la información en los sistemas de información de la Cooperativa de Ahorro y Crédito Yuyay Ltda. Utiliza metodologías estructuradas y herramientas especializadas en el contexto de pruebas de penetración (pentesting). Las fases de reconocimiento, análisis de vulnerabilidades, explotación controlada e informes detallados, que forman parte del proceso de pentesting, son los elementos principales del estudio. También se enfocará en los activos tecnológicos distintivos de la cooperativa. Además, se limitará al análisis de los sistemas instalados y en uso, sin proponer nuevos sistemas y soluciones, y sin perturbar las operaciones cotidianas de la cooperativa.<br>El estudio incluye una evaluación de las defensas actuales contra amenazas cibernéticas en los sistemas de la cooperativa y sugiere mejoras que están en línea con las mejores prácticas internacionales en ciberseguridad. Busca lograr un equilibrio entre el fortalecimiento de los sistemas de ciberseguridad y las limitaciones/realidades de la cooperativa (por ejemplo, la falta de recursos financieros para implementar nuevos sistemas avanzados y/o la ausencia de recursos humanos capacitados para desarrollar sistemas de defensa avanzados).<br>La investigación tiene el potencial de crear un punto de referencia para futuras evaluaciones de ciberseguridad de la Cooperativa de Ahorro y Crédito Yuyay Ltda. y otras cooperativas de servicios financieros. |

## H. CONCEPTOS RELACIONADOS

El propósito de este estudio es comprender e identificar los conceptos principales relacionados con el análisis del rendimiento de las técnicas y herramientas de pruebas de penetración frente a las estrategias contemporáneas en ciberseguridad y marcos de evaluación de vulnerabilidades.

### Pentesting

La prueba de penetración, o pentesting, es una simulación deliberada de un ataque para capturar y catalogar debilidades en la infraestructura de una organización. En la literatura reciente se sugiere que el pentesting cumple un propósito técnico y estratégico. Como una prueba de exposición a brechas, ayuda a informar y avanzar en la seguridad de la información de una organización (Alqahtani, 2024).

### Metodologías de pentesting

Crean marcos organizados para la ejecución segura y sistemática de los procesos de prueba. La investigación reciente señala el desarrollo de estas metodologías para adoptar marcos más automatizados de herramientas de análisis continuo que emplean métodos como el reconocimiento automatizado, análisis con inteligencia artificial y la generación automatizada de informes periódicos Sharma et al. (2023). Estas metodologías buscan mejorar el proceso y minimizar la dependencia manual.

### Metodología PTES (Penetration Testing Execution Standard)

La metodología PTES, siendo la más popular en el entorno laboral, consiste en fases claramente definidas: pre-compromiso (definición del alcance), recopilación de información, modelado de la amenaza, análisis de vulnerabilidades, explotación, post-explotación y elaboración de informes. Proporciona al evaluador la capacidad de realizar una simulación del comportamiento de un atacante y ayuda a descubrir las áreas de superficie de ataque más críticas de un sistema de información. Esta metodología se describe en estudios recientes como la directiva más completamente desarrollada y exhaustiva, que incorpora elementos de un proceso de evaluación de seguridad tanto técnico como gerencial (Mahditia Adam, Widyawan, & Dharma Putra, 2023).

**Metodología NIST SP 800-115**

En su marco, el Instituto Nacional de Estándares y Tecnología ofrece un método para la evaluación gradual de la seguridad de un sistema utilizando un enfoque por fases de cuatro partes: Planificación, Descubrimiento, Ataque e Informe. Debido a sus características prescriptivas y su relación con las directrices internacionales, el método tiene una amplia aplicabilidad en el entorno institucional. Permite evaluaciones seguras de vulnerabilidad de sistemas y preserva eficazmente la seguridad de los sistemas sometidos a examen. Recientemente se ha demostrado que este método de enfoque por fases proporciona una evaluación del cumplimiento y la gestión del riesgo dentro de la organización (Fadhli, 2024).

**Metodología OWASP**

La metodología OWASP es única para aplicaciones web. Categoriza su proceso en fases como recopilación de información, prueba de autenticación, prueba de control de acceso,

prueba de gestión de sesiones, prueba de control de entrada y prueba de lógica de negocio. Su proceso ayudó a evaluar algunas vulnerabilidades comunes de seguridad web, incluyendo, pero no limitándose a, inyección SQL, Cross-Site Scripting (XSS) y fallos de autenticación. Estudios recientes han sugerido que, debido a su enfoque categorizado y meticuloso en amenazas web, OWASP se ha convertido en un punto de referencia destacado para la evaluación de la seguridad de aplicaciones (Alabbad, Mhaskar, & Khedri , 2024)

**Herramientas de pentesting**

Cuando se trata de pruebas de penetración, se desarrollan herramientas para ayudar a encontrar y explotar debilidades en los sistemas. Los nuevos estudios han demostrado que existe una gran disparidad en su rendimiento, particularmente en los aspectos de precisión, cobertura y tasa de falsos positivos, creando una demanda de comparación en un entorno controlado Albahar et al. (2022) Además, la nueva ola de herramientas automatizadas de pruebas de penetración basadas en inteligencia artificial está transformando la forma en que pensamos y abordamos las evaluaciones de vulnerabilidades.

**Nmap**

Nmap es un software libre y de código abierto para escanear redes y probar su seguridad. Permite el escaneo de redes y puede determinar qué sistemas están activos, qué servicios y sistemas operativos están en uso, e incluso qué posibles exploits pueden estar disponibles en servicios en varios puertos abiertos.

Dentro del campo de la piratería ética, ayuda a describir la red y a probar cada componente individual. Ayuda a identificar sistemas activos en la red e incluso ayuda a determinar qué puertos están abiertos en los sistemas. Además de describir los componentes de la red, incluso ayuda a determinar los servicios generales del sistema para etapas posteriores de explotación del sistema.

Nmap es una de las herramientas fundamentales utilizadas en cualquier prueba de penetración debido a su precisión y funciones avanzadas. Incluso ofrece la capacidad de personalizar las opciones de escaneo y usar servicios de red más avanzados y técnicas de explotación (Albahar, Alansari, & Jurcut, 2022).

**Metasploit Framework**

El Marco de Trabajo de Metasploit se desarrolla para construir, probar y ejecutar exploits, y es una plataforma de código abierto útil para profesionales de la seguridad. Proporciona un entorno modular estructurado para la explotación, post-explotación, escalada de privilegios y pruebas de explotación.

Aunque se preocupa principalmente por la fase de explotación cuando se aprovechan las vulnerabilidades previamente descubiertas y se controlan los ataques, a menudo proporciona las condiciones para modelar ataques reales. Entonces, es posible determinar el efecto real de las vulnerabilidades en un sistema y el daño que puede causar.

Publicaciones recientes indican que Metasploit es, sin duda, una de las herramientas de pruebas de penetración más avanzadas debido a sus muchas funciones de automatización y su

extensa base de datos de exploits. Por lo tanto, se ha convertido en una herramienta estándar de elección en el campo de las evaluaciones de seguridad (Sharma & Pilli, 2023).

**Nessus**

Uno de los escáneres de vulnerabilidades comerciales más populares en Seguridad Informática es Nessus. Nessus realiza la identificación automatizada de vulnerabilidades en sistemas, redes y aplicaciones, y se utiliza ampliamente en el análisis.

Se emplea en la fase de análisis de vulnerabilidades y presenta informes de riesgo, evaluaciones de severidad y soluciones propuestas para las vulnerabilidades identificadas. Nessus también es capaz de identificar configuraciones inseguras, vulnerabilidades conocidas (parte de la base de datos CVE) y brechas de cumplimiento.

**Rendimiento de Herramientas de Seguridad**

El rendimiento de las herramientas de seguridad significa medir su capacidad para detectar fallos. Los matices de las capacidades de detección actúan en términos de tasa, precisión, tiempo y recursos para los interesados. Cada vez más, estudios recientes comparan y se basan en estas métricas para comparar varias tecnologías (Hassan, 2023).

## I. TRABAJOS RELACIONADOS

Se han realizado diferentes estudios a nivel internacional para abordar el análisis y comparación de herramientas de prueba de penetración con un enfoque en los criterios basados en la experimentación. Un trabajo relevante es el desarrollado por Albahar et al. (2022), llevaron a cabo una evaluación comparativa de herramientas de análisis de vulnerabilidades en entornos controlados y analizaron problemas de precisión, cobertura y generación de falsos positivos (pág. 23) Las herramientas no demostraron una efectividad completa por sí solas, lo que puso de manifiesto la necesidad de integrar varias soluciones para lograr una detección de vulnerabilidades más integral.

Además, investigaciones curiosas se han centrado en emplear características de inteligencia artificial en pruebas de penetración, sugiriendo métodos automatizados que mejoran la facilidad para identificar vulnerabilidades y la reducción del tiempo de análisis. En este sentido, Sharma et al. (2023) observan que el avance de los métodos hacia esquemas híbridos (manual-automatizado) permite una optimización marcada de la eficiencia y la reproducibilidad en la ejecución de pruebas de seguridad. Estos trabajos construyen una base sólida para la evaluación experimental del rendimiento de las herramientas en un entorno virtualizado. Sharma et al. (2023). Estos estudios aportan una base sólida para la evaluación experimental del rendimiento de herramientas en entornos virtualizados.

En América Latina, la investigación sugiere que asegurar la información sigue siendo un problema estructural difícil en las organizaciones que trabajan con información sensible. Un ejemplo de esto es un estudio realizado en Ecuador y publicado en una revista indexada, que

analiza las principales vulnerabilidades en la región e identifica problemáticas como el uso de software obsoleto, la falta de seguridad y la incapacidad del personal para ser capacitado en estos temas, factores significativos que aumentan el riesgo de exposición para su organización Unda et al. (2023). Esta investigación es de gran interés para el estudio actual porque muestra que las debilidades de seguridad pueden ser tanto técnicas como organizacionales, lo que valida que las pruebas de penetración se utilicen para constatar el estado real de la seguridad de los sistemas.

Los estudios recientes también han reconocido que las pruebas de penetración pueden servir como la solución principal para detectar vulnerabilidades en las infraestructuras corporativas. Un artículo publicado en América Latina destaca que, para el descubrimiento de vulnerabilidades dentro del sistema antes de que puedan ser explotadas, las auditorías de seguridad y las pruebas de penetración son fundamentales, y además señala que métodos alternativos, como bug bounty, no sustituyen la necesidad de especialistas en pruebas de penetración (Restrepo Gomez & Correa Ortiz , 2024).

También se señalaron estudios que evaluaban herramientas específicas de detección de vulnerabilidades, y medían su capacidad para encontrar fallos de seguridad en sistemas web y sistemas de red local Albahar et al. (2022). Sin embargo, estos estudios tienden a centrarse en herramientas individuales, en lugar de en comparaciones exhaustivas de herramientas organizadas en torno a una metodología, destacando una brecha en la literatura nacional, que esta investigación busca llenar.

Universidad Católica de Cuenca

## J. METODOLOGÍA

La presente investigación adopta un enfoque mixto, combinando el análisis cualitativo de la postura de seguridad de los sistemas de información con la evaluación cuantitativa de las vulnerabilidades identificadas mediante pruebas de penetración. El nivel de investigación es descriptivo–aplicado, ya que se busca analizar el estado actual de la seguridad informática en la Cooperativa de Ahorro y Crédito Yuyay Ltda. y aplicar técnicas de pentesting para identificar y evaluar riesgos reales.

## K. CRONOGRAMA DE ACTIVIDADES

| N° | ACTIVIDAD | MES | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | I | II | III | IV | V | VI | MEDIOS DE VERIFICACIÓN |
| 1 | Realizar un estudio teórico sobre seguridad informática, pentesting y gestión de vulnerabilidades | X | | | | | | Repositorio de documentos (Mendeley) |
| 1.1 | Bases teóricas: ciberseguridad, ethical hacking, pentesting, OWASP | X | | | | | | Fichas bibliográficas |
| 1.2 | Estado del arte de investigaciones similares | | X | | | | | Matriz en Excel |
| 2 | Análisis del marco normativo y estándares aplicables | | X | | | | | Documento de análisis |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **2.1** | Revisión de normas (ISO 27001, OWASP, NIST) | | X | | | | | Fuentes oficiales |
| **2.2** | Identificación de políticas de seguridad de la cooperativa | | | X | | | | Documento institucional |
| **2.3** | Selección del marco metodológico de pentesting (OWASP Testing Guide, PTES) | | | X | | | | Matriz comparativa |
| **3** | Levantamiento de información del sistema de la cooperativa | | | X | | | | Entrevistas / informes |
| **3.1** | Identificación de activos y arquitectura del sistema | | | X | | | | Diagramas |
| **3.2** | Definición del alcance del pentesting | | | X | | | | Documento de alcance |
| **4** | Ejecución del pentesting | | | | X | X | | Reportes técnicos |
| **4.1** | Recolección de información (Footprinting, Scanning) | | | | X | | | Resultados de herramientas |
| **4.2** | Análisis de vulnerabilidades | | | | X | | | Reportes (Nmap, Nessus, etc.) |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **4.3** | Explotación controlada de vulnerabilidades | | | | | X | | Evidencias técnicas |
| **5** | Evaluación de resultados y análisis de riesgos | | | | | X | | Matriz de riesgos |
| **5.1** | Clasificación de vulnerabilidades (criticidad) | | | | | X | | Tabla de priorización |
| **5.2** | Evaluación del impacto en el sistema | | | | | X | | Informe técnico |
| **6** | Elaboración de propuesta de mejora | | | | | | X | Documento PDF |
| **6.1** | Recomendaciones de mitigación | | | | | | X | Informe final |
| **6.2** | Diseño de políticas de seguridad | | | | | | X | Propuesta estructurada |
| **7** | Redacción del informe final de tesis | | | | | | X | Documento de tesis |
| **7.1** | Revisión y corrección | | | | | | X | Documento versión final |

| L. DECLARACIÓN FINAL |
|---|
| Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna. |

| M. PARTICIPANTES | |
|---|---|
| DIRECTOR: | Ing.Cristhian Humberto Flores Urgiles |
| ESTUDIANTE 1 | CARLOS ISRAEL AVALOS GOMESCOELLO |

| N. FIRMAS DE RESPONSABILIDAD | |
|---|---|
| **Lugar:** | Cañar |
| **Fecha:** | 27 de Abril de 2026 |

**Firmas:**

| | |
|---|---|
| Nombre:<br>Ing.Cristhian Humberto Flores Urgiles<br><br>CC: 0301638375<br>**Director del Proyecto** | Nombre:<br>CARLOS ISRAEL AVALOS GOMESCOELLO<br>C.C.:0302546635<br>**Estudiante / Egresado** |

| O. APROBACIÓN | |
|---|---|
| **Firmas:** | |
| Nombre:<br>CC:<br>**Primer Par Revisor** | Nombre:<br>C.C.:<br>**Segundo Par Revisor** |

**P. REFERENCIAS**

## Bibliografía


Abdullatif Altulaihan, E., Alismail, A., & Frikha, M. (2023). A Survey on Web Application Penetration Testing. *Electronics*.

Alabbad, M., Mhaskar, N., & Khedri , R. (2024). Hardening of network segmentation using automated referential penetration testing. *ELSEVIER*.

Albahar, M., Alansari, D., & Jurcut, A. (2022). An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities. *Electronics*.

Albahar, M., Alansari, Z., & Jurcut, A. D. (2022). Benchmarking vulnerability assessment tools in cybersecurity: Effectiveness and limitations. *Electronics*.

Alhogail, A., & Alkahtani, M. (2024). Automated Extension-Based Penetration Testing for Web Vulnerabilities. *ScienceDirect*.

Almeida, F., & Torres, R. (2023). Cybersecurity challenges in small financial institutions. *Journal of Information Security*, 85–97.

Alqahtani, S. A. (2024). Penetration testing in modern cybersecurity: Techniques, tools, and challenges. *IEEE Access*.

ASAMBLEA NACIONAL. (2021, Mayo 26). *ASAMBLEA NACIONAL*. Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/920-lmoreno/ro-459-5to-sup-26-05-2021.pdf

Behl, A., & Behl, K. (2021). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

CISA. (2026). CISA Adds Two Known Exploited Vulnerabilities to Catalog. *American's Cyber Defense Agency*.

ENISA. (2025). ENISA THREAT LANDSCAPE: FINANCE SECTOR. *European Union Agency for Cybersecurity*.

Fadhli, M. (2024). Comprehensive Analysis of Penetration Testing Frameworks and Tools: Trends, Challenges, and Opportunities. *Indonesian Journal of Electrical Engineering and Renewable Energy*.

FIRST. (2023). Common Vulnerability Scoring System version 4.0. *FIRST Improving Secirity Together*.

Hassan, R. K. (2023). Performance evaluation of cybersecurity tools using empirical metrics. *Computers & Security*.

*Help Net Security*. (2025, Abril 15). Obtenido de https://www.helpnetsecurity.com/2025/04/15/regular-pentesting-strategy-for-organizations/?utm_source=chatgpt.com

ISO/IEC. (2022). Information security, cybersecurity and privacy protection — Information security controls. *ISO/IEC 27005:2022*.

ISO/IEC. (2022a). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. *International Organization for Standardization/International Electrotechnical Commission.*

ISO/IEC. (2022c). Information security, cybersecurity and privacy protection — Guidance on managing information security risks. *ISO*.

ISO/IEC. (2023). Information technology — Information security incident management. *ISO*.

ISTARI. (2024, Septiembre ). *ISTARI*. Obtenido de https://istari-global.com/insights/spotlight/the-state-of-pentesting-2024/?utm_source=chatgpt.com

Lazarov, W., Seda, P., Martinasek, Z., & Kummel, R. (2025). Penterep: Comprehensive penetration testing with adaptable interactive checklists. *ScienceDirect*.

Mahditia Adam, H., Widyawan, W., & Dharma Putra, G. (2023). A Review of Penetration Testing Frameworks, Tools, and Application Areas. *ResearchGate*.

MITRE. (2024). CWE Top 25 Most Dangerous Software Weaknesses - 2024. . *MITRE*.

MITRE Corporation. (2025). CWE Top 25 Most Dangerous Software Weaknesses. *CWE*.

MITRE Corporation. (2026). MITRE ATT&CK version history. . *MITRE ATT&CK* .

National Institute of Standards and Technology. (2022). *Technical guide to information security testing and assessment (SP 800-115)*. Obtenido de https://www.nist.gov

NIST. (2024). National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29).* .

OWASP Foundation. (2023). OWASP API Security. *OWASP*.

OWASP Foundation. (2025). OWASP Top 10:2025. *OWASP* .

OWASP. (s.f). OWASP Web Security Testing Guide. *OWASP*.

Presidencia de la Republica. (2023). REGLAMENTO DE LA LEY ORGÁNICA DE. *Lexis*.

Restrepo Gomez, J., & Correa Ortiz , L. (2024). Bug-Bounty, ¿el futuro del pentesting? *Ciencia e Ingeniería Neogranadina*, 11-22.

SEPS. (2022). Norma de control de seguridades en el uso de canales electrónicos para las entidades financieras controladas por la Superintendencia de Economía Popular y Solidaria. *Superintendencia de Economía Popular y Solidaria*.

SEPS. (2023). NORMA DE CONTROL DE SEGURIDADES EN EL USO DE CANALES ELECTRÓNICOS PARA LAS ENTIDADES FINANCIERAS CONTROLADAS POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA . *Superintendencia de Economia Popular y Solidaria* .

SEPS. (2024). Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116: Norma de control para la administración del riesgo operativo. *Superintendencia de Economía Popular y Solidaria*.

Sharma, P., & Pilli, E. S. (2023). Advancements in penetration testing methodologies using automation and AI. *Cybersecurity*.

Simbaña, F., Flor-Unda , O., Larriva-Novo, X., Acuña , A., Tipán , R., & Acosta-Vargas, P. (2023). A comprehensive analysis of the worst cybersecurity vulnerabilities in Latin America. *informatics*, 71.

## Anexo 2 Guía de entrevista estructurada

## PARTE I. Validación del levantamiento de información

### A. Sistemas, arquitectura y alcance

| |
|---|
| **1. ¿Qué sistemas y servicios aloja el servidor de réplica y cuáles autoriza la cooperativa para las pruebas?** |
| *Respuesta registrada en el levantamiento:*<br>La página web institucional, la aplicación de marcación y los servicios e infraestructura de red asociados. |
| **2. ¿El servidor de réplica reproduce el entorno de producción?** |
| *Respuesta registrada en el levantamiento:*<br>Sí. Reproduce la configuración, las versiones de software y los datos representativos del entorno de producción. |
| **3. ¿En qué segmento de red se ubica el servidor de réplica?** |
| *Respuesta registrada en el levantamiento:*<br>En un segmento de red de laboratorio aislado del entorno de producción. |
| **4. ¿Qué información y accesos se facilitan al evaluador y qué condiciones deben respetarse?** |
| *Respuesta registrada en el levantamiento:*<br>Información parcial y credenciales limitadas (modalidad de caja gris). Sin acciones destructivas, denegación de servicio ni extracción innecesaria de datos; ejecución en horario autorizado. |

## PARTE II. Controles de seguridad existentes

### B. Gestión de accesos

| **5. ¿Existe una política de contraseñas? ¿Se usa autenticación multifactor?** |
| --- |
| *Información registrada:*<br>La cooperativa entregó una Política de control de accesos y gestión de usuarios. Se usa un código de autentificación que llega al correo de cada usuario. |

### C. Cifrado y exposición de servicios

| **6. ¿Los servicios web y las aplicaciones utilizan HTTPS/TLS?** |
| --- |
| Respuesta:<br>Sí. Según el responsable de TI, los servicios web y las aplicaciones de la cooperativa utilizan HTTPS/TLS. |

### D. Actualizaciones y configuración segura

| **7. ¿Con qué frecuencia se aplican parches de seguridad? ¿Existe un procedimiento de configuración segura de servidores antes de ponerlos en operación?** |
| --- |
| Respuesta:<br>La cooperativa cuenta con un proceso formal de gestión de parches, definido en el Manual de políticas para la administración de TI (V5). El proceso comprende identificación de actualizaciones, evaluación técnica, aprobación del cambio, implementación, validación posterior y monitoreo. Los parches se clasifican en críticos, altos, medios y bajos, y se aplican según la criticidad del activo, la severidad de la vulnerabilidad, el impacto operativo y las recomendaciones del fabricante; cuando pueden afectar la disponibilidad de los servicios, se |

| |
|---|
| integran al proceso de gestión de cambios. La política no establece una frecuencia fija de aplicación. |

**E. Políticas y cumplimiento**

| **8. ¿Qué políticas de seguridad están formalmente aprobadas y cuándo se actualizaron?** |
|---|
| *Información registrada:*<br>La cooperativa entregó diez documentos: política general de seguridad de la información; inventario y clasificación de activos de información; metodología de gestión de riesgos de seguridad; política de control de accesos y gestión de usuarios; procedimiento de respaldos y recuperación; plan de continuidad del negocio o de recuperación ante desastres; procedimiento de gestión de incidentes de seguridad; política de protección de datos personales; designación del oficial o responsable de seguridad de la información; plan de capacitación en seguridad. |
| **9. ¿Se han realizado auditorías o evaluaciones de seguridad anteriores?** |
| *Información registrada:*<br>La formulación del problema de la tesis señala la falta de evaluaciones periódicas de seguridad en la cooperativa. |

## Anexo 3 Comandos ejecutados durante el pentesting

Este anexo consolida los comandos ejecutados durante la fase de ejecución del pentesting, con su objetivo y sus parámetros principales, para dar trazabilidad a los hallazgos de la Tabla 10 y la Tabla 13. El descubrimiento inicial se realizó sobre la red 192.168.10.0/24 y el host 192.168.10.179; las pruebas detalladas se ejecutaron sobre el servidor de réplica, referido como $TARGET (192.168.163.1). Las herramientas empleadas fueron Nmap con sus scripts NSE, Gobuster, WhatWeb, curl, Nikto, netstat y nc.

### *Reconocimiento y descubrimiento*

**Tabla A6.1**

| Comando | Objetivo | Parámetros clave |
|---|---|---|
| nmap -sn 192.168.10.0/24 | Red 192.168.10.0/24 | -sn (descubrimiento de hosts, sin puertos) |
| sudo nmap -sn 192.168.10.179 -oN 01_descubrimiento_servidor.txt | 192.168.10.179 | -sn; -oN (salida a archivo) |
| ping -c 4 $TARGET | 192.168.163.1 | -c 4 (cuatro paquetes) |

### *Escaneo de puertos y servicios*

**Tabla A6.2**

| Comando | Objetivo | Parámetros clave |
|---|---|---|
| sudo nmap -Pn -sT -sV --version-light -T3 -p 80,443,8080,3306 192.168.163.1 -oA 01_servicios_iniciales | 192.168.163.1 | -Pn; -sT; -sV; --version-light; -T3; -p; -oA |
| sudo nmap -Pn -n -sT -sV --version-light -T3 -p 80,135,139,443,445,3306,3389,8080 $TARGET | 192.168.163.1 | -Pn; -n; -sT; -sV; -p (barrido ampliado) |
| sudo nmap -Pn -n -O --osscan-limit $TARGET | 192.168.163.1 | -O (detección de SO); --osscan-limit |
| sudo nmap -Pn -n -sU --top-ports 20 --open -T2 --max-rate 20 $TARGET | 192.168.163.1 | -sU (UDP); --top-ports 20; --open; -T2; --max-rate 20 |
| sudo nmap -Pn -n -sT -sV --script "default and safe" -p 80,135,445,3389 $TARGET | 192.168.163.1 | --script "default and safe" |

### *Servicio web / IIS (HTTP)*

**Tabla A6.3**

| Comando | Objetivo | Parámetros clave |
|---|---|---|
| curl -I --max-time 5 http://192.168.163.1/marcacion/ | Ruta /marcacion | -I (HEAD); --max-time |
| curl -i http://$TARGET/ | 192.168.163.1 | -i (cabeceras y cuerpo) |
| curl -i -X OPTIONS http://$TARGET/ | 192.168.163.1 | -X OPTIONS (métodos permitidos) |
| for ruta in / /marcacion/ /phpmyadmin/ /dashboard/ /xampp/; do curl -I --max-time 10 "http://$TARGET$ruta"; done | Rutas comunes | bucle for; -I; --max-time |
| whatweb -a 1 http://$TARGET/ | 192.168.163.1 | -a 1 (nivel de agresividad) |
| whatweb -a 1 http://$TARGET/marcacion/ | Ruta /marcacion | -a 1 |
| sudo nmap -Pn -n -p 80,443,8080,8443 --script http-title,http-headers,http-methods,http-cookie-flags $TARGET | 192.168.163.1 | scripts NSE HTTP |
| sudo nmap -Pn -n -p 80 --script http-title,http-server-header,http-methods,http-enum $TARGET | 192.168.163.1 | scripts NSE HTTP |

### *Enumeración de directorios*

**Tabla A6.4**

| Comando | Objetivo | Parámetros clave |
|---|---|---|
| gobuster dir -u http://192.168.10.179/marcacion -w /usr/share/wordlists/dirb/common.txt | 192.168.10.179 | -u; -w (falló: red inalcanzable) |
| gobuster dir -u http://$TARGET/ -w /usr/share/wordlists/dirb/common.txt -t 5 --delay 200ms -x php,html,txt,bak,old | 192.168.163.1 | -t 5; --delay 200ms; -x (extensiones) |
| gobuster dir -u http://$TARGET/marcacion/ -w /usr/share/wordlists/dirb/common.txt -t 5 --delay 200ms -x php,html,txt,bak,old | Ruta /marcacion | -t 5; --delay 200ms; -x |

### *Análisis con Nikto (sin hallazgos reportados)*

**Tabla A6.5**

| Comando | Objetivo | Parámetros clave |
|---|---|---|
| nikto -h http://$TARGET/ -maxtime 10m | 192.168.163.1 | -h; -maxtime |
| nikto -h http://$TARGET/marcacion/ -maxtime 10m | Ruta /marcacion | -h; -maxtime |

### *HTTPS / TLS*

**Tabla A6.6**

| Comando | Objetivo | Parámetros clave |
|---|---|---|
| sudo nmap -Pn -n -p 443,8443 --script ssl-cert,ssl-enum-ciphers $TARGET | 192.168.163.1 | scripts NSE TLS (443/8443 cerrados o filtrados) |
| curl -k -I --max-time 10 https://$TARGET/ | 192.168.163.1 | -k; -I (conexión TLS fallida) |

### *Base de datos (MySQL, 3306)*

**Tabla A6.7**

| Comando | Objetivo | Parámetros clave |
|---|---|---|
| netstat -ano \| findstr 3306 | Servidor (local, Windows) | -ano (confirma escucha en 0.0.0.0:3306) |
| nc -vz $TARGET 3306 | 192.168.163.1 | -v; -z (prueba de conexión) |
| sudo nmap -Pn -n -p 3306 --script mysql-info $TARGET | 192.168.163.1 | --script mysql-info |

***SMB y RDP***

**Tabla A6.8**

| Comando | Objetivo | Parámetros clave |
|---|---|---|
| sudo nmap -Pn -n -p 445 --script smb2-protocols,smb2-security-mode,smb2-capabilities $TARGET | 192.168.163.1 | scripts NSE SMB |
| sudo nmap -Pn -n -p 3389 --script rdp-enum-encryption $TARGET | 192.168.163.1 | --script rdp-enum-encryption |

*Nota.* Elaboración propia con base en las capturas.

## Anexo 4 Controles y políticas de seguridad propuestos

Este anexo desarrolla los controles técnicos y las políticas de seguridad enunciados en la Fase 5 de la propuesta (sección 4.6). Su finalidad es ofrecer a la Cooperativa de Ahorro y Crédito Yuyay Ltda. un instrumento operativo que traduzca cada hallazgo del pentesting (Tabla 10 y Tabla 13) en un control verificable y en un lineamiento administrativo que sostenga la mejora en el tiempo. Los controles se formulan con base en ISO/IEC 27002:2022, el NIST Cybersecurity Framework 2.0, las guías OWASP y la normativa de la Superintendencia de Economía Popular y Solidaria (SEPS, 2022, 2023, 2024), en concordancia con la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional, 2021).

El anexo se organiza en dos partes. La primera consolida las fichas de control técnico por hallazgo, con el detalle de configuración, la referencia normativa, el responsable, el plazo y el criterio de verificación. La segunda desarrolla las seis políticas de seguridad propuestas, cada una con su objetivo, alcance, lineamientos, responsable y referencia normativa.

### *A4.1 Fichas de control técnico por hallazgo*

La Tabla A4.1 amplía el plan de tratamiento de la Tabla 14, incorporando el detalle de la configuración esperada y el criterio con el que se verificará el cierre de cada hallazgo durante la reprueba (retest).

**Tabla A4.1**

*Fichas de control técnico por hallazgo*

| ID | Control y configuración esperada | Referencia | Verificación (retest) |
|---|---|---|---|
| H-01 | Restringir MySQL a la interfaz local (bind-address = 127.0.0.1) o a la red interna estrictamente necesaria; aplicar firewall de host; actualizar el motor y ocultar la versión; endurecer credenciales y privilegios. | ISO/IEC 27002: 8.20, 8.9; NIST CSF: PROTECT; SEPS seguridad de la información | netstat confirma escucha solo en 127.0.0.1; nc desde la red no establece conexión al 3306. |
| H-02 | Implementar HTTPS con certificado válido; forzar redirección de HTTP a HTTPS; deshabilitar protocolos y cifradores obsoletos; habilitar HSTS. | OWASP WSTG; ISO/IEC 27002: 8.24; SEPS canales electrónicos | Conexión TLS establecida (443); redirección 301 desde HTTP; cabecera HSTS presente. |
| H-03 | Deshabilitar el método HTTP TRACE (y TRACK); limitar los métodos permitidos a los estrictamente necesarios (GET, HEAD, POST). | OWASP; ISO/IEC 27002: 8.9 | La respuesta a OPTIONS ya no anuncia TRACE; una petición TRACE devuelve 405. |
| H-04 | Configurar las cabeceras de seguridad HSTS, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options y Referrer-Policy. | OWASP Secure Headers; NIST CSF: PROTECT | curl -I muestra las cinco cabeceras con valores válidos. |
| H-05 | Suprimir o enmascarar la cabecera Server y los banners de versión; reemplazar la página por defecto de IIS por una configuración endurecida. | ISO/IEC 27002: 8.9; OWASP | La cabecera Server no revela producto ni versión; no se sirve la página por defecto de IIS. |
| H-06 | Inventariar y justificar el segundo servidor web (8080); deshabilitarlo si no es requerido; endurecerlo y restringir su acceso por firewall si lo es. | ISO/IEC 27002: 8.9, 8.20; NIST CSF: IDENTIFY | El servicio 8080 está deshabilitado o restringido por firewall al ámbito autorizado. |
| H-07 | Segmentar la red y restringir por firewall los servicios de Windows (SMB, NetBIOS, MSRPC, UPnP/SSDP) al ámbito estrictamente necesario; deshabilitar los no requeridos. | ISO/IEC 27002: 8.20, 8.22; NIST CSF: PROTECT; SEPS riesgo operativo | Un escaneo desde otro segmento ya no expone SMB/NetBIOS/MSRPC/UPnP. |

*Nota.* Elaboración propia con base en la Tabla 14 y en las evidencias de la Fase 3.

### *A4.2 Políticas de seguridad propuestas*

Las siguientes políticas complementan los controles técnicos y buscan institucionalizar la gestión de la seguridad de la información como un proceso continuo. Cada política debe ser aprobada por la instancia competente de la cooperativa, difundida al personal y revisada de forma periódica.

### *A4.2.1 Política de gestión de vulnerabilidades*

**Objetivo.** Establecer un ciclo periódico y documentado de identificación, valoración, tratamiento y verificación de las vulnerabilidades de los sistemas de información de la cooperativa.

**Alcance.** Aplica a todos los sistemas, servicios, aplicaciones e infraestructura de red administrados por la cooperativa o por terceros bajo su responsabilidad.

**Lineamientos.**

- Realizar evaluaciones de vulnerabilidades y pruebas de penetración con una periodicidad definida y ante cambios significativos en la infraestructura.
- Registrar cada hallazgo con su severidad (CVSS v4.0), su riesgo asociado (ISO/IEC 27005:2022 y MAGERIT), el responsable, el plazo y el estado de tratamiento.
- Ejecutar una reprueba (retest) tras aplicar los controles para confirmar la reducción del riesgo residual.
- Conservar la trazabilidad de las evidencias de detección, tratamiento y cierre.

**Responsable.** Oficial de Seguridad de la Información / Área de TI

**Referencia normativa.** Res. SEPS 2022-002; ISO/IEC 27002: 8.8; NIST CSF: IDENTIFY, RESPOND

### *A4.2.2 Política de endurecimiento (hardening) de servidores y servicios*

**Objetivo.** Garantizar que los servidores y servicios se configuren de forma segura antes de su puesta en producción y se mantengan en ese estado durante su ciclo de vida.

**Alcance.** Aplica a servidores, servicios web, bases de datos y servicios de red de la cooperativa.

**Lineamientos.**

- Definir líneas base de configuración segura por tipo de servicio y verificarlas antes de la puesta en producción.

- Deshabilitar servicios, puertos, métodos y páginas por defecto innecesarios (p. ej., TRACE, banners de versión, página por defecto de IIS).
- Aplicar las cabeceras de seguridad HTTP y ocultar la información de versión de los servicios expuestos.
- Gestionar los parches de seguridad con una frecuencia definida y documentada.

**Responsable.** Área de TI

**Referencia normativa.** ISO/IEC 27002: 8.9; OWASP Secure Headers; NIST CSF: PROTECT

### *A4.2.3 Política de gestión de accesos y credenciales*

**Objetivo.** Asegurar que el acceso a los sistemas se otorgue bajo el principio de mínimo privilegio y que las credenciales se gestionen de forma segura.

**Alcance.** Aplica a todas las cuentas de usuario, de servicio y administrativas de los sistemas de la cooperativa.

**Lineamientos.**

- Aplicar el principio de mínimo privilegio y revisar periódicamente los permisos asignados.
- Exigir credenciales robustas y habilitar la autenticación multifactor en los accesos críticos y administrativos.
- Restringir el acceso a las bases de datos únicamente a los servidores de aplicación autorizados.
- Registrar y auditar los accesos a los activos críticos.

**Responsable.** Área de TI / Oficial de Seguridad de la Información

**Referencia normativa.** ISO/IEC 27002: 5.15, 5.16, 5.18, 8.2; Res. SEPS 2022-002

### *A4.2.4 Política de cifrado y protección del transporte*

**Objetivo.** Proteger la confidencialidad e integridad de la información en tránsito mediante el uso obligatorio de cifrado en los servicios que transmiten datos de los socios.

**Alcance.** Aplica a todos los servicios web, aplicaciones y canales electrónicos que transmitan información institucional o de socios.

**Lineamientos.**

- Utilizar HTTPS/TLS con certificado válido en todos los servicios que transmitan información de socios.
- Forzar la redirección de HTTP a HTTPS y habilitar HSTS.
- Deshabilitar los protocolos y cifradores obsoletos o inseguros.
- Revisar periódicamente la vigencia de los certificados.

**Responsable.** Área de TI

**Referencia normativa.** ISO/IEC 27002: 8.24; OWASP WSTG; SEPS canales electrónicos; LOPDP

### *A4.2.5 Política de segmentación de red*

**Objetivo.** Reducir la superficie de ataque y dificultar el movimiento lateral mediante la separación de entornos y la restricción del tráfico entre segmentos.

**Alcance.** Aplica a la infraestructura de red que soporta los sistemas financieros y administrativos de la cooperativa.

**Lineamientos.**

- Separar los entornos y los servicios según su criticidad y función.
- Restringir por firewall los servicios propios de Windows (SMB, NetBIOS, MSRPC, UPnP/SSDP) al ámbito estrictamente necesario.
- Inventariar y justificar todo servicio expuesto; deshabilitar los no requeridos.
- Controlar y registrar el tráfico entre segmentos.

**Responsable.** Área de TI / Redes

**Referencia normativa.** ISO/IEC 27002: 8.20, 8.22; NIST CSF: PROTECT; SEPS riesgo operativo

### *A4.2.6 Política de capacitación y concienciación en seguridad*

**Objetivo.** Fortalecer el factor humano mediante la formación periódica del personal técnico y administrativo en buenas prácticas de seguridad de la información.

**Alcance.** Aplica a todo el personal de la cooperativa con acceso a los sistemas de información.

**Lineamientos.**

- Capacitar al personal técnico en configuración segura, gestión de vulnerabilidades e interpretación de los resultados de las evaluaciones.
- Concienciar al personal administrativo sobre phishing, ingeniería social y manejo seguro de credenciales.
- Programar la capacitación de forma periódica y registrar la asistencia.
- Difundir los procedimientos de reporte de incidentes de seguridad.

**Responsable.** Oficial de Seguridad de la Información / Talento Humano

**Referencia normativa.** Res. SEPS 2022-002; ISO/IEC 27002: 6.3; NIST CSF: GOVERN

# AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

**CARLOS ISRAEL AVALOS GOMESCOELLO** portador de la cédula de ciudadanía N.º **0302546635**. En calidad de autor y titular de los derechos patrimoniales del trabajo de investigación **"Evaluación de la seguridad informática mediante pentesting en los sistemas de información de la Cooperativa de Ahorro y Crédito Yuyay Ltda."** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de investigación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

**Cañar, 29 de septiembre 2026**



**Carlos Israel Avalos Gomescoello**

**C.I. 0302546635**