Articulo de revisión

Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web

Computer security, methodologies, standards, and management framework in an approach to web applications

Iván Alberto Coronel Suárez ✉ https://orcid.org/0000-0002-2084-189
Daniel Ivan Quirumbay Yagual ✉ https://orcid.org/000-0002-6513-3520

Universidad Estatal Península de Santa Elena, UPSE | La Libertad - Ecuador | CP 240350

✉ icoronel@upse.edu.ec

https://doi.org/10.26423/rctu.v9i2.672
Páginas: 97- 109

Resumen

Existen diferentes métodos para evaluar la seguridad de las aplicaciones Web, principalmente basados en algún técnico automatizado de escaneo El objetivo de la presente investigación refiere de los conceptos básicos necesarios para entender temas de seguridad informática en sistemas de información y servicios, con el propósito de enfocarlos en pruebas de penetración en las aplicaciones web, se abordan metodologías que pueden aplicarse y marcos de referencia que deben ser tomados en cuenta en el ciclo de vida de desarrollo de aplicaciones, así mismo, se aporta con tablas descriptivas de las metodologías utilizadas en pruebas de *Pentesting* llegando finalmente a abarcar la familia de ISO/IEC 27 000 dejando plasmado en la discusión una breve descripción de las mismas y el uso que da en las implantaciones de SGSI, evaluaciones y auditorias de seguridad de la información.

Palabras clave: ciberseguridad, ISSAF, OWASP, OSSTMM.

Abstract

There are various methods for evaluating the security of Web applications, most of which rely on automated scanning technicians. The goal of this research is to address the fundamental concepts required to understand computer security issues in information systems and services, with a focus on penetration tests in web applications. Methodologies that can be applied and reference frameworks that must be taken into account in the application development life cycle are addressed; additionally, descriptive tables of the methodologies used in pen-testing tests are provided, finally reaching the ISO/IEC 27000 family, leaving a brief description of the same and the use it gives in ISMS implementations, information security evaluations and audits.

Keywords: cybersecurity, ISSAF, OWASP, OSSTMM.

Recepción: 02/05/2022 | Aprobación: 24/10/2022 | Publicación: 23/12/2022

1. Introducción

Hoy en día, el avance tecnológico y el apogeo del Internet hacen posible que se puedan ofrecer un sinnúmero de servicios por parte de las instituciones, tales como: sistemas de ventas, transacciones financieras, inventarios, consultas médicas, pagos de tasas, servicios de correo, repositorios, portales bancarios y académicos; entre otros, que permiten tener acceso completo a datos que a su vez viajan por diferentes redes públicas y pueden ser accedidos desde cualquier lugar o dispositivo.

En años anteriores, la protección de la información era más sencilla, ya que las grandes plataformas de datos actuaban de forma independiente sin conectividad alguna, las arquitecturas existentes eran totalmente centralizadas y las terminales tenían capacidades de procesamiento limitadas [1].

Este desarrollo ha ocasionado un aumento en la exposición de las organizaciones y de los usuarios a violaciones de seguridad que pueden poner en riesgo la confidencialidad, integridad y reputación de estos.

El estudio de la calidad de los componentes software juega un papel muy importante en el DSBC, los procesos de selección de componentes es necesario conocer con detalle el comportamiento relativo a aquellos criterios que se corresponden con los requisitos del sistema en desarrollo, tanto funcionales como no-funcionales [2].

Las aplicaciones web son plataformas que convergen una serie de servicios que hacen uso de datos para posterior tratamiento y entrega de información, estas se desarrollan para ser accedidas desde programas (navegadores) que permiten interpretar la información que viaja por medio del protocolo de transferencia de hipertexto que a su vez acceden a datos en servidores, dicho proceso de petición y respuesta en esta infraestructura cliente – servidor pueden producir agujeros de seguridad o vulnerabilidades que deben ser correctamente tratadas en los procesos de desarrollo e implementación de las aplicaciones que brindará un determinado servicio.

Existen diferentes métodos para evaluar la seguridad de las aplicaciones Web, principalmente basados en algún técnico automatizado de escaneo. Un tipo de método de escaneo alimenta datos aleatorios a la aplicación y monitorea su comportamiento.

El otro tipo utiliza una base de datos con vulnerabilidades predefinidas que se verifican una por una hasta que se encuentra una vulnerabilidad o se puede afirmar que la aplicación no tiene ninguna vulnerabilidad conocida [3].

Estas vulnerabilidades que existen en las aplicaciones web pueden ser descubiertas por delincuentes informáticos incluso llegando a ser explotadas por medio de herramientas automatizadas, en la actualidad existe un acelerado desarrollo de ataques informáticos ya sea a la infraestructura tecnológica, servidores, aplicaciones y a los usuarios.

El presente trabajo proporciona, en primer lugar, una breve introducción a las aplicaciones web y una serie de términos que deben ser abordados para la comprensión de la investigación planteada. Se describe los diferentes enfoques de las pruebas que se realizan en el diagnóstico de las aplicaciones.

Seguidamente, se analiza las tendencias en las evaluaciones de seguridad y buenas prácticas y finalmente, en la última la sección de esta investigación se concluye y se plantean futuros trabajos de investigación.

2. Materiales y métodos

La presente investigación se realiza utilizando el método analítico-sintético para el desglose del tema abordado, detallando en partes y elementos del mismo, para su completa comprensión en cuanto a los significados exactos de los términos de ciberseguridad, pentesting o hacking ético y los principales estándares y metodologías existentes en el área de seguridad informática, direccionando su estudio final al campo de las aplicaciones web.

La seguridad informática se enfoca en minimizar los riesgos y vulnerabilidades en los recursos de hardware y software relacionados con el acceso y la utilización malintencionada de la información de los sistemas de software, para garantizar la integridad, confidencialidad y disponibilidad de esta [4].

Amenazas (Threat)

Es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático [5]. Las amenazas informáticas están relacionadas con la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre los activos informáticos y los sistemas de información [6].

Vulnerabilidad (Vulnerability)

Cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades, también conocidas como “agujeros de seguridad”, pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas, etc [5].

Riesgo (Risk)

Es la probabilidad de que una amenaza se materialice aprovechándose de alguna vulnerabilidad existente causando un impacto en la organización.

Ataque informático (Computer attack)

Acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo, se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema [5].

Hacker (Hacker)

Sujetos con grande conocimiento sobre tecnologías de la información y comunicación, tienen habilidades sobre hardware, software, lenguajes de programación, protocolos, etc., interesados en cómo funcionan los sistemas de información, su categorización está de acuerdo con su accionar.

Hackers de sombrero negro (Black Hat Hackers)

Los hackers que se infiltran en redes y computadoras con fines maliciosos [5].

Los hackers de sombrero son aquellos que explotan las vulnerabilidades en los sistemas con el propósito de demostrar que han burlado la seguridad de la entidad [7].

Hackers de sombrero gris (Gray Hat Hacker)

El gris designa a hackers cuyas acciones se sitúan en la frontera de la legalidad, siendo el caso, por ejemplo, de aquellos individuos que utilizan la ingeniería inversa para deconstruir, conocer y socializar el funcionamiento del software privativo [8].

Un híbrido entre los hackers de sombrero negro y los hackers de sombrero blanco, buscan vulnerabilidades en sistemas sin tener autorización la motivación de ellos es la curiosidad de entrar a sistemas, algunos después de hacerlo ofrecen sus servicios para solucionar las vulnerabilidades.

Hackers de sombrero blanco (White Hat Hackers)

Se refiere a los expertos en seguridad informática que se especializan en realizar pruebas de penetración con el fin de asegurar que los sistemas de información y las redes de datos de las empresas [9].

El blanco hace refe- rencia a hackers que evalúan y penetran los sistemas informáticos en el marco de una relación contractual [8].

Pruebas de penetración (Pentesting)

Este tipo de pruebas caracterizan aspectos esenciales para determinar hasta qué punto son válidos los procedimientos, herramientas y pruebas de seguridad propuestas en las metodologías para abordar los retos actuales en el campo de las aplicaciones web [10].

Hacking ético (Ethical Hacking)

Hace referencia a la realización de diferentes pruebas de seguridad a un sistema de TI, con el fin de emitir un informe en el cual describa las brechas de seguridad existentes, permitiendo a los administradores de TI de las organizaciones ejecutar medidas preventivas y salvaguardar la integridad de los sistemas y de la información [11].

El Hacking ético es una herramienta que permite probar las medidas de seguridad informática de una organización, mediante pruebas de intrusión a sistemas informáticos, mediante las cuales se pueden poner en funcionamiento herramientas para realizar ataques informáticos y si se sigue un orden ya escrito y probado, resulta factible introducirse a sistemas que no cuenten con las medidas de seguridad adecuadas, o que no han sido sometidos a pruebas de intrusión para detectar sus debilidades [12].

Aplicaciones web (Web applications)

Todas las aplicaciones web son semejantes en su utilización e incluso en su forma de descarga, pero diferencian entre ellas en la tecnología, cantidad de servicios y muchas veces en los protocolos que se encuentran detrás, si se hace una comparación con sus análogas que son las aplicaciones de escritorio incluso podríamos llegar a ver que se ejecutan en ambientes diferentes.

Las aplicaciones web ha propiciado el surgimiento de riesgos de seguridad que atentan contra la disponibilidad, integridad y confidencialidad de la información, normalmente con un objetivo lucrativo; esto se debe a que los sistemas informáticos modernos son susceptibles a problemas de seguridad, por la conectividad, extensibilidad y complejidad de estos [13].

Las aplicaciones web se ejecutan en entornos operativos que pueden ser accedidos desde Internet, al hablar de acceso no necesariamente es ingresar al uso de esta, sino más bien el hecho de llegar a tener una interacción con el equipo que las aloja, lo que hace que este sea susceptible a diversos ataques como podría ser ataques de denegación de servicio distribuido (DDoS).

Un DDoS es un procedimiento que atenta contra los recursos de red de un servidor principalmente web y de base de datos, dejando no disponible el servicio para los usuarios de forma temporal o indefinidamente [14].

La norma ISO 27001, aporta un Sistema de Gestión de Seguridad de la Información (SGSI) que consiste en medidas para proteger la información planteando garantizar la confidencialidad, integridad y disponibilidad de esta, adicionales también se integran autenticidad, trazabilidad, no repudio y auditabilidad [15].

Las aplicaciones web cumplen con un ciclo de vida para su desarrollo, tratando de asegurar que se efectúen los procesos, medidas adecuadas para su correcto funcionamiento y niveles aceptables de seguridad y calidad. Metodologías como SDLC (Software

Development Life Cycle) dentro de sus fases presenta la de pruebas que se ejecuta después de la creación de la aplicación para la identificación de fallos o errores y proceder al tratamiento de este, muchas veces este proceso se enfoca al análisis de pruebas de funcionamiento y no a niveles de seguridad por lo que suele pasarse a la fase de despliegue o puesta en producción.

Webcrawler

Conocido con varias denominaciones tales como rastreador, araña, robot de búsqueda, crawler, bot, es un instrumento que cumple múltiples propósitos de análisis y extracción de información de la web. Esta herramienta de investigación principalmente para realizar estudios cibermétricos y webmétircos [16].

Un adversario de la red podría arrancar con algo muy simple como una recopilación de información, aunque la recopilación inteligente puede parecer desalentadora a primera vista, se podría revelar muchas fuentes de información sobre la empresa víctima, que podrían ir desde lo más benigno hasta las más peligrosas, por tanto, el webcrawler se convierte en una técnica cada vez más utilizados por hackers [17].

2.1. Metodologías, certificaciones y marcos de referencia

La movilidad es inevitable, a la vez que costosa, por ello departamentos de tecnología necesitan plataformas para desarrollar, integrar y dar seguridad a las aplicaciones corporativas, independientemente de la interfaz que el usuario elija para acceder a las mismas. Para lograr este objetivo se requiere una plataforma completa que gestione desde el desarrollo de la interfaz hasta la integración con las aplicaciones internas, y todo ello de una forma segura y escalable [18].

A continuación, se mencionan metodologías disponibles para realización de pruebas de penetración:

Open-Source Security Testing Methodology Manual (OSSTMM)

Metodología de fuente abierta para realizar pruebas de seguridad intensivas, precisas y eficientes, publicada por el Institute for Security and Open Methodologies (ISECOM). Se pueden considerar cuatro fases: [10].

a. Inducción donde se establece el alcance, los requerimientos y restricciones de la auditoría.
b. Interacción aquí se trata de descubrir relaciones entre el alcance, los objetivos y los activos involucrados.
c. Requerimientos donde se realizan verificaciones de procesos, de configuraciones, capacitaciones, propiedad intelectual, información expuesta y otros.
d. Intervención esta se enfoca en la penetración de los objetivos y su afectación

Esta metodología propone una mirada holística de la seguridad; sin embargo, al tener un alcance tan amplio utiliza como fundamento en su estructura una división de clases y canales, que representan las interacciones que puede tener un activo dentro de la organización; la metodología sugiere que se debe realizar pruebas de seguridad sobre cada canal [19].

La metodología se subdivide en aspectos más importantes de la organización:

- Seguridad de la Información.
- Seguridad de los Procesos.
- Seguridad de las Tecnologías de Internet.
- Seguridad en las Comunicaciones.
- Seguridad Inalámbrica.
- Seguridad Física.

Se pueden distinguir fases como:

a. Fase de inducción.
b. Fase de interacción
c. Fase de investigación
d. Fase de intervención

Security Information Systems Assessment Framework (ISSAF)

Metodología del marco de evaluación de la seguridad de los sistemas de información, la misma cuenta con el apoyo del grupo de seguridad de los sistemas de información abiertos (OISSG).

ISSAF divide el proceso de pentesting en tres fases

a. Planificación y preparación.
b. Evaluación
c. Informar, limpiar y destruir artefactos

Debe utilizarse principalmente para cumplir con los requisitos de evaluación de seguridad de una organización y, además, puede utilizarse como referencia para satisfacer otras necesidades de seguridad de la información. Dentro de las principales ventajas de esta metodología se tiene que no requiere un conocimiento previo sobre pruebas de seguridad o metodologías de intrusión. Además, brinda suficiente información para que un especialista con pocos conocimientos comprenda cómo aplicar las pruebas de seguridad [20].

Open Web Security Project Application (OWASP)

Proyecto abierto de seguridad de aplicaciones web, recopila y estructura pruebas de seguridad enfocadas en las aplicaciones web. Esta guía está reconocida como la más amplia y abarcadora con respecto a las demás metodologías, para el campo de las aplicaciones web [20].

Plantea la estructura de una prueba de seguridad de una aplicación web, esta se divide en dos: pasiva y activa. Pasiva hace referencia a interacción con la aplicación directamente en busca de entender lógica, entradas y salidas.

En la activa con el conocimiento adquirido en las pruebas pasivas se intenta vulnerar la aplicación, para las pruebas de seguridad activas [19].

Esta metodología propone 11 categorías y 91 controles

a. Recopilación de información.
b. Pruebas de gestión de configuración e implementación
c. Pruebas de gestión de identidad
d. Pruebas de autenticación
e. Pruebas de autorización
f. Pruebas de gestión de sesión
g. Pruebas de validación de ingreso
h. Manejo de errores
i. Criptografía
j. Pruebas de lógica del negocio
k. Pruebas del punto de vista del cliente

Ethical Hacking Certificate (CEH)

Es una certificación más que una metodología, el objetivo de esta es formar profesionales en seguridad informática (hackers éticos) es orientada en su totalidad a la práctica en busca de vulnerabilidades haciendo uso de herramientas y técnicas que usan los atacantes.

En ella se pueden ver 5 fases que van desde recopilación de información hasta borrado de logs:

a. Reconocimiento
b. Descubrimiento, escaneo
c. Obtención de acceso
d. Mantener el acceso
e. Limpiar el rastro

Ante la amenaza de ataques informáticos, las organizaciones deben demostrar que realizan una gestión competente y efectiva de la seguridad de los recursos y datos que gestionan. Este aspecto hace necesario el uso de estándares o normas que le orienten de forma estructurada, sistemática y coherente cómo proceder ante una situación de este tipo [4].

2.2. Estándares y marco de referencia

La utilización de técnicas de programación segura siguiendo marcos y estándares se relaciona significativamente con la cantidad de vulnerabilidades encontradas en aplicaciones web y por lo tanto mejora el nivel de seguridad de estas [21].

Parte importante para un profesional de la seguridad es la aplicación de estándares, marcos de referencia y mejores prácticas como ISO, COBIT, ITIL. Si se analiza los pilares fundamentales de la seguridad informática como son: integridad, confidencialidad, disponibilidad, no repudio y autenticación, estos se abordan en las normas ISO.

ISO 17799

Recomendaciones para gestionar la seguridad de la información dirigidas a los responsables de mantener la misma en las organizaciones.

Ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar y mantener la seguridad de una organización. Define la información como un activo que posee valor y requiere por tanto de una protección adecuada [4].

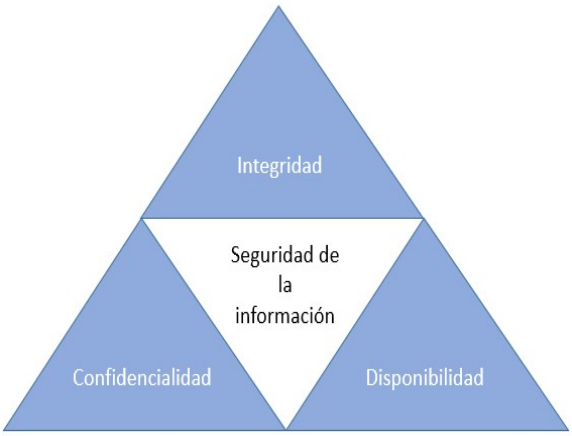

Figura 1: Seguridad Informática según la norma ISO/IEC 17799

Familia de ISO/IEC 27000

Las normas para implementar un SGSI corresponden a la serie ISO/IEC 27000 publicadas por la ISO y

la Comisión Electrotécnica Internacional (IEC), compuesta por aproximadamente 17 normas, clasificadas en cuatro categorías: [22].

i. La norma que contiene el vocabulario, contenido en la norma ISO/IEC 27000.

ii. las normas de requerimientos, contenidos en la norma ISO/IEC 27001 y la norma ISO/IEC 27006.

iii. las normas guía desarrolladas a través de 10 normas: ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008, ISO/IEC 27013, ISO/IEC 27014, TR 27016, ISO/IEC 27032

iv. las normas para sectores específicos, contenidas en las normas ISO/IEC 27010, ISO/IEC 27011, TR 27015 y TS 27017

ISO/IEC 27000:2014

Descripción de los sistemas de gestión de seguridad de la información (SGSI), términos y definiciones comúnmente utilizados en la familia de normas de SGSI, aplicable a todos los tipos y tamaños de organizaciones.

ISO/IEC 27001:2013

Especifica requerimientos para establecer, implementar, mantener y mejorar un SGSI dentro de una organización. Incluye además requisitos para la evaluación y tratamiento de riesgos de seguridad de la información, así mismo, los requerimientos establecidos son aplicables a todo tipo de organización independiente de su tipo o tamaño.

ISO/IEC 27002:2013

Brinda pautas para los estándares de seguridad de la información de la organización y las prácticas para la gestión de esta, incluye pautas para los procesos de selección, implementación y gestión de controles. Antigua ISO 17799:2005.

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Cuenta con 14 Dominios, 35 Objetivos de Control y 114 Controles. Se diferencia de la anterior (27001) que está enfocada a controles y no a procesos [4].

Control Objetives for Information and related Technology (COBIT)

Es un marco de referencia desarrollado, mantenido por la Asociación de Auditoría y Control de Sistemas de Información del Instituto de Gobernanza de las Tecnologías de la Información (ITGI por las siglas en inglés de Information Technology Governance Institute).

Este marco de referencia permite gobernar y gestionar de manera holística las infraestructuras TI, logrando el equilibrio entre la generación de beneficios, la optimización de niveles de riesgo y el uso eficiente de recursos [23].

El Marco COBIT es muy utilizado por auditores en todo el mundo, los miembros de ISACA (Information System Audit and Control Association), estos utilizan la metodología de COBIT en sus operaciones cotidianas. COBIT fue inicialmente publicado e implementado en 1996 y durante los últimos años, su alcance ha ido creciendo gradualmente.

Presenta un conjunto de mejores prácticas, enfocadas en el control más que en la ejecución, que permiten optimizar la inversión en TI que una organización realiza. Este modelo define un conjunto de criterios de control, en base a requisitos de calidad, confianza y seguridad [24].

3. Discusión

Tipos de hackers

La recopilación de información presentada en el marco teórico sobre tres tipos de hacker que existen, da una perspectiva general de su clasificación, en la Tabla 1 se amplía, además de la descripción, las motivaciones que podrían tener dependiendo de su clasificación.

Para la ejecución de las pruebas de penetración se requieren múltiples recursos, herramientas, scripts, escáner de red, sin embargo, dentro de todos estos requerimientos es necesario definir una metodología a seguir para poder obtener los resultados de todo el proceso de las pruebas realizadas, en la Tabla 2 se presenta las tres metodologías objetos de este trabajo como los son OSSTMM, ISSAF y OWASP, el objetivo principal de esta agrupación es proporcionar una visión rápida en la selección de una a seguir, de los cuales se puede apreciar que la primera metodología revisada cuenta con cuatro fases que cuentan con 17 módulos a aplicar en la organización en sus áreas de: seguridad de la información, seguridad de los procesos, seguridad de las tecnologías de Internet, seguridad en las comunicaciones, seguridad inalámbrica, seguridad física.

ISSAF, cuenta con tres fases y cada una de ellas con sus respectivas actividades (AF1 - AF3) se puede apreciar desde las reuniones iniciales hasta la presentación de informes, esta metodología o marco de evaluación de seguridad incluye su propio framework para pruebas de intrusión (Penetration Testing Framework - PTF) que podría ser abordado en caso de seleccionar ISSAF para cumplir con los requerimientos de seguridad de la organización y, además puede ser tomada como referencia para pruebas en las aplicaciones web que son objetos del estudio realizado

Tabla 1: Vista general de tipos de hackers y sus motivaciones

Tipos de Hackers	Descripción	Motivación
White Hat Hackers / Hackers sombrero blanco	Profesionales de la seguridad informática, realizan investigaciones en busca de vulnerabilidades y fallos, pero bajo un contrato y previa autorización de la organización que se evalúa. Las empresas cuentan con uno entre sus empleados de TIC o contratan externamente para poner a prueba sus sistemas, exponer dichas vulnerabilidades y corregirlas antes de que un delincuente informático las explote.	Buscan mejorar los sistemas en temas de seguridad. Buscan salvaguardar los pilares de la seguridad informática, confidencialidad, integridad y disponibilidad. Remuneración constante de la empresa que los tiene entre sus filas
Black Hat Hackers / Hackers sombrero negro	Clasificados como delincuentes informáticos, crackers, infractores de la ley tienen un conocimiento amplio al igual que los profesionales de seguridad, la diferencia es que estos utilizan sus habilidades para ingresar a sistemas sin autorización con el fin de robar o secuestrar información que podría darle un beneficio económico por medio de la venta de esta o rescate por ella.	Buscan beneficio propio/económico. Robar, modificar, destrozar información por medio de spam, programas malignos, explotación de vulnerabilidades de servidores o aplicaciones web, con el fin de vender luego los datos al mejor postor
Gray Hat Hackers / Hackers sombrero gris	Estos híbridos entre un hacker de sombrero blanco y un hacker de sombrero negro no utilizan sus conocimientos para conseguir un beneficio económico, realizan intrusiones de seguridad sin autorización para exponer a una determinada organización "haciéndole un favor a la empresa" y luego vender sus servicios para remediar los fallos	Rompen sistemas para luego ofrecer sus servicios para solucionar los mismos. Espiar países. Defender algunas veces ideologías, y otras veces atacar según el movimiento que apoye.

Finalmente OWASP, que se aplica en el ciclo de vida de desarrollo de software (SDLC) pero en sus etapas finales F4 o F5 según podemos apreciar la Tabla 2, el análisis que se realiza pretende plasmar la necesidad de aplicar desde las primeras fases F1 (antes del inicio del desarrollo) en el análisis de la elección de la tecnología con la que se va a desarrollar la aplicación (framework) que muchas veces se deja demasiada responsabilidad a estos sin estudiar o analizar las extensiones internas que estos ocupan, resulta necesario el análisis de la versiones de estas.

OWASP con su guía de pruebas versión 4.0 se enfoca a las aplicaciones web por lo que el estudio presente lo toma como referencia a aplicar en este tipo de trabajos con el fin de desarrollar software confiable que permita salvaguardar los pilares de la seguridad informática. La discusión de las metodologías y la elección de la que más se dirige a aplicaciones web crea la necesidad de analizar el AF4 de la Tabla 2, que es donde se empieza a aplicar las pruebas de penetración que OWASP lo aplica con un enfoque de prueba de intrusión de caja negra (se conoce muy poco del objetivo) y que dependiendo de las pruebas a realizar, herramientas y fase en la que el profesional de seguridad se encuentre, las pruebas serán de modo pasivo (sin interacción con equipos, ni las aplicaciones directas de la organización auditada) en este caso las pruebas de recopilación de información. Las siguientes pruebas o actividades según la información presentada catalogan de modo activo (se necesita interactuar con las aplicaciones y los servidores que las alojan).

Tabla 2: Vista general de tipos de hackers y sus motivaciones

OSSTMM	ISSAF	OWASP 4.0
	Fases	
F1 De inducción	F1 Planificación y preparación	F1 Antes del inicio del desarrollo
F2 De interacción	F2 Evaluación	F2 Durante la definición y diseño
F3 De investigación	F3 Informar, limpiar y destruir artefactos	F3 Durante el desarrollo
F4 De intervención		F4 Durante la fase de implementación F5 Mantenimiento y operaciones
	Módulos y actividades por fases	
MF1 Revisión de postura logística	AF1 Reuniones iniciales, definición alcance, contactos y ruta de pruebas	AF1 Revisar el proceso SDLC, revisión de políticas, revisión de estándares.
MF2 Verificación de detección activa, auditoria de visibilidad, verificación de accesos, verificación de confianza, verificación de controles, verificación de procesos.	AF2 Recolección de información, mapeo de red, identificación de vulnerabilidades, penetración, obtener acceso y escalamiento de privilegios, enumeración, compromiso remoto de usuarios y sitios, mantener acceso, cubrir huellas.	AF2 Revisión de requerimientos, revisión de diseño y arquitectura, creación/revisión de modelos UML, creación/revisión de modelos amenaza
MF3 Verificación de configuración, validación de la propiedad, revisión de la segregación, verificación de la exposición, exploración de la inteligencia competitiva.	AF3 Presentación de avances, hallazgos encontrados y evidencias de trabajos realizados, Informes (actividades realizadas, fechas, horas, herramientas, resultados obtenidos de cada actividad, lista de vulnerabilidades, lista de acciones propuestas).	AF3 Revisión de código, tutoriales de código, pruebas de sistema y unidad AF4 Prueba de penetración, revisión de configuración de administración, pruebas de sistema y unidad, pruebas de aceptación.
MF4 Verificación de la cuarentena, auditoria de privilegios, Validación de la supervivencia/continuidad del servicio, revisión de alertas y registros/estudio final		AF5 Oportunidad de verificación, controles de salud, revisión de administración de operación, pruebas de regresión.

Dentro de los ciclos de vida de desarrollo es necesario implementar controles de seguridad y validación, inicialmente se define y documenta las normas y los procedimientos que se efectúan en las fases de desarrollo de software, aplicativos y en la infraestructura en las que se van a alojar. Para ejecutar lo mencionado anteriormente es necesario la aplicación de las normas ISO/IEC 27000 que aplica a todos los sistemas de información y comunicación.

En la Tabla 3 se realiza un extracto de norma ISO/IEC 27000, en la que se clarifica de una manera resumida lo que presenta cada una de las normas dentro de la familia de la 27000, donde, necesariamente se debe introducir primeramente en esta ya que contiene la terminología necesaria para su entendimiento, así como la terminología de los Sistemas de Gestión de Sistemas de Información, luego se detallan los documentos donde se describen objetivos de control, buenas prácticas y directrices para gestión de incidentes y riesgos, dentro de los controles el A14 abarca temas de Adquisición, desarrollo y mantenimiento de los sistemas de información que se podría ampliar en un trabajo futuro, pero que va ligado directamente con el desarrollo de software.

Tabla 3: Extracto ISO/IEC 27 000

Norma	Descripción
ISO/IEC 27000	Visión general de las normas de toda la ISO 27000, terminología general, introducción a los Sistemas de Gestión de Sistemas de Información (SGSI), etc.
ISO/IEC 27001	Norma principal, contiene los requisitos del SGSI. Norma utilizada por los auditores externos para certificar los SGSI en las organizaciones.
ISO/IEC 27002	Guía de buenas prácticas en la que se describen los objetivos de control y controles recomendables relativos a la seguridad de la información. No es certificable.
ISO/IEC 27003	Se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. No es certificable.

ISO/IEC 27005	Proporciona las directrices para la gestión del riesgo en la seguridad de la información. No es certificable.
ISO/IEC 27006	Especifica los requerimientos para la acreditación de entidades de auditoría y certificación de SGSI.
ISO/IEC 27007 ISO/IEC TR 27008	Guías de auditoría.
ISO/IEC 27011	Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

En cuanto a COBIT, el presente trabajo trata de enfocar su investigación en la seguridad de las aplicaciones web, lo que justifica la incorporación de este a los procesos de desarrollo seguro, dentro de sus dominios de este tenemos:

- Planificar y Organizar (procesos PO6, PO8, PO9).
- Adquirir e Implementar (procesos AI2, AI7)
- Entrega y Soporte (Procesos DS2, DS5, DS10)

Estos dominios con los procesos indicados se involucran directamente con el desarrollo de aplicaciones, la descripción completa de los dominios y procesos se encuentran en la documentación oficial de COBIT [25].

Posteriormente, en el presente trabajo se abarca también un vistazo rápido a una certificación importante dentro de las pruebas de penetración de EC-Council y es la Certified Ethical Hacker que tiene una gran demanda a nivel mundial.

En la tabla 4, se presentan las fases con una breve descripción general en lo referente a pruebas de penetración, en el ciclo de vida de desarrollo de software como ya se ha discutido en esta investigación se aplica muy tarde las pruebas mencionadas, pero que se deja planteado la posibilidad de adoptarlo durante todo el ciclo de vida.

Tabla 4: Fases de pruebas de *Pentesting*

Fase	Descripción
Reconocimiento (Reconnaissance)	Fase inicial y preparatoria, en esta se recopila información por medio de varias herramientas y técnicas sobre el objetivo a evaluar.
Escaneo (Scanning)	Se trabaja con la información obtenida en la fase anterior, se realizan escaneo de red, listados de IP, en esta etapa se utiliza muchas veces herramientas automatizadas.
Obtener acceso (Gaining Access)	Una vez escaneado y testeado, en esta fase se trata de explotar los servicios o vulnerabilidades encontradas en la fase anterior, con el fin de ganar acceso.
Mantener acceso (Maintaining Access)	También conocido como elevación de privilegios.
Borrar huellas (Clearing Tracks)	Este es un proceso que en los procedimientos de pruebas de penetración no es muy abordado, por temas de que es un proceso autorizado y no habría porqué borrar evidencias del acceso, aquí mejor se trabaja en la elaboración de informes.

4. Conclusiones

Este documento proporciona un conocimiento enfocado en conceptos para tener en cuenta en materia de seguridad informática, pasando a metodologías que se pueden aplicar en la evaluación y búsqueda de vulnerabilidades en sistemas y servicios web, cubriendo también una certificación que mucho más de ser una metodología, menciona las fases resumidas e importantes en procedimientos de Pentesting, no dejando de lado normas y un marco de referencia que debería ser abordado en temas de desarrollo seguro.

Las metodologías analizadas en la investigación buscan dar una vista general de las fases a seguir en la evaluación de seguridad en sistemas de información, aplicable por supuesto a las aplicaciones web, si bien no existe un camino definido en las pruebas de hacking ético, las fases principales se podrían concluir como: recolección de información, descubrimiento o evaluación de vulnerabilidades, obtención de acceso o explotación, pasando luego si se trata de pruebas autorizadas a elaboración y entregas de informes,

dejando de lado a mantener acceso y borrado de huellas.

El ciclo de vida de desarrollo de software tiene sus etapas generales que son: planificación y requisitos, arquitectura y diseño, prueba de planificación, codificación, pruebas y resultados terminado en el lanzamiento y mantenimiento, es importante mencionar que durante el ciclo se debe implementar el marco de gestión en los dominios mencionados en el estudio e implementar un análisis de vulnerabilidades en cada una de sus etapas.

Las pruebas de penetración permiten descubrir las vulnerabilidades presentes en un sistema; y, entender los riesgos que representaría la explotación de alguna de ellas. En este contexto, sería necesario la aplicación de la presente investigación en un ambiente más práctico, señalando la intervención de cada uno de los temas tratados en cada una de las fases del ciclo de vida de desarrollo de una aplicación.

Fuente de financiamiento

Los autores declaran que no existen fuentes de financiamiento para la elaboración de este artículo

Conflictos de intereses

Los autores declaran que no existen conflictos de intereses.

5. Referencias

1. BOHADA, John; DELGADO, Iván y BARINAS, Alexander. Criterios y métricas para evaluar la seguridad en aplicaciones Web:Metodología MESW. En: *Investigación e Innovación en Ingeniería de Software*. Tunja-Colombia 2019, págs. 43-53. isbn 978-958-52397-5-3. Disponible en: https://www.researchgate.net/publication/343166986_Criterios_y_metricas_para_evaluar_la_seguridad_en_aplicaciones_Web.
2. VELOZ SEGURA, Elizabeth Alexandra (2022). Componentes de calidad software y su utilización en aplicaciones web. *Ciencia Latina Revista Científica Multidisciplinar* [En línea]. 6(3), 3193-3204. Disponible en: https://doi.org/10.37811/cl_rcm.v6i3.2456.
3. KOZINA, Mario; GOLUB, Marin y GROS, Stjepan (2009). A method for identifying Web applications. *International Journal of Information Security* [En línea]. 8(6), 455-467. Disponible en: https://doi.org/10.1007/s10207-009-0092-3.
4. NIÑO BENITEZ, Yisel y SILEGA MARTÍNEZ, Nemury (2018). Requisitos de Seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas* [En línea]. 12(1), 205-221. ISSN 2227-1899 Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992018000500015&lng=es&nrm=iso.
5. ESCRIVÁ GASCÓ, Gema; ROMERO SERRANO, Rosa; RAMADA, David y ONRUBIA, Ramón. *Seguridad Informátic*. España: MACMILLAN, 2013. isbn 978-84-15656-64-7. Disponible en: https://www.machadolibros.com/libro/seguridad-informatica_528475.
6. SOLARTE-SOLARTE, Francisco; ENRIQUEZ-ROSERO, Edgar y BENAVIDES-RUANO, Mirían del Carmen (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL* [En línea]. 28(5), 497-498.Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321.
7. RODRÍGUEZ LLERENA, Alain (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica* [En línea]. 12(1), 116-131. ISSN 1684-1859 [consulta: 01-Jun-2020] Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100116&lng=es.
8. VILLÉN HIGUERAS, Sergio y RUIZ DEL OLMO, Francisco (2022). La cultura hacker en las estrategias transmediade las series de televisión:el caso de Mr. Robot (2015-2019). *Zer: Revista de estudios de comunicación* [En línea]. 27(52), 35-56. ISSN 1137-1102 Disponible en: https://doi.org/10.1387/zer.22991.
9. BURGOS RIVERA, Daniel (2004). La importancia del hacking ético en el sector

financiero [En línea]. 122(4401), 77380. Disponible en: http://polux.unipiloto.edu.co:8080/00003049.pdf.

10. GONZÁLEZ BRITO, Henry y MONTESINO PERURENA, Raydel (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. *Revista Cubana de Ciencias Informáticas* [En línea]. 12(4), 52-65. ISSN 2227-1899 Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992018000400005&lang=es.

11. VELOZ, Jorge; ALCIVAR, Andrea y SILVA, Carlos (2017). Ethical hacking, una metodolog´ıa para descubrir fallas de seguridad en sistemas inform´aticos mediante la herramienta KALI-LINUX. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones* [En línea]. 1(1), 1-12. Disponible en: https://doi.org/10.33936/isrtic.v1i1.194.

12. MENDEZ, Florentino; AQUINO, Adrian; RONQUILLO, Armando y VALDEZ, José (2014). Técnicas de Hacking Ético en un Laboratorio de Pentesting Virtualizado. *Springer-Verlag* [En línea]. 1-9. Disponible en: https://www.researchgate.net/publication/308312418_Tecnicas_de_Hacking_Etico_en_un_Laboratorio_de_Pentesting_Virtualizado.

13. HERNÁNDEZ YEJA, Adrian y PORVEN RUBIER, Joelsy (2016). Procedimiento para la seguridad del proceso de despliegue de aplicaciones web. *Revista Cubana de Ciencias Informáticas* [En línea]. 10(2), 1-12. ISSN 2227-1899 Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992016000200004.

14. AMARU, Tupac; LOPEZ, Henry y PAREDES, Oscar (2015). Mitigación de Ataques DDoS en Base de Datos Mediante un Balanceador de Carga. *Revista" GEEKS"-DECC-Report* [En línea]. 6(1), 7-13. ISSN 1390-5236 Disponible en: https://www.semanticscholar.org/paper/Mitigaci%C3%B3n-de-Ataques-DDoS-en-Base-de-Datos-un-de-Cartuche-L%C3%B3pez/a5445d31556ba781bc00ceaa834003692d65dfb6.

15. ISO - Organización Internacional de Normalización. *Serie "27000"*. ISO 2018. Disponible en: https://www.iso27000.es/iso27000.html.

16. BLÁZQUEZ-OCHANDO, Manuel. *Sistemas de recuperación e internet: metadescripción, procesamiento, webcrawling, técnicas de consulta avanzada, hacking documental y posicionamiento web*. Madrid: mblazquez.es, 2013. isbn 978-84-695-7019-7. Disponible en: http://mblazquez.es/wp-content/uploads/ebook-mbo-sistemas-recuperacion-internet1.pdf.

17. FORD, Richard y RAY, Helayne (2004). Googling for gold: Web crawlers, hacking and defense explained. *Network Security* [En línea]. 2004(1), 10-13. ISSN 1353-4858 Disponible en: https://doi.org/10.1016/S1353-4858(04)00023-6.

18. MALIZA MARTINEZ, Carlos; LÓPEZ MENDIZÁBAL, Verónica y MACKLIFF PEÑAFIEL, Verónica (2016). Framework for software architecture for Web and Mobile applications. *Revistas Científicas de la Universidad Técnica de Babahoyo* [En línea]. 1(1), 72-75. Disponible en: https://doi.org/10.26910/issn.2528-8083vol1issCITT2016.2016pp72-75.

19. CASTRO VASQUEZ, Carlos Arturo (2019). Pruebas de penetración e intrusión. *Universidad Piloto de Colombia* [En línea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6273.

20. NAVARRO, Michel (2017). Guía del PMBOK para la gestión de pruebas de intrusión a aplicaciones web. PMBOK guide for web application penetration testing management [En línea]. 1(1), 26-34. Disponible en: https://www.

researchgate . net / publication / 342545006_Guia_del_PMBOK_para_la_gestion_de_pruebas_de_intrusion_a_aplicaciones_web_PMBOK_guide_for_web_application_penetration_testing_management.

21. MONAR, Joffre; PÁSTOR, Danilo; ARCOS, Gloria y OÑATE, Alejandra (2018). Técnicas de programación segura para mitigar vulnerabilidades en aplicaciones web. *Congreso de Ciencia y Tecnología ESPE* [En línea]. 13(1). Disponible en: https : //doi.org/10.24133/cctespe.v13i1.753.

22. VALENCIA-DUQUE, Francisco y OROZCO-ALZATE, Mauricio (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação* [En línea]. n°22, 73-88. ISSN: 1646-9895. Disponible en: https : //doi.org/10.17013/risti.22.73-88.

23. PEÑA-CASANOVA, Mónica y ANIAS-CALDERÓN, Caridad (2020). Integración de marcos de referencia para gestión de Tecnologías de la Información Integration of frames of reference for information technology. *Ingeniería Industrial,* [En línea]. 41(1). 1-12. ISSN: 1815-5936 Disponible en: https://www.redalyc.org/articulo.oa?id=360464918003.

24. TOVAR, Edmundo; CARILLO, Jóse; VEGA, Vianca y GASCA, Gloria (2006). Desarrollo de productos de software seguros en sintonía con los modelos SSE-CMM, COBIT E ITIL. *Revista de Procesos y Metricas - AEMES* [En línea]. 3(1). 62-69. Disponible en: https : / / www . researchgate . net / publication/309566968_Desarrollo_de_productos_de_software_seguros_en_sintonia_con_los_modelos_SSE-CMM_COBIT_E_ITIL.

25. PÉREZ VILLAMAR, MIGUEL (2017). Aplicación de la metodología ITIL para impulsar la gestión de TI en empresas del Norte de Santander (Colombia): revisión del estado del arte. *Revista Espacios* [En línea]. 39(9). 17. ISSN 0798 1015 Disponible en: https://www.revistaespacios.com/a18v39n09/a18v39n09p17.pdf.