ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

UNIDAD DE TITULACIÓN

ANÁLISIS DE VULNERABILIDADES DE UNA INFRAESTRUCTURA DE RED UTILIZANDO METODOLOGÍAS DE ETHICAL HACKING

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

RICHARD ANDRÉS MIRANDA SALVADOR
richard.miranda@epn.edu.ec

Director: MSc. PABLO FERNANDO DEL HIERRO CADENA
pablo.delhierro@epn.edu.ec

Codirector: PhD. DENYS ALBERTO FLORES ARMAS
denys.flores@epn.edu.ec

Quito, Julio 2022

APROBACIÓN DEL DIRECTOR Y CODIRECTOR

Como director y codirector respectivamente del trabajo de titulación “ANÁLISIS DE VULNERABILIDADES DE UNA INFRAESTRUCTURA DE RED UTILIZANDO METODOLOGÍAS DE ETHICAL HACKING” desarrollado por el Sr. Richard Andrés Miranda Salvador, estudiante de la Facultad de Ingeniería de Sistemas, habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, damos por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

MSc. Pablo Fernando del Hierro Cadena

DIRECTOR

PhD. Denys Alberto Flores Armas

CODIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Richard Andrés Miranda Salvador, con cédula de identidad Nº 1750297978 declaro bajo juramento que el trabajo aquí descrito es de autoría propia; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

Richard Andrés Miranda Salvador

CI: 1750297978

DEDICATORIA

Dedico esta tesis a todas aquellas personas que han dejado una huella en mi vida y lo siguien haciendo, me han guiado, apoyado y alentado en ser una mejor persona, ser un mejor profesional en el área en la cual me estoy especializando, dejando su confianza, enseñanzas y legados tanto en lo personal como en lo académico.

Su apoyo y aprecio me han permitido lograr cosas que no hubiera podido solo.

“Soy mejor de lo que fui ayer, pero no mejor de lo que seré mañana, queda prohibido rendirse”

AGRADECIMIENTOS

Quiero comenzar expresando mi gratitud al MSc. Pablo del Hierro, quien decidió recibirme como tesista, por su paciencia y sus comentarios a lo largo de esta tesis, también al Dr. Denys Flores, quien proporcionó sus recomendaciones para que este sea un trabajo sea mejor aún. Además, quiero agradecer al personal de TICs de la FIS, en especial al MSc. Jorge Miño, quien me proporcionó su colaboración que influyó en gran medida para el desarrollo de esta tesis y se volvió un amigo.

Agradezco a mi familia por su cariño y apoyo en los diferentes momentos de mi vida, por su paciencia y comprensión durante la carrera y el desarrollo de este proyecto y estar conmigo de diferentes maneras.

Agradezco a mi novia por todo su apoyo en la vida y en el desarrollo de esta tesis, por apoyarme y estar ahí para mí, por alentarme las veces en las que estuve a punto de derrumbarme y por impulsarme siempre a ser mejor. Te amo mi pequeña.

Me gustaría agradecer profundamente a mis amigos, soy afortunado de tener buenas personas a mi alrededor que estuvieron ahí dentro y fuera de las aulas haciendo de mi viaje estudiantil una gran experiencia.

Agradezco al equipo de ciberseguridad que me abrió las puertas profesionalmente y estuvo al pendiente de este logro académico y está siempre presto con su apoyo, destacando a Nelson Pillajo, quien me brindó la guía necesaria y sus conocimientos para que esta tesis tenga aún mayor realce, a Alejandro Guzmán, quien me ha apoyado y alentado para poder terminar esta tesis de la mejor manera.

Por último, me gustaría dar las gracias sinceramente a todos los que no he mencionado en los últimos cinco párrafos. No me olvidé de nadie y siempre reconozco a todos en mi corazón. Si incluyera a todo el mundo en este agradecimiento, me temo que se convertiría en el agradecimiento de tesis más largo del mundo.

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

CID	:	Confidencialidad, Integridad, Disponibilidad, triada de la seguridad de la información, describe los pilares que la rigen.
CSIRT	:	Computer Security Incident Response Team, grupo de expertos en seguridad informática que se encarga de prevenir, detectar, responder y recuperarse de incidentes de seguridad en sistemas informáticos y redes.
DDoS	:	Distributed Denial of Services, es un ataque a la disponibilidad de un sistema, en el cual, por lo general, múltiples sistemas informáticos o redes de computadores comprometidos o bots son utilizados para inundar un objetivo específico, como un sitio web o un servidor con una gran cantidad de tráfico, datos o solicitudes de conexión.
DGIP	:	Dirección de Gestión de la Información y Procesos, es una dirección perteneciente a la EPN que se encarga de la administración de sus recursos informáticos y tecnológicos.
DNS	:	Domain Name System, es un sistema fundamental en Internet que se utiliza para traducir los nombres de dominio legibles por humanos en direcciones IP numéricas que los computadores utilizan para identificarse y comunicarse en la red.
E-C Council	:	E-Commerce Council, es una organización internacional de seguridad cibernética con sede en Estados Unidos que se dedica a proporcionar capacitación, certificaciones y servicios relacionados con la ciberseguridad y la ética en la seguridad informática.
EPN	:	Escuela Politécnica Nacional, es una institución de educación superior ubicada en Quito, Ecuador. Esta es una de las principales universidades técnicas y científicas del país.
FIS	:	Facultad de Ingeniería de Sistemas perteneciente a la Escuela Politécnica Nacional, sujeto de análisis de vulnerabilidades.
IP	:	Internet Protocol, es un conjunto de reglas y normas que rigen la forma en que los datos se transmiten a través de una red de computadoras, como Internet.
ISSAF	:	Information Systems Security Assessment Framework, metodología de *ethical hacking*.
NIST	:	National Institute of Standards and Technology, agencia del gobierno de E.E.U.U. cuya misión principal es promover la innovación y la competitividad económica de los Estados Unidos a través de la promulgación y promoción de estándares y medidas de calidad, seguridad y eficiencia en diversas áreas, incluyendo la tecnología, la metrología, la ciberseguridad y la ciencia.
OSSTMM	:	Open-Source Security Testing Methodology Manual, metodología de *ethical hacking*.
PTES	:	Penetration Testing Execution Standard, metodología de *ethical hacking*.
TIC	:	Tecnología de Información y Comunicación, un conjunto de tecnologías y herramientas que se utilizan para gestionar y comunicar información a través de medios digitales.

RESUMEN

El objetivo del presente trabajo de titulación es analizar las vulnerabilidades de la infraestructura de red de la FIS mediante el uso de metodologías de ethical hacking, tomando como base la metodología ISSAF. Este análisis permitirá sentar un precedente y concientizar al personal a cargo sobre el estado actual de la seguridad en dicha infraestructura, siendo el primer paso en la planificación de las estrategias y acciones futuras que llevarán a la FIS a un punto esperado.

La metodología tiene una estructura que cubre las diferentes aristas de la infraestructura, iniciando con la recolección de información de la FIS EPN, entendiendo su caracterización, misión, visión y estructura orgánica. Posteriormente se analiza la conectividad virtual y física mediante las diferentes herramientas para dicha tarea, lo cual permite obtener un mapa o topología de la red. A partir de la topología obtenida se diseña un conjunto de procesos a modo de pruebas para identificar las vulnerabilidades presentes en la infraestructura de la FIS con la estructura definida por ISSAF. Al final de cada prueba, se obtendrán las vulnerabilidades halladas en cada ítem de la infraestructura.

Palabras clave: Vulnerabilidades, ISSAF, seguridad, infraestructura, metodología, *ethical hacking*.

ABSTRACT

The objective of this thesis is to analyze the vulnerabilities of the FIS network infrastructure using ethical hacking methods based on the ISSAF methodology. This analysis will set a precedent and raise awareness among the personnel responsible for the current state of security in this infrastructure, this being the first step in planning future strategies and actions that will bring the FIS to an expected point.

The methodology has a structure that covers the different aspects of the infrastructure, starting with the collection of information about the FIS EPN, understanding its characterization, mission, vision and organizational structure. Next, the virtual and physical connectivity is analyzed using the different tools for this task, which allows obtaining a map or topology of the network. Based on the topology obtained, a series of processes are designed as tests to identify the vulnerabilities present in the FIS infrastructure with the structure defined by ISSAF. At the end of each test, the vulnerabilities found in each element of the infrastructure are obtained.

Keywords: Vulnerabilities, ISSAF, security, infrastructure, methodology, ethical hacking.

CAPÍTULO I INTRODUCCIÓN

1.1. Introducción

En la actualidad la información digital es uno de los activos más valiosos para una organización, ya que facilita la toma de decisiones y el correcto flujo de procesos. Los sistemas de información digitales ofrecen un ambiente en el cual los datos pueden ser analizados, procesados y/o transportados a la par con la generación de nuevos datos.

La dependencia de una organización a los datos y la infraestructura detrás de ellos hace importante que se tenga consciencia sobre las vulnerabilidades de las que puede ser víctima. A través de una entrevista realizada al Ing. Jorge Miño, a cargo de la infraestructura de la Facultad de Ingeniería de Sistemas de la Escuela Politécnica Nacional, desde este punto mencionada como FIS por sus siglas, se aclaró que el ambiente de datos que es manejado por la FIS mediante su infraestructura de red contempla hardware de red, como también plataformas administradas internamente [1]. Por lo tanto, es importante conocer el estado actual de la infraestructura con respecto a su seguridad lógica.

La FIS se encuentra en un proyecto de ampliación de su infraestructura, por lo cual han existido cambios tanto a nivel físico como lógico de los diferentes dispositivos que la conforman, lo cual hace necesario un precedente que permita garantizar los servicios que proporciona. Esta es la razón principal por la cual se aplicará el análisis de vulnerabilidades sobre la infraestructura de red de la FIS.

1.2. Planteamiento del problema

La seguridad de la red se refiere a toda actividad diseñada para preservar la confidencialidad, integridad, disponibilidad de la red y los datos que se transportan a través de esta, esta incluye tecnologías de hardware y software y está orientada a la gestión de diversas amenazas y vulnerabilidades, evitando su ingreso y propagación por la red [2].

Una arquitectura de red es compleja debido principalmente a la escalabilidad en número de dispositivos terminales y de red, como también en protocolos y servicios que por ella se utilizan y se enfrenta a un entorno de defectos o debilidades llamadas vulnerabilidades que al ser explotadas pueden comprometer algún aspecto de la red relacionada con la triada de la seguridad de la información [3].

Las amenazas a la seguridad de la red se dividen en dos categorías: amenazas pasivas, que suponen el intento de un atacante de obtener información relacionada a una comunicación, y las amenazas activas, que suponen alguna modificación de los datos transmitidos o la creación de transmisiones falsas [4].

De acuerdo con la publicación de Global Cybersecurity Index 2020 correspondiente al ranking de ciberseguridad, listando a los estados desde aquel con mayor puntuación hasta el de menor puntuación, Ecuador ocupa el lugar 119 de 194 estados a nivel mundial, mientras que, a nivel regional, Ecuador ocupa el lugar 19 de 35 estados [5].

Por lo cual, muchas organizaciones hacen un gran esfuerzo para evitar que las amenazas a las cuales están expuestas se conviertan en un ataque. Para prevenir la ciberdelincuencia, es imprescindible contar con una estrategia de seguridad informática eficaz.

Sin embargo, para determinar el mejor plan para su organización se debe empezar por una tarea, la cual es la aplicación de auditorías y evaluaciones de seguridad periódicas antes de poner en marcha un plan de prevención de riesgos [6].

La aplicación de un análisis de vulnerabilidades sobre una infraestructura de red permitirá, por una parte, obtener resultados sobre el estado actual referente a la seguridad de la red, por otra parte, sentar precedentes, los cuales permitirán comparar el estado de la seguridad de la red frente a las auditorías futuras y tomar los correctivos internos necesarios.

1.3.Justificación

Dentro del campo de la informática, una red puede ser descrita como un sistema de dispositivos interconectados que pueden comunicarse entre sí usando estándares comunes llamados protocolos. Estos dispositivos se comunican para intercambiar recursos y/o servicios [7].

Una red necesita garantizar la confidencialidad, integridad y disponibilidad de los datos que por ella transitan. Por esta razón, es necesario conocer y aplicar las mejores prácticas de seguridad para hacer frente a las amenazas sobre la misma.

Una infraestructura de red es el conjunto de recursos de hardware y software de toda una red que permite la conectividad, la comunicación, las operaciones y la gestión de una red. Proporciona una vía de comunicación y los servicios disponibles entre los usuarios, los procesos, las aplicaciones y las redes externas/Internet [8].

Dentro de una infraestructura, el ethical hacking (o prueba de penetración) es una práctica de gran importancia, ya que permite la explotación de un sistema de TI con el permiso de su propietario para determinar sus vulnerabilidades y puntos débiles. Es una forma eficaz de probar y validar la posición de ciberseguridad de una organización [9]. Las principales técnicas de *ethical hacking* son *phishing, sniffing, social engineering, SQL injection, cryptography.*

Dentro de las metodologías para el análisis de vulnerabilidades en una organización se destacan ISSAF, OSSTMM, NIST 800-115, PTES, que permiten planificar y realizar pruebas de seguridad mediante técnicas de ethical hacking.

El uso de las metodologías mencionadas proporciona un esquema para determinar las áreas vulnerables dentro de una infraestructura de red, lo que permite tomar medidas correctivas y así, evitar ser víctima de futuros ataques informáticos [10].

1.4. Objetivos

1.4.1. Objetivo General

Este trabajo tiene como objetivo:

- Analizar las vulnerabilidades de una infraestructura de red utilizando metodologías de ethical hacking, en este caso de la FIS.

1.4.2. Objetivos específicos

Este trabajo tiene como objetivos específicos:

- Recolectar información acerca de la FIS de la EPN.
- Analizar la conectividad virtual y física de la red para obtener un mapa de red.
- Diseñar un conjunto de procesos para identificar las vulnerabilidades presentes en la infraestructura de red.
- Obtener los resultados del análisis de vulnerabilidades.

1.5. Alcance

El presente trabajo tiene como objetivo analizar las vulnerabilidades de la infraestructura de red de la Facultad de Ingeniería en Sistemas de la Escuela Politécnica Nacional utilizando las metodologías de *ethical hacking* más relevantes, en donde destacará ISSAF.

Para cumplir con este objetivo se utilizará los pasos establecidos dentro de cada metodología que más se ajusten al análisis, tomando como base la estructura de ISSAF.

El alcance del análisis abarcará como elementos sujetos de análisis a todos aquellos que formen de la infraestructura de red de la FIS; es decir, aquellos que se encuentren en las instalaciones físicas y sean administrados por la misma, analizando a un componente de la misma naturaleza en representación de los demás para los casos en los que aplique.

Este análisis no cubre las fases de generación de recomendaciones, ni implementación de estas; sin embargo, sí se mencionará los hallazgos de cada prueba.

Con el fin de la adhesión a las normativas relacionadas con el manejo de la información vigentes en la EPN debido a la criticidad y la confidencialidad de la información, las acciones para la aplicación de las pruebas y la información recolectada se encuentran limitadas. El tipo de pruebas que se aplicarán serán de caja blanca, en donde se dispone o facilitará información puntual, además, la naturaleza de las pruebas será no intrusiva, es decir, aquellas que no alteren los datos dentro de cualquier activo de la infraestructura, por lo cual se adoptará un enfoque de obtención de resultados mediante la generación y aplicación de encuestas que pretenden cubrir aspectos críticos de cada componente de la infraestructura de la FIS, mismas que se basarán en los puntos críticos tratados en la metodología, las observaciones obtenidas por parte del director y codirector del presente trabajo de titulación, los controles de fortalecimiento o *hardening* del *Center for Internet Security* [11] y las recomendaciones del fabricante en los casos que aplique.

CAPÍTULO II MARCO TEÓRICO

2.1 CONCEPTOS

A continuación, se describen los conceptos teóricos de seguridad informática que abarcan el desarrollo del análisis de vulnerabilidades.

Seguridad Informática

Para comprender este concepto, hay dos términos previos que se necesitan describir. Uno es “seguridad”, el otro es “informática”.

Primero, examinando la definición de seguridad. Existen varios significados para este término, sin embargo, se encontró que la definición que ofrece el glosario de la NIST es la más relevante para el contexto que se pretende definir, siendo así, “Condición que resulta del establecimiento y mantenimiento de medidas de protección que permiten a una organización llevar a cabo su misión o funciones críticas a pesar de los riesgos planteados por las amenazas al uso de sus sistemas” [12].

Segundo, examinando la definición de informática. Según la Real Academia de la Lengua Española es un “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadores” [13].

Por lo que, teniendo en cuenta los términos anteriores, es posible definir la seguridad informática como el conjunto de medidas y normas de protección aplicados a los sistemas de información basados en computadores con el objetivo de preservar las propiedades de los recursos de dichos sistemas. Las propiedades principales de un sistema de información se denominan la triada CID de la seguridad informática, nombrada de esa manera por sus siglas y se muestran a continuación [14].

Triada CID

Existe un modelo que se conoce como triada CID por sus siglas Confidencialidad, Integridad y Disponibilidad y hace referencia a estos tres pilares que en su conjunto brindan una protección adecuada a la seguridad informática. A continuación, se detalla cada uno de los términos mencionados.

Figura 1: Triada CID
Fuente: **[15]**

Confidencialidad

Propiedad de la información de preservar las restricciones y permisos autorizados para el acceso y su divulgación indebida, incluidos los medios para proteger la privacidad personal y la información propietaria [16].

Una definición útil relacionada a la confidencialidad es la sensibilidad, la cual es una medida de la importancia asignada a la información por parte de su propietario, con lo cual se pretende denotar la necesidad de su protección. Esta información sensible es aquella que, en caso de su divulgación indebida o su modificación, genera un perjuicio al propietario de esta, sea una organización o un individuo [17].

Integridad

Propiedad de la información o datos, sean estos en almacenamiento, durante su procesamiento o en tránsito, por la que se registra, utiliza y mantiene de manera que permita medir y garantice su grado de exactitud, coherencia interna y utilidad para un fin determinado, evitando su modificación o destrucción de manera no autorizada, e incluye la garantía de no repudio y autenticidad de esta [18], resultando un factor primario en la confiabilidad de la información. Este concepto se aplica a información, datos, sistemas y procesos, organizaciones, personas y sus acciones [17].

Disponibilidad

Propiedad de la información de garantizar su acceso oportuno, fiable y capacidad de utilizarla por parte de usuarios autorizados [19]. Esto permite a los usuarios autorizados el

acceso a la información cuando y donde lo necesiten y en la forma y formato requeridos; lo cual no implica que los datos estén siempre disponibles durante el 100 % del tiempo.

Una definición útil relacionada a la disponibilidad es la criticidad [20], la cual es la medida del grado de dependencia que una organización tiene sobre la información para la realización de sus operaciones o el cumplimiento de sus objetivos [17].

Vulnerabilidad

Debilidad en un sistema de información [21], procedimiento de seguridad, control de seguridad o implementación que podría ser explotada [17] o activada por una fuente de amenaza y hacer que esta se vuelva una realidad [22].

Infraestructura de red

Parte de la infraestructura de TI de una organización que comprende hardware y software de red, sistemas y dispositivos dentro de la red y permite la comunicación de red entre usuarios, servicios y aplicaciones [23].

Prueba

Dentro del contexto de ethical hacking es necesario definir el significado de un elemento de evaluación dentro de un análisis, es decir, una prueba. La NIST la define como un tipo de método de evaluación que se caracteriza por el proceso de ejercitar uno o más objetos de evaluación o activos bajo condiciones específicas con el fin de comparar el comportamiento real con el esperado [24]. El resultado de cada una de las pruebas que se apliquen dentro del análisis permitirá determinar el estado actual de la seguridad informática de la infraestructura de red de la FIS, lo que a su vez permitirá a la misma tomar las acciones necesarias para llegar a un estado deseado.

Para descubrir las vulnerabilidades que puede tener un sistema o una infraestructura existen tres tipos de pruebas que se pueden utilizar, las cuales son:

- **Prueba de caja negra:**
  También conocida como enfoque de prueba y error, es un tipo de prueba en la cual no se proporciona información acerca de la infraestructura a evaluar [25], simulando un escenario muy cercano en el que un atacante externo comprometería a una organización [26]. Por lo tanto, este tipo de prueba puede tomar mucho tiempo para completarla, además, resulta ser la opción más costosa [27].

- **Prueba de caja blanca:**
  También conocida como prueba de caja transparente, es un tipo de prueba en la cual la organización comparte toda la información acerca de la infraestructura a evaluar [25], incluyendo credenciales, simulando un ataque dirigido hacia un sistema o activo específico mediante todos los vectores de ataque posibles [26]. Por lo tanto, este tipo de prueba permite ahorrar tiempo y dinero para su realización [27].

- **Pruebas de caja gris:**
  También conocida como prueba de caja translúcida, es un tipo de prueba resultante de la combinación de la prueba de caja blanca y prueba de caja negra, en la cual la organización comparte información parcial acerca de la infraestructura a evaluar [25], siendo por lo general las credenciales de acceso. Este tipo de prueba permite comprender el nivel de acceso que podría obtener un atacante externo y el daño potencial que podría causar [26], simulan una amenaza interna y un ataque que ha traspasado el perímetro a la vez [27].

Ethical Hacking

Aunque este término no es fácil de definir, una definición concisa es la que provee la organización estadounidense *EC-Council*, la cual lo explica de la siguiente manera:

Es el proceso de detección y explotación de vulnerabilidades en una aplicación, sistema o infraestructura de una organización que un atacante puede utilizar para explotar a un individuo u organización mediante pruebas que pueden o no ser intrusivas, con el fin de recolectar información que ayude a una organización a tomar medidas ante posibles ataques [28]. Este proceso se debe llevar a cabo dentro del marco de la ley que rige sobre un territorio y con el conocimiento y acuerdo de una organización, definiendo todos los criterios necesarios como lo son el alcance, el tipo de pruebas, el tiempo que tomará el proceso, entre otros [28].

Fases del Ethical Hacking

El proceso de ethical hacking, consiste en un conjunto de fases que sigue un *ethical hacker* o un atacante con el fin de vulnerar una infraestructura o un sistema, las cuales aportarán al cumplimiento de los objetivos específicos y se muestran a continuación.

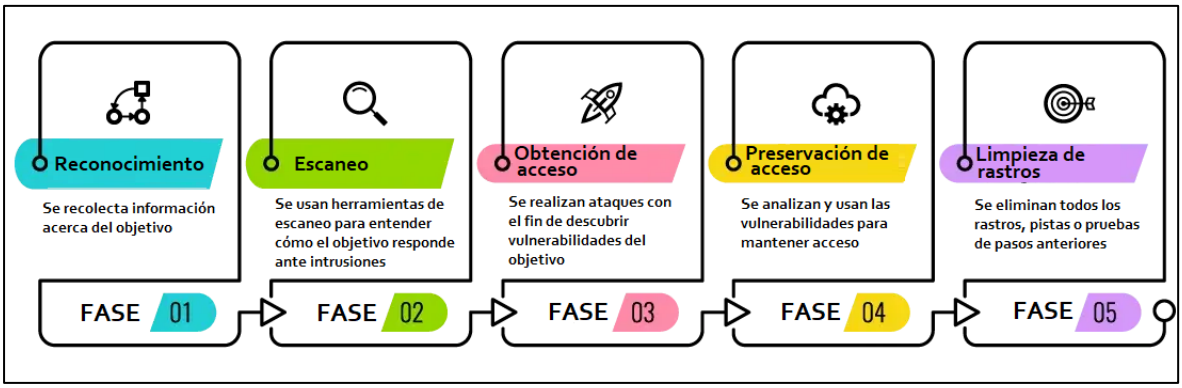


Figura 2: Fases de ethical hacking
Fuente: **[29]**

- **Fase 1: Reconocimiento**

En esta primera fase del *ethical hacking* también conocida como *footprinting* o recolección de información se recolecta la mayor cantidad de información posible acerca de un objetivo, esto incluye tanto a información de fuentes abiertas y mediante contacto con personas relevantes como a información sobre los sistemas o infraestructuras.

Esta fase sirve de aporte al desarrollo del presente proyecto de titulación, ya que se encuentra alineado con el primer objetivo específico que recolecta información acerca de la FIS y gracias a la información que se recopile acerca de la FIS será posible comprender su estructura de mejor manera y se obtendrá un análisis de vulnerabilidades eficaz.

- **Fase 2: Escaneo**

En esta fase del *ethical hacking* se trata de encontrar diferentes formas de obtener información acerca del objetivo relacionada con la red y registros, por ejemplo, cuentas de usuario, credenciales, direcciones IP, puertos, etc. Esta fase implica el uso de herramientas como *dialers*, escáneres de puertos, mapeadores de red [29]. Dentro del ethical hacking existe tres prácticas de escaneo, las mismas son:

  - **Escaneo de vulnerabilidades:** Esta práctica se centra en las vulnerabilidades del objetivo y en la manera de intentar explotarlas.
  - **Escaneo de puertos:** Esta práctica implica el uso de herramientas de recopilación de datos para escuchar los puertos TCP y UDP abiertos.
  - **Escaneo de red:** Esta práctica es utilizada para detectar dispositivos activos dentro de la red y para encontrar la manera de explotar la red.

Esta fase sirve de aporte al desarrollo del presente proyecto de titulación, ya que se encuentra alineado tanto con el objetivo general que analiza las vulnerabilidades de la infraestructura de la FIS como con el segundo objetivo específico que analiza la conectividad virtual y física de la red de la FIS. A partir de la información de red que se recopile en esta fase acerca de la FIS será posible comprender de mejor manera los aspectos técnicos de su infraestructura y será posible el planteamiento de las preguntas necesarias para tomar las mejores decisiones al momento de seleccionar el tipo de pruebas y las herramientas para ejecutarlas, lo que a su vez implica un aporte al tercer objetivo específico que implica diseñar un conjunto de procesos para identificar las vulnerabilidades gracias a los resultados que se obtengan de la aplicación de dichas pruebas.

- **Fase 3: Obtención de Acceso**

En esta fase se explotan las vulnerabilidades encontradas durante la fase de escaneo mediante varios métodos, el atacante intenta ingresar a los sistemas, aplicaciones o redes del objetivo sin hacer saltar alarmas. Al final de esta fase el atacante termina haciendo daño a la organización mediante el robo de su información sensible o termina pidiendo un rescate, etc [29].

Esta fase se encuentra fuera del alcance del proyecto de titulación, debido a que se trata de un análisis de vulnerabilidades y como resultado de su aplicación se limita a mostrar resultados acerca de las vulnerabilidades, es decir, no aprovecha dichos resultados para explotar las vulnerabilidades encontradas.

- **Fase 4: Preservación de Acceso**

En esta fase, una vez obtenido el acceso al sistema se hace todo lo posible por mantener dicho acceso mediante la continua explotación del sistema, ataques *DDoS*, robo de toda la base de datos hasta completar las actividades propuestas, en caso de ser un *ethical hacker*, sin la sospecha de la organización [29].

Esta fase se encuentra fuera del alcance del proyecto de titulación, debido a que se trata de un análisis de vulnerabilidades y como resultado de su aplicación se limita a mostrar resultados acerca de las vulnerabilidades y no se requiere preservar el acceso en un sistema ya que las pruebas son de naturaleza no intrusiva y las acciones para aplicarlas son puntuales.

- **Fase 5: Limpieza de rastros**

En esta última fase, el atacante o ethical hacker elimina todos los rastros, pistas o pruebas generadas en fases anteriores que puedan ser rastreadas con el fin de evitar ser atrapados. Esta fase incluye la edición, corrupción y/o eliminación de registros o valores dentro de los sistemas; tomando en cuenta también el borrado o desinstalación de carpetas, aplicaciones y software [29].

Esta fase es irrelevante para al proyecto de titulación, ya que, las pruebas se las realizará con el previo conocimiento y consentimiento total de la FIS y como parte de los acuerdos se encuentra la no divulgación de los resultados y la limpieza de toda la información relacionada al análisis por parte del autor.

2.2. Descripción de metodologías de Ethical Hacking

Con el fin obtener la mejor calidad en el análisis de vulnerabilidades propuesto, se decidió adoptar una de las mejores prácticas para la realización de pruebas de penetración, que recomienda combinar múltiples metodologías con el fin de adaptarlas a los objetivos que se desea lograr. Para realizar esta tarea, se procede a comparar las diferentes metodologías de *ethical hacking* tomando en cuenta diferentes métricas, así como también determinando las actividades de dichas metodologías que se encuentren más alineadas con los objetivos específicos propuestos.

Debido a la naturaleza del *ethical hacking*, existen varias metodologías que facilitan el proceso de detección y explotación de vulnerabilidades de un sistema o la infraestructura de una organización cuyos hallazgos sobre las vulnerabilidades pueden ser utilizados por dicha organización para crear un plan de acción y ejecutar acciones de remediación que permitan mejorar la seguridad de los sistemas o de la infraestructura ante posibles ataques o brechas existentes.

Entre las metodologías más ampliamente utilizadas para los fines mencionados anteriormente, destacan PTES, OSSTMM, NIST 800-115 e ISSAF, es por ello por lo que resulta imperativo describir cada una de ellas y compararlas con el fin de determinar cuál de ellas responde mejor al cumplimiento de los objetivos propuestos.

2.2.1. METODOLOGÍA PTES

El *Penetration Testing Execution Standard* (PTES) es un documento elaborado por especialistas en auditorias de seguridad. Este documento presenta una guía sobre la

manera de ejecutar una prueba de penetración práctica para todo tipo de ambiente y abarca desde las interacciones precontractuales, incluyendo el alcance hasta la manera en la que se debe tratar con terceros. Además, este estándar incluye técnicas y conceptos de pruebas de penetración [30]. PTES se organiza en 7 fases, las cuales aportan con el cumplimiento de los objetivos de la manera que se detalla a continuación:

Fase 1: Interacciones previas

Define las negociaciones y acuerdos de las partes, se determinará las fechas de la evaluación, etc.

Esta fase aporta al desarrollo del análisis de vulnerabilidades ya que permitirá dar a conocer las limitaciones y compromisos que se esperan por parte del tesista, como lo son la divulgación de información recolectada y resultante, como también el uso de pruebas no intrusivas en la infraestructura.

Fase 2: Recolección de Información

Se dedica a conseguir y reunir la información probable acerca del objetivo. En esta fase aparece el *footprinting* que es una técnica utilizada para recopilar información sobre los sistemas informáticos y las entidades a las que pertenecen como es el nombre de dominio, dirección IP, DNS, Sistema Operativo, etc.

Esta fase sirve de aporte al desarrollo del presente proyecto de titulación, ya que se encuentra alineado con el primer objetivo específico que recolecta información acerca de la FIS y al segundo objetivo específico que analiza la conectividad virtual y física de la red y gracias al resultado de esta recopilación será posible comprender su estructura de mejor manera y se obtendrá un análisis de vulnerabilidades eficaz.

Fase 3: Modelado de amenaza

Se examina el equipo técnico, las herramientas a utilizar, la red, hardware, software, el plan de contingencia, lo que permite determinar la viabilidad de los diferentes vectores de ataque.

Esta fase sirve de aporte al desarrollo del presente proyecto de titulación, ya que permite cubrir el segundo objetivo específico, debido a que, a partir de la información de red que se recopile de la FIS será posible comprender de mejor manera su infraestructura, además, permitirá seleccionar el enfoque y las herramientas a utilizar que mejor se ajusten para la

evaluación de cada componente de infraestructura cubierto, lo que a su vez implica un aporte al tercer objetivo específico.

Fase 4: Análisis de Vulnerabilidades

Con los datos obtenidos, se identifica los posibles procedimientos de ataque, aquí entra el *fingerprinting*, esto permite obtener información de una víctima por medio de los sistemas informáticos.

Esta fase sirve de aporte al desarrollo del presente proyecto de titulación, ya que representa el objetivo general del proyecto gracias a la aplicación de las pruebas mediante las herramientas seleccionadas sobre la infraestructura de red de la cual se obtuvo información relevante en fases previas.

Fase 5: Explotación

Por medio de las herramientas utilizadas se ataca a las vulnerabilidades detectadas para comprometer al sistema y conseguir acceso.

Esta fase se encuentra fuera del alcance del proyecto de titulación, debido a que el objetivo general se limita a mostrar resultados acerca de las vulnerabilidades encontradas.

Fase 6: Post-Explotación

Busca tener acceso al sistema de manera constante y así realizar los ataques a las vulnerabilidades detectadas, además, se trata de inyectar código malicioso en el objetivo; así como también se analiza el borrado de huellas.

Esta fase no aporta al proyecto de titulación, ya que, una vez obtenidos los resultados, la limpieza de toda la información relacionada al análisis por parte del autor será eliminada como parte de los acuerdos entre la FIS y el autor.

Fase 7: Informe

Analiza y explica los resultados obtenidos luego del análisis, con las pruebas recolectadas y las pruebas ejecutadas y así dar un juicio sobre el estado de la seguridad.

Esta fase aporta tanto al desarrollo del presente proyecto de titulación como a la FIS, ya que permitirá conocer el estado actual de su infraestructura de red en cuanto a vulnerabilidades relacionadas con la seguridad informática se refiere.

Entre los puntos fuertes de esta metodología destaca su adaptabilidad a la dificultad de un análisis de vulnerabilidades o un *pentesting*, dependiendo de los requerimientos de la organización a evaluar.

Otro punto que destacar es el nivel de detalle que ofrece para llevar a cabo los *tests* en una organización. Sin embargo, contiene una lista extensa de herramientas, métodos y técnicas a usar en cada sección dentro de un documento, sin embargo, la guía técnica no es lo suficientemente detallada para ser utilizada por auditores sin experiencia.

2.2.2. METODOLOGÍA OSSTMM

El *Open Source Security Testing Methodology Manual* (OSSTMM,) es uno de los estándares más completos y de los más utilizados para las organizaciones que desean desplegar un *testing* de calidad, ordenado y eficiente, ya que contiene información sobre análisis, métricas, flujos de trabajo, seguridad física e inalámbrica [30].

Los puntos que destacan son:

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

Para incrementar la calidad del desarrollo, la metodología indica que se debe probar tanto la manera en la que se puede ejecutar como el momento adecuado para ejecutar un análisis. Al dar seguimiento a esta metodología, se puede tener la seguridad de que se cumplen los objetivos determinados.

Esta metodología, además, de centrarse en los aspectos técnicos de seguridad, comprende a los responsables del testeo; integra el concepto de Valores de Evaluación de Riesgo, este permite distinguir y catalogar las diferentes problemáticas gracias a su guía de interpretación y correlación de resultados obtenidos mediante la valoración de los riesgos bajo tres factores, seguridad operacional, pérdida de control y limitaciones, obteniendo una puntuación final sobre el estado de la seguridad de la FIS.

El enfoque de OSSTMM es en seguridad operacional, por lo cual OSSTMM define las siguientes dimensiones de seguridad:

1. Visibilidad
2. Acceso
3. Confianza
4. Autenticación
5. Confidencialidad
6. Privacidad
7. Autorización
8. Integridad
9. Seguridad

Esta metodología resulta de aporte al desarrollo del presente proyecto, ya que permite cubrir la arista de operaciones relacionadas a la seguridad de la FIS, por ejemplo, sus controles de acceso, sus protecciones perimetrales, el nivel de conciencia de seguridad de la organización.

Cabe mencionar que, para la aplicación de esta metodología se necesita mucha información para recabar las métricas por lo que es necesario de experiencia y tiempo para conseguir información clara y concisa, por lo que un analista sin experiencia tendría dificultar en llevar a la práctica su aplicación.

2.2.3. METODOLOGÍA NIST 800-115

Dentro de las normas que ofrece la NIST se encuentra una que incluye pruebas de penetración en su publicación 800-115, siendo una guía técnica para pruebas y evaluación de la seguridad de la información. Este documento sirve de guía tratando los aspectos técnicos, donde se presenta los métodos y técnicas de prueba y examen técnico que una organización podría utilizar como parte de una evaluación y ofrece ideas sobre su ejecución e impacto potencial que pueden tener sobre los sistemas y las redes.

La guía se encuentra organizada en 8 secciones, las cuales son:

1. Presenta la introducción, presentando a la NIST, el propósito y alcance de la guía, como también su audiencia.
2. Presenta una visión general de las evaluaciones de seguridad de la información, incluyendo políticas, funciones, responsabilidades, metodologías y técnicas.
3. Proporciona una descripción detallada de varias técnicas del análisis técnico, incluyendo la revisión de la documentación, la revisión de los registros, el rastreo de la red y la comprobación de la integridad de los archivos.
4. Describe varias técnicas para identificar objetivos y analizarlos en busca de posibles vulnerabilidades.
5. Explica las técnicas comúnmente utilizadas para validar la existencia de vulnerabilidades.
6. Presenta un enfoque y un proceso para planificar una evaluación de seguridad.
7. Analiza los factores clave para la ejecución de las evaluaciones de seguridad, incluyendo la coordinación, el análisis y el tratamiento de los datos.
8. Presenta un enfoque para informar de los resultados de la evaluación y proporciona una visión general de actividades de corrección.

Su propuesta como metodología de evaluación de seguridad de la información propone los siguientes beneficios:

- Proporcionar coherencia y estructura a las pruebas de seguridad, lo que puede minimizar los riesgos de las pruebas.
- Acelerar la transición del nuevo personal de evaluación.
- Abordar las limitaciones de recursos asociadas a las evaluaciones de seguridad.

Además, propone pasos consecutivos mínimos para obtener ventajas sobre una evaluación de seguridad de la información que aportan al presente proyecto, los cuales son:

- **Planificación**

  Este paso es fundamental para el éxito de una evaluación, en este paso se recopila información sobre la organización, por ejemplo, los activos a evaluar, las amenazas de interés, los controles de seguridad a utilizar y el desarrollo del enfoque de evaluación.

Este paso aporta al desarrollo del análisis de vulnerabilidades ya que permitirá tomar decisiones con base en información acerca de la selección del tipo de pruebas y las herramientas para ejecutarlas que mejor se ajusten a la FIS, lo que implica un aporte al tercer objetivo específico.

- **Ejecución**

  Los objetivos en esta fase son la identificación y validación de vulnerabilidades. Además, en esta fase se debe abordar las actividades asociadas con el método y técnica de evaluación previstos.

  Este paso sirve de aporte al desarrollo del presente proyecto de titulación, ya que permite cumplir con el objetivo general del proyecto gracias a la aplicación de las pruebas previamente planificadas en el paso anterior.

- **Post-Ejecución**

  Esta fase es posterior a la de ejecución, ya que se centra en el análisis de vulnerabilidades identificadas para determinar causas raíz, establecimiento de recomendaciones de mitigación de estas y el desarrollo de un informe final.

  Este paso no aporta al proyecto de titulación, ya que el proyecto concluye con la presentación de resultados y no incluye procesos reactivos a los mismos.

2.2.4. METODOLOGÍA ISSAF

El *framework* metodológico *Information Systems Security Assessment Framework* (ISSAF) es desarrollado por la *Open Information Systems Security Group* (OISSG) y es uno de los marcos de pruebas de penetración más detallados en cada uno de sus dominios y pruebas dentro de cada uno de ellos, por lo que sirve de referencia dentro de la evaluación de seguridad de las organizaciones [31].

Su valor agregado frente a otros documentos guía es que sugiere herramientas para llevar a cabo cada prueba que se decida aplicar. Además, indica la razón de ser de las medidas de seguridad y su importancia, abarcando para la FIS desde la recolección de información hasta el análisis de vulnreabilidades mediante la aplicación de las respectivas pruebas.

ISSAF consiste en un enfoque de evaluación de tres fases y nueve pasos, lo cual se presenta a continuación:

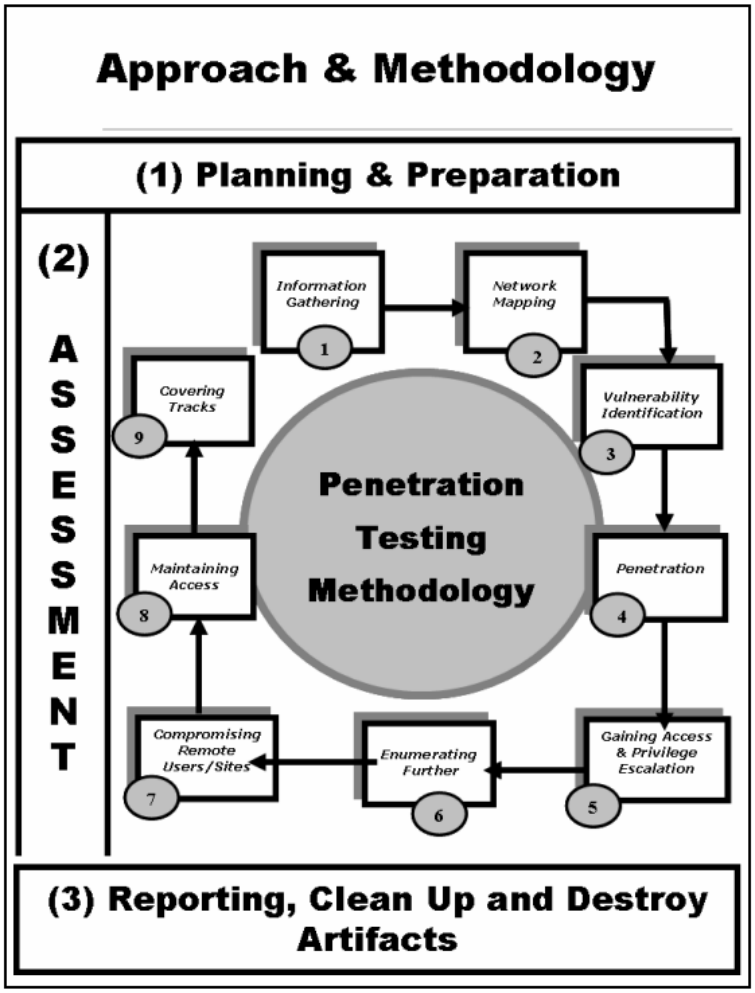


Figura 3: Metodología ISSAF
Fuente: **[31]**

Fase-I: Planificación y preparación

Esta fase incluye los pasos para obtención e intercambio de información con la organización. Esto implica la firma de un documento que contiene los acuerdos de evaluación entre ambas partes de manera formal y el nivel de colaboración, lo cual servirá de base para la realización de las pruebas y definición de las implicaciones legales. Dicho acuerdo definirá el alcance de las pruebas, las fechas, los horarios de aplicación de estas, entre otras características.

Las actividades que comprende esta fase son las siguientes:

- Identificación de los individuos implicados de ambos lados.

- Reunión de apertura para definir alcance, enfoque y metodología de evaluación.
- Acuerdo de los casos de prueba específicos y los caminos de escalado.

Esta fase aporta al desarrollo del análisis de vulnerabilidades, ya que se encuentra alineado con el primer objetivo específico que recolecta información acerca de la FIS y permitirá crear acuerdos entre la FIS y el autor, lo que será considerado al momento de planificar las pruebas y herramientas a ejecutar. Además, esta fase analizar la conectividad virtual y física de la red de la FIS, cubriendo así el segundo objetivo específico. Por último, esta fase permitirá planificar los procesos que servirán para identificar las vulnerabilidades de la infraestructura de red de la FIS, siendo este el tercer objetivo específico.

Fase-II: Evaluación

Esta fase implica la aplicación de las pruebas, siguiendo un enfoque estructurado de pasos acuerdo con un mayor nivel de acceso a los activos de información a medida que se los ejecuta. Estos pasos en su conjunto forman un ciclo iterativo, como se lista a continuación:

1. Recolectar la información
2. Mapear de la red
3. Identificar las vulnerabilidades
4. Penetrar en el o los sistemas
5. Obtener de acceso y escalar privilegios
6. Enumerar (más allá)
7. Comprometer Usuarios/Sitios Remotos
8. Mantener el acceso
9. Cubrir el rastro

Las pruebas que contiene esta metodología se encuentran categorizadas de la siguiente manera:

1 Seguridad en la red

1.1 Pruebas de seguridad de contraseñas

1.2 Evaluación de la seguridad de switch

1.3 Evaluación de la seguridad de router

1.4 Evaluación de la seguridad de firewall

1.5 Evaluación de la seguridad de sistema de detección de intrusos

1.6 Evaluación de la seguridad de Vpn

1.7 Estrategia de gestión y evaluación de seguridad de sistema antivirus

1.8 Seguridad de la red de área de almacenamiento (san)

1.9 Evaluación de la seguridad de WLAN

1.10 Seguridad de usuario de internet

1.11 Seguridad AS 400

1.12 Seguridad de notas de lotus/balanceadores de carga

2 Seguridad de hosts

2.1 Evaluación de la seguridad de sistemas *unix/linux*

2.2 Evaluación de la seguridad de sistemas *windows*

2.3 Evaluación de la seguridad de *netware novell*

2.4 Evaluación de la seguridad de servidor web

3 Seguridad de aplicaciones web

4 Seguridad física

Esta fase sirve de aporte al desarrollo del presente proyecto de titulación, ya que cubre el objetivo general del proyecto gracias a la aplicación de las pruebas de una manera estructurada y categorizada a partir de una planificación previa sobre la infraestructura de red de la FIS, identificando los componentes que forman parte de su infraestruca y administración y ejecutando acciones tomando en cuenta las limitaciones definidas en el acuerdo entre ambas partes. Además, debido a la criticidad, la confidencialidad de la información, de acuerdo con las normativas relacionadas con el manejo de la información vigentes en la EPN y el alcance definido del presente proyecto, no todas estas pruebas se pueden aplicar.

Fase-III: Reportes, limpieza y destrucción de artefactos

Esta fase implica la descripción tanto de los resultados obtenidos con posibles recomendaciones como de cualquier incidente identificado. Por lo que existen reportes verbales y escritos dependiendo del nivel de detalle y la criticidad de los hallazgos.

Además, en esta fase se procede a la destrucción o almacenamiento de la información generada durante la aplicación de las pruebas y se ejecutarán las acciones definidas por ambas partes como parte de su acuerdo.

La metodología mencionada resulta un aporte fundamental para el presente análisis de vulnerabilidades, destacando su adaptabilidad a los procesos dentro de la FIS, centrándose en el área técnica y de gestión. Otra ventaja de usar ISSAF es su enfoque estructurado, garantizando que no se omita ninguna fase crítica y se siga un proceso sistemático para identificar y abordar las vulnerabilidades de seguridad. Además, propone herramientas y procedimientos para llevar a cabo cada una de las pruebas.

2.3. EVALUACIÓN DE METODOLOGÍAS

Se muestra a continuación, una tabla comparativa con aspectos decisivos y discriminantes con los que se comparará a las metodologías descritas anteriormente.

Cada criterio que se muestra en la tabla se lo seleccionó tomando en cuenta tanto a los objetivos propuestos como el alcance del presente proyecto y tendrá una calificación entre [1-4], siendo 1 la calificación más baja y 4 la más alta, con el fin de seleccionar aquellas que se adapten de mejor manera al cumplimiento de los objetivos del análisis propuesto. Los criterios que permitieron comparar las diferentes metodologías, son detallados a continuación:

- **Alineación con los objetivos:**

  Este criterio permite medir el grado de alineación que tiene la metodología con los objetivos propuestos en el presente proyecto, es decir, dentro de las fases que contiene la metodología se identificó la cantidad de objetivos propuestos que esta permite cubrir.

- **Extensión de la guía:**

  Este criterio permite medir el contenido que tiene la metodología tomando en cuenta la cantidad de páginas que esta contiene.

- **Propuesta de herramientas a usar:**

  Este criterio permite medir el nivel de detalle del aporte que tiene la metodología al momento de aplicación de cada una de las pruebas, es decir, las recomendaciones de herramientas y su utilización.

- **Facilidad de implementación:**

  Este criterio permite medir la complejidad que tiene la utilización de la metodología, es decir, el contenido detallado acerca de las actividades a realizarse junto con recomendaciones y contenido subyacente.

- **Reportes:**

  A pesar de ser uno de los objetivos propuestos, fue necesario separar la fase de reportes al momento de comparar las metodologías, ya que, por definición, una metodología no necesariamente toma en cuenta la presentación de resultados y por lo tanto, puede cubrir en baja o nula medida esta fase.

  Este criterio permite medir el nivel de detalle que tiene la metodología en cuanto a presentación de resultados se refiere. Esta actividad, además de contener las acciones a realizar, puede recomendar plantillas para utilizar.

Como resultado preliminar de la comparación de las metodologías, se obtuvo que, aquellas que mejor calificación obtuvieron fueron ISSAF y PTES, con lo cual son las dos metodologías que aportarán en mayor grado al análisis de vulnerabilidades.

Tabla 1: Comparación de metodologías de ethical hacking

METODOLOGÍA /ASPECTO	ALINEACIÓN CON LOS OBJETIVOS	EXTENSIÓN DE LA GUÍA	PROPUESTA DE HERRAMIENTAS A USAR	FACILIDAD DE IMPLEMENTACIÓN	REPORTES	TOTAL
PTES	4	1	4	3	4	**16**
OSSTMMN	2	3	1	2	3	11
NIST 800-115	2	2	1	1	1	8
ISSAF	3	4	3	4	2	**16**

Fuente: Elaboración del autor

Una vez obtenidos los resultados preliminares, los cuales indican que las metodologías que destacan son ISSAF y PTES, es necesario analizar en mayor detalle su compatibilidad con los objetivos propuestos. Este análisis se muestra a continuación:

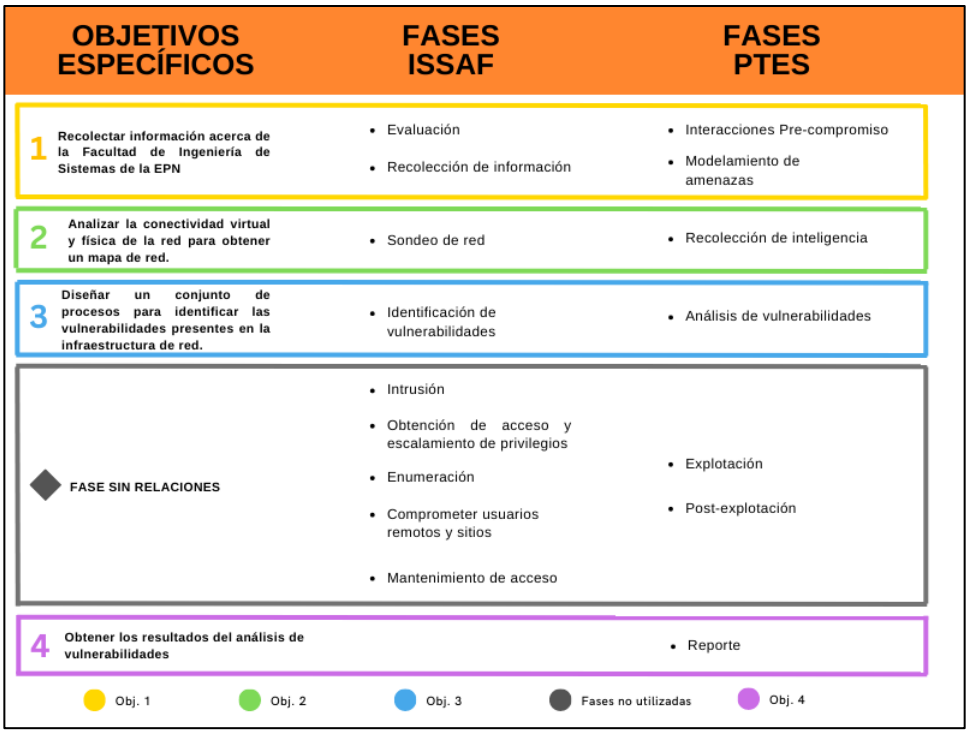


Figura 4: Relación entre los objetivos específicos y las fases de las metodologías seleccionadas
Fuente: Elaboración del autor

Es necesario mencionar que existen fases intermedias de cada metodología que no aportan al cumplimiento de los objetivos propuestos, sin embargo, no se las excluyó de la figura 4, esto con evitar la confusión acerca de la cantidad de fases que realmente tienen y la metodología PTES contiene una fase final que se relaciona directamente con el último objetivo específico.

Como conclusión de la comparación de las cuatro metodologías de *ethical hacking* donde se evaluó la idoneidad de cada una para el análisis propuesto, se constató que los marcos apoyaban de manera general al cumplimiento de los objetivos específicos.

Aunque se muestra en la tabla mostrada anteriormente las metodologías ISSAF y PTES como aquellas que más alineadas se encuentran, su aplicación o nivel de cobertura sobre cada uno de los objetivos sobre el presente análisis difiere.

ISSAF con los pasos que ofrece, tiene un mayor nivel de cobertura sobre el objetivo 1 o caracterizar la FIS, el objetivo 2 o planificar y preparar el análisis y el objetivo 3 o analizar

las vulnerabilidades de la red de la FIS; mientras que PTES con las fases que ofrece, tiene un mayor nivel de cobertura sobre el objetivo 4 o presentar resultados.

Por lo tanto, por una parte, ISSAF servirá como metodología principal para cumplir los primeros objetivos, por otra parte, se podría utilizar los recursos relacionados a la generación de reportes que ofrece la metodología PTES, generados como parte de los acuerdos entre el autor y la FIS, con el fin de obtener la mejor calidad en el análisis de vulnerabilidades en la FIS.

CAPÍTULO III MARCO METODOLÓGICO

3.1. PROCESO DE IDENTIFICACIÓN DE VULNERABILIDADES

Para el análisis de vulnerabilidades sobre cada componente o elemento de infraestructura de red de la FIS se realiza varios procesos, los cuales se recopilan a su vez en el proceso de identificación de vulnerabilidades, mismo que cumple con el tercer objetivo específico relacionado con el diseño de un conjunto de procesos para la identificación de vulnerabilidades y se muestra a continuación.

Figura 5 - Proceso de Identificación de vulneabilidades
Fuente: Elaboración del autor

- **Selección de componente:** Este proceso consiste en el análisis de las categorías definidas por ISSAF y cada componente dentro de cada una de ellas con el fin de determinar aquellos componentes que forman la infraestructura de la FIS.

- **Recolección de información:** Este proceso consiste en la recolección de información relacionada con los componentes de infraestructura de la FIS mediante reuniones presenciales y virtuales.
- **Preparación de pruebas:** Este proceso consiste en la definición del enfoque de pruebas, sea mediante la ejecución de software o la aplicación de encuestas para cada componente de infraestructura que, gracias a la información obtenida en el proceso anterior permite ejecutar software y sus configuraciones alternas a las definidas por ISSAF, así como también los temas a tratar por medio de las encuestas.
- **Aplicación de pruebas:** Este proceso consiste en la ejecución de las pruebas que requieran el uso de hardware, solicitud de permisos para dichas ejecuciones tanto al personal de la FIS como al personal de la DGIP debido a la criticidad de los sistemas, además, planificación de reuniones para la aplicación de las encuestas al personal de la FIS.
- **Identificación de vulnerabilidades:** Este proceso consiste en analizar los resultados obtenidos de manera posterior a la aplicación de las pruebas sobre cada componente de infraestructura de la FIS.

Los procesos mencionados serán socializados con el personal de la FIS y los resultados obtenidos serán entregados al mismo, lo cual servirá como un precedente y permitirá crear un plan de acción para mitigar las vulnerabilidades en su infraestructura de red.

Es necesario mencionar que, la información confidencial, los resultados obtenidos, las conclusiones y recomendaciones de carácter técnico serán recopilados en el reporte de ethical hacking y entregadas al equipo de TICs de la FIS.

3.2. CARACTERIZACIÓN DE LA FIS

“La Escuela Politécnica Nacional, debido al creciente desarrollo en el ámbito de la computación e informática y con la finalidad de formar profesionales solventes en el desarrollo de software, manejo de sistemas computacionales, sistemas de información, y demás disciplinas relacionadas decidió crear la carrera de Ingeniería de Sistemas en el año de 1985, quedando adscrita al Instituto de Informática y Computación. Formalmente se fundó en el año 1987 en las oficinas donde actualmente se encuentra la escuela de formación de tecnólogos (ESFOT), siendo además la primera Facultad de Ingeniería de Sistemas en el país” [32].

3.2.1. Misión de la FIS

“La Facultad de Ingeniería de Sistemas es el referente de la Escuela Politécnica Nacional en el campo de conocimiento y aplicación de las Tecnologías de Información y Comunicaciones; actualiza en forma continua y pertinente la oferta académica en los niveles de pregrado y postgrado para lograr una formación de calidad, ética y solidaria; desarrolla proyectos de investigación, vinculación y proyección social en su área científica y tecnológica para solucionar problemas de transcendencia para la sociedad” [32].

3.2.2. Visión de la organización

“La Facultad de Ingeniería de Sistemas está presente en posiciones relevantes de acreditación a nivel nacional e internacional y es referente de la Escuela Politécnica Nacional en el campo de las Tecnologías de la Información y Comunicaciones por su aporte de excelencia en las carreras de pregrado y postgrado que auspicia, la calidad y cantidad de proyectos de investigación, vinculación y proyección social que desarrolla y su aporte en la solución de problemas nacionales a través del uso intensivo y extensivo de la ciencia y la tecnología” [32].

3.2.3. Estructura Orgánica

La EPN define una estructura organizativa global, dentro de la cual, cada facultad, incluyendo a la FIS cuenta en la cima de la jerarquía con la máxima autoridad, la cual se encuentra en el decanato, bajo esta jerarquía se encuentra el subdecanato y en su conjunto tienen una responsabilidad clave en la gestión y desarrollo académico de una facultad universitaria.

Debajo de las autoridades de gestión y desarrollo académico se encuentran los equipos correspondientes a los diferentes departamentos que se encargan de la extensión de su área de especialización y los laboratorios de la FIS, que se encargan de la investigación en un área específica, en donde cada departamento y laboratorio cuenta con un equipo de coordinadores que realizan tareas específicas y reportan a sus respectivos jefes de departamento.

Esta estructura jerárquica ha permitido a la FIS mantener una organización eficiente y bien coordinada en su funcionamiento interno.

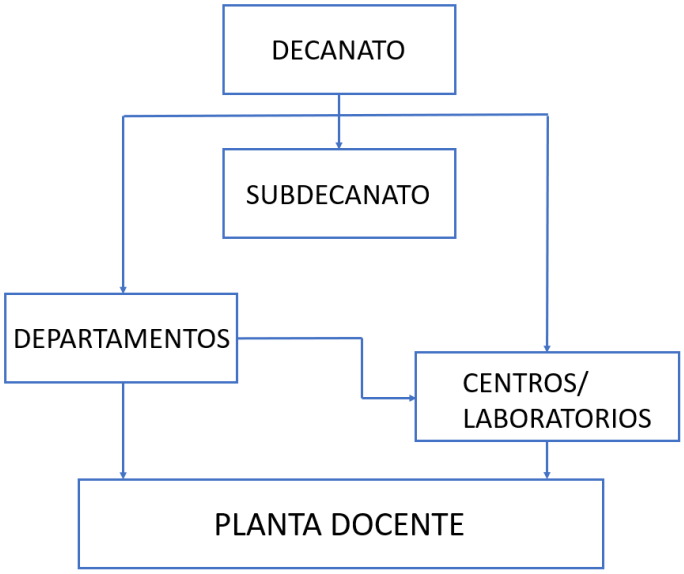


Figura 6: Estructura jerárquica de la FIS
Fuente: **[33]**

3.3. Desarrollo del análisis

3.3.1. Ambiente para las pruebas

Para el desarrollo del análisis de vulnerabilidades, en la medida de lo posible y dentro de los parámetros definidos dentro del acuerdo entre la FIS y el autor se utilizarán herramientas para obtener resultados en cada uno de los puntos que se cubrirán según corresponda de manera alineada con los acuerdos firmados al inicio del proyecto, sean estas herramientas de software o encuestas para obtención de información para aquellos casos en los cuales la naturaleza de las pruebas sugerida en las metodologías sea intrusiva. La obtención de información acerca de la infraestructura de red de la FIS implica

las tareas de recolección de información pública y el producto de la colaboración entre la FIS y el autor.

Las herramientas de software se las ha seleccionado con base en aquellas que sugiera la metodología para cada prueba y en aquellas pruebas en las que se necesite la ejecución de pruebas intrusivas se tomará en cuenta alternativas en software, en acciones o la adopción del enfoque de aplicación de encuestas.

El sistema operativo que se utilizará será *Windows* 11 [34] con las características que se muestran en la siguiente figura y para aquellas actividades que requieran de un navegador web se utilizará *Brave* [35] en su versión 1.51.110.

Figura 7 - Características del computador utilizado
Fuente: Elaboración del autor

Figura 8: Características de sistema operativo del computador utilizado
Fuente: Elaboración del autor

3.3.2. Recolección de información de fuentes públicas

Esta tarea es una de las más importantes para la aplicación del análisis de vulnerabilidades sobre la infraestructura de red de la FIS, ya que, el cumplimiento de los objetivos definidos depende en gran medida del grado de conocimiento que se tenga acerca de la FIS, tomando en cuenta desde su contexto, es decir, aquella información relacionada con su definición hasta su infraestructura. La recolección de la información permitirá conocer el grado de exposición de la FIS en el internet, el cual se muestra a continuación:

- **Sitios web corporativos**

  Esta fuente permitirá obtener información del sitio web de la FIS mediante el uso de la extensión de navegador web *Wappalyzer* [36], que permitirá identificar las tecnologías involucradas en el desarrollo del sitio web objetivo con sus respectivas versiones para aquellas que apliquen.

  Una vez instalada la extensión en el navegador web, se navegó hacia el sitio web oficial de la FIS https://www.fis.epn.edu.ec y se hizo uso de la extensión, cuyo resultado se muestra en el reporte de ethical hacking:

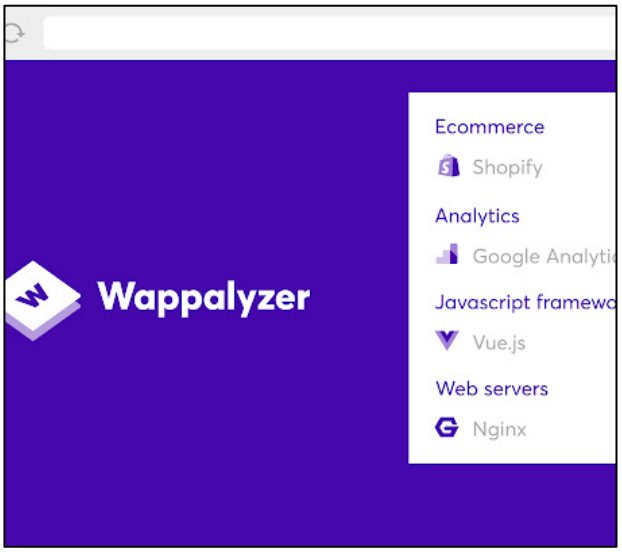


Figura 9: Herramienta de análisis de tecnologías utilizadas en el sitio web de la FIS
Fuente: **[36]**

Para complementar la tarea se utilizó adicionalmente la herramienta *Website Recon Report (Light)* [37] proporcionada por el sitio web https://pentest-tools.com/ especializado en herramientas de esta naturaleza.

Esta herramienta, además de identificar el *software* detrás de la página web de la FIS provee un apartado de descripción de riesgo encontrado y un apartado de recomendaciones, cuyo resultado se muestra en el reporte de ethical hacking.

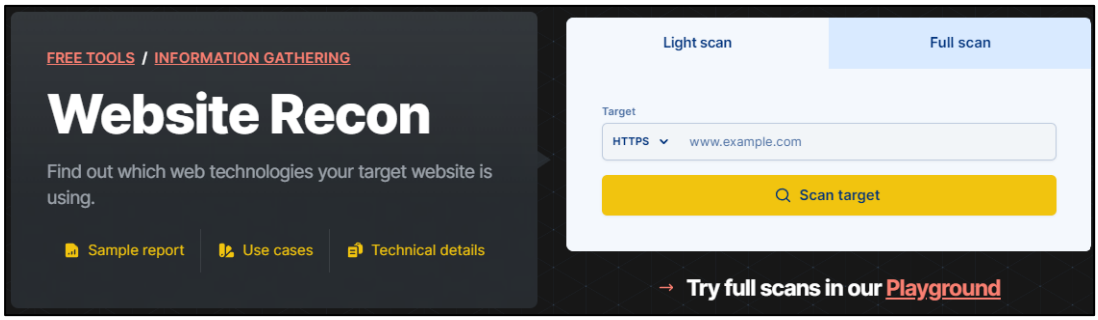


Figura 10: Website Recon Report en la página de la FIS
Fuente: **[37]**

- ***Google dorks***

  Google [38], al ser un potente motor de búsqueda en Internet, dispone de una estructura específica al momento de realizar búsquedas específicas, a esto se le conoce como *dorks* [39]. La página https://pentest-tools.com/ utilizada en el punto anterior dispone de *dorks* listos para su uso sobre el objetivo del caso de estudio la FIS, cuyo resultado se muestra en el reporte de ethical hacking|:

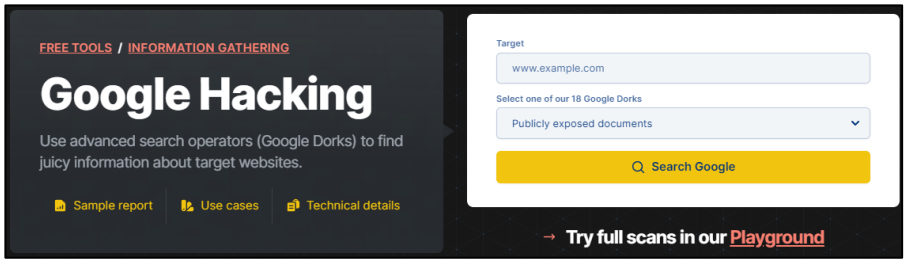


Figura 11: Documentos expuestos publicamente
Fuente: Elaboración del autor

- ***Wayback Machine***

  La organización sin ánimo de lucro Internet Archive ofrece el servicio en línea conocido como *Wayback Machine* [40], cuya función principal es capturar periódicamente sitios web y almacenar versiones antiguas de páginas web a lo largo del tiempo. El uso del sitio sobre la FIS es el de dimensionar las versiones existentes a la fecha de la página web, lo cual permitirá a la FIS analizar detalladamente las vulnerabilidades históricas e identificar los cambios no autorizados sobre la misma. El resultado de la búsqueda de la FIS en el sitio se muestra en el reporte de ethical hacking.

Figura 12: Sitio web Wayback Machine
Fuente: Elaboración del autor

- **Ataques sobre la página web de la FIS**

  Usando la herramienta online Is-It-Hacked [41], desde su página web www.isithacked.com, la cual permite determinar si la página web ha sido atacada mediante la comparación de la dirección IP del sitio web con una lista de sitios web pirateados conocidos se realizó una búsqueda, misma que dio el siguiente resultado:

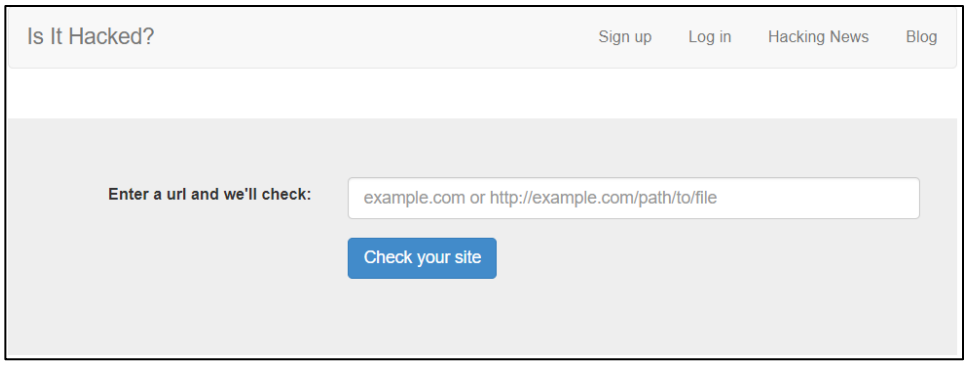


Figura 13: Sitio web IsItHacked
Fuente: Elaboración del autor

- **Redes Sociales**

  Las redes sociales son lugares en internet en donde se comparte información y se interactúa con las comunidades, por lo cual, es relevante revisar la actividad de la FIS dentro de ellas, con el fin de determinar su gestión de información e identificar posibles filtraciones sean estas intencionales o involuntarias. Para ello, se navegó en las redes sociales oficiales de la FIS, las cuales son *Facebook* [42] y *Twitter* [43].

- *Facebook*

Una vez que se navegó dentro de la red social *Facebook*, su resultado se muestra en el reporte de *ethical hacking*.

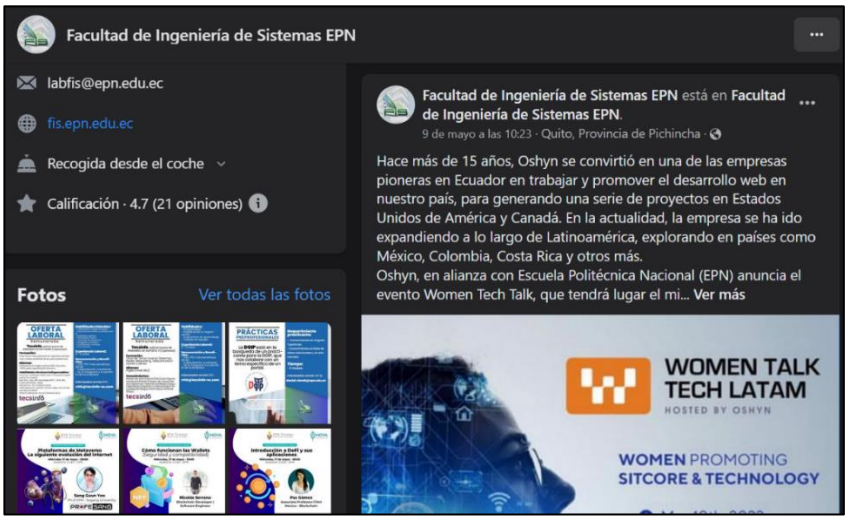


Figura 14: Contenido del perfil de la FIS en Facebook
Fuente: Facultad de Ingeniería de Sistemas EPN **[44]**

- *Twitter*

Una vez que se navegó dentro de la red social *Twitter*, su resultado se muestra en el reporte de *ethical hacking*.

Figura 15: Contenido del perfil de la FIS en Twitter
Fuente: FIS – EPN **[45]**

3.3.3. Topología de red y mapeo de red subyacente

El mapeo de la topología de la red de la FIS es una actividad clave del análisis de vulnerabilidades ya que permitirá identificar la estructura de la red, los sistemas operativos y las aplicaciones en uso, así como posibles vectores de ataque, cuyas acciones se encuentran limitadas a aquellas acordadas en un inicio con la FIS, pretendiendo cubrir los siguientes puntos en la medida en la que sea posible:

- *Hosts* activos.
- Mapeo del perímetro de la red.
- Identificación de rutas mediante la base de información de gestión (MIB).

Por lo tanto, lo que se muestra a continuación es producto de la colaboración y las reuniones entre el autor con el área de *TIC*s de la FIS y con la DGIP EPN al tratarse de información que no es de carácter crítico.

- **Identificación de activos de la organización**

  A pesar de que la metodología ISSAF no sugiere procedimientos para la identificación de activos, resalta la importancia de realizar esta tarea mediante la consideración de la arquitectura de red, diagramas funcionales, componentes de seguridad, puntos de acceso y la colaboración por parte de una organización, siendo en este caso el área de *TICs* de la FIS; debido a que se trata de un punto de partida para la aplicación de todas las pruebas que contiene el análisis de vulnerabilidades.

- **Administración de infraestructura de la FIS**

  Las instalaciones de la FIS constan de un edificio de 7 pisos distribuidos de la siguiente manera:

  - **Planta baja:** Cafetería de la EPN.
  - **Primer piso:** Servicio médico, diversas especialidades.
  - **Segundo piso:** Oficinas administrativas y de docentes de la FIS.
  - **Tercer piso:** Centro de datos y aulas con computadores.
  - **Cuarto piso:** Laboratorios de investigación.
  - **Quinto:** Aulas sin computadores.

La infraestructura de red que se distribuye para toda la FIS se origina en el centro de datos que se encuentra en el tercer piso y está constituido por un switch principal, el cual se encarga de recibir información a través de fibra óptica, a su vez conectado a un switch secundario de distribución para los switches localizados entre el segundo piso y el quinto piso. El centro de datos de la FIS se encuentra dentro de un espacio que dispone de las condiciones necesarias para un correcto desempeño, tomando como referencia las recomendaciones de la norma ISO 27001.

A partir del *switch* secundario se comparte información a los usuarios finales mediante puntos de acceso, teniendo en el segundo piso dos de ellos, en el tercer piso 3 de ellos, en el cuarto piso dos de ellos y en el quinto piso 2 de ellos.

La infraestructura de red descrita en el párrafo anterior es administrada en gran parte por la propia FIS, sin embargo, comparte administración con la dirección de gestión de la información y procesos DGIP de la EPN.

- **Arquitectura de red por capas**

La metodología ISSAF define cinco capas o niveles que recomienda utilizar con el fin de evaluar y proteger la seguridad de la información en la FIS. Cada una de estas capas está diseñada para proteger un aspecto específico del sistema de información y tiene una función específica dentro de la protección de su información, sin embargo, no todas las organizaciones tienen su arquitectura de esta manera.

Para obtener las diferentes capas definidas por ISSAF para la FIS se partió de la topología general de su infraestructura, la cual se muestra en el reporte de *ethical hacking*.

El detalle de las capas de red de la arquitectura se detalla a continuación:

- **Capa de acceso**

  Esta capa es la responsable de conectar dispositivos finales como estaciones de trabajo, servidores e impresoras a la red y es en esta capa en donde se aplican controles de seguridad como seguridad de puertos, autenticación 802.1X y VLAN para limitar el acceso a la red.

El detalle de estos switches secundarios se lo obtendrá mediante la aplicación de una encuesta al equipo de la DGIP, cuyos resultados se muestran en el reporte de *ethical hacking*

- **Capa de distribución**

Esta capa es la responsable de conectar múltiples switches de capa de acceso y enrutar el tráfico entre ellos, lo cual implica la posibilidad de proporcionar redundancia, equilibrio de carga y aplicación de políticas en el borde de la red. Además, en esta capa es posible la aplicación de controles de seguridad como listas de control de acceso (ACL) y filtrado en esta capa para evitar que el tráfico no autorizado ingrese a la capa central.

- **Capa central**

Esta capa es la responsable de proporcionar conectividad de alta velocidad entre los switches de la capa de distribución y está diseñada para un reenvío rápido de paquetes con una latencia mínima. Esta capa a menudo está diseñada para ser altamente disponible y resistente, con enlaces y equipos redundantes para garantizar el tiempo de actividad de la red. Permite la implementación de controles de seguridad como sistemas de firewall y detección y prevención de intrusiones (IDS/IPS) para proteger la red de amenazas externas.

3.3.4. Análisis de riesgos

En el contexto actual de la ciberseguridad, es fundamental que las organizaciones cuenten con medidas adecuadas para proteger sus activos críticos de la información. En este sentido, el análisis de riesgos y el análisis de vulnerabilidades son actividades fundamentales que permiten identificar, evaluar y gestionar los riesgos asociados a las vulnerabilidades presentes en la infraestructura de red.

El análisis de vulnerabilidades es una actividad que permite detectar y evaluar las debilidades presentes en la infraestructura de red, mientras que el análisis de riesgos permite identificar y evaluar las amenazas asociadas a dichas vulnerabilidades, así como determinar la probabilidad de que se materialicen y el impacto que podrían causar en caso de materializarse. Por esta razón, el análisis de riesgos sobre la FIS resulta esencial para establecer prioridades en cuanto a la implementación de medidas de seguridad y para tomar decisiones informadas en cuanto a la gestión de los riesgos asociados a las

vulnerabilidades que puedan estar presentes en su infraestructura de red y analizadas en la sección posterior al presente.

A pesar de que, comúnmente se realiza primero el análisis de vulnerabilidades y posteriormente el análisis de riesgos, para el caso de la FIS se cuenta previamente la información correspondiente al análisis de riesgos. Por lo tanto, se ha decidido utilizar dicha información como base para enfocar de mejor manera el análisis de vulnerabilidades sobre los riesgos identificados. Esto permitirá el ahorro de tiempo y recursos, ya que no se realizará un análisis exhaustivo de todas las vulnerabilidades, sino que se enfocará en aquellas que representan un mayor riesgo para la organización. Además, al utilizar el análisis de riesgos existente como base, se garantiza que el análisis de vulnerabilidades se encuentre alineado con los objetivos estratégicos y de seguridad de la FIS.

El análisis de riesgos realizado sobre la FIS es cuantitativo y contempla riesgos determinados como parte de una auditoría con los siguientes tipos de impactos:

- **Ambiental:** Son aquellos relacionados con daños producidos al medio ambiente.
- **Con terceros:** Son aquellos relacionados con daños o afectaciones a los grupos de interés de la entidad.
- **Conocimiento:** Son aquellos asociados con daños por la pérdida del conocimiento e información vital para el desarrollo de las actividades de una entidad.
- **Financiero:** Son aquellos asociados con daños en los activos de la entidad o en su capacidad para producir ingresos.
- **Imagen:** Son aquellos que generan un daño en la confianza por parte de la ciudadanía hacia la entidad.
- **Legal:** Son aquellos Relacionados con sanciones de tipo legal como intervenciones, multas, pérdida de una licencia de operación o de la personería jurídica, entre otros. Estos riesgos suelen estar vinculados también con sanciones económicas.
- **Operacional:** Son aquellos relacionados al daño o degradación que limita o restringe el desarrollo normal de los procesos, la producción y entrega de productos y la prestación de servicios.

- **Recursos:** Son aquellos asociados a daños en insumos, compras, y, en general, en los servicios y suministros que permiten desarrollar el objeto social.
- **Regulatorio:** Son aquellos asociados con los daños ocasionados por la violación de una prescripción u obligación legal.
- **Tecnológico:** Son aquellos relacionados al daño de sistemas o equipos.

La valoración de los riesgos identificados en orden descendente en función de su criticidad se muestra a continuación.

Tabla 2 - Valoración de riesgos en función de su criticidad

VALOR	ESCALA
Entre 1 – 10	Bajo
Entre 11 – 20	Moderado
Entre 21 – 40	Alto
Entre 41 – 75	Extremo

Fuente: Documentación de TICs FIS

La valoración de impacto de un riesgo en orden ascendente sobre la FIS se presenta a continuación.

Tabla 3 - Valoración de impacto de riesgos

VALOR	ESCALA
Entre 0 – 3	Insignificante
Entre 4 – 6	Menor
Entre 7 – 9	Moderado
Entre 10 – 12	Mayor
Entre 13 – 15	Catastrófico

Fuente: Documentación de TICs FIS

La valoración de probabilidad de un riesgo en orden ascendente se presenta a continuación.

Tabla 4 - Valoración de la probabilidad de riesgos

VALOR	ESCALA
1	Raro
2	Improbable
3	Posible
4	Probable
5	Casi seguro

Fuente: Documentación de TICs FIS

El listado de los riesgos identificados en orden descendente de acuerdo con su criticidad junto a su valoración se encuentra en el Anexo IV y su evaluación se muestra a continuación.

Tabla 5 - Evaluación de riesgos

PROBABILIDAD	VALOR	3	6	9	12	15
RARO	1				7, 12, 24 (3)	
IMPROBABLE	2	16, 19 (2)		22, 26, 30, 31 (4)	21, 33 (2)	
POSIBLE	3			10, 23, 32 (3)		36 (1)
PROBABLE	4			1, 13, 15, 17, 25, 27, 34, 35 (8)	9, 14, 18, 28, 29 (5)	
CASI SEGURO	5		2 (1)		3, 4, 5, 6, 11, 20 (6)	8 (1)
	IMPACTO	INSIGNIFI-CANTE	MENOR	MODERA-DO	MAYOR	CATASTRÓ-FICO

EXTREMO	Riesgo extremo: requiere acción inmediata	13 riesgos
ALTO	Riesgo alto: requiere acción a corto plazo	14 riesgos
MODERADO	Riesgo moderado: requiere acción a mediano plazo	7 riesgos

BAJO	Riesgo bajo: requiere acción a largo plazo	2 riesgos
	Total riesgos	**36 riesgos**

Fuente: Documentación de TICs FIS

De acuerdo con los resultados del análisis de riesgos que afectan los diferentes aspectos dentro de la FIS, es importante tomar medidas preventivas y mitigar los riesgos de acuerdo con su criticidad e impacto. La información obtenida del análisis de riesgos permitirá a la FIS junto con el autor identificar las vulnerabilidades a las cuales prestar mayor atención dentro del análisis de vulnerabilidades que se realizará en la siguiente sección, y así establecer un plan de acción que permita a la FIS minimizar sus riesgos y estar preparados ante posibles ataques o incidentes.

3.3.5. Análisis de vulnerabilidades

El análisis de vulnerabilidades es una parte fundamental en la seguridad de cualquier infraestructura de red, ya que permite identificar y evaluar las posibles vulnerabilidades en la misma. El análisis de riesgos previo junto a este análisis es complementario, ya que permite identificar de manera específica las posibles amenazas que pueden materializarse en la red y las vulnerabilidades que pueden ser explotadas para llevar a cabo dichas amenazas.

A través de este análisis, será posible conocer con mayor profundidad los sistemas y servicios de la red, así como los posibles vectores de ataque que podrían ser utilizados por un atacante, para lo cual se aplicarán pruebas sobre cada aspecto dentro de la infraestructura de la FIS mediante el uso tanto de herramientas de software como del enfoque de aplicación de encuestas. De esta manera, se pueden tomar medidas preventivas y correctivas para minimizar los riesgos y garantizar la seguridad de la infraestructura de red.

Es necesario mencionar que, la información confidencial, los resultados obtenidos, las conclusiones y recomendaciones de carácter técnico serán recopilados en el reporte de ethical hacking y entregadas al equipo de TICs de la FIS. Sin embargo, las encuestas aplicadas se mostrarán en el presente documento para cada componente de red que corresponda.

3.3.5.1 Pruebas de seguridad en la red

Este tipo de pruebas se enfocan en el análisis de los componentes de la red, identificando vulnerabilidades en *routers*, *switches*, entre otros dispositivos dentro de la infraestructura de red de la FIS.

Debido a la criticidad, la confidencialidad de la información y de acuerdo con las normativas relacionadas con el manejo de la información vigentes en la EPN, no es posible aplicar pruebas con software en componentes considerados críticos, por lo cual, se procede a la aplicación de encuestas para los casos mencionados.

- **Evaluación de seguridad de contraseñas**

El análisis de contraseñas utilizando ISSAF implica la aplicación de pruebas intrusivas, sin embargo, debido al alcance y los acuerdos con la FIS la naturaleza de las pruebas que se aplican durante el análisis es no intrusiva.

Para esta evaluación, se procede a verificar las políticas de contraseñas tomando como referencia los controles que provee CIS [46].

Tabla 6 - Evaluación de seguridad de contraseñas

POLÍTICA DE CONTRASEÑA	DETALLE
Autenticación multifactor (MFA)	
Servidor de autenticación	
Longitud mínima obligatoria	
Longitud máxima	
Composición	
Expiración(obligatorio)/Rotación	
Baneo	
Bloqueo de la sesión frente a inactividad	
Límite de intentos fallidos	
Monitoreo de intentos fallidos	
Suspensión de cuentas en desuso	
Pista de contraseña	
Visualización de contraseña	
Permitir pegado del portapapeles	

Fuente: Controles CIS [47]

- **Evaluación de la seguridad de switch**

La metodología sugiere la aplicación de pruebas de seguridad para los *switches* de capa de red, tomando en cuenta a su vez los puntos de acceso de los *switches* de capa de enlace de una manera intrusiva, debido a lo cual se procede con un enfoque alternativo para su evaluación, el cual es la aplicación de una encuesta tomando como referencia los controles que provee CIS [46] tanto para el *switch* principal como para el secundario, sin embargo, la información recolectada se limita a aquella que no se considere crítica para la DGIP.

Tabla 7 - Evaluación de la seguridad de switch principal

CRITERIO DE SEGURIDAD	DETALLE
Fabricante y modelo	
Asignaciones de IP (estática, dinámica)	
Uso de configuraciones por defecto	
Puertos utilizados y su estado	
Implementación de listas de control de acceso (ACL)	
Protocolos habilitados	
Acceso remoto al switch	
Segmentación de VLANs	
Uso de autenticación para su acceso	
Logging para registro de eventos de seguridade	

Mecanismos de registro y auditoría para supervisar los intentos de acceso y cambios en configuración, notificaciones	
Tipo de dispositivos conectados directamente al switch	
Actualización de firmware	
Aplicación de parches de seguridad recomendadas por el fabricante	
Análisis periódicos de registros y eventos para identificar posibles intrusiones o comportamientos anómalos	

Fuente: Elaboración del autor

Tabla 8 - Evaluación de la seguridad de switch secundario

CRITERIO DE SEGURIDAD	DETALLE
Fabricante y modelo	
Asignaciones de IP (estática, dinámica)	
Uso de configuraciones por defecto	
Puertos utilizados y su estado	
Implementación de listas de control de acceso (ACL)	
Protocolos habilitados	
Acceso remoto al switch	
Segmentación de VLANs	

Uso de autenticación para su acceso	
Logging para registro de eventos de seguridade	
Mecanismos de registro y auditoría para supervisar los intentos de acceso y cambios en configuración, notificaciones	
Actualización de firmware	
Aplicación de parches de seguridad recomendadas por el fabricante	
Análisis periódicos de registros y eventos para identificar posibles intrusiones o comportamientos anómalos	

Fuente: Elaboración del autor

Además, gracias a la colaboración de la FIS y de la DGIP se tuvo acceso a uno de los *switches* secundarios, del cual se extrajo información mediante comandos, cuyos resultados se muestran en el reporte de *ethical hacking*.

Comando *show vlan*

Este comando se utiliza para mostrar las VLANs configuradas en el switch. La salida del comando incluye el ID, el nombre, el estado y los puertos troncales de la VLAN.

Comando *show version*

Este comando se utiliza para mostrar la versión de software y la configuración de un dispositivo Cisco.

Comando *show interfaces description*

Este comando se utiliza para mostrar la descripción de cada interfaz de un dispositivo Cisco. La salida del comando incluye la interfaz, el estado y la descripción del protocolo.

Comando *show interfaces status*

Este comando se utiliza para mostrar el estado de las interfaces de un dispositivo Cisco. La salida del comando incluye el puerto, el nombre, el estado, la vlan, el dúplex, la velocidad de la interfaz.

Comando *show arp*

Este comando se utiliza para mostrar la tabla ARP en un dispositivo Cisco. La tabla ARP es una base de datos que almacena las direcciones IP y las direcciones MAC de todos los dispositivos conectados al switch.

Comando *show spanning-tree*

Este comando se utiliza para mostrar la información del árbol de expansión en un dispositivo Cisco. El árbol de expansión es un protocolo que se utiliza para evitar bucles en una red.

Comando *show running-config*

Este comando se utiliza para para mostrar la configuración actual de un dispositivo Cisco.

Comando *show startup-config*

Este comando se utiliza para mostrar la configuración de início del *switch*. La configuración de inicio es aquella que se carga en la memoria al arrancar el dispositivo, normalmente se almacena en memoria no volátil (NVRAM) para que no se pierda al apagar el dispositivo.

Comando *show port-security*

Este comando se utiliza para mostrar la configuración de seguridad de puertos en un switch.

- **Evaluación de la seguridad de *router***

La metodología sugiere la aplicación de pruebas de seguridad para los *routers* con el fin de identificar información acerca del estado de los puertos, estado de los servicios, protocolos de enrutamiento, entre otros datos.

Por la criticidad de estos componentes, la confidencialidad de la información y de acuerdo con las normativas relacionadas con el manejo de la información vigentes en la EPN no es posible aplicar pruebas sobre este componente de infraestructura de red, por lo cual se procede a verificar la seguridad de *router* mediante la aplicación de una encuesta al personal de la DGIP, cuyos resultados se muestran en el reporte de *ethical hacking*.

Tabla 9 - Evaluación de la seguridad de router

CRITERIO DE SEGURIDAD	DETALLE
Fabricante y modelo	
Uso de configuraciones predeterminadas	
Uso de autenticación para su acceso	
Asignaciones de IP	
Acceso remoto al switch	
Medidas de seguridad implementadas	
Logging para registro de eventos de seguridad (Lugar de almacenamiento de registros, información almacenada)	

Mecanismos de registro y auditoría para supervisar los intentos de acceso y cambios en configuración, notificaciones	
Tipo de dispositivos conectados directamente al router	
Conexiones VPN configuradas en el router	
Actualización de firmware (gestión de versiones, hasta cuántas atrás se admite)	
Aplicación de parches de seguridad recomendadas por el fabricante	

Fuente: Controles CIS [11]

- **Evaluación de la seguridad de VPN**

El objetivo de esta prueba es comprobar las restricciones que se pudiera tener hacia el Internet desde su acceso mediante VPN.

Debido a que las VPN se utilizan para crear una conexión segura entre dos redes los usuarios podrían acceder a recursos de la red privada de la FIS y/o de la EPN desde una red pública. Sin embargo, las VPN también pueden ser vulnerables a ataques, lo que podría permitir a los atacantes obtener acceso a los recursos de la red privada.

Para lo cual, se procede a verificar el acceso a páginas *web* de redes sociales, servicios de *streaming*, informativas y de dominio de nivel superior epn.edu.ec mediante el uso de la herramienta *NetScaler Gateway* [48] utilizada dentro de la EPN para servicios de VPN.

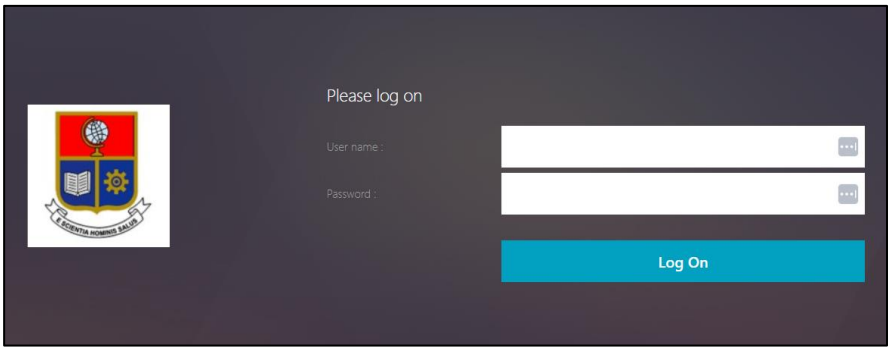


Figura 16 – Uso de la herramienta NetScaler Gateway
Fuente: Elaboración del autor

- **Estrategia de gestión y evaluación de seguridad de sistema antivirus**

El objetivo de esta prueba es comprobar el aporte que tiene el sistema antivirus a la infraestructura de la FIS.

La FIS se encarga de la instalación del agente antivirus y supervisar su uso en los computadores preparados para entregar al personal asignado.

Para lo cual, se procede a verificar las políticas vigentes sobre el sistema antivirus partiendo tanto de las recomendaciones del fabricante como de los controles que provee CIS [46].

Tabla 10 - Evaluación de seguridad del sistema antivirus

CRITERIO DE SEGURIDAD	DETALLE
Instalado junto al Firewall	
Restricción de acceso remoto y local de los computadores que tienen instalado antivirus	
Servidor admite la administración	
Acceso solamente a interfaces de la aplicación por parte de personal autorizado para instalar y configurar la aplicación	
Configuración por defecto	
Actualización de base de datos de virus administrada	
Actualización de versión de software administrada	
Escaneos automáticos	
Capacidad de detectar de virus	
Capacidad de identificar virus	
Capacidad de detectar de gusanos	

Capacidad de detectar de troyanos	
Capacidad de detectar de macros	
Capacidad de detectar de ransomware	
Usuarios tienen la posibilidad de desactivar la protección	

Fuente: Controles CIS [11]*, características de antivirus.*

- **Evaluación de la seguridad de WLAN**

El objetivo de esta prueba es comprobar la seguridad de las redes inalámbricas de la FIS, las cuales principalmente son 4.

Para lo cual, se procede a verificar los diferentes criterios de seguridad sobre la red inalámbrica.

Tabla 11 - Evaluación de seguridad de WLAN

CRITERIO DE SEGURIDAD	DETALLE
Existe más de una red wifi a nivel de facultad y administrada por la FIS	
¿Cuántos dispositivos y conexiones son soportados a través de Wi-Fi?	
¿Cuáles son las necesidades de velocidad de datos de estos dispositivos a través de Wi-Fi?	
Fuentes de interferencia y su potencia	
Estándar de la red	
Configuración por defecto	
Capacidad de aplicar políticas (administración)	
SSID por defecto	
SSID broadcast active	
Tipo de autenticación	
Tipo de encriptación	
Gestión de las credenciales de acceso	
Control de acceso para administrar la red	
Controles mediante direcciones MAC	
Actualizaciones de firmware	

Fuente: Controles CIS [11]

- **Seguridad de usuario de internet**

El objetivo de esta prueba es comprobar la seguridad que tiene la sesión de un usuario final en la FIS, sea este parte del personal docente, personal administrativo, personal estudiantil o personas externas a la FIS y la EPN.

Para lo cual, se procede a verificar la seguridad de usuario mediante la siguiente encuesta.

Tabla 12 - Evaluación de seguridad de usuario de internet

CRITERIO DE SEGURIDAD	DETALLE
Uso de IRC	
Revelación de IP	
Instalación de aplicaciones IRC	
Transferencia de código malicioso	
Intercambio de archivos P2P	
Uso de navegadores de internet	
Actualización de navegadores	
Uso de programas para administración remota de dispositivos	
Activación de RDP en escritorios Windows	
Ataques de ingeniería social	

Fuente: Controles CIS [11]

3.3.5.2. Pruebas de seguridad de hosts

Este tipo de pruebas se enfocan en el análisis de los equipos de cómputo y servidores, buscando identificar vulnerabilidades, configuraciones inseguras o posibles puntos de entrada para un atacante.

- **Evaluación de la seguridad de sistemas operativos unix/linux**

El objetivo de esta prueba es comprobar la seguridad que tienen los sistemas operativos Unix/Linux disponibles para los estudiantes dentro de la FIS.

Para esta evaluación, se procede a verificar la seguridad de sistemas operativos Unix/Linux mediante la siguiente encuesta.

Tabla 13 - Evaluación de seguridad de sistemas operativos Unix/Linux

CRITERIO DE SEGURIDAD	DETALLE
Versión mínima obligatoria de SO	
Gestión de acceso	
Configuración de roles y permisos dentro del SO	
Control de tráfico de red	
Parcheo de vulnerabilidades	
Remoción de software innecesario	
Monitoreo continuo	
Comunicaciones seguras	
Backups regulares	
Protección de sesiones remotas	
Ejecución de dispositivos removibles	

Fuente: Controles CIS [11]

- **Evaluación de la seguridad de sistemas operativos *windows***

El objetivo de esta prueba es comprobar la seguridad que tienen los sistemas operativos Windows disponibles para los estudiantes dentro de la FIS.

Para lo cual, se procede a verificar la seguridad de sistemas operativos Windows mediante la siguiente encuesta.

Tabla 14 - Evaluación de seguridad de sistemas operativos windows

CRITERIO DE SEGURIDAD	DETALLE
Versión mínima obligatoria de SO	
Gestión de acceso	
Configuración de roles y permisos dentro del SO	
Control de tráfico de red	
Parcheo de vulnerabilidades	
Remoción de software innecesario	
Monitoreo continuo	
Comunicaciones seguras	
Backups regulares	
Protección de sesiones remotas	
Ejecución de dispositivos removibles	

Fuente: Controles CIS [11]

- **Evaluación de la seguridad de sistemas operativos Mac OS**

A pesar de no formar parte de ISSAF, es necesario aplicar la evaluación de seguridad de sistemas operativos Mac OS ya que existe un laboratorio que forma parte de la infraestructura de la FIS que contiene computadores con este sistema operativo.

El objetivo de esta prueba es comprobar la seguridad que tienen los sistemas operativos Mac OS disponibles dentro de la FIS.

Para lo cual, se procede a verificar la seguridad de sistemas operativos Mac OS mediante la siguiente encuesta.

Tabla 15 - Evaluación de seguridad de sistemas operativos Mac OS

CRITERIO DE SEGURIDAD	DETALLE
Versión mínima obligatoria de SO	
Gestión de acceso	
Configuración de roles y permisos dentro del SO	
Control de tráfico de red	
Parcheo de vulnerabilidades	
Remoción de software innecesario	
Monitoreo continuo	
Comunicaciones seguras	
Backups regulares	

Protección de sesiones remotas	
Ejecución de dispositivos removibles	

Fuente: Controles CIS [11]

- **Evaluación de seguridad del ambiente de virtualización**

A pesar de no formar parte de ISSAF, es necesario aplicar la evaluación de seguridad del ambiente de virtualización, cuya infraestructura se encuentra alojada en las instalaciones de la DGIP, pero su administración lógica se encuentra a cargo de la FIS.

Este ambiente de virtualización permite el abastecimiento de infraestructura para diferentes fines, como lo son el aprovisionamiento de VDIs a los estudiantes que lo requieran con el software que oferta la EPN, el aprovisionamiento de entornos con máquinas virtuales y capacidad de almacenamiento para el uso de estudiantes de pregrado bajo la supervisión de un profesor para el aprendizaje de varias materias, el aprovisionamiento de máquinas virtuales con fines de investigación para profesores cursando maestría o doctorado.

El detalle acerca de las capacidades de este ambiente se muestra en el reporte de *ethical hacking*.

Para comprobar el estado de la seguridad del ambiente de virtualización, se procede a la aplicación de la siguiente encuesta.

Tabla 16 - Evaluación de seguridad de ambiente de virtualización

CRITERIO DE SEGURIDAD	DETALLE
Rendimiento cumple con las necesidades	
Escalabilidad (aplicación, a nivel de componentes)	
Integración de los recursos con servidores o políticas de autenticación utilizados	
Elasticidad	
Seguridad	
Cumplimiento	
Facilidad de administración	
Disponibilidad	
Autenticación	
Control de la infraestructura subyacente (PaaS, SaaS)	

Fuente: Controles CIS [11]

3.3.5.3. Pruebas de seguridad de aplicaciones web

Este tipo de pruebas se enfocan en la evaluación de la seguridad de aplicaciones web, arquitectura y configuración, para identificar vulnerabilidades que puedan ser explotadas por atacantes.

Sin embargo, el contenido web como aplicaciones y el *back-end* de las páginas dentro de la EPN, incluidas las relacionadas con la FIS es administrado por la DGIP, mientras que la administración del *front-end* de las páginas que se muestra a continuación está a cargo de la FIS, por lo cual, el *front-end* es sujeto de análisis y consiste en insertar acciones específicas con el objetivo de comprobar el estado de seguridad de cada una de las páginas.

Debido a la criticidad, la confidencialidad de la información y de acuerdo con la normativa vigente de la DGIP, no es posible aplicar pruebas con software en componentes considerados críticos, como lo son las páginas web, por lo cual, se procede a la aplicación de encuestas para los casos mencionados.

- **Frontend - página principal fis**

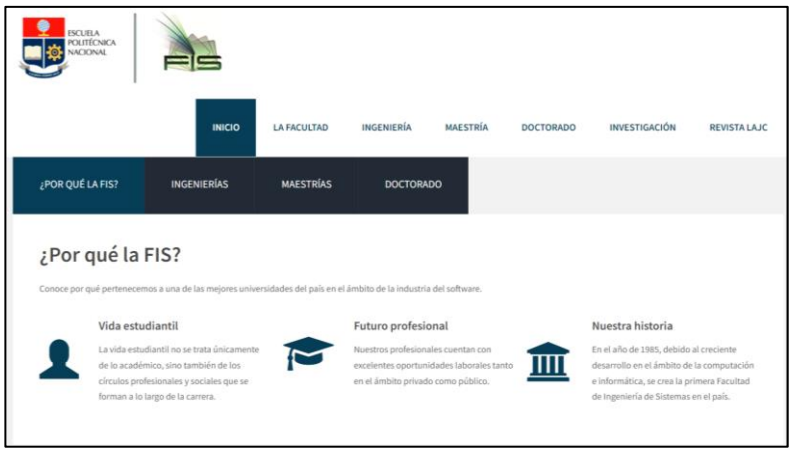


Figura 17 - Página web de la FIS
Fuente: FIS

Para comprobar el estado de la seguridad de la página web, se procede a la aplicación de la siguiente encuesta.

Tabla 17 - Evaluación de página web de la FIS

CRITERIO DE SEGURIDAD	DETALLE
Próposito de la página web	
Audiencia objetiva	
Políticas y procedimientos sobre esta página web	
Factores humanos que contribuyen con la seguridad de esta página web	
Alojamiento de la página web	
Tráfico	
Antecedentes de ataques	
Uso de conexiones seguras	
Políticas de privacidad y protección de datos de usuarios al momento de su ingreso	
Uso de *Logs* para registro de actividades	
Versiones de software utilizados	
Periodicidad de análisis (qué análisis hacen y cada cuánto)	
Uso de *plugins* y complementos de terceros	

Acceso mediante HTTPS	
Uso de WAF	
Uso de herramientas para detectar y/o responder ante posibles incidentes	

Fuente: Elaboración del autor

- **Frontend – Página web de las Jisic**

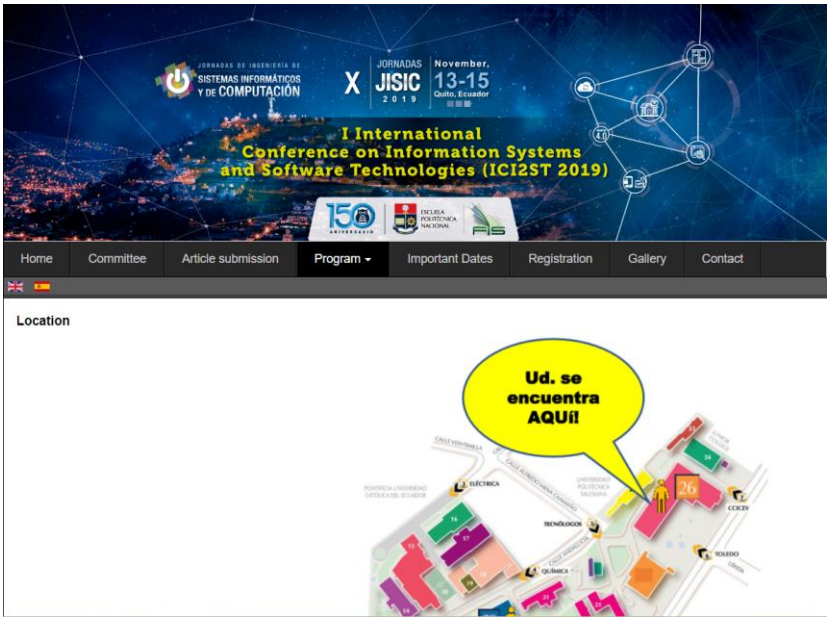


Figura 18 - Página web de las Jisic
Fuente: FIS

Para comprobar el estado de la seguridad de la página web, se procede a la aplicación de la siguiente encuesta.

Tabla 18 - Evaluación de página web de las JISIC

CRITERIO DE SEGURIDAD	DETALLE
Próposito de la página web	
Audiencia objetiva	
Políticas y procedimientos sobre esta página web	

Factores humanos que contribuyen con la seguridad de esta página web	
Alojamiento de la página web	
Tráfico	
Antecedentes de ataques	
Uso de conexiones seguras	
Políticas de privacidad y protección de datos de usuarios al momento de su ingreso	
Uso de *Logs* para registro de actividades	
Versiones de software utilizados	
Periodicidad de análisis	
Uso de *plugins* y complementos de terceros	
Acceso mediante HTTPS	
Uso de WAF	
Uso de herramientas para detectar y/o responder ante posibles incidentes	

Fuente: Elaboración del autor

- **Frontend – Página web ICI2ST**

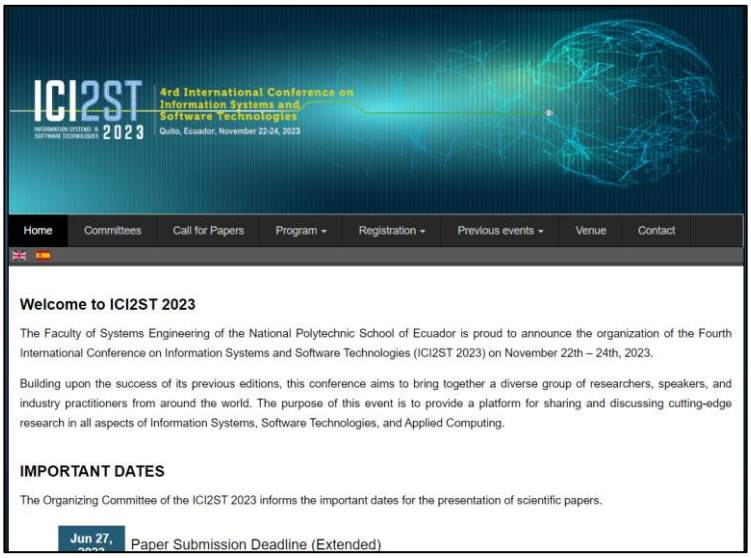


Figura 19 - Página web ICI2ST
Fuente: FIS

Para comprobar el estado de la seguridad de la página web, se procede a la aplicación de la siguiente encuesta.

Tabla 19 - Evaluación de página web de ICI2ST

CRITERIO DE SEGURIDAD	DETALLE
Próposito de la página web	
Audiencia objetiva	
Políticas y procedimientos sobre esta página web	
Factores humanos que contribuyen con la seguridad de esta página web	
Alojamiento de la página web	
Tráfico	
Antecedentes de ataques	
Uso de conexiones seguras	

Políticas de privacidad y protección de datos de usuarios al momento de su ingreso	
Uso de *Logs* para registro de actividades	
Versiones de software utilizados	
Periodicidad de análisis	
Uso de *plugins* y complementos de terceros	
Acceso mediante HTTPS	
Uso de WAF	
Uso de herramientas para detectar y/o responder ante posibles incidentes	

Fuente: Elaboración del autor

3.3.5.4. Pruebas de seguridad física

Este tipo de pruebas se enfoca en la evaluación de la seguridad de los sistemas físicos de la organización, como cámaras, controles de acceso, sistemas de alarmas, entre otros, con el fin de identificar posibles vulnerabilidades que puedan ser explotadas por atacantes.

La FIS, al ser una de las facultades en donde más se estudian y aplican las ciencias de la computación, necesita una infraestructura más robusta en comparación con otras facultades dentro de la EPN. Dicha infraestructura incluye *switches, routers*, servidores y equipos finales, lo cual requiere la aplicación de seguridad física y ambiental para garantizar las condiciones mínimas de desempeño.

- **Control de acceso magnético:**

Este tipo de control se encuentra implementado en la FIS, como se muestra a continuación:

Figura 20 - Cerraduras magnéticas del sistema de control de acceso magnético
Fuente: FIS

Figura 21 - Lector biométrico de acceso implementado en la FIS
Fuente: FIS

Figura 22 - Lector biométrico de acceso implementado en la FIS
Fuente: FIS

- **Cámaras de seguridad**

Esta implementación permite a los guardias el monitoreo de las instalaciones en tiempo real, como se muestra a continuación.

Figura 23 - Cámara de seguridad implementada en la FIS
Fuente: FIS

Figura 24 - Cámara de seguridad implementada en la FIS
Fuente: FIS

- **Señalética:**

La señalética de la FIS presenta indicaciones para el caso de incendios, desastres naturales, botiquín y nomenclatura para los puntos de conexión, como se muestra a continuación.

Figura 25 - Señalética de prohibiciones
Fuente: FIS

Figura 26 - Señalética de botiquín primeros auxilios
Fuente: FIS

Figura 27 - Señalética de tomacorrientes y puertos
Fuente: FIS

- **Alarmas de emergencia**

Este sistema de alarmas dispuesto en puntos estratégicos de la FIS funciona para alertar a tiempo real alguna eventualidad que exista y requiera tanto de la evacuación de las instalaciones como de la atención de la comunidad politécnica, lo cual semuestra a continuación.

Figura 28 - Alarmas de emergencia
Fuente: FIS

- **Sistema de enfriamiento continuo**

Este sistema se encuentra implementado en la FIS y actúa de manera independiente de la temperatura del ambiente garantizando una temperatura constante de 17 °C, como se muestra a continuación.

Figura 29 - Sistema de enfriamiento continuo
Fuente: FIS

Figura 30 - Controlador del sistema de enfriamiento
Fuente: FIS

- **Acceso a los Access Points:**

Los *Access Points* presentan dificultad de acceso para cualquier persona, ya que, para su manipulación se requiere la autorización previa por parte de la FIS y el uso de escaleras.

Figura 31 - Ubicación de Access Point en la parte superior
Fuente: FIS

- **Dificultad de acceso a los puntos de conexión**

Los puntos de conexión presentan dificultad de acceso para cualquier persona y se encuentra restringido por puertas de vidrio.

Figura 32 - Obstáculo para acceso a puntos de conexión
Fuente: FIS

- **Protección de Switches:**

Los *switches* de la FIS se encuentran protegidos por una caja metálica asegurada con candado y su acceso es mediante el uso de llaves de seguridad para abrir el seguro que los contiene.

Figura 33 - Protección de switches
Fuente: FIS

- **Control de acceso e identificación de terceros:**

Debido a la necesidad de reconocimiento de personal externo a la EPN con el personal docente incluyendo la planta estudiantil, existe un control de acceso implementado por la EPN. Sin embargo, es necesario aplicar un control de acceso para personas que deseen ingresar a las instalaciones de la FIS que no sean parte del personal docente o administrativo, es decir aplicable sobre personal externo en los casos que aplique y la planta estudiantil. Para ello, se cuenta con un guardia que solicita credenciales de identidad para el ingreso hacia donde se encuentra el personal docente y administrativo de la FIS.

La identificación de terceros es apoyada por el uso del sistema de cámaras, como se muestra en el reporte de *ethical hacking*.

CAPÍTULO IV CONLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El análisis de vulnerabilidades utilizando metodologías de ethical hacking ha sido fundamental para identificar y evaluar las debilidades en la infraestructura de red de la FIS. Lo cual, a su vez, ha proporcionado una visión clara de las posibles amenazas y riesgos a los que se enfrenta el entorno de TI.
- La recolección de información sobre la FIS de la universidad ha permitido obtener un conocimiento detallado tanto de la FIS como de la infraestructura, incluyendo activos de red, configuraciones relevantes y sistemas críticos. Esto ha sido esencial para comprender el alcance del análisis de vulnerabilidades.
- El diseño de un conjunto de procesos para identificar vulnerabilidades en la infraestructura de red de la FIS ha permitido la mejora de la eficiencia y efectividad del análisis. Estos procesos estandarizados permiten una evaluación sistemática y exhaustiva de los activos de red y garantizan una cobertura completa ante posibles vulnerabilidades.
- Se realizó la entrega del documento que contiene los resultados de las pruebas aplicadas sobre la infraestructura de red de la FIS según los lineamientos internos y acuerdos realizados.
- La selección de la metodología de *ethical hacking* a utilizar depende de varios factores y debe estar alineada con el tipo de organización, como también con los objetivos propuestos como lo fue ISSAF para este caso de estudio.

4.2 RECOMENDACIONES

- Mantener un programa continuo de análisis de vulnerabilidades utilizando metodologías actualizadas de *ethical hacking*. Esto garantizará una evaluación constante de la infraestructura de red y una respuesta proactiva a las nuevas amenazas y vulnerabilidades.
- Establecer un sistema de seguimiento y monitoreo para evaluar regularmente los resultados del análisis de vulnerabilidades. Esto garantizará la implementación efectiva de las acciones correctivas necesarias y la mejora continua de la seguridad de la infraestructura de red.
- Implementar un plan de educación a los usuarios de la infraestructura de red, con el fin de conseguir un marco de gobernanza y seguridad adecuado.
- Aplicar ingeniería del caos sobre los sistemas dentro de la infraestructura con el fin de identificar posibles puntos de mejora tras monitorear su reacción y su nivel de resiliencia.
- Sin importar el rol o la función que desempeñe un usuario en la FIS es necesario el cumplimiento de todos los controles, las políticas y las acciones definidas con el fin de garantizar la seguridad de la información y evitar excepcionamientos para usuarios privilegiados.

REFERENCIAS BIBLIOGRÁFICAS

[1] I. J. Miño, Interviewee, *Infraestructura de la FIS.* [Entrevista]. 2022.

[2] CISCO, «Cisco,» 2023. [En línea]. Available: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#~how-network-%20security-works.

[3] «Escuela Europea de Excelencia,» 2023. [En línea]. Available: https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/.

[4] W. Stallings, Comunicaciones y Redes de Computadores, 7th ed., PEARSON EDUCACIÓN, S.A., 2004, p. 724.

[5] «ITU Publications,» 2022. [En línea]. Available: https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.

[6] New Era Technology, «Converge Tech Media,» 2022. [En línea]. Available: https://convergetechmedia.com/importance-security-audits-assessments/.

[7] «Study CCNA,» 2022. [En línea]. Available: https://study-ccna.com/what-is-a-network.

[8] «Techopedia Network Infrastructure,» 2022. [En línea]. Available: https://www.techopedia.com/definition/16955/network-infrastructure.

[9] «IT Governance,» 2022. [En línea]. Available: https://www.itgovernance.co.uk/ethical-hacking.

[10] «Core,» 2022. [En línea]. Available: https://core.ac.uk/download/pdf/230932015.pdf.

[11] CIS, «CIS Lista de controles,» 2023. [En línea]. Available: https://www.cisecurity.org/controls/cis-controls-navigator.

[12] CSRC, «CSRC NIST Definición de seguridad,» 2022. [En línea]. Available: https://csrc.nist.gov/glossary/term/security.

[13] RAE, «Definición de informático,» 2022. [En línea]. Available: https://dle.rae.es/inform%C3%A1tico#LY8zQy3.

[14] CSRC, «CSRC NIST Definición de seguridad de la información,» 2022. [En línea]. Available: https://csrc.nist.gov/glossary/term/information_security#:~:text=NIST%20SP%20800-209,confidentiality%2C%20integrity%2C%20and%20availability.

[15] NIST, «CIA triad,» 2022. [En línea]. Available: https://www.nist.gov/image/cia-triad.

[16] CSRC, «CSRC NIST Definición de confidencialidad,» 2022. [En línea]. Available: https://csrc.nist.gov/glossary/term/confidentiality.

[17] (ISC)², 2022. [En línea]. Available: https://learn.isc2.org/d2l/le/enhancedSequenceViewer/9541?url=https%3A%2F%2Fbabe4806-440f-4af0-91ac-9d7c60651b42.sequences.api.brightspace.com%2F9541%2Factivity%2F403477%3FilterOnDatesAndDepth%3D1.

[18] CSRC, «CSRC NIST Definición de integridad,» 2022. [En línea]. Available: https://csrc.nist.gov/glossary/term/integrity.

[19] CSRC, «CSRC NIST Definición de disponibilidad,» 2022. [En línea]. Available: https://csrc.nist.gov/glossary/term/availability.

[20] NIST, «NIST SP 800-60 Vol. 1, Rev. 1 Criticidad,» 2022. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.

[21] CSRC, «CSRC NIST Definición de vulnerabilidad,» 2022. [En línea]. Available: https://csrc.nist.gov/glossary/term/vulnerability.

[22] NIST, «NIST SP 800-30 Rev 1 Definición de apoyo a vulnerabilidad,» 2022. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[23] «Techopedia,» 2022. [En línea]. Available: https://www.techopedia.com/7/32126/it-business/it-management/how-is-it-infrastructure-different-from-network-infrastructure.

[24] C. NIST, «CSRC NIST Definición de prueba,» 2022. [En línea]. Available: https://csrc.nist.gov/glossary/term/test.

[25] R. Das, «Infosecinstitute Tipos de pen testing 1,» 2022. [En línea]. Available: https://resources.infosecinstitute.com/topic/the-types-of-penetration-testing/.

[26] Reciprocity, «Reciprocity Tipos de pen testing 2,» 2022. [En línea]. Available: https://reciprocity.com/resources/different-types-of-penetration-testing/.

[27] The Redscan Team, «Redscan Tipos de pen testing 3,» 2022. [En línea]. Available: https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/.

[28] «EC-Council,» 2022. [En línea]. Available: https://www.eccouncil.org/ethical-hacking/.

[29] EC-Council, «EC-Council Fases de ethical hacking,» 2022. [En línea]. Available: https://www.eccouncil.org/ancillary-what-is-ethical-hacking/.

[30] M. Chapple y D. Seidl, CompTIA PenTest+ Study Guide 2nd Edition, 2022.

[31] «Untrustednetwork,» 2022. [En línea]. Available: https://untrustednetwork.net/files/issaf0.2.1.pdf.

[32] EPN, «EPN,» 2023. [En línea]. Available: https://www.epn.edu.ec/ingenieria-de-sistemas/.

[33] EPN, «EPN Organigrama,» 2022. [En línea]. Available: https://www.epn.edu.ec/wp-content/uploads/2010/10/ORGANIGRAMA-768x697.jpg.

[34] Microsoft, «Windows 11,» 2023. [En línea]. Available: https://www.microsoft.com/en-us/windows/windows-11?r=1.

[35] Brave, «Brave Browser,» 2023. [En línea]. Available: https://brave.com/.

[36] «Wappalyzer,» 2022. [En línea]. Available: https://chrome.google.com/webstore/detail/wappalyzer-technology-pro/gppongmhjkpfnbhagpmjfkannfbllamg.

[37] W. Recon, «Pentest tools,» 2023. [En línea]. Available: https://pentest-tools.com/.

[38] Google, «Google,» 2023. [En línea]. Available: https://www.google.com/.

[39] Exploit-DB, «Exploit-DB,» 2023. [En línea]. Available: https://www.exploit-db.com/google-hacking-database.

[40] W. Archive, «Wayback Machine,» 2023. [En línea]. Available: https://web.archive.org/.

[41] I. I. Hacked, «Is It Hacked,» 2023. [En línea]. Available: www.isithacked.com.

[42] Meta, «Facebook,» 2023. [En línea]. Available: https://www.facebook.com/ .

[43] Twitter, «Twitter,» 2023. [En línea]. Available: https://twitter.com/.

[44] F. FIS, «Perfil de la FIS en Facebook,» 2023. [En línea]. Available: https://www.facebook.com/fisepn.

[45] T. FIS, «Perfil de la FIS en Twitter,» 2023. [En línea]. Available: https://twitter.com/FIS_EPN.

[46] C. f. I. Security, «Center for Internet Security,» 2023. [En línea]. Available: https://www.cisecurity.org/.

[47] CIS, «CIS Politicas de contrasenas,» 2023. [En línea]. Available: https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide.

[48] Netscaler, «VPN Netscaler,» 2023. [En línea]. Available: https://docs.netscaler.com/en-us/citrix-gateway.html.

[49] N. Org, «Nmap,» 2023. [En línea]. Available: https://nmap.org/.

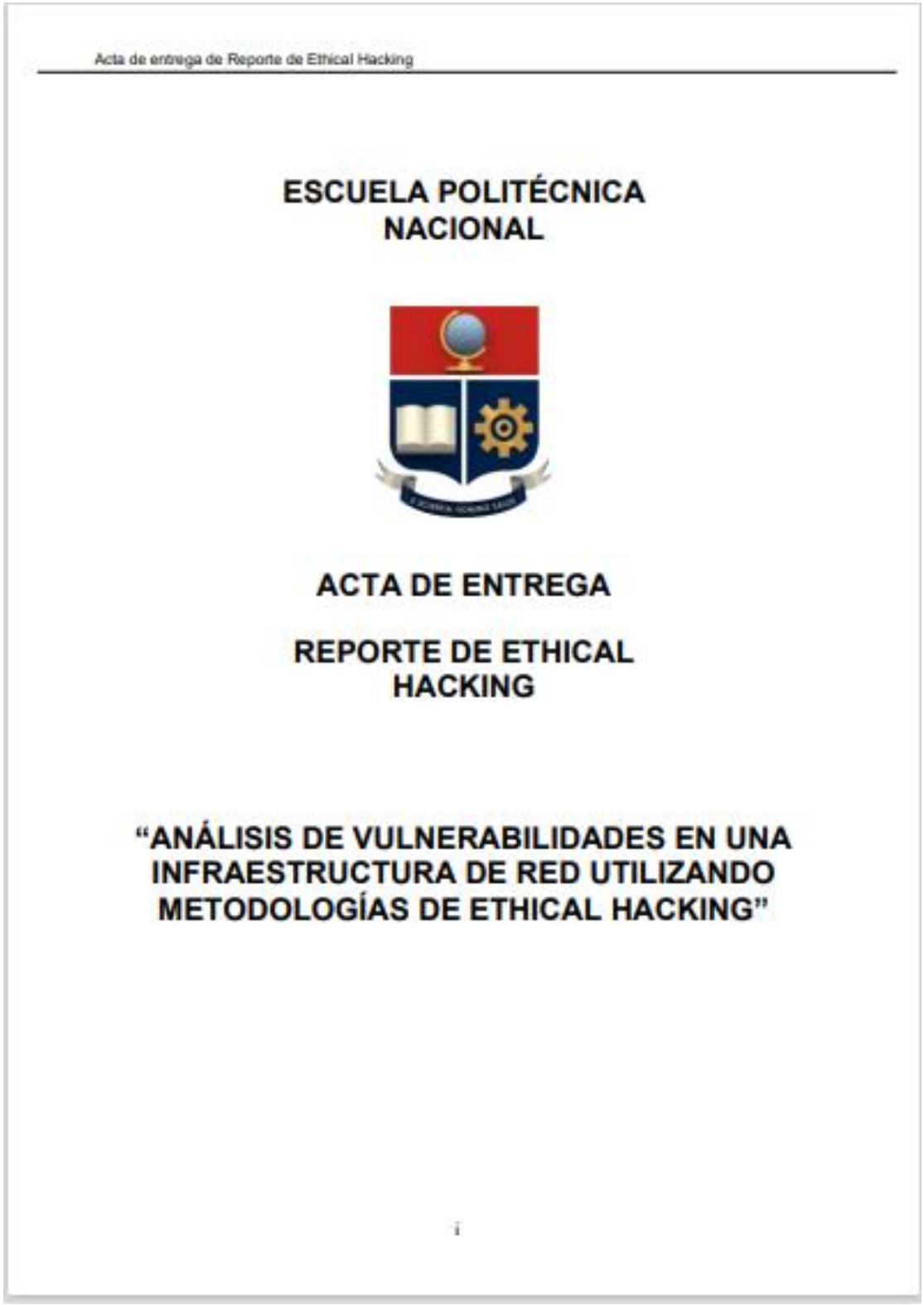
[50] VMware, «VMware,» 2023. [En línea]. Available: https://www.vmware.com/.

[51] Citrix, «Citrix,» 2023. [En línea]. Available: https://www.citrix.com/.

[52] Kasperski, «Kasperski,» 2023. [En línea]. Available: https://www.kaspersky.es/standard.

ANEXOS

Anexo I – Acta de entrega del reporte de ethical hacking.



Acta de entrega de Reporte de Ethical Hacking

ESCUELA POLITÉCNICA NACIONAL

ACTA DE ENTREGA

REPORTE DE ETHICAL HACKING

"ANÁLISIS DE VULNERABILIDADES EN UNA INFRAESTRUCTURA DE RED UTILIZANDO METODOLOGÍAS DE ETHICAL HACKING"

i

ACTA DE ENTREGA
REPORTE DE ETHICAL HACKING

Richard Miranda
richard.miranda@epn.edu.ec

Quito, septiembre 2023

A través de la presente yo, Richard Miranda, egresado de la carrera de Ingeniería en Sistemas Informáticos y de Computación hago entrega oficial del reporte de *ethical hacking* aplicado sobre la infraestructura de red de la FIS EPN.

La información contenida en el reporte ha sido certificada por ambas partes. Por ello, por parte de la FIS EPN se afirma que hay pleno consentimiento de la entrega y esta corresponde a lo tratado en el acuerdo de no divulgación.

Entrega:

Ejecutor del análisis
Nombre: Richard Miranda
CI: 1750297978

Recibe:

Responsable de Infraestructura FIS

Equipo de TI de la FIS