UNIVERSIDAD TÉCNICA DE AMBATO

MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES

COHORTE 2021

Tema: DETECCIÓN DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN A LA RED DE SERVIDORES Y SERVICIOS DEL INSTITUTO SUPERIOR TECNOLÓGICO SUCRE

Trabajo de Titulación, previo a la obtención del grado académico de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de Investigación Aplicada

Autora: Ingeniera María Elizabeth Cedeño Zambrano

Director: Ingeniero Oscar Fernando Ibarra Torres Magister.

Ambato – Ecuador

2022

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Héctor Fernando Gómez Alvarado. PhD, e integrado por los señores: *Ingeniero Leonardo David Torres Valverde Magister; Ingeniero Marcos Raphael Benítez Aldas Magíster,* designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: *"Detección de vulnerabilidades mediante pruebas de penetración a la red de servidores y servicios del Instituto Superior Tecnológico Sucre"* elaborado y presentado por la señora *Ingeniera María Elizabeth Cedeño Zambrano,* para optar por el Grado Académico de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Héctor Fernando Gómez Alvarado. PhD.
Presidente y Miembro del Tribunal

Ing. Leonardo David Torres Valverde. Mg.
Miembro del Tribunal

Ing. Marcos Raphael Benítez Aldas, Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Detección de vulnerabilidades mediante pruebas de penetración a la red de servidores y servicios del Instituto Superior Tecnológico Sucre, le corresponde exclusivamente a: Ingeniera María Elizabeth Cedeño Zambrano, Autora bajo la Dirección del Ingeniero Oscar Fernando Ibarra Torres, Magister, Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniera María Elizabeth Cedeño Zambrano
c.c.: 1714712971
AUTORA

Ingeniero Oscar Fernando Ibarra Torres Magister.
c.c.: 1804003497
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniera María Elizabeth Cedeño Zambrano
c.c.: 1714712971

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

Agradezco a la Universidad Técnica de Ambato y al personal docente por darme las herramientas que necesitaba para cumplir mi propósito.

A mi tutor, Mg. Fernando Ibarra, por su apoyo y guía constante, mismos que me permitieron alcanzar esta meta.

A mis compañeros de aula (Juan Mecánico) que en el camino de la maestría se convirtieron en un apoyo a pesar de la distancia, lo cual permitió que creciera entre nosotros una camaradería que hoy me permite llamarlos amigos.

A la CCDH, que más que compañeros son amigos, por todo el apoyo brindado de principio a fin.

De manera especial al Instituto Superior Tecnológico Sucre por permitirme desarrollar este trabajo.

Ma. Elizabeth Cedeño

DEDICATORIA

Dedico este trabajo a Dios, a la Virgencita de Guadalupe y al Divino Niño por ser la luz que guía mi camino y por permitirme cumplir esta meta, a mis hijos Daniela y Jesús Velasco Cedeño que son mi razón de ser, a mi padre Lorenzo Cedeño que, aunque ahora está al lado del creador sigue motivándome para ser siempre mejor que ayer, a mi madre Nancy Zambrano por su apoyo incondicional y constante, y a mis hermanos Danilo y Eliana Cedeño Zambrano que sin importar las circunstancias siempre han estado a mi lado apoyándome.

Ma. Elizabeth Cedeño

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

TEMA:

DETECCIÓN DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN A LA RED DE SERVIDORES Y SERVICIOS DEL INSTITUTO SUPERIOR TECNOLÓGICO SUCRE

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente de Investigación Aplicada*

AUTORA: *Ingeniera María Elizabeth Cedeño Zambrano*

DIRECTOR: *Ingeniero Oscar Fernando Ibarra Torres Magister*

FECHA: *Quince de noviembre de dos mil veintidós*

RESUMEN EJECUTIVO

Hoy en día la seguridad informática es un punto clave para todas las organizaciones tanto públicas como privadas, sin importar su giro de negocio, es así que, el Instituto Superior Tecnológico Sucre desea brindar a su personal administrativo, docente y estudiantil una infraestructura tecnológica de calidad y eficiente, pero sobre todo segura, por lo cual, el presente trabajo investigativo busca desarrollar un plan de mejoras que permita mitigar las vulnerabilidades identificadas mediante la ejecución de pruebas de penetración en la red de servidores y servicios del Instituto.

Para desarrollar el presente trabajo se utilizó la metodología de investigación cualitativa con un enfoque exploratorio, empleando además una investigación de campo mediante la realización de entrevistas, la observación, listas de cotejo y la ejecución de pruebas de penetración externas de caja negra sobre la red de servidores y servicios del Instituto Superior Tecnológico Sucre.

Las pruebas de penetración se las realizó siguiendo un proceso de fases, tal es el caso, que en primer lugar se ejecutó una fase de reconocimiento y recopilación de

información a través del uso de herramientas para analizar el dominio, pagina web y direcciones IP proporcionadas por el Instituto, para posteriormente realizar una fase de análisis para detectar y obtener las vulnerabilidades que afectan dichas aplicaciones y servicios, lo cual permitió además conocer el nivel de criticidad de cada vulnerabilidad; con estos datos se pudo ejecutar la fase de explotación de las vulnerabilidades críticas que afectan a dichos servicios.

Con la ejecución adecuada de las pruebas de penetración se logró detectar de forma eficiente las vulnerabilidades que afectan a la red de servidores y servicios del Instituto Superior Tecnológico Sucre, lo cual, permitió además, desarrollar un plan de mejora que contiene las recomendaciones de las acciones que el Instituto Superior Tecnológico Sucre debe implementar para mitigar las vulnerabilidades que afectan a su red y así minimizar los riesgos a los que su infraestructura se encuentra expuesta, garantizando así cumplir con lo dispuesto en la Norma ISO 27001 en cuanto a asegurar en todo momento la integridad, disponibilidad y confidencialidad de la información.

DESCRIPTORES: *CIBERSEGURIDAD, HACKING ÉTICO, INTRUSOS, INTRUSIÓN, PENETRACIÓN, PENTESTING, PRUEBAS, SEGURIDAD INFORMÁTICA, TEST DE INTRUSIÓN, VULNERABILIDADES.*

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA ACADÉMICA (MA) CON TRAYECTORIA PROFESIONAL (TP) EN MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

THEME:

DETECTION OF VULNERABILITIES THROUGH PENETRATION TESTS TO THE NETWORK OF SERVERS AND SERVICES OF SUCRE HIGHER TECHNOLOGICAL INSTITUTE

DEGREE MODALITY: *Degree Project with an applied research component*
AUTHOR: *Engineer Maria Elizabeth Cedeño Zambrano*
DIRECTED BY: *Engineer Oscar Fernando Ibarra Torres, Master*
DATE: *November fifteenth, two thousand and twenty-two*

EXECUTIVE SUMMARY

Nowadays, computer security is a key point for all organizations, both public and private, regardless of their line of business. Thus, Sucre Higher Institute of Technology wants to provide its administrative, teaching and student staff with a quality and efficient technological infrastructure, but above all safe, so this research work seeks to develop an improvement plan to mitigate the vulnerabilities identified through the execution of penetration tests on the network of servers and services of the Institute.

In order to develop the present work, the qualitative research methodology was used with an exploratory approach, using also a field research through interviews, observation, checklists and the execution of external black box penetration tests on the network of servers and services of Sucre Higher Institute of Technology.

The penetration tests were carried out following a process of phases, such is the case, that in the first place a phase of recognition and collection of information was executed through the use of tools to analyze the domain, web page and IP addresses provided by the Institute, to subsequently perform an analysis phase to detect and obtain the vulnerabilities that affect these applications and services, which also allowed to know

the level of criticality of each vulnerability; with this data it was possible to execute the phase of exploitation of the critical vulnerabilities that affect these services.

With the proper execution of the penetration tests it was possible to efficiently detect the vulnerabilities affecting the network of servers and services of Sucre Higher Institute of Technology, which also allowed the development of an improvement plan containing the recommendations of the actions that Sucre Higher Institute of Technology should implement to mitigate the vulnerabilities affecting its network and thus minimize the risks to which its infrastructure is exposed, thus guaranteeing compliance with the provisions of ISO 27001 in terms of ensuring the integrity, availability and confidentiality of the information at all times.

KEYWORDS: *COMPUTER SECURITY, CYBERSECURITY, ETHICAL HACKING, INTRUDERS, INTRUSION, PENETRATION, PENETRATION TESTING, PENTESTING, TESTING, VULNERABILITIES.*

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1. Introducción

En la actualidad las TIC han permitido mejorar tiempo y recursos en las empresas, es así que, el acceso a la red ha permitido que los usuarios realicen las tareas dispuestas por los jefes de una manera eficiente y de forma remota, en una modalidad conocida como teletrabajo, lo cual le permite a los usuarios poder acceder a los recursos, sistemas y servicios que dispone la organización a través del Internet sin necesidad de salir de su hogar (Cifuentes-Leiton & Londoño-Cardozo, 2020). Es por esto que los sistemas informáticos, los equipos de computación y la información generada por las instituciones en general, son sumamente importantes para la continuidad de su negocio y, por lo tanto, deben ser protegidos contra personas malintencionadas que quieran vulnerar y provocar daños en este patrimonio. Un análisis adecuado de vulnerabilidades permite determinar las accione que la organización debe ejecutar para mitigar las mismas y así evitar ser víctima de un ciberataque, delitos que en la actualidad se ha vuelto muy popular y rentable para los delincuentes que se mueven en este medio (Huamantingo Navarro, 2022).

En Ecuador se cuenta con el Centro de Respuesta a Incidentes Informáticos EcuCERT de la Agencia de Regulación y Control de las Telecomunicaciones, ARCOTEL, que tiene como propósito principal el prevenir y coordinar las acciones correspondientes al tratamiento de incidentes de seguridad de la información, así mismo, apoya en la instrucción de centros de respuesta a incidentes informáticos a nivel nacional. Trabaja de forma conjunta con equipos como CERT y CSIRT a nivel nacional e internacional. De acuerdo a sus estadísticas, en diciembre de 2021 se reportaron 17.292 eventos de vulnerabilidades, de las cuales las más recurrentes fueron DNS Open Resolver, CWMP, Open TFTP, NTP Versión y Poodle SSL v3 (EcuCERT, 2022).

El presente estudio tiene como objeto desarrollar un plan de mejoras que permita mitigar las vulnerabilidades identificadas mediante la ejecución de pruebas de

penetración en la red de servidores y servicios del Instituto Superior Tecnológico Sucre.

El Instituto Superior Tecnológico Sucre es una institución pública, por lo cual, su presupuesto es asignado por el Gobierno Central a través del SENESCYT, lo que conlleva a que dicha institución no cuente con un flujo corriente que le permita adquirir de forma inmediata la infraestructura tecnológica que requiere para mejorar sus sistemas de seguridad informática y de la información, sino que, al contrario requiere levantar un proyecto tecnológico que tenga costos adecuados y además sea sostenible en el tiempo, con la finalidad de robustecer la eficiencia y la eficacia del gasto público, permitiendo a su vez optimizar la prestación de los servicios electrónicos que entrega a la ciudadanía, todo esto en cumplimiento del "*Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (Código INGENIOS – COESCCI)"* publicado en el Registro Oficial Nro. 899 de 9 de diciembre de 2016 y en concordancia con lo estipulado en la "*Norma Técnica que regula el proceso para la evaluación de viabilidad técnica de proyectos de gobierno electrónico y autorización de criticidad de software y servicios relacionados*" emitida mediante ACUERDO MINISTERIAL No. 031-2020 de 21 de octubre de 2020. Dicho proyecto deberá ser presentado ante el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), para lo cual, se debe entregar como documentación de respaldo el Perfil de proyecto, el Cuadro de componentes, los Términos de Referencia y/o las Especificaciones Técnicas y el Informe de criticidad, documentos requeridos para que el proyecto sea analizado y se verifique su viabilidad técnica dentro de los plazos establecidos por el MINTEL de acuerdo a la Figura 1 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021).

Figura 1

Evaluación de Proyectos TIC

Nota. Adaptado de *Evaluación de Proyectos TIC*, MINTEL, 2021, Fuente (https://www.gobiernoelectronico.gob.ec/asesoria-evaluacion-y-aprobacion-de-proyectos/)

En el CAPÍTULO I se plantea el problema de investigación a través de la justificación y el bosquejo de los objetivos requeridos para llevar a cabo este estudio.

En el CAPÍTULO II se aborda el estado del arte y la base científica de la seguridad de redes y pentesting.

En el CAPÍTULO III se describe el marco metodológico empleado para llevar a cabo este estudio.

En el CAPÍTULO IV se presentan los resultados de este estudio y el análisis de los mismos.

En el CAPÍTULO V se determinan las conclusiones, recomendaciones, bibliografías y anexos resultantes del presente estudio.

1.2. Justificación

Con la situación de emergencia que vivió el país, muchas instituciones se vieron en la necesidad imperiosa de llevar sus oficinas al hogar de sus colaboradores para mantener la continuidad de sus negocios, lo cual, ha conllevado a que pongan más interés en reforzar sus seguridades en la red; y en este ámbito el Instituto Superior Tecnológico Sucre desea brindar a su personal administrativo, docente y estudiantil una infraestructura tecnológica de calidad, eficiente pero sobre todo segura; lo que ha generado la necesidad de conocer las vulnerabilidades que actualmente afectan a la red de servidores y servicios de dicho IST Sucre. Para lograr este propósito se ha considerado analizar los niveles de seguridad que tienen estas redes, mediante la realización de pruebas de penetración y por medio de entrevistas al personal que se encuentra a cargo de la administración de la infraestructura tecnológica del IST Sucre, para así poder plantear un plan de mejora que permita mitigar la penetración de intrusos en dicha red, consiguiendo a su vez garantizar la integridad, disponibilidad y confidencialidad de la información. Todo esto debe ir enfocado en una correcta selección de las normas, estándares y/o manuales aplicables que permitan alcanzar los intereses institucionales.

1.3.Objetivos

1.3.1. General

Desarrollar un plan de mejoras que permita mitigar vulnerabilidades identificadas mediante la ejecución de pruebas de penetración en la red de servidores y servicios del Instituto Superior Tecnológico Sucre.

1.3.2. Específicos

a. Investigar el estado del arte de la seguridad de redes y pentesting basado en las normativas, estándares, manuales y procedimientos vigentes.
b. Identificar las vulnerabilidades que tiene la red de servidores y servicios del Instituto Superior Tecnológico Sucre.

c. Ejecutar pruebas de penetración en la red de servidores y servicios del Instituto Superior Tecnológico Sucre en base a las vulnerabilidades encontradas.
d. Analizar las mejores opciones de solución a las vulnerabilidades encontradas, para poder establecer el plan de mejoras.

CAPÍTULO II
ANTECEDENTES INVESTIGATIVOS

2.1.Estado del arte

Es fundamental detectar de forma oportuna las vulnerabilidades que tenga una red en particular, por lo cual, la realización de pruebas de penetración desde una red externa y el posterior análisis de las vulnerabilidades encontradas es la base para que una organización tome conciencia de su estado real en cuanto a seguridad de la información se trata (Briceño, 2021).

La realización del proceso de investigación conlleva un método para desarrollar de forma adecuada la auditoría, este proceso se origina con el entendimiento de la estructura de la empresa y termina con la ejecución de las mejoras recomendadas (Narvaez Taranto, 2018).

Tal como lo indican Sabillon et al. (2017) es fundamental contar con un modelo para desarrollar la auditoría de seguridad.

Se debe tener en cuenta que la implementación de una infraestructura tecnológica robusta dificulta el trabajo de un auditor al momento que desea detectar de forma eficaz las vulnerabilidades existentes en una red, por lo cual, los auditores se han visto en la necesidad de llevar a cabo acciones que le permitan conocer de forma adecuada los efectos de un evento de ciberseguridad (Rosati et al., 2022).

Es primordial que el resultado de dicha auditoría sea presentada a los altos mandos de las empresas para que conozcan las señales de alerta que existen en cuanto a la seguridad y cuáles son las vulnerabilidades con las que cuenta la infraestructura y la información que utilizan tanto sus usuarios internos como externos, y presentarle las mejoras siempre basadas en normas y estándares de buena práctica que conlleven al desarrollo del negocio de la empresa (Mahecha, 2022).

Coronel (2017) en su trabajo de investigación amparado en el Hackeo Ético realizó pruebas de penetración a las aplicaciones de una Institución de Educación Superior, ubicada en la ciudad de Guayaquil, mediante la utilización de herramientas de software libre con la finalidad de determinar las vulnerabilidades que afectan a su infraestructura tecnológica, con lo cual, concluyó que la institución presenta vulnerabilidades críticas por medio de las cuales los ciberdelincuentes lograrían afectar seriamente la confidencialidad, integridad y disponibilidad de la información de dicha institución.

Cruz et al. (2020) pudo demostrar que mediante la utilización de exploits a través de herramientas preinstaladas en Kali Linux se pueden detectar múltiples vulnerabilidades en una variedad de servicios si trabajan sobre un servidor linux, dicha información fue utilizada para aplicar medidas que le permitieron reducir los riesgos.

Paltán Orellana (2019) en su estudio por medio de la utilización de herramientas de hackeo ético pudo detectar que entre las principales vulnerabilidades que afectaban a la red inalámbrica de una entidad privada estaba que los equipos permitían el acceso no autorizado a la red que se podía perpetuar por la escucha no autorizada del tráfico a través de un MITM (hombre en el medio), esto le permitió levantar un plan de mitigación de dichas vulnerabilidades, para lo cual, se basó en algunas metodologías de buenas prácticas y en la Norma ISO/IEC 27002:2013.

Galarza García (2020) en su estudio por medio del uso de herramientas como Kali Linux y sus múltiples aplicaciones, así como, NMAP y otras herramientas web llevó a cabo un análisis de vulnerabilidades sobre el servicio WEB del Instituto Tecnológico Quito, con la finalidad de desarrollar una estrategia que le permita evaluar de forma eficiente las vulnerabilidades que afectan al sistema de notas de dicha institución. Finalmente concluyó su trabajo indicando que el sistema de notas del instituto presenta un riesgo muy alto y crítico en la etapa de explotación, lo cual, conlleva a que la seguridad de la información académica que maneja la institución se vea seriamente comprometida.

Giannone (2019) mediante la utilización de herramientas para realizar hacking ético pudo encontrar las vulnerabilidades que afectaban a una red y servicio específico, lo cual le permitió generar un método para incluir el hacking ético como un proceso a desarrollarse de manera periódica en el escaneo de vulnerabilidades de un software y así en el tiempo ir mejorando las seguridades de dicho software, este método está dividido en tres fases que son de planificación, ejecución y mantenimiento, las cuales a su vez incluyen varias etapas entre las que se encuentran la detección, la mitigación y aceptación, dependiendo del nivel de criticidad, de las vulnerabilidades que se vayan encontrando en cada prueba realizada.

2.2.Seguridad Informática

La seguridad informática es el conjunto de medidas organizacionales sean estas administrativas, técnicas o legales que se ejecutan sobre los recursos informáticos de una organización con la finalidad de minimizar los riesgos que pueden afectar a la continuidad del negocio (Zambrano & Valencia, 2017).

2.3. Seguridad de la Información

La seguridad de la información son el conjunto de medidas que implementa una organización con la finalidad de resguardar y garantizar la disponibilidad, integridad y confidencialidad de sus activos de información (ISO/IEC, 2022a).

2.4.Normativa y Estándares de Seguridad de la Información

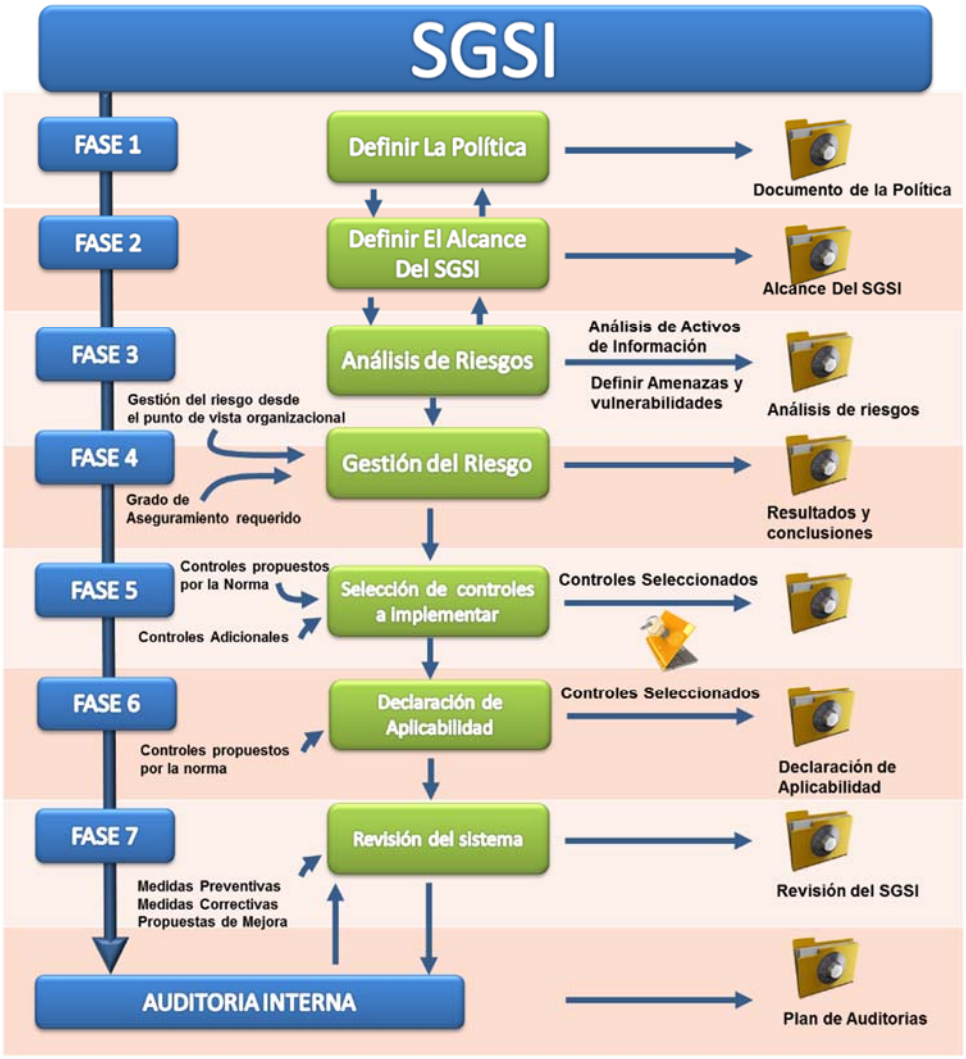
La Organización Internacional de Normalización ISO (del inglés International Organization for Standardization) y la Comisión Electrotécnica Internacional IEC (del inglés International Electrotechnical Commission) conforman el sistema especializado de normalización mundial. Los organismos que son miembros de la ISO y de la IEC, así como, otras organizaciones internacionales sean estas gubernamentales y no gubernamentales, colaboran de manera conjunta para la elaboración de las normas internacionales de determinados campos de actividad técnica (ISO & IEC, 2022).

2.4.1. ISO/IEC 27001

La norma ISO/IEC 27001 permite implementar un Sistema de Gestión de Seguridad de la Información (SGSI) con la finalidad de gestionar la seguridad de la información de una organización mediante el aseguramiento de la disponibilidad, integridad y confidencialidad de dicha información, con lo cual, se garantiza la continuidad del negocio de dicha empresa. La Norma ISO 27001 propone un esquema en fases para la implantación de un SGSI adecuado, estas fases se describen en la Figura 2. Esta Norma determina que para una buena gestión de la seguridad de la información es primordial realizar una adecuada evaluación de los riesgos, dentro de los cuales se encuentra la identificación de las vulnerabilidades o debilidades que afectan a los activos o servicios de la organización (ISO/IEC, 2022c).

Figura 2

Fases para la Implementación de un SGSI



Nota. La figura detalla las fases que propone la Norma ISO 27001 para la implementación de un SGSI. Adaptado de *Elementos o fases para la Implementación de un SGSI*, Normas ISO, 2022, Fuente (https://www.normas-iso.com/iso-27001/)

En Ecuador el Gobierno Central a través del Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL mediante el Registro Oficial Nro. 228 publicado el 10 de enero de 2020, emitió el Esquema Gubernamental de Seguridad de la Información (EGSI), el cual es de implementación obligatoria para todas las instituciones de administración pública ecuatorianas, este esquema está basado en la ISO/IEC 27001 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020a).

De igual forma el MINTEL ha proporcionado una Guía para la implementación del EGSI, misma que sirve de apoyo a las instituciones para conocer cual es el perfil que deben cumplir el Oficial de Seguridad de la Información (OSI) y las personas que conformen el Comité de Seguridad de la Información (CSI), además les permite conocer cómo pueden llegar a implementar un Sistema de Gestión de Seguridad de la Información (SGSI) adecuado y fundamentado en el ciclo de vida del modelo PDCA (planificar, hacer, verificar y actuar) (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020c).

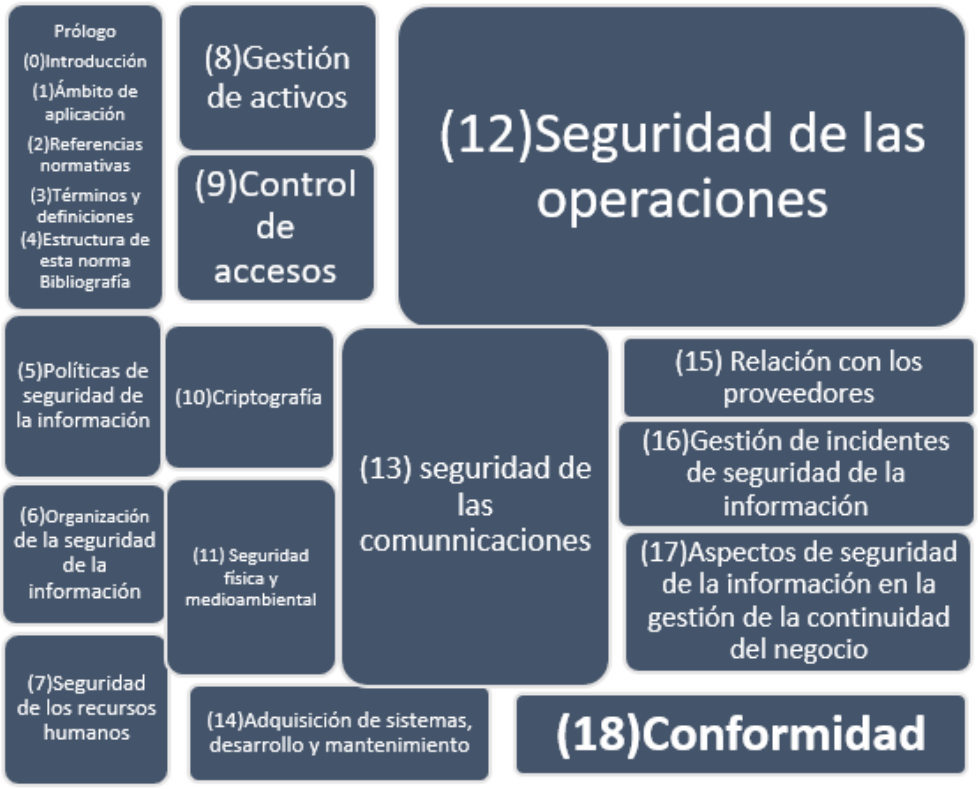
2.4.2. ISO/IEC 27002

La norma ISO/IEC 27002 es una de las normas que se derivan de la ISO/IEC 27000, esta norma es una guía que le permite a las organizaciones conocer los pasos que deben seguir para implementar de forma adecuada la seguridad de la información. Esta norma permite que las organizaciones escojan de manera libre los controles que les permitan alcanzar sus objetivos y la forma de ejecutarlos, considerando siempre la evaluación de riesgos que hayan ejecutado (Sulistyowati et al., 2020).

La norma ISO 27002:2013 comprende los objetivos de control descritos en la Figura 3.

Figura 3

Objetivos de Control Norma ISO 27002:2013



Nota. Adaptado de *Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss.*, Sulistyowati, D., Handayani, F., & Suryanto, Y., 2020, JOIV: International Journal on Informatics Visualization, 4(4), 225-230

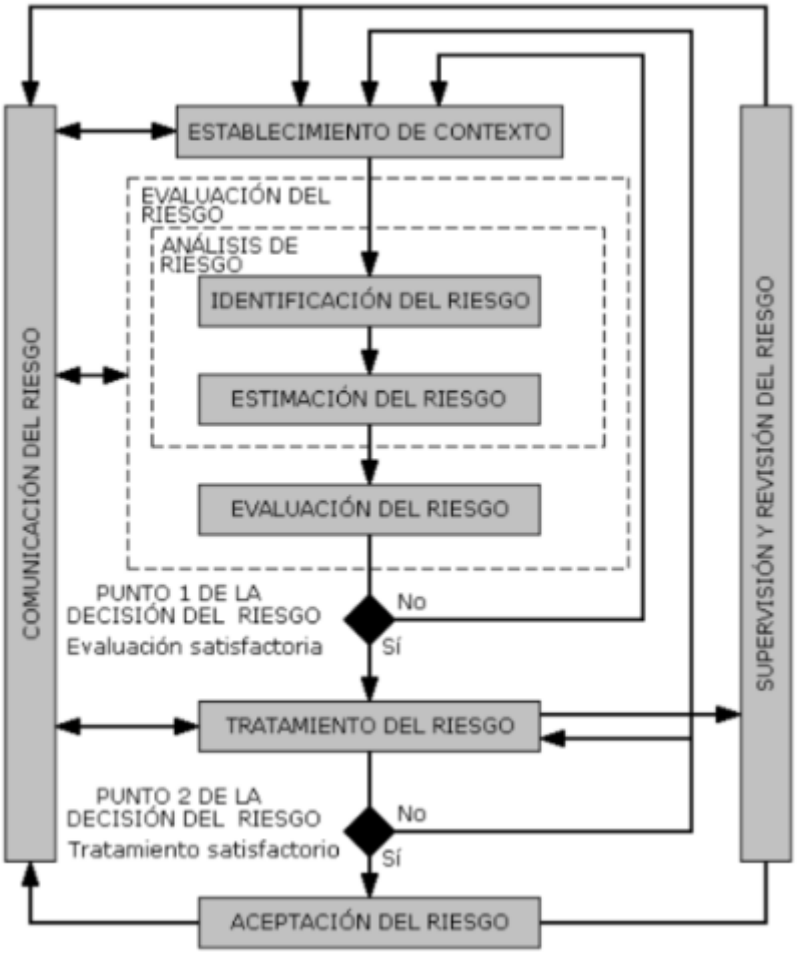
2.4.3. ISO/IEC 27005

Esta norma proporciona una guía para aplicar una gestión de riesgos sobre la seguridad de la información. Esta norma apoya en el cumplimiento del propósito de la norma ISO/IEC 27001. La gestión del riesgo se la desarrolla en siete etapas que son el reconocimiento del contexto organizacional, la evaluación del riesgo, el tratamiento del riesgo, la comunicación del riesgo, la consulta del riesgo, supervisión del riesgo y la revisión del riesgo (Taherdoost, 2022).

En Ecuador el Gobierno Central a través del Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL emitió la Guía para la Gestión de Riesgos de Seguridad de la Información, basada en la ISO 27005, esta guía es de aplicación

obligatoria para todas las instituciones ecuatorianas del sector público. Esta guía adopta el proceso de gestión del riesgo en la seguridad de la información descrito en la Figura 4.

Figura 4
Proceso de Gestión del Riesgo en la Seguridad de la Información



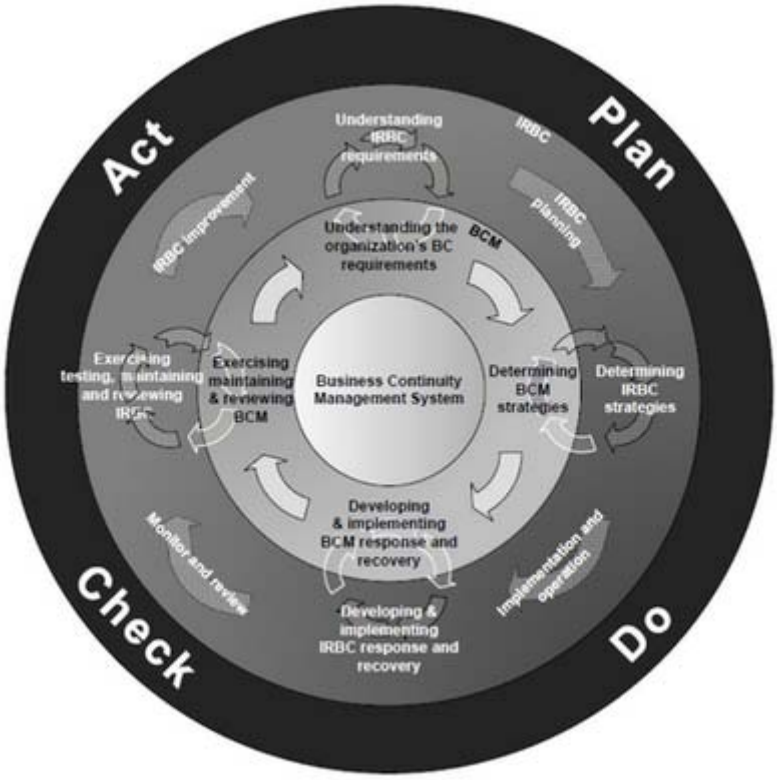
Nota. Adaptado de *GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.*, MINTEL, 2020

2.4.4. ISO/IEC 27031

La norma ISO/IEC 27031 detalla los procesos que una institución sea pública o privada, grande o pequeña, deben seguir para desarrollar e implementar las tecnologías de la información y la comunicación (TIC del inglés Information and Communication Technology (ICT)) permitiéndole garantizar la continuidad del negocio, por lo cual, es

un marco de referencia en la preparación de las TIC para la continuidad del negocio IRBC (del inglés ICT Readiness for Business Continuity), con lo cual podrá generar un sistema de gestión de la continuidad del negocio BCMS (del inglés Business Continuity Management System); la integración de ambos procesos se encuentra descrita en la Figura 5. Actualmente esta norma se encuentra en la versión 2011 (ISO/IEC, 2022b).

Figura 5
Integracion de un IRBC con un BCMS



Nota. Adaptado de *ISO/IEC 27031*, ISO/IEC, 2022

2.4.5. ISO/IEC 15408-1

La norma ISO/IEC 15408-1 Tecnología de la información - Técnicas de seguridad - Criterios de evaluación de la seguridad informática - Parte 1: Introducción y modelo general, está enfocada y define la conceptualización y las nociones generales para evaluar la seguridad de las tecnologías de la información, además determina la guía de evaluación. Actualmente se encuentra en revisión la versión ISO/IEC 15408-1:2022 (ISO, 2022).

2.4.6. ISO 31000

Esta norma es una guía que brinda las directrices para una correcta gestión del riesgo, para que la implementación de esta norma de resultados favorables, la misma se debe aplicar en todas las áreas y procesos de la organización, independientemente de su giro de negocio, por lo cual, para asegurar una correcta aplicación de esta norma se requiere un involucramiento y compromiso total por parte de la alta gerencia. El marco de referencia debe ejecutarse cumpliendo los componentes descritos en la Figura 6 (ISO, 2018).

Figura 6
Componentes del Marco de Referencia ISO 31000

Nota. Adaptado de *ISO 31000:2018(es) Gestión del riesgo — Directrices,* ISO, 2018

2.5.Normativa Ecuatoriana de Seguridad de la Información

En Ecuador se ha adoptado las normas y estándares ISO/IEC a través de las normas técnicas descritas en la Tabla 1 (Servicio Ecuatoriano de Normalización, 2022).

Tabla 1
Normas Técnicas Ecuatorianas

Norma Ecuatoriana	Año	Norma ISO/IEC
NTE INEN-ISO/IEC 27031	2010	ISO/IEC 27031:2011
NTE INEN-ISO/IEC 27005:2012	2012	ISO/IEC 27005:2008
NTE INEN-ISO/IEC 15408-1	2014	ISO/IEC 15408-1:2009
NTE INEN-ISO 31000	2014	ISO 31000:2009
NTE INEN-ISO/IEC 27000	2016	ISO/IEC 27000:2016
NTE INEN-ISO/IEC 27001	2017	ISO/IEC 27001:2013+Cor.1:2014+Cor. 2:2015
NTE INEN-ISO/IEC 27002	2017	ISO/IEC 27002:2013+Cor.1:2014+Cor.2:2015

Fuente: Elaboración propia

2.6.Otros Marcos de Referencia de Seguridad de la Información

2.6.1. COBIT

Los Objetivos de Control para la Información y Tecnologías Relacionadas COBIT (del inglés Control Objectives for Information and Related Technology) fueron desarrollados por la Asociación de Auditoría y Control de Sistemas de Información ISACA (del inglés Information Systems Audit and Control Association), que está conformada por profesionales en las áreas de auditoría, riesgo y gobierno de tecnologías de la información. Aun cuando COBIT fue levantado en un principio como apoyo en la auditoría financiera, actualmente se considera un marco referente para el gobierno de tecnologías de la información.

La versión actual 2019 contiene 40 objetivos de gobierno y gestión, los cuales, a su vez contienen sus propios objetivos específicos que le permiten a las organizaciones alinear sus propios objetivos a este marco de referencia (De Haes et al., 2020).

2.6.2. ITIL v4

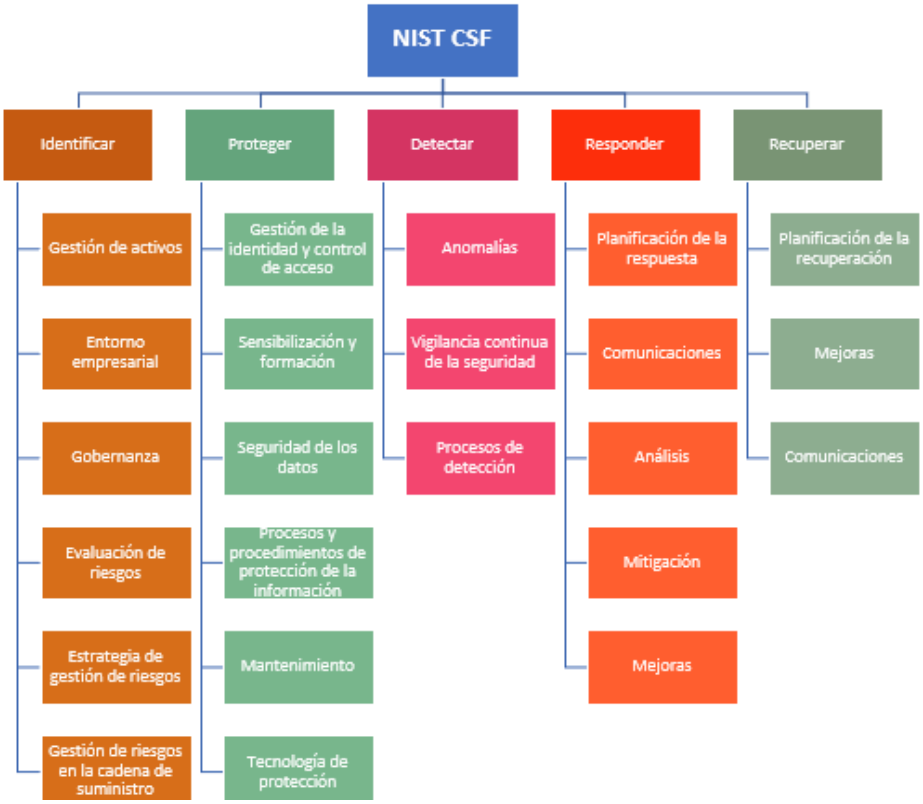
La Biblioteca de Infraestructura de Tecnologías de Información ITIL (del inglés Information Technology Infrastructure Library) es un maro de referencia de buenas prácticas para la administración de servicios de tecnologías de la información. Actualmente este marco de referencia se encuentra en la versión 4, misma que contiene 34 prácticas, de las cuales 14 corresponden al tema Prácticas de gestión general, 17 pertenecen al tema Prácticas de gestión del servicio y 3 corresponden al tema Prácticas de gestión técnica (Chergui & Chakir, 2020).

2.6.3. NIST CSF

El Marco de Ciberseguridad del NIST (del inglés NIST Cybersecurity Framework) es la recopilación de las mejores prácticas de diversos organismos de normalización, cuya eficacia ha quedado demostrada en el momento de su aplicación, además este Marco de referencia ofrece muchos beneficios a nivel normativo y jurídico para las organizaciones del sector privado que lo acojan como referencia. La Figura 7 detalla las funciones y categorías que estipula este Marco de referencia (Roy, 2020).

Figura 7

Funciones y categorías NIST CSF



Nota. Adaptado de *Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss.*, Sulistyowati, D., Handayani, F., & Suryanto, Y., 2020, JOIV: International Journal on Informatics Visualization, 4(4), 225-230

2.7.Hacker

Es una persona con una gran experiencia en seguridad informática que busca infiltrarse en los sistemas y servicios de una organización vulnerando sus seguridades.

2.7.1. Tipos de Hackers

En la actualidad existe una gran variedad de tipos de hackers, sin embargo, los más comunes y conocidos son los hackers de sombrero negro, sombrero blanco y sombrero gris.

Hackers de Sombrero Negro. Los hackers de sombrero negro son las personas que realizan intrusiones o vulneran las seguridades de una organización solo por sacar un beneficio propio muchas veces económico.

Hackers de Sombrero Blanco. Los hackers de sombrero blanco son también conocidos como hackers éticos ya que actúan solo con la única intención de encontrar vulnerabilidades para reforzar los sistemas de la organización para la que trabajan.

Hackers de Sombrero Gris. Los hackers de sombrero gris no tienen malas intenciones, aunque actúan de manera ilegal para infiltrarse en la red o servicios de una organización, lo hacen para descubrir las vulnerabilidades que afectan a dichos sistemas con la intención de comunicar a dicha organización estas vulnerabilidades. Se puede decir que este tipo de hacker es una mezcla entre los hackers de sombrero negro y blanco (Harper et al., 2022).

2.8.Hacking Ético y Pentesting

2.8.1. Bug

Es una propiedad no deseada de un sistema informático que puede generar vulnerabilidades en los sistemas.

2.8.2. Sistema de Detección de Intrusiones

Un sistema de detección de intrusos IDS permite identificar el tráfico malicioso y el tráfico inofensivo que atraviesa una red, mientras que un sistema de prevención de intrusos IPS puede bloquear el tráfico malicioso o permitir el tráfico inofensivo (Asad & Gashi, 2022).

2.8.3. Hacking Ético

También conocido como pruebas de penetración, es básicamente una auditoría realizada por personal experto en seguridad de la información, que consiste en la

ejecución de una serie de pruebas rigurosas sobre una red o servicios, con la finalidad de detectar vulnerabilidades en los sistemas y servicios de la empresa, para evitar a futuro la fuga de información que ponga en riesgo y comprometa la integridad de la empresa (P. Kim, 2018).

2.8.4. Enfoques de Pruebas de Penetración

Las pruebas que se utilizan para detectar vulnerabilidades en las aplicaciones, redes y dispositivos de una empresa son fundamentales para mantener la seguridad a nivel de Internet. Independientemente de quien realice estas pruebas (fabricantes, empresas consultoras, equipos de seguridad de las empresas, investigadores de seguridad) el alcance variará en base a la información que obtienen quienes realizan dichas pruebas (Guzman & Gupta, 2017).

2.8.5. Tipos de Pentesting

Test Intrusivo Externo. También conocido como test de caja negra, se enfoca en determinar el nivel de seguridad de la red externa de una empresa. En este escenario el pentester se convierte en un atacante externo, para obtener acceso a la información sensible comprometiendo la privacidad de la empresa.

Test Intrusivo Interno. Conocido también como test de caja blanca o caja gris dependiendo de los niveles de permisos que se tengan. Este método busca determinar el nivel de la seguridad del entorno privado de la empresa. Aquí el pentester simula ser un atacante que dispone de acceso a la red interna de la empresa (Grant, 2019).

2.8.6. Etapas o Fases del Pentesting

Recopilación o Recolección de Información. El pentester se dedica a buscar la información del cliente que sea pública y que esté disponible, con lo cual, se enfocará en identificar las formas que le permitan conectarse a la red y sistemas de la empresa.

Análisis de Vulnerabilidades. El pentester intentará conocer las vulnerabilidades de los sistemas que pueden ser aprovechadas en la fase de explotación, mediante la ejecución de acciones que puedan comprometer la seguridad de dichos sistemas.

Explotación. En esta fase se explotan las vulnerabilidades encontradas en la fase anterior a través del uso de técnicas o acciones, así como, el uso de los usuarios y contraseñas que se hayan podido descubrir con la finalidad de vulnerar y acceder a la red interna de la víctima. Aun cuando se haya detectado una vulnerabilidad, en el momento de realizar la etapa de explotación se puede dar el caso de que dicha vulnerabilidad no pueda ser explotada debido a que pueden existir otras seguridades implementadas en el sistema, las cuales pueden evitar que se realice de manera satisfactoria el proceso completo de la etapa de explotación.

Informe. En la última etapa el pentester plasmará en un informe ejecutivo las vulnerabilidades encontradas, los pasos y acciones ejecutados, así como, las recomendaciones que le permitan a la víctima tomar las acciones correctivas para mitigar las vulnerabilidades encontradas, este informe será presentado tanto a la alta gerencia como al personal técnico que administra los servicios y la red (Gutierrez, 2018).

2.9.Herramientas Para Pruebas de Penetración (Pentesting)

Son múltiples las herramientas que existen en el mercado para realizar las pruebas de penetración en todas sus fases contribuyendo a obtener los mejores resultados posibles, es así que dentro de la gran variedad que existe en el mercado de estas herramientas, se han considerado las siguientes de las cuales la mayoría se maneja sobre software libre.

2.9.1. Gobuster

Gobuster es una herramienta desarrollada para las pruebas de penetración con fuerza bruta, lo cual permite extraer información de las páginas web y dominios, como son

los directorios y archivos que se encuentran alojados en dicha página, además de obtener los subdominios, nombres de hosts de los servidores, entre otros (GitHub, 2022a).

2.9.2. Httpmethods

Es un script que permite a través de fuerza bruta conocer cuáles métodos de HTTP están habilitados en una página web y así conocer cómo atacar de mejor manera dicha página (GitHub, 2022b).

2.9.3. IPAddress.com

IPAddress.com es una herramienta en línea que permite realizar consultas sobre un dominio o una IP, para conocer de manera rápida y eficaz los datos de propietario de dominio, localización de IP, datos de contacto, entre otros (IPAddress.com, 2022).

2.9.4. Kali Linux

Kali Linux es una distribución de Linux de código abierto basada en Debian para una variedad de tareas de seguridad de la información, como pruebas de intrusión, investigación de seguridad, análisis forense informático e ingeniería inversa. Por esta razón, se considera la herramienta más avanzada para la distribución de pruebas de penetración (Najera-Gutierrez, 2019).

2.9.5. Maltego

Maltego es una herramienta de análisis gráfico de páginas web que permite extraer los datos de dicha página en el instante, presentando dicha información a manera de gráficos de fácil visualización (Harper et al., 2022).

2.9.6. Metasploit Framework

Es un framework de software libre que es muy utilizado para realizar la explotación de las vulnerabilidades encontradas en sistemas operativos, sitios web, aplicaciones, entre otras. Se basa en la ejecución de una secuencia de comandos llamados exploits que el atacante utiliza para realizar la intrusión de las vulnerabilidades que afectan a una organización y así poder obtener información sensible de la misma (Najera-Gutierrez, 2019).

2.9.7. Nessus

Nessus es una de las herramientas más utilizadas para la evaluación de vulnerabilidades, que permite conocer los problemas críticos que pueden afectar a una organización. Esta herramienta se puede implementar en diversas plataformas, e incluso se puede usar esta herramienta de forma portátil. Contiene alrededor de 450 plantillas preconfiguradas que permiten encontrar las vulnerabilidades, y permite realizar configuraciones personalizadas para la elaboración de informes de acuerdo a las necesidades del usuario. Dentro de sus opciones se encuentra Nessus Essentials que permite escanear hasta 16 direcciones IP por escáner, permitiendo realizar evaluaciones a profundidad (Tenable, 2022a).

Esta herramienta utiliza cinco (5) niveles de severidad para catalogar los tipos de vulnerabilidades encontrados, estos niveles se describen en la Figura 8.

Figura 8

Índices de Gravedad

Rating	Description	Example
Critical	Information explaining that the scan may have impacted the web application's availability or integrity. The scan note title appears in red.	**Service Stopped Responding** – The scanner aborted the scan after encountering too many consecutive request timeouts. The scan results may be incomplete, and you should verify that the target is not corrupted or unavailable. Tenable recommends that you investigate the repeated timeouts to determine why the target cannot support the requests the scanner sent. You may need to decrease performance configurations in the scan template.
High	Information explaining that the scan stopped unexpectedly before the scanner finished analyzing the web application targets. As a result, the scan did not sufficiently analyze the web application for vulnerabilities, and the user should troubleshoot and re-attempt the scan. The scan note title appears in yellow.	**Scan Crashed** – The scan crashed for an unexpected reason. As a result, the scan results are be missing or incomplete.
Medium	Information explaining why scan results are missing or incomplete. The findings usually concern scans that could not be started due to configuration errors. The web application is not impacted. The scan note title appears in black and white.	**Out of Scope URL** – The scanner did not scan the target URL because it matches one of the scope exclusion criteria specified in the scan template settings.
Low	Information explaining variations in scan duration. The findings do not impact the web application or scan results. The scan note title appears in green.	**Target Response Has Been Truncated** – The target scan results exceeded the **Max Response Size** specified in the scan configurations. As a result, the content is truncated, which could cause data collection and assessment errors.
Info	Information that does not impact the scan results, but that can help you configure your scan settings more efficiently. The scan note title appears in blue.	**Authentication Detected** – The scanner detected an HTTP server authentication or login form. You can configure your credentials to allow the scanner to access more pages.

Nota. La figura detalla los niveles de severidad con los que Nessus cataloga las vulnerabilidades encontradas. Adaptado de *Tenable.io User Guide - Scan Notes Severity Details in WAS,* Tenable.io, 2022, Pág. 376-377

2.9.8. Nmap

Network Mapper (Nmap) es una herramienta gratuita de código abierto que permite el descubrimiento de redes y pruebas de seguridad. Muchos administradores de redes y sistemas también ayudan con tareas como el inventario de redes, la gestión de programas de actualización de servicios y la supervisión de la disponibilidad de servidores o servicios. Nmap utiliza paquetes de IP sin procesar de una nueva manera para los servidores disponibles en su red, los servicios proporcionados por este servidor (nombre y versión de la aplicación), el sistema operativo en ejecución (y la versión del sistema operativo) y los paquetes/cortafuegos, además determina el tipo en uso y docenas de otras características (SINGH, 2022).

2.9.9. Nslookup

Esta herramienta permite conocer información que sirve para determinar la infraestructura del servidor de nombres de dominio. Se puede utilizar únicamente si se encuentra habilitado el protocolo TCP/IP y se puede usar tanto en sistemas Windows como Linux (Microsoft, 2022).

2.9.10. theHarvester

theHarvester es una herramienta desarrollada para la fase de reconocimiento en las pruebas de penetración. Permite conocer las amenazas externas que afectan a un dominio, por medio de la recolección de información que incluye correos electrónicos, subdominios e IPs atados a un dominio (GitHub, 2022c).

2.9.11. Wappalyzer

Wappalyzer es una extensión que se instala en el navegador web que se esté utilizando, el cual permite descubrir las tecnologías que utiliza un determinado sitio web (Wappalyzer, 2022).

2.9.12. Whois

Whois es una plataforma que permite realizar la búsqueda de dominios, permitiendo conocer los datos del propietario de un dominio específico. Además, en relación a dicho dominio se pueden conocer datos como la fecha de adquisición, la fecha de expiración, datos de contacto del dueño del dominio, datos del servidor de dominio, a través de quien (registrador) se adquirió dicho dominio, entre otros datos. La cantidad de datos a obtener depende de si el registrador ha habilitado la opción de protección de la privacidad para el propietario del dominio, con lo cual, los datos reales del propietario serán enmascarados evitando así que caigan en manos de personas mal intencionadas (Arun & Bijimol, 2021).

CAPÍTULO III
MARCO METODOLÓGICO

3.1.Ubicación

El Instituto Superior Tecnológico Sucre es una institución pública de educación superior. Su vida institucional ha sufrido una serie de cambios. Su origen se remonta al año 1959, cuando se fundó el Colegio Técnico Nacional Sucre. El 17 de julio de 1996, la Dirección Nacional de Planeamiento de la Educación, mediante acuerdo Nº 4191, resuelve elevar a la categoría de Instituto Técnico Superior. En el año 2003, con base en el informe de evaluación de los institutos técnicos del país, realizado por la Universidad Politécnica del Litoral, que ubicó en primer lugar al Instituto Técnico Sucre, se reconoce, a través del acuerdo Nº 166 otorgado por el Conesup, como Instituto Tecnológico Superior Sucre. El 15 de febrero del 2019, mediante comunicado RPC-SO-04-No. -057-2019, de la Senescyt, de conformidad a las disposiciones transitorias Sexta y Tercera del Reglamento de las Instituciones de Educación Superior de Formación Técnica y Tecnológica se da el cambio en la denominación del instituto llamándose ahora Instituto Superior Tecnológico Sucre (la palabra superior luego de instituto). Mediante resolución RPC-SO-06-No.171-2021 de 17 de marzo de 2021, el CES, autoriza la fusión de los institutos: Instituto Superior Tecnológico Consejo Provincial de Pichincha, Instituto Superior Tecnológico Cinco de Junio e Instituto Superior Tecnológico Andrés F. Córdova al Instituto Superior Tecnológico Sucre. A través del artículo 2 de la Resolución RPC-SO-34-No.770-2021 de 8 de diciembre de 2021, el CES, otorga la condición de superior universitario al Instituto Superior Tecnológico Sucre, con lo cual, pasa a ser Instituto Superior Universitario Sucre. Este Instituto tiene su domicilio en la provincia de Pichincha, cantón Quito, en la Avenida 10 de agosto N26-21 y Luis Mosquera Narváez.

3.2.Equipos y Materiales

Para este trabajo de investigación se utilizaron dos computadores, software y plataformas para recopilar información, software para la detección y análisis de vulnerabilidades, software para ejecutar las pruebas de penetración, Internet, papel y

otros insumos de oficina. Así como, cursos de capacitación enfocados al pentesting y detección de vulnerabilidades.

En la Tabla 2 se presenta el detalle de las cantidades y los costos de los recursos utilizados en este trabajo de investigación.

Tabla 2

Equipos y Materiales Utilizados

Orden	Descripción	Unidad	Cantidad	Costo unitario (USD)	Costo total (USD)
1	Computador	Unidad	2	$700,00	$1.400,00
2	Conjunto de Software especializado para realizar el pentesting	Unidad	1	$0,00	$0,00
4	Internet	Horas	1.800	$0,10	$180,00
5	Transporte (taxi)	Días	5	$30,00	$150,00
6	Cursos de capacitación enfocados al pentesting y detección de vulnerabilidades	Unidad	2	$100,00	$200,00
7	Insumos de oficina	Unidad	1	$100,00	$100,00
	Costo total				**$2.030,00**

Fuente: Elaboración propia

3.3.Tipo de Investigación

La metodología de investigación utilizada, una vez que el Coordinador de TIC del Instituto Superior Tecnológico Sucre ha planteado su necesidad, es una investigación de campo y además exploratoria puesto que el estudio se lleva a cabo sobre la red de servidores y servicios del Instituto Superior Tecnológico Sucre mediante la ejecución de pruebas de penetración externas, con la finalidad de conocer cuáles son las vulnerabilidades que afectan actualmente a dicha red de servidores y servicios.

3.4.Prueba de Hipótesis

Considerando que el presente trabajo investigativo corresponde a un estudio de casos que tiene un alcance exploratorio no aplica el planteamiento de la hipótesis.

3.5.Población o Muestra

La granja de servidores con la que cuenta el Instituto Superior Tecnológico Sucre está compuesta por 2 servidores que alojan y brindan los servicios de Moodle y Alfresco. Adicionalmente, se tiene contratado un hosting con Ecuahosting, en donde se tienen alojados los servicios del Sistema escolástico Saga, el Sistema de evaluación docente y el Acceso a servicios estudiantiles.

Sin embargo, se firmó un acuerdo entre el Coordinador Gestión de la Información del Instituto Superior Tecnológico Sucre y la autora de este trabajo de titulación MARIA ELIZABETH CEDEÑO ZAMBRANO denominado "DOCUMENTO DE AUTORIZACIÓN PARA REALIZACIÓN DE PRUEBAS DE PENTESTING" mediante el cual se acordó que las actividades de verificación de seguridad de la red de servidores y servicios del Instituto Superior Tecnológico Sucre se debían realizar únicamente sobre los siguientes servicios:

- http://www.tecnologicosucre.edu.ec
- 186.4.188.30
- 186.4.195.178

3.6.Recolección de Información

Para el desarrollo del presente trabajo se han utilizado como técnicas de recolección de información la observación mediante el uso y aplicación de una lista de cotejo, además, se ha realizado una entrevista al Coordinador de TIC del Instituto a través de un guion estructurado de diez preguntas, las cuales permitieron conocer algunos parámetros sobre la realidad actual de la red del Instituto, la información recolectada es la línea base utilizada para llevar a cabo las diferentes etapas del pentesting, con lo

cual, se pueden conocer cuáles son las vulnerabilidades que afectan a la red de servidores y servicios del Instituto , así como, cuál es su nivel de criticidad.

3.7.Procesamiento de la Información y Análisis Estadístico

Se realizó un trabajo pre-experimental de un solo grupo, puesto que se aplicó un diseño de preprueba mediante pruebas de penetración sobre los activos autorizados por el Coordinador de TIC del Instituto, con la utilización del método de la observación para evaluar los resultados y así elaborar la propuesta de plan de mejora que permitirá mitigar la penetración de intrusos en la red de servidores y servicios del Instituto.

3.8.Variables Respuesta o Resultados Alcanzados

Con la ejecución adecuada de las pruebas de penetración se lograron detectar las vulnerabilidades que actualmente afectan a la red de servidores y servicios del Instituto Superior Tecnológico Sucre, información que sirve como base para desarrollar un plan de mejora que permitirá mitigar la penetración de intrusos en dicha red. En este sentido se han podido detectar las variables de respuesta detalladas en la Tabla 3.

Tabla 3

Variables de Respuesta

Variable	Definición	Dimensión	Indicador	Técnica / Instrumento
Seguridad perimetral	La seguridad perimetral consiste en colocar una barrera lo más inquebrantable posible entre la red interna e Internet, con el propósito de bloquear y controlar los datos que entran y salen de la red local de una organización (Bolaños Botina, 2018).	Hardware de seguridad perimetral	Dispone el Instituto de Hardware de seguridad perimetral.	Entrevista / Cuestionario. Lista de Cotejo
		Configuraciones de seguridad perimetral (VLANs, ACLs, etc)	Se han implementado o no configuraciones de seguridad perimetral	

Variable	Definición	Dimensión	Indicador	Técnica / Instrumento
Seguridad de la Información	La seguridad de la información consiste en garantizar la integridad, disponibilidad y confiabilidad de la información en todo momento (Bolaños Botina, 2018).	Contar con una Política de generación de contraseñas seguras y robustas.	Dispone el Instituto de una política de generación de contraseñas seguras y robustas	Entrevista / Cuestionario. Lista de Cotejo
Acceso a Internet	El acceso a Internet consiste en estar comunicado por medio de un dispositivo a la red global de datos acortando las distancias y generando mayor productividad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).	Contar con una Política de seguridad para el acceso a Internet. **S**eguridades que controlan el acceso a Internet de los usuarios.	Dispone el Instituto de una política de seguridad para el acceso a Internet El Instituto tiene o no implementadas seguridades para el acceso a Internet.	Entrevista / Cuestionario. Lista de Cotejo

Fuente: Elaboración propia

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1.Resultados Pre-Implementación

Para recopilar la información requerida, en primer lugar, se realizó una entrevista de 10 preguntas al Coordinador Gestión de la Información del Instituto Superior Tecnológico Sucre y a través de la observación se completó una lista de cotejo de diez parámetros., con la finalidad de conocer los parámetros básicos de seguridad con los que cuenta la red de servidores y servicios del Instituto. Posteriormente, con el uso de herramientas accesibles desde Internet y software especializado se llevaron a cabo las etapas del pentesting con el propósito de realizar el reconocimiento de las principales vulnerabilidades que afectan dichos servicios.

4.2.Periodo de Ejecución de Pruebas de Penetración

Una vez que se firmó el acuerdo entre el Coordinador Gestión de la Información del Instituto Superior Tecnológico Sucre y la autora de este trabajo de titulación MARIA ELIZABETH CEDEÑO ZAMBRANO denominado "DOCUMENTO DE AUTORIZACIÓN PARA REALIZACIÓN DE PRUEBAS DE PENTESTING", las pruebas de penetración fueron realizadas en el periodo de tiempo descrito en la Tabla 4.

Tabla 4
Periodo de Ejecución de Pruebas de Penetración

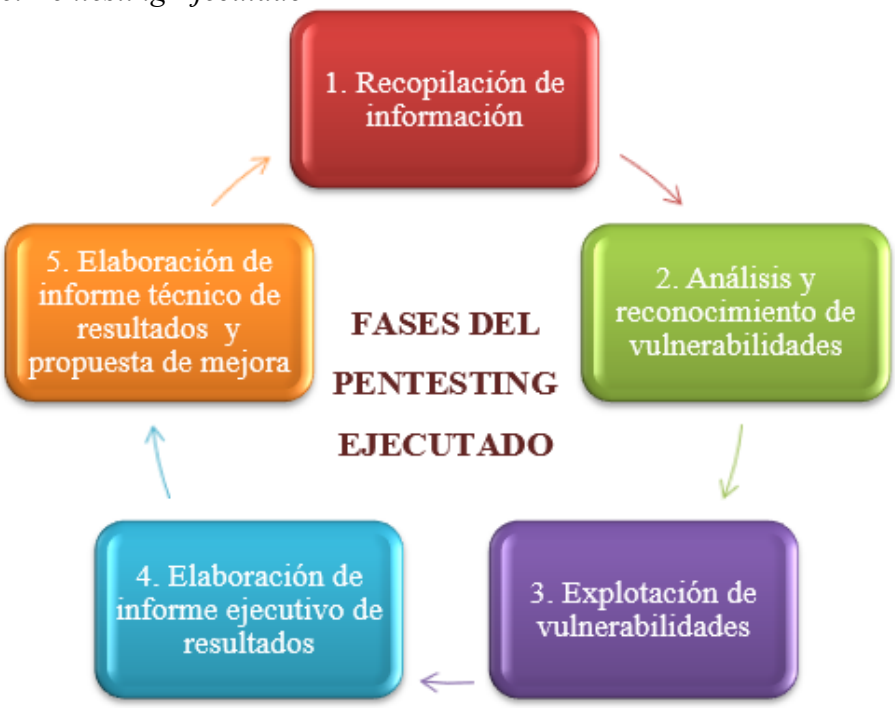
Actividad	Fecha de Inicio	Fecha de Fin
Ejecución de pruebas de penetración a la red de servidores y servicios del Instituto Superior Tecnológico Sucre	22 de agosto de 2022	13 de noviembre de 2022

Fuente: Elaboración propia

4.3.Fases de Pentesting Ejecutadas

El presente trabajo se lo realizó de acuerdo a las fases detalladas en la Figura 9.

Figura 9
Fases del Pentesting Ejecutado



Nota: Fases del proceso realizado en el presente trabajo. Elaboración propia

4.4.Herramientas y Software Utilizados en el Pentesting

En la Tabla 5 se detallan las distintas herramientas y software utilizados en todas las fases del pentesting para llevar a cabo el presente trabajo.

Tabla 5
Detalle Herramientas Utilizadas en el Pentesting

Item	Herramienta/Software	Versión	Fase de Uso
1	Microsoft Windows	10.0.17763.1	Todas las Fases
2	Kali GNU/Linux Rolling	43.0	Todas las Fases
3	Nslookup	Microsoft Windows [Versión 10.0.17763.1]	Fase de Recopilación de Información

Item	Herramienta/Software	Versión	Fase de Uso
4	Whois	NA	Fase de Recopilación de Información
5	IPAddress.com	NA	Fase de Recopilación de Información
6	Maltego	4.3	Fase de Recopilación de Información
7	TheHarvester	4.2.0	Fase de Recopilación de Información
8	Wappalyzer	6.10.47	Fase de Recopilación de Información
9	NMAP	7.93	Fase de Análisis y Detección de Vulnerabilidades
10	Gobuster	3.3	Fase de Análisis y Detección de Vulnerabilidades
11	Nessus Essentials	10.3.0	Fase de Análisis y Detección de Vulnerabilidades
12	Metasploit	6.2.25-dev	Fase de Explotación
13	Httpmethods	3	Fase de Explotación

Nota: Herramientas que fueron utilizadas para ejecutar las pruebas de penetración

4.5.Fase de Recopilación de Información

4.5.1. Entrevista Coordinador Gestión de la Información - ITS SUCRE

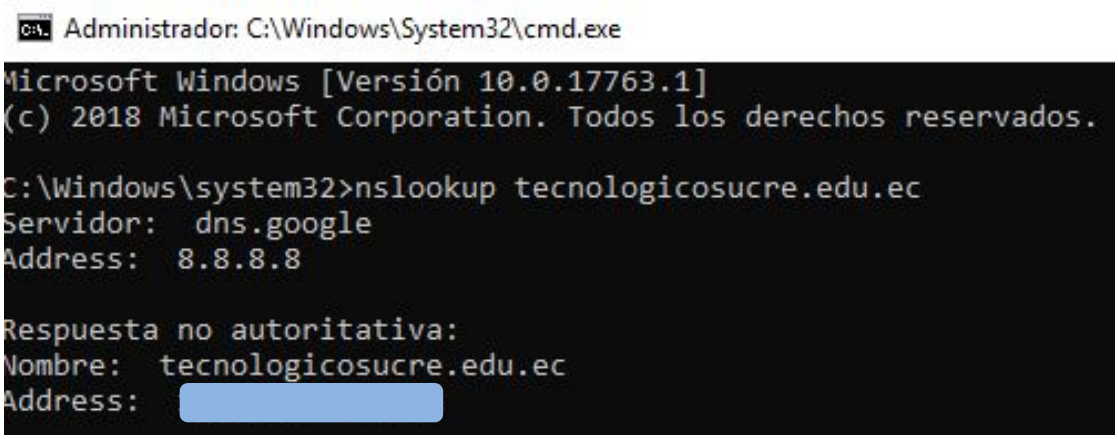
De la entrevista realizada se obtuvo como información que el Instituto Superior Tecnológico Sucre no cuenta con un equipo que realice las funciones de seguridad perimetral, además no cuenta con VLANs ni con la generación de ACLs que le permita filtrar y controlar el tipo de tráfico que se genera entre los servidores y servicios desde y hacia el Internet. Tampoco se cuenta con políticas que determinen y guíen a los usuarios en cómo deben realizar la generación de contraseñas, así como, tampoco se tiene una política que determine la forma en la que se accede a Internet. Finalmente, se pudo conocer que el dominio **tecnologicosucre.edu.ec** se encuentra alojado en un hosting externo y que el encargado de TI no conoce a detalle cuáles son los riesgos y las vulnerabilidades a las que está expuesta la red de servidores y servicios del instituto. Con estos datos se pudo llenar una parte de la lista de cotejo utilizada.

4.5.2. Resolución del Dominio

En esta parte se realizó el análisis del dominio con la ayuda de herramientas disponibles a través de Internet y con software libre, para extraer la mayor cantidad de información posible en cuanto a DNS, dominios, propietarios, ubicación, entre otros datos.

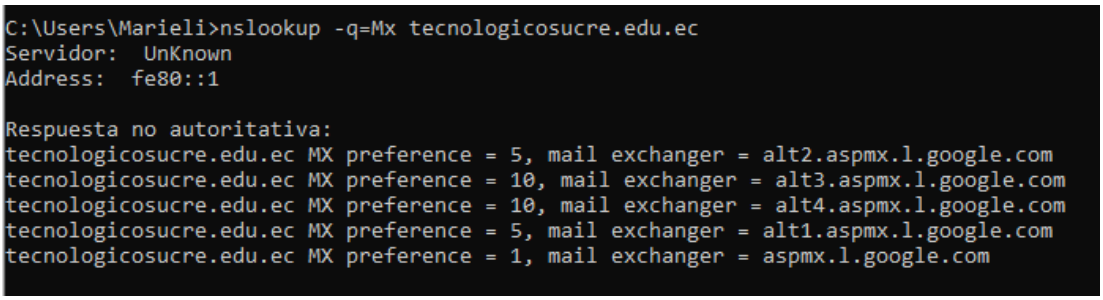
A través de la herramienta Nslookup se resolvió el dominio tecnologicosucre.edu.ec para conocer la IP pública a la que está asociado, este resultado se presenta en las Figuras 10 y 11.

Figura 10
Resolución del Dominio



Fuente: Elaboración propia. Por temas de confidencialidad no se pueden revelar los datos encontrados.

Figura 11
Obtención de los DNS

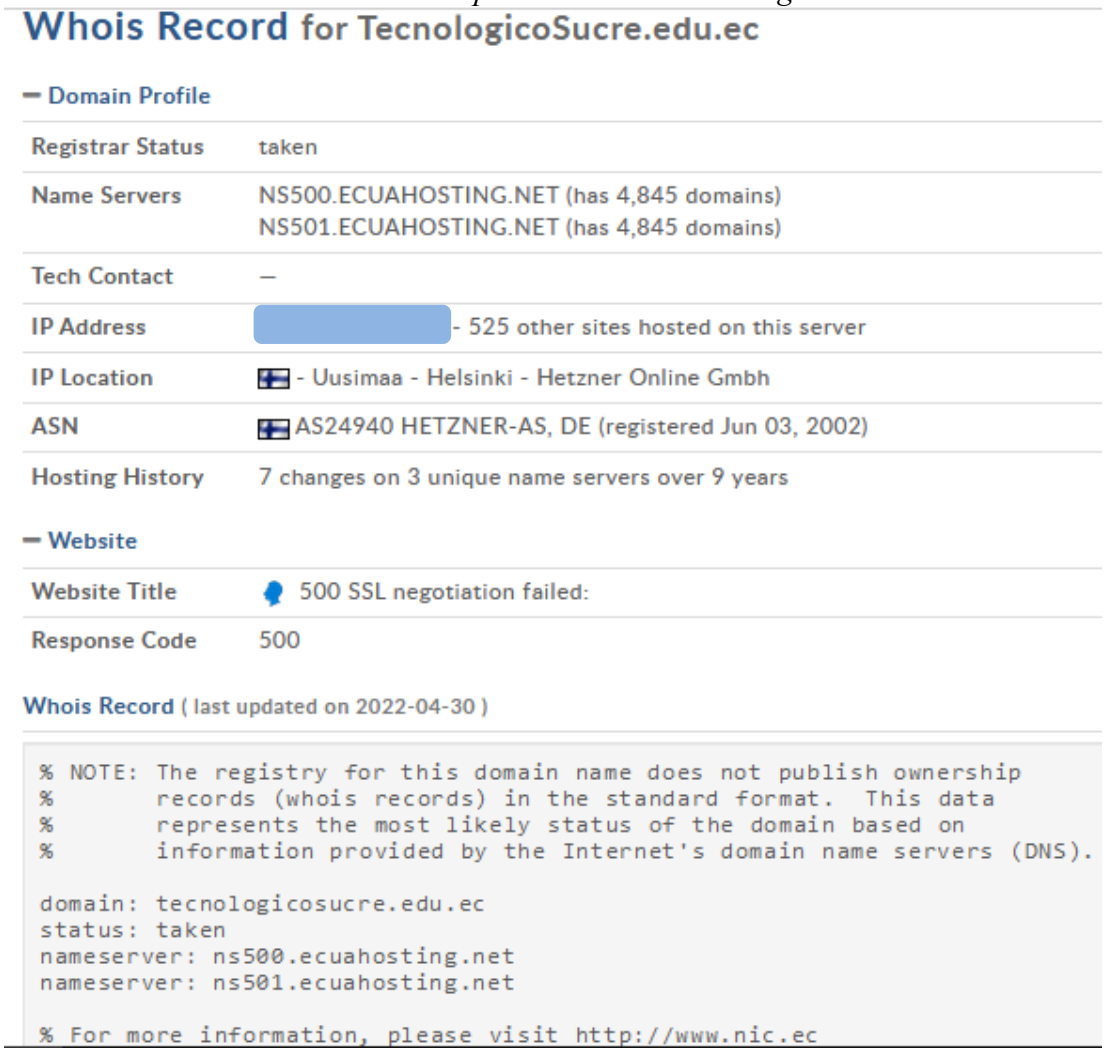


Fuente: Elaboración propia.

Mediante el uso de las herramientas Whois e IPAddress.com, cuyos resultados se presentan en las Figuras 12 y 13, se ha podido comprobar que el dominio del instituto se encuentra registrado con Ecuahosting y la IP pública de dicho dominio se encuentra ubicada en Europa, además se ha podido verificar que la administración de este dominio se encuentra configurada con niveles de seguridad de tal manera que no se pueden visualizar los datos del propietario del dominio.

Figura 12

Resolución de Dominio con WHOIS para Conocer el Hosting



Whois Record for TecnologicoSucre.edu.ec

— Domain Profile

Registrar Status	taken
Name Servers	NS500.ECUAHOSTING.NET (has 4,845 domains) NS501.ECUAHOSTING.NET (has 4,845 domains)
Tech Contact	–
IP Address	[redacted] - 525 other sites hosted on this server
IP Location	- Uusimaa - Helsinki - Hetzner Online Gmbh
ASN	AS24940 HETZNER-AS, DE (registered Jun 03, 2002)
Hosting History	7 changes on 3 unique name servers over 9 years

— Website

Website Title	500 SSL negotiation failed:
Response Code	500

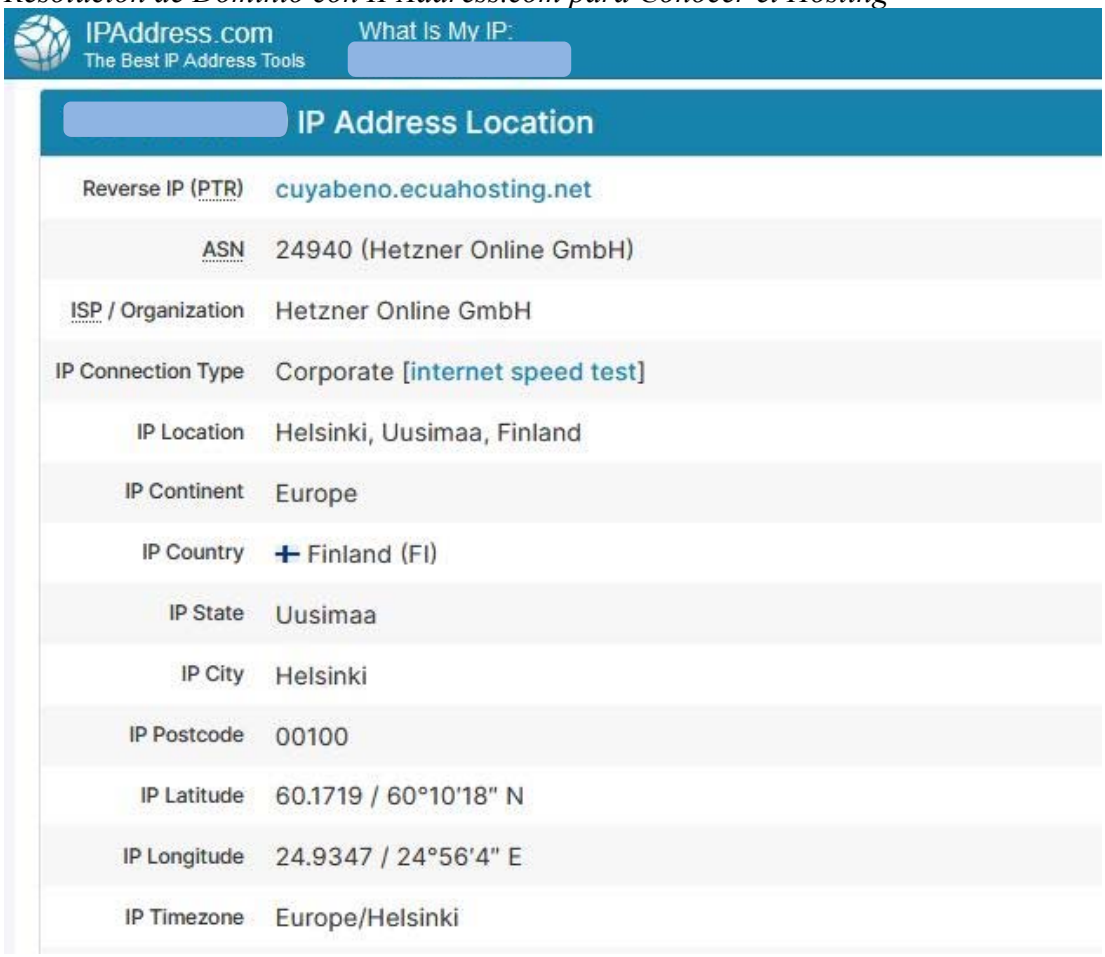
Whois Record (last updated on 2022-04-30)

```
% NOTE: The registry for this domain name does not publish ownership
%       records (whois records) in the standard format.  This data
%       represents the most likely status of the domain based on
%       information provided by the Internet's domain name servers (DNS).

domain: tecnologicosucre.edu.ec
status: taken
nameserver: ns500.ecuahosting.net
nameserver: ns501.ecuahosting.net

% For more information, please visit http://www.nic.ec
```

Fuente: Elaboración propia

Figura 13

Resolución de Dominio con IPAddress.com para Conocer el Hosting



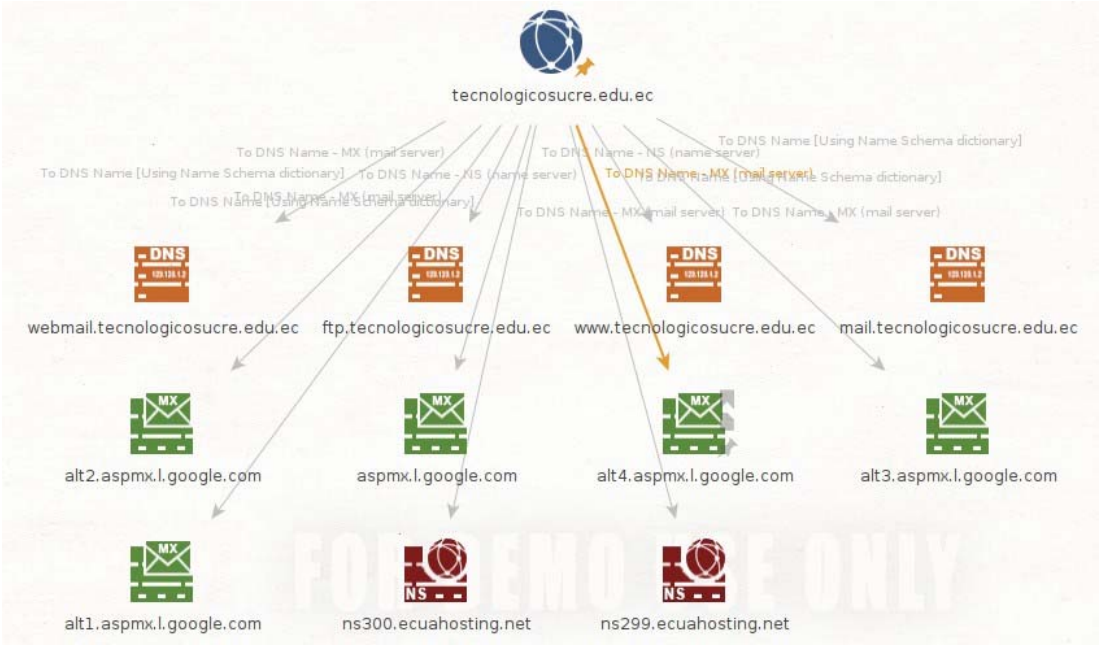
Fuente: Elaboración propia

Con la ayuda de la herramienta Maltego, instalada en Kali Linux, se pudo determinar los correos electrónicos que se encuentran publicados en la página web del Instituto, además, de los datos de los servidores DNS a los que está atado el dominio tecnologicosucre.edu.ec. Estos resultados se presentan en las Figuras 14 y 15 respectivamente.

Figura 14
Correos Electrónicos Alojados en la Página WEB

Fuente: Elaboración propia

Figura 15
Servidores DNS



Fuente: Elaboración propia. Se presentan los servidores DNS a los que se encuentra atado el dominio tecnologicosucre.edu.ec

Con la ayuda de la herramienta TheHarvester, instalada en una máquina con Kali Linux, a través de la ejecución del script ***sudo theHarvester -d tecnologicosucre.edu.ec -l 500 -b all*** se realizó la enumeración de los subdominios

que tiene el dominio tecnologicosucre.edu.ec, los resultados se presentan en la Figura 16.

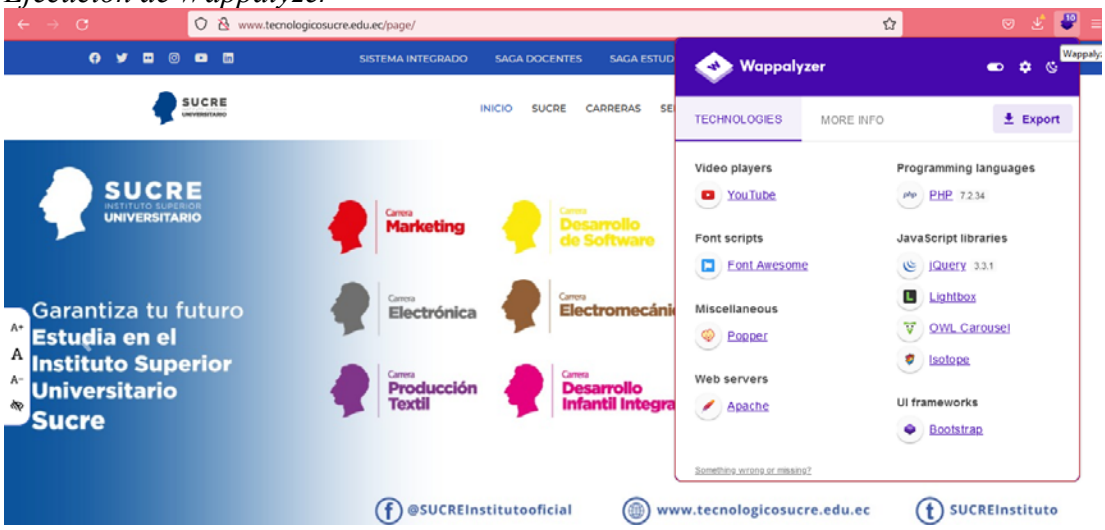
Figura 16
Enumeración de Subdominios

Fuente: Elaboración propia. Por temas de confidencialidad no se pueden revelar los datos encontrados.

A través de la extensión de Firefox Wappalyzer, se pudo determinar la tecnología sobre la cual está desarrollada la página web del Instituto, tal como, se puede observar en las Figuras 17 y 18.

Figura 17

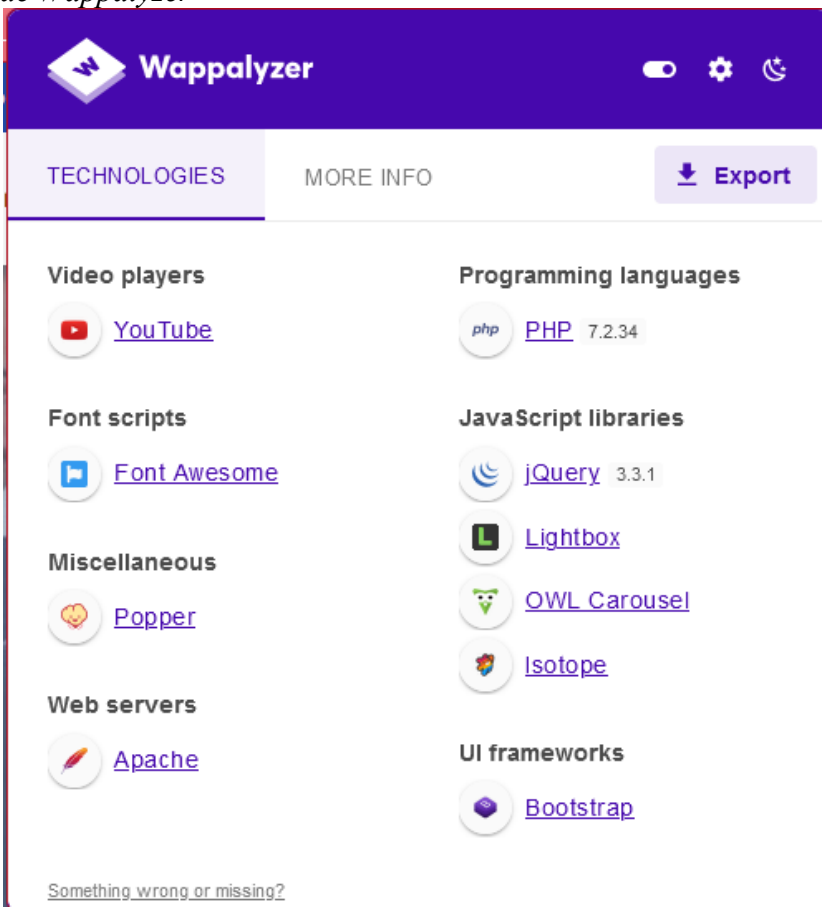
Ejecución de Wappalyzer



Fuente: Elaboración propia. Ejecución de Wappalyzer en la página web del Instituto.

Figura 18

Resultado de Wappalyzer



Fuente: Elaboración propia. Tecnología con la que está desarrollada la página web del Instituto.

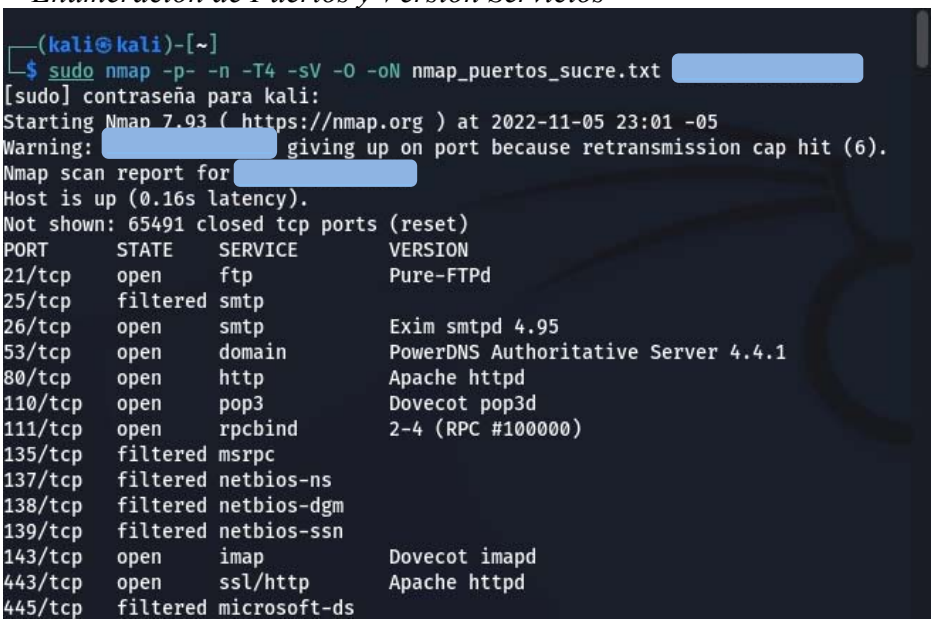
4.6.Fase de Análisis y Detección de Vulnerabilidades

Para conocer cuáles son las vulnerabilidades que afectan al dominio y a las direcciones IP públicas entregadas por el Instituto, se utilizaron las herramientas Nmap, Nessus.

4.6.1. Análisis Página Web del Instituto

Con la ayuda de la herramienta NMAP, instalada en Kali Linux, en una primera revisión en el mes de agosto de 2022, se pudo identificar que el servidor en el que se encuentra alojada la página web del Instituto http://www.tecnologicosucre.edu.ec tenía puertos críticos abiertos, sobre los cuales un ciberdelincuente podría generar ataques para infiltrarse y robar la información sensible del Instituto. En la Figura 19 se detallan estos puertos.

Figura 19
NMAP - Enumeración de Puertos y Versión Servicios



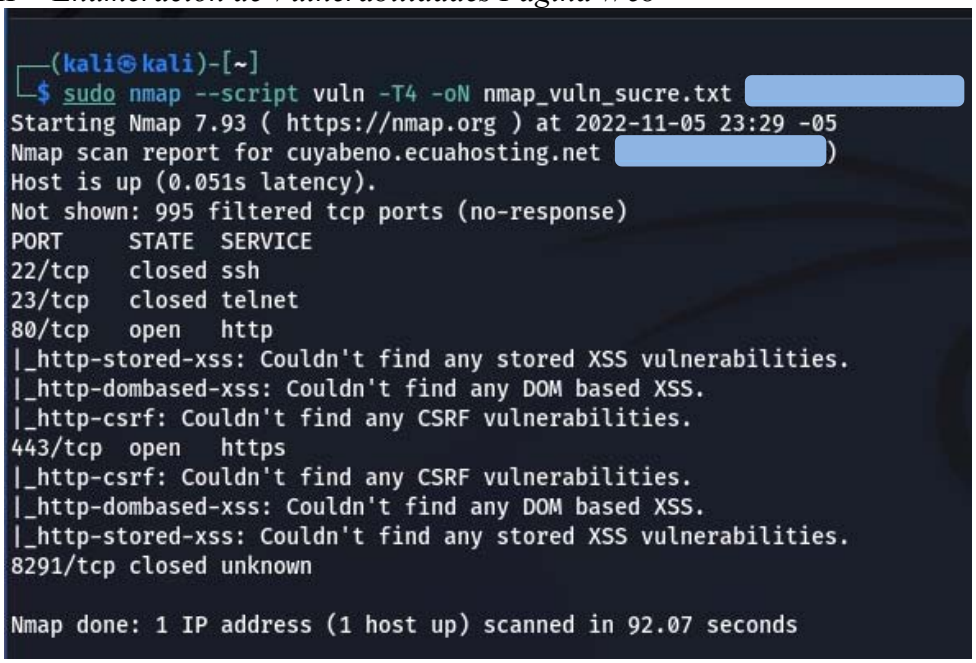
Fuente: Elaboración propia. Enumeración de los puertos abiertos y la versión de los servicios que tiene el servidor sobre el que se encuentra alojada la página web del Instituto.

Adicionalmente, con la ayuda de NMAP se validó que la página web del Instituto no tiene vulnerabilidades de XSS y CSRF que afecten al protocolo HTTP (puerto 80) y

HTTPS (puerto 443), tal como se puede observar en la Figura 20. Sin embargo, esto no garantiza que dichos puertos no puedan ser vulnerados con otros tipos de ataques.

Figura 20

NMAP - Enumeración de Vulnerabilidades Página Web

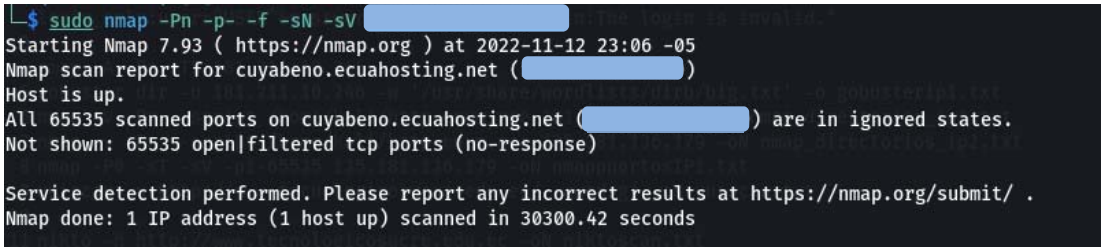


Fuente: Elaboración propia. Enumeración de las vulnerabilidades que afectan a la página web del Instituto

Posteriormente, en el mes de noviembre de 2022, se volvió a correr el análisis de puertos confirmándose que a dicha fecha el servidor en el que se encuentra alojada la página web del Instituto http://www.tecnologicosucre.edu.ec ya no tiene puertos abiertos, tal como se muestra en la Figura 21, lo cual da a entender que el proveedor que le brinda este servicio al Instituto, detectó las infiltraciones que los análisis de agosto ocasionaron, por lo cual, dicho proveedor realizó las acciones correctivas necesarias para asegurar el dominio y página web del Instituto.

Figura 21

NMAP -Nueva Enumeración de Puertos



Fuente: Elaboración propia. Estado actual de los puertos de los servicios que tiene el servidor donde se encuentra alojada la página web del Instituto.

A través de la herramienta Gobuster, instalada en Kali Linux, a través del script ***gobuster dir -u [IP] -w '/usr/share/wordlists/dirb/big.txt' -o gobusterip2.txt*** se pudo enumerar los directorios que se encuentran alojados en la página web y así conocer cuáles pueden ser de fácil acceso para un atacante. En la Figura 22 se puede observar los resultados de esta consulta.

Figura 22

Enumeración de Directorios en la Página Web

Fuente: Elaboración propia. Por temas de confidencialidad no se pueden revelar los datos encontrados.

Por medio de la herramienta Nessus, instalada en Kali Linux, se realizó el escaneo de las vulnerabilidades que presenta la página web del Instituto. En la Figura 23 se puede

observar que existen únicamente 23 vulnerabilidades a nivel informativo que no implican afectación para los servicios.

Figura 23

Nessus-Vulnerabilidades Página Web

0	0	0	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 23

SEVERITY	CVSS V3.0	PLUGIN	NAME
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	31658	DNS Sender Policy Framework (SPF) Enabled
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	54615	Device Type
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	10919	Open Port Re-check
INFO	N/A	34043	PowerDNS Version Detection
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	22964	Service Detection
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	62564	TLS Next Protocols Supported
INFO	N/A	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

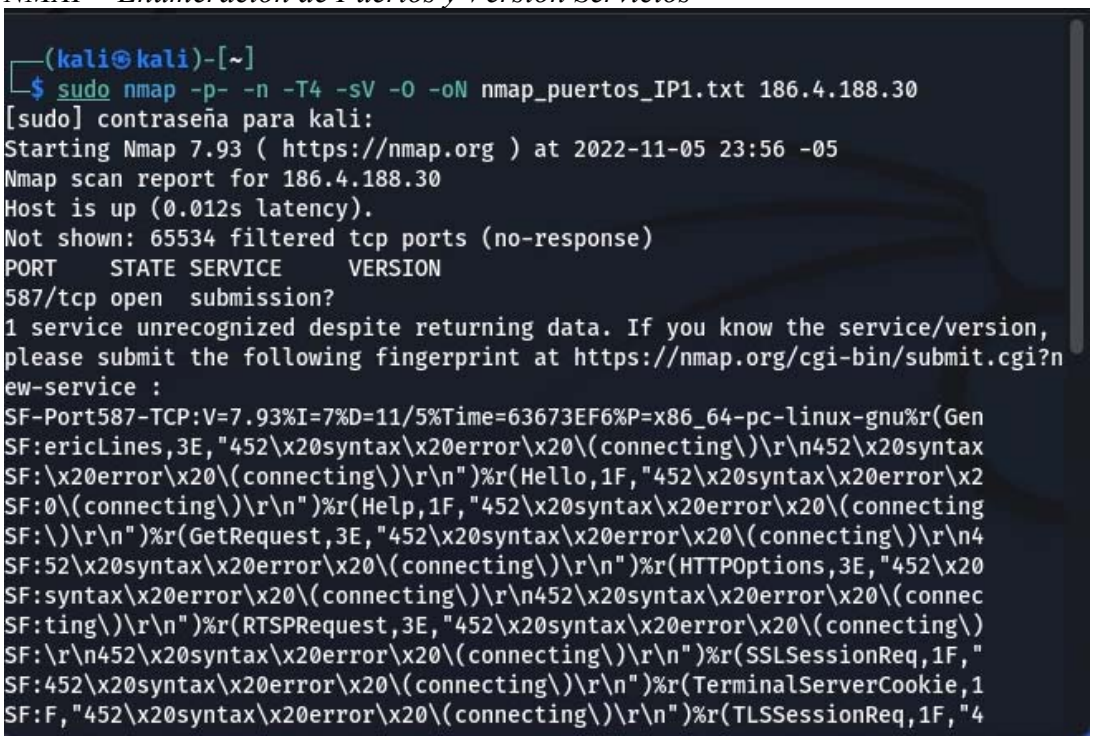
Fuente: Elaboración propia. Listado de vulnerabilidades encontradas en la página web del Instituto.

4.6.2. Análisis Direcciones IP Públicas del Servicio de Internet

Tal como lo supo manifestar el Coordinador de TIC del Instituto las IPs públicas 186.4.188.30 y 186.4.195.178 corresponden a los equipos por los cuales los usuarios del Instituto Superior Tecnológico Sucre acceden al servicio de Internet.

Con la ayuda de la herramienta NMAP, se pudo identificar los puertos que tiene abiertos la IP pública 186.4.188.30. En la Figura 24 se puede observar que este equipo tiene abierto únicamente el puerto 587/TCP.

Figura 24
NMAP - Enumeración de Puertos y Versión Servicios



Fuente: Elaboración propia. Enumeración de los puertos abiertos y la versión de los servicios que tiene el equipo con IP 186.4.188.30 que le brinda el servicio de Internet al Instituto.

Según la IANA (Internet Assigned Numbers Authority) (2022) a través de su documento de referencia Nro. RFC 6409, el puerto 587/TCP debe ser utilizado para el envío de mensajes (message submission), separándolo así de la retransmisión de

mensajes, con lo cual, se posibilita para que cada servicio maneje sus propios requisitos de políticas o seguridad.

La Figura 25 presenta el número de referencia mediante el cual la IANA asigna el puerto 587/TCP para el envío de mensajes.

Figura 25

Puerto 587/TCP

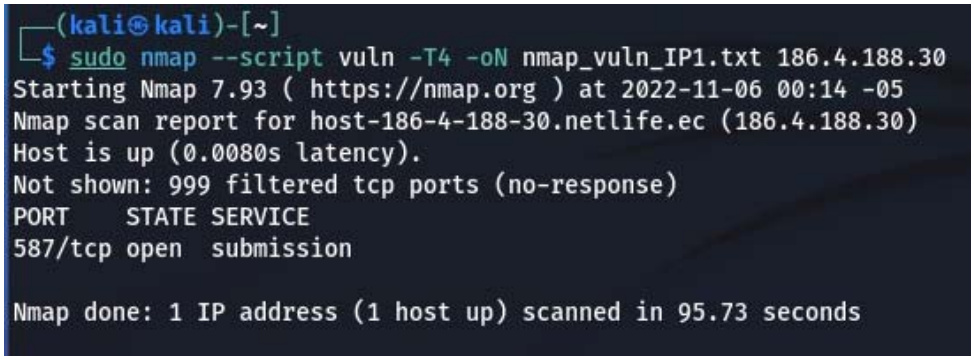
Service Name	Port Number	Transport Protocol	Description	Assignee	Contact	Registration Date	Modification Date	Reference
submission	587	tcp	Message Submission				2011-11-17	[RFC6409]

Nota. Adaptado de *Service Name and Transport Protocol Port Number Registry*., IANA, 2022

Tal como lo muestra la Figura 26 se pudo observar que el equipo con IP 186.4.188.30 no presenta vulnerabilidades a nivel externo.

Figura 26

NMAP - Enumeración de Vulnerabilidades IP Pública



Fuente: Elaboración propia. Enumeración de las vulnerabilidades que afectan a la IP 186.4.188.30

Por medio de la herramienta Nessus, se realizó el escaneo de las vulnerabilidades que presenta la IP 186.4.188.30. En la Figura 257 se puede observar que no existen vulnerabilidades que afecten a dicha IP.

Figura 27

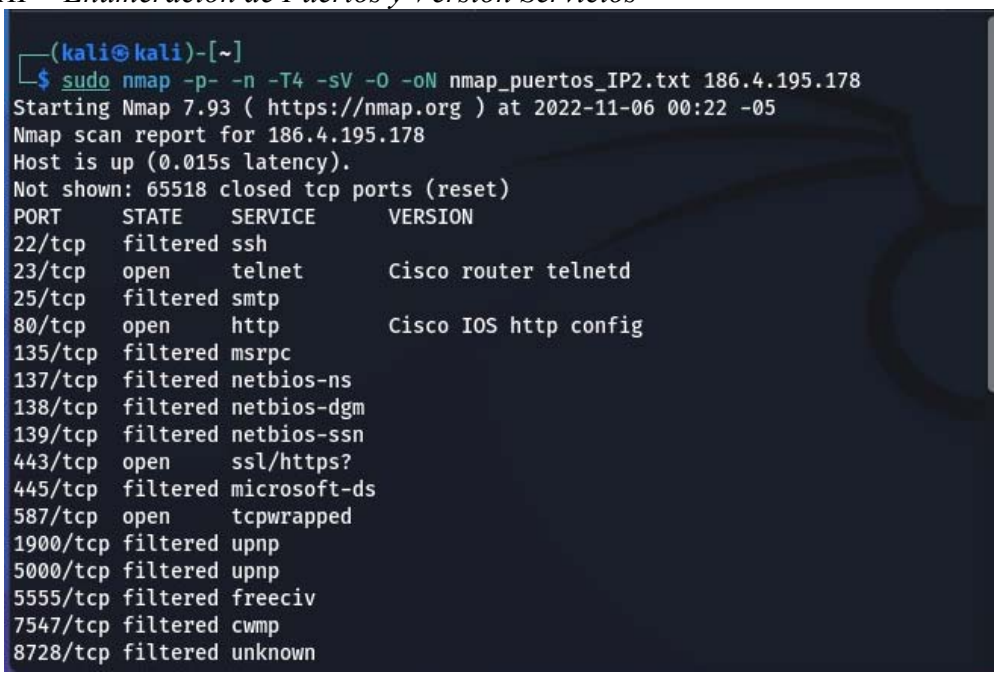
Nessus-Escaneo Vulnerabilidades IP Pública

Fuente: Elaboración propia.

Con la ayuda de la herramienta NMAP, se pudo identificar los puertos que tiene abiertos la IP pública 186.4.195.178. En la Figura 28 se detallan estos puertos, algunos de los cuales son críticos ya que posibilitan que el equipo sea atacado, además se pudo conocer que el equipo es un CISCO.

Figura 28

NMAP - Enumeración de Puertos y Versión Servicios

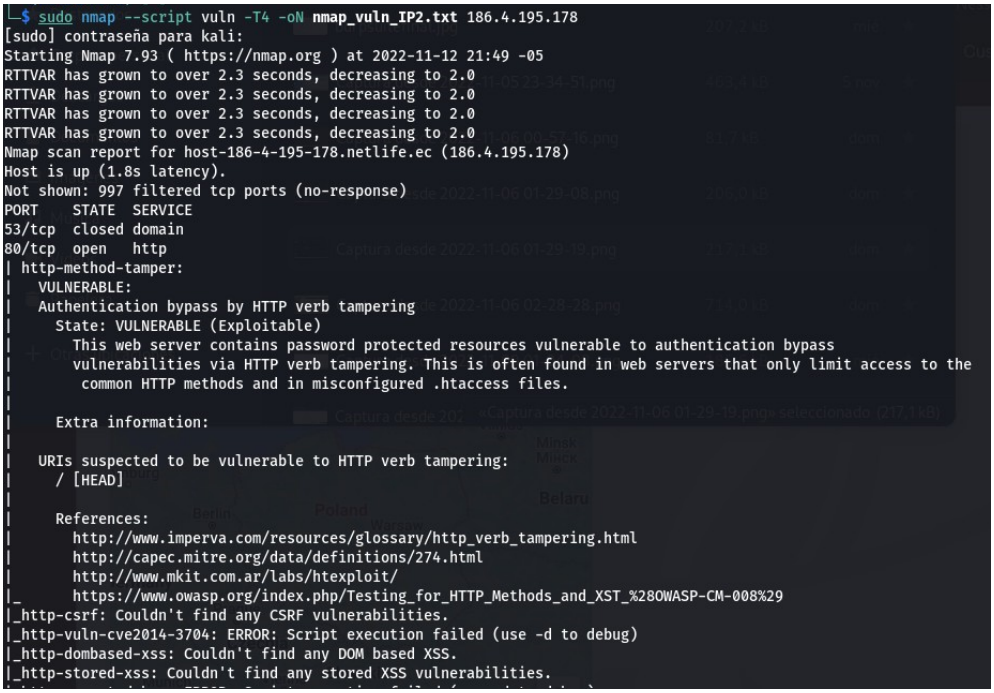


Fuente: Elaboración propia. Enumeración de los puertos abiertos y la versión de los servicios que tiene el equipo con IP 186.4.195.178 que le brinda el servicio de Internet al Instituto.

Con la ayuda de NMAP se ha podido conocer que la IP 186.4.195.178 tiene dos vulnerabilidades críticas que pueden ser explotadas fácilmente, estas vulnerabilidades son http-method-tamper y ssl-ccs-injection, tal como, se puede observar en las Figuras 29, 30, 31 y 32.

Figura 29

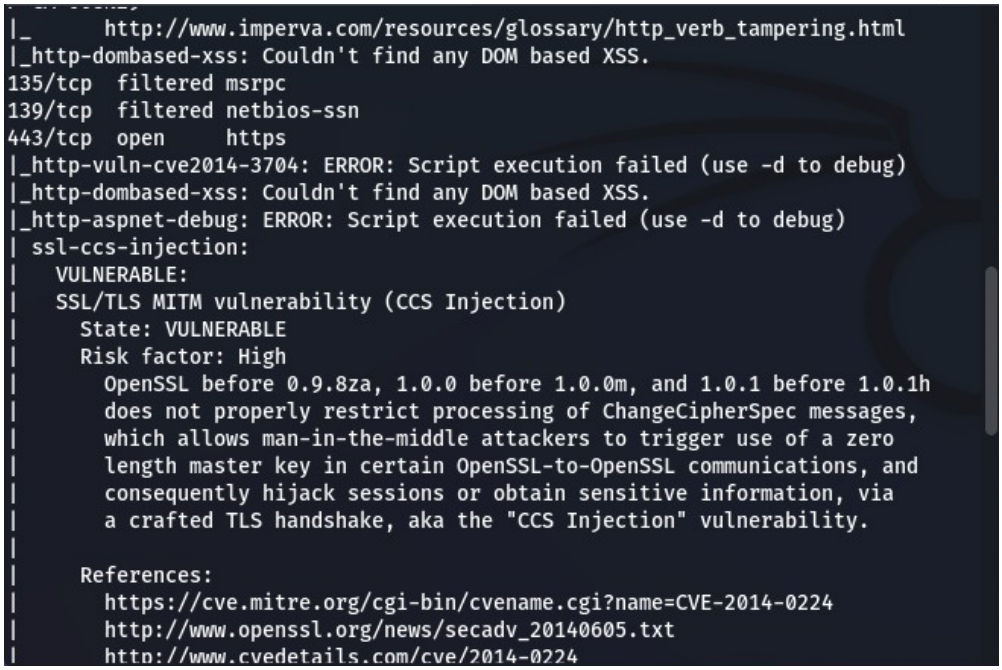
NMAP - Enumeración de Vulnerabilidades IP Pública



Fuente: Elaboración propia. Enumeración de las vulnerabilidades que afectan a la IP 186.4.195.178

Figura 30

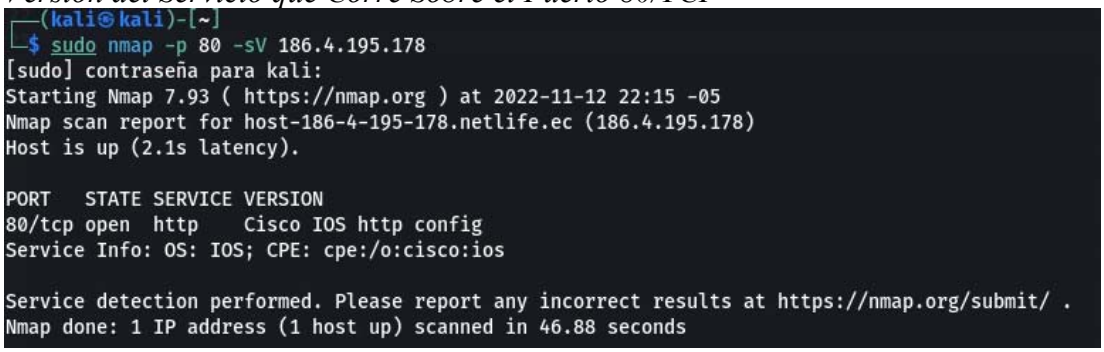
NMAP - Enumeración de Vulnerabilidades IP Pública Cont.



Fuente: Elaboración propia. Enumeración de las vulnerabilidades que afectan a la IP 186.4.195.178

Figura 31

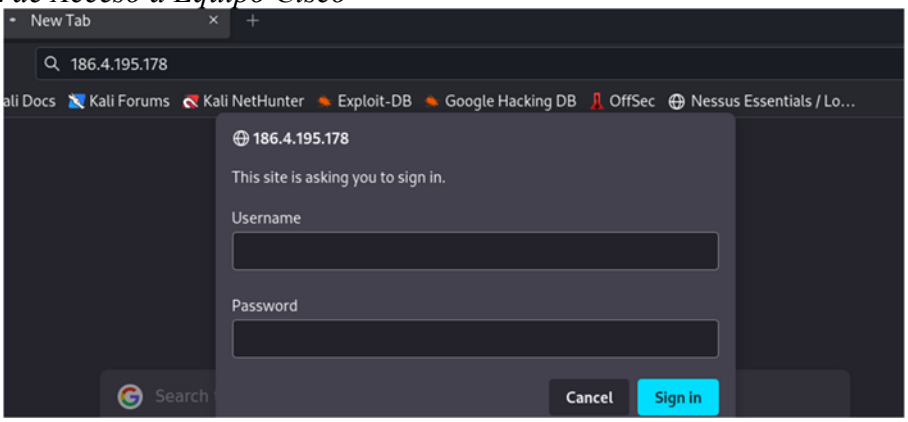
Versión del Servicio que Corre Sobre el Puerto 80/TCP



Fuente: Elaboración propia. Versión del servicio HTTP que corre sobre el puerto 80/TCP en el equipo Cisco con IP 186.4.195.178

Figura 32

Interfaz de Acceso a Equipo Cisco



Fuente: Elaboración propia. Interfaz de acceso a través del puerto 80/TCP al equipo Cisco con IP 186.4.195.178

El método http-method-tamper intenta omitir los recursos protegidos por contraseña (estado HTTP 401) al manejar verbos HTTP. Si no hay un conjunto de rutas para verificar, escanea el servidor web y busca los recursos protegidos con contraseña encontrados. La especificación HTTP incluye métodos de solicitud que difieren de las solicitudes GET y POST estándar. Los servidores web que cumplen con los estándares pueden responder a estas soluciones que el desarrollador no pretendía. Una explicación general es la modificación de verbos, el estándar HTTP 1.1 trata estos tipos de solicitudes como métodos HTTP distintos (OWASP Foundation, 2022).

Una vulnerabilidad de secuencias de comandos entre sitios (Cross Site Scripting CSS) implica la inyección de código CSS arbitrario en el contexto de un sitio de confianza que se representa en el navegador de la víctima. El impacto de tales vulnerabilidades varía según la carga útil de CSS entregada. Esto puede conducir a secuencias de comandos entre sitios o minería de datos. Un atacante man-in-the-middle (MITM) podría explotar la vulnerabilidad esperando una nueva conexión TLS seguida de un mensaje de protocolo de enlace ClientHello ServerHello. Transmita paquetes CCS en ambas direcciones obligando al código OpenSSL a usar una clave inicial de longitud cero. Los paquetes se envían a ambos extremos del enlace. Las claves de sesión se obtienen utilizando una clave de longitud cero, y las futuras claves de sesión también tendrán este defecto. Discuta los parámetros del apretón de manos. Los atacantes ahora pueden descifrar e incluso modificar los paquetes de envío. El script funciona enviando

un mensaje "ChangeCipherSpec" dañado y verificando el servidor en busca de un registro de advertencia "UNEXPECTED_MESSAGE". Dado que el servidor sin parches aceptó el mensaje, se enviaron dos paquetes CCS para obligar al servidor a reactivarse. Si el tipo de alerta es diferente de "UNEXPECTED_MESSAGE", podemos concluir que el servidor es vulnerable (Gupta & Chaudhary, 2020).

Por medio de la herramienta Nessus, se realizó el escaneo de las vulnerabilidades que presenta la IP 186.4.195.178. En las Figuras 33 y 34 se puede observar que existen 34 vulnerabilidades que afectan a dicha IP.

Figura 33

Nessus-Escaneo Vulnerabilidades IP Pública

Vulnerabilities — Total: 34

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
HIGH	7.5	96802	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	57582	SSL Self-Signed Certificate
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	42263	Unencrypted Telnet Server
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	62694	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
MEDIUM	5.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	60108	SSL Certificate Chain Contains Weak RSA Keys
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	19689	Embedded Web Server Detection
INFO	N/A	10107	HTTP Server Type and Version

Fuente: Elaboración propia

Figura 34

Nessus-Escaneo Vulnerabilidades IP Pública Cont.

INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	11935	IPSEC Internet Key Exchange (IKE) Version 1 Detection
INFO	N/A	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	22964	Service Detection
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

Fuente: Elaboración propia

En la Tabla 6 se detallan la cantidad por cada nivel de severidad a los que corresponden las 34 vulnerabilidades encontradas.

Tabla 6

Detalle de Vulnerabilidades Encontradas

Nivel de Severidad	Cantidad de Vulnerabilidades Encontradas
Critical	1
High	3
Medium	9
Low	1
Info	20
Total	**34**

Fuente: Elaboración propia

Enfocándonos en las vulnerabilidades críticas y altas, tal como lo describe Nessus en el informe de reporte de vulnerabilidades que se generó, encontramos que las mismas

pueden afectar a la integridad de la red y por ende a la información del Instituto de la siguiente forma:

SSL Version 2 and 3 Protocol Detection. El servicio remoto permite que se generen conexiones encriptadas utilizando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL son perjudicadas por diversas debilidades criptográficas, como lo son los esquemas de relleno inseguros que utilizan cifrados por encadenamiento de bloques CBC (cipher-block chaining) o esquemas de renegociación y reconexión débiles (Nessus - Tenable, 2022).

Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (cisco-sa-20160916- ikev1) (BENIGNCERTAIN) (uncredentialed check). El servicio IKE que corre en los equipos Cisco IOS remoto se ve perjudicado por una vulnerabilidad de propagación de información, llamada BENIGNCERTAIN, el cual se da por una administración incorrecta de las peticiones de negociación de IKEv1. Un ciberdelincuente puede aprovechar esta vulnerabilidad mediante la utilización de un paquete IKEv1 con modificaciones que le permitan obtener la información de la memoria, con lo cual se pierde la integridad y confidencialidad de la información (Nessus - Tenable, 2022).

SSL Certificate Signed Using Weak Hashing Algorithm. La conexión remota se realiza por medio de una cadena de certificados SSL que ha sido suscrita con un método de encriptación frágil como lo son MD2, MD4, MD5 o SHA1. Es bien conocido que estos métodos de encriptación se ven afectados por ataques de choque. Con esta vulnerabilidad un ciberdelincuente puede crear otro certificado con la misma firma digital, permitiendo así acceder a los servicios de la víctima (Nessus - Tenable, 2022).

SSL Medium Strength Cipher Suites Supported (SWEET32). El dispositivo al que se intenta acceder permite la utilización de cifrados SSL, dichos certificados permiten una encriptación de nivel medio. Esto básicamente se refiere al uso de un algoritmo de cifrado de datos triple 3DES (Data encryption algorithm). Esta

vulnerabilidad es principalmente útil si el ciberdelincuente se encuentra dentro de la red de la víctima (Nessus - Tenable, 2022).

Por temas de confidencialidad el informe completo de los resultados obtenidos será entregado únicamente al Instituto Superior Tecnológico Sucre.

4.7.Fase de Explotación

En esta fase se llevaron a cabo un conjunto de acciones con la finalidad de explotar por fuerza bruta las vulnerabilidades encontradas. Considerando que en todo momento fue primordial mantener activos los servicios del Instituto, no se explotaron todas las vulnerabilidades encontradas, únicamente se realizaron acciones mínimas sobre las vulnerabilidades de SSL y HTTP detectadas sobre el equipo con IP 186.4.195.178 y descritas anteriormente, con la finalidad de evitar comprometer la disponibilidad, confidencialidad e integridad de los servicios e información que posee el Instituto.

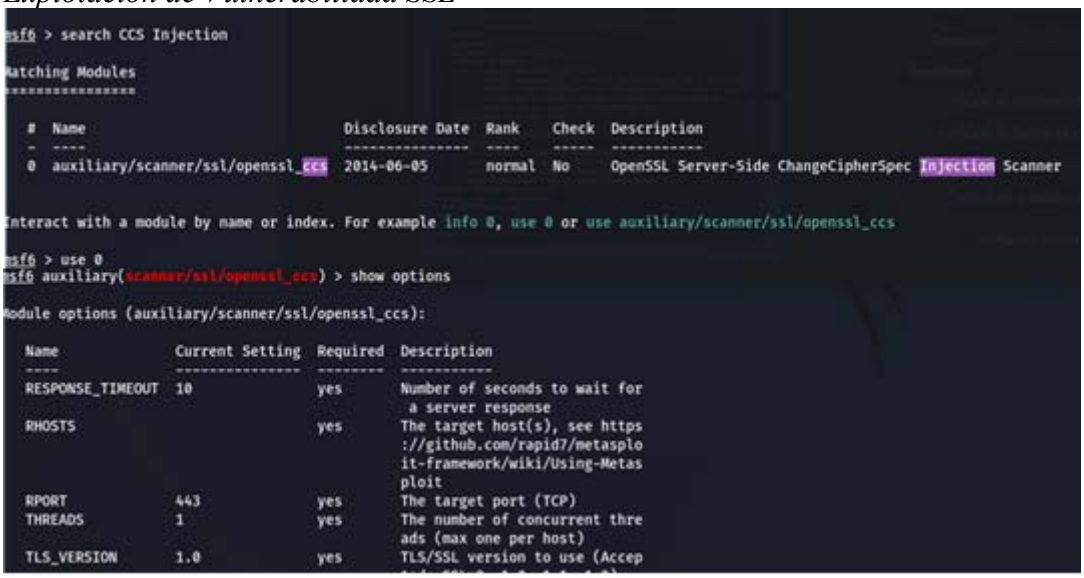
4.7.1. Explotación de Vulnerabilidad SSL

Con la ayuda de la herramienta Metasploit se ejecutó un exploit que por medio de un ataque de fuerza bruta permite comprometer la seguridad del equipo con IP 186.4.195.178 atacando la vulnerabilidad de SSL que tiene este equipo.

Las Figuras 35 y 36 presentan los resultados del ataque por fuerza bruta ejecutado, el mismo que se completó correctamente, lo que implica que se pudo colocar un script espía conocido como hombre en el medio (MITM) mismo que permitirá que el atacante que está escuchando estas comunicaciones pueda hacerse con las credenciales de acceso al equipo en cuanto un usuario legítimo trate de ingresar al mismo.

Figura 35

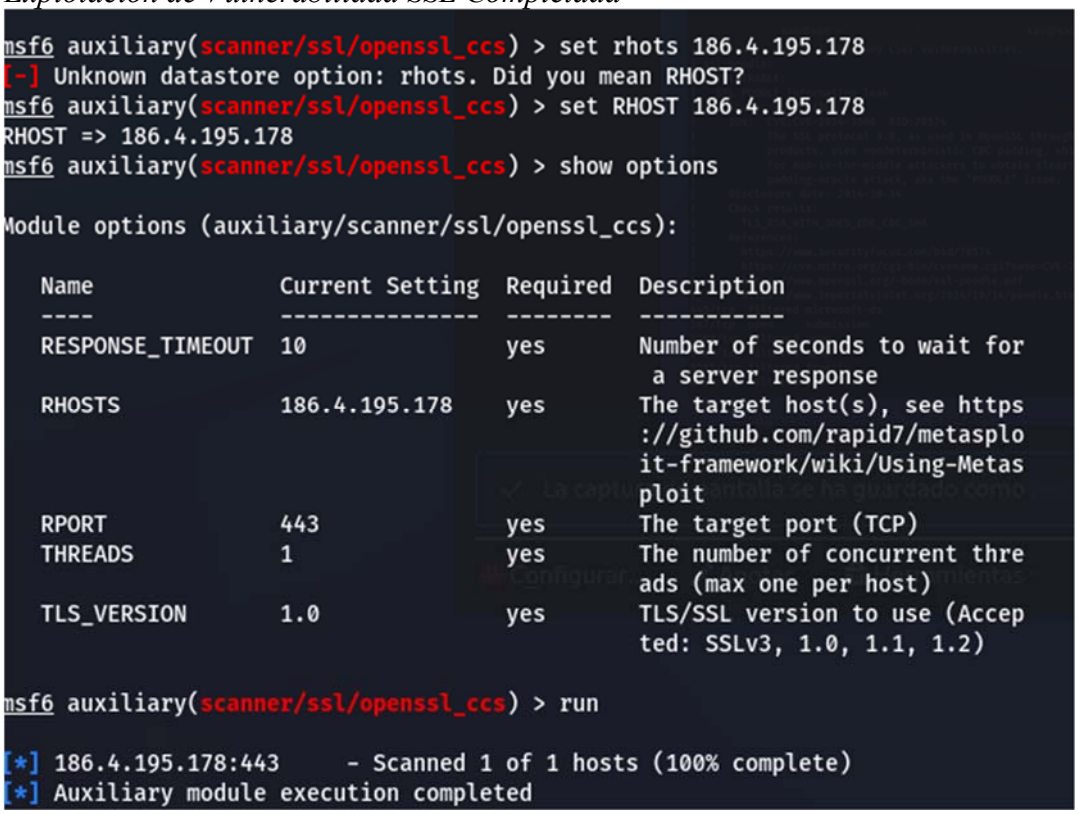
Explotación de Vulnerabilidad SSL



Fuente: Elaboración propia

Figura 36

Explotación de Vulnerabilidad SSL Completada

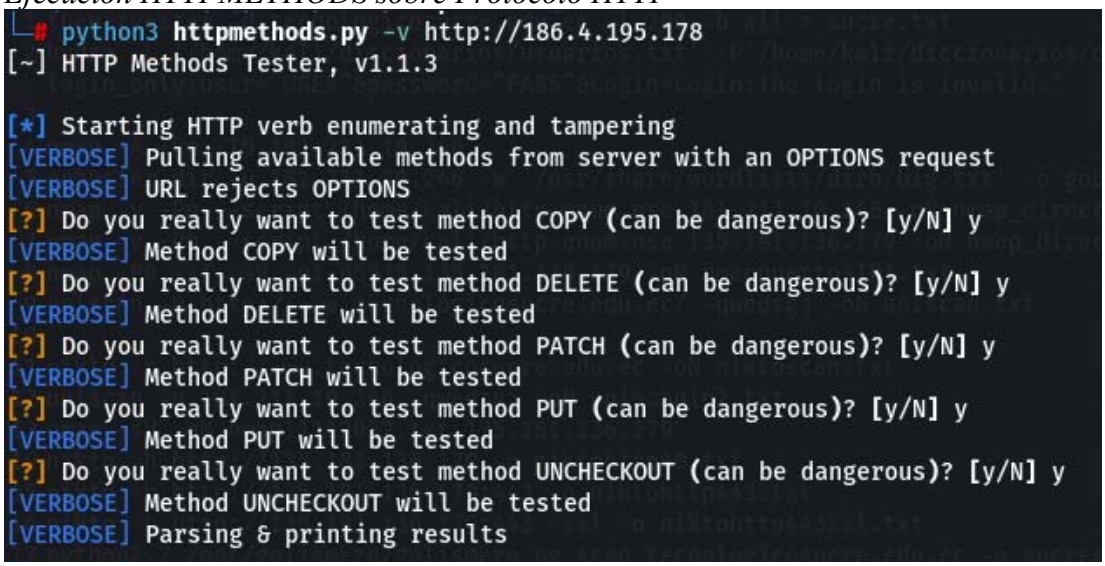


Fuente: Elaboración propia

Por medio de la herramienta Httpmethods, instalado en Kali Linux, se ejecutó un escaneo de fuerza bruta para determinar qué métodos de HTTP se encuentran habilitados en el equipo con IP 186.4.195.178. Las Figuras 37 y 38 presentan los resultados de este ataque de fuerza bruta, el cual reveló que el protocolo HTTP tiene habilitados muchos métodos, tal como lo describe OWASP Foundation (2022).

Figura 37

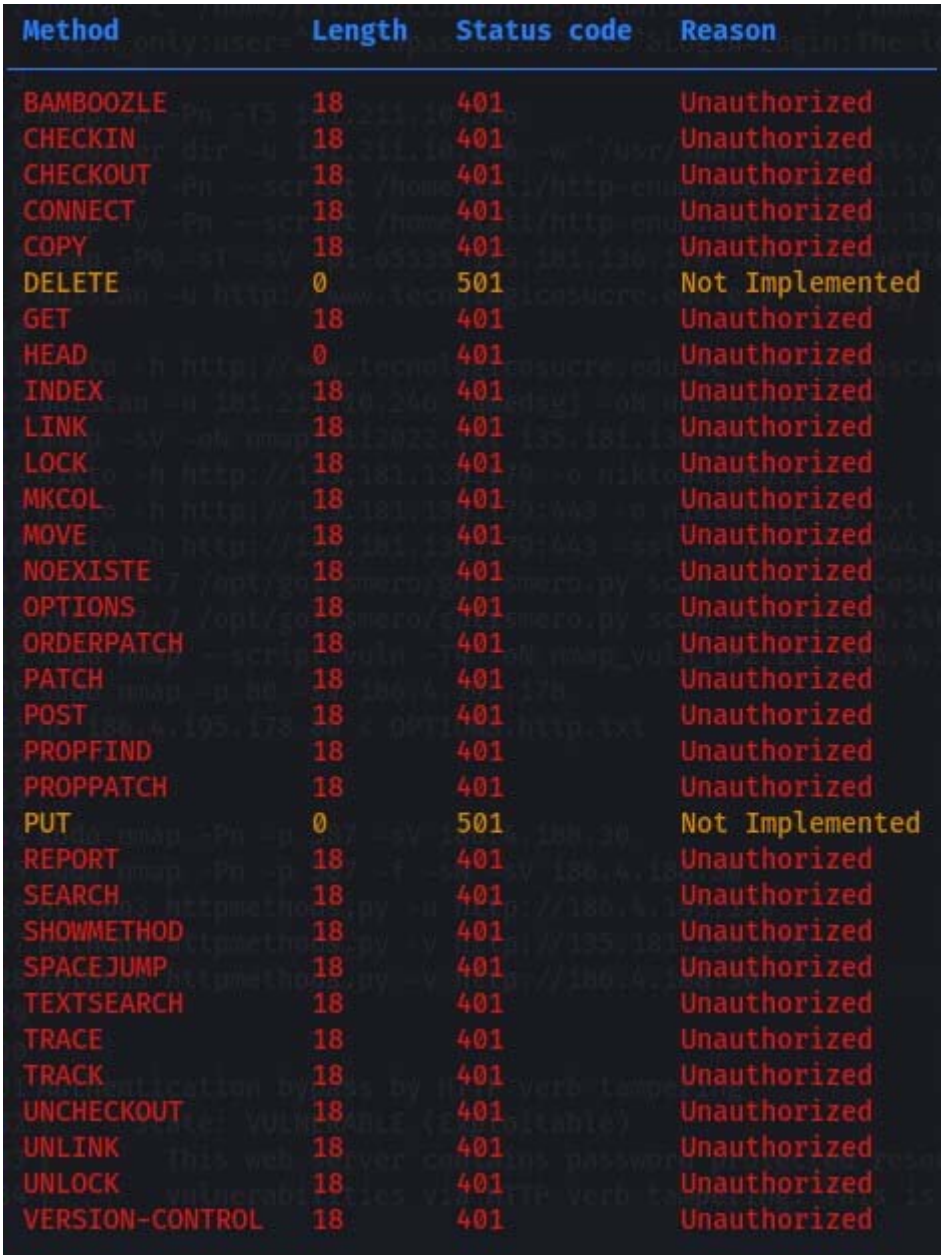
Ejecución HTTPMETHODS sobre Protocolo HTTP



Fuente: Elaboración propia. Ejecución de herramienta para determinar por fuerza bruta que métodos de respuesta tiene habilitados el protocolo HTTP en el equipo con IP 186.4.195.178

Figura 38

Resultado HTTPMETHODS



Method	Length	Status code	Reason
BAMBOOZLE	18	401	Unauthorized
CHECKIN	18	401	Unauthorized
CHECKOUT	18	401	Unauthorized
CONNECT	18	401	Unauthorized
COPY	18	401	Unauthorized
DELETE	0	501	Not Implemented
GET	18	401	Unauthorized
HEAD	0	401	Unauthorized
INDEX	18	401	Unauthorized
LINK	18	401	Unauthorized
LOCK	18	401	Unauthorized
MKCOL	18	401	Unauthorized
MOVE	18	401	Unauthorized
NOEXISTE	18	401	Unauthorized
OPTIONS	18	401	Unauthorized
ORDERPATCH	18	401	Unauthorized
PATCH	18	401	Unauthorized
POST	18	401	Unauthorized
PROPFIND	18	401	Unauthorized
PROPPATCH	18	401	Unauthorized
PUT	0	501	Not Implemented
REPORT	18	401	Unauthorized
SEARCH	18	401	Unauthorized
SHOWMETHOD	18	401	Unauthorized
SPACEJUMP	18	401	Unauthorized
TEXTSEARCH	18	401	Unauthorized
TRACE	18	401	Unauthorized
TRACK	18	401	Unauthorized
UNCHECKOUT	18	401	Unauthorized
UNLINK	18	401	Unauthorized
UNLOCK	18	401	Unauthorized
VERSION-CONTROL	18	401	Unauthorized

Fuente: Elaboración propia. Métodos de respuesta que tiene habilitados el protocolo HTTP en el equipo con IP 186.4.195.178

4.8.Resultados Obtenidos

Una vez ejecutadas las fases del pentesting de recopilación de información, análisis y detección de vulnerabilidades y explotación, se ha podido determinar, tal como, se presenta en la Tabla 7 que en la red de servidores y servicios del Instituto Superior Tecnológico Sucre existen 16 vulnerabilidades con niveles de severidad entre críticas, altas, medias y bajas, así mismo, se tienen 20 vulnerabilidades que son de nivel informativas que aunque no representan un riesgo para el Instituto pueden ser tomadas a consideración para su análisis en un futuro.

Tabla 7

Detalle de Vulnerabilidades Encontradas

Ítem	Vulnerabilidad	Nivel de Severidad	Proceso Afectado / No Ejecutado
1	http-method-tamper	Crítico	Seguridad de la información Gestión del riesgo Continuidad del negocio
2	SSL - Cross Site Scripting CSS	Crítico	Seguridad de la información Gestión del riesgo Continuidad del negocio
3	SSL Version 2 and 3 Protocol Detection	Crítico	Seguridad de la información Gestión del riesgo Continuidad del negocio
4	Cisco IOS IKEv1 Packet Handling Remote Information Disclosure (ciscosa-20160916-ikev1) (BENIGNCERTAIN) (uncredentialed check)	Alto	Seguridad de la información Gestión del riesgo Continuidad del negocio
5	SSL Certificate Signed Using Weak Hashing Algorithm	Alto	Seguridad de la información Gestión del riesgo Continuidad del negocio

Ítem	Vulnerabilidad	Nivel de Severidad	Proceso Afectado / No Ejecutado
6	SSL Medium Strength Cipher Suites Supported (SWEET32)	Alto	Seguridad de la información Gestión del riesgo Continuidad del negocio
7	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Medio	Seguridad de la información Gestión del riesgo
8	SSL Certificate Cannot Be Trusted	Medio	Seguridad de la información Gestión del riesgo
9	SSL Self-Signed Certificate	Medio	Seguridad de la información Gestión del riesgo
10	TLS Version 1.0 Protocol Detection	Medio	Seguridad de la información Gestión del riesgo
11	Unencrypted Telnet Server	Medio	Seguridad de la información Gestión del riesgo Continuidad del negocio
12	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medio	Seguridad de la información Gestión del riesgo
13	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Medio	Seguridad de la información Gestión del riesgo
14	SSL Weak Cipher Suites Supported	Medio	Seguridad de la información Gestión del riesgo
15	SSL Certificate Chain Contains Weak RSA Keys	Medio	Seguridad de la información Gestión del riesgo
16	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Bajo	Seguridad de la información Gestión del riesgo

Fuente: Elaboración propia

Tal como, lo determinaron Cruz et al. (2020) y Galarza García (2020) en sus estudios, la utilización de las herramientas Nmap, Kali Linux, Nessus entre otras, ayudó a determinar la existencia de 16 vulnerabilidades y entre ellas 3 catalogadas como críticas, que afectan a la red de servidores y servicios del instituto.

Se debe señalar que además de las vulnerabilidades encontradas a través de las pruebas de penetración, también se cuenta con vulnerabilidades que fueron expuestas por el Coordinador Gestión de la Información del Instituto Superior Tecnológico Sucre, las cuales son: no contar con un firewall, no contar con Vlans y ACLs, no contar con una política para la generación de contraseñas y no contar con una política para el acceso a Internet, al ser los usuarios uno de los mayores generadores de riesgo que puede tener una organización, estas vulnerabilidades pueden ser catalogadas como críticas.

4.9.Plan de Mejora para Mitigar las Vulnerabilidades Existentes

Una vez realizado el análisis y conocidas las vulnerabilidades que afectan a la red de servidores y servicios del Instituto Superior Tecnológico Sucre, en la Tabla 8 se presentan las mejoras e implementaciones que el Instituto si así lo desea puede implementar en su infraestructura tanto física como lógica, con la finalidad de mitigar las vulnerabilidades detectadas y su nivel de impacto.

Tabla 8

Recomendaciones para Mitigar las Vulnerabilidades Existentes

Ítem	Vulnerabilidad	Proceso Afectado / No Ejecutado	Recomendación
1	No contar con un firewall	Gobernanza de las TIC Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe implementar un firewall para garantizar la seguridad perimetral de la red. Ya que un firewall va a permitir cerrar todos los puertos de forma automática, y abrir únicamente los que se necesiten en un momento determinado. Considerando que el Instituto no cuenta con el presupuesto para invertir en un Firewall de hardware, se recomienda realizar la implementación de un firewall virtual o de nube, ya que al ser

Ítem	Vulnerabilidad	Proceso Afectado / No Ejecutado	Recomendación
			basados en software o ambientes virtualizados brindan la misma seguridad que uno físico, aunque se debe tomar en cuenta que al ser un software está sujeto igual a ser vulnerado si no se lo implementa con todas las medidas de seguridad a ser consideradas (Palo Alto Networks, 2022; Toumi et al., 2019).
2	No contar con Vlans y ACLs	Gobernanza de las TIC Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe segmentar la red con VLANs por grupos de usuarios a utilizar la red y servicios del Instituto, además, de habilitar ACLs que permitan controlar el tráfico en la red interna, con lo cual, se asegurará que cada usuario accede únicamente a la red y servicios que le estén permitidos. Para realizar las configuraciones requeridas se puede consultar las guías de Cisco para crear Vlans y configurar ACLs (CISCO, 2022b, 2022c).
3	No contar con una política para la generación de contraseñas	Gobernanza de las TIC Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe levantar una política para la generación de contraseñas que le permita a los usuarios conocer cuáles son las consideraciones que deben tener en cuenta el momento que generen las mismas. Además de los lineamientos que el Instituto considere importantes incluir dentro de la política se pueden considerar los siguientes para la generación y manejo de contraseñas robustas y seguras: Una contraseña robusta deberá tener las siguientes características: - Deberá contener mínimo 8 caracteres como máximo 128. - Deberá contener mayúsculas, minúsculas, números y caracteres especiales. - No puede contener datos personales como nombres, números telefónicos y fechas

Ítem	Vulnerabilidad	Proceso Afectado / No Ejecutado	Recomendación
			importantes ya sean propias o de familiares. - No pueden tener una secuencia lógica como por ejemplo una cadena de números o letras secuenciales. - No se pueden usar palabras que se encuentren fácilmente en el diccionario. - No se puede usar como contraseña el mismo usuario de acceso a la aplicación. Para el manejo o gestión de las contraseñas se deben tener en cuenta las siguientes recomendaciones: - No se puede utilizar la misma contraseña para varios servicios o aplicaciones. - No se deben escribir las contraseñas en post it o cualquier papel y dejarlas a la vista de todos. - No se puede compartir la contraseña con ninguna otra persona ya sea familiar o compañero de trabajo de confianza. - Se debe cambiar la contraseña de manera periódica. - Para evitar que se olviden las contraseñas creadas se pueden utilizar reglas mnemotécnicas que permitan recordarlas de manera fácil (Pincay Romero, 2021).
4	No contar con una política para el acceso a Internet	Gobernanza de las TIC Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe generar una política para el acceso a Internet donde además de los lineamientos dados por el Mintel como ente rector de las telecomunicaciones, se deberán tener en cuenta las siguientes consideraciones para generar una buena política: - La elaboración, administración y custodia del documento debe estar bajo la responsabilidad de una persona que tenga el

Ítem	Vulnerabilidad	Proceso Afectado / No Ejecutado	Recomendación
			conocimiento y la experiencia en temas de seguridad informática. - La elaboración del documento se hará en conjunto con un grupo de personas delegadas y que estarán lideradas por la máxima autoridad del Instituto. - Para la elaboración del documento se deben conocer las políticas de seguridad establecidas en el Instituto. - El documento debe contar con la descripción detallada de lo que está o no permitido al momento de acceder al Internet. - El documento debe detallar el cuidado que se debe tener con los equipos que se utilizan para acceder al Internet. - El documento debe detallar de manera clara cuáles serán las consecuencias y penalizaciones por incumplir la política. - Una vez elaborada la política deberá ser firmada por todos los involucrados y deberá ser puesta en conocimiento de todo el personal, de manera directa a través de charlas y capacitaciones que les permitan a los usuarios tomar conocimiento y hacer un uso correcto de la misma. - El documento en todo momento debe estar al alcance de todo el personal del Instituto. - El documento debe estar en un formato que impida su edición por parte de los usuarios (Pincay Romero, 2021).
5	http-method-tamper	Seguridad de la información Gestión del riesgo Continuidad del negocio	Un ataque por la manipulación de verbos de HTTP es aprovechado cuando existe un fallo en la configuración del método de control de acceso, por lo cual, para solventar esta vulnerabilidad se debe reducir

Ítem	Vulnerabilidad	Proceso Afectado / No Ejecutado	Recomendación
			al máximo los métodos HTTP utilizados en el servidor web, además, se debe configurar y activar la autenticación para todos los métodos HTTP habilitados. La reducción de la cantidad de métodos HTTP a habilitar se lo puede realizar levantando una restricción para los métodos que no se vayan a utilizar en el archivo web.xml (IBM, 2022).
6	SSL - Cross Site Scripting CSS o XSS	Seguridad de la información Gestión del riesgo Continuidad del negocio	Utilizar frameworks seguros que, por diseño, automáticamente codifiquen el contenido para prevenir XSS. Codificar los datos de requerimientos HTTP no confiables en los campos de salida HTML. Aplicar codificación sensitiva al contexto, cuando se modifica el documento en el navegador del cliente, ayuda a prevenir XSS DOM. Habilitar una Política de Seguridad de Contenido (CSP) (Gupta & Chaudhary, 2020).
7	SSL Version 2 and 3 Protocol Detection	Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe desactivar SSL 2.0 y 3.0. Además, en lugar de estas versiones se puede utilizar TLS 1.2 (con suites de cifrado aprobadas) o superior (Nessus - Tenable, 2022).
8	Cisco IOS IKEv1 Packet Handling Remote	Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe actualizar a una versión donde se corrija esta vulnerabilidad. Para conocer las versiones aplicables se puede consultar la referencia en el ID de error de Cisco CSCvb29204 (CISCO, 2022a; Nessus - Tenable, 2022).
9	SSL Certificate Signed Using Weak Hashing Algorithm	Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe solicitar a la autoridad certificadora que se vuelva a emitir el certificado SSL (Nessus - Tenable, 2022).

Ítem	Vulnerabilidad	Proceso Afectado / No Ejecutado	Recomendación
10	SSL Medium Strength Cipher Suites Supported (SWEET32)	Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe reconfigurar la aplicación afectada, con la finalidad de evitar que se usen cifrados de fuerza media (Nessus - Tenable, 2022).
11	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	Seguridad de la información Gestión del riesgo	Se debe deshabilitar SSLv3, así mismo, si existen servicios que trabajen con SSLv3 deberá habilitarse en dichos servicios TLS Fallback SCSV hasta que SSLv3 pueda ser deshabilitado (Nessus - Tenable, 2022).
12	SSL Certificate Cannot Be Trusted	Seguridad de la información Gestión del riesgo	Se debe comprar o generar un nuevo certificado SSL que sea el apropiado para el servicio (Nessus - Tenable, 2022).
13	SSL Self-Signed Certificate	Seguridad de la información Gestión del riesgo	Se debe comprar o generar un nuevo certificado SSL que sea el apropiado para el servicio (Nessus - Tenable, 2022).
14	TLS Version 1.0 Protocol Detection	Seguridad de la información Gestión del riesgo	Se debe habilitar el soporte para TLS 1.2 y 1.3, y deshabilitar el soporte para TLS 1.0 (Nessus - Tenable, 2022).
15	Unencrypted Telnet Server	Seguridad de la información Gestión del riesgo Continuidad del negocio	Se debe deshabilitar la conexión por Telnet y habilitar la conexión por SSH (Nessus - Tenable, 2022).
16	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Seguridad de la información Gestión del riesgo	Se debe reconfigurar la aplicación afectada, con lo cual se busca evitar el uso de cifrados RC4. Si se desea se puede implementar TLS 1.2 con suites AES-GCM sujeto al soporte del navegador y del servidor web (Nessus - Tenable, 2022).
17	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	Seguridad de la información Gestión del riesgo	Se debe deshabilitar el modo agresivo si es compatible, no se debe utilizar la clave precompartida para la autenticación y en el caso de que no se pueda evitar su uso se deben generar claves fuertes, además, se deben bloquear las conexiones por VPN (Nessus - Tenable, 2022).

Ítem	Vulnerabilidad	Proceso Afectado / No Ejecutado	Recomendación
18	SSL Weak Cipher Suites Supported	Seguridad de la información Gestión del riesgo	Se debe volver a configurar la aplicación vulnerable con la finalidad de permitir el uso únicamente de cifrados fuertes (Nessus - Tenable, 2022).
19	SSL Certificate Chain Contains Weak RSA Keys	Seguridad de la información Gestión del riesgo	Se debe reemplazar el certificado de clave RSA débil por uno que contenga una clave más fuerte, luego de lo cual, se deben volver a generar los certificados que ya hayan sido firmados (Nessus - Tenable, 2022).
20	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	Seguridad de la información Gestión del riesgo	Se debe reemplazar el certificado de clave RSA de menos de 2048 bits de longitud por una clave más larga, además, se debe volver a generar los certificados que ya hayan sido firmados (Nessus - Tenable, 2022).

Fuente: Elaboración propia

Todas estas recomendaciones se basan en las normativas, estándares y marcos de referencia sobre seguridad de la información descritas en el Capítulo II, es así que, si el Instituto lo desea puede aplicar una o la combinación de varias de estas normativas, con lo cual, además de mitigar las vulnerabilidades existentes podrá obtener un nivel de seguridad de la información acorde a lo que dispone el MINTEL a través del EGSI. En la Tabla 9 se detallan las normativas, estándares y marcos de referencia que se le recomienda al Instituto aplicar.

Tabla 9

Recomendaciones de Norma/Estándar/Marco Teórico Aplicable

Ítem	Proceso Afectado / No Ejecutado	Norma / Estándar / Marco Teórico Aplicable	Justificación
1	Gobernanza de las TIC	COBIT 2019 ITILv4 NIST CSF	Una correcta gobernanza de las TIC, le permitirá al Instituto ofrecer servicios de calidad a la ciudadanía, asegurándose además de contar con un control y gestión de sus TIC. Aun cuando NIST CSF es aplicable a entidades del sector privado, esto no

Ítem	Proceso Afectado / No Ejecutado	Norma / Estándar / Marco Teórico Aplicable	Justificación
			impide que el Instituto lo pueda tomar como referencia de buenas prácticas.
2	Seguridad de la información	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 15408-1	El Instituto al ser una entidad pública debe regirse a las disposiciones del Gobierno Central y por ende a las disposiciones que por temas de seguridad emita el MINTEL, es así que con la aplicación de estas normas el Instituto estará dando cumplimiento a lo dispuesto por el MINTEL a través del EGSI, además de asegurar y proteger sus redes y sistemas de ataques cibernéticos.
3	Gestión del riesgo	ISO/IEC 27005 ISO 31000	La garantía de obtener una gobernanza de TIC y una seguridad de la información exitosos radica en realizar una adecuada gestión de los riesgos. Con la utilización de estas normativas el Instituto se asegura además de cumplir de manera adecuada con lo dispuesto por el MINTEL.
4	Continuidad del negocio	ISO/IEC 27031	El Instituto puede asegurarse y mantener una constante vigilancia de que está cumpliendo con los objetivos estratégicos para garantizar la continuidad de su negocio a través de la utilización e implementación de esta normativa, misma que debe aplicarse en conjunto con las anteriormente ya descritas.

Fuente: Elaboración propia

4.10. Informes Ejecutivo y Técnico

4.10.1. Informe Ejecutivo

El informe ejecutivo presentado a la máxima autoridad del Instituto Superior Tecnológico Sucre consta de las siguientes partes:

Asunto: Informe Ejecutivo "DETECCIÓN DE VULNERABILIDADES MEDIANTE PRUEBAS DE PENETRACIÓN A LA RED DE SERVIDORES Y SERVICIOS DEL INSTITUTO SUPERIOR TECNOLÓGICO SUCRE"

Objetivo: Desarrollar un plan de mejoras que permita mitigar las vulnerabilidades identificadas mediante la ejecución de pruebas de penetración en la red de servidores y servicios del Instituto Superior Tecnológico Sucre.

Antecedentes: Con la situación de emergencia que vivió el país, muchas instituciones se vieron en la necesidad imperiosa de llevar sus oficinas al hogar de sus colaboradores para mantener la continuidad de sus negocios, lo cual, ha conllevado a que pongan más interés en reforzar sus seguridades en la red; y en este ámbito el Instituto Superior Tecnológico Sucre no se quiere quedar atrás, y desea brindar a su personal administrativo, docente y estudiantil una infraestructura tecnológica de calidad, eficiente pero sobre todo segura; lo que ha generado la necesidad de conocer las vulnerabilidades que actualmente afectan a la red de servidores y servicios de dicho IST Sucre.

Mediante correo electrónico de 05 de julio de 2021, se solicitó al PhD. Santiago Illescas, RECTOR INSTITUTO SUPERIOR TECNOLÓGICO SUCRE, la autorización para desarrollar en el Instituto el trabajo de titulación con tema: "Detección de vulnerabilidades mediante pruebas de penetración a la red de servidores y servicios del Instituto Superior Tecnológico Sucre", requisito para obtener el título de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones.

Mediante correo electrónico de 07 de julio de 2021, el Instituto Superior Tecnológico Sucre da la autorización para desarrollar el trabajo de titulación.

Desarrollo de Pruebas: Una vez que se firmó el acuerdo entre el Coordinador Gestión de la Información del Instituto Superior Tecnológico Sucre y la autora de este trabajo de titulación MARIA ELIZABETH CEDEÑO ZAMBRANO denominado "DOCUMENTO DE AUTORIZACIÓN PARA REALIZACIÓN DE PRUEBAS DE PENTESTING", las pruebas de penetración fueron realizadas en el periodo de tiempo descrito en la Tabla 10.

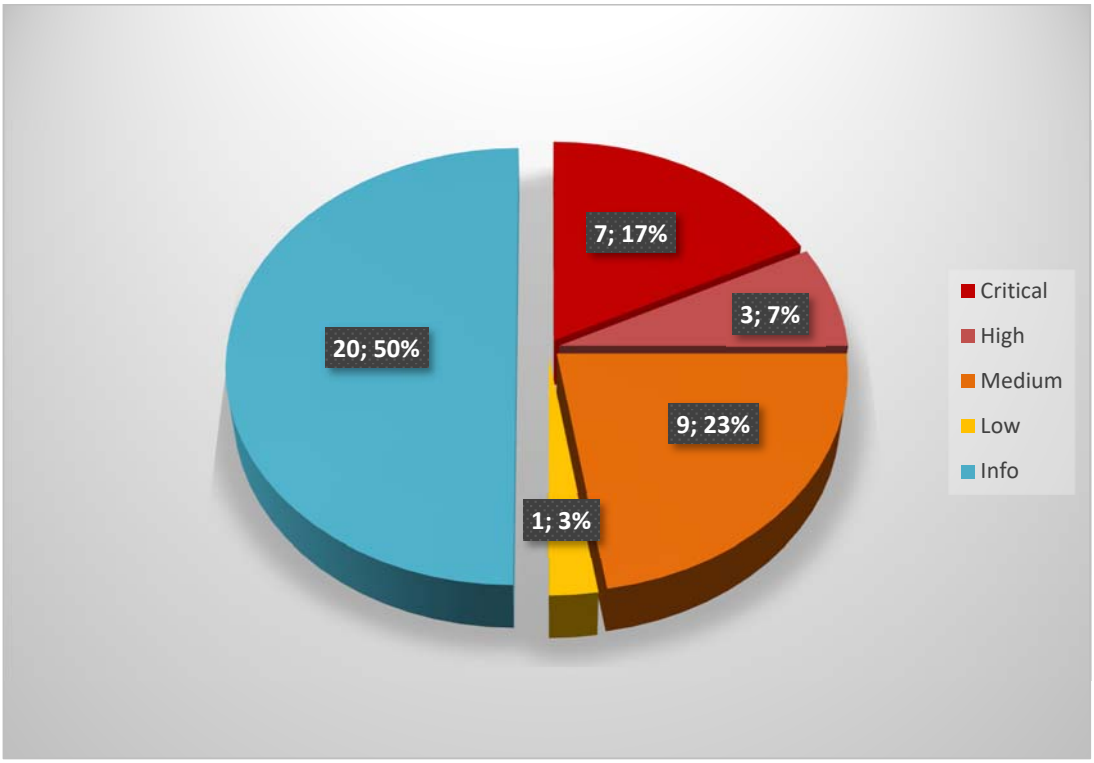
Tabla 10
Periodo de Ejecución de Pruebas de Penetración

Actividad	Fecha de Inicio	Fecha de Fin
Ejecución de pruebas de penetración a la red de servidores y servicios del Instituto Superior Tecnológico Sucre	22 de agosto de 2022	13 de noviembre de 2022

Presentación de Resultados: En la Figura 39 se presenta el resumen de las vulnerabilidades encontradas de acuerdo a su nivel de severidad o criticidad.

Figura 39

Detalle de Vulnerabilidades Encontradas



Estos niveles de severidad o criticidad han sido catalogados de acuerdo al catálogo de niveles detallado en la Tabla 11.

Tabla 11

Niveles de Criticidad de las Vulnerabilidades

Clasificación	**Descripción**
Crítico	La explotación de la vulnerabilidad podría poner en riesgo la disponibilidad, integridad y confidencialidad de la información de la organización. Su explotación es sencilla ya que la página web o el recurso analizado tienen niveles de seguridad bajos o en algunos casos no los tiene.
Alto	La explotación podría provocar el robo de información sensible y tiempos altos de indisponibilidad del servicio. Su explotación es difícil de realizar, pero una vez realizada podría dar acceso a niveles con privilegios elevados.
Medio	Para la explotación de estas vulnerabilidades el atacante debe realizar ingeniería social para obtener información que le permita acceder a la red de su víctima, además, para realizar su ataque debe encontrarse dentro de la organización. El nivel de infiltración que logra realizar es mínimo.
Bajo	Este tipo de vulnerabilidades no implican un riesgo considerable para la organización. Para explotarlas el atacante debe estar

	físicamente conectado dentro de la red de su víctima, para lograr acceso a sus servicios.
Info	Este tipo de vulnerabilidades no representan un riesgo para la organización, únicamente dan información de acciones que si la organización lo considera apropiado puede tomar para asegurar aún más sus sistemas y servicios.

Nota. Adaptado de *Tenable.io User Guide - Scan Notes Severity Details in WAS,* Tenable.io, 2022, Pág. 376-377

Análisis de Resultados: De acuerdo a lo indicado en la Figura 39 existen 7 vulnerabilidades de nivel crítico y 3 de nivel alto que pueden generar una afectación severa a la red de servidores y servicios del Instituto Superior Tecnológico Sucre sino se las mitiga de forma inmediata. Existen además 9 vulnerabilidades catalogadas como medias y 1 de nivel bajo que, aunque no representan un riesgo inmediato igual deben ser analizadas y corregidas.

Plan de Mejora Propuesto: Entre las actividades más urgentes y primordiales que se recomienda que el Instituto realice para mitigar las vulnerabilidades encontradas, se encuentran las siguientes:

- Adquirir un firewall o implementar uno virtual.
- Establecer configuraciones de Vlans y ACLs en sus equipos de comunicación, como switches y routers.
- Establecer una política para la generación de contraseñas robustas
- Establecer una política para el acceso a Internet.
- Actualizar los certificados de encriptación de datos.
- Solicitar a sus proveedores de los servicios de Dominio, Pagina Web e Internet las políticas que están implementando para garantizar la integridad, disponibilidad y confidencialidad de la información que es propiedad del Instituto.

En base a las vulnerabilidades encontradas, se recomienda que el Instituto tome como referencia de mejores prácticas e implemente las normativas, estándares y marcos de referencia descritas en la Tabla 12.

Tabla 12

Recomendaciones de Norma/Estándar/Marco Teórico Aplicable

Ítem	Proceso Afectado / No Ejecutado	Norma / Estándar / Marco Teórico Aplicable	Justificación
1	Gobernanza de las TIC	COBIT 2019 ITILv4 NIST CSF	Una correcta gobernanza de las TIC, le permitirá al Instituto ofrecer servicios de calidad a la ciudadanía, augurándose además de contar con un control y gestión de sus TIC. Aun cuando NIST CSF es aplicable a entidades del sector privado, esto no impide que el Instituto lo pueda tomar como referencia de buenas prácticas.
2	Seguridad de la información	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 15408-1	El Instituto al ser una entidad pública debe regirse a las disposiciones del Gobierno Central y por ende a las disposiciones que por temas de seguridad emita el MINTEL, es así que con la aplicación de estas normas el Instituto estará dando cumplimiento a lo dispuesto por el MINTEL a través del EGSI, además de asegurar y proteger sus redes y sistemas de ataques cibernéticos.
3	Gestión del riesgo	ISO/IEC 27005 ISO 31000	La garantía de obtener una gobernanza de TIC y una seguridad de la información exitosos radica en realizar una adecuada gestión de los riesgos. Con la utilización de estas normativas el Instituto se asegura además de cumplir de manera adecuada con lo dispuesto por el MINTEL.
4	Continuidad del negocio	ISO/IEC 27031	El Instituto puede asegurarse y mantener una constante

Ítem	Proceso Afectado / No Ejecutado	Norma / Estándar / Marco Teórico Aplicable	Justificación
			vigilancia de que está cumpliendo con los objetivos estratégicos para garantizar la continuidad de su negocio a través de la utilización e implementación de esta normativa, misma que debe aplicarse en conjunto con las anteriormente ya descritas.

Fuente: Elaboración propia

Conclusión: La propuesta planteada en este estudio es una alternativa muy adecuada que le permite al Instituto Superior Tecnológico Sucre mejorar a futuro las seguridades de su infraestructura tecnológica garantizando mantener la confidencialidad, integridad y disponibilidad de la información y asegurando además de darle continuidad al negocio.

Recomendaciones: Se sugiere que el Instituto Superior Tecnológico Sucre aplique e implemente las normativas, estándares y marcos de referencia propuestos en este estudio. Además, se recomienda que se realicen análisis de vulnerabilidades de manera periódica con la finalidad de mantener actualizada la lista de las vulnerabilidades que pueden afectar a su red e infraestructura en determinado momento.

4.10.2. Informe Técnico

Por temas de confidencialidad el informe técnico que contiene la información completa de los resultados obtenidos en el presente trabajo, será entregado únicamente al Instituto Superior Tecnológico Sucre.

CAPÍTULO V
CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS

5.1.Conclusiones

Conocer de antemano el estado del arte sobre pruebas de penetración y detección de vulnerabilidades realizadas por otros investigadores permitió identificar de forma adecuada y en un tiempo considerable los riesgos tanto físicos como lógicos, a los que está expuesta la red del Instituto Superior Tecnológico Sucre.

La ejecución de pruebas de penetración en la red de servidores y servicios del Instituto Superior Tecnológico Sucre, permitió desarrollar un plan de mejoras que permitirá mitigar las vulnerabilidades identificadas.

La propuesta planteada en este estudio es una alternativa muy adecuada que le permite al Instituto Superior Tecnológico Sucre mejorar a futuro las seguridades de su infraestructura tecnológica garantizando mantener la confidencialidad, integridad y disponibilidad de la información.

El principal inconveniente o limitación con el que se enfrenta actualmente el Instituto Superior Tecnológico Sucre, es que no cuenta con los recursos económicos necesarios que le permitan tomar acciones correctivas de manera inmediata sobre las vulnerabilidades que afectan su red y así poder implementar las mejoras sugeridas en este estudio, sin embargo, a futuro podría afrontarse esta dificultad levantando proyectos de tesis entre los estudiantes del mismo instituto, donde se les permita generar proyectos de titulación que vayan enfocados a atacar estas vulnerabilidades con recursos propios de la institución y basados en software libre.

5.2.Recomendaciones

Se recomienda que el Instituto Superior Tecnológico Sucre realice todas las gestiones que considere pertinentes a fin de que pueda presentar ante el MINTEL el proyecto de TIC que le permita mejorar su infraestructura tecnológica.

Se sugiere que el Instituto Superior Tecnológico Sucre aplique e implemente las normativas, estándares y marcos de referencia propuestos en este estudio, lo cual, además le permitirá dar cumplimiento a las disposiciones emitidas por el MINTEL.

Para que el Instituto Superior Tecnológico Sucre pueda mitigar las vulnerabilidades que afectan actualmente a su red de servidores y servicios, cuando lo desee, puede implementar las acciones correctivas que se proponen en este estudio.

Se recomienda que el Instituto realice análisis de vulnerabilidades de manera periódica con la finalidad de mantener actualizada la lista de las vulnerabilidades que pueden afectar a su red e infraestructura en determinado momento.

5.3. Bibliografía

Arun, S., & Bijimol, T. K. (2021). A Research Work on Information Gathering Tools. *Proceedings of the National Conference on Emerging Computer Applications (NCECA)*, 118.

Asad, H., & Gashi, I. (2022). Dynamical Analysis of Diversity in Rule-Based Open Source Network Intrusion Detection Systems. *Empirical Software Engineering*, *27*(1), 4.

Bolaños Botina, J. (2018). *Diseño de la arquitectura de seguridad perimetral de la red informática en la Industria de Licores del Valle*.

Briceño, E. V. (2021). *SEGURIDAD DE LA INFORMACIÓN* (3ciencias (ed.); 1ra ed.).

Chergui, M., & Chakir, A. (2020). IT Governance Knowledge: From Repositories to Artificial Intelligence Solutions. *Journal of Engineering Science \& Technology Review*, *13*(5).

Cifuentes-Leiton, D. M., & Londoño-Cardozo, J. (2020). Teletrabajo: el problema de la institucionalización. *Aibi Revista de Investigación, Administración e Ingeniería*, *8*(1), 12–20.

CISCO. (2022a). *Cisco Bug: CSCvb29204*.

CISCO. (2022b). *Configurar ACL de IP de uso general*. CISCO.

CISCO. (2022c). *Creating Ethernet VLANs on Catalyst Switches*.

Coronel, I. A. (2017). *Aplicar hackeo ético para detección de vulnerabilidades mediante herramientas Open Source en las aplicaciones web de una institución de educación superior*. Espol.

Cruz, M. A., Ibarra, M., Carrasco, W. L., IlasacaCahuata, E., Chahuaya, J. A. S., & Apaza-Tarqui, A. (2020). Use of exploit for vulnerability detection of Linux Servers. *KnE Engineering*, 138–149.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). COBIT as a Framework for Enterprise Governance of IT. In *Enterprise governance of information technology* (pp. 125–162). Springer.

EcuCERT. (2022). *EcuCERT*. https://www.ecucert.gob.ec/

Galarza García, D. E. (2020). *Estrategia para la evaluación de vulnerabilidades del sistema de notas de instituciones educativas utilizando técnicas de hacking ético. caso de estudio: Instituto Tecnológico Quito*. Quito, 2020.

Giannone, A. O. (2019). *Método de inclusión de hacking ético en el proceso de testing de software.*

GitHub. (2022a). *Gobuster*. https://github.com/OJ/gobuster

GitHub. (2022b). *httpmethods*. https://github.com/ShutdownRepo/httpmethods

GitHub. (2022c). *theHarvester*. https://github.com/laramies/theHarvester

Grant, J. (2019). *Hackeo Ético: Guia completa para principiantes para aprender y comprender el concepto de hacking ético*. Amazon Digital Services LLC - Kdp.

Gupta, B. B., & Chaudhary, P. (2020). *Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures* (1st ed.). CRC Press.

Gutierrez, P. (2018). *Hacker's WhiteBook*. Independently published.

Guzman, A., & Gupta, A. (2017). *IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices*. Packt Publishing Ltd.

Harper, A., Linn, R., Sims, S., Baucom, M., Tejeda, H., Fernandez, D., & Frost, M. (2022). *Gray Hat Hacking: The Ethical Hacker's Handbook, Sixth Edition* (6th ed.). McGraw-Hill Companies.

Huamantingo Navarro, R. R. (2022). *Modelo para el análisis de vulnerabilidades digitales en una entidad pública de Lima, 2021*.

IBM. (2022). *Restricción del uso de métodos HTTP*. https://www.ibm.com/docs/es/odm/8.11.0?topic=methods-restricting-use-http

Internet Assigned Numbers Authority IANA. (2022). *RFC 6409*.

IPAddress.com. (2022). *IPAddress.com*. https://www.ipaddress.com/

ISO/IEC. (2022a). *ISO/IEC 27000*.

ISO/IEC. (2022b). *ISO/IEC 27031*.

ISO/IEC. (2022c). *ISO 27001 - Seguridad de la información: norma ISO IEC 27001/27002*.

ISO. (2018). *ISO 31000* (ISO (ed.); 2nd ed.).

ISO. (2022). *ISO/IEC 15408-1:2022*.

ISO & IEC. (2022). *ISO standards are internationally agreed by experts*. https://www.iso.org/standards.html

Kim, P. (2018). *THE HACKER PLAYBOOK 3: Practical Guide to Penetration Testing* (K. Kim (ed.); 3ra ed.). Secure Planet LLC.

Mahecha, L. H. M. (2022). *Auditoría Forense.: Una guía práctica para la excelencia en la ciencia, auditoría e informática forense*. Ediciones de la U.

Microsoft. (2022). *nslookup*. Microsoft.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020a). *Esquema Gubernamental de Seguridad de la Información (EGSI)*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020b). *GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020c). *GUÍA PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *Evaluación de Proyectos TIC*. https://www.gobiernoelectronico.gob.ec/asesoria-evaluacion-y-aprobacion-de-proyectos/

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Aumento de Conexiones de Internet Fijo y Móvil, mejoran el acceso de Internet en Ecuador*. https://www.telecomunicaciones.gob.ec/aumento-de-conexiones-de-internet-fijo-y-movil-mejoran-el-acceso-de-internet-en-ecuador/

Najera-Gutierrez, G. (2019). *Improving your Penetration Testing Skills: Strengthen your defense against web attacks with Kali Linux and Metasploit* (1st, ed. ed.). Packt Publishing.

Narvaez Taranto, L. I. (2018). *GUÍA PRÁCTICA PARA REALIZAR AUDITORÍA A LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN CON ENFOQUE EN EL CONTROL INTERNO EN LAS INSTITUCIONES DEL ESTADO ECUATORIANO.*

Nessus - Tenable. (2022). *Vulnerabilities by Host: 186.4.195.178*.

OWASP Foundation. (2022). *WSTG - v4.1 | Testing for HTTP Verb Tampering*. https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/07-Input_Validation_Testing/03-Testing_for_HTTP_Verb_Tampering

Palo Alto Networks. (2022). *¿Qué es un firewall virtual?* https://www.paloaltonetworks.lat/cyberpedia/what-is-a-virtual-firewall

Paltán Orellana, H. A. (2019). *Desarrollo de un plan de mitigación de seguridad informática a una red inalámbrica de comunicación de datos para una institución privada, a través de la aplicación de hacking ético para la identificación de amenazas, riesgos y vulnerabilidades*.

Pincay Romero, K. G. (2021). Características de la conectividad a internet en el cantón Pasaje. *Revista Universidad y Sociedad*, *13*(3), 150–160.

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review*, *31*(3), 701–728.

Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, 1–3. https://doi.org/10.1109/NCETSTEA48365.2020.9119914

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. (2017). A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM). *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, 253–259.

Servicio Ecuatoriano de Normalización. (2022). *CATÁLOGO DE NORMAS TECNICAS INEN*.

SINGH, G. D. (2022). *THE ULTIMATE KALI LINUX BOOK : PERFORM ADVANCED PENETRATION TESTING USING NMAP, METASPLOIT, AIRCRACK-NG, AND EMPIRE*. PACKT PUBLISHING LIMITED.

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *JOIV: International Journal on Informatics Visualization*, *4*(4), 225–230.

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards-A Review and Comprehensive Overview. *Electronics*, *11*(14), 2181.

Tenable. (2022a). *Nessus*. https://es-la.tenable.com/products/nessus

Tenable. (2022b). *Tenable.io User Guide*. Tenable.

Toumi, H., Fagroud, F. Z., Zakouni, A., & Talea, M. (2019). Implementing Hy-IDS, mobiles agents and virtual firewall to enhance the security in IaaS Cloud. *Procedia Computer Science*, *160*, 819–824.

Wappalyzer. (2022). *Identify technologies on websites*. https://www.wappalyzer.com/

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Seguridad en informática: consideraciones. *Dominio de Las Ciencias*, *3*(3), 676–688.

5.4.Anexos

Anexo 1

Guion de Entrevista Utilizada

GUION DE ENTREVISTA ENCARGADO DE TI

Fecha:

Buenos días, mi nombre es Elizabeth Cedeño, al momento estoy en el proceso de obtener una Maestría en Tecnologías de la Información mención en Seguridad de Redes en la Universidad Técnica de Ambato, para lo cual me encuentro desarrollando un trabajo de titulación enfocado a detectar las vulnerabilidades que tiene la red de servidores y servicios del INSTITUTO SUPERIOR TECNOLÓGICO SUCRE con la finalidad de desarrollar un plan que permita mitigar dichas vulnerabilidades.

Con el propósito de tener claro el escenario del instituto a nivel de seguridad le solicito me ayude contestando las siguientes preguntas:

1. ¿Cuál es su nombre?

   —----------

   —----------

2. ¿Qué cargo ocupa en el instituto?

   —----------

   —----------

3. ¿Cuánto tiempo lleva ejerciendo este cargo dentro del instituto?

   —----------

   —----------

   ¿Con qué tipo de hardware de seguridad perimetral cuenta el instituto?

   —----------

   —----------

4. ¿Con qué tipo de configuraciones de seguridad perimetral cuenta el instituto?

   —----------

   —----------

5. ¿Cuenta el instituto con una política de generación de contraseñas seguras y robustas?

   —----------

   —----------

6. ¿Cuenta el instituto con una política de seguridad para el acceso a Internet?

   ——----------

   ——----------

7. ¿Qué seguridades tiene implementadas el instituto para el acceso a Internet?

   ——----------

   ——----------

8. ¿El dominio del instituto se encuentra alojado en un servidor externo?

   ——----------

   ——----------

9. ¿Conoce usted el estado actual de los riesgos y vulnerabilidades que afectan a la red de servidores y servicios del instituto?

   ——----------

   ——----------

——----------

Nombre y Firma del Entrevistado

Anexo 2

Lista de Cotejo Utilizada

LISTA DE COTEJO SEGURIDAD REDES

INSTITUCIÓN:

RESPONSABLE DE VALORACIÓN:

FECHA DE INICIO:

FECHA DE FIN:

PARÁMETRO	CUMPLE	NO CUMPLE	N/A
Existe un diagrama lógico de la red de servidores			
Se cuenta con hardware de seguridad perimetral			
Se cuenta con configuraciones de seguridad perimetral			
Se dispone de una política de generación de contraseñas seguras y robustas			
Se dispone de una política de seguridad para el acceso a Internet			
Se tienen implementadas seguridades para el acceso a Internet			
El Dominio está alojado en un servidor externo			
El dominio tiene implementado la seguridad de información del propietario			
El dominio cuenta con subdominios			
Los puertos abiertos son los estrictamente necesarios para el funcionamiento de los servicios que proveen			

Anexo 3

Correo de Autorización del Instituto Superior Tecnológico Sucre

Cedeño Zambrano Maria Elizabeth

From: Secretaria Tecnologico Sucre <secretaria@tecnologicosucre.edu.ec>
Sent: Wednesday, July 7, 2021 5:19 PM
To: Cedeño Zambrano Maria Elizabeth
Cc: DANILO MINIGUANO
Subject: DOC. ENVIADO: Solicitud de Autorización para Ejecutar Tema de Tesis María Cedeño
Attachments: Solicitud Autorización Ejecutar Tesis MariaCedeño-signed (2)-signed.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Estimada
Se pone en conocimiento que su solicitud fue aprobada.
Saludos Cordiales
Atentamente
RECTORADO

Instituto Superior Tecnológico SUCRE
Matriz | Av. 10 de Agosto N26-27 y Luis Mosquera Narváez
Campus Sur | Av. Teodoro Gómez de la Torre S14-72 y Joaquín Gutiérrez.
Campus Consejo Provincial | Av. Ajaví Oe4-154 y Cardenal de la Torre.
Telf.: 022547356 **Ext** 101 / 022910513
E- mail: secretaria@tecnologicosucre.edu.ec
Sitio web: **www.tecnologicosucre.edu.ec**

El mié, 7 jul 2021 a las 17:17, Alexandra Maza (<amaza@tecnologicosucre.edu.ec>) escribió:

---------- Forwarded message ---------
De: **Santiago Illescas** <sillescas@tecnologicosucre.edu.ec>
Date: lun, 5 jul 2021 a las 10:22
Subject: Fwd: Solicitud de Autorización para Ejecutar Tema de Tesis María Cedeño
To: Alexandra Maza <amaza@tecnologicosucre.edu.ec>

alexita para la firma de autorización

saludos

1

---------- Forwarded message ---------
De: **Cedeño Zambrano Maria Elizabeth** <mcedeno2971@uta.edu.ec>
Date: lun, 5 jul 2021 a las 10:06
Subject: Solicitud de Autorización para Ejecutar Tema de Tesis María Cedeño
To: sillescas@tecnologicosucre.edu.ec <sillescas@tecnologicosucre.edu.ec>
Cc: dminiguano@tecnologicosucre.edu.ec <dminiguano@tecnologicosucre.edu.ec>

Estimado PhD. Santiago Illescas

RECTOR INSTITUTO SUPERIOR TECNOLÓGICO SUCRE

Reciba un cordial saludo, mi nombre es MARÍA ELIZABETH CEDEÑO ZAMBRANO con documento de identidad Nro. 1714712971, estudiante de la Maestría en Tecnologías de la Información de la Universidad Técnica de Ambato, con la finalidad de cumplir con los requisitos de mi proceso de titulación, me permito solicitar la autorización para ejecutar en el Instituto Superior Tecnológico Sucre el tema de tesis, el cual, está enfocado de la siguiente manera:

Tema: **"Detección de vulnerabilidades mediante pruebas de penetración a la red de servidores y servicios del Instituto Superior Tecnológico Sucre".**

El objetivo de este tema es identificar las vulnerabilidades que tiene la red de servidores y servicios del Instituto Superior Tecnológico Sucre mediante la ejecución de pruebas de penetración, para posteriormente proponer un plan de mejora que permita mitigar la penetración de intrusos en dicha red.

Este tema se encuentra enfocado en la necesidad que fue planteada por la Unidad de Tecnologías de la Información y Comunicaciones (TIC) del Instituto que usted preside.

Al presente correo electrónico remito adjunta la carta de solicitud debidamente firmada para que pueda ser considerada.

Por la atención que pueda dar a la presente, anticipo mi agradecimiento.

Atentamente,

2

Ing. María Cedeño Z.

SUCRE
Instituto Superior Tecnológico

Instituto Superior Tecnológico SUCRE
Matriz | Av. 10 de Agosto N26-27 y Luis Mosquera Narváez
Campus Sur | Av. Teodoro Gómez de la Torre S14-72 y Joaquín Gutiérrez.
Campus Consejo Provincial| Av. Ajavi Oe4-154 y Cardenal de la Torre.
Telf.: 022547356 **Ext** 101 / 022910513
Sitio web: www.tecnologicosucre.edu.ec

Anexo 4

Documento de Autorización para Realización de Pruebas de Pentesting

1. Datos de autorización de pruebas de Pentesting

Institución: INSTITUTO SUPERIOR TECNOLÓGICO SUCRE
Nombre: Ing. Carlos Guevara
Puesto: Coordinador Gestión de la Información
Fecha: 19 de agosto de 2022

Autoriza a MARÍA ELIZABETH CEDEÑO ZAMBRANO para llevar a cabo las actividades de verificación de seguridad de la red de servidores y servicios del Instituto Superior Tecnológico Sucre que se describen a continuación, según las siguientes condiciones:

- Ámbito de las pruebas (Activos/servicios autorizados):
  - http://www.tecnologicosucre.edu.ec
  - 186.4.188.30
  - 186.4.195.178

- Condiciones:
  - Las pruebas serán externas y se realizarán desde fuera de la red del Instituto Superior Tecnológico Sucre utilizando Internet.
  - Se realizará un único TEST de penetración denominado Caja Negra, sobre los servicios autorizados por el Instituto Superior Tecnológico Sucre.
  - Las pruebas se realizarán fuera de horario laboral, preferiblemente en horas de la noche y la fecha de realización será acordada directamente con el Coordinador Gestión de la Información del Instituto Superior Tecnológico Sucre, sin necesidad de que exista una evidencia escrita de este acuerdo.

- Teléfonos de soporte en caso de presentarse novedades:
  - **Por parte del Instituto Superior Tecnológico Sucre:**
    - Nombre: Carlos Guevara Herrera
    - Teléfono: 0992731439
    - Email: cguevara@tecnologicosucre.edu.ec

  - **Ejecutor de Pruebas**:
    - Nombre: Elizabeth Cedeño Zambrano
    - Teléfono: 0998554539
    - Email: mcedeno2971@uta.edu.ec

2. Tipos de pruebas (Pentesting)

Para llevar a cabo este trabajo de detección de vulnerabilidades se realizará un **Test de Intrusión Externo,** el cual se ejecutará desde internet sobre la infraestructura del Instituto Superior Tecnológico Sucre, más concretamente, sobre los activos autorizados por el Instituto Superior Tecnológico Sucre y que están expuestos a internet.

Además, este test será del tipo **Intrusión de Caja Negra,** considerando que no se cuenta con mayor información, únicamente se cuenta con la URL e IPs públicas de los servicios a ser auditados y se desconoce la información relativa a arquitectura, usuarios/credenciales, etc.

Dada la naturaleza de los trabajos a realizar cabe la posibilidad de que, de forma no intencionada, se produjese algún efecto colateral indeseado. Si así fuese, el Ejecutor de las Pruebas lo notificará inmediatamente al Teléfono de soporte correspondiente o se pondría a disposición del Instituto Superior Tecnológico Sucre para aportar la información requerida sobre las acciones realizadas.

3. Conformidades

De conformidad con la concesión de esta autorización, el Instituto Superior Tecnológico Sucre declara que:

- El Instituto Superior Tecnológico Sucre es dueño de los sistemas donde se realizará la auditoría de vulnerabilidades y el suscrito tiene la autoridad adecuada para poder llevar a cabo las actividades de verificación de seguridad de aplicaciones.

- El servicio implica necesariamente el uso de herramientas y técnicas diseñadas para detectar las vulnerabilidades de seguridad, y que es imposible identificar y eliminar todos los riesgos que implica el uso de estas herramientas y técnicas.

4. Acuerdo de confidencialidad

MARÍA ELIZABETH CEDEÑO ZAMBRANO se compromete a utilizar toda la información que se genere del siguiente procedimiento únicamente con la finalidad de cumplir con los requisitos de su proceso de titulación, evitando divulgar esta información a terceros que no guarden relación alguna con su trabajo de titulación.

Así mismo, deberá exponer en su trabajo escrito la menor cantidad de la información que llegare a conocer, por ejemplo, deberá colocar direcciones IPs incompletas, no detallar usuarios y contraseñas descubiertos de ser el caso y demás información sensible que resulte del presente análisis.

La información completa sólo podrá ser revelada a los funcionarios del Instituto Superior Tecnológico Sucre, que hayan intervenido en algún punto del proceso de ejecución del presente análisis.

5. Firmas de aceptación

Por el Instituto Superior Tecnológico Sucre:	**Ejecutor de Pruebas:**
Msc. Carlos Guevara	**Ing. Elizabeth Cedeño**

Anexo 5

Acta de Entrega - Recepción de los Informes Ejecutivo y Técnico

En la ciudad de Quito, D.M. a los xx días del mes de noviembre de 2022, se realiza la entrega de los Informes ejecutivo y técnico producto de las pruebas de penetración realizadas desde el 22 de agosto de 2022 al 13 de noviembre de 2022, a la red de servidores y servicios del Instituto Superior Tecnológico Sucre.

Se entrega la siguiente documentación:

- Informe ejecutivo firmado en físico
- Informe técnico firmado en físico
- CD que contiene los informes ejecutivo y técnico firmados electrónicamente.

Para constancia se firman dos ejemplares de igual tenor del presente documento.

Por el Instituto Superior Tecnológico Sucre:	**Ejecutor de Pruebas:**
Msc. Carlos Guevara	**Ing. Elizabeth Cedeño**