UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

Implementación de un sistema Honeypot en los servidores de FACSISTEL, mediante virtualización y análisis de logs para monitorear y prevenir amenazas cibernéticas en la red de estudiantes de la UPSE.

AUTOR

Gamarra Borja, Luis Eduardo

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Ing. Coronel Suárez, Iván Alberto, Msia.

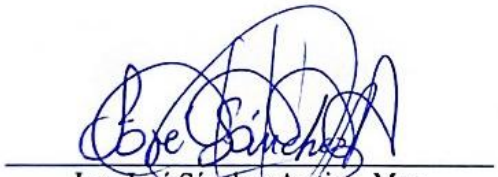
Santa Elena, Ecuador

Año 2025

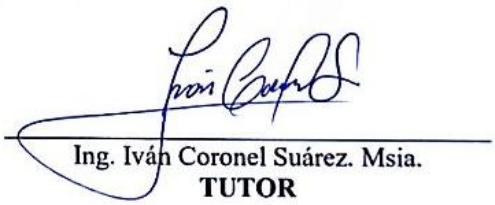
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN



Ing. José Sánchez Aquino. Msc.
DIRECTOR DE LA CARRERA



Ing. Iván Coronel Suárez. Msia.
TUTOR

Lsi. Daniel Quirumbay Yagual. Msia.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez. Mgti.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **GAMARRA BORJA LUIS EDUARDO**, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 17 días del mes de noviembre del año 2025

TUTOR

Firmado electrónicamente por:
IVAN ALBERTO CORONEL SUAREZ
Validar únicamente con FirmaEC

Ing. Coronel Suárez Iván Alberto, Msia.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
DECLARACIÓN DE RESPONSABILIDAD

Yo, **GAMARRA BORJA LUIS EDUARDO**

DECLARO QUE:

El trabajo de Titulación**, Implementación de un sistema Honeypot en los servidores de FACSISTEL, mediante virtualización y análisis de logs para monitorear y prevenir amenazas cibernéticas en la red de estudiantes de la UPSE**, previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 17 días del mes de noviembre del año 2025

EL AUTOR

Luis Eduardo Gamarra Borja

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **Implementación de un sistema Honeypot en los servidores de FACSISTEL, mediante virtualización y análisis de logs para monitorear y prevenir amenazas cibernéticas en la red de estudiantes de la UPSE**, presentado por el estudiante **GAMARRA BORJA LUIS EDUARDO** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

Tesis_Luis Eduardo Gamarra Borja

5% Textos sospechosos

2% Similitudes
0 % similitudes entre comillas
< 1 % entre las fuentes mencionadas
6% Idiomas no reconocidos (ignorado)
3% Textos potencialmente generados por la IA

Nombre del documento: Tesis_Luis Eduardo Gamarra Borja.pdf
ID del documento: b2b32dc94b0fcfc0ecb6be8ae695f7fee4e64b29
Tamaño del documento original: 3,68 MB

Depositante: IVAN ALBERTO CORONEL SUAREZ
Fecha de depósito: 14/11/2025
Tipo de carga: interface
fecha de fin de análisis: 14/11/2025

Número de palabras: 20.944
Número de caracteres: 161.707

Ubicación de las similitudes en el documento:

TUTOR

Firmado electrónicamente por:
IVAN ALBERTO CORONEL SUAREZ
Validar únicamente con FirmaEC

Ing. Coronel Suárez Iván Alberto, Msia.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Gamarra Borja Luis Eduardo**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del presente trabajo de titulación con fines de difusión pública, además apruebo la reproducción dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 17 días del mes de noviembre del año 2025

EL AUTOR

Luis Eduardo Gamarra Borja

AGRADECIMIENTO

A Dios, por guiarme en cada paso de este camino universitario y darme la fortaleza necesaria para superar cada obstáculo. A mi tutor, Ing. Iván Alberto Coronel Suárez, por su dedicación y valiosos conocimientos compartidos durante el desarrollo de este proyecto. Su orientación fue fundamental para convertir esta idea en realidad y por enseñarme que la ciberseguridad va más allá de la tecnología, es un compromiso con la protección de nuestra comunidad.

A la Universidad Estatal Península de Santa Elena por brindarme la oportunidad de desarrollar este proyecto de investigación.

Luis Eduardo, Gamarra Borja

DEDICATORIA

Este logro va dedicado a mis padres quienes fueron mis primeros maestros y mi mayor inspiración. Gracias por cada sacrificio, por esas noches que trabajaron incansablemente para darme la oportunidad de estudiar, por creer en mis sueños incluso cuando parecían imposibles. Este título es tanto suyo como mío, porque sin su amor incondicional y su apoyo constante nada de esto sería posible. Los amo infinitamente.

A mis familiares cercanos, quienes me han acompañado con palabras de aliento durante esta trayectoria académica.

Luis Eduardo, Gamarra Borja

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo propone la implementación de un sistema Honeypot en los servidores de FACSISTEL para monitorear y prevenir amenazas cibernéticas en la red de estudiantes de la UPSE. La investigación aborda la vulnerabilidad de las redes universitarias de acceso libre, donde Ecuador registra el 12% de detecciones de malware en Latinoamérica. El objetivo es implementar un sistema virtualizado que registre intentos de intrusión, analice comportamientos maliciosos y genere inteligencia de seguridad. La metodología incluye cinco fases: investigación preliminar, diseño e implementación usando T-Pot, monitoreo continuo, análisis de datos con Elastic Stack, y documentación de resultados. Se estudiará una muestra de 340 usuarios de los 15,286 activos en la red. Los resultados esperados incluyen la identificación de patrones de ataque, clasificación de amenazas y generación de informes técnicos que fortalezcan la seguridad institucional mediante análisis de logs y correlación de eventos.

Palabras claves: Honeypot, Ciberseguridad, Virtualización

ABSTRACT

This work proposes the implementation of a Honeypot system on FACSISTEL servers to monitor and prevent cybernetic threats in the UPSE student network. The research addresses the vulnerability of open-access university networks, where Ecuador registers 12% of malware detections in Latin America. The objective is to implement a virtualized system that records intrusion attempts, analyzes malicious behaviors, and generates security intelligence. The methodology includes five phases: preliminary research, design and implementation using T-Pot, continuous monitoring, data analysis with Elastic Stack, and results documentation. A sample of 340 users from the 15,286 actives on the network will be studied. Expected results include attack pattern identification, threat classification, and generation of technical reports that strengthen institutional security through log analysis and event correlation.

Keywords: Honeypot, Cybersecurity, Virtualization

INTRODUCCIÓN

La ciberseguridad se ha convertido en uno de los principales desafíos de la era digital, especialmente en las instituciones educativas, donde el acceso abierto a los recursos tecnológicos representa tanto una oportunidad como una posible amenaza. En el contexto latinoamericano, Ecuador ocupa una posición preocupante, al concentrar el 12 % de las detecciones de *malware* y situarse como el tercer país con mayor incidencia, después de Perú y México, según el ESET Security Report 2023. Esta realidad pone de manifiesto la necesidad urgente de fortalecer e implementar sistemas de seguridad informática proactivos en las instituciones del país.

Las universidades, en su papel de generadores y transmisores del conocimiento, tienen que hacer frente a desafíos singulares en cuanto a su ciberseguridad en virtud de su naturaleza abierta y colaborativa. La Universidad Estatal Península de Santa Elena (UPSE) tampoco se salva de esto, sobre todo en su red estudiantil llamada "ESTUDIANTES" que da acceso libre para conectar dispositivos sin medidas de autentificación sólidas. Dicha configuración, si bien agiliza el acceso académico, aumenta en forma exponencial la superficie de ataque y deja a la infraestructura institucional a múltiples vectores de amenazas.

El factor humano es el eslabón más vulnerable de la cadena de seguridad informática y tal situación empeora en entornos universitarios en los que se dan cita usuarios con dispares conocimientos técnicos y niveles de concienciación en materia deciberseguridad. Investigaciones del Equipo de Respuesta ante Emergencias Informáticas (CERT) indican que el 85% de los incidentes en universidades resultan de la utilización de técnicas de ingeniería social, mientras que la existencia de dispositivos personales inseguros agrega amenazas externas que tienen la potencial de propagarse lateralmente en la red institucional.

En vistas a esto, los honeypots se presentan como una técnica innovadora y proactiva para la observación, alertamiento y análisis de amenazas cibernéticas. Estos sistemas actúan como señuelos digitales, atrayendo, engañando y registrando las actividades del atacante, con lo que se obtiene inteligencia importante de sus métodos, técnicas, y procedimientos. Encontrando diferencias con los sistemas de

seguridad convencionales que trabajan de forma reactiva, los Honeypots brindan un enfoque preventivo que permite a las empresas anticiparse a las amenazas y proteger sus perímetros.

El FACSISTEL de la UPSE declara un ambiente propicio para la aplicación de esta tecnología no sólo por contar con una infraestructura tecnológica de punta, sino que también es capaz de producir conocimiento trasmutable a otros similares contextos académicos. La puesta en marcha de un sistema Honeypot virtualizado en esta plataforma, facilitará no solo fortalecer la seguridad institucional, sino que también potenciar las capacidades locales en ciberseguridad y consolidad una base de conocimiento en relación con las amenazas particulares que enfrentan las universidades ecuatorianas.

Este trabajo de investigación plantea la implementación del sistema Honeypots en los servidores que se encuentran en la facultad de sistemas y telecomunicaciones (FACSISTEL), haciendo uso de tecnologías de virtualización y análisis de logs, para de esta forma definir un ecosistema de monitoreo proactivo. La propuesta busca cambiar el enfoque de seguridad informática universitaria, desde un modelo reactivo hacia uno predictivo, sustentado por inteligencia de amenazas.

1. CAPÍTULO I FUNDAMENTACIÓN

1.1. Antecedentes

Hoy día, las instituciones educativas necesitan responder a desafíos sin precedentes en materia de ciberseguridad, sobre todo en ambientes en los que la facilidad de acceso es prioridad [1]. En la Universidad Politécnica Estatal del Carchi, existe internet en toda la institución pero con una red estudiantil que en teoría les permite conectarse sin restricción a los dispositivos propios y que al mismo tiempo los deja vulnerables a ataques cibernéticos [2]. Reciente estudio muestra que la mayoría de los incidentes cibernéticos registrados se debe al phishing, Ecuador es uno de los más perjudicados en Latinoamérica [3].

Lo más preocupante es la falta de conciencia sobre ciberseguridad de parte de los usuarios de la red [4]. Muchas personas que estudian no se enteran de las estrategias que los atacantes emplean para captar su información personal, y ello contribuye a que se propaguen las amenazas [5]. Investigaciones revelan que el factor humano seguirá siendo el eslabón más débil en ciberseguridad, por ello, es importante considerar entre las acciones a desarrollar para la comunidad universitaria, la implementación de programas de formación [6].

Las redes universitarias al ser entornos dinámicos y de acceso masivo, enfrentan desafíos únicos en ciberseguridad debido a factores técnicos y humanos [7]. Este acceso indiscriminado, sumado a la ausencia de autenticación, no solo facilita intrusiones externas, sino que también expone a la institución a riesgos internos, como la manipulación o robo de información sensible por parte de usuarios con privilegios excesivos [8].

Una de las estrategias más empleadas por los atacantes es la implantación de malware en los dispositivos de red, modificando los archivos del sistema operativo, el código ejecutable en memoria que carga el sistema operativo [9]. Estas alteraciones pueden violar la integridad de los datos, facilitar la exfiltración de información sensible, y a veces causar denegaciones de servicio (DoS) [10]. La falta de información correcta sobre cuestiones elementales como identificar correos de phishing, hace de ellos un vehículo habitual de ataques [11].

El riesgo ha sido agravado por uso de dispositivos personales que traen amenazas externas en la infraestructura de la universidad [12]. El computador portátil, las tablets o los celulares se convierten en vectores para ransomware u otro tipo de malware que se mueve lateralmente [13]. Los casos documentados demostraron cómo un solo dispositivo infectado puede comprometer sistemas enteros, interrumpiendo servicios y así generar pérdidas económicas [14]. Ante esta situación la implementación de un sistema honeypot surge como una estrategia para monitorear y prevenir comportamientos anómalos [15].

1.2. Objetivos del Proyecto

1.2.1. Objetivo General

Implementar un sistema Honeypot en los servidores de FACSISTEL, mediante virtualización y análisis de logs para monitorear y prevenir amenazas cibernéticas en la red de estudiantes de la UPSE.

1.2.2. Objetivos Específicos

• Implementar un sistema Honeypot en los servidores de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL), con el fin de registrar intentos de intrusión en la red de estudiantes.

• Monitorear el comportamiento de actores maliciosos que interactúan con el sistema Honeypot, identificando patrones de ataque y técnicas empleadas.

• Clasificar los datos recopilados por el Honeypot mediante análisis estadístico y correlación de eventos.

• Generar informes técnicos detallados mediante la implementación de scripts automatizados que procesen y documenten los registros de ataques capturados por el Honeypot.

1.3. Justificación del Proyecto

En los años recientes, el Ecuador se ha destacado en la cantidad de detección de malware en Latino América [16]. Según el ESET Security Report 2023, Ecuador concentró el 12% de las detecciones de malware en la región ubicándose como el

tercer país más afectado, seguido de Perú (24%) y México (16%) [17]. Esta situación manifiesta la necesidad urgente de implementar sistemas de seguridad informática robustos en todas las instituciones del país principalmente en entornos académicos donde se maneja información sensible de varios usuarios [18]. Las universidades como centros de conocimiento necesitan proteger todos sus activos digitales frente a las amenazas cibernéticas que evolucionan constantemente en cuanto a la complejidad [19].

En la actualidad, la red de estudiantes de la UPSE, denominada “ESTUDIANTES”, carece de un control de monitoreo de seguridad para los diversos dispositivos conectados a la infraestructura de red, lo que causa una red insegura, llegando a atentar contra la integridad de los datos que circulan a través de ella [20]. Estas vulnerabilidades representan un riesgo significativo para la información académica, administrativa y personal almacenada en los sistemas universitarios [21]. Las anomalías en el tráfico de red deberían ser motivo de análisis constante para detectar comportamientos sospechosos y prevenir posibles ataques informáticos [22]. Sin un sistema adecuado de monitoreo, resulta imposible identificar intentos de intrusión, infecciones de malware o comportamientos anómalos que podrían comprometer la seguridad de toda la red universitaria [23].

1.4. Alcance del Proyecto

El presente proyecto tiene como alcance la implementación de un sistema Honeypot en la infraestructura de servidores de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) de la Universidad Estatal Península de Santa Elena. Esta implementación se centrará específicamente en el monitoreo y análisis de la red estudiantil denominada "ESTUDIANTES", la cual cuenta actualmente con 15,286 usuarios activos. El sistema permitirá el registro sistemático de intentos de intrusión y actividades maliciosas dirigidas hacia la infraestructura universitaria.

La parte técnica consistirá en desplegar la solución T-Pot como una plataforma principal honeypot con componentes especializados analógicos a Cowrie para emular servicios SSH/Telnet en modo de simulación y Suricata como IDPS en tiempo real. El sistema será implementado en una infraestructura virtualizada en Proxmox garantizando así el aislamiento para no poner en riesgo los sistemas

productivos. La integración con Elastic Stack facilitará procesar, almacenar y visualizar los datos capturados.

Monitoreo del comportamiento de ocupantes maliciosos es un elemento crítico dentro de la perspectiva, con un enfoque en la determinación y documentación de las huellas de un ataque. Se documentarán y analizarán las técnicas utilizadas por los atacantes, como técnicas de reconocimiento, vulnerabilidades de explotación y técnicas de post explotación. El análisis conductual permitirá generar perfiles de amenazas específicos para el ámbito universitario, lo que aportará a la generación de inteligencia de seguridad aplicable. Por otro lado, el proyecto incluye la evaluación del desempeño del entorno honeypot bajo cargas variables de tráfico para comprobar la estabilidad del mismo.

La clasificación de los datos recolectados se llevará a cabo mediante análisis estadístico con validación cruzada de eventos, con información de múltiples fuentes honeypot. La información obtenida por el honeypot se analizará para realizar un seguimiento y comparar los ataques en función de su tipo, área geográfica de origen, los vectores utilizados y nivel de sofisticación. Esta categorización hará posible detectar tendencias y patrones que ayuden a entender el panorama de amenazas particulares para las instituciones de educación en Ecuador.

Se automatizará la generación de informes técnicos con la creación de un script que procesará los logs del honeypot y los documentará. Dichos informes proporcionarán análisis estadísticos, gráficos, indicadores de compromiso y recomendaciones de seguridad basadas en los hallazgos. La documentación técnica será la que sustente decisiones estratégicas en materia de ciberseguridad institucional

Tiempo de duración El plazo de ejecución del proyecto será de 2 meses de monitorización continua en el mínimo, dicho tiempo es necesario para la obtención de datos significativos que permitan realizar análisis estadísticos sólidos. Durante ese tiempo, se realizará una captura automatizada de logs, un procesamiento en tiempo real de eventos de seguridad, y reportes de estado periódicos. La sección de análisis y redacción final tomará 1 mes adicional, para procesar totalmente la información y resultados.

Entre las limitaciones del alcance están la de limitarse la implementación a los servidores de FACSISTEL, sin llegar a otras facultades de la universidad. El sistema será instalado y ejecutado bajo condiciones controladas y aisladas para asegurar que no tenga ningún impacto en la red productiva. Este trabajo no contempla el estudio forense de incidentes de seguridad anteriores a la puesta en marcha del honeypot, sino que se limita a la captura de amenazas y a su posterior análisis.

1.5. Descripción del Proyecto

1.5.1. Metodología de Desarrollo del Proyecto

Las fases metodológicas empleadas en este estudio se adaptaron del trabajo de Pablo Javier Barrio Navarro, quien propuso un enfoque estructurado para el análisis de vulnerabilidades en entornos virtualizados [24].

Fase 1: Investigación y análisis preliminar

En esta etapa inicial se llevará a cabo un estudio profundo sobre los sistemas Honeypot, incluyendo sus distintas tipologías, también su implementación dentro de arquitecturas más complejas como las Honeynets. Se analizarán tecnologías complementarias como los Sistemas de Detección y Prevención de Intrusiones (IDS/IPS).

• Investigar qué es un Honeypot y su propósito en ciberseguridad.

• Clasificar los tipos de Honeypots: de baja, media y alta interacción.

• Estudiar las arquitecturas de Honeynets y su aplicación práctica.

• Analizar herramientas Honeypot: *T-Pot, Cowrie, Dionaea, Kippo.*

• Investigar sistemas IDS e IPS.

Fase 2: Diseño, implementación y configuración del entorno

Durante esta fase se procederá a la instalación, configuración y despliegue del sistema Honeypot. Esto incluye tanto la infraestructura necesaria para su operación (servidores, redes y servicios falsos), como la integración con sistemas de

monitoreo, bases de datos para almacenamiento de logs. El sistema se implementará en los servidores de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL).

• Diseñar la arquitectura de red donde estará el Honeypot.

• Preparar los equipos físicos o virtuales.

• Configurar la red para que el Honeypot esté accesible.

• Instalar y configurar T-Pot.

• Validar la conectividad, funcionalidad y visibilidad del Honeypot en la red.

Fase 3: Monitoreo y recolección de datos

Una vez el sistema esté en funcionamiento comenzará a operar en tiempo real permitiendo así la captura de eventos de intentos de intrusión y comportamientos maliciosos. Esta fase implica una observación del tráfico capturado, así como el almacenamiento y categorización de los datos recolectados para su posterior análisis.

• Supervisar el tráfico con la ayuda de plataformas de visualización y análisis de datos.

• Registrar los logs de ataques.

• Automatizar la recolección de datos.

• Clasificar los eventos por escaneo, explotación y fuerza bruta.

• Revisar la integridad del sistema.

• Documentar cada evento relevante con capturas.

Fase 4: Análisis y evaluación de resultados

Se realizará el análisis de los datos obtenidos por medio de los registros de patrones de ataque y origen de estos, también se evaluará la efectividad del sistema para prevenir estas amenazas.

• Exportar y organizar los logs en una base de datos.

• Comparar el comportamiento del Honeypot bajo diferentes configuraciones.

• Evaluar si el sistema fue capaz de engañar y registrar al atacante.

Fase 5: Elaboración de la documentación final

En esta fase se procede a documentar las configuraciones aplicadas, los resultados obtenidos, gráficas estadísticas, credenciales capturadas y servicios atacados. También se debe indicar las recomendaciones para la mejora continua del sistema.

• Redactar un informe técnico estructurado.

1.6. Metodología de Investigación

1.6.1. Contexto de la investigación

La investigación se desarrollará en el entorno de la Universidad Estatal Península de Santa Elena (UPSE) y tendrá como ámbito de implementación en los servidores de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) [25]. El estudio se enfoca en la red utilizada por los estudiantes, la cual se caracteriza por ser un ambiente académico donde la facilidad de acceso a la red es una prioridad, lo que aumenta la vulnerabilidad a diversas amenazas cibernéticas [26]. Actualmente se ha identificado una deficiencia en el monitoreo de seguridad de los dispositivos conectados a la infraestructura de red de UPSE, lo que resulta en una red potencialmente insegura y pone en riesgo la integridad de los datos [27].

1.6.2. Diseño y alcance de la investigación

El diseño de esta investigación tiene un componente experimental ya que la implementación del Honeypot se basa en un entorno real para observar y analizar los ataques que reciba [28].

El alcance de la investigación es de carácter analítico, explicativo y correlacional. La parte analítica implica un análisis en profundidad de los datos recogidos para identificar el origen de los ataques, así como un análisis de tecnologías como honeypots e IDS/IPS [29]. El componente explicativo tiene como objetivo comprender cómo ocurren los ataques en la red universitaria y la efectividad del sistema para mitigarlos, además de entender el comportamiento de actores maliciosos y las técnicas que emplean [30]. El aspecto correlacional se enfoca en relacionar eventos y clasificar los datos recopilados [31].

1.6.3. Tipo y métodos de investigación

Esta investigación tiene en un enfoque cuantitativo orientado hacia la recopilación y posterior examen de información numérica y estadística extraída de los registros generados por el Honeypot [32].

En cuanto a los métodos de investigación se empleará el método analítico el cual permitirá descomponer los datos recolectados para estudiar en detalle los patrones de ataque, las herramientas utilizadas por los atacantes y las vulnerabilidades explotadas [33]. Por otro lado, se empleará el método sintético que facilitará la integración de los hallazgos del análisis para formular conclusiones sobre las amenazas presentes en la red y la efectividad del Honeypot [34].

El método inductivo será útil para que a partir de la observación y el análisis de los ataques específicos registrados por el Honeypot pueda identificar patrones y generalizar sobre las tácticas, técnicas y procedimientos (TTP) de los atacantes dirigidos a la red universitaria [35]. El método deductivo permitirá partir de los conocimientos generales sobre ciberseguridad y Honeypots para implementar el sistema y luego contrastar los resultados obtenidos con la teoría existente [36].

Se aplicará el método hipotético deductivo ya que la implementación del honeypot tendrá como objetivo analizar amenazas y estos resultados validarán o refutarán esta efectividad [37].

1.6.4. Beneficiarios del Proyecto

Los destinatarios inmediatos de este proyecto son los 15,286 usuarios activos de la red estudiantil "ESTUDIANTES" de la UPSE, quienes gozarán de un entorno digital más seguro y protegido ante amenazas cibernéticas. También el personal docente y administrativo de la Facultad de Sistemas y Telecomunicaciones se verá beneficiado al disponer de herramientas avanzadas de monitoreo que permitirán una gestión proactiva de la seguridad informática. La habilitación del sistema Honeypot les brindará a estos usuarios una plataforma tecnológica más sólida y confiable sobre la cual apoyar sus actividades académicas.

Otro grupo beneficiario es la comunidad académica ya que el proyecto producirá conocimiento especializado que podrían ser extendidas a otras instituciones de

educación superior del país. Investigadores de carreras relacionadas con la ciberseguridad tendrán a su disposición datos reales de amenazas para realizar sus investigaciones. La sociedad ecuatoriana será beneficiada indirectamente debido a que dispondrá de profesionales mejor formados para enfrentar los retos en seguridad informática.

1.6.5. Variables

La implementación de un sistema Honeypot en los servidores de FACSISTEL permitirá analizar el comportamiento de los actores maliciosos en la red de estudiantes de la UPSE.

Para la comprobación de la variable se establecerá un período de evaluación controlada donde se medirán métricas específicas de detección de amenazas.

1.6.6. Análisis de recolección de datos

Esta investigación empleará un enfoque mixto de recolección de datos. Se realizará un estado del arte para revisar investigaciones previas complementado con encuestas, observación directa y análisis de fuentes bibliográficas especializadas [38].

Se aplicó una entrevista al personal administrativo del área de Tecnologías de la Información y Comunicación (TICs) para obtener información importante sobre el estado actual de la red y las medidas de seguridad [39].

Una técnica clave es el conteo automático basado en la Honeypot que utiliza dos enfoques: monitoreo de red continua para capturar todo el tráfico malicioso hacia el sistema, y análisis sistemático de logs para investigar los logs generados por todos los módulos de Honeypot [40].

1.6.7. Entrevista al Personal Administrativo de TICs

Se realizó una entrevista al personal administrativo del área de Tecnologías de la Información y Comunicación de la UPSE el día 5 de junio de 2025 (ver Anexo 1), con el objetivo de recabar información del estado actual de la red wifi “ESTUDIANTES”, así mismo, identificar medidas de seguridad que tiene implementadas y evaluar la viabilidad de implementación del sistema honeypot.

Los hallazgos proporcionaron base empírica para fundamentar la relevancia del proyecto dentro del entorno operacional específico de la institución. Con la información recopilada durante la entrevista, fue posible modelar un diagrama de Sankey con los respectivos códigos de la entrevista, utilizando la herramienta ATLAS.ti tal como se observa en la Figura 1 y Figura 2.

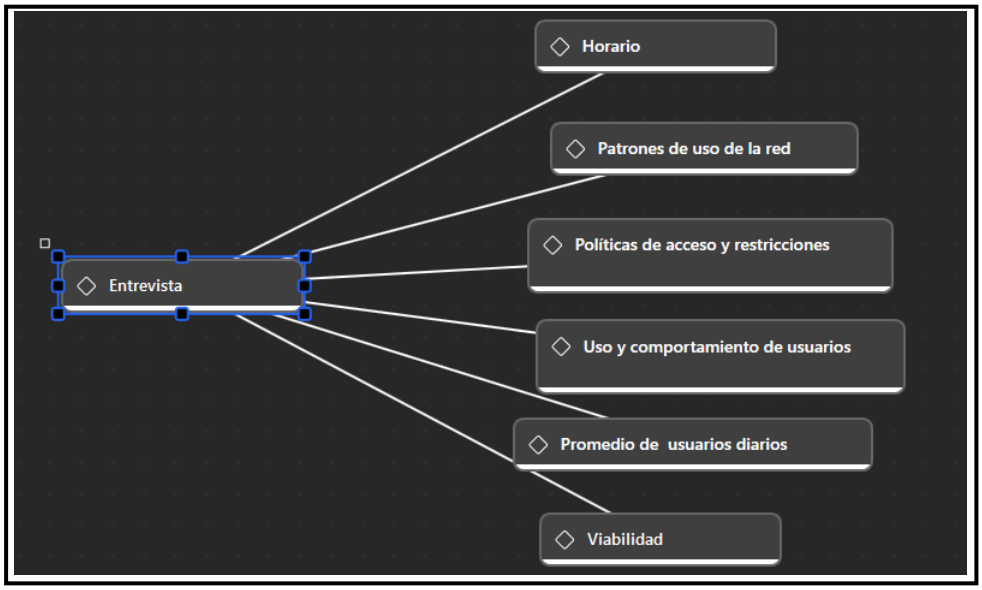


Figura 1: Diagrama de Sankey

El análisis indicó que la actividad máxima de la red de esta institución educativa estaba entre 07:30 y 15:30 horas. El número total de usuarios en promedio por día es aproximadamente 2,500 dispositivos, lo que es bastante representativo considerando la población total de estudiantes. Tal nivel de conectividad da lugar a un tráfico significativo que aumenta la superficie de ataque debido a la variedad de dispositivos, sistemas operativos y aplicaciones. La escala de operación confirmó la necesidad de sistemas de monitoreo automatizados tal como el honeypot sugerido, dado que el volumen de operaciones supera toda supervisión manual efectiva. Durante la entrevista se hizo evidente que la navegación (a través de la web) en este tipo de red estudiantil opera por un sistema de reglas y permisos, con restricciones sobre los tipos de tráfico permitidos y los recursos que se podían visitar, u opuesto a la percepción de un acceso bastante libre. Los protocolos mayoritarios son HTTP y HTTPS para web, SSH para acceso remoto seguro y FTP para transferencia de archivos, habilitados de forma selectiva en función de las

necesidades académicas. Esta estructura determina el abanico de vectores de ataques observables potencialmente a través del honeypot, lo que justifica implementar *Cowrie* (SSH) y honeypots web para capturar ataques HTTP/HTTPS.

Se detectó, según reportes del personal administrativo, uso de redes privadas virtuales dentro de la red institucional con el fin aparente de evadir controles de seguridad y saltar restricciones de permisos impuestas (ver Anexo 1).

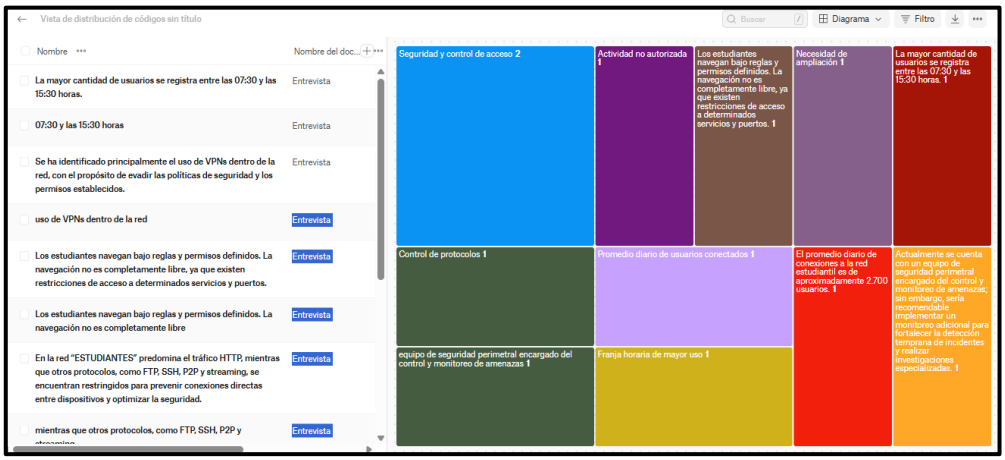


Figura 2: Frecuencia de códigos en la entrevista

Esta técnica representa un esfuerzo consciente de los usuarios por evadir las políticas a través del ruteo del tráfico mediante túneles cifrados que hacen más difícil la detección de los monitoreos convencionales. Tomar en cuenta esta conducta no sólo lleva a pensar en las limitaciones de los sistemas tradicionales, sino que también pone en evidencia la importancia de soluciones complementarias como honeypots que operan bajo principios de engaños en lugar de bloqueo directo. El personal de TICs evaluó positivamente la viabilidad de implementación de un servidor virtual adicional dedicado al sistema honeypot con fines de investigación y monitoreo de amenazas como se puede observar en la **¡Error! No se encuentra e l origen de la referencia.**.

Segmentación de respuestas:

Las respuestas que se obtuvieron a partir de la entrevista realizada al personal encargado de TICs; se organizaron según los códigos asignados, lo que permitió un análisis con más detalles de cada uno de los aspectos mencionados de una manera

concisa, facilitando una interpretación más precisa y coherente de la información proporcionada por los participantes.

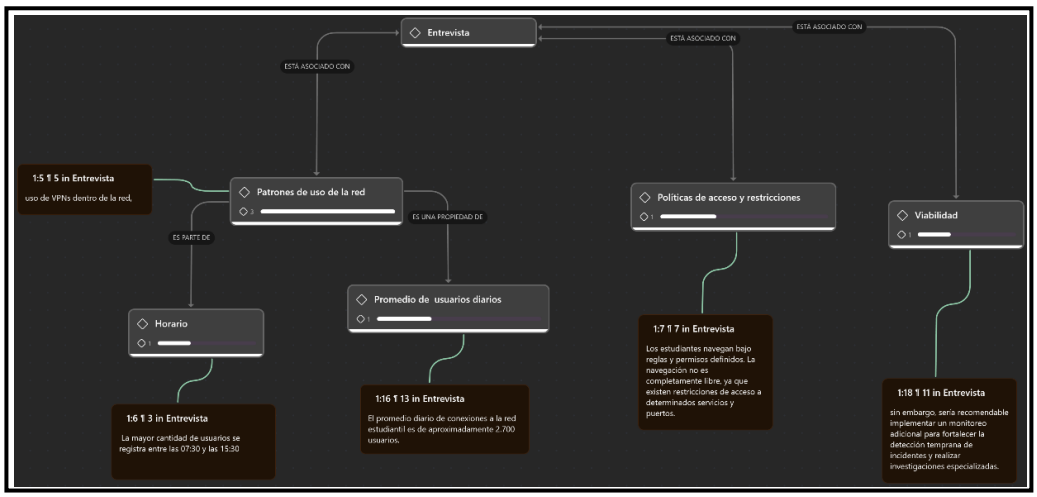


Figura 3: Diagrama de relación con código y respuesta

1.6.8. Análisis de resultados de la encuesta

Se realizó una encuesta dirigida a estudiantes de la Universidad Península de Santa Elena con el objetivo de medir el grado de conocimiento (ver Anexo 2), prácticas de seguridad digital y percepción de amenazas de suplantación informática en el ambiente universitario. La obtención de datos se realizó a través de un cuestionario estructurado, en relación con el uso de contraseñas, conocimiento de técnicas de ataque, incidentes de seguridad previos, concienciación frente a vulnerabilidades comunes.

Los resultados obtenidos permitieron identificar niveles diferenciados de conocimiento entre los encuestados, mostrando brechas importantes en el entendimiento de conceptos básicos de ciberseguridad y en el cumplimiento de las mejores prácticas para el resguardo de la información personal. Asimismo, el análisis estadístico reveló que un porcentaje significativo de estudiantes ha experimentado, directa o indirectamente, intentos de suplantación o actividades sospechosas en entornos digitales universitarios, lo que refuerza la necesidad de implementar programas de capacitación continua. Estos hallazgos no solo ayudan a dimensionar el nivel de exposición, sino que también permiten orientar estrategias

Ítem 1: Facultad a la que pertenece:

Respuesta	Frecuencia	Porcentaje
Facultad de Sistemas y Telecomunicaciones	292	85,9 %
Facultad de Ciencias Sociales y de la Salud	15	4,4 %
Facultad de Ciencias de la Educación e Idiomas	11	3,2 %
Facultad de Ciencias del Mar	8	2,4 %
Facultad de Ciencias Administrativas	8	2,4 %
Facultad de Ciencias Agrarias	6	1,8 %
TOTAL	340	100 %

Tabla 1: Facultad a la que pertenece

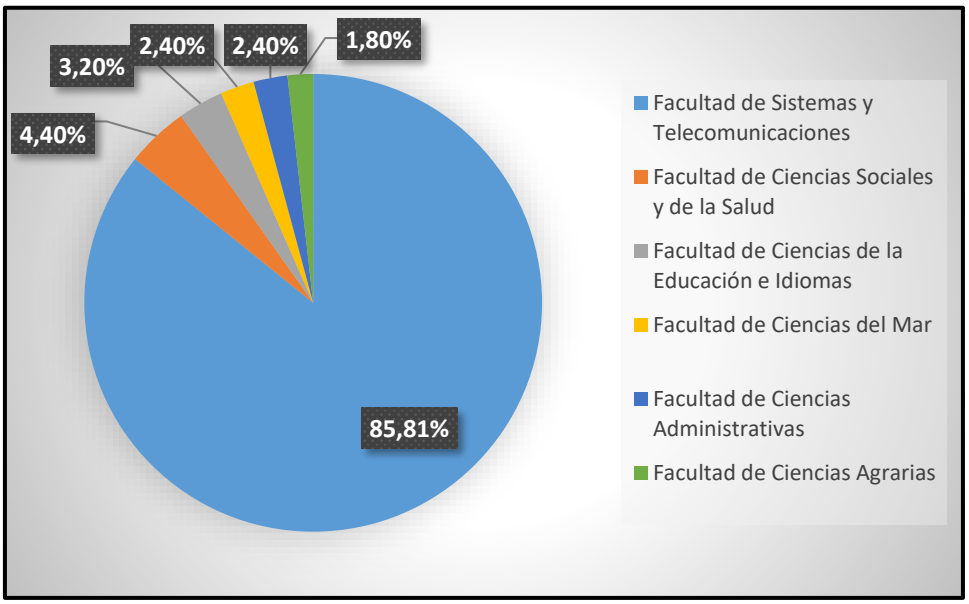


Figura 4: Facultad a la que pertenece

Interpretación: La muestra reveló Predominancia de estudiantes de la Facultad de Sistemas y Telecomunicaciones concentrando la mayor parte de respuestas con un 85,81%.

Conclusión: Las conclusiones son válidas para este grupo mayoritario los cuales son estudiantes de la Facultad de Sistemas y Telecomunicaciones, pero deben extrapolarse con cuidado al resto de facultades.

Ítem 2: Semestre académico que cursa actualmente

Respuesta	Frecuencia	Porcentaje
1 - 2 semestre	77	22,6 %
3 - 4 semestre	89	26,2 %
5 - 6 semestre	105	30,9 %
7 - 8 semestre	69	20,3 %
TOTAL	340	100 %

Tabla 2: Semestre académico que cursa actualmente

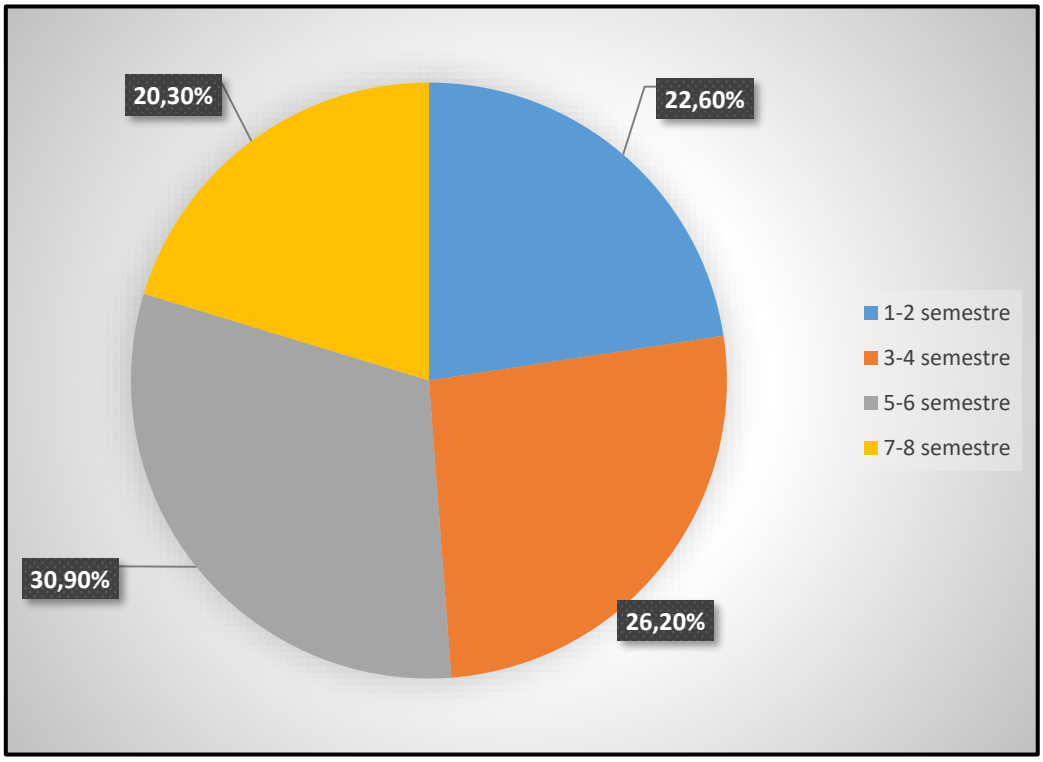


Figura 5: Porcentaje de semestre académico

Interpretación: Los estudiantes de un nivel intermedio representaron el 57,3% acumulado, esto sugiere que la muestra capturó adecuadamente las experiencias de los estudiantes en diferentes etapas de su formación universitaria.

Conclusión: La existencia de diversos niveles académicos puede ayudar a un análisis comparativo de cómo las prácticas de seguridad pueden variar entre los estudiantes a lo largo de su carrera universitaria.

Ítem 3: ¿Con qué frecuencia se conecta a la red Wi-Fi "ESTUDIANTES"?

Respuesta	Frecuencia	Porcentaje
Diariamente	66	19,4 %
3 – 4 veces por semana	106	31,2 %
1 – 2 veces por semana	77	22,6 %
Ocasionalmente	91	26,8 %
TOTAL	340	100 %

Tabla 3: Frecuencia con la que se conectan a la red

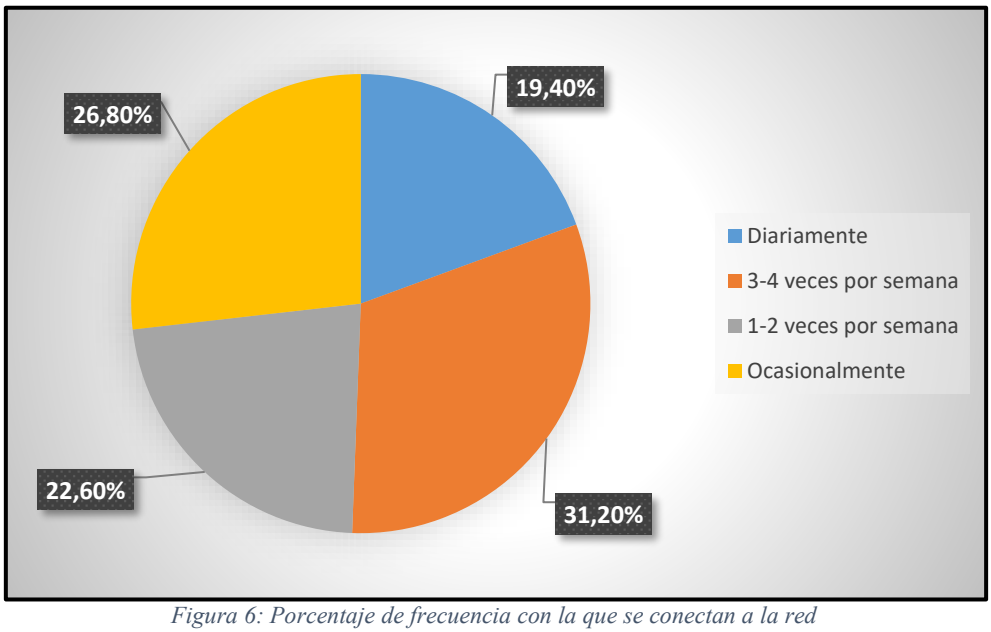


Figura 6: Porcentaje de frecuencia con la que se conectan a la red

Interpretación: El análisis reveló que la conexión diaria o varias veces por semana suma la mayoría con más del 70%, por otra parte, las conexiones esporádicas y poco frecuentes son minoritarias y que posiblemente dependan de redes alternativas.

Conclusión: La frecuencia de uso permite sugerir la inversión en seguridad en la red "ESTUDIANTES" ya que, si se llega a comprometer esta red afectaría directamente a las actividades académicas de una gran parte de la población estudiantil que accede cotidianamente a esta red.

Ítem 4: ¿En qué horarios se conecta con mayor frecuencia?

Respuesta	Frecuencia	Porcentaje
7:00 – 10:00 AM	68	20 %
10:00 – 1:00 PM	100	29,4 %
1:00 – 3:00 PM	78	22,9 %
3:00 – 5:00 PM	94	27,6
TOTAL	340	100 %

Tabla 4: Horarios de mayor frecuencia de conectividad a la red

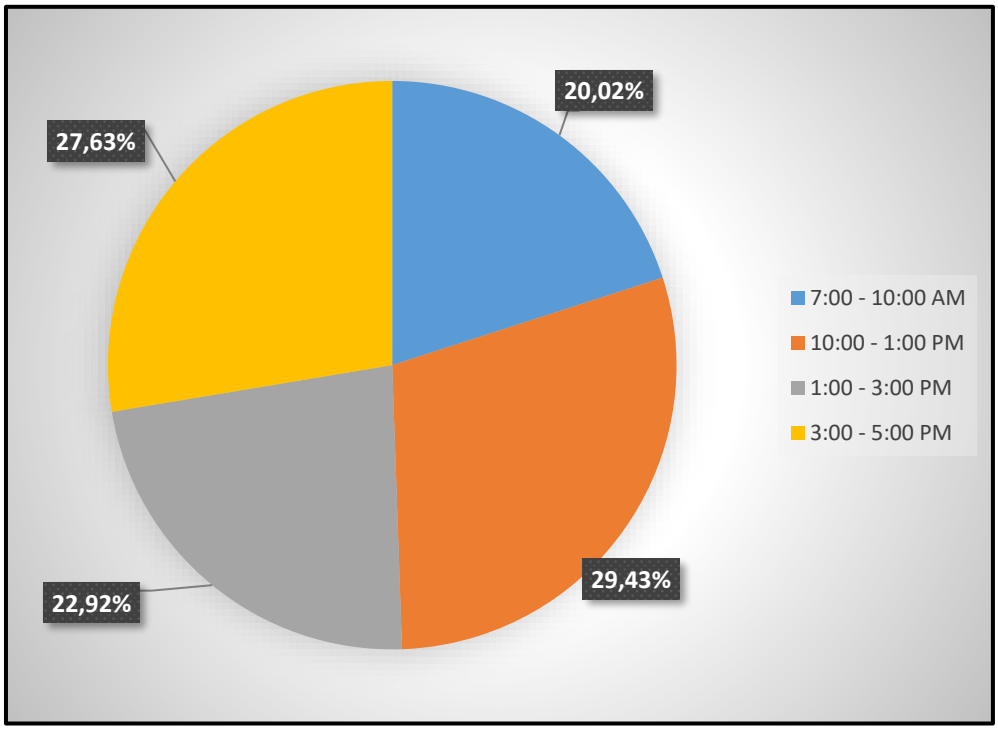


Figura 7: Porcentaje de horarios con mayor frecuencia de conectividad

Interpretación: Se puede observar un agrupamiento de la actividad durante la mañana con un 29,43%, compatible con el horario académico tradicional que fue validado a través de las entrevistas con el personal de TIC que reportó picos entre 7:30 y 15:30.

Conclusión: La relación entre los patrones reportados por los estudiantes junto a las observaciones por parte del personal técnico validan la fiabilidad de los datos de la encuesta. El honeypot debe mantener capacidad de análisis en tiempo real precisamente entre las 7:30 AM y 15:30 PM.

Ítem 5: ¿Qué dispositivos utiliza para conectarse a la red estudiantil? (Puede seleccionar varios)

Respuesta	Frecuencia
Tablet	181
Computadora de escritorio	215
Smartphone	221
Laptop	229

Tabla 5: Dispositivos utilizados en la red "ESTUDIANTES

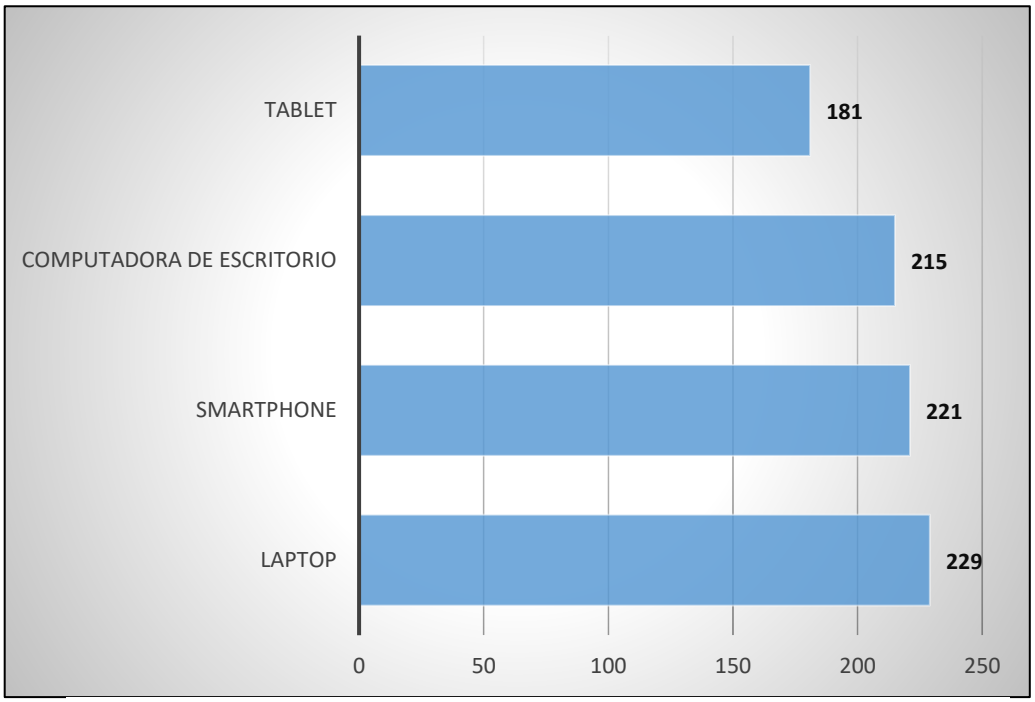


Figura 8: Porcentaje de dispositivos utilizados en la red "ESTUDIANTES"

Interpretación: El análisis reveló que las laptops lideran con claridad con 229 de menciones, seguido por los Smartphones con 221 votos, seguido por las PCs de escritorio con 215 votos y por ultimo las Tablets con 181 votos.

Conclusión: Las políticas de seguridad deben enfocarse primero en los dispositivos propios de los estudiantes como lo son las laptops y los Smartphone los cuales representan vectores de acceso principal.

Ítem 6: ¿Para qué actividades utiliza principalmente la red estudiantil? (Puede seleccionar varios)

Respuesta	Frecuencia
Descarga de archivos	165
Streaming de videos / música	130
Comunicación (Redes sociales, mensajería)	138
Acceso a plataformas institucionales (EVA, correo institucional, etc.)	156
Investigación académica y consulta de recursos educativos	165

Tabla 6: Actividades realizadas en la red

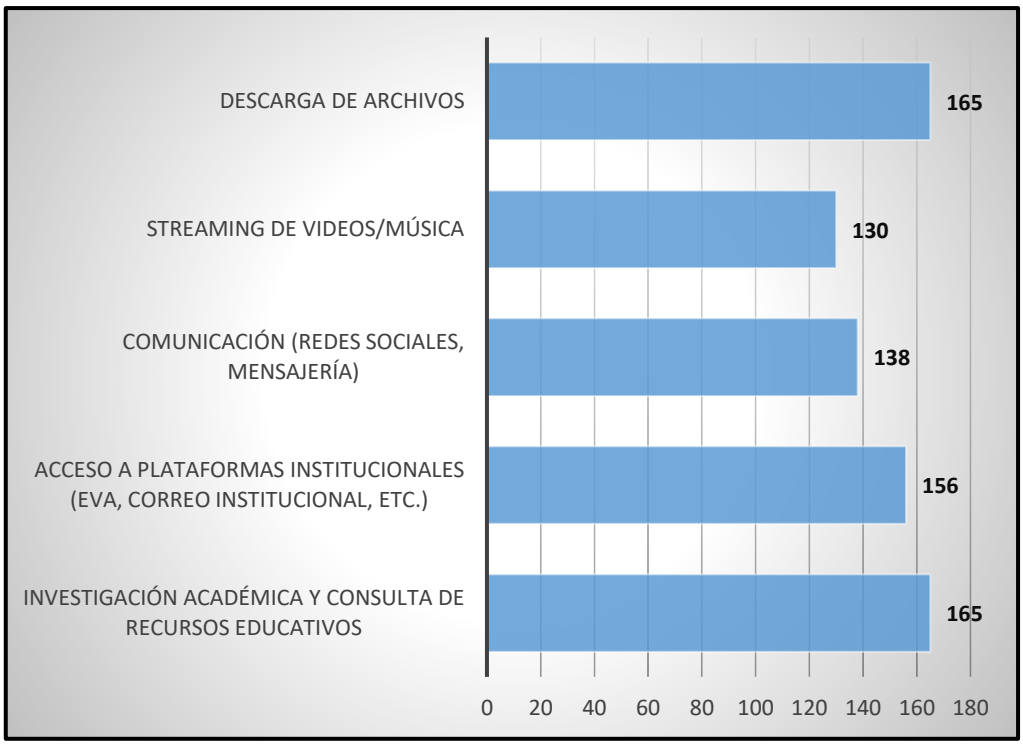


Figura 9: Porcentaje de actividades realizadas en la red

Interpretación: El uso académico domina las plataformas institucionales, búsqueda y descargas de materiales y comunicación académica concentran la mayoría con un 70% combinados.

Conclusión: El uso en el entorno académico sugiere una política de seguridad que garantice la protección sin llegar a limitar las actividades con fines educativos en la red.

Ítem 7: ¿Qué tan familiarizado está con conceptos de seguridad informática?

Respuesta	Frecuencia	Porcentaje
Muy familiarizado	77	22,6 %
Familiarizado	106	31,2 %
Poco familiarizado	82	24,1 %
Nada familiarizado	75	22,1 %
TOTAL	340	100 %

Tabla 7: Conceptos de seguridad informática

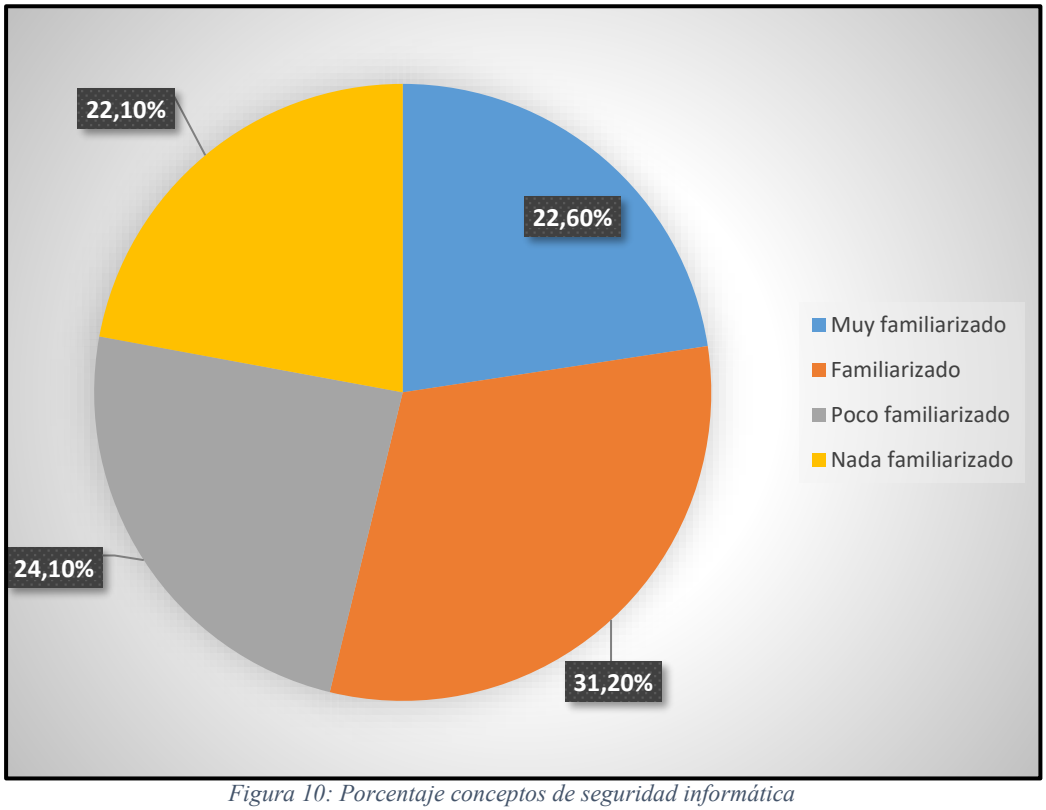


Figura 10: Porcentaje conceptos de seguridad informática

Interpretación: El análisis evidencia que el 53,75% de estudiantes de una muestra aleatoria declaró tener un nivel alto o muy alto de familiaridad con los conceptos de seguridad y el 46,25% informó estar poco o nada familiarizado con dichos conceptos.

Conclusión: El conocimiento de los encuestados sugiere que la intervención educativa sea diferenciada con contenidos en un nivel alto para el 53.75 % de los estudiantes y formación básica para el 46.25 %.

Ítem 8: ¿Conoce qué es el phishing (suplantación de identidad digital)?

Respuesta	Frecuencia	Porcentaje
Sí, y sé cómo protegerme	123	36,2 %
Sí, pero no sé cómo protegerme	65	19,1 %
He escuchado el término pero no sé qué significa	75	22,1 %
No	77	22,6 %
TOTAL	340	100 %

Tabla 8: Conocimiento del phishing

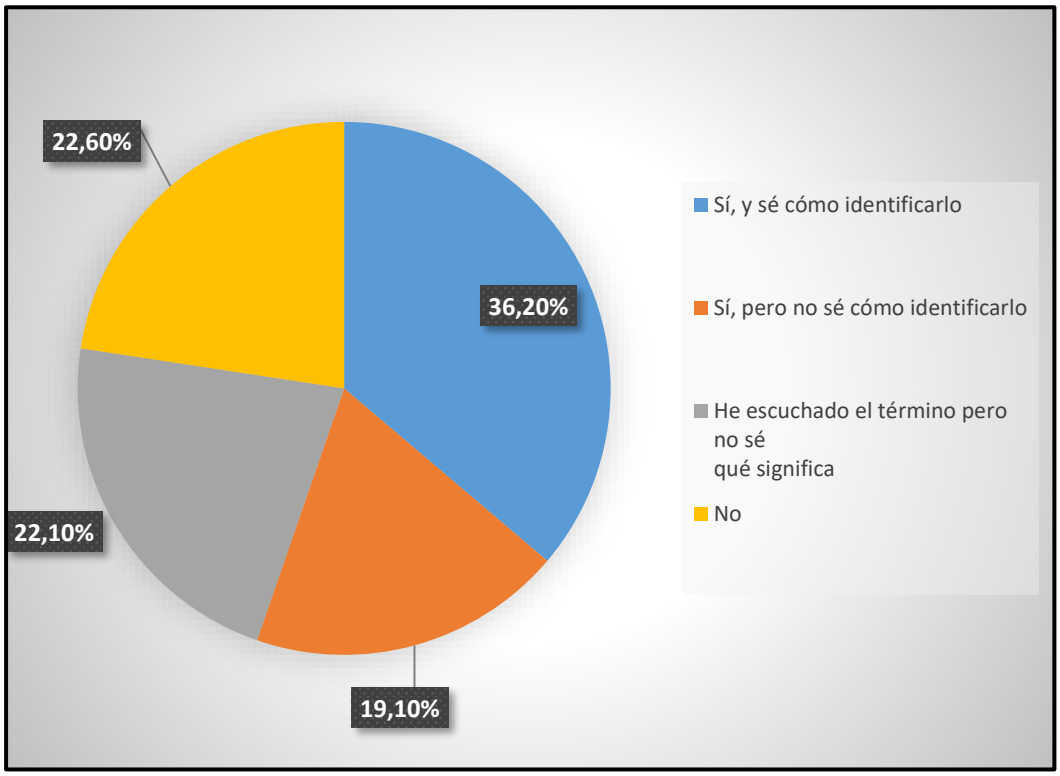


Figura 11: Porcentaje del conocimiento del phishing

Interpretación: La encuesta demuestra que el conocimiento sobre phishing mostró que 36,2% pueden identificar ataques de suplantación, 19,1% conocen el concepto pero no pueden identificarlo, 22,1% solo escucharon término sin comprenderlo, y 22,6% desconocen completamente.

Conclusión: El sistema honeypot puede capturar intentos de phishing dirigidos a la institución para el posible desarrollo de material educativo basado en amenazas reales observadas.

Ítem 9: ¿Conoce qué es el *Malware* (software malicioso)?

Respuesta	Frecuencia	Porcentaje
Sí, y sé cómo protegerme	76	22,4 %
Sí, pero no sé cómo protegerme	104	30,6 %
He escuchado el término pero no sé qué significa	75	22,1 %
No	85	25 %
TOTAL	340	100%

Tabla 9: Conocimiento de Malware

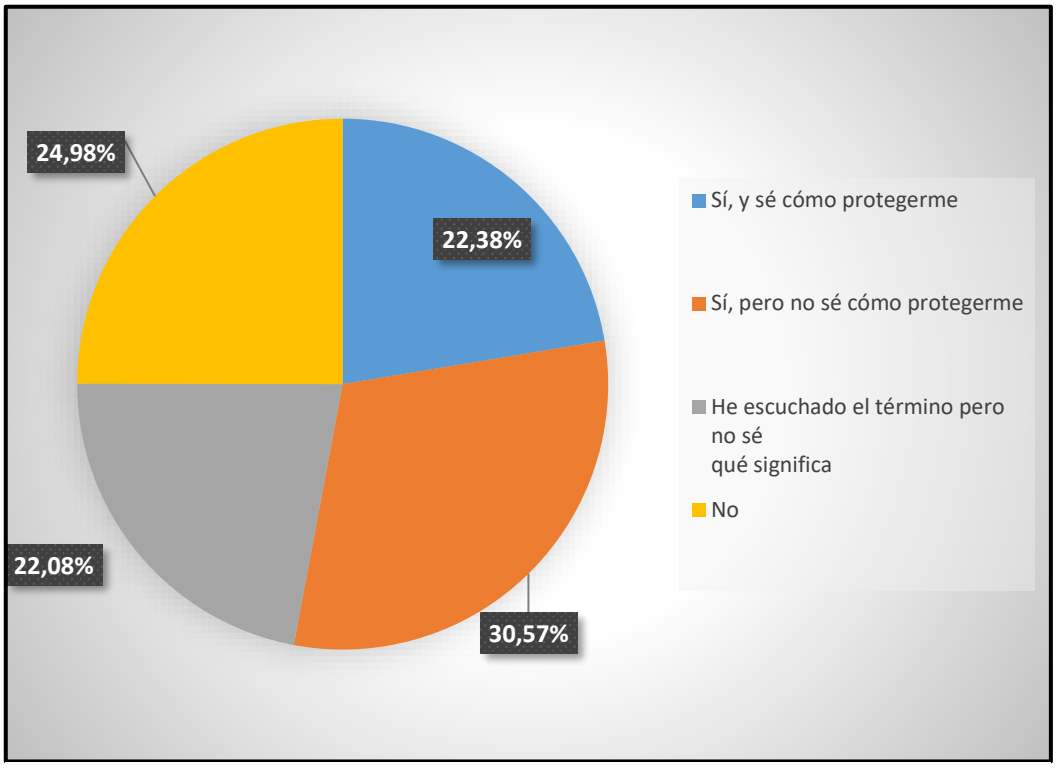


Figura 12: Porcentaje de conocimiento de Malware

Interpretación: El conocimiento acerca del malware mostró un 22,4% de las personas que saben cómo protegerse, mientras que el 30,6% tienen conocimiento de un malware más no saben cómo protegerse, un 22,1% ignoran el concepto y el 25% desconocen en lo absoluto este término.

Conclusión: Esto permite afirmar que es necesario implementar el sistema Honeypot sugerido no sólo como una herramienta para la detección de amenazas, sino que puede convertirse en una fuente de inteligencia para desarrollar programas de sensibilización que busquen fortalecer la cultura de ciberseguridad en la comunidad universitaria de la UPSE.

Ítem 10: ¿Qué tan importante considera que la universidad implemente mejores medidas de seguridad en la red estudiantil?

Respuesta	Frecuencia	Porcentaje
Muy Importante	146	42,9 %
Importante	91	26,8 %
Nada importante	103	30,3 %
TOTAL	340	100 %

Tabla 10: Implemente mejores medidas de seguridad

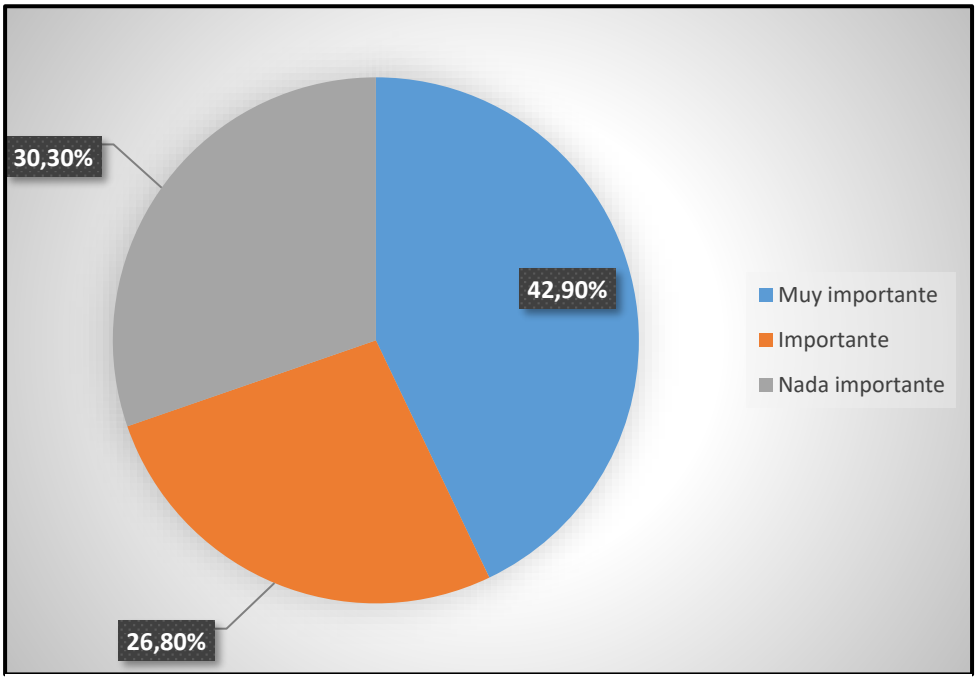


Figura 13: Porcentaje de importancia en mejoras a las medidas de seguridad

Interpretación: Los resultados muestran que el 42,9 % de los encuestados piensa que la aplicación de medidas de ciberseguridad en el entorno universitario es muy importante, mientras que un 26,8 % opina que son importantes. Por otro lado, el 30,3 % de los estudiantes las considera poco importantes, evidenciando una falta de concienciación importante en alrededor de un tercio de la población estudiantil sobre la importancia de protegerse digitalmente en el campo académico.

Conclusión: Aun cuando hay una mayoría positiva 69,7% que hace un reconocimiento a la importancia de las acciones de seguridad informática, nada despreciable casi unos 30% de los alumnos no la consideraban relevante, lo que es preocupante.

Ítem 11: ¿Utiliza alguna medida adicional de seguridad al conectarse a la red estudiantil? (Puede seleccionar varios)

Respuesta	Frecuencia
VPN (Red Privada Virtual)	187
Navegación en modo incógnito / privado	184
Extensiones de navegador para seguridad	140
Verificación de certificados de sitios web (HTTPS)	196
Ninguna medida adicional	141

Tabla 11: Medida adicional de seguridad

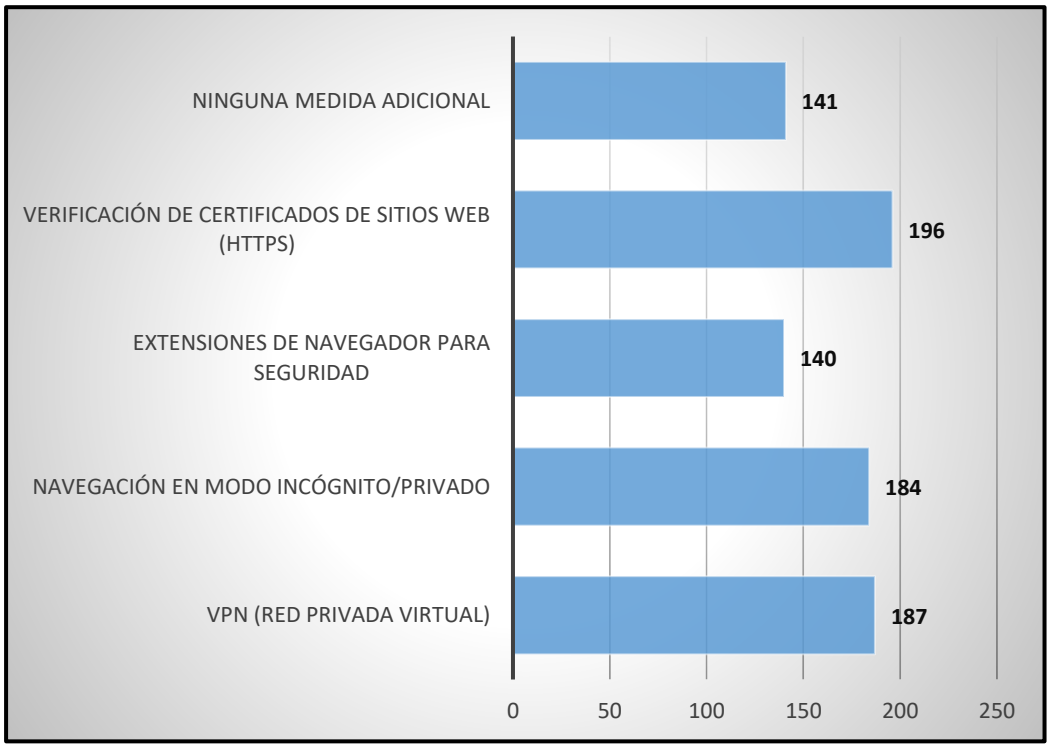


Figura 14: Medida adicional de seguridad

Interpretación: El uso de medidas de seguridad adicionales reveló que 40% emplean al menos una medida, siendo más común verificación de certificados de sitios web con 57,6%.

Conclusión: Existe una brecha de seguridad ya que el 60% de los encuestados no toma ninguna medida adicional de protección, lo que los expone a amenazas cibernéticas y se puede evidenciar la falta de cultura preventiva en ciberseguridad.

Ítem 12: ¿Con qué frecuencia cambia sus contraseñas?

Respuesta	Frecuencia	Porcentaje
Cada 1-3 meses	64	18,8 %
Cada 6 meses	65	19,1 %
Una vez al año	88	25,9 %
Solo cuando me lo solicitan o cuando olvido mi contraseña	67	19,7 %
Nunca	56	16,5 %
TOTAL	340	100 %

Tabla 12: Frecuencia de cambio de contraseña

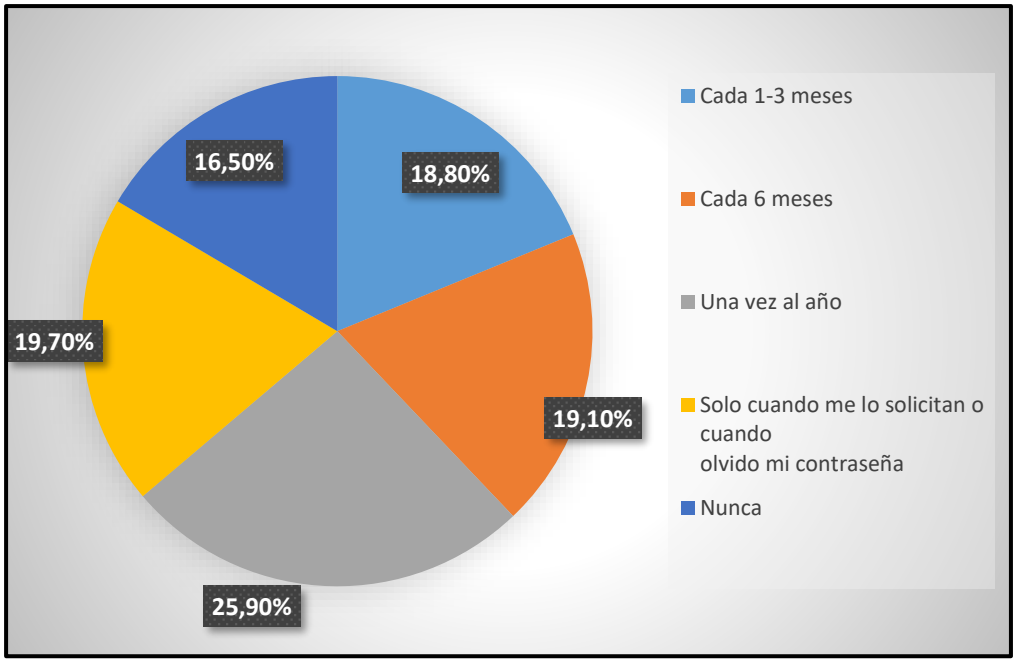


Figura 15: Porcentaje del cambio de contraseña

Interpretación: Se puede evidenciar que 19,1% de los usuarios realizan cambios proactivos con regularidad en contraste con el 36,2% de los usuarios son reactivos o no cambian la contraseña nunca. La práctica de alguien que nunca cambia su contraseña (16,5%) aumenta la ventana de oportunidad para un compromiso a través de ataques de fuerza bruta o mediante la reutilización de credenciales viejas.

Conclusión: Los registros de credenciales capturadas por el honeypot puede mostrar si contraseñas institucionales están siendo reutilizadas en ataques externos.

Ítem 13: ¿Ha experimentado alguno de los siguientes problemas al usar la red estudiantil? (Puede seleccionar varios)

Respuesta	Frecuencia
Ralentización inexplicable de conexión	163
Desconexión frecuente	164
Redirección a páginas web sospechosas	126
Ventanas emergentes (pop-ups) excesivas	126
Mensajes de advertencia de seguridad	164
Ninguno	120

Tabla 13:Experiencia de problemas al usar la red

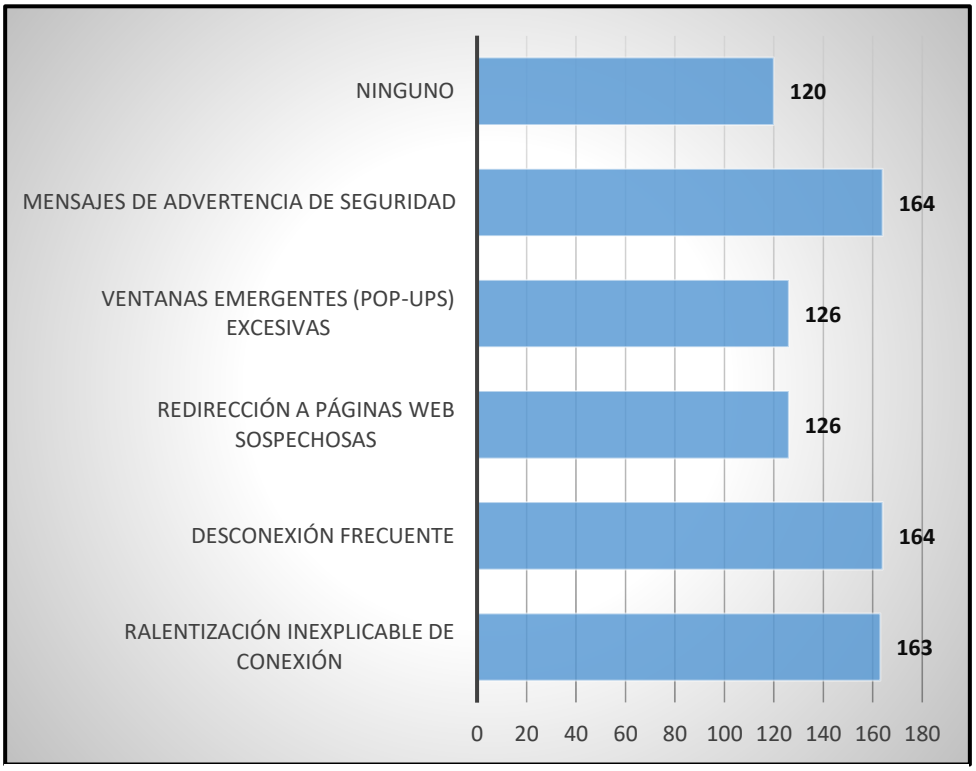


Figura 16: Porcentaje de experiencia de problemas al usar la red

Interpretación: El análisis reveló que 48,2% experimentaron al menos un problema, siendo más común mensajes de advertencia de seguridad con 164 menciones.

Conclusión: La muestra de errores reportados puede también justificar la necesidad de una más avanzada monitorización a través de honeypot para diferenciar si se tratase de problemas técnicos.

Ítem 14: ¿Se siente cómodo/a ingresando información personal o confidencial mientras está conectado/a a la red estudiantil?

Respuesta	Frecuencia	Porcentaje
Sí, muy cómodo	91	26,8 %
No, nada cómodo	133	39,1 %
Depende del tipo de información	116	34,1 %
TOTAL	340	100 %

Tabla 14: Confianza en la red

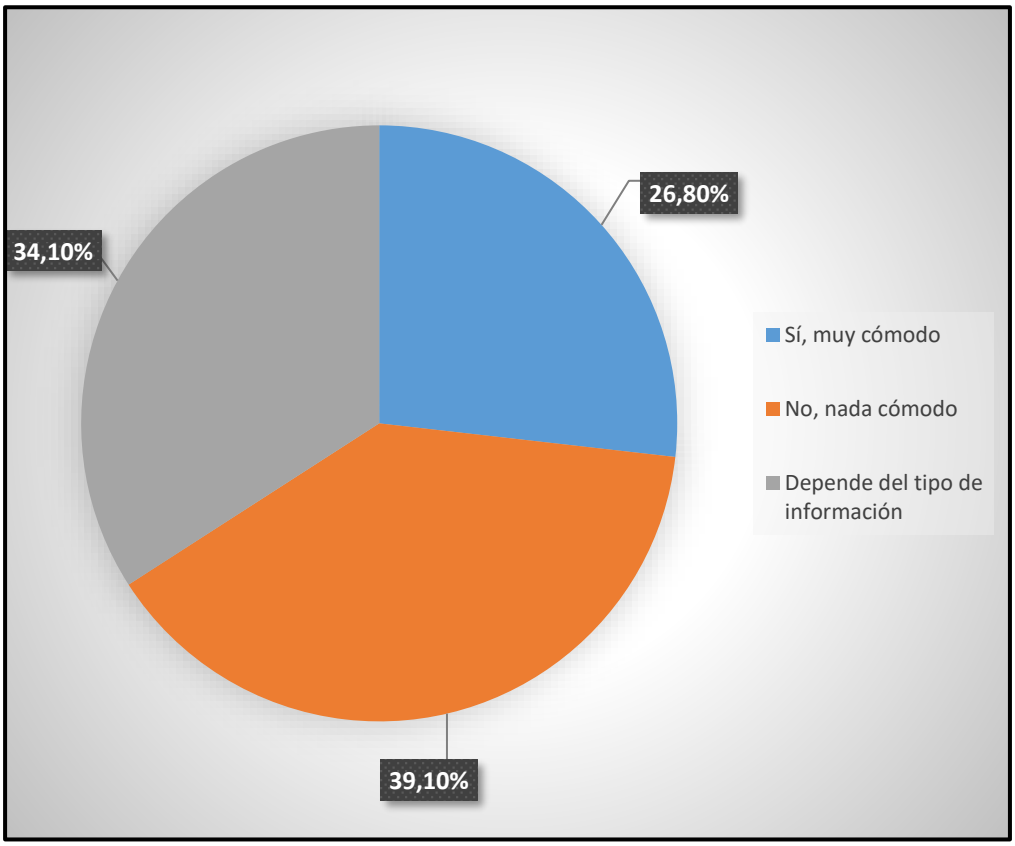


Figura 17: Porcentaje de confianza en la red

Interpretación: Se muestra que el 26,8 % de los usuarios está sienten cómodos y el 34,1 % es cauteloso; sin embargo, un 39,1 % de los usuarios dijo que no estaba cómodo en absoluto.

Conclusión: Se tiene una sensación general de inseguridad con más de un 30 % de los estudiantes que consideran que sus datos personales no están seguros, esto evidencia la necesidad de reforzar las medidas de seguridad en la universidad.

2. CAPÍTULO II PROPUESTA

2.1. Marco Contextual

La Universidad Estatal Península de Santa Elena (UPSE) es una institución de educación superior pública ubicada en la provincia de Santa Elena, Ecuador, que ha experimentado un crecimiento significativo en su matrícula estudiantil y expansión de servicios tecnológicos durante la última década. La institución atiende a más de 15,000 estudiantes distribuidos en diversas facultades. Este crecimiento ha generado una demanda creciente de servicios de conectividad y acceso a recursos digitales, posicionando a la universidad como un referente regional en la implementación de tecnologías educativas.

La infraestructura tecnológica de la universidad dispone de una red para estudiantes llamada "ESTUDIANTES", en la cual se brinda acceso gratuito y sin una autenticación a recursos de internet y servicios institucionales. Esta configuración, si bien facilita el acceso en el ámbito académico y contribuye a la inclusión digital, constituye un reto desde el punto de vista de la seguridad informática por la falta de controles estrictos sobre el acceso y monitoreo de los dispositivos de los usuarios. La red estudiantil es una red abierta la cual prioriza la facilidad de uso en contra medidas de seguridad, es un hecho muy común entre instituciones de educación donde tratan de equilibrar accesibilidad con protección de datos.

En la Facultad de Sistemas y Telecomunicaciones de la UPSE existe una infraestructura de servidores centralizada que puede soportar los servicios académicos incluyendo plataformas de aprendizaje. Esta infraestructura procesa grandes volúmenes de información académica y del personal estudiantil, docentes y personal administrativo, convirtiéndose así en un objetivo para potenciales atacantes que buscan acceder a bases de datos educativas. La centralización de servicios es eficiente desde un punto de vista operativo pero tiene riesgos de seguridad en puntos críticos que requieren un monitoreo.

La implementación de un sistema honeypot en el campo universitario ecuatoriano propone una aproximación novedosa que aprovecha las características específicas del entorno académico para generar inteligencia de seguridad. El proyecto se

enmarca en un momento de creciente concienciación sobre la importancia de la ciberseguridad en el sector educativo, coincidiendo con iniciativas gubernamentales de fortalecimiento de capacidades digitales y programas de transformación tecnológica en universidades públicas. Esta convergencia de factores crea un contexto favorable para la implementación del sistema.

2.2. Marco Conceptual

2.2.1. Honeypot

Un honeypot es un sistema diseñado para simular servicios vulnerables con el propósito de atraer y registrar actividades maliciosas permitiendo así el análisis detallado de técnicas y tácticas utilizadas por atacantes [24]. Es fundamental comprender que los honeypots no constituyen un reemplazo de los sistemas tradicionales de seguridad, sino que funcionan como elementos complementarios que enriquecen la arquitectura defensiva mediante la provisión de inteligencia sobre amenazas [41]. Su valor se centra en la capacidad de generar información sobre vectores de ataque (ver Figura 18), herramientas utilizadas por los ciberdelincuentes y patrones de comportamiento malicioso [15].

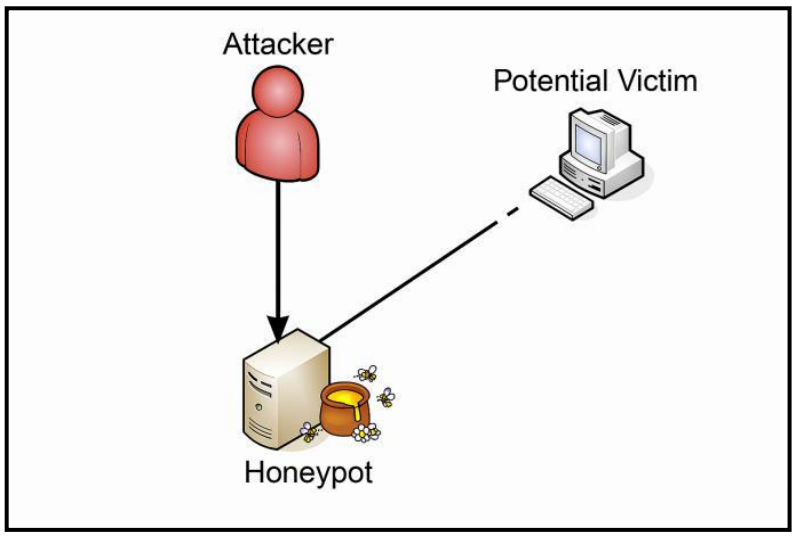


Figura 18: Funcionamiento básico de un sistema Honeypot

2.2.2. Virtualización

La virtualización es una técnica fundamental que permite la creación de entornos simulados por medio de un software facilitando así la instalación del sistema

honeypot sin comprometer la infraestructura real de la organización [42]. Esta tecnología proporciona el aislamiento necesario para que los sistemas señuelo puedan operar de manera controlada, minimizando los riesgos asociados con la exposición a actividades maliciosas [43]. Herramientas como VMware y VirtualBox han demostrado ser efectivas para este propósito ofreciendo plataformas que permiten la creación, configuración y gestión de múltiples entornos virtualizados [44].

2.2.3. Análisis de Logs y Procesamiento de Información

El análisis de log es una actividad que consiste en examinación sistemática de logs producidos por los sistemas para descubrir patrones de ataque y conducta anómala [45]. En relación a los honeypots en particular, los logs son relevantes ya que proveen una completa captura de las interacciones maliciosas incluyendo IPs origen, las técnicas de explotación usadas y los comandos a las que estas fueron sometidas [46]. El nivel de detalle en la información contenida en estos logs hace que sea capaz no sólo de detectar amenazas concretas sino también de generar perfiles de comportamiento que ayuden a robustecer los mecanismos de detección y respuesta [47].

2.2.4. Amenazas Cibernéticas Contemporáneas

Las amenazas cibernéticas comprenden un espectro amplio de riesgos asociados a actividades maliciosas que incluyen phishing, distribución de malware y explotación de vulnerabilidades de software, todas las cuales pueden comprometer gravemente la confidencialidad, integridad o disponibilidad de los datos organizacionales [23]. Estas amenazas han evolucionado tanto en sofisticación como en frecuencia, requiriendo enfoques más dinámicos y adaptativos para su detección y mitigación [48]. En el contexto específico de los entornos educativos, se amenazas se vuelven más graves debido a características propias de las instituciones como el hecho de que sus redes suelen ser de acceso abierto, la diversidad de usuarios con diferentes niveles de conocimiento técnico y la falta de concienciación sobre prácticas de seguridad [3]. Para mitigar con éxito las repercusiones de las amenazas modernas y mejorar la resiliencia digital de las instituciones educativas, estas deben abordar sus retos de manera holística.

2.2.5. Sistemas de Detección y Prevención de Intrusiones

Los sistemas de detección de intrusiones (IDS) y prevención de intrusiones (IPS) como Suricata constituyen herramientas que identifican y bloquean actividades maliciosas en redes, basándose en firmas de ataques conocidos o comportamientos anómalos [49]. Estas tecnologías forman parte del monitoreo de red, una práctica esencial para detectar actividades anómalas en tiempo real que permite la identificación temprana de amenazas y la respuesta ante incidentes de seguridad [50]. El monitoreo de red facilita la detección de comportamientos anómalos, definidos como actividades inusuales en redes tales como escaneos de puertos no autorizados, intentos de acceso sospechosos o patrones de tráfico irregulares [51]. Cuando se implementan en combinación con honeypots, el monitoreo a la red permite una aproximación ante posibles incidentes de seguridad ya que las interacciones con los sistemas señuelo pueden servir como indicadores tempranos de actividad maliciosa dirigida hacia la infraestructura real [52].

2.3. Marco Teórico

Análisis Y Estudio De Honeynets En Entorno Doméstico E Institucional.

Esta investigación desarrollada por Pablo Javier Barrio Navarro se centra en la creciente importancia de las Honeynets y Honeypots para la detección y análisis de amenazas en las redes [24]. La investigación remarca cómo el avance tecnológico ha dado paso a la creación de entornos controlados que atraen y registran ataques cibernéticos, facilitando la comprensión de las técnicas empleadas por los ciberdelincuentes y permitiendo fortalecer las defensas de los sistemas [53].

Pablo concluye que las Honeynets y Honeypots son herramientas fundamentales en la lucha contra las amenazas cibernéticas, ya que estas recopilan y muestra información valiosa para comprender técnicas de intrusión y mejorar las medidas de protección [54]. Es importante mantener actualizadas estas tecnologías y ajustar las configuraciones a los cambios en las tácticas de los cibercriminales, teniendo una respuesta proactiva ante el incremento de ciberataques en diversos entornos [55]. La obra de Barrio Navarro demuestra que las Honeynets y Honeypots no son solo herramientas experimentales, sino elementos estratégicos en la ciberdefensa.

Implementación De Una Herramienta Honeypot Para Detección Y Respuesta A Ataques.

Yury Avilés estableció que los honeypots no sustituyen los sistemas tradicionales de seguridad, por el contrario, refuerzan la postura defensiva al ofrecer un ambiente controlado para atraer y analizar actividades maliciosas de cibercriminales [56]. Así mismo destaca que la efectividad de estos dispositivos depende de una correcta implementación, configuración y ubicación en la red, los honeypots también pueden ser usados para proteger entornos reales [57]. La investigación permite revisar cómo los honeypots captan ataques desconocidos, la inteligencia sobre las técnicas empleadas por los atacantes y también mejorar la capacidad de respuesta frente amenazas cada vez mejor elaboradas [58]. La investigación evidencia que cuando se integran de forma correcta los honeypots aportan a fortalecer la seguridad de las organizaciones en un entorno digital [41].

Propuesta De Implementación De Un Honeypot De Seguridad Informática En La Agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.

Terrones Víctor en su trabajo de investigación aborda la creciente amenaza de ataques cibernéticos que desafía la integridad de la información de la empresa por el aumento de los ciberdelitos, la necesidad de implementar mecanismos de protección efectivos se vuelve cada vez más indispensable [42].

A fin de realizar este trabajo se planteó una revisión sobre la percepción del personal y las vulnerabilidades existentes en la seguridad corporativa [59]. Se utilizó el enfoque metodológico PPDIOO de Cisco para seguir un proceso estructurado en el diseño, la implementación y administración del honeypot, empleándose los entornos virtuales VirtualBox para recrear escenarios reales sin arriesgar la infraestructura. El estudio también se enfocó en la elaboración de diagramas de flujo, procedimientos y protocolos orientados a fortalecer la gestión de tareas asociadas a la protección de la red [42]. Esta propuesta no solo evidenció la viabilidad de incorporar un honeypot como herramienta de defensa digital, sino que además resaltó la importancia de integrar prácticas de monitoreo continuo y análisis forense como parte fundamental de una estrategia integral de ciberseguridad. [42].

Implementación De Honeypots Mediante T-Pot Para Mejora De La Seguridad Corporativa.

En esta investigación, Angel Camuñas trata el reto que las ciberamenazas suponen para las organizaciones actuales, en las que los métodos de seguridad tradicionales son insuficientes [60]. La investigación se focaliza en la implementación de honeypots y honeynet como sistemas señuelos avanzados que permiten atraer a potenciales atacantes, dando una cobertura de seguridad más efectiva [60].

Para la realización de este trabajo, Angel, utilizó la solución virtualizada T-Pot como plataforma para la implementación de los honeypots, que posibilita la obtención sistematizada de información sobre comportamientos maliciosos [61]. La metodología siguió un análisis en profundidad de las series de ataque, técnicas de los delincuentes y la cobertura ofrecida a aquellas vulnerabilidades que no pueden ser encontradas por sistemas convencionales [62]. El proyecto se enfocó en convertir los datos recopilados por los honeypots en inteligencia de seguridad que incluían el estudio de comportamientos de atacantes y técnicas de explotación para mejorar las defensas organizacionales [53].

2.4. Marco Normativo

La investigación titulada "Implementación de un sistema Honeypot en los servidores de FACSISTEL, mediante virtualización y análisis de logs para monitorear y prevenir amenazas cibernéticas en la red de estudiantes de la UPSE" se sustenta en el marco jurídico nacional e internacional que regula la seguridad informática, la protección de datos y el uso de tecnologías de la información en instituciones de educación superior.

Normativa	Artículo / Sección	Relación con la Investigación
Constitución de la República del Ecuador (2008)	Art. 66, numeral 19	Garantiza el derecho a la protección de datos personales, respaldando la necesidad de mecanismos de seguridad en los servidores universitarios [63].

Código Orgánico Integral Penal – COIP (2014)	Arts. 229–232	Describe todos los delitos informáticos y que respalda el despliegue de honeypots para evitar accesos no autorizados [64].
Ley Orgánica de Educación Superior – LOES (2010, reformada)	Art. 8	Obliga a las universidades a garantizar un entorno académico seguro con acceso protegido a las TIC [65].
Ley Orgánica de Protección de Datos Personales (2021)	Arts. 3–7 (principios)	Establece la obligación de proteger la información digital [66].
Política Nacional de Seguridad de la Información (MINTEL)	Lineamientos estratégicos	Fomenta la implementación de sistemas de monitoreo y protección contra ciberataques en instituciones públicas [67].
Normas ISO/IEC 27001 y 27002	Estándares internacionales de seguridad de la información	Brindan directrices para la gestión de la seguridad de la información y controles técnicos, como la implementación de honeypots para detección temprana de amenazas [68].

Tabla 15: Marco normativo

En este sentido, la Constitución de la República del Ecuador reconoce como derecho fundamental la protección de los datos personales y el acceso seguro a la información, lo que justifica la exigencia de implementación de medidas de seguridad digital en la infraestructura universitaria. Esta disposición legal permite

fundamentar la implementación de herramientas tecnológicas orientadas a salvaguardar la integridad de la información y fortalecer la confianza en el uso de servicios digitales en el ámbito académico [69].

El Código Orgánico Integral Penal (COIP) tipifica como delito informático el acceso no autorizado a sistemas, la interceptación ilícita de datos y la alteración de información almacenada en sistemas [70]. Estas leyes regulan la necesidad de que las entidades establezcan mecanismos de protección para la detección de intentos de vulneración a la seguridad. En tal sentido es que la implementación de un sistema honeypot en la facultad de sistemas y telecomunicaciones se plantea como un mecanismo de defensa activa ante eventuales ataques cibernéticos que otorga una documentación minuciosa de ellos y da pie a estudiar a los atacantes.

De igual manera, la Ley Orgánica de Educación Superior – LOES establece la obligación de las universidades de garantizar un entorno académico seguro, promoviendo el uso responsable y protegido de las tecnologías de la información y comunicación [65]. Esto implica que las instituciones de educación superior deben contar con políticas y herramientas que aseguren la disponibilidad, integridad y confidencialidad de los servicios tecnológicos. Por lo tanto, la implementación del sistema Honeypot se alinea con las disposiciones de la LOES, ya que busca garantizar un ambiente confiable de acceso a la red estudiantil y reducir los riesgos derivados de amenazas cibernéticas.

También la Ley Orgánica de Protección de Datos Personales dispone principios básicos como: seguridad, confidencialidad y responsabilidad en el tratamiento de datos personales que deben ser observados por las instituciones públicas y privadas [71]. Esta regulación resulta aplicable en nuestro trabajo dado a que el sistema honeypot estará recolectando los registros de acceso dentro de la red universitaria, con la necesidad de ser manejados bajo estándares legales que protejan y aseguren la privacidad y adecuada protección de la información obtenida. Así, la propuesta cumple no solo con aspectos técnicos, sino también con un marco jurídico que regula el manejo ético de los datos digitales [66].

Por último. es necesario atender la Política Nacional de Seguridad de la Información y las normas internacionales de la serie ISO 27001 e ISO 27002, las cuales

representan directrices estratégicas y buenas prácticas para la gestión de la seguridad de la información. [67]. Estas directrices internacionales sugieren la adopción de controles técnicos que permitan una detección temprana de amenazas y fortalezcan la resiliencia de las instituciones frente a ciberataques [72]. En este sentido, la implementación del sistema Honeypot en los servidores de FACSISTEL se presenta como una medida alineada tanto a las políticas nacionales como a estándares globales, asegurando que la propuesta tenga un respaldo legal y técnico que garantice su pertinencia, viabilidad y sostenibilidad en el tiempo.

2.5. Requerimientos

La implementación del sistema honeypot en la facultad de sistemas y telecomunicaciones (FACSISTEL) se orienta a posibilitar un registro sistemático y automatizado del tráfico malicioso, mimetizándose en servicios de red reales para captar interacciones de atacantes. Este sistema debe centralizar y procesar la información con herramientas tales como Elastic Stack permitiendo un análisis detallado y monitoreo en tiempo real. Adicionalmente debe satisfacer elevados niveles de aislamiento y disponibilidad para permitir una confiable investigación en ciberseguridad.

Requerimiento	Descripción
Registro sistemático del tráfico malicioso	El sistema podrá registrar información precisa, como la dirección IP de origen, el puerto, el protocolo, la fecha y hora del evento.
Emulación de servicios de red	Simular servicios como SSH, Telnet, HTTP, HTTPS y FTP, permitiendo interacción natural con atacantes, registrando credenciales, comandos y archivos descargados. Integrar

	herramientas como Cowrie para SSH/Telnet.
Procesamiento centralizado de logs	Centralizar, procesar y almacenar registros de eventos usando Elastic Stack para indexación estructurada, consultas rápidas y análisis detallados, garantizando integridad y persistencia de datos.
Clasificación y correlación de eventos	Clasificar los eventos en función de la naturaleza del ataque, el vector empleado, su ubicación geográfica y el nivel de sofisticación que ha exhibido el atacante. Este procedimiento da cabida a la agrupación en patrones significativos, diferenciando entre actividades automatizadas, ataques selectivos y prospecciones preliminares.
Visualización en tiempo real	Proporcionar monitoreo continuo mediante paneles en Kibana, mostrando métricas como ataques por unidad de tiempo, distribución geográfica de los orígenes maliciosos, servicios más frecuentemente atacados, técnicas empleadas por los atacantes y tendencias temporales asociadas al comportamiento de las amenazas.

Generación automatizada de informes técnicos	Producir reportes periódicos con estadísticas, indicadores de compromiso, patrones de comportamiento y recomendaciones, mediante scripts que procesen datos almacenados.
Aislamiento completo de la red	Ejecutar en entorno virtualizado segregado de la infraestructura de producción, con segmentación de red y controles estrictos para evitar uso como punto de apoyo por atacantes.
Capacidad de procesamiento y almacenamiento	Dimensionar recursos para emular servicios y procesar logs en tiempo real sin cuellos de botella, contemplando crecimiento de datos.

Tabla 16: Requerimientos

2.6. Fase 1: Investigación Y Análisis Preliminar

2.6.1. Propósito de los Sistemas Honeypot en Ciberseguridad

2.6.1.1. Definición de Honeypot

Un honeypot es un sistema de señuelo computacional diseñado específicamente para simular servicios y recursos vulnerables con el objetivo fundamental de atraer, engañar y registrar las actividades maliciosas ejecutadas por atacantes cibernéticos

[73]. Estos sistemas operan como trampas digitales que tratan de imitar a las infraestructuras reales pero no tienen valor productivo, permitiendo así la captura y análisis detallado de comportamientos hostiles sin comprometer sistemas críticos de la organización [74]. La funcionalidad principal de un honeypot está en su capacidad para generar inteligencia de amenazas mediante la observación pasiva de técnicas, tácticas y procedimientos empleados por actores maliciosos [75].

A diferencia de los sistemas defensivos que operan bloqueando ataques, los honeypots toman un enfoque proactivo permitiendo que las intrusiones ocurran en un entorno controlado [76]. Esta aproximación facilita la comprensión profunda de las metodologías empleadas por atacantes, incluyendo herramientas utilizadas, vulnerabilidades explotadas y patrones de comportamiento específicos [77]. Los honeypots funcionan como laboratorios de seguridad en vivo donde es posible estudiar amenazas emergentes y técnicas de ataque novedosas que podrían no ser detectadas por sistemas convencionales de monitoreo [78].

2.6.1.2. Propósito Estratégico en Ciberseguridad

El propósito de los sistemas honeypot en el ámbito de la ciberseguridad se alinean en varios niveles estratégicos, los cuales complementan las arquitecturas tradicionales de seguridad [79]. Lo anterior implica que pueda desempeñar una función de aviso temprano de amenazas, dando alertas de actividad maliciosa que podría estar encaminándose hacia sistemas productivos [80]. Esta capacidad para detectar anticipadamente actividades maliciosas es particularmente útil en escenarios donde los métodos de monitoreo tradicionales no podrían detectar ataques nuevos [81]. La implementación de los honeypots permite a las organizaciones mantenerse un paso más adelante ante las amenazas mediante la captura de inteligencia sobre nuevas técnicas de explotación [82].

La generación de inteligencia de amenazas representa otro propósito crítico, facilitando la comprensión profunda de las metodologías empleadas por atacantes específicos [83]. Los honeypots pueden capturar información de las herramientas utilizadas y vulnerabilidades explotadas estos datos pueden utilizarse para fortalecer defensas organizacionales para desarrollar contramedidas efectivas [84]. Esta información es valiosa para la generación de firmas de detección [85].

Estos sistemas tienen una función preventiva debido a que incrementa la incertidumbre por parte de los atacantes quienes deben invertir tiempo y recursos adicionales para poder distinguir entre objetivos reales y los simulados [86]. Esta cualidad ayuda a elevar la complejidad de los ataques y puede desalentar a los atacantes con poca experiencia [87]. La presencia de los honeypots en una red también puede retardar el progreso de un atacante, dando tiempo extra para que el equipo de seguridad responda a las amenazas antes de que puedan acceder a los activos críticos [88].

2.6.2. Clasificación de Honeypots según Nivel de Interacción

2.6.2.1. Honeypots de Baja Interacción

Los honeypots de baja interacción constituyen implementaciones simplificadas que emulan únicamente funcionalidades básicas de servicios de red específicos [89]. Estos sistemas operan mediante la simulación limitada de protocolos y servicios, respondiendo a interacciones básicas, pero careciendo de la capacidad para ejecutar comandos complejos o proporcionar acceso completo al sistema operativo simulado [90]. La arquitectura de estos honeypots se basa en scripts predefinidos y respuestas automatizadas que simulan comportamientos esperados de servicios legítimos, aunque con funcionalidades reducidas que pueden resultar evidentes para atacantes experimentados [91].

Las características técnicas principales incluyen la emulación superficial de servicios mediante respuestas predefinidas, recursos computacionales mínimos requeridos para operación, riesgo reducido de compromiso del sistema anfitrión, capacidad limitada para capturar técnicas de post-explotación avanzadas y facilidad de despliegue y mantenimiento simplificado [92]. Estos sistemas resultan particularmente efectivos para la detección de escaneos automáticos, ataques de fuerza bruta básicos y técnicas de reconocimiento rudimentarias [93]. Su implementación requiere configuración mínima y pueden desplegarse rápidamente en múltiples puntos de la red para proporcionar cobertura extensiva de monitoreo [94].

Las ventajas operacionales incluyen implementación rápida con configuración mínima, consumo reducido de recursos del sistema, menor superficie de ataque

contra la infraestructura del honeypot y adecuación para detección de escaneos automáticos y ataques masivos [95]. Sin embargo, presentan limitaciones significativas como la incapacidad para engañar atacantes experimentados por períodos prolongados, recolección limitada de información sobre técnicas de explotación avanzadas y falta de interactividad realista que podría alertar a atacantes sofisticados sobre la naturaleza del señuelo [96].

2.6.2.2. Honeypots de Media Interacción

Los honeypots de media interacción representan una solución intermedia que proporciona mayor realismo en la simulación de servicios mientras mantiene un nivel controlado de funcionalidad [97]. Estos sistemas implementan emulaciones de sistemas operativos y aplicaciones, permitiendo interacciones más complejas sin proporcionar acceso completo a un sistema real [98]. La arquitectura técnica de estos honeypots posee la implementación de shells simulados, sistemas de archivos virtuales y respuestas dinámicas que se adaptan a las acciones del atacante, creando una experiencia más realista [99].

Las características técnicas principales comprenden la emulación avanzada de servicios con funcionalidades específicas implementadas, capacidad para simular vulnerabilidades conocidas y respuestas del sistema, registro detallado de comandos ejecutados y archivos transferidos, e implementación de shells simulados con funcionalidades limitadas pero convincentes [100]. Estos sistemas pueden mantener atacantes comprometidos durante períodos extendidos, permitiendo la observación de técnicas de post-explotación intermedias y la captura de herramientas y scripts utilizados por los actores maliciosos [101].

Las ventajas operacionales incluyen un balance entre realismo y seguridad operacional, capacidad para mantener atacantes comprometidos por períodos extendidos, recolección de inteligencia más detallada sobre técnicas de explotación e implementación de múltiples servicios simultáneos en una plataforma única [102]. Las limitaciones identificadas comprenden complejidad incrementada en configuración y mantenimiento, recursos computacionales moderados requeridos y posibilidad de detección por parte de atacantes mediante técnicas de fingerprinting avanzadas [103]. A pesar de estas limitaciones, los honeypots de media interacción

representan la opción más equilibrada para la mayoría de las implementaciones organizacionales [104] .

2.6.2.3. Honeypots de Alta Interacción

Los honeypots de alta interacción son implementaciones completas, que utilizan sistemas operativos reales con aplicaciones funcionales, proporcionando un entorno completamente interactivo para los atacantes [105]. Estos sistemas ofrecen la máxima fidelidad en la simulación de infraestructuras objetivo, permitiendo que los actores maliciosos ejecuten técnicas completas de post-explotación, instalen herramientas personalizadas y realicen actividades que serían idénticas a las ejecutadas en sistemas de producción reales [106]. La implementación técnica requiere sistemas operativos completos, aplicaciones reales en funcionamiento y mecanismos sofisticados de monitoreo y contención [107].

Las funcionalidades técnicas más relevantes son sistemas operativos completos con aplicaciones reales en ejecución, shells totalmente funcionales, sistemas de ficheros y servicios de red, posibilidad de ejecutar malware real y observar su comportamiento, así como mecanismos de monitorización transparente y logging exhaustivo [108]. Estos ambientes pueden capturar técnicas de ataque tales como *persistence, privilege escalation, movimento lateral, y data exfiltration* [109]. La fidelidad completa del entorno permite que incluso atacantes altamente sofisticados permanezcan comprometidos durante períodos extensos sin detectar la naturaleza del señuelo [110]. Los Honeypots de alta interacción suelen utilizarse en laboratorios de investigación, centros de respuesta ante incidentes (CSIRTs) y proyectos académicos [111].

Las ventajas operacionales comprenden máximo realismo en la simulación de sistemas objetivo, capacidad para capturar técnicas de ataque completas y malware sofisticado, posibilidad de analizar técnicas de persistencia y movimiento lateral, y generación de inteligencia de amenazas de máxima calidad [111]. Sin embargo, los riesgos y consideraciones incluyen elevado riesgo de compromiso del sistema anfitrión si el aislamiento falla, recursos computacionales significativos requeridos, complejidad extrema en configuración, monitoreo y mantenimiento, y necesidad de medidas de contención para prevenir ataques hacia sistemas productivos [112].

2.6.3. Arquitecturas de Honeynets y Aplicación Práctica

2.6.3.1. Concepto de Honeynet

Una *honeynet* es una arquitectura de seguridad de red llena de honeypots interconectados, diseñada para simular un entorno organizacional [113]. Esta aproximación proporciona un ecosistema controlado donde los atacantes pueden navegar entre múltiples sistemas, permitiendo la observación de técnicas de reconocimiento lateral, escalación de privilegios y persistencia en redes corporativas. Las Honeynets operan bajo principios arquitectónicos específicos que garantizan el control de datos, la captura de información y la contención de amenazas, creando un ambiente donde es posible estudiar campañas de ataques completas y comportamientos de atacantes sofisticados [114].

El control de datos previene que los atacantes utilicen la honeynet como plataforma para lanzar ataques contra terceros, implementando mecanismos de limitación de tráfico saliente y filtrado de conexiones potencialmente maliciosas. La captura de datos registra todas las actividades maliciosas para análisis posterior, incluyendo tráfico de red, comandos ejecutados, archivos transferidos y comunicaciones entre sistemas comprometidos. La contención asegura que las actividades permanezcan dentro del entorno controlado sin afectar sistemas productivos, utilizando técnicas de aislamiento de red y virtualización para crear barreras efectivas entre el entorno de señuelo y la infraestructura real [115].

2.6.3.2. Aplicaciones Prácticas en Entornos Organizacionales

Las *honeynets* en entornos organizacionales da beneficios sustanciales a nivel de seguridad institucional [116]. En el entorno educativo estas arquitecturas pueden simular infraestructuras universitarias completas, abarcando sistemas académicos, portales estudiantiles y recursos de investigación proporcionando inteligencia específica sobre amenazas que tienen por objetivo al sector educativo. La implementación en los entornos universitarios aporta al estudio de vectores de ataque específicos que explotan las características únicas de las redes académicas, incluyendo acceso abierto y diversidad de dispositivos [117].

Los casos de uso organizacionales incluyen la detección de Amenazas Persistentes Avanzadas mediante la identificación de técnicas de reconocimiento prolongado,

análisis de métodos de persistencia en redes corporativas, documentación de técnicas de exfiltración de datos y comprensión de ciclos de vida completos de ataques dirigidos [118]. El análisis de malware *in the wild* comprende la captura de muestras de malware en entornos controlados, análisis comportamental de código malicioso, identificación de indicadores de compromiso específicos y desarrollo de firmas de detección para sistemas productivos [119].

La inteligencia de amenazas contextualizada incluye la identificación de amenazas específicas para el sector industrial, análisis de patrones geográficos y temporales de ataques, comprensión de motivaciones y objetivos de atacantes y desarrollo de perfiles de amenazas organizacionales [120]. Esta inteligencia contextualizada resulta valiosa para organizaciones que operan en sectores específicos o regiones geográficas particulares, permitiendo el desarrollo de estrategias de defensa adaptadas a las amenazas más relevantes para su contexto operacional [121].

2.6.4. Análisis de Herramientas Honeypot Especializadas

2.6.4.1. T-Pot

T-Pot representa una solución de honeypot que integra varias herramientas especializadas en una plataforma basada en contenedores [122]. Esta herramienta proporciona una implementación simplificada de honeynets complejas, incluyendo capacidades de visualización, análisis y gestión centralizadas [123]. La arquitectura basada en contenedores facilita el despliegue, mantenimiento y escalamiento de múltiples tipos de honeypots simultáneamente, mientras que la integración nativa con herramientas de análisis y visualización proporciona capacidades inmediatas de monitoreo y reporting [124]. T-Pot elimina muchas de las complejidades tradicionalmente asociadas con la implementación de honeypots, permitiendo que organizaciones sin experiencia técnica en estas tecnologías puedan beneficiarse de sus capacidades [125].

Las características técnicas únicas poseen una arquitectura basada en contenedores Docker para el aislamiento, integración de más de 20 herramientas de honeypot distintas, dashboard web para monitoreo, implementación automatizada mediante scripts de instalación y soporte de múltiples arquitecturas de hardware [126]. La

integración elimina la configuración y mantenimiento de herramientas de honeypot, permitiendo una solución turnkey que puede ser desplegada en múltiples entornos [127]. La plataforma tiene mecanismos automáticos de actualización y mantenimiento que reducen la carga operacional asociada con la gestión de honeypots [128].

Los componentes integrados principales son Cowrie para emulación de servicios de **Secure Shell** (SSH) y Telnet, *Dionaea* para captura de malware, *Honeytrap* para emulación de servicios **Transmission Control Protocol/ User Datagram Protocol** (TCP/UDP), *Suricata* para detección de intrusiones y Elastic Stack para análisis y visualización de datos [129]. Las ventajas operacionales suponen un despliegue fácil con configuración mínima, escalabilidad horizontal agregando nodos, correlación de eventos automáticamente entre honeypots, así como actualización automática de componentes. [130]. Esta integración hace que las organizaciones puedan disfrutar de las ventajas de múltiples tipos de honeypots y a la vez tener la complicación de gestionar una única herramienta.

2.6.4.2. Infraestructura de Análisis y Visualización

El núcleo de *T-Pot* se fundamenta en la implementación de la pila *ELK*, proporcionando capacidades a nivel empresarial para gestión, análisis y visualización de los datos de seguridad capturados [131]. Elasticsearch constituye el motor de almacenamiento y búsqueda distribuida que indexa todos los eventos y logs generados por los múltiples honeypots desplegados, proporcionando capacidades de consulta en tiempo real sobre volúmenes masivos de datos [132]. La arquitectura de Elasticsearch permite escalamiento horizontal mediante la adición de nodos adicionales, asegurando que el sistema pueda manejar el crecimiento del volumen de datos sin degradación del rendimiento [133].

Logstash actúa como el pipeline de procesamiento de datos, responsable de la ingesta, transformación, enriquecimiento y envío de eventos hacia Elasticsearch [134]. Este componente convierte a un formato común los logs de varios honeypots, filtra y transforma para extraer campos relevantes, enriquece los datos con información geográfica basada en direcciones IP y realiza correlaciones preliminares antes del almacenamiento [135]. La flexibilidad de Logstash permite

la implementación de pipelines de procesamiento personalizados adaptados a las necesidades específicas del análisis de amenazas [136].

Kibana proporciona la interfaz de usuario web para visualización, análisis y exploración de los datos almacenados en Elasticsearch [137]. Esta herramienta ofrece capacidades avanzadas de creación de dashboards interactivos, visualizaciones geográficas de origen de ataques, gráficos temporales de actividad maliciosa, tablas de análisis de credenciales capturadas y reportes de indicadores de compromiso identificados [138]. Los dashboards previamente configurados de T-Pot proporcionan visualizaciones inmediatas de métricas clave incluyendo volumen de ataques por honeypot, distribución geográfica de atacantes, servicios más atacados, técnicas de explotación más frecuentes y tendencias temporales de actividad maliciosa [139]. La capacidad de crear consultas personalizadas y visualizaciones ad-hoc facilita la investigación profunda de incidentes específicos y el análisis de patrones complejos de comportamiento [140].

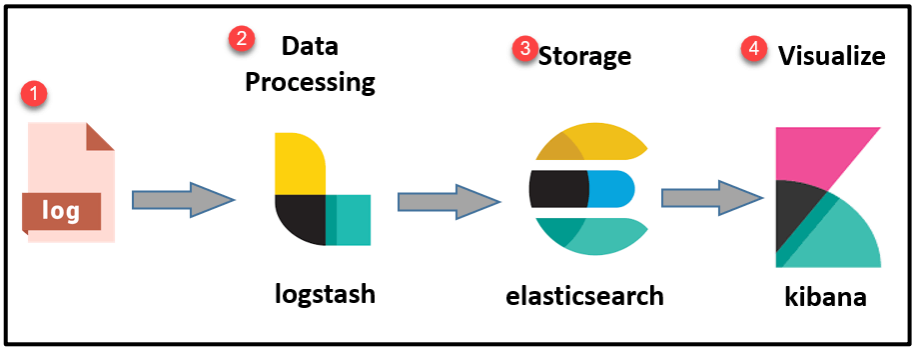


Figura 19: Arquitectura de pila ELK

Nota. Fuente: David Carter

2.6.4.3. Herramientas de Monitoreo

T-Pot posee herramientas especializadas de monitoreo de seguridad de red y análisis de datos que complementan las capacidades de los honeypots, proporcionando capas adicionales de detección e inteligencia. Suricata opera como motor de monitoreo de seguridad de red, analizando el tráfico dirigido hacia los honeypots para identificar patrones de ataque, técnicas de explotación y comunicaciones de comando y control [141]. La capacidad de Suricata para

inspección profunda de paquetes y extracción de archivos complementa la inteligencia capturada por los honeypots mediante el análisis del contexto de red más amplio [142].

CyberChef ofrece una aplicación web para encriptar, codificar, decodificar, comprimir y analizar datos capturados, actuando como un laboratorio digital para los analistas de seguridad [143]. Esta utilidad permite analizar payloads codificados, scripts ofuscados o datos exfiltrados vistos en ataques [144]. Elasticvue ofrece una interfaz web moderna para facilitar la navegación y ejecución directa con el clúster Elasticsearch [145].

2.6.4.4. Cowrie

Cowrie constituye un honeypot de media interacción especializado en la emulación convincente de servicios SSH y Telnet [146]. Esta herramienta proporciona un shell simulado que permite a los atacantes ejecutar comandos, descargar archivos y realizar actividades post-explotación mientras registra todas las interacciones [147]. La emulación incluye respuestas realistas a comandos del sistema, simulación de sistemas de archivos con contenido convincente y comportamientos que imitan fielmente sistemas Unix/Linux reales [148]. Cowrie ha evolucionado para convertirse en uno de los honeypots SSH más ampliamente deployados debido a su efectividad para capturar actividades de atacantes y la calidad de la inteligencia que genera [149].

Las funcionalidades especializadas contienen emulaciones completas de shells bash, simulación de sistemas de archivos con diversos contenidos realistas, capturas de credenciales utilizadas en ataques de fuerza bruta, incorpora mecanismos integrados para la captura de malware mediante la interceptación de intentos de descarga, registro de comandos ejecutados y archivos transferidos [150]. La herramienta puede simular múltiples usuarios del sistema con diferentes niveles de privilegios, crear respuestas personalizadas a comandos específicos y mantener sesiones de atacantes durante períodos extendidos sin revelar su naturaleza de señuelo, incrementando significativamente la cantidad y calidad de los datos recolectados para fines de análisis, monitoreo y correlación de eventos de seguridad [151].

2.6.4.5. Dionaea

Dionaea representa un honeypot de baja interacción específicamente diseñado para la captura y análisis de malware que se propaga a través de vulnerabilidades de red [152]. Esta herramienta emula servicios vulnerables que son típicamente explotados por gusanos y botnets, permitiendo la extracción de muestras de código maliciosos al ofrecer una convincente capa de emulación basada en vulnerabilidades conocidas en servicios de red populares [153]. La especialización de Dionaea en captura de malware la convierte en un elemento complementario clave para mayores ecosistemas de honeypots, aportando capacidades específicas para el análisis de amenazas automatizadas y campañas de malware masivas [154].

Los servicios emulados especializados incluyen protocolos SMB/CIFS para captura de malware de red, servicios HTTP/HTTPS con vulnerabilidades simuladas, emulación de servicios FTP con funcionalidades básicas, protocolos de bases de datos como MySQL y MSSQL, y servicios de correo electrónico SMTP simulados [155]. La emulación de estas vulnerabilidades específicas permite atraer diferentes tipos de malware y campañas de ataques automatizados, proporcionando una visión del paisaje de amenazas que afecta a servicios comúnmente deployados en entornos corporativos [156].

Las capacidades de análisis de malware comprenden descarga automática de payloads maliciosos, análisis básico de ejecutables capturados, integración con motores de análisis de malware externos, generación de hashes criptográficos para identificación de muestras y envío automático de muestras a plataformas de análisis como VirusTotal [157]. Esta integración con servicios externos de análisis permite que las organizaciones obtengan inteligencia inmediata sobre las muestras de malware capturadas, incluyendo información sobre familias de malware, técnicas utilizadas e indicadores de compromiso asociados [158].

2.6.4.6. Conpot

Conpot es un honeypot de alto nivel que permite la simulación de Sistemas de Control Industrial y entornos de automatización incluyendo sistemas SCADA, controladores lógicos programables y dispositivos utilizados en tecnologías operativas. Esta herramienta es fundamental para identificar amenazas a

infraestructuras críticas tales como plantas de energía, sistemas de tratamiento de agua, plantas de fabricación y otro tipo de ambientes industriales donde una violación de seguridad podría acarrear severas consecuencias físicas.

2.6.4.7. Heralding

Es un *honeypot* especializado en la captura de credenciales utilizadas en intentos de autenticación contra diversos protocolos de red comunes [159]. La herramienta simula servicios de autenticación para *FTP, Telnet, SSH, HTTP, POP3, IMAP, SMTP, VNC* y *PostgreSQL*, registrando todas las combinaciones de usuario y contraseña intentadas por atacantes durante ataques de fuerza bruta [160]. La especialización de Heralding en captura de credenciales genera inteligencia sobre las credenciales comprometidas circulando en el ecosistema de cibercrimen [161].

2.6.4.8. Elasticpot

Elasticpot es un honeypot dedicado a simular instancias de *Elasticsearch* vulnerables y captura a los atacantes que explotan configuraciones vulnerables de esta plataforma de búsqueda [162]. ha sido un blanco común debido a instalaciones configuradas incorrectamente que permiten acceso sin autenticación, exfiltración de datos indexados y ejecución de código mediante características de scripting [163]. Elasticpot reproduce estas vulnerabilidades en un ambiente controlado donde captura los ataques, consultas maliciosas y técnicas de extracción de datos utilizadas por atacantes que tienen como objetivo bases de datos Elasticsearch expuestas [164].

2.6.4.9. Honeypots de Aplicaciones Web

Snare y *Tanner* funcionan como sistemas de honeypot distribuido para aplicaciones web en el cual Snare actúa como frontend ya que captura solicitudes HTTP que van dirigidas a las aplicaciones web simuladas, mientras que Tanner trabaja como backend analizando el tráfico y posteriormente pudiera detectar intentos de explotación y generando respuestas dinámicas [165]. La arquitectura distribuida permite una emulación escalable de varias aplicaciones web, con Snare replicando las páginas web verdaderas y Tanner evaluando cada solicitud para poder determinar si se trata de un intento de ataque [166]. Este sistema puede simular

vulnerabilidades comunes de aplicaciones web incluyendo inyección SQL, cross-site scripting, inclusión de archivos remotos y directory traversal [167]. La integración entre ambos componentes facilita la obtención de registros.

2.6.4.10. Honeypots para Dispositivos Móviles y Acceso Remoto

Rdpy es un honeypot especializado en emular el protocolo Remote Desktop Protocol, fue diseñado para capturar intentos de acceso remoto no autorizado a sistemas Windows [168]. RDP es uno de los vectores de ataque más prevalentes en entornos corporativos, y es común que las credenciales asociadas a este sean objeto de ataques de fuerza bruta, así como que se exploten vulnerabilidades relacionadas con ello, como es el caso de BlueKeep. Rdpy emula sesiones RDP reales, lo que permite a los atacantes iniciar conexiones y enviar credenciales, mientras que el sistema registra cada interacción [169].

2.6.5. Sistemas de Detección y Prevención de Intrusiones

2.6.5.1. Snort

Snort es uno de los sistemas de detección de intrusiones de código abierto más ampliamente deployados, operando mediante el análisis de tráfico de red basado en reglas predefinidas y análisis de anomalías [170]. Su integración con honeypots proporciona capacidades complementarias de detección que enriquecen la inteligencia de amenazas recopilada mediante la correlación de eventos de red con actividades observadas en sistemas señuelo [171]. La arquitectura técnica fundamental de Snort incluye un motor de detección basado en firmas configurable, capacidades de análisis de protocolos en tiempo real, sistema de reglas extensible y personalizable, integración con bases de datos para logging estructurado y soporte para múltiples modos operacionales incluyendo sniffer, logger y NIDS [172].

2.6.5.2. Suricata

Suricata constituye un sistema de detección y prevención de intrusiones de próxima generación que proporciona capacidades avanzadas de análisis de tráfico, incluyendo inspección profunda de paquetes y análisis de flujos de red [173]. Su arquitectura multi-threading y capacidades de procesamiento de alta velocidad lo convierten en una herramienta necesaria para entornos de honeypot de alto volumen

donde es necesario procesar grandes cantidades de tráfico malicioso sin impactar el rendimiento del sistema [174]. Las capacidades técnicas avanzadas incluyen motor de detección multi-threading para procesamiento paralelo, inspección profunda de paquetes con análisis de aplicaciones, extracción automática de archivos para análisis de malware, detección de amenazas basada en inteligencia de feeds externos y análisis de flujos de red para identificación de comportamientos anómalos [175].

Las funcionalidades específicas para honeypots comprenden registro detallado de actividades de red en formato JSON estructurado, extracción automática de payloads y archivos transferidos, análisis de protocolos de aplicación para identificación de exploits, detección de técnicas de evasión y obfuscación utilizadas por atacantes e integración nativa con Elastic Stack para análisis y visualización [176]. Esta integración nativa con herramientas de análisis modernas facilita el procesamiento y visualización de grandes volúmenes de datos capturados por honeypots, permitiendo la identificación rápida de patrones y tendencias en las actividades maliciosas observadas [177].

Las configuraciones para el entorno del honeypot deben poseer reglas para la detección de actividades en el sistema e implementación de reglas personalizadas para amenazas específicas [178]. Dichas optimizaciones aseguran que *Suricata* pueda manejar efectivamente el tráfico dirigido hacia los honeypots sin generar alertas excesivas [179].

2.6.5.3. Conclusiones de la Investigación Preliminar

La investigación previa en sistemas honeypot contribuye a un marco de referencia para la ejecución del proyecto en FACSISTEL. Los resultados sugieren que la implementación de T-Pot como plataforma integral es técnicamente factible para el contexto universitario. Esta herramienta formaría un ecosistema compacto que ayudará a la captura de inteligencia de amenazas al tiempo que mantiene la complejidad operativa en niveles manejables.

Se realizó un análisis de arquitecturas *honeynet*; sirviendo de base para demostrar la factibilidad de implementar entornos distribuidos que simulen infraestructuras organizacionales proporcionando así de realismo para la captura de técnicas de

ataque avanzadas. La integración con sistemas IDS/IPS como Suricata permite mejorar la calidad de la inteligencia recopilada mediante la correlación de eventos de red. Los resultados de esta etapa de investigación avalan que la solución propuesta empleando T-Pot en plataforma virtualizada con Proxmox VE, y análisis de datos mediante Elastic Stack, constituye una aproximación técnicamente sólida que maximizará el valor de la inteligencia de amenazas generada para el entorno académico de la UPSE.

2.7. Fase 2: Diseño, implementación y configuración del entorno

El diseño arquitectónico del sistema Honeypot es lo que la implementación del proyecto se basa principalmente. La arquitectura propuesta emplea un modelo en capas que logra separar los componentes, lo cual ayuda en el despliegue y el mantenimiento del sistema. Este diseño tiene tres capas: captura, procesamiento y presentación.

La capa de captura es un conjunto de honeypots especializados desplegados para simular servicios vulnerables y captar actividad maliciosa. Esta capa abarca numerosas instancias de honeypots de distintas clases, cada cual concebido para representar ciertos servicios tales como SSH con Cowrie, servicios Web vía honeypots HTTP, protocolos de red adicionales según los requerimientos de monitoreo. Estos componentes se distribuyen de manera inteligente para obtener una máxima cobertura de detección sin poner en riesgo la seguridad de la infraestructura real.

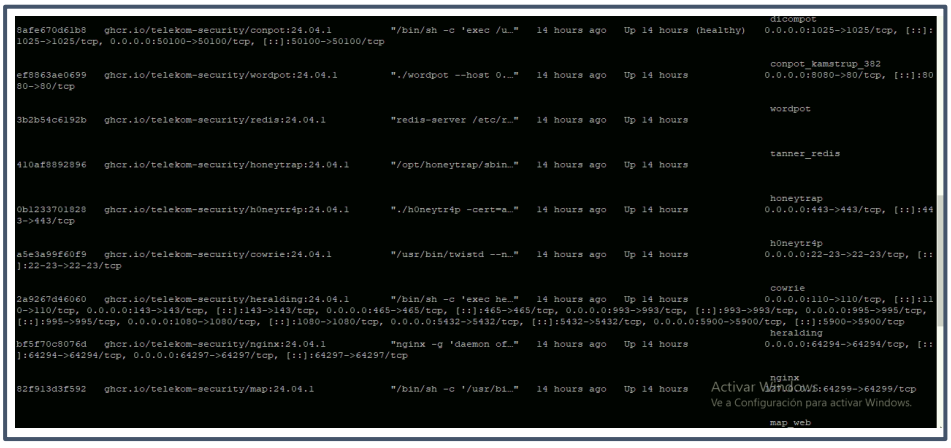


Figura 20: Honeypots desplegados

La capa de procesamiento centraliza el análisis y almacenamiento de los datos capturados por los honeypots. Esta capa se implementa mediante el Elastic Stack, que proporciona capacidades robustas de indexación, búsqueda y análisis de logs. Elasticsearch actúa como el motor de almacenamiento y búsqueda, permitiendo consultas complejas sobre grandes volúmenes de datos en tiempo real. Logstash se encarga del procesamiento y normalización de los logs provenientes de diferentes fuentes, aplicando filtros y transformaciones que estructuran la información para su análisis posterior.

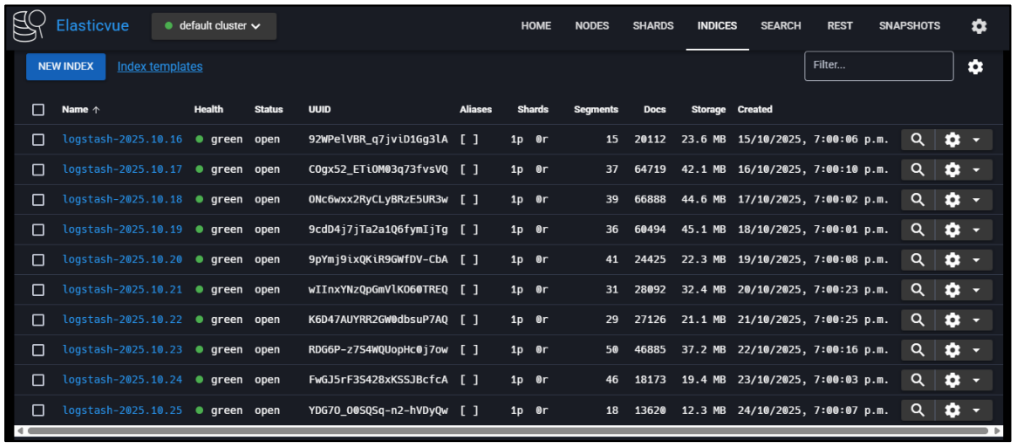


Figura 21: Capa de procesamiento

La capa de presentación ofrece interfaces visuales para el monitoreo. *Kibana* tiene dashboards interactivos para visualizar métricas importantes y distribuciones geográficas de los ataques.

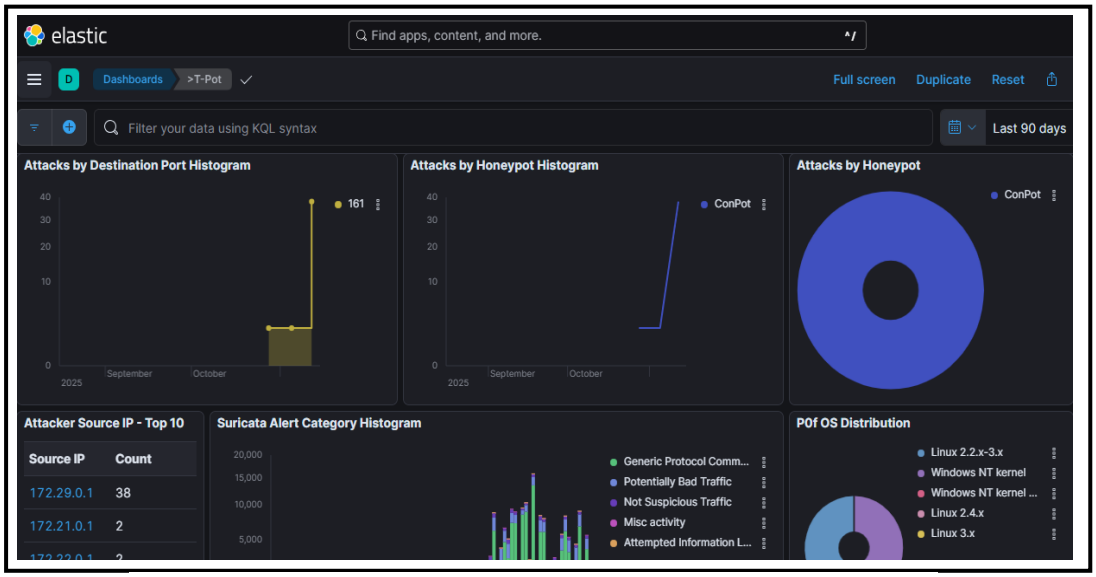


Figura 22: Capa de presentación

2.7.1. Topología de Red y Segmentación

La topología de red para este proyecto aplica varias capas de segmentación que da como resultado un aislamiento completo entre el sistema honeypot y la infraestructura de producción real. La arquitectura de red está diseñada para utilizar una VLANs dedicada destinada al honeypot, separando así el tráfico del honeypot del tráfico legítimo de la universidad. Esta división se complementa con reglas de firewall que controlan el flujo de información entre segmentos permitiendo únicamente las comunicaciones necesarias para el funcionamiento del sistema.

El diseño tiene una zona desmilitarizada (DMZ) en la cual se alojan el servidor AlmaLinux virtualizado en Proxmox y la máquina administradora del servidor virtualizado AlmaLinux, que contiene el honeypot. Esta estructura garantiza un aislamiento adecuado evitando que un posible atacante pueda escalar privilegios o comprometer los sistemas críticos de la infraestructura universitaria.

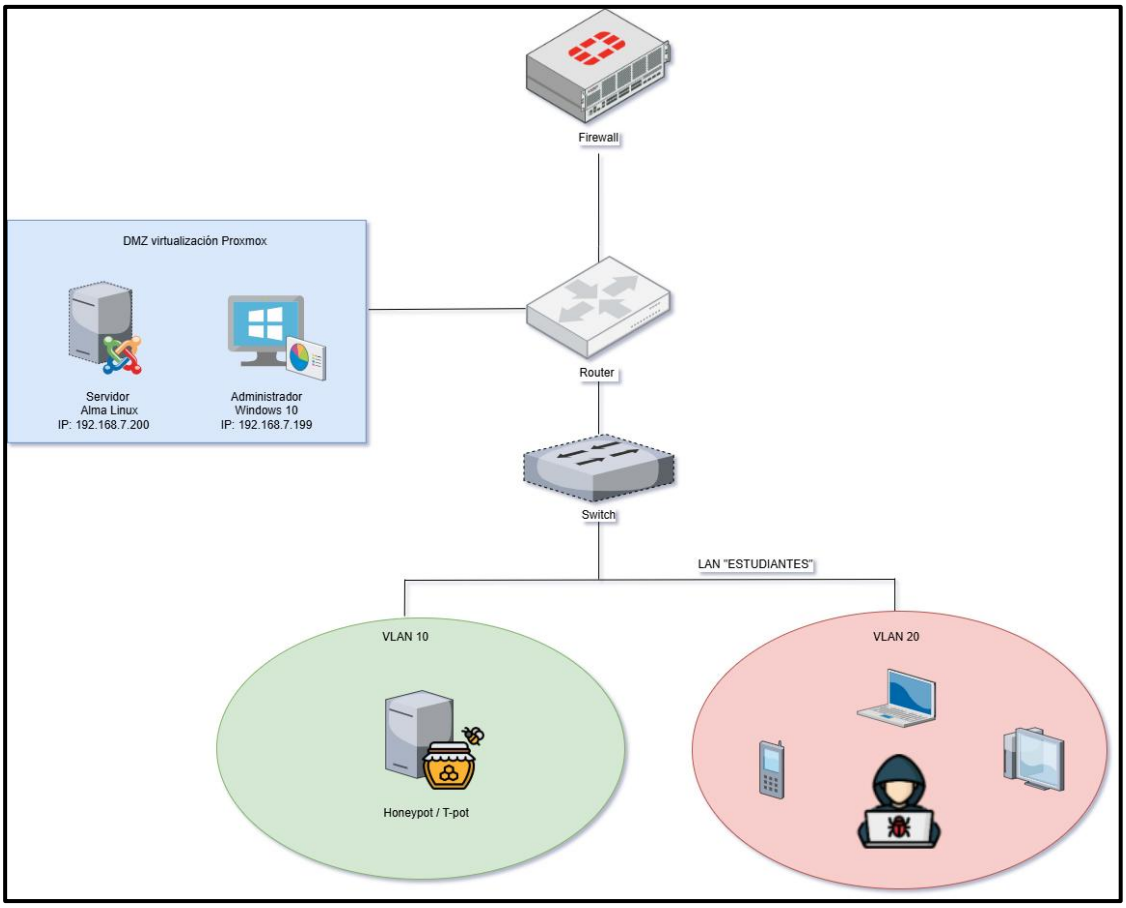


Figura 23: Topología de honeypot en la red

2.7.2. Preparación de la Infraestructura Virtualizada

La instalación del sistema necesita una infraestructura virtualizada lo suficientemente sólida para proveer el aislamiento y flexibilidad necesaria para ejecutar múltiples honeypots. La plataforma de virtualización escogida es Proxmox VE, un hipervisor opensource que combina virtualización basada en KVM (Kernel-based Virtual Machine). Esta decisión se basa en la madurez de la plataforma, en su rendimiento en ambientes de producción y en la fácil disponibilidad de una interfaz Web de administración.

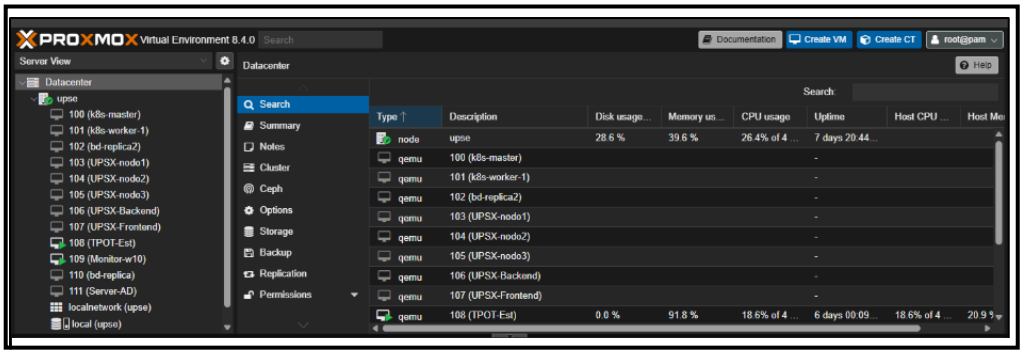


Figura 24: Virtualización en Proxmox VE

2.7.3. Despliegue de la Plataforma T-Pot

T-Pot fue el honeypot seleccionado para desplegarse en este proyecto. Esta solución de código abierto fue desarrollada por Deutsche Telekom Security GmbH, este sistema unifica diversos honeypots especializados en una sola distribución con base en contenedores Docker. La arquitectura modular de T-Pot ayuda a la activación selectiva de componentes según las diversas necesidades específicas de monitoreo facilitando la configuración inicial del sistema.

2.7.4. Preparación para T-Pot

El despliegue de T-Pot necesita la creación de una máquina virtual con especificaciones que garanticen el funcionamiento adecuado de todos los componentes. La distribución oficial sugiere un sistema con al menos 8GB de RAM y 128GB de almacenamiento. La máquina virtual debe ser configurada con múltiples interfaces de red las cuales separen el tráfico de gestión del tráfico de honeypot para así proteger la infraestructura virtual de la institución. Es fundamental establecer políticas de aislamiento mediante VLANs.

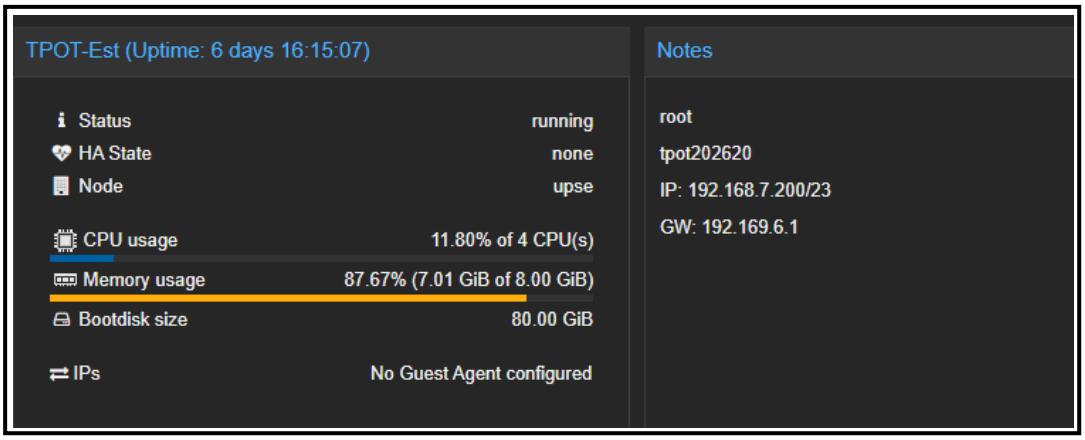


Figura 25: Especificaciones del servidor AlmaLinux

La interfaz de gestión debe tener una dirección IP estática en la VLAN de administración, y la interfaz honeypot debe configurarse para recibir tráfico de la red monitorizada. Es fundamental verificar que el firewall del sistema operativo (iptables o nftables) esté bien configurado para permitir sólo las conexiones que sean necesarias.

```
[usuario_tpot@localhost ~]$ sudo nft list ruleset
# Warning: table ip nat is managed by iptables-nft, do not touch!
table ip nat {
        chain DOCKER {
                iifname "br-0fb5fc577390" counter packets 0 bytes 0 return
                iifname "br-50e2fc556170" counter packets 0 bytes 0 return
                iifname "br-82dbe23b020a" counter packets 0 bytes 0 return
                iifname "br-8f27a715d61e" counter packets 0 bytes 0 return
                iifname "br-1262b581df4b" counter packets 0 bytes 0 return
                iifname "br-50926dafe252" counter packets 0 bytes 0 return
                iifname "br-00853d3c4233" counter packets 0 bytes 0 return
                iifname "br-1abfa17ef493" counter packets 0 bytes 0 return
                iifname "br-dbb1cdf538a3" counter packets 0 bytes 0 return
                iifname "br-32963527500e" counter packets 0 bytes 0 return
                iifname "br-6f373cab644f" counter packets 0 bytes 0 return
                iifname "br-85d9b3a0d568" counter packets 0 bytes 0 return
                iifname "br-ef15fbf0216d" counter packets 0 bytes 0 return
                iifname "br-12ed753a4052" counter packets 0 bytes 0 return
                iifname "br-875037e938e6" counter packets 0 bytes 0 return
                iifname "br-fc99a56bb407" counter packets 0 bytes 0 return
                iifname "br-5dee2cad6eed" counter packets 0 bytes 0 return
                iifname "br-ea5bdbac3aff" counter packets 0 bytes 0 return
                iifname "br-cfa25c4b5801" counter packets 0 bytes 0 return
                iifname "br-e541c7026a0e" counter packets 0 bytes 0 return
                iifname "br-6886842880cf" counter packets 0 bytes 0 return
                iifname "br-232b3463bd05" counter packets 0 bytes 0 return
                iifname "br-c8ee0216dd21" counter packets 0 bytes 0 return
                iifname "docker0" counter packets 0 bytes 0 return
                ip daddr 127.0.0.1 iifname != "br-e541c7026a0e" tcp dport 64299 counter packets 0 bytes 0 dnat to 172.20.0.2:64299
                iifname != "br-875037e938e6" tcp dport 22 counter packets 0 bytes 0 dnat to 172.25.0.2:22
                iifname != "br-875037e938e6" tcp dport 23 counter packets 0 bytes 0 dnat to 172.25.0.2:23
                iifname != "br-1abfa17ef493" tcp dport 3000 counter packets 0 bytes 0 dnat to 192.168.16.2:8080
                iifname != "br-dbb1cdf538a3" tcp dport 5555 counter packets 0 bytes 0 dnat to 172.31.0.2:5555
                iifname != "br-8f27a715d61e" udp dport 5000 counter packets 0 bytes 0 dnat to 192.168.80.2:5000
                iifname != "br-8f27a715d61e" tcp dport 8443 counter packets 0 bytes 0 dnat to 192.168.80.2:8443
                iifname != "br-85d9b3a0d568" tcp dport 5060 counter packets 0 bytes 0 dnat to 172.28.0.2:5060
                iifname != "br-85d9b3a0d568" udp dport 5060 counter packets 0 bytes 0 dnat to 172.28.0.2:5060
                iifname != "br-c8ee0216dd21" tcp dport 8080 counter packets 0 bytes 0 dnat to 172.17.0.2:80
                ip daddr 127.0.0.1 iifname != "br-e541c7026a0e" tcp dport 64303 counter packets 0 bytes 0 dnat to 172.20.0.3:8080
                iifname != "br-32963527500e" tcp dport 25 counter packets 0 bytes 0 dnat to 172.30.0.2:25
                iifname != "br-32963527500e" tcp dport 587 counter packets 0 bytes 0 dnat to 172.30.0.2:25
                iifname != "br-cfa25c4b5801" tcp dport 9100 counter packets 0 bytes 0 dnat to 172.21.0.2:9100
                iifname != "br-ea5bdbac3aff" tcp dport 9200 counter packets 0 bytes 0 dnat to 172.22.0.2:9200
                iifname != "br-6886842880cf" tcp dport 6379 counter packets 0 bytes 0 dnat to 172.19.0.2:6379
```

Figura 26: Verificación del firewall

2.7.5. Proceso de Instalación de T-Pot

La instalación de T-Pot se realiza por medio de un script automatizado proporcionado por el proyecto oficial en *GitHub*. Este instalador descarga todas las dependencias necesarias, también las configuraciones del entorno de los contenedores y establece la configuración inicial del sistema. El proceso de instalación presenta un menú que facilita seleccionar el tipo de despliegue.

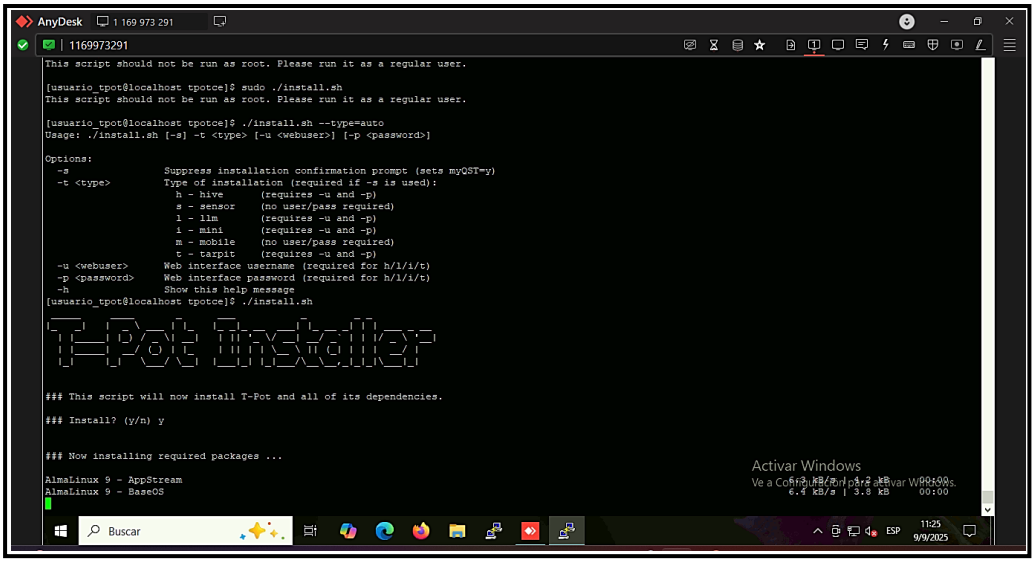


Figura 27: Instalador de T-pot

Para este proyecto se utilizó el "HIVE" (High Interaction Virtual Environment), que incluye el conjunto completo de honeypots disponibles y todas las herramientas de análisis. Esta configuración proporciona la cobertura más amplia de servicios emulados, maximizando las oportunidades de captura de actividad maliciosa.

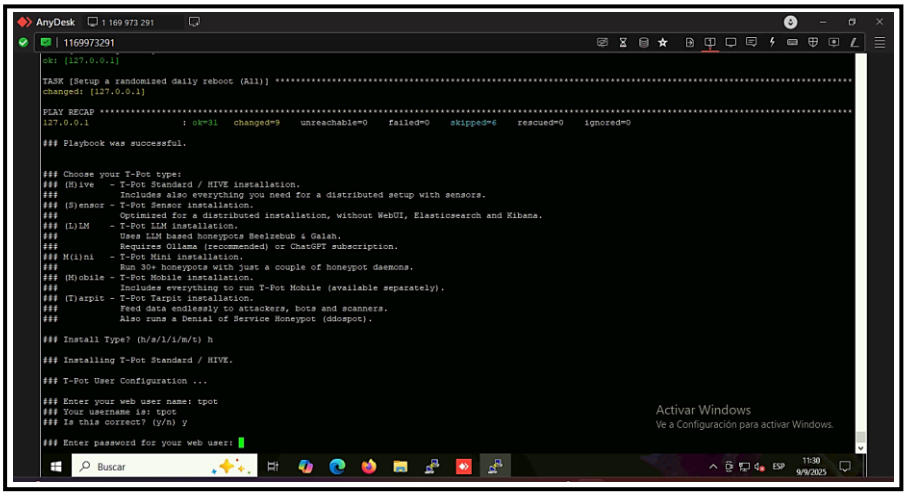


Figura 28: Instalacion de T-pot "HIVE"

Durante la instalación, el sistema solicita la configuración de las credenciales administrativas para conectarse a través de la interfaz web. Es necesario elegir contraseñas fuertes y que se ajusten a las políticas de seguridad institucionales, debido a que a través de esta interfaz se tiene acceso total a toda la información que el sistema recaba. También, se establece la zona horaria (timezone) del sistema para garantizar que en los eventos se registran en la zona horaria local.

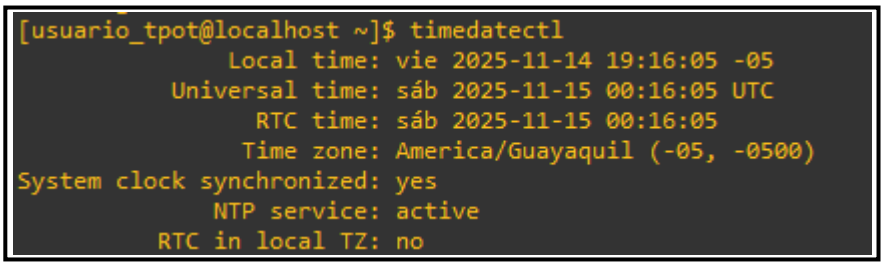


Figura 29: Zona horaria del servidor

2.7.5.1. Configuración de Honeypots Especializados

Una vez completada la instalación base de T-Pot, se procede con la configuración detallada de cada honeypot especializado según los objetivos de monitoreo del proyecto. La configuración se realiza en los archivos YAML los cuales definen los parámetros operacionales de cada uno de los componentes, incluyendo los puertos de escucha y políticas de respuesta ante actividad maliciosa.

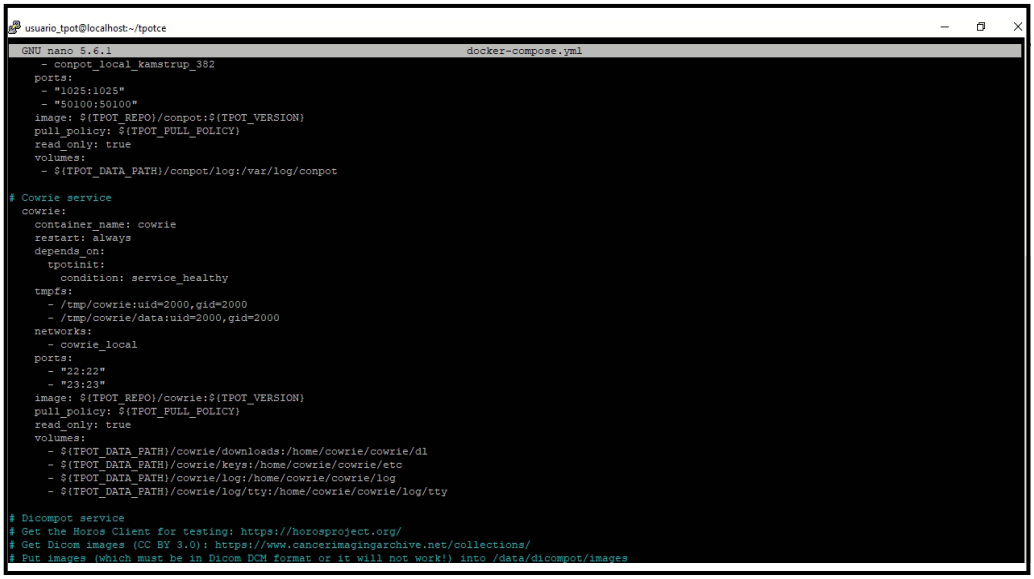


Figura 30: Configuraciones en el archivo YAML

Cowrie, el honeypot de SSH/Telnet, necesita ser configurado específicamente para simular un sistema Linux vulnerable de forma creíble. La configuración permite especificar usuarios y contraseñas débiles que serán encontrados por atacantes en ataques de fuerza bruta, la estructura de un sistema de archivos falso que el atacante buscará al obtener acceso, y los comandos del SO que serán accesibles durante las sesiones comprometidas. Esta emulación debe ser lo suficientemente realista para mantener el interés del atacante mientras se registran todas sus acciones.

Dionaea se debe configurar para capturar muestras de malware que los atacantes intenten desplegar en el sistema comprometido. La configuración debe especificar directorios seguros en donde se puedan almacenar estos binarios para su análisis posterior, implementando de esta forma mecanismos de cuarentena que previenen la ejecución accidental de código malicioso.

Suricata se ejecuta como un sistema de detección de intrusiones en red (NIDS), necesita reglas de detección actualizadas en las que se pueda basar para la detección de patrones de ataques conocidos. La configuración comprende la suscripción a feeds de inteligencia de amenazas que entregan reglas en constante actualización. Las alertas generadas por Suricata se conectan con Elastic Stack para correlacionar eventos de otros honeypots.

2.7.5.2. Integración del Elastic Stack

Elastic Stack es el núcleo para el procesamiento y análisis de datos dentro del proyecto. Este conjunto de herramientas de código abierto brinda funcionalidades de extremo a extremo para el procesamiento y visualización de registros. Aunque Elastic Stack viene ya preconfigurado para integrarse con T-Pot, es importante realizar una personalización a fin de adaptarlo a los requerimientos específicos de este proyecto.

2.7.5.3. Configuración de Elasticsearch

Elasticsearch actúa como el motor de almacenamiento y búsqueda distribuido del sistema. La configuración se debe optimizar teniendo en cuenta el volumen de datos esperado. Los parámetros de memoria de Elasticsearch son modificados para utilizar aproximadamente el 50% de la memoria RAM disponible en el sistema y liberando el resto para caches del sistema operativo.

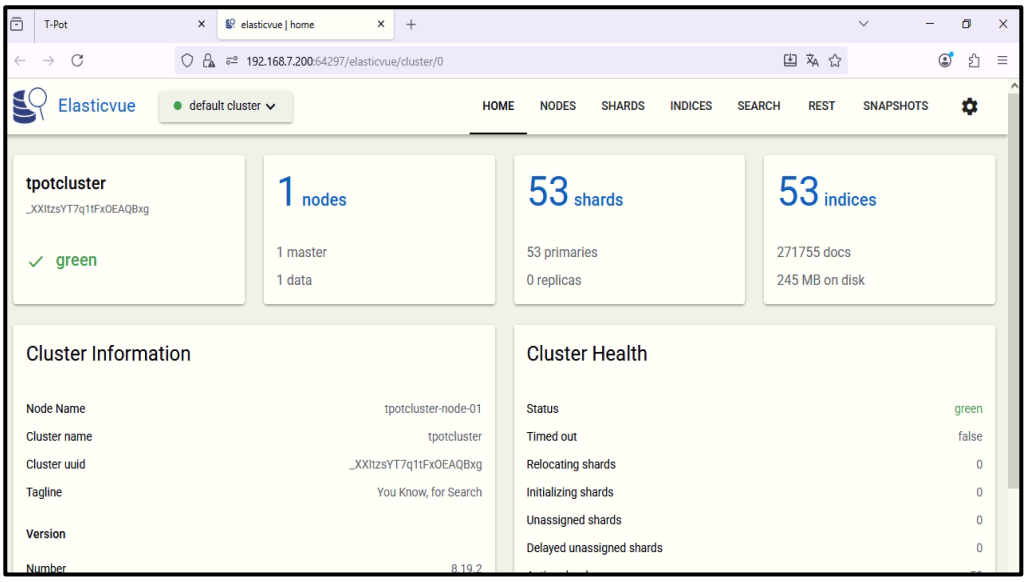


Figura 31: Configuración de Elasticsearch

2.7.5.4. Configuración de Kibana

Kibana proporciona una interfaz visual que ayuda al análisis de los datos almacenados en Elasticsearch. Durante la configuración inicial se definen los patrones de índice, los cuales vinculan los índices de Elasticsearch con objetos consultables dentro de Kibana.

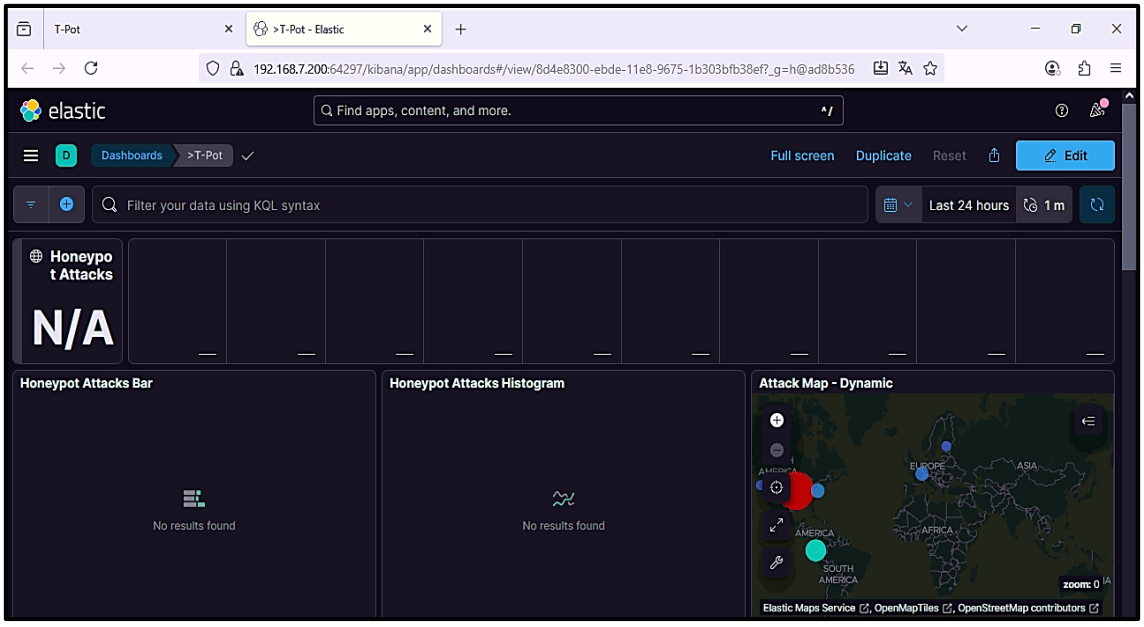


Figura 32: Configuración de Kibana

La creación de visualizaciones en Kibana comienza con visualizaciones básicas que muestran métricas fundamentales: conteos de eventos por tiempo, distribuciones de tipos de ataque, y rankings de direcciones IP más activas. Estas visualizaciones se agregan en paneles de control que generan vistas para diferentes aspectos del análisis [138].

En cuanto a las visualizaciones avanzadas, estas integran mapas de calor temporal que muestran patrones de actividades maliciosas por hora del día y día de la semana, así mismo cuenta con gráficos de red que visualizan relaciones entre atacantes y servicios comprometidos.

Figura 33: Visualizaciones en Kibana

2.8. Fase 3: Monitoreo y recolección de datos

2.8.1. Inicio del Período de Monitoreo

El período de monitoreo del sistema honeypot implementado en los servidores de FACSISTEL se inició el 09 de septiembre del 2025 a las 13:00 h, estableciendo el comienzo formal de la fase de captura de datos que se extendería durante 2 meses continuos.

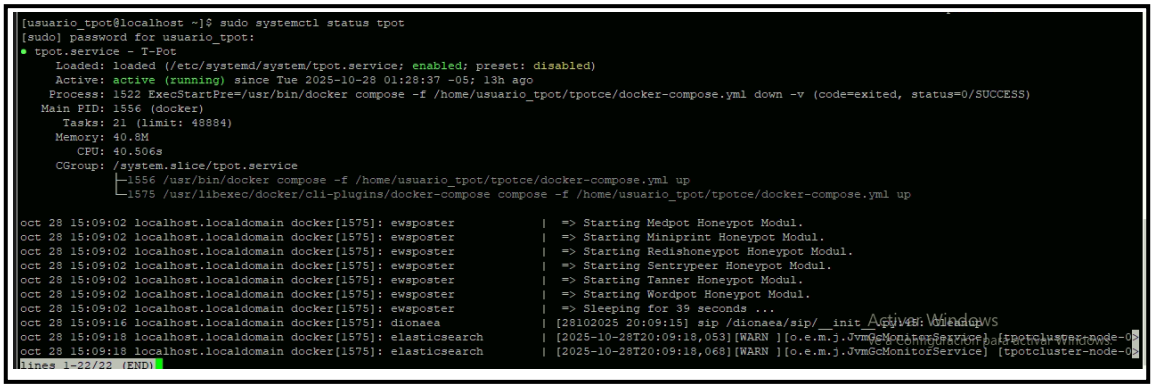


Figura 34: Estado de los Honeypots

La activación del sistema se realizó siguiendo un protocolo definido que incluyó la verificación exhaustiva de todos los componentes de T-Pot, confirmación de conectividad de cada honeypot individual hacia la pila ELK, validación de funcionamiento de Suricata como motor de detección de intrusiones, y comprobación de capacidad de almacenamiento suficiente para el volumen de datos esperado durante el período de investigación.

Los honeypots activados para el monitoreo incluyeron: *ciscoasa, conpot, cowrie, dionaea, elasticpot, heralding, honeytrap, mailoney, medpot, rdpy, snare, tanner y adbhoney* cada uno de ellos con configuraciones específicas adaptadas de acuerdo al ambiente de la universidad UPSE. La red fue configurada para que el sistema honeypot esté totalmente aislado de la red de producción a través de VLAN, para que ningún agresor pudiese utilizar al sistema señuelo como pivote para comprometer otros recursos institucionales. El monitoreo se realizó de manera completamente pasiva desde la perspectiva de los atacantes, sin generar ningún tipo de tráfico activo que pudiera revelar la naturaleza de los sistemas como honeypots o alertar sobre la presencia de capacidades de detección avanzadas.

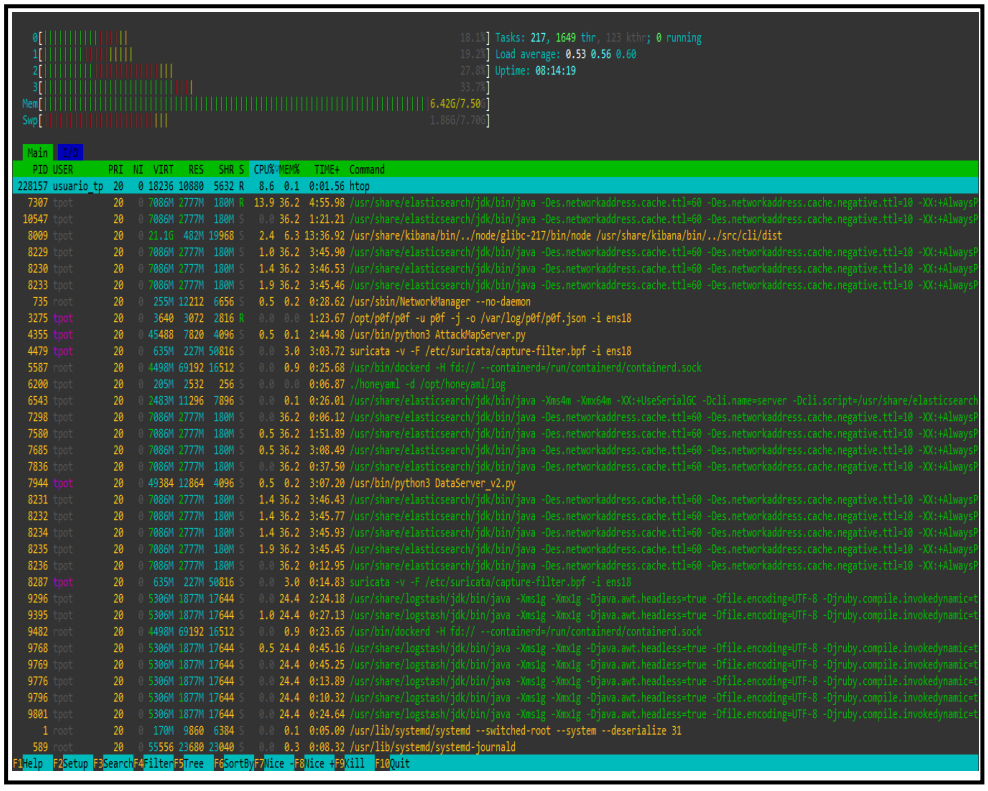
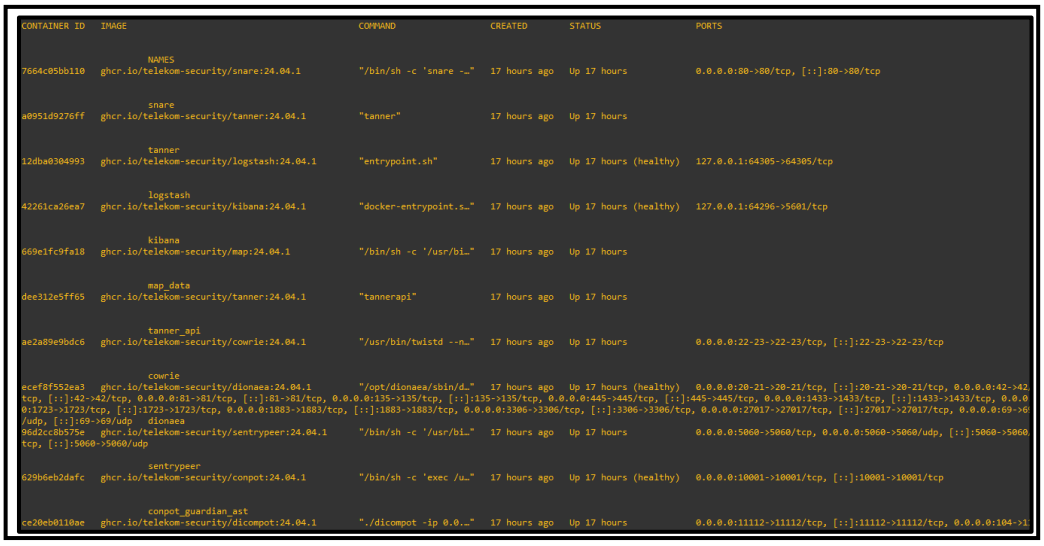


Figura 35: Actividad de los honeypots



CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
7664c05bb110	ghcr.io/telekom-security/snare:24.04.1	"/bin/sh -c 'snare -…"	17 hours ago	Up 17 hours	0.0.0.0:80->80/tcp, [::]:80->80/tcp	snare
a0951d9276ff	ghcr.io/telekom-security/tanner:24.04.1	"tanner"	17 hours ago	Up 17 hours		tanner
12dba0304993	ghcr.io/telekom-security/logstash:24.04.1	"entrypoint.sh"	17 hours ago	Up 17 hours (healthy)	127.0.0.1:64305->64305/tcp	logstash
42261ca26ea7	ghcr.io/telekom-security/kibana:24.04.1	"docker-entrypoint.s…"	17 hours ago	Up 17 hours (healthy)	127.0.0.1:64296->5601/tcp	kibana
669e1fc9fa18	ghcr.io/telekom-security/map:24.04.1	"/bin/sh -c '/usr/bi…"	17 hours ago	Up 17 hours		map_data
dee312e5ff65	ghcr.io/telekom-security/tanner:24.04.1	"tannerapi"	17 hours ago	Up 17 hours		tanner_api
ae2a89e9bdc6	ghcr.io/telekom-security/cowrie:24.04.1	"/usr/bin/twistd --n…"	17 hours ago	Up 17 hours	0.0.0.0:22-23->22-23/tcp, [::]:22-23->22-23/tcp	cowrie
ecef8f552ea3	ghcr.io/telekom-security/dionaea:24.04.1	"/opt/dionaea/sbin/d…"	17 hours ago	Up 17 hours (healthy)	0.0.0.0:20-21->20-21/tcp, [::]:20-21->20-21/tcp, 0.0.0.0:42->42/tcp, [::]:42->42/tcp, 0.0.0.0:81->81/tcp, [::]:81->81/tcp, 0.0.0.0:135->135/tcp, [::]:135->135/tcp, 0.0.0.0:445->445/tcp, [::]:445->445/tcp, 0.0.0.0:1433->1433/tcp, [::]:1433->1433/tcp, 0.0.0.0:1723->1723/tcp, [::]:1723->1723/tcp, 0.0.0.0:1883->1883/tcp, [::]:1883->1883/tcp, 0.0.0.0:3306->3306/tcp, [::]:3306->3306/tcp, 0.0.0.0:27017->27017/tcp, [::]:27017->27017/tcp, 0.0.0.0:69->69/udp, [::]:69->69/udp	dionaea
96d2cc8b575e	ghcr.io/telekom-security/sentrypeer:24.04.1	"/bin/sh -c '/usr/bi…"	17 hours ago	Up 17 hours	0.0.0.0:5060->5060/tcp, 0.0.0.0:5060->5060/udp, [::]:5060->5060/tcp, [::]:5060->5060/udp	sentrypeer
629b6eb2dafc	ghcr.io/telekom-security/conpot:24.04.1	"/bin/sh -c 'exec /u…"	17 hours ago	Up 17 hours (healthy)	0.0.0.0:10001->10001/tcp, [::]:10001->10001/tcp	conpot_guardian_ast
ce20eb0110ae	ghcr.io/telekom-security/dicompot:24.04.1	"./dicompot -ip 0.0.…"	17 hours ago	Up 17 hours	0.0.0.0:11112->11112/tcp, [::]:11112->11112/tcp, 0.0.0.0:104->1	

Figura 37: Docker de los honeypots

La red estudiantil "ESTUDIANTES" de la UPSE, con aproximadamente 15286 usuarios activos al momento del inicio del monitoreo, proporcionó el contexto operacional para la captura de amenazas. La exposición de los honeypots a esta red facilitó observar amenazas tanto internas como externas y de este modo capturando intentos de ataque originados desde dispositivos conectados a la red de la universidad. En las primeras 24 horas de operación el sistema registró actividad inicial que confirmó el funcionamiento correcto de todos los componentes y estableció líneas base de tráfico normal que más adelante facilitarían la identificación de anomalías.

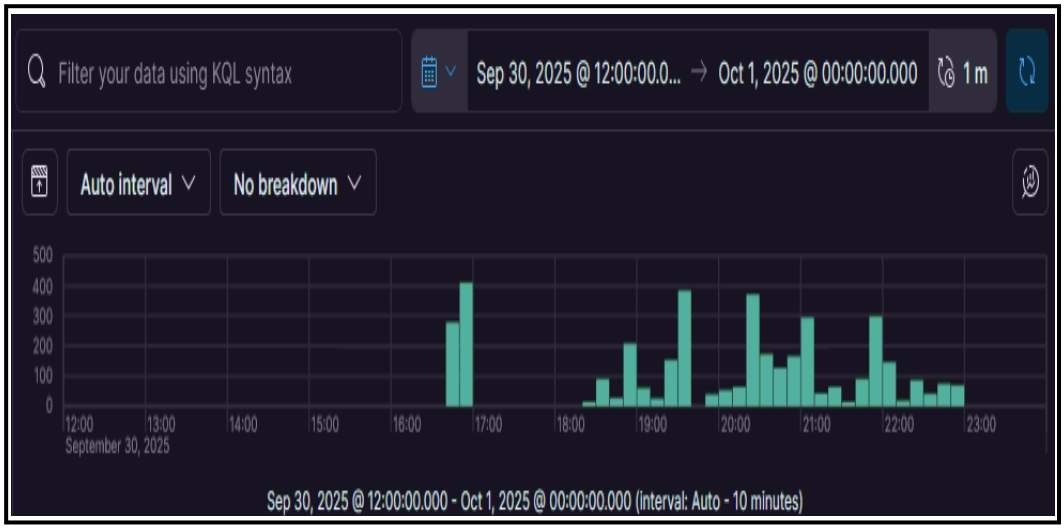


Figura 36: Promedio de actividad diaria del sistema

2.8.2. Supervisión en Tiempo Real del Sistema

La supervisión en tiempo real del ecosistema honeypot se realizó mediante Kibana, proporcionando visibilidad continua sobre las actividades maliciosas capturadas por los múltiples honeypots desplegados. Los dashboards de Kibana configurados específicamente para este proyecto incluyeron visualizaciones de geolocalización, histograma de ataques y actividad de elasticpot, permitiendo la identificación inmediata de picos anómalos de actividad, cambios en patrones geográficos de origen de ataques, y surgimiento de nuevas técnicas de explotación. El monitoreo en tiempo real se realizó cada 12 horas, con revisiones más frecuentes durante el medio día cuando se anticipaban volúmenes de tráfico elevados o actividad académica intensa. Durante la primera semana de monitoreo, el sistema registró un promedio de 26,356 eventos de seguridad diarios distribuidos entre los diferentes honeypots

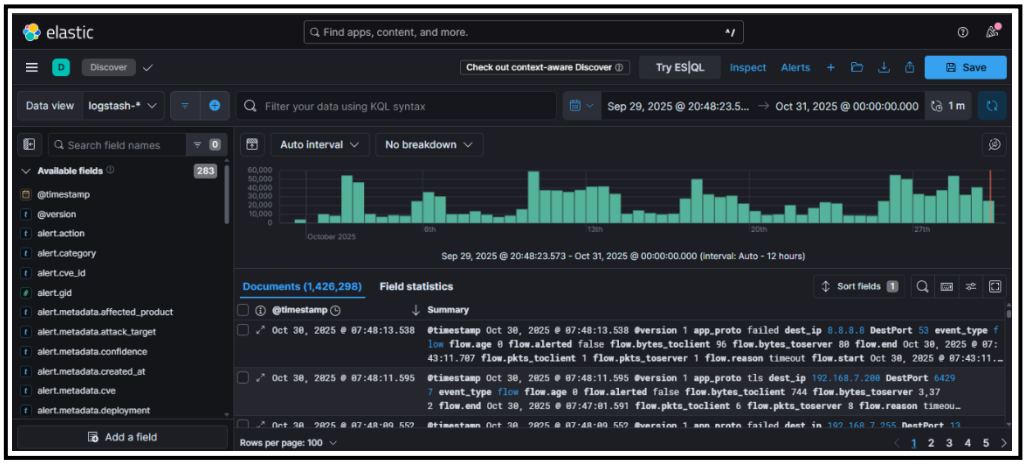


Figura 38: Registro de actividades del Honeypot

El mapa de ataques proporcionó visualizaciones geográficas que revelaron patrones de origen de ataques, identificando que aproximadamente 70 % del tráfico malicioso se originó desde Norte América, mientras que 30% provino de fuentes dentro de Ecuador. El análisis temporal combinado con la distribución geográfica permitió observar que ciertos picos de actividad maliciosa coincidían con horarios específicos, esto posibilitó distinguir entre actividad de botnets distribuidos globalmente y ataques dirigidos potencialmente lanzados desde ubicaciones específicas. En contraste, algunos eventos provenientes de direcciones ecuatorianas mostraron patrones menos uniformes.

Figura 39: Mapa de ataques (1)

La visualización cartográfica obtenida mediante el sistema AttackMap de T-Pot revela la distribución global de los intentos de intrusión capturados durante el período de monitoreo. El mapa presenta concentraciones significativas de actividad maliciosa en regiones específicas del continente americano, evidenciándose mediante marcadores de alta densidad que señalan los puntos de origen de los ataques. La mayor intensidad de eventos se observa en la región de América del Norte.

Figura 40: Mpara de ataques (2)

2.8.3. Registro y Captura de Eventos de Seguridad

El sistema de logging implementado capturó todos los eventos de seguridad mediante la integración de Logstash con Elasticsearch, procesando un volumen promedio de 40 eventos por día que generaron aproximadamente 2 GB de datos estructurados diariamente. Cada evento registrado incluyó campos como *timestamp* con precisión de milisegundos, dirección IP de origen y destino, incluyendo información geográfica y *ASN* del origen. La estructuración de logs facilitó posteriormente el análisis estadístico y la correlación de eventos complejos. Los honeypots web capturaron alrededor de 96000 solicitudes HTTP maliciosas en el período de monitoreo.

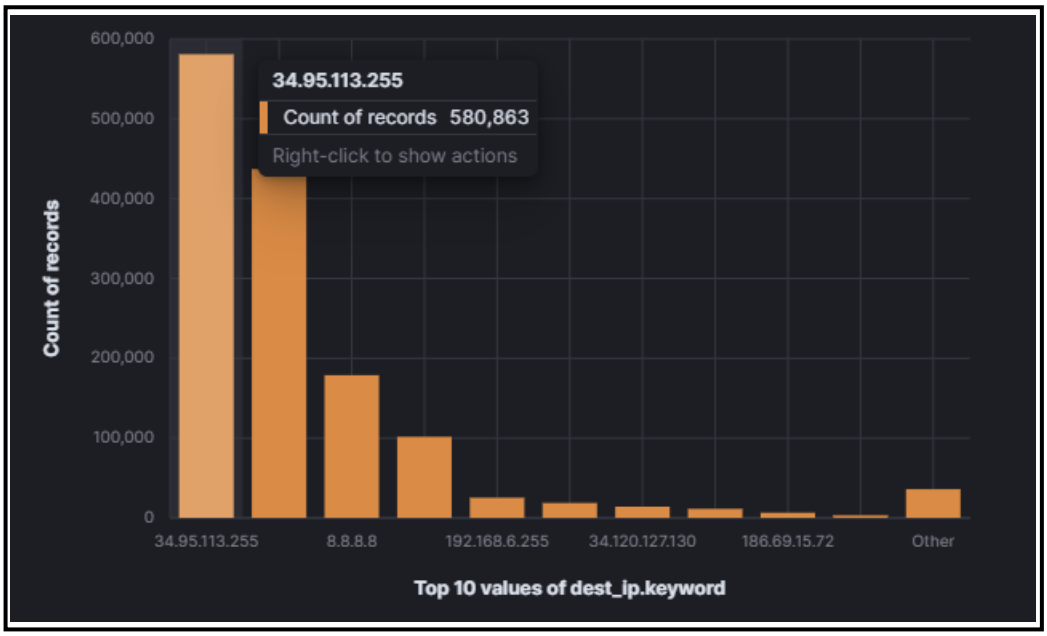


Figura 41: Registro de actividades por IP

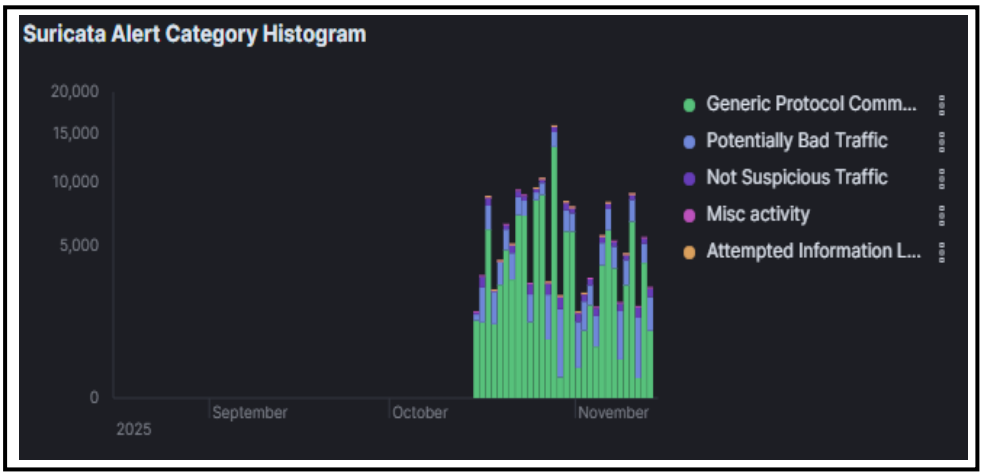


Figura 42: Registro de alertas de Suricata

2.9. Fase 4: Análisis y evaluación de resultados

2.9.1. Exportación y Organización de Datos

La fase de análisis comenzó con la exportación sistemática de todos los logs capturados durante la fase de monitoreo del sistema, se extrajo todos los eventos de seguridad registrados en Elasticsearch mediante consultas. La exportación de los registros se llevó a cabo con herramientas especializadas haciendo que esta tarea se convirtiera en la extracción total de los datos estructurados generados durante la investigación. La exportación se realizó en varios conjuntos de datos divididos por el tipo de honeypot, período temporal y categoría de los eventos, facilitando así el análisis que se realizará más adelante por medio de la creación de subconjuntos manejables que permitieron la reducción de tiempos de consulta para análisis estadísticos.

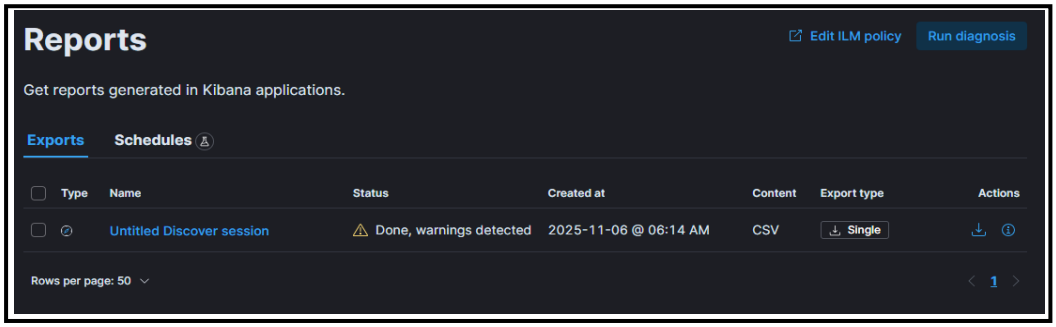


Figura 43:Reporte de kibana

2.9.2. Análisis Estadístico Descriptivo

El análisis estadístico de los eventos registrados brindó una descripción cuantitativa del panorama de amenazas observada durante el período de estudio. La distribución temporal de eventos reveló patrones diurnos con picos de actividad durante las 7:30 de la mañana hasta las 15:00 de la tarde, por el contrario, a partir de las 20:00 de la noche hasta las 04:00 de la mañana se observó casi nula actividad.

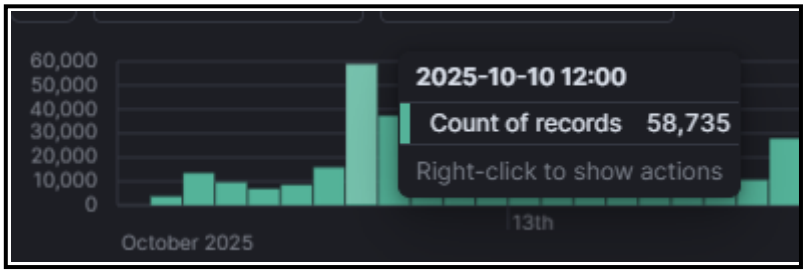


Figura 44: Horario con mayor registro de actividad

La diferencia en la distribución geográfica de las procedencias de ataque se estudió mediante visualizaciones cartográficas y análisis estadísticos de frecuencia a nivel de país y región, mostrando que un pequeño número de países fue responsable de la mayor parte del volumen total de ataques observados. Entre los principales países identificados como fuentes de mayor actividad maliciosa estaban países como Estados Unidos que había aparecido en varias ocasiones como anfitrión de infraestructura de hosting barata para operadores de botnets y cibercriminales, y países con grandes números de dispositivos IoT comprometidos formando parte de botnets distribuidos. El análisis de clustering geográfico utilizando algoritmos de agrupamiento espacial identificó concentraciones significativas de actividad maliciosa en regiones específicas, correlacionando con factores contextuales como la existencia de infraestructura de alojamiento comercial, regímenes laxos de ciberseguridad y zonas horarias.

Figura 45: Regiones de ataques

El análisis de los servicios más atacados mostró que los servicios HTTP y HTTPS simulados por nginx recibieron el mayor porcentaje del tráfico total malicioso. Los servicios de propagación de malware emulados capturaron intentos significativos de distribución de código malicioso mediante protocolos de red comunes, mientras que los servicios de autenticación multi-protocolo documentaron volúmenes considerables de intentos de credenciales contra diversos protocolos de autenticación. La distribución de ataques entre honeypots reflejó tanto la configuración de exposición implementada como la prevalencia relativa de diferentes tipos de amenazas en el ecosistema de cibercrimen contemporáneo. Estos hallazgos fortalecen la comprensión del panorama actual de amenazas y demuestran la utilidad de los honeypots como sensores activos para detectar tendencias emergentes en ciberataques.

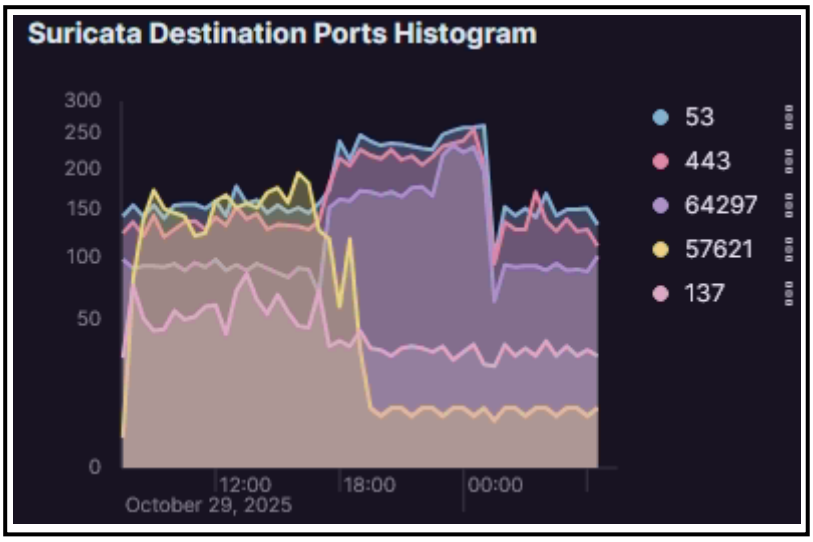


Figura 46: Puertos con mayor tasa de ataque

2.9.3. Identificación de Patrones de Ataque

La identificación sistemática de patrones de ataque se realizó mediante técnicas de análisis de secuencias y clustering de comportamientos procesando secuencias de eventos para identificar comportamientos recurrentes que caracterizaran diferentes tipos de amenazas y tácticas de atacantes. Se identificaron múltiples patrones principales de ataque cada uno caracterizado por secuencias específicas de acciones, tiempos de ejecución típicos, y objetivos aparentes que permitieron clasificar y comprender mejor las amenazas observadas. El patrón más prevalente consistió en escaneos automatizados seguidos de intentos de fuerza bruta contra servicios de autenticación, típicamente ejecutado mediante herramientas automatizadas de botnets que operaban con mínima interacción humana y buscaban maximizar cobertura mediante alta velocidad de escaneo.

El segundo patrón observado consistió en un reconocimiento más consciente y se observa seguido de intentos dirigidos de explotación de vulnerabilidades, sugiriendo actores con mayor nivel de sofisticación. La secuencia incluyó enumeración de servicios y versiones, búsqueda de vulnerabilidades conocidas asociadas con las versiones identificadas, y finalmente intentos de explotación utilizando exploits públicamente disponibles o herramientas de explotación comerciales. Este patrón difirió del primero en duración de sesiones, diversidad de técnicas empleadas, y nivel de adaptación a respuestas del sistema, indicando

probable intervención humana o automatización más sofisticada que ajustaba tácticas basándose en retroalimentación del objetivo.

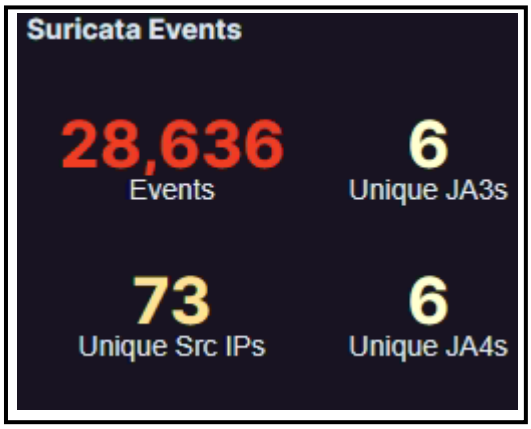


Figura 47: Captura de eventos de Suricata

2.9.4. Análisis de Vectores de Ataque

El análisis de vectores de ataque utilizado demostró la diversidad de técnicas empleadas por los atacantes para comprometer los sistemas honeypot. Los vectores principales identificados fueron los ataques de fuerza bruta contra servicios de autenticación, la explotación de vulnerabilidades conocidas en servicios de red, propagación de malware mediante protocolos automáticos. Los ataques de fuerza bruta reflejaron su facilidad de implementación por medio de herramientas automatizadas ampliamente disponibles y tasa de éxito suficiente para justificar su uso continuo por atacantes con recursos limitados.

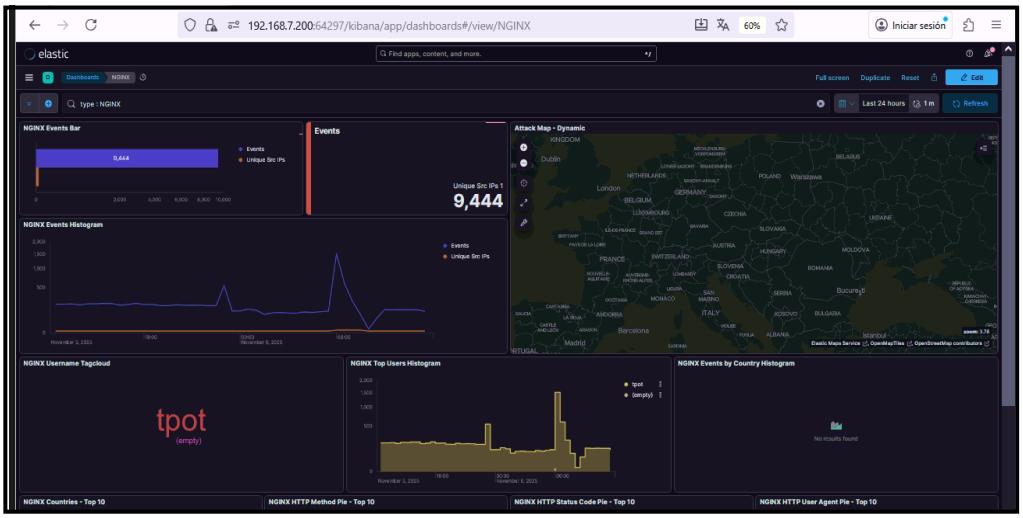


Figura 48: Visualización de ataques web

2.9.5. Análisis de Frecuencia y Temporalidad

En el análisis de frecuencia de ataques se pudo observar variaciones significativas a través de diferentes dimensiones temporales que proporcionaron insights sobre patrones de operación de atacantes y factores que influencian actividad maliciosa. La frecuencia diaria promedio de eventos mostró variabilidad considerable con desviación estándar que indicó presencia de días con actividad extraordinariamente alta posiblemente asociados con campañas específicas o factores contextuales. El análisis de autocorrelación aplicando técnicas de series temporales identificó presencia o ausencia de tendencias de largo plazo, sugiriendo que el volumen de ataques mostró comportamiento relativamente estable durante el período de monitoreo o exhibió tendencias al alza o baja que podrían correlacionar con factores externos al honeypot.

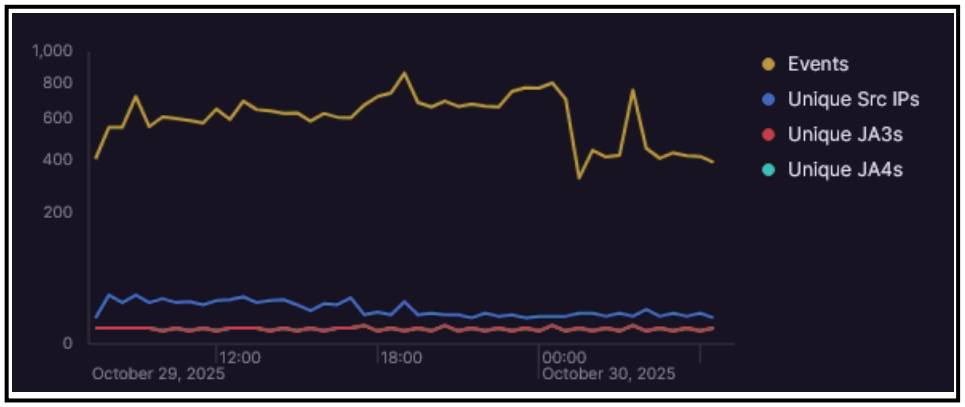


Figura 49: Tasa de eventos diarios registrado por el sistema

Los patrones semanales revelaron diferencias sistemáticas entre días de semana y fines de semana, con días laborales mostrando promedios de actividad que difirieron de fines de semana en proporciones que sugirieron influencia de patrones de trabajo humano ya sea por parte de atacantes operando durante horarios laborales o por factores de infraestructura que afectaron conectividad y visibilidad del honeypot. Esta variación a fin de cuentas terminó alineándose con algunas pautas ya conocidas tanto en documentación académica como en industria para contextos similares, aunque mostró características únicas posiblemente atribuibles a ubicación geográfica específica, configuración de red particular, o características demográficas de atacantes dirigidos a infraestructura ecuatoriana. El análisis

específico por tipo de ataque reveló que ciertos vectores exhibieron mayor variación semanal sugiriendo componente humano en su ejecución, mientras que otros mostraron patrones más uniformes consistentes con operación automatizada continua de botnets.

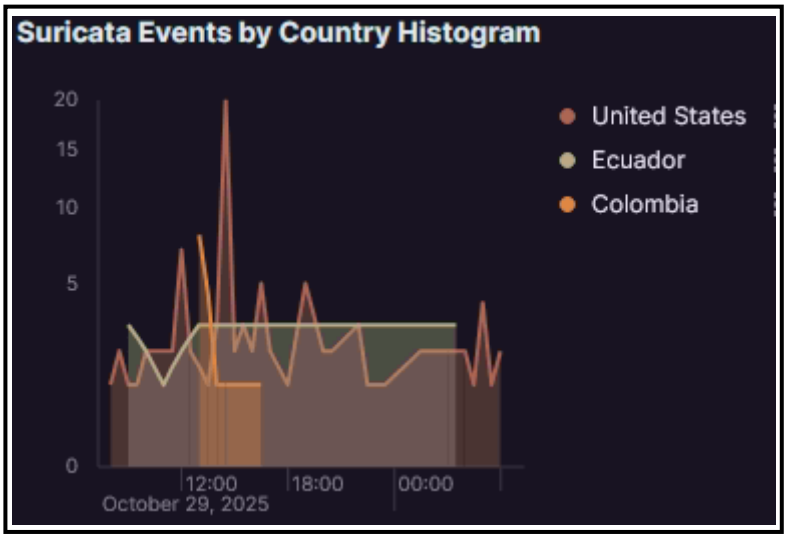


Figura 50: Eventos registrados por país

El período de actividad moderada representó proporciones intermedias de eventos, mientras que el período de mínima actividad concentró únicamente la fracción menor durante horarios de madrugada en zonas horarias principales de atacantes. La correlación con horarios académicos y operacionales de la universidad reveló correlaciones débiles o ausentes, sugiriendo que la mayoría de actividad maliciosa provenía de fuentes externas independientes de patrones de uso legítimo de la red universitaria.

Suricata Alert Signature - Top 10

ID	Description
2200003	SURICATA IPv4 truncated packet
2200122	SURICATA AF-PACKET truncated packet
2002752	ET INFO Reserved Internal IP Traffic
2210020	SURICATA STREAM ESTABLISHED packet out of window
2027397	ET INFO Spotify P2P Client
2210045	SURICATA STREAM Packet with invalid ack
2210029	SURICATA STREAM ESTABLISHED invalid ack
2210065	SURICATA STREAM ESTABLISHED ack for ZWP data
2210061	SURICATA STREAM spurious retransmission
2047703	ET INFO External IP Address Lookup Domain (ipify .org) in TL

Figura 51: Top 10 alertas de Suricata

2.10. Fase 5: Elaboración de la documentación final

Esta fase se consolida toda la información recopilada durante el desarrollo del proyecto mediante la generación automatizada de documentación técnica. Se utiliza un script desarrollado en Python que procesa archivos en formato JSON como entrada y genera reportes completos en PDF. Este enfoque garantiza la estandarización, reproducibilidad y presentación profesional de los resultados obtenidos.

2.10.1. Conversión de datos CSV a formato JSON

Se utiliza un script especializado Python para automatizar la conversión de los archivos CSV en archivos JSON. Muchos de los registros y logs del sistema honeypot se producen en formato CSV con el mismo formato entre ellos, por loque esta herramienta es imprescindible para el posterior procesamiento. El script hace validación de datos, limpieza de registros inconsistentes, normalización de campos y estructuración jerárquica de la información. La transformación facilita la integración con el sistema de generación de reportes.

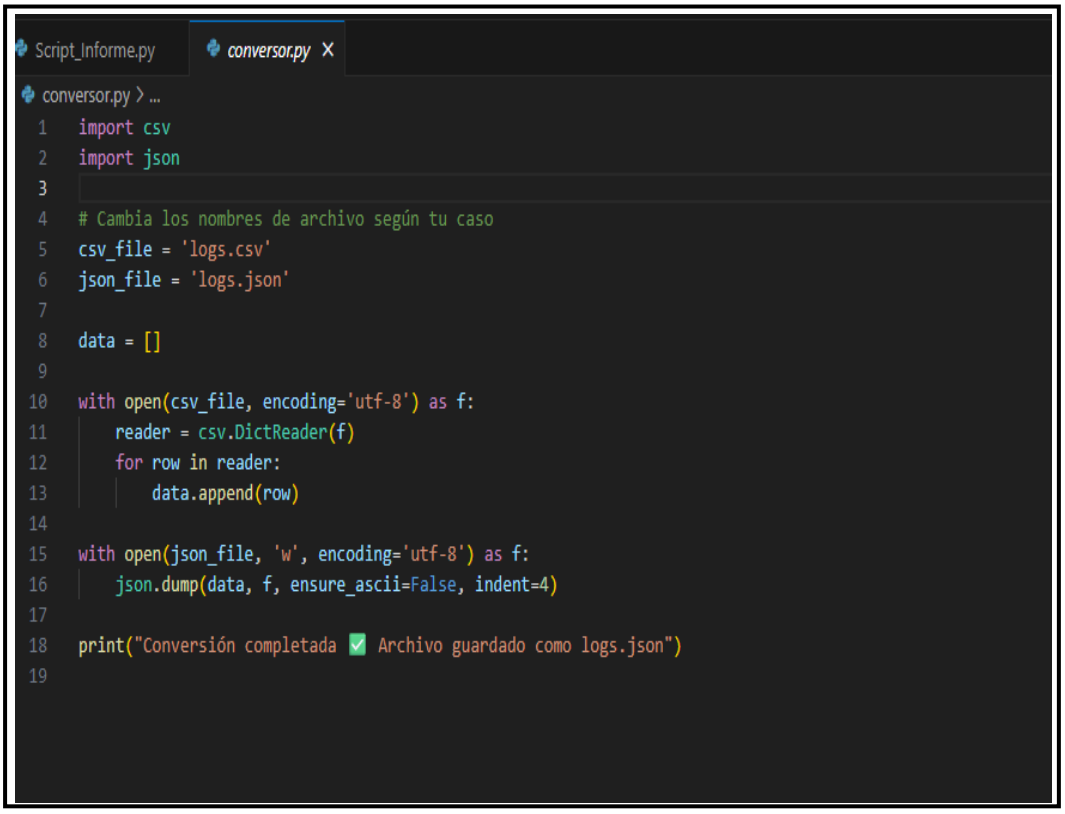


Figura 52: Script conversor de CSV a JSON

2.10.2. Preparación de datos para documentación

Se recopilan y organizan todos los datos generados durante las fases anteriores del proyecto en archivos JSON estructurados. Estos archivos contendrán información sobre configuraciones de red, parámetros de los ataques ejecutados, logs del sistema, credenciales capturadas y métricas de rendimiento. La estructuración adecuada de estos datos es fundamental para el correcto funcionamiento del script de generación de informes.

2.10.3. Generación automatizada de informes

Mediante el script desarrollado en Python se procesan los archivos JSON para crear reportes técnicos en formato PDF. El script importa librerías especializadas para la graficación estadística de vectores de ataques, tasas de exito, distribuciones temporales de intentos de autenticación. El informe generado también incluye secciones diferenciadas que cubren aspectos técnicos, resultados experimentales y análisis de datos.

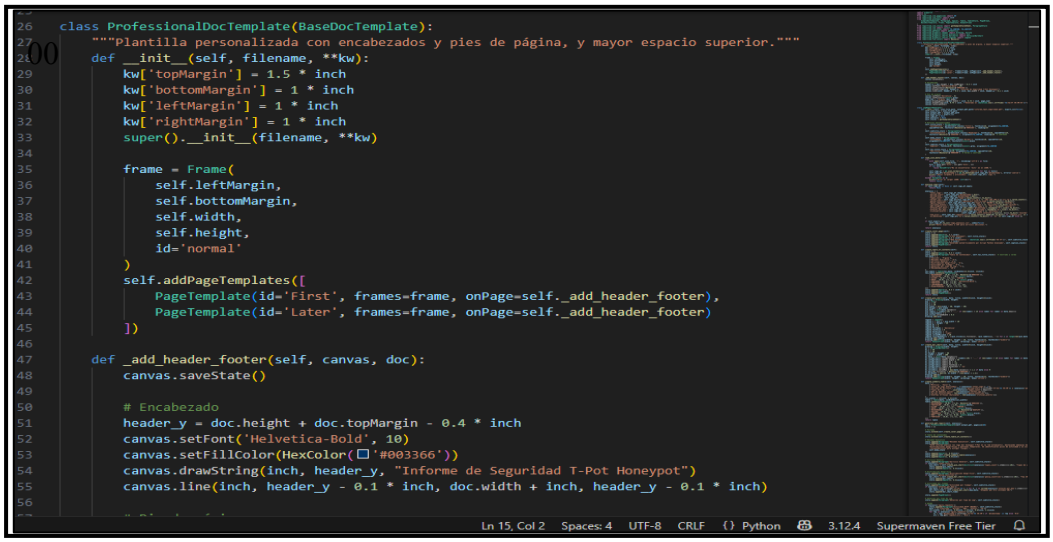


Figura 53: Script para la generación informes

2.10.4. Análisis de resultados y generación de gráficas

Se elaboran representaciones visuales de los datos recopilados mediante gráficas estadísticas generadas automáticamente por el script. Estas incluyen histogramas de intentos de acceso por servicio, gráficos de líneas temporales de actividad maliciosa, diagramas de dispersión de direcciones IP atacantes y gráficos circulares de distribución de protocolos atacados. El análisis visual facilita la identificación de patrones y tendencias en el comportamiento de los atacantes.

CONCLUSIONES

- La implementación del sistema Honeypot T-Pot en los servidores de FACSISTEL se completó por medio de una arquitectura virtualizada en Proxmox VE, logrando el despliegue de más de 13 honeypots especializados. La configuración de tipo "HIVE" (High Interaction Virtual Environment) proporcionó una cobertura amplia de servicios emulados incrementando las oportunidades de captura de actividad maliciosa dirigida hacia la red “ESTUDIANTES”. El sistema honeypot operó de manera continua durante 2 meses iniciando el 09 de septiembre de 2025 pudiendo de esta manera registrar un promedio de 26,356 eventos de seguridad diarios sin comprometer la estabilidad de la infraestructura productiva de la UPSE.
- La topología de red implementada garantizó el aislamiento del sistema Honeypot mediante segmentación con VLANs dedicadas y políticas de firewall, previniendo que los atacantes pudieran utilizar los sistemas comprometidos como punto de pivote para acceder a recursos institucionales críticos. La configuración de una DMZ (Zona Desmilitarizada) permitió la exposición controlada de servicios vulnerables simulados. Esta arquitectura de seguridad en capas pudo validar la viabilidad de operar sistemas de engaño en entornos académicos sin poner en riesgo la infraestructura real y cumpliendo con los estándares de seguridad establecidos en el marco normativo ecuatoriano.
- La correlación de eventos entre varios honeypot llevó a la detección de campañas de ataque organizadas, en las cuales un atacante probaba diferentes servicios vulnerables, esto se demuestra por las siendo estas mismas IPs las que se conectaban a múltiples honeypots en un corto intervalo temporal. Esta correlación temporal y de origen reveló que aproximadamente el 35% de las direcciones IP observadas interactuaron con más que un tipo de honeypot, indicando reconocimiento sistemático de la superficie de ataque completa más que explotación oportunista de servicios individuales.
- La clasificación de los datos recopilados durante el período de monitoreo se realizó mediante análisis estadístico descriptivo e inferencial que procesaron el volumen total de eventos de seguridad registrados, exportados desde

Elasticsearch en formato CSV. La distribución temporal de eventos reveló patrones diurnos claros con picos de actividad alcanzando máximos durante el horario académico entre 07:30 y 15:30 horas, coincidiendo con los períodos de mayor conectividad estudiantil identificados tanto en las encuestas como en las entrevistas con el personal de TICs. El análisis de series temporales aplicando técnicas de descomposición estacional identificó componentes cíclicos con períodos característicos semanales sugiriendo comportamientos recurrentes de atacantes que podrían explotarse para optimización de recursos de monitoreo y respuesta a incidentes.

- La generación de los informes técnicos se automatizó con éxito utilizando Python para crear scripts que toman archivos JSON como datos de entrada y producen informes en PDF. El script principal incluye funciones para convertir los datos del CSV exportado de Elasticsearch hacia JSON estructurado, limpieza de registros inconsistentes, normalización de campos asegurar consistencias en el procesamiento, estructuración jerárquica de información según taxonomías predefinidas, y generación automatizada de visualizaciones gráficas mediante librerías especializadas como Matplotlib.

RECOMENDACIONES

- Se recomienda mantener el sistema Honeypot en operación como componente permanente de la arquitectura de seguridad de FACSISTEL, estableciendo un programa de monitoreo sostenido con ciertas revisiones periódicas cada 12 horas y con análisis profundos mensuales de los datos capturados. La información de inteligencia de amenazas generada por el sistema debe ser utilizada para fortalecer los sistemas de seguridad perimetral, como son las reglas de firewalls, actualización de firmas en sistemas IDS/IPS y refinamiento de políticas de control de acceso. Establecer un procedimiento operativo estándar para la respuesta ante patrones de ataque inusuale que incluya mecanismos de escalamiento, coordinación con el equipo de TICs y comunicación con las autoridades competentes cuando sea necesario.
- Realizar un programa de concientización en ciberseguridad para toda la comunidad universitaria con contenidos diferenciados según el nivel de conocimiento técnico de cada usuario. Para el 46.25% de estudiantes con conocimiento limitado se sugieren talleres básicos sobre identificación de phishing, gestión segura de contraseñas, reconocimiento de sitios web maliciosos y prácticas de navegación segura.
- Fortalecer la seguridad en cuanto a la autenticación de la red "ESTUDIANTES", un sistema de autenticación robusto pero que a su vez mantenga la facilidad de acceso y que incluya los controles mínimos esenciales de seguridad. Se recomienda el uso de autenticación 802.1X con las credenciales institucionales con segmentación de red en VLANs dinámicas de acuerdo al perfil del usuario y sistemas de control de acceso a red (NAC) que verifiquen el estado de seguridad de los dispositivos antes de permitir el acceso completo.

REFERENCIAS

[1] «Ciberseguridad en el sector educativo | Empresas | INCIBE». Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://www.incibe.es/empresas/blog/ciberseguridad-en-el-sector-educativo

[2] «Riesgos de las redes Wi-Fi públicas y por qué no debes temerlas», /. Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

[3] F. Derenzin Martinez, «¿Están los institutos universitarios en Ecuador preparados para los ciberataques?», *593 Digital Publisher CEIT*, vol. 9, n.º 6, pp. 1220-1232, 2024.

[4] J. A. G. Pineda, G. R. Hernández, M. A. T. Bonilla, y L. B. Florez, «Adolescentes en la Institución Educativa San Luis».

[5] «Consejos de ciberseguridad para estudiantes de la UTEQ». Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://www.uteq.edu.ec/comunicacion/noticia/consejos-ciberseguridad-estudiantes-uteq

[6] «El factor humano: pilar esencial en la ciberseguridad. – Revista Zona Libre». Accedido: 22 de abril de 2025. [En línea]. Disponible en: https://www.revistazonalibre.ec/2023/08/05/el-factor-humano-pilar-esencial-en-la-ciberseguridad/

[7] Septiembre 26, 2022 Por Francisco Javier Rocha Estrada, y C. E. G. R. y L. D. G. Morales, «La seguridad digital de los jóvenes universitarios», Observatorio / Instituto para el Futuro de la Educación. Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://observatorio.tec.mx/edu-bits-blog/seguridad-digital-estudiantes-universitarios/

[8] «Todo lo que Necesitas Saber sobre el Uso Indebido de Privilegios», Kiteworks | Your Private Data Network. Accedido: 22 de abril de 2025. [En

línea]. Disponible en: https://www.kiteworks.com/es/glosario-riesgo-cumplimiento/uso-indebido-de-privilegios/

[9] «Exploit, definición y características - Panda Security». Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://www.pandasecurity.com/

[10] «Protección de infraestructuras de red: mejores prácticas y estrategias.», Ciberprisma - alianza por la ciberseguridad. Accedido: 2 de abril de 2025. [En línea]. Disponible en: https://ciberprisma.org/2024/08/31/proteccion-de-infraestructuras-de-red-mejores-practicas-y-estrategias/

[11] «Phishing: Cómo los hackers roban tu información personal». Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://www.campusciberseguridad.com/blog/phishing-como-hackers-roban-tu-informacion-personal

[12] A. Trevino, «¿Cuáles son los riesgos de seguridad asociados al BYOD?», Keeper Security Blog - Cybersecurity News & Product Updates. Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://www.keepersecurity.com/blog/es/2024/02/22/what-are-the-security-risks-of-byod/

[13] «Ransomware | INCIBE | INCIBE». Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://www.incibe.es/aprendeciberseguridad/ransomware

[14] «What Happens When Students Bring Malware to Campus? | EdTech Magazine». Accedido: 13 de mayo de 2025. [En línea]. Disponible en: https://edtechmagazine.com/higher/article/2025/01/what-happens-when-students-bring-malware-campus

[15] B. B. J. Enrique, «DISEÑO E IMPLEMENTACIÓN DE HONEYPOTS PARA LA DETECCIÓN DE CIBERATAQUES».

[16] «Ecuador está entre los países con más ciberataques en América Latina - El Comercio». Accedido: 26 de mayo de 2025. [En línea]. Disponible en: https://www.elcomercio.com/tecnologia/ecuador-ciberataques-america-latina-hacker.html

[17] «ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina». Accedido: 15 de abril de 2025. [En línea]. Disponible en: https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/

[18] «Ciberseguridad - Protección de datos y sistemas con Grctools». Accedido: 26 de mayo de 2025. [En línea]. Disponible en: https://grctools.software/soluciones/ciberseguridad/

[19] D. Ortiz, «Ecuador está entre los países con más ciberataques en América Latina», El Comercio. Accedido: 14 de abril de 2025. [En línea]. Disponible en: https://www.elcomercio.com/tecnologia/ecuador-ciberataques-america-latina-hacker.html

[20] M. Arce Aguilar, «¿Qué Es un Riesgo de Ciberseguridad? Ejemplos y Cómo Prevenirlo?» Accedido: 27 de mayo de 2025. [En línea]. Disponible en: https://www.deltaprotect.com/blog/riesgos-de-ciberseguridad-ejemplos-y-prevencion

[21] «La importancia de la Ciberseguridad en la Educación». Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://thebridge.tech/blog/ciberseguridad-en-educacion/

[22] «¿Qué es la detección de anomalías? | Una guía de detección de anomalías integral». Accedido: 27 de mayo de 2025. [En línea]. Disponible en: https://www.elastic.co/es/what-is/anomaly-detection

[23] «El 69% de las organizaciones de Latinoamérica sufrió algún incidente de seguridad durante el último año | | ESET». Accedido: 11 de agosto de 2025. [En línea]. Disponible en: https://www.eset.com/pa/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/el-69-de-las-organizaciones-de-latinoamrica-sufrio-algun-incidente-de-seguridad-durante-el-ultimom-ano/

[24] P. J. Barrio Navarro, «Análisis y estudio de Honeynets en entorno doméstico e institucional», *Honeynets analysis and study in domestic and*

institutional environment, jul. 2022, Accedido: 2 de abril de 2025. [En línea]. Disponible en: https://buleria.unileon.es/handle/10612/24372

[25] «La definición del contexto en Investigación - Proyecto Académico». Accedido: 5 de junio de 2025. [En línea]. Disponible en: https://proyectoacademico.com/la-definicion-del-contexto-en-investigacion/

[26] Gabriela. Bustelo, «Ciberseguridad en el sector educativo: riesgos y prevención», Red Seguridad. Accedido: 25 de mayo de 2025. [En línea]. Disponible en: https://www.redseguridad.com/actualidad/ciberseguridad-sector-educacion-riesgos-prevencion_20250422.html

[27] «¿Qué es el Monitoreo de Red? Mejora la Seguridad y el Rendimiento», Splashtop Inc. Accedido: 25 de mayo de 2025. [En línea]. Disponible en: https://www.splashtop.com/es/blog/network-monitoring

[28] H. Martínez Ruiz, *Metodología de la investigación con enfoque en competencias: sexto semestre*. México, D.F.: Cengage Learning, 2012.

[29] «¿Qué son las analíticas de logs?» Accedido: 27 de mayo de 2025. [En línea]. Disponible en: https://www.elastic.co/es/what-is/log-analytics

[30] C. A. Bernal, «Metodología de la investigación».

[31] «¿Qué es la investigación correlacional?» Accedido: 5 de junio de 2025. [En línea]. Disponible en: https://www.questionpro.com/blog/es/investigacion-correlacional/

[32] L. D. M. Solís, «El enfoque cuantitativo de investigación», Investigalia. Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://investigaliacr.com/investigacion/el-enfoque-cuantitativo-de-investigacion/

[33] «Método analítico - Qué es, características y ejemplos». Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://concepto.de/metodo-analitico/

[34] E. R. Arias, «¿Qué es el método sintético? Características y ejemplos», Economipedia. Accedido: 5 de junio de 2025. [En línea]. Disponible en: https://economipedia.com/definiciones/metodo-sintetico.html

[35] M. Narvaez, «Método inductivo: Qué es, características y ejemplos», QuestionPro. Accedido: 11 de agosto de 2025. [En línea]. Disponible en: https://www.questionpro.com/blog/es/metodo-inductivo/

[36] M. Narvaez, «Método deductivo: Qué es y cuál es su importancia», QuestionPro. Accedido: 11 de agosto de 2025. [En línea]. Disponible en: https://www.questionpro.com/blog/es/metodo-deductivo/

[37] «Método hipotético-deductivo», *Wikipedia, la enciclopedia libre*. 3 de octubre de 2024. Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://es.wikipedia.org/w/index.php?title=M%C3%A9todo_hipot%C3%A9tico-deductivo&oldid=162816918

[38] «¿Qué es la investigación con métodos mixtos? - ATLAS.ti». Accedido: 4 de junio de 2025. [En línea]. Disponible en: https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/investigacion-con-metodos-mixtos

[39] «La entrevista como poderoso método de investigación», ATLAS.ti. Accedido: 5 de junio de 2025. [En línea]. Disponible en: https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/entrevistas

[40] «Investigación cuantitativa: definición y procedimiento», Qualtrics. Accedido: 4 de junio de 2025. [En línea]. Disponible en: https://www.qualtrics.com/es-es/gestion-de-la-experciencia/investigacion/investigacion-cuantitativa/

[41] Y. L. Avilés Bajaña, «Implementación de una herramienta honeypot para detección y respuesta a ataques», masterThesis, ESPOL. FIEC, 2016. Accedido: 2 de abril de 2025. [En línea]. Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/37409

[42] V. M. Terrones Bedon, «Propuesta de implementación de un Honeypot de seguridad informática en la agropecuaria Wilian & Roque S.R.L. – Chimbote; 2021.», sep. 2022, Accedido: 2 de abril de 2025. [En línea]. Disponible en: https://repositorio.uladech.edu.pe/handle/20.500.13032/28896

[43] «Honeypot: 5 tipos principales para proteger tus datos», OBS Business School. Accedido: 5 de junio de 2025. [En línea]. Disponible en: https://www.obsbusiness.school/blog/honeypot-5-tipos-principales-para-proteger-tus-datos

[44] «¿Qué es VMware? | IBM». Accedido: 8 de abril de 2025. [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/vmware

[45] «ELK Stack: Elasticsearch, Kibana, Beats y Logstash», Elastic. Accedido: 8 de abril de 2025. [En línea]. Disponible en: https://www.elastic.co/es/elastic-stack

[46] *cowrie/cowrie*. (22 de abril de 2025). Python. Cowrie. Accedido: 22 de abril de 2025. [En línea]. Disponible en: https://github.com/cowrie/cowrie

[47] «Log Avanzado: ¿Qué es y qué importancia tiene en seguridad?» Accedido: 5 de junio de 2025. [En línea]. Disponible en: https://www.age2.es/noticias/ciberseguridad-que-es-un-log-avanzado/

[48] «La Evolución de las Amenazas Cibernéticas: Visión General y Amenazas Emergentes - Parte 1». Accedido: 5 de junio de 2025. [En línea]. Disponible en: https://blog.gigas.com/es/la-evolucion-de-las-amenazas-ciberneticas-vision-general-y-amenazas-emergentes

[49] «What Is An Intrusion Detection System - IDS?» Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://www.sophos.com/en-us/cybersecurity-explained/ips-and-ids

[50] «¿Qué son los sistemas IDS/IPS? | Glosario | HPE LAMERICA». Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://www.hpe.com/lamerica/es/what-is/ids-ips.html

[51] «¿Qué es un sistema de detección de intrusiones (IDS)?| IBM». Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/intrusion-detection-system

[52] A. M. Camuñas Hilario, «Honeypot: resiliencia y conocimiento del adversario», jun. 2024, Accedido: 3 de junio de 2025. [En línea]. Disponible en: http://hdl.handle.net/10609/150610

[53] «What is a honeypot and how does it work?» Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://us.norton.com/blog/iot/what-is-a-honeypot

[54] «OWASP Honeypot | OWASP Foundation». Accedido: 14 de mayo de 2025. [En línea]. Disponible en: https://owasp.org/www-project-honeypot/

[55] «What is Proactive Cybersecurity and Why Does it Matter». Accedido: 27 de mayo de 2025. [En línea]. Disponible en: https://www.threatintelligence.com/blog/what-is-proactive-cybersecurity

[56] B. Santander, «Honeypot», Banco Santander. Accedido: 27 de mayo de 2025. [En línea]. Disponible en: https://www.bancosantander.es/glosario/honeypot

[57] B. Rossi, «How to set up a cybersecurity honeypot for your business», Information Age. Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://www.information-age.com/how-set-cybersecurity-honeypot-your-business-30347/

[58] «What is a honeypot? How it protects against cyberattacks | Definition from TechTarget», Search Security. Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://www.techtarget.com/searchsecurity/definition/honey-pot

[59] Qualityseg, «Las empresas en la mira de los Hackers: ¿Cómo evitar los ciberataques?» Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://qualityseg.com.ec/blog/como-impacta-la-crisis-de-inseguridad-en-la-salud-mental-y-como-enfrentarlo-0

[60] «Amenazas de ciberseguridad modernas: todo lo que necesitas saber», Acronis. Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://www.acronis.com/es-es/blog/posts/modern-cybersecurity-threats/

[61] A. Issa, «Honeypots 104: T-Pot — Your All-in-One Honeypot Platform Guide», Medium. Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://infosecwriteups.com/honeypots-104-t-pot-your-all-in-one-honeypot-platform-guide-0ba2643bc597

[62] «Comprensión de las tácticas de fraude cibernético y su impacto - SearchInform». Accedido: 3 de junio de 2025. [En línea]. Disponible en: https://searchinform.com/cybersecurity/cyber-threats/fraud/essentials/tactics/

[63] «La Constitución establece que el Ecuador tiene derecho a la protección de datos personales – Dirección Nacional de Registros Públicos». Accedido: 30 de octubre de 2025. [En línea]. Disponible en: https://www.registrospublicos.gob.ec/la-constitucion-establece-que-el-ecuador-tiene-derecho-a-la-proteccion-de-datos-personales/

[64] defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf». Accedido: 30 de octubre de 2025. [En línea]. Disponible en: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

[65] «ces.gob.ec/documentos/Normativa/LOES.pdf». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://www.ces.gob.ec/documentos/Normativa/LOES.pdf

[66] H. D. P. Barrezueta, «DIRECTOR DEL REGISTRO OFICIAL».

[67] «telecomunicaciones.gob.ec/wp-content/uploads/2020/06/Acuerdo-No.-012-2019-Guía-para-Tratamiento-de-Datos-Personales.pdf». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2020/06/Acuerdo-No.-012-2019-Gu%C3%ADa-para-Tratamiento-de-Datos-Personales.pdf

[68] «ISO 27001 vs. ISO 27002: Understanding the difference (FAQ)». Accedido: 30 de octubre de 2025. [En línea]. Disponible en: https://www.nemko.com/iso-27001-vs-iso-27002

[69] «oas.org/juridico/pdfs/mesicic4_ecu_const.pdf». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

[70] «biblioteca.defensoria.gob.ec/bitstream/37000/4083/1/Constitución de la República del Ecuador. Actualizada.pdf». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://biblioteca.defensoria.gob.ec/bitstream/37000/4083/1/Constituci%c3%b3n%20de%20la%20Rep%c3%bablica%20del%20Ecuador.%20Actualizada.pdf

[71] «asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes 2013-2017/920-lmoreno/ro-459-5to-sup-26-05-2021.pdf». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/920-lmoreno/ro-459-5to-sup-26-05-2021.pdf

[72] G. Disterer, «ISO/IEC 27000, 27001 and 27002 for Information Security Management», *Journal of Information Security*, vol. 4, n.º 2, pp. 92-100, abr. 2013, doi: 10.4236/jis.2013.42011.

[73] J. Walter, «Explicación de los Honeypots y Honeynets en ciberseguridad», Geekflare Spain. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://geekflare.com/es/honeypots-honeynets/

[74] Imagar, «Honeypot: qué es y cómo ayuda a la ciberseguridad de tu empresa», Imagar. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.imagar.com/blog-desarrollo-web/honeypot-como-ayuda-ciberseguridad-empresa/

[75] C. Levante, «Implementación de un Honeypot para la monitorización y prevención de ataques», Cloud Levante. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://cloudlevante.com/es/2022/11/16/honeypot/

[76] Juan, «Honeypots: La trampa perfecta para ciberdelincuentes y una valiosa herramienta de defensa cibernética», Cibersafety. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://cibersafety.com/honeypots-trampa-ciberdelincuentes/

[77] «Honeypot». Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.hacker-mentor.com/blog/honeypot

[78] Captcha, «¿Qué es un campo Honeypot?», captcha.eu. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.captcha.eu/es/que-es-un-campo-honeypot/

[79] L. Calvo, «Honeypots: Descubre cómo mejorar prácticas para proteger tu red de amenazas cibernéticas», GoDaddy Resources - Spain. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.godaddy.com/resources/es/crearweb/que-es-un-honeypot-y-como-usarlo-en-beneficio-de-tu-negocio

[80] «Honeypots: una guía completa sobre señuelos de ciberseguridad». Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.startupdefense.io/es-us/blog/honeypots-una-guia-completa-sobre-senuelos-de-ciberseguridad

[81] D. M. Rondina, «Honeypot Cyber Security: Overview, How They Work, FAQs», Network Solutions Blog. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.networksolutions.com/blog/honeypot-network-security/

[82] «It’s a Trap — Honeypots Help Defenders Gather Threat Intel». Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.coalitioninc.com/blog/security-labs/undefined/blog/security-labs/what-are-honeypots

[83] «Honeypots avanzados: Mejora la ciberseguridad empresarial | OpenWebinars», OpenWebinars.net. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://openwebinars.net/blog/honeypots-avanzados-mejora-la-ciberseguridad-empresarial/

[84] «What is a Honeypot in Cybersecurity? | CrowdStrike», CrowdStrike.com. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/

[85] Juan, «Honeypots: La trampa perfecta para ciberdelincuentes y una valiosa herramienta de defensa cibernética», Cibersafety. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://cibersafety.com/honeypots-trampa-ciberdelincuentes/

[86] Rapid7, «Rapid7», Rapid7. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.rapid7.com/fundamentals/honeypots/

[87] «¿Qué es un tarro de miel? Trampas de ciberseguridad», ¿Qué es un tarro de miel? Trampas de ciberseguridad. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.avg.com/es/signal/what-is-a-honeypot

[88] «What is a Honeypot in Cybersecurity? [Types and Benefits]», Acalvio. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.acalvio.com/resources/glossary/honeypot/

[89] «Interaction Honeypot - an overview | ScienceDirect Topics». Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.sciencedirect.com/topics/computer-science/interaction-honeypot

[90] «Low Interaction Honeypot - an overview | ScienceDirect Topics». Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.sciencedirect.com/topics/computer-science/low-interaction-honeypot

[91] Z. Moric, L. Mršić, Z. Kunić, y G. Đambić, «Honeypots in Cybersecurity: Their Analysis, Evaluation and Importance», 13 de agosto de 2024, *Preprints*: 2024080946. doi: 10.20944/preprints202408.0946.v1.

[92] CounterCraft, «What's the Real Difference Between Cyber Deception and Honeypots?», CounterCraft. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.countercraftsec.com/blog/whats-real-difference-between-cyber-deception-and-honeypots/

[93] «What is a Honeypot in Cybersecurity? | CrowdStrike», CrowdStrike.com. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/

[94] https://www.linkedin.com/company/xsec, «Honeypots | X Sec - Comunidad de Ciberseguridad». Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://xsec.sh/blog/honeypots/

[95] «Honeypots: una guía completa sobre señuelos de ciberseguridad». Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://www.startupdefense.io/es-us/blog/honeypots-una-guia-completa-sobre-senuelos-de-ciberseguridad

[96] «Honeypot: 5 tipos principales para proteger tus datos», OBS Business School. Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://www.obsbusiness.school/blog/honeypot-5-tipos-principales-para-proteger-tus-datos

[97] BBVA, «"Honeypot", la trampa del tarro de miel para engañar a los ciberdelincuentes», BBVA NOTICIAS. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.bbva.com/es/innovacion/honeypot-la-trampa-del-tarro-de-miel-para-enganar-a-los-ciberdelincuentes/

[98] McAfee, «What Is a Honeypot and Why Is it Important?», McAfee. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://www.mcafee.com/learn/what-is-a-honeypot/

[99] msmk, «¿Qué es un honeypot? - MSMK University», MSMK. Accedido: 2 de septiembre de 2025. [En línea]. Disponible en: https://msmk.university/que-es-un-honeypot-msmk-university/

[100] «Los mejores HoneyPots: ejemplos, tipos, características y configuración», Blog elhacker.NET. Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://blog.elhacker.net/2021/01/los-mejores-honeypots-ejemplos-y-tipos-trampas-rdp-ssh-cowrie-docker-rdpy.html

[101] «seguridad.unam.mx/sites/default/files/20181106-iimashoneypots.pdf». Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://www.seguridad.unam.mx/sites/default/files/20181106-iimashoneypots.pdf

[102] «PDF». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=6540&context=etd

[103] F. G. T. Barahona, «TÍTULO ANÁLISIS DE T-POT, UN HONEYPOT OPEN SOURCE».

[104] «PDF». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://elhacker.info/Cursos/(Tutorial)%20Hacking%20Etico%20Avanzado/Sesion%2012%20HoneyPots/docs/honeypots_teoria.pdf

[105] «¿Qué es un honeypot?», IONOS Digital Guide. Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://www.ionos.com/es-us/digitalguide/servidores/seguridad/honeypot-seguridad-informatica-para-detectar-amenazas/

[106] admin, «Honeypots Industriales: Conoce a tu Enemigo», InprOTech. Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://inprotech.es/techpaper-industrial-honeypots-know-your-enemy/

[107] Z. Morić, V. Dakić, y D. Regvart, «Advancing Cybersecurity with Honeypots and Deception Strategies», *Informatics*, vol. 12, n.º 1, p. 14, mar. 2025, doi: 10.3390/informatics12010014.

[108] «Low, Medium and High Interaction Honeypot Security», Akamai. Accedido: 28 de septiembre de 2025. [En línea]. Disponible en: https://www.akamai.com/blog/security/high-interaction-honeypot-versus-low-interaction-honeypot-comparison

[109] «An Overview of Honeypot Systems». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://www.researchgate.net/publication/332113726_An_Overview_of_Honeypot_Systems

[110] «Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://www.mdpi.com/2079-9292/13/13/2465

[111] X. Yang, J. Yuan, H. Yang, Y. Kong, H. Zhang, y J. Zhao, «A Highly Interactive Honeypot-Based Approach to Network Threat Management», *Future Internet*, vol. 15, n.º 4, p. 127, abr. 2023, doi: 10.3390/fi15040127.

[112] Salahaddin University-Erbil, R. B. Khoshnaw, y Cihan University-Erbil, «A Comparative Analysis Between Low and High Level Honeypots», *Cihan Univ.-Erbil Sci. J.*, vol. 2017, n.º Special-1, pp. 41-50, 2017, doi: 10.24086/cuesj.si.2017.n1a4.

[113] «unb.ca/cic/_assets/documents/cic_honeynet_07-09_21-09_2018.pdf». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://www.unb.ca/cic/_assets/documents/cic_honeynet_07-09_21-09_2018.pdf

[114] «A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks», ResearchGate. Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://www.researchgate.net/publication/222261404_A_hybrid_honeypot_framework_for_improving_intrusion_detection_systems_in_protecting_organizational_networks

[115] staffadmin, «LACNIC CSIRT - HoneyNet del CSIRT de LACNIC», LACNIC CSIRT. Accedido: 19 de octubre de 2025. [En línea]. Disponible

en: https://csirt.lacnic.net/articulos-y-novedades/honeynet-del-csirt-de-lacnic

[116] «LACNIC CSIRT - LACNIC Honeynet», LACNIC CSIRT. Accedido: 19 de octubre de 2025. [En línea]. Disponible en: https://csirt.lacnic.net/honeynet

[117] «What is Honeypot?», GeeksforGeeks. Accedido: 17 de octubre de 2025. [En línea]. Disponible en: https://www.geeksforgeeks.org/blogs/what-is-honeypot/

[118] F. Samu, «Design and Implementation of a Real-Time Honeypot System for the Detection and Prevention of Systems Attacks».

[119] X. Yang, J. Yuan, H. Yang, Y. Kong, H. Zhang, y J. Zhao, «A Highly Interactive Honeypot-Based Approach to Network Threat Management», *Future Internet*, vol. 15, n.º 4, p. 127, abr. 2023, doi: 10.3390/fi15040127.

[120] «Honeypot vs Honeynet», GeeksforGeeks. Accedido: 17 de octubre de 2025. [En línea]. Disponible en: https://www.geeksforgeeks.org/ethical-hacking/honeypot-vs-honeynet/

[121] H. Fernández, J. Sznek, y E. Grosclaude, «Detección y limitaciones de ataques clásicos con Honeynets virtuales».

[122] X. Bellekens, «Set up T-POT honeypot in the cloud in less than 30 minutes», Lupovis. Accedido: 17 de septiembre de 2025. [En línea]. Disponible en: https://www.lupovis.io/set-up-t-pot-honeypot-in-cloud-in-less-than-30-minutes/

[123] «¿Qué es un honeypot? Cómo colaboran los honeypots con la seguridad», /. Accedido: 6 de abril de 2025. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot

[124] Hexshubz, «Honeypot(T-Pot) with AWS», Medium. Accedido: 17 de septiembre de 2025. [En línea]. Disponible en: https://medium.com/@hexshubz/tpot-05ef42c5f2a4

[125] PricewaterhouseCoopers, «Unveiling the threat landscape: Insights from T-Pot honeypot on cyber attacks in Malta», PwC. Accedido: 17 de septiembre de 2025. [En línea]. Disponible en: https://www.pwc.com/mt/en/publications/technology/tpot.html

[126] Waidroc, «Implementación de un Honeypot con T-Pot», Waidroc. Accedido: 17 de septiembre de 2025. [En línea]. Disponible en: https://waidroc.github.io/posts/TPot/

[127] V. Valeros, «Installing T-Pot Honeypot Framework in the Cloud», Stratosphere Laboratory. Accedido: 17 de septiembre de 2025. [En línea]. Disponible en: https://www.stratosphereips.org/blog/2020/10/10/installing-t-pot-honeypot-framework-in-the-cloud

[128] A. Matthews, «My T-pot setup», Medium. Accedido: 17 de septiembre de 2025. [En línea]. Disponible en: https://systemweakness.com/my-t-pot-setup-672a45044ad5

[129] A. Matthews, «T-pot: Cowrie Honeypot Analysis», Medium. Accedido: 17 de septiembre de 2025. [En línea]. Disponible en: https://medium.com/@ashlyncmatthews/t-pot-cowrie-honeypot-analysis-5e3793bb9128

[130] X. Bellekens, «Getting Threat Intel from T-Pot: An Analysis», Lupovis. Accedido: 17 de septiembre de 2025. [En línea]. Disponible en: https://www.lupovis.io/getting-threat-intel-from-t-pot-an-analysis/

[131] D. Horovits, «The Complete Guide to the ELK Stack», Logz.io. Accedido: 7 de octubre de 2025. [En línea]. Disponible en: https://logz.io/learn/complete-guide-elk-stack/

[132] «¿Qué es la pila ELK? Explicación de las pilas Elasticsearch, Logstash y Kibana. AWS», Amazon Web Services, Inc. Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://aws.amazon.com/es/what-is/elk-stack/

[133] Sumayasomow, «30-Day SOC Challenge — Day 26», Medium. Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://medium.com/@sumayasomow/30-day-soc-challenge-day-26-a4c4b2cc0e2b

[134] S. Ducksbury, «Elastic Beats and Where They Fit With ELK Stack», Instaclustr. Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://www.instaclustr.com/blog/elastic-beats-and-where-they-fit-with-elk-stack/

[135] D. Horovits, «The Complete Guide to the ELK Stack», Logz.io. Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://logz.io/learn/complete-guide-elk-stack/

[136] «Not sure whether to use Logstash or Beats | Beats». Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://www.elastic.co/docs/reference/beats/filebeat/diff-logstash-beats

[137] «Panels and visualizations | Elastic Docs». Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://www.elastic.co/docs/explore-analyze/visualize

[138] «Kibana dashboards | Elastic Docs». Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://www.elastic.co/docs/explore-analyze/dashboards

[139] «Exploring dashboards | Elastic Docs». Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://www.elastic.co/docs/explore-analyze/dashboards/using

[140] «Building dashboards | Elastic Docs». Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://www.elastic.co/docs/explore-analyze/dashboards/building

[141] «Suricata — Security Onion Documentation 2.4 documentation». Accedido: 17 de octubre de 2025. [En línea]. Disponible en: https://docs.securityonion.net/en/2.4/suricata.html

[142] «Visualizar con Grafana los eventos del IDS/IPS Suricata (Eve.json)», Blog elhacker.NET. Accedido: 17 de octubre de 2025. [En línea]. Disponible en: https://blog.elhacker.net/2024/11/visualizar-con-grafana-los-eventos-del-ids-suricata-eve-json.html

[143] «Conoce Cyberchef: una navaja suiza digital para facilitar análisis y decodificación». Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://www.welivesecurity.com/es/recursos-herramientas/cyberchef-navaja-suiza-digital-analisis-decodificacion/

[144] Informática, «CyberChef: Convierte, analiza y decodifica datos fácilmente en un solo lugar», CEC. Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://www.cec.es/cyberchef-convierte-analiza-y-decodifica-datos-facilmente-en-un-solo-lugar/

[145] R. Parekh, «Best Open Source Tools for Elasticsearch», simplyblock. Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://www.simplyblock.io/blog/best-open-source-tools-for-elasticsearch/

[146] «Cowrie — cowrie 2.7.1.dev11+g3639a6847 documentation». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://docs.cowrie.org/en/latest/README.html#documentation

[147] «Using the Proxy — cowrie 2.7.1.dev11+g3639a6847 documentation». Accedido: 30 de septiembre de 2025. [En línea]. Disponible en: https://docs.cowrie.org/en/latest/PROXY.html

[148] M. Oosterhof, «cowrie Documentation».

[149] «Cowrie Honeypot: Ataques de fuerza bruta | Revista .Seguridad». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://revista.seguridad.unam.mx/numero-28/cowrie-honeypot

[150] C. Kelly, N. Pitropakis, A. Mylonas, S. McKeown, y W. J. Buchanan, «A Comparative Analysis of Honeypots on Different Cloud Platforms», *Sensors*, vol. 21, n.º 7, p. 2433, ene. 2021, doi: 10.3390/s21072433.

[151] «Cowrie Honeypot Analysis - 24hrs of Attacks», HackerTarget.com. Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://hackertarget.com/cowrie-honeypot-analysis-24hrs/

[152] «PoC: Captura de malware con el honeypot Dionaea - II | Proyecto Honeynet UNAM Chapter». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://www.honeynet.unam.mx/es/content/poc-captura-de-malware-con-el-honeypot-dionaea-ii

[153] «Introduction — dionaea 0.11.0 documentation». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://dionaea.readthedocs.io/en/latest/introduction.html

[154] S. Shahrivartehrani, «Dionaea Honeypot Implementation and Malware Analysis in Cloud Environment», 2016.

[155] «Tips and Tricks — dionaea 0.11.0 documentation». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://dionaea.readthedocs.io/en/latest/old/tips_and_tricks.html#http

[156] Latoya, «Dionaea Honeypot Review with Splunk», Medium. Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://version-laa.medium.com/dionaea-honeypot-review-with-splunk-8e743760bd2

[157] «HoneyPots Parte 3 - Configuración y análisis de malware con Dionaea - The Hacker Way». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://thehackerway.es/2015/04/14/honeypots-parte-3-configuracion-y-analisis-de-malware-con-dionaea/

[158] «PoC: Captura de malware con el honeypot Dionaea - Parte I | Revista .Seguridad». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://revista.seguridad.unam.mx/numero23/poc-captura-de-malware-con-el-honeypot-dionaea-parte-i

[159] «The Honeynet Project». Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://www.honeynet.org/2016/03/23/heralding-the-credentials-catching-honeypot/

[160] J. Trost, «Adventures with Heralding, a Credential Grabbing Honeypot», Medium. Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://jason-trost.medium.com/adventures-with-heralding-a-credential-grabbing-honeypot-ec820c848c7e

[161] C. De Novellis, «Analysis of application layer attacks on honeypot logs», laurea, Politecnico di Torino, 2022. Accedido: 14 de octubre de 2025. [En línea]. Disponible en: https://webthesis.biblio.polito.it/23596/

[162] «Red de señuelos T-Pot: Cómo configurar y monitorizar tu propia red de señuelos». Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://www.bokehsolutions.com/component/content/article/t-pot-honeynet-how-to-set-up-and-monitor-your-own-network-of-decoys.html?catid=12&Itemid=101

[163] «T-Pot: Una colmena de Honeypots para atraparlos a todos». Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://www.elladodelmal.com/2017/07/t-pot-una-colmena-de-honeypots-para.html

[164] «GitHub - bontchev/elasticpot: An Elasticsearch honeypot». Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://github.com/bontchev/elasticpot?tab=readme-ov-file

[165] «SNARE — SNARE v0.3 documentation». Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://snare.readthedocs.io/en/latest/quick-start.html#basic-concepts

[166] «Tanner WEB — tanner 1.0 documentation». Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://tanner.readthedocs.io/en/latest/web.html

[167] «Quick Start — tanner 1.0 documentation». Accedido: 10 de noviembre de 2025. [En línea]. Disponible en: https://tanner.readthedocs.io/en/latest/quick-start.html#basic-concept

[168] «Honeypots: Tracking Attacks Against Misconfigured or Exposed Services», ReliaQuest. Accedido: 10 de noviembre de 2025. [En línea].

Disponible en: https://reliaquest.com/blog/honeypots-tracking-attacks-against-misconfigured-or-exposed-services/

[169] C. Kelly, N. Pitropakis, A. Mylonas, S. McKeown, y W. J. Buchanan, «A Comparative Analysis of Honeypots on Different Cloud Platforms», *Sensors*, vol. 21, n.º 7, p. 2433, ene. 2021, doi: 10.3390/s21072433.

[170] «Snort - Network Intrusion Detection & Prevention System». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://www.snort.org/

[171] S. Perez, «Practical SIEM tools for SCADA environment», Iowa State University, Ames (Iowa), ene. 2018. doi: 10.31274/cc-20240624-1140.

[172] «The Basics - Snort 3 Rule Writing Guide». Accedido: 3 de octubre de 2025. [En línea]. Disponible en: https://docs.snort.org/rules/

[173] «Cómo detectar malware con reglas de Suricata». Accedido: 5 de octubre de 2025. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2021/10/21/como-detectar-codigos-maliciosos-reglas-suricata/

[174] «What is Suricata? A Powerful Tool for Cybersecurity Professionals», Huntress. Accedido: 5 de octubre de 2025. [En línea]. Disponible en: https://www.huntress.com/cybersecurity-education/cybersecurity-101/topic/what-is-suricata

[175] D. Robinette, «What is the Difference Between Snort and Zeek?» Accedido: 5 de octubre de 2025. [En línea]. Disponible en: https://www.stamus-networks.com/blog/what-is-the-difference-between-snort-and-zeek

[176] A. Wallace, «Spot trouble early with honeypots and Suricata», Pen Test Partners. Accedido: 5 de octubre de 2025. [En línea]. Disponible en: https://www.pentestpartners.com/security-blog/spot-trouble-early-with-honeypots-and-suricata/

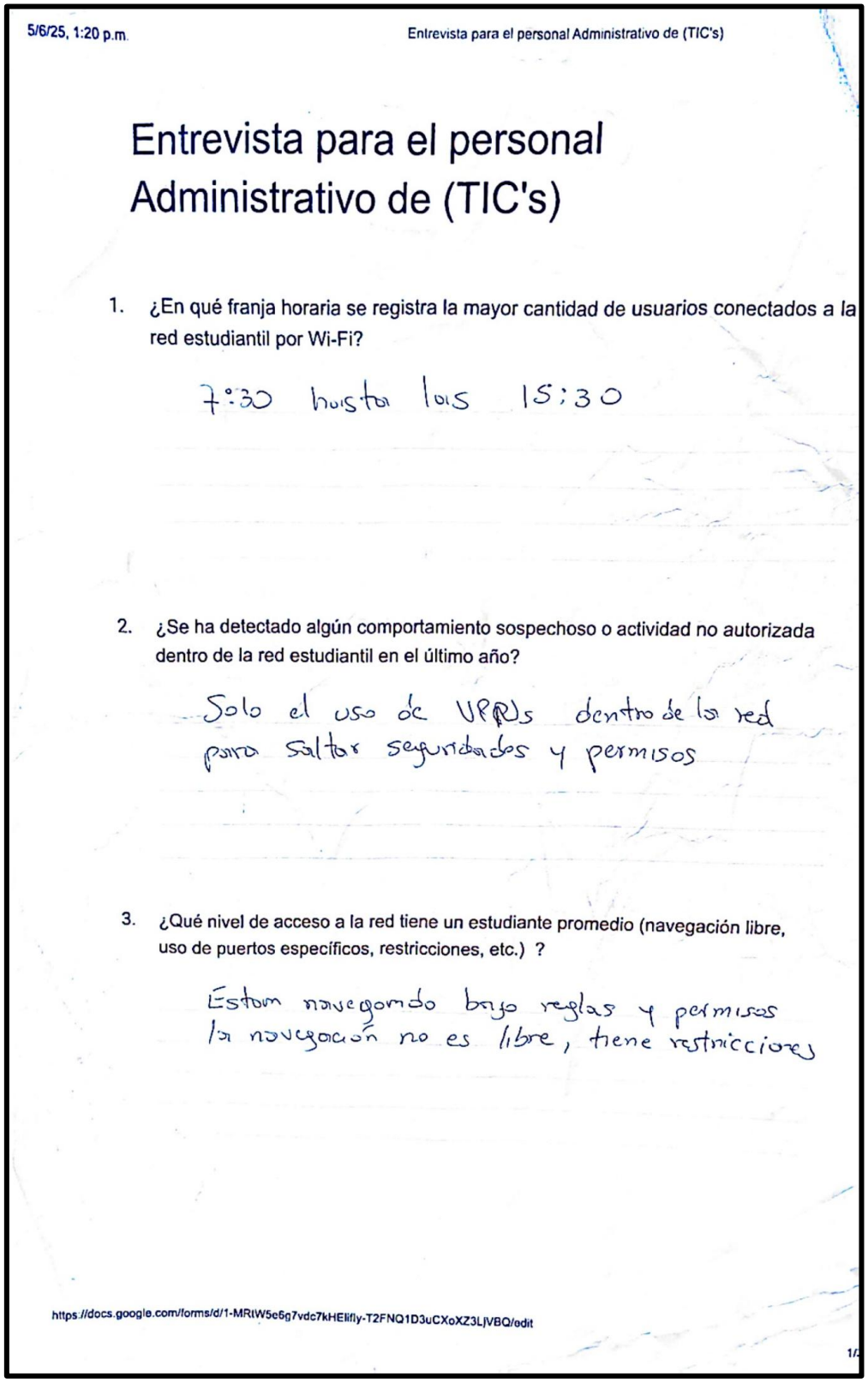
[177] gabrielrc2, «Análisis de honeypots mediante T-Pot», Seguridad en las Comunicaciones. Accedido: 5 de octubre de 2025. [En línea]. Disponible

en: https://seguridadcomunicaciones.wordpress.com/2023/12/17/analisis-de-honeypots-mediante-t-pot/

[178] «TFG-G5283.pdf». Accedido: 5 de octubre de 2025. [En línea]. Disponible en: https://uvadoc.uva.es/bitstream/handle/10324/50446/TFG-G5283.pdf?sequence=1&isAllowed=y

[179] R. Perdigón-Llanes, «Evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio», *Revista Científica de Sistemas e Informática*, vol. 2, n.º 2, pp. e363-e363, jul. 2022, doi: 10.51252/rcsi.v2i2.363.

ANEXOS



5/6/25, 1:20 p.m. Entrevista para el personal Administrativo de (TIC's)

Entrevista para el personal Administrativo de (TIC's)

1. ¿En qué franja horaria se registra la mayor cantidad de usuarios conectados a la red estudiantil por Wi-Fi?

   7:30 hasta las 15:30

2. ¿Se ha detectado algún comportamiento sospechoso o actividad no autorizada dentro de la red estudiantil en el último año?

   Solo el uso de VPNs dentro de la red para saltar seguridades y permisos

3. ¿Qué nivel de acceso a la red tiene un estudiante promedio (navegación libre, uso de puertos específicos, restricciones, etc.) ?

   Estoy navegando bajo reglas y permisos la navegación no es libre, tiene restricciones

https://docs.google.com/forms/d/1-MRtW5e6g7vdc7kHEIifly-T2FNQ1D3uCXoXZ3LjVBQ/edit

1/

Anexo 1: Entrevista

4. ¿Qué tipo de tráfico o protocolos son más comunes en la red estudiantil? (HTTP, FTP, SSH, etc.)

En red Estudiantes solo navegación HTTP los demás protocolos estan restringidos sobre todo puertos protocolos que permiten conexiones entre dispositivos FTP o SSH así tambien de P2P y streaming.

5. ¿Considera viable implementar un servidor virtual adicional con fines de investigación y monitoreo de amenazas?

Contamos con un equipo de seguridad perimetral que controla y monitorea amenazas pero si consideramos que sería necesario contar con monitoreo adicional.

6. ¿Cuál es el promedio diario de usuarios que se conectan a la red de "ESTUDIANTES" por medio Wi-Fi?

Un promedio de 2700 al día.

ENCUESTA SOBRE SEGURIDAD EN LA RED ESTUDIANTIL DE LA UPSE

Objetivo: Conocer la percepción y experiencias de los estudiantes de la UPSE respecto a la seguridad de la red estudiantil "ESTUDIANTES", con el fin de identificar comportamientos, incidentes y necesidades que contribuyan al diseño de mejores medidas de protección institucional.

Instrucciones: Esta encuesta es anónima y tomará aproximadamente 5-7 minutos. Por favor, responda con sinceridad.

Facultad a la que pertenece:

- ◯ Facultad de Sistemas y Telecomunicaciones
- ◯ Facultad de Ciencias Sociales y de la Salud
- ◯ Facultad de Ciencias de la Educación e Idiomas
- ◯ Facultad de Ciencias del Mar
- ◯ Facultad de Ciencias Administrativas
- ◯ Facultad de Ciencias Agrarias

Semestre académico que cursa actualmente: *

- ◯ 1-2 semestre
- ◯ 3-4 semestre
- ◯ 5-6 semestre
- ◯ 7-8 semestre

¿En qué horarios se conecta con mayor frecuencia? *

- ◯ 7:00 - 10:00 AM
- ◯ 10:00 - 1:00 PM
- ◯ 1:00 - 3:00 PM
- ◯ 3:00 - 5:00 PM

¿Qué dispositivos utiliza para conectarse a la red estudiantil? (Puede seleccionar varios) *

- ☐ Laptop
- ☐ Smartphone
- ☐ Tablet
- ☐ Computadora de escritorio
- ☐ Otros: _____

Semestre académico que cursa actualmente: *

- ◯ 1-2 semestre
- ◯ 3-4 semestre
- ◯ 5-6 semestre
- ◯ 7-8 semestre

¿Con qué frecuencia se conecta a la red Wi-Fi "ESTUDIANTES"? *

- ◯ Diariamente
- ◯ 3-4 veces por semana
- ◯ 1-2 veces por semana
- ◯ Ocasionalmente

¿Para qué actividades utiliza principalmente la red estudiantil? (Puede seleccionar varios) *

- ☐ Investigación académica y consulta de recursos educativos
- ☐ Acceso a plataformas institucionales (EVA, correo institucional, etc.)
- ☐ Comunicación (redes sociales, mensajería)
- ☐ Streaming de videos/música
- ☐ Descarga de archivos
- ☐ Juegos en línea
- ☐ Otros: _____

¿Qué tan familiarizado está con conceptos de seguridad informática? *

- ◯ Muy familiarizado
- ◯ Familiarizado
- ◯ Poco familiarizado
- ◯ Nada familiarizado

¿Conoce qué es el phishing (suplantación de identidad digital)? *

- ◯ Sí, y sé cómo identificarlo
- ◯ Sí, pero no sé cómo identificarlo
- ◯ He escuchado el término pero no sé qué significa
- ◯ No

¿Conoce qué es el malware (software malicioso)? *

- ◯ Sí, y sé cómo protegerme
- ◯ Sí, pero no sé cómo protegerme
- ◯ He escuchado el término pero no sé qué significa
- ◯ No

¿Qué tan importante considera que la universidad implemente mejores medidas de seguridad en la red estudiantil? *

- ◯ Muy importante
- ◯ Importante
- ◯ Nada importante

¿Utiliza alguna medida adicional de seguridad al conectarse a la red estudiantil? *
(Puede seleccionar varios)

- [ ] VPN (Red Privada Virtual)
- [ ] Navegación en modo incógnito/privado
- [ ] Extensiones de navegador para seguridad
- [ ] Verificación de certificados de sitios web (HTTPS)
- [ ] Ninguna medida adicional
- [ ] Otros: _____

¿Ha experimentado alguno de los siguientes problemas al usar la red estudiantil? *
(Puede seleccionar varios)

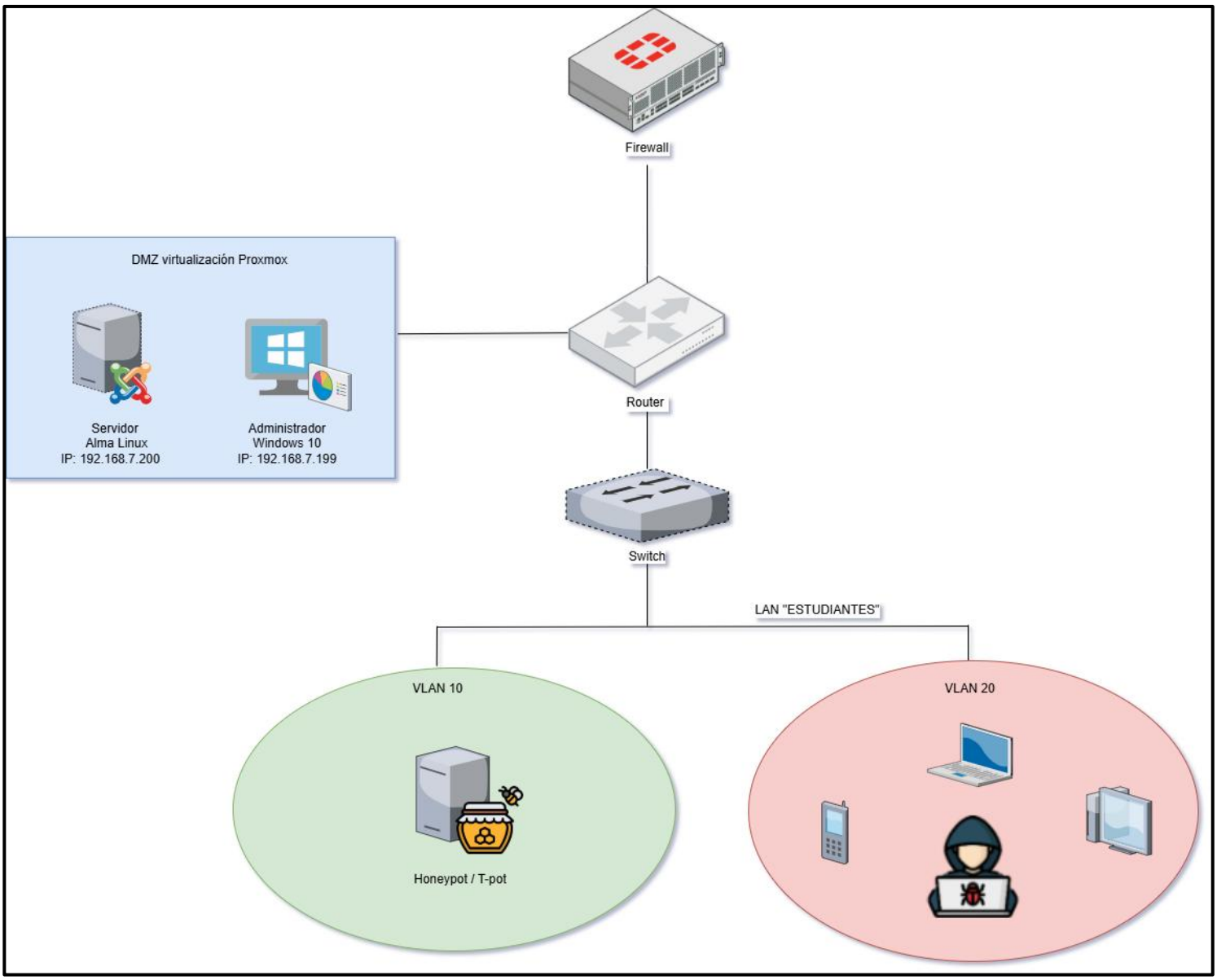
- [ ] Ralentización inexplicable de conexión
- [ ] Desconexión frecuente
- [ ] Redirección a páginas web sospechosas
- [ ] Ventanas emergentes (pop-ups) excesivas
- [ ] Mensajes de advertencia de seguridad
- [ ] Ninguno
- [ ] Otros: _____

¿Con qué frecuencia cambia sus contraseñas? *

- ◯ Cada 1-3 meses
- ◯ Cada 6 meses
- ◯ Una vez al año
- ◯ Solo cuando me lo solicitan o cuando olvido mi contraseña
- ◯ Nunca

¿Se siente cómodo/a ingresando información personal o confidencial mientras está conectado/a a la red estudiantil? *

- ◯ Sí, muy cómodo
- ◯ No, nada cómodo
- ◯ Depende del tipo de información



Anexo 3: Topología de red

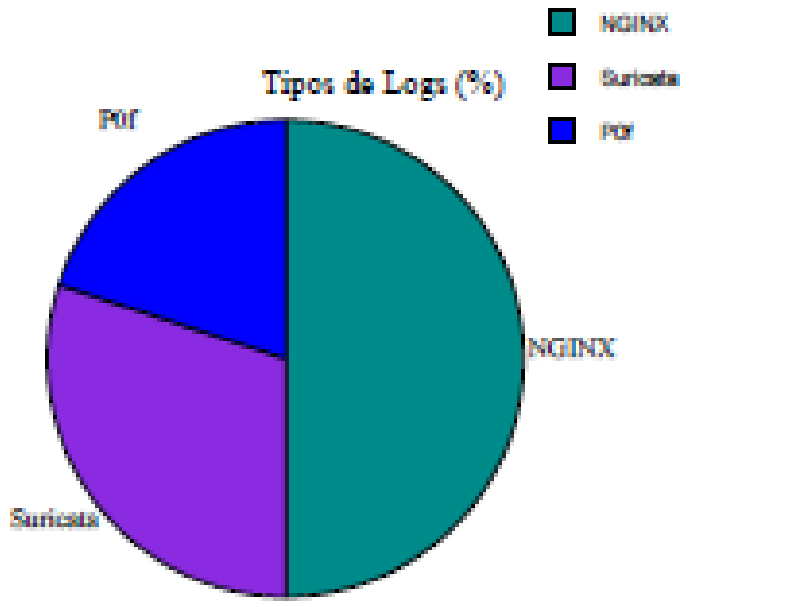
Informe de Seguridad T-Pot Honeypot

Resumen Ejecutivo

Este informe analiza los logs del honeypot T-Pot en la red estudiantil, destacando amenazas detectadas, distribuciones geográficas y patrones temporales. Se identificaron picos de actividad y se incluyen recomendaciones para mitigar riesgos.

Métrica	Valor
Total de Logs Analizados	10
Periodo de Análisis	2025-06-03 02:52 a 2025-06-03 02:52
Tipos de Logs	NGINX, Suricata, P0f
IPs de Amenaza Únicas	0
Países Involucrados	1
Alertas Críticas (Suricata)	0

Análisis General



Anexo 4: Resultado del informe (2)

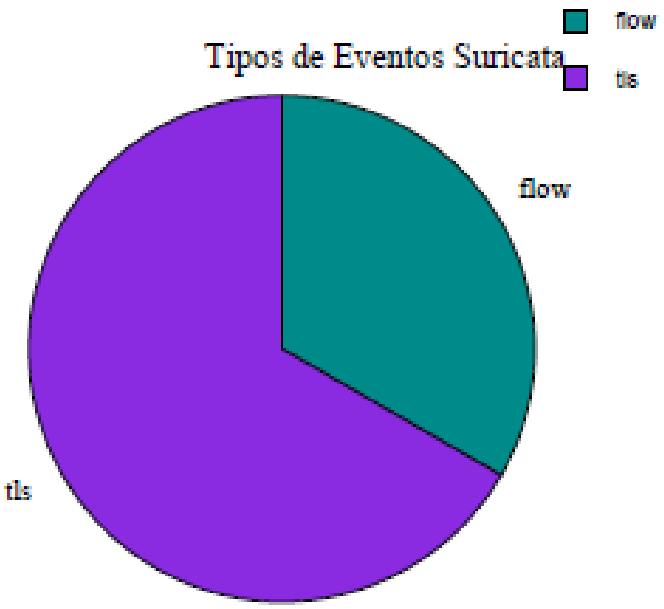
Informe de Seguridad T-Pot Honeypot

Detalles por Tipo de Log

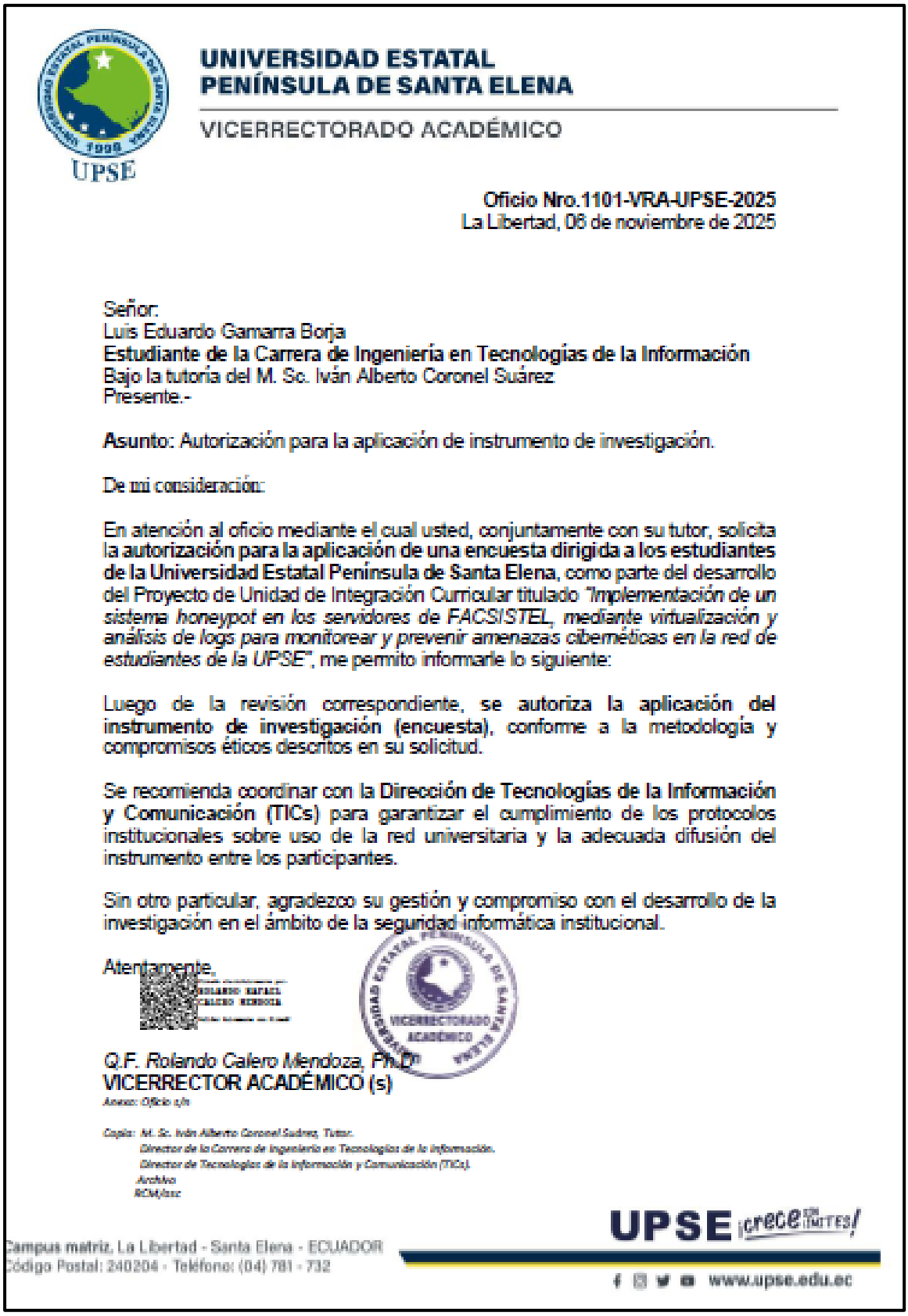
Actividad HTTP (NGINX)

Timestamp	Método	URI	Status	IP
2025-06-03 02:52	GET	/es/	200.0	192.168.100.5
2025-06-03 02:52	GET	/es/_cluster/health	200.0	192.168.100.5
2025-06-03 02:52	GET	/es/_snapshot	200.0	192.168.100.5
2025-06-03 02:52	GET	/elasticvue/assets/hack-italic-CQtdA7T5.woff2?sha=...	200.0	192.168.100.5
2025-06-03 02:52	GET	/es/_cat/indices/?h=index%2Chealth%2Cpri%2Crep%2Cs...	200.0	192.168.100.5

Eventos Suricata



Anexo 5: Resultado del informe (2)



UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

VICERRECTORADO ACADÉMICO

Oficio Nro.1101-VRA-UPSE-2025
La Libertad, 06 de noviembre de 2025

Señor:
Luis Eduardo Gamarra Borja
Estudiante de la Carrera de Ingeniería en Tecnologías de la Información
Bajo la tutoría del M. Sc. Iván Alberto Coronel Suárez
Presente.-

Asunto: Autorización para la aplicación de instrumento de investigación.

De mi consideración:

En atención al oficio mediante el cual usted, conjuntamente con su tutor, solicita la **autorización para la aplicación de una encuesta dirigida a los estudiantes de la Universidad Estatal Península de Santa Elena**, como parte del desarrollo del Proyecto de Unidad de Integración Curricular titulado *"Implementación de un sistema honeypot en los servidores de FACSISTEL, mediante virtualización y análisis de logs para monitorear y prevenir amenazas cibernéticas en la red de estudiantes de la UPSE"*, me permito informarle lo siguiente:

Luego de la revisión correspondiente, se **autoriza la aplicación del instrumento de investigación (encuesta)**, conforme a la metodología y compromisos éticos descritos en su solicitud.

Se recomienda coordinar con la **Dirección de Tecnologías de la Información y Comunicación (TICs)** para garantizar el cumplimiento de los protocolos institucionales sobre uso de la red universitaria y la adecuada difusión del instrumento entre los participantes.

Sin otro particular, agradezco su gestión y compromiso con el desarrollo de la investigación en el ámbito de la seguridad informática institucional.

Atentamente,

Q.F. Rolando Calero Mendoza, Ph.D
VICERRECTOR ACADÉMICO (s)
Anexo: Oficio s/n

Copia: M. Sc. Iván Alberto Coronel Suárez, Tutor.
Director de la Carrera de Ingeniería en Tecnologías de la Información.
Director de Tecnologías de la Información y Comunicación (TICs).
Archivo
RCM/asc

Campus matriz, La Libertad - Santa Elena - ECUADOR
Código Postal: 240204 - Teléfono: (04) 781 - 732

UPSE ¡crece los mites!
www.upse.edu.ec

Anexo 6: autorización de la herramienta de investigación