



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

**Implementación de una herramienta Open Source
para el registro de incidentes de seguridad digital del
Centro Nacional de Seguridad Digital del Perú**

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Paul Fernando SALAZAR ESCOBEDO

ASESOR

Nilo Eloy CARRASCO ORE

Lima, Perú

2022



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Salazar, P. (2022). *Implementación de una herramienta Open Source para el registro de incidentes de seguridad digital del Centro Nacional de Seguridad Digital del Perú*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	PAUL FERNANDO SALAZAR ESCOBEDO
Tipo de documento de identidad	DNI
Número de documento de identidad	43044227
URL de ORCID	https://orcid.org/0000-0001-8614-1602
Datos de asesor	
Nombres y apellidos	Nilo Eloy Carrasco Ore
Tipo de documento de identidad	DNI
Número de documento de identidad	09342780
URL de ORCID	https://orcid.org/0000-0001-5664-9309
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Joel Fernando Machado Vicente
Tipo de documento	DNI
Número de documento de identidad	40476778
Miembro del jurado 1	
Nombres y apellidos	FanyYexeniaSobero Rodríguez
Tipo de documento	DNI
Número de documento de identidad	20120467
Datos de investigación	
Línea de investigación	No aplica
Grupo de investigación	No aplica
Agencia de financiamiento	Sin financiamiento
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Cercado de Lima

	Jr. Carlos Amezaga No. 375 Universidad Nacional Mayor de San Marcos Latitud: -12.0564232 Longitud: -77.0843327
Año o rango de años en que se realizó la investigación	2022
URL de disciplinas OCDE	2.02.04 -- Ingeniería de sistemas y comunicaciones https://purl.org/pe-repo/ocde/ford#2.02.04



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
Escuela Profesional de Ingeniería de Sistemas

Acta Virtual de Sustentación
del Trabajo de Suficiencia Profesional

Siendo las 19:00 horas del día 23 de agosto del año 2022, se reunieron virtualmente los docentes designados como Miembros de Jurado del Trabajo de Suficiencia Profesional, presidido por el Mg. Machado Vicente Joel Fernando (Presidente), Mg. Sobero Rodríguez Fany Yexenia (Miembro) y el Ing. Carrasco Ore Nilo Eloy (Miembro Asesor), usando la plataforma Meet (<https://meet.google.com/nvd-sypk-tbu>), para la sustentación virtual del Trabajo de Suficiencia Profesional intitulado: **“IMPLEMENTACIÓN DE UNA HERRAMIENTA OPEN SOURCE PARA EL REGISTRO DE INCIDENTES DE SEGURIDAD DIGITAL DEL CENTRO NACIONAL DE SEGURIDAD DIGITAL DEL PERÚ”**, por el Bachiller Salazar Escobedo Paul Fernando; para obtener el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición del Trabajo de Suficiencia Profesional, el Presidente invitó al Bachiller a dar las respuestas a las preguntas establecidas por los miembros del Jurado.

El Bachiller en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros del Jurado, el Bachiller obtuvo la nota de **17 (DIECISIETE)**.

A continuación el Presidente de Jurados el Mg. Machado Vicente Joel Fernando, declara al Bachiller **Ingeniero de Sistemas**.

Siendo las 19:58 horas, se levantó la sesión.

Presidente

Mg. Machado Vicente Joel Fernando

Miembro

Mg. Sobero Rodríguez Fany Yexenia

Miembro Asesor

Ing. Carrasco Ore Nilo Eloy



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, DECANA DE AMÉRICA
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA
Escuela Profesional de Ingeniería de Sistemas

INFORME DE EVALUACIÓN DE ORIGINALIDAD

1. Facultad de Ingeniería de Sistemas e Informática
2. Escuela Profesional de Ingeniería de Sistemas
3. Autoridad académica que emite el informe de originalidad
Directora (e) de la EPIS
4. Apellidos y Nombres de la autoridad académica
Dra. Luzmila Elisa Pró Concepción
5. Operador del programa informático de similitudes
Dra. Luzmila Elisa Pró Concepción
6. Documento evaluado
Título de pregrado: "Implementación de una Herramienta Open Source para el Registro de Incidentes de Seguridad Digital del Centro Nacional de Seguridad Digital del Perú"
7. Autor del documento
Bach. Salazar Escobedo, Paul Fernando
8. Fecha de recepción del documento **10/09/2022**
9. Fecha de aplicación del programa informático de similitudes **10/09/2022**
10. Software utilizado
 - Turnitin
11. Configuración del programa detector de similitudes
 - Excluye textos entrecomillados
 - Excluye bibliografía
 - Excluye cadenas menores a 40 palabras
12. Porcentaje de similitudes según programa detector de similitudes **7(siete)%**
13. Fuentes originales de las similitudes encontradas
Se adjunta en el anexo 1
14. Observaciones
15. Calificación de originalidad
 - Documento cumple criterios de originalidad, sin observaciones ☒
 - Documento cumple criterios de originalidad, con observaciones ☐
 - Documento no cumple criterios de originalidad ☐
16. Fecha de informe **16/09/2022**



Firmado digitalmente por PRO
CONCEPCION Luzmila Elisa FAU
20148092282 soft
Motivo: Soy el autor del documento
Fecha: 18.11.2022 10:09:45 -05:00

Firma de evaluador
Dra. Luzmila E. Pró Concepción
Directora (e) de la EPIS



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú, DECANA DE AMÉRICA
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA
Escuela Profesional de Ingeniería de Sistemas

ANEXO 1

Fuentes originales de las similitudes encontradas

1. **cdn.www.gob.pe: 3%**
2. **hdl.handle.net: 2%**
3. **mchughsecurity.com: 1%**
4. **cybertesis.unmsm.edu.pe: 1%**



UNMSM

Firmado digitalmente por PRO
CONCEPCION Luzmila Elisa FAU
20148092282 soft
Motivo: Soy el autor del documento
Fecha: 14.11.2022 23:20:06 -05:00

Firma de evaluador

Dra. Luzmila E. Pró Concepción

Director (e) de la EPIS

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Implementación de una herramienta open source para el registro de incidentes de seguridad digital del Centro Nacional De Seguridad Digital Del Perú

Autor: Salazar Escobedo, Paul Fernando

Asesor: Carrasco Ore, Nilo Eloy

Título: Trabajo de Suficiencia Profesional para optar el Título Profesional de Ingeniero de Sistemas

Fecha: Mayo 2022

RESUMEN

El presente informe de experiencia laboral describe la implementación de una herramienta open source para el registro de incidentes en el Centro Nacional de Seguridad Digital (CNSD), dado que las incidencias tecnológicas son parte del día a día, el objetivo general es llevar un control adecuado del registro de incidencias tecnológicas. Buscando una solución de bajo presupuesto se optó por el uso de un software Open Source eligiendo TheHive (versión 4.0) porque nos brinda diferentes beneficios ya que tiene un diseño modular, es decir que se puede integrar a otras herramientas como MISP (plataforma de inteligencia contra amenazas) o Cortex (motor de análisis), además este sistema fue implementado en Amazon Web Services (AWS) que es un conjunto de herramientas y servicios de cloud computing. También se usó las herramientas como MariaDB para la gestión de Base de datos, Apache Cassandra, Elasticsearch que se ejecuta en una instancia de Amazon EC2. Como resultado, el uso de este Sistema permitió llevar el control del registro de incidencias tecnológicas presentadas.

Palabras claves: Gestión de incidentes, Implementación, seguridad digital, integración, herramientas.

MAJOR NATIONAL UNIVERSITY OF SAN MARCOS
FACULTY OF SYSTEMS AND INFORMATICS ENGINEERING
PROFESSIONAL SCHOOL OF SYSTEM ENGINEERING

**Implementation of an open source tool for recording digital security incidents at
the National Digital Security Center of Peru**

Author: Salazar Escobedo, Paul Fernando

Advisor: Carrasco Ore, Nilo Eloy

**Title: Professional Sufficiency Work to opt for the Professional Title of
Systems Engineer**

Date: May 2022

ABSTRACT

This work experience report describes the implementation of an open source tool for the registration of incidents in the National Digital Security Center (CNSD), since technological incidents are part of the day to day, the overall objective is to keep an adequate control of the registration of technological incidents. Looking for a low budget solution we opted for the use of an Open Source software choosing TheHive (version 4.0) because it gives us different benefits since it has a modular design, that is, it can be integrated with other tools such as MISP (threat intelligence platform) or Cortex (analysis engine), in addition this system was implemented in Amazon Web Services (AWS) which is a set of tools and cloud computing services. We also used tools such as MariaDB for database management, Apache Cassandra, Elasticsearch running on an Amazon EC2 instance. As a result, the use of this system allowed to keep track of the log of technological incidents.

Key words: Incident management, Implementation, digital security, integration, tools.

Índice de contenido

INTRODUCCIÓN	1
CAPÍTULO I - TRAYECTORIA PROFESIONAL	2
1.1 Formación	2
1.2 Cursos	2
1.3 Experiencia Profesional	3
CAPÍTULO II - CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA	7
2.1 Empresa - Actividad Que Realiza	7
2.2 Visión	10
2.3 Misión	10
2.4 Organización De La Empresa	11
2.5 Área, Cargo Y Funciones Desempeñadas	12
2.6 Experiencia Profesional Realizada En La Organización	13
CAPÍTULO III - ACTIVIDADES DESARROLLADAS	14
3.1 Situación Problemática	14
3.1.1 Definición Del Problema	14
3.2 Solución	15
3.2.1 Objetivos	15
3.2.2 Alcance	15
3.2.3 Etapas Y Metodología	16
3.2.4 Fundamentos Utilizados	17
3.2.4.1 Soluciones de computación en la nube.	17
3.2.4.2 Amazon Web Services (AWS).	21
3.2.4.3 Plataforma de respuesta a incidentes de seguridad.	22
3.2.4.4 TheHive.	22
3.2.5 Implementación De Las Áreas, Procesos, Sistemas Y Buenas Prácticas	24
3.2.5.1 Creación de una máquina virtual.	24
3.2.5.2 Conexión a la máquina remota por medio del EC2.	32
3.2.5.3 Instalación del L.A.M.P.	35
3.2.5.4 Configurar el firewall UFW de Ubuntu 20.04 para la pila LAMP.	39
3.2.5.5 Configurar los componentes de la pila LAMP en Ubuntu 20.04.	40
3.2.5.6 Configuración de PHP.	41
3.2.5.7 Configuración de MariaDB.	43
3.2.5.8 Probar la pila LAMP.	45
3.2.5.9 Configuración e instalación de TheHive.	51
3.2.5.10 Instalar el entorno de tiempo de ejecución de Java	55

3.2.5.11 Instalación de Cassandra.	56
3.2.5.12 Instalar Elasticsearch.	62
3.2.5.13 Instalar TheHive.	63
3.2.5.14 Configurar TheHive y reiniciar.	65
3.3 Evaluación	69
3.3.1 Evaluación Económica / Evaluación Costo-Beneficio	69
3.3.2 Interpretación Del Van Y Del Tir	72
CAPÍTULO IV. REFLEXIÓN CRÍTICA DE LA EXPERIENCIA	75
CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES	76
5.1 Conclusiones	76
5.2 Recomendaciones	76
5.3 Fuentes De Información	77
5.4 Glosario	78

Índice de Figuras

1.	Organigrama de la Presidencia del Consejo de Ministros, 2021	11
2.	Arquitectura de la computación en nube	18
3.	Investigación de Eurostat en el uso de servicios de computación en la nube	19
4.	Clasificación utilizando las puntuaciones medias de todos los criterios.....	20
5.	Figura que muestra el porcentaje de confianza y servicios disponibles.....	21
6.	Flujo de trabajo de StorReduce.	22
7.	Servicios que brinda AWS.....	24
8.	Aparato EC2 de AWS.....	25
9.	Apartado donde se elige una imagen de Amazon Machine (AMI)	25
10.	Apartado donde se elige el tipo de instancia.	26
11.	Apartado donde muestra un resumen de las configuraciones elegidas.....	27
12.	Apartado donde podemos crear una key tipo RSA o ED25519	28
13.	Figura que muestra el lanzamiento de la instancia	29
14.	La imagen muestra el lanzamiento de la instancia.....	30
15.	La figura muestra la nueva instancia en el apartado de EC2	31
16.	La figura muestra el estado de la nueva instancia en el apartado de EC2	32
17.	La imagen recalca cómo ingresar al EC2 de AWS	32
18.	La imagen muestra la selección de una instancia y el botón para conectar a está.....	33
19.	Figura que muestra la conexión con una instancia.	34
20.	La figura muestra la conexión a una instancia.	34
21.	Figura que muestra el comando para actualizar ubuntu.	35
22.	La Figura muestra la instalación previa de algunas herramientas.....	36
23.	Instalación del repositorio.....	37
24.	Actualización de repositorios.....	38
25.	Instalación de PHP 7.4.....	38

26.	Comprobación del estado de servicios	39
27.	permitir el acceso de HTTP.....	39
28.	Permisos de acceso HTTPS	40
29.	Comando para ingresar al archivo de configuración de apache	40
30.	Ingresando directiva en la configuración de apache.	41
31.	Comando para recargar la configuración de apache.	41
32.	Ingresando a la configuración de PHP.	42
33.	Directiva de la zona horaria.....	42
34.	Comando para recargar la configuración.....	42
35.	Lanzamiento del cliente de mysql.	43
36.	Comando para cambiar la forma de autenticación.	43
37.	Registrando contraseña.	44
38.	Actualización de la tabla de privilegios.	44
39.	Comando para cerrar la conexión a la base de datos.....	44
40.	Creando Script en PHP para probar la pila LAMP.	45
41.	Script PHP.	45
42.	Propiedades de la instancia.	46
43.	Apartado de seguridad de una instancia.	46
44.	Reglas de entrada de la instancia.....	47
45.	Edición de reglas de entrada.....	48
46.	Ingresando las reglas de entrada HTTP y HTTPS.	49
47.	Ingresando a la dirección pública de la instancia por medio de un navegador web.....	50
48.	Ingresando al Script generada.	51
49.	Actualizamos todos los repositorios.....	52
50.	Gestionado la lista de claves APT.	52
51.	Agregando repositorio para Apache Cassandra.....	52
52.	Descargando key APT de elasticsearch.	53
53.	Pre-requisitos para elasticSearch.	53
54.	Pre-requisitos para TheHive.....	54
55.	Pre-requisitos para TheHive.....	54
56.	Actualización de todos los repositorios.....	54
57.	Instalación de JDK.....	55
58.	Configuración de JDK.....	55
59.	Configuración de JDK.....	56

60.	Instalación de Cassandra.....	56
61.	Instalación de net-tools.	56
62.	Configurando Cassandra con cqlsh.....	57
63.	Actualizando el nombre de cluster.....	57
64.	Saliendo del cqlsh.	58
65.	nodetool flush.	58
66.	Ingresando al yaml de Cassandra.	58
67.	Configuración para agregar al yaml de Cassandra.	58
68.	Cluster_name para yaml de Cassandra.	59
69.	listen_address para el yaml de Cassandra.....	59
70.	rpc_address para el yaml de Cassandra.	59
71.	Seed_provider para el yaml de Cassandra.	60
72.	Data_file_directories para el yaml de Cassandra.....	60
73.	Commitlog_directory para el yaml de Cassandra.....	60
74.	Saved_caches_directory para el yaml de Cassandra.	60
75.	Hints_directory para el yaml de Cassandra.....	61
76.	Reiniciar Cassandra.	61
77.	Habilitar Cassandra.....	61
78.	Instalar elasticsearch.....	62
79.	Iniciando elasticsearch.	62
80.	Habilitar elasticsearch.	62
81.	Probando el puerto 9200.....	63
82.	Instalando TheHive 4.....	63
83.	Comando de configuración de TheHive.....	64
84.	Comando de configuración de TheHive.....	64
85.	Comando de configuración de TheHive.....	64
86.	Comando de configuración de TheHive.....	65
87.	Ingresando al archivo de configuración de TheHive.	65
88.	Configuración para agregar a TheHive.....	65
89.	Agregar configuración a TheHive.....	66
90.	Agregar configuración a TheHive.....	67
91.	Inicializando TheHive.	67
92.	Habilitar TheHive.	67
93.	Configuración para elasticsearch.....	68
94.	Configuración de TheHive.....	68

95.	Probando el puerto 9000.....	68
96.	Ingresando a la IP pública de la instancia.	69
97.	Estimación de costos con calculadora de AWS	70
98.	Estimación de costos de almacenamiento.....	72
99.	Estimación de costos de almacenamiento.....	72
100.	Diagrama de Flujo del Proyecto	73

Índice de tablas

1. Formación académica	2
2. Estudios complementarios	2
3. Trayectoria profesional	3
4. Configuración para la instancia EC2.....	70
5. Configuración de almacenamiento.....	71
6. Inversión y Tasa de descuento	73
7. Cuadro de ingresos y egresos	73
8. Resultado del VAN y TIR	74

INTRODUCCIÓN

El Centro Nacional de Seguridad Digital gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la seguridad digital a nivel nacional como parte integral de la seguridad nacional para fortalecer la confianza digital.

Una de las funciones es actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas, técnicas de protección y defensa, para lo cual se utilizaba archivo excel compartido ya que no se tenía un software especializado para llevarlo a cabo, generando que no haya un adecuado control del registro de las incidencias tecnológicas además involucra un proceso complejo en dónde hay procedimientos que se tienen que realizar en un determinado tiempo, también existen una serie de indicadores de compromiso que nos van delimitando de qué tipo de incidente se trata, cuantos incidentes hay y quien lo está atendiendo.

Para solucionar este problema, se decidió realizar la implementación del software open source, TheHive (versión 4), el cual nos permite gestionar los registros de incidentes tecnológicos en una plataforma única centralizada y donde actúa un conjunto de usuarios que generan un *workflow* de los diferentes pasos que se dan, esto nos permite cumplir con los indicadores de compromisos. El trabajo contará con los siguientes capítulos:

- CAPÍTULO I, en este apartado se demuestra la experiencia adquirida.
- CAPÍTULO II, se describe el contexto en el que se desarrolló la experiencia, además de todo lo relacionado a la empresa, así como la experiencia profesional realizada en la organización.
- CAPÍTULO III, se especifica las funciones ejecutadas en el trabajo realizado, como la problemática, metodología, objetivos y resultados de la solución propuesta.
- CAPÍTULO IV, se declara la reflexión crítica sobre la experiencia y el aporte del presente trabajo, los puntos críticos que se atendieron, experiencia y la formación necesaria.
- CAPÍTULO V, se define las conclusiones y recomendaciones del autor en el presente trabajo.

CAPÍTULO I - TRAYECTORIA PROFESIONAL

1.1 Formación

Tabla 1

Formación académica

Grado académico	Especialidad	Fecha del grado académico	Institución
Bachillerato	Ingeniería de sistemas	04/12/2017	UNMSM
Técnico	Computación e informática	09/02/2007	Instituto Superior Tecnológico público Argentina

Nota: Estudios superiores culminados, 2022

1.2 Cursos

Tabla 2

Estudios complementarios

Concepto	Especialidad	Institución	Estudios Realizados
-----------------	---------------------	--------------------	----------------------------

Idiomas	Inglés	Británico	02/08/2017
Informática	Curso básico de informática	UNMSM	07/2010
Informática	Soluciones de negocio con Microsoft Excel	UNMSM	01/2011
Informática	Oracle	Banco de la nación	01/2017
Informática	Java 8.0 Web Developer	Cibertec	08/2017
Informática	Agile Fundamentals	Cibertec	03/2018
Informática	API Owner	Api Additcs Perú	02/2020

Nota: Estudios complementarios, 2022

1.3 Experiencia Profesional

Tabla 3

Trayectoria profesional

No.	Nombre de la Entidad o Empresa
1	Banco de la Nación Prácticas Pre - profesionales Sección de operaciones y control de plataformas • Elaboración y ejecución de query en Oracle 10g, 11g. • Apoyo en revisión de código de aplicaciones java antes de ser subido a producción. • BMC Impact Explorer para el monitoreo de enlaces operativos. • BMC Control-M, Control-M Enterprise Manager, carga de trabajo de aplicaciones por lote. • BMC Patrol Central, para monitorear el comportamiento de Servidores was.

-
- IBM Personal Communications (consola de administración de los diversos procesos que se ejecutan en el MAINFRAME), para ver las conexiones con entidades como PNP, RENIEC, SUNAT, Claro, Movistar, Entel para el pago de sus servicios.
 - Secure Shell Client, para revisar las conexiones con Visa y Mastercard
 - PC Edit Package 4.0, realizar proceso de Incoming, Visanet.
 - Internet Information Services (IIS), para el mantenimiento de aplicaciones internas del banco.
 - WebSphere Integrated Solutions Console, IBM (Administration, gestión, pases a producción de aplicativos creados por banco).
 - Sistema de control de circuitos digitales, administración de los circuitos e interconexiones del banco, conexiones internas (agencias, oficinas especiales, cajeros) y externas (Sedapal, Reniec, PNP, Sunat, claro, movistar, Entel, Bitel).
 - Manejo de Linux red had a nivel básico.
 - Windows Server 2003 R2 a nivel básico.
-

2 Banco de la Nación

Prácticas Profesionales

Sección de operaciones y control de plataformas

- Elaboración y ejecución de query en Oracle 10g, 11g.
- Apoyo en revisión de código de aplicaciones java antes de ser subido a producción.
- BMC Impact Explorer para el monitoreo de enlaces operativos.
- BMC Control-M, Control-M Enterprise Manager, carga de trabajo de aplicaciones por lote.
- BMC Patrol Central, para monitorear el comportamiento de Servidores was.
- IBM Personal Communications (consola de administración de los diversos procesos que se ejecutan en el MAINFRAME), para ver las conexiones con entidades como PNP, RENIEC, SUNAT, Claro, Movistar, Entel para el pago de sus servicios.
- Secure Shell Client, para revisar las conexiones con Visa y Mastercard
- PC Edit Package 4.0, realizar proceso de Incoming, Visanet.
- Internet Information Services (IIS), para el mantenimiento de aplicaciones internas del banco.

Del
21/09/2017
Hasta
20/09/2018

	• WebSphere Integrated Solutions Console, IBM (Administration, gestión, pases a producción de aplicativos creados por banco). • Sistema de control de circuitos digitales, administración de los circuitos e interconexiones del banco, conexiones internas (agencias, oficinas especiales, cajeros) y externas (Sedapal, Reniec, PNP, Sunat, claro, movistar, Entel, Bitel). • Manejo de Linux red had a nivel básico. • Windows Server 2003 R2 a nivel básico.	
3	Everis Perú S.A. Solutions Assistant Cliente: Banco de Crédito del Perú (BCP) Desempeño como desarrollador de aplicaciones backend. • Pruebas automatizadas con Selenium. • Desarrollo en Java Yape en Banca móvil BCP • Desarrollo de APIS con RxJava (Nueva Banca móvil BCP, Login). • Desarrollo de request para Lynx BCP (Motor de detección de fraudes) para transferencias monetarias y no monetarias. • Spring Boot • Spring Security	Del 04/02/2019 Hasta 31/03/2021
4	Entelgy Perú Analista Programador Cliente: Banco BBVA Perú Desempeño en el área de Arquitectura APX • Encargado de guiar, apoyar y supervisar los proyectos en el uso correcto de la arquitectura APX desde la etapa de diseño, desarrollo y despliegue en producción según el flujo E2E de la arquitectura APX; proyectos a cargo: ○ GEMA Productos PNN - My Business ○ Andes & Third party wallets ○ GEMA Productos PNN 2.0 ○ Digitalización Notificaciones push Transaccional ○ GEMA Productos PNN - Seguros Multirriesgo ○ GEMA: Productos PNN 3.0 ○ Mejoras en Procesos digitales ○ Real Time Offer Manager con NBO ○ Motor de Notificaciones 2.0 ○ Digital Client Acquisition 2.0 ○ Plataforma de Firma Digital	Del 24/03/2021 Hasta la actualidad
5	PCM	Del

Analista de Seguridad Digital	22/02/2022
Subsecretaría de Tecnologías y seguridad digital.	Hasta
• Análisis de soluciones en nube. • Implementación de la plataforma TheHive para el Centro Nacional De Seguridad Digital. • Migración de plataforma Moodle del Centro De Conocimiento Digital para el Centro Nacional De Seguridad Digital.	31/05/2022

Nota: Trayectoria profesional, 2022

CAPÍTULO II - CONTEXTO EN EL QUE SE DESARROLLA LA EXPERIENCIA

2.1 Empresa - Actividad Que Realiza

La Presidencia del Consejo de Ministros es un organismo del Poder Ejecutivo, con personería jurídica de derecho público y constituye pliego presupuestal.

La Presidencia del Consejo de Ministros ejerce sus funciones a nivel nacional en el marco de sus competencias. Tiene su domicilio legal en la provincia y ciudad de Lima.

La Presidencia del Consejo de Ministros ejerce sus competencias a nivel nacional en las siguientes materias: Modernización de la Gestión Pública, Ética Pública, Integridad y lucha contra la corrupción, Desarrollo Territorial, Descentralización, Demarcación Territorial, Diálogo y Concertación Social, Transformación Digital, Comunicación de las acciones del Poder Ejecutivo, así como la coordinación de las políticas nacionales de carácter sectorial y multisectorial del Poder Ejecutivo y la coordinación de las relaciones con los demás Poderes del Estado, los organismos constitucionales autónomos, los gobiernos regionales, los gobiernos locales, y la sociedad civil, y las demás competencias que le asigne la ley.

Es rector del Sistema Administrativo de Modernización de la Gestión Pública, Sistema Nacional de Gestión del Riesgo de Desastres, Sistema Nacional de

Transformación Digital y Sistema Nacional de Demarcación Territorial. Constituye la más alta autoridad técnico - normativa sobre dichas materias.

Ejecuta sus competencias mediante la realización de sus labores, teniendo en cuenta el punto de vista de los derechos humanos, género, discapacidad, intercultural, entre otros, guiadas para que los resultados tengan un impacto en el confort de la ciudadanía y el avance nacional.

La Presidencia del Consejo de Ministros tiene las siguientes funciones:

- a) Proporcionar soporte al/a la Presidente/a del Consejo de Ministros en la realización de las facultades y tareas asignadas por la Constitución Política del Perú y la Ley.
- b) Realizar los acuerdos con los otros Poderes del Estado, sociedad civil, organismos constitucionales autónomos, gobiernos regionales y locales, concretando prioridades para asegurar los objetivos de interés del país.
- c) Proponer, constituir, planificar, guiar, organizar, realizar, inspeccionar y evaluar las políticas nacionales y sectoriales en razón de su competencia, responsabilizando la rectoría respecto de ellas, en los asuntos que incumbe.
- d) Autorizar las disposiciones normativas que le compete; como realizar y hacer cumplir el marco normativo vinculado con su ámbito de competencia ejecutando la potestad sancionadora que le compete.
- e) Ejecutar seguimiento al desempeño y resultados obtenidos en el país, en el ejercicio de sus competencias, y tomar las decisiones oportunas para agilizar los resultados deseados.
- f) Realizar la rectoría de los sistemas; y establecer la normativa y procedimientos vinculados con estos sistemas, coordinar su acción técnica y vigilar su correcto funcionamiento.

- g) Organizar, guiar, inspeccionar y evaluar los procesos para modernizar la administración pública y del Estado, ética pública, integridad y lucha de anticorrupción, evolución digital, avance territorial, descentralización, diálogo, acuerdos sociales y delimitación territorial.
- h) Establecer normas, aconsejar, inspeccionar e investigar a las entidades públicas en razón de simplificación administrativa, así como fomentar la calidad de las regulaciones que difunde la administración pública, en el entorno de su competencia.
- i) Liderar, impulsar y cooperar en los procesos de diálogo y concertación con la sociedad.
- j) Apoyar al/a la Presidente/a del Consejo de Ministros para guiar al Consejo de Ministros, Comisión Interministerial de Asuntos Económicos y Financieros - CIAEF, Comisión Interministerial de Asuntos Sociales - CIAS y del Consejo de Coordinación Intergubernamental - CCI.
- k) Vigilar el desenvolvimiento de las políticas aprobadas por el Foro del Acuerdo Nacional.
- l) Apoyar a las Comisiones en las que interviene la Presidencia del Consejo de Ministros.
- m) Planificar la defensa judicial de la Presidencia del Consejo de Ministros y de los organismos públicos asignados y entidades públicas asociadas al sector.
- n) Solucionar las disputas de debate entre los organismos del Poder Ejecutivo.
- o) Otras que se decretan por Ley. Igualmente, la Presidencia del Consejo de Ministros colabora al/a la Presidente/a de la República en la administración de la política global de gobierno, a través de:
 - El seguimiento a la realización de las prioridades de gobierno.

- Administración de la planificación de comunicación de las políticas del Poder Ejecutivo.
- Dirigir del plan de diálogo con las diversas entidades de la sociedad.
- Guiar los nexos entre el Poder Ejecutivo y el Poder Legislativo.
- Mediar las participaciones del Poder Ejecutivo entre las entidades públicas del gobierno nacional con los gobiernos locales y regionales.
- Promover una ética pública y cultura de integridad.

2.2 Visión

La PCM lidera un estado moderno, eficiente, transparente, descentralizado, con menor desigualdad social y económica, impulsando políticas nacionales para el desarrollo sostenible en los tres niveles de gobierno.

2.3 Misión

Nuestra misión es mantener las relaciones con los demás poderes del Estado con el fin de construir un país moderno, articulado y descentralizado, sobre la base del logro de las metas nacionales y en el marco de la Política General del Gobierno.

2.4 Organización De La Empresa

El Centro Nacional de Seguridad Digital (CNSD) se crea a través del Decreto de Urgencia N° 007-2020 y es parte del Subsecretaría de tecnologías y seguridad Nacional y a la vez está esta es un sub área de la secretaría de Gobierno y Transformación digital que pertenece a la secretaría general de la Presidencia del Consejo de Ministros.

Figura 1

Organigrama de la Presidencia del Consejo de Ministros, 2021



El presente trabajo se desarrolló en la Subsecretaría de Tecnologías y seguridad digital para el Centro Nacional de Seguridad Digital (CNSD), desempeñando el cargo de Analista de Seguridad Digital realizando las siguientes funciones:

- 12

- Migración de plataforma Moodle del Centro De Conocimiento Digital para el Centro Nacional De Seguridad Digital.

2.6 Experiencia Profesional Realizada En La Organización

1. Evaluación y migración de sistemas de información a AWS.
2. Implementación de nuevas herramientas informáticas en AWS.
3. Configuración de herramientas informáticas en AWS.

CAPÍTULO III - ACTIVIDADES DESARROLLADAS

3.1 Situación Problemática

Los incidentes (ataques) de seguridad digital de entidades públicas o empresas privadas son reportados al El Centro Nacional de Seguridad Digital del Perú mediante llamada telefónica, correo o del formulario que se encuentra en la página de la entidad, estos incidentes eran anotados en un archivo Excel que se compartía con los Analistas de seguridad para su revisión.

3.1.1 Definición Del Problema

La ausencia del registro de incidentes de seguridad digital en una plataforma especializada, causando:

- Que no exista un adecuado registro de incidencias de seguridad digital.
- Que no se dé un control y monitoreo adecuado de los incidentes registrados.
- Que no se determine una clasificación del incidente.

3.2 Solución

3.2.1 Objetivos

Objetivo general:

- Implementar un sistema para la gestión de registro de incidentes de seguridad digital del Centro Nacional de Seguridad Digital del Perú.

Objetivos específicos:

- Realizar un seguimiento del ciclo de vida de los incidentes tecnológicos registrados.
- Clasificar los incidentes de acuerdo a su nivel de criticidad.

3.2.2 Alcance

La implementación de la plataforma TheHive conlleva los siguientes pasos:

- Se investigó las posibles soluciones en nube y que servicios nos brinda cada una.
- Se seleccionó la solución en nube AWS que brinda mayor beneficio al área.
- Se investigó soluciones open source para la gestión de incidencias indicando los beneficios más resaltantes de cada uno.

- Se seleccionó la plataforma TheHive la cual calza con las necesidades de los incidentes reportados al CNSD.
- Se implementó y configuro la plataforma TheHive en una cuenta de prueba para validar si cumple con los requerimientos solicitados, así como también se realizó pruebas de esfuerzo, seguridad y confiabilidad.
- Se realizó un informe con las pruebas realizadas.
- Se dimensionaron los requisitos necesarios de la aplicación para la puesta en marcha en producción.
- Se implementó y configuro la plataforma TheHive en la cuenta AWS de producción.
- Se realizó la documentación de capacitación.
- Se capacito sobre el uso de la plataforma a los usuarios.

3.2.3 Etapas Y Metodología

Se utilizó la metodología Scrum generando reuniones diarias donde se indica lo que se hizo un día antes y lo que se realizará el día presente (hoy), los spring tiene una duración de dos semanas, hay reuniones de retrospectiva, así como reuniones de planning finalizando los spring.

Las etapas para la implementación de TheHive fueron las siguientes:

- Creación de una máquina virtual.
- Conexión a la máquina remota por medio del EC2.
- Instalación del L.A.M.P.

- Configurar el firewall UFW de Ubuntu 20.04 para la pila LAMP.
- Configurar los componentes de la pila LAMP en Ubuntu 20.04.
- Configuración de PHP.
- Configuración de MariaDB.
- Probar la pila LAMP.
- Pre-requisitos para la instalación TheHive.
- Instalar el entorno de tiempo de ejecución de Java
- Instalación de Cassandra.
- Instalar Elasticsearch.
- Instalar TheHive.
- Configurar TheHive y reiniciar.

3.2.4 Fundamentos Utilizados

Para la elaboración del presente trabajo se usaron conceptos de solución de computación en la nube, Amazon Web Services, Plataformas de respuestas de respuesta a incidente de seguridad, TheHive; a continuación, se presenta los conceptos e investigaciones utilizados:

3.2.4.1 Soluciones de computación en la nube.

Una de las ventajas esenciales de las soluciones en la nube es que los usuarios y empresas pueden obtener y acceder a sus datos desde distintas ubicaciones

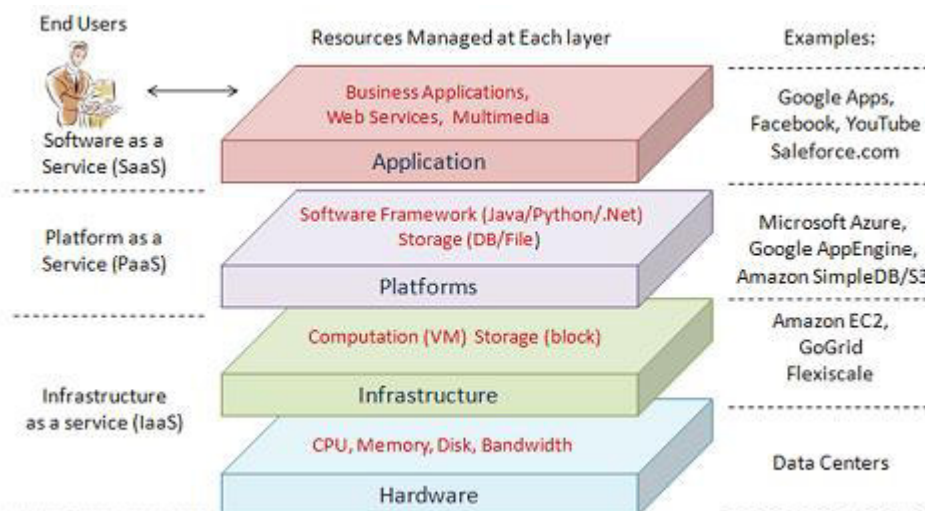
de los dispositivos. El almacenamiento en la nube tiene una serie de características, como la **disponibilidad** (los datos están siempre disponibles desde diferentes dispositivos, como ordenadores y teléfonos móviles), la **durabilidad** (los datos están protegidos contra las caídas) y el **rendimiento** (se puede acceder a los datos en el momento oportuno).

Existen tres tipos de modelos de servicios en la nube (Figura N°2):

- a) **Software como servicio** (SaaS), por ejemplo, Gmail, en el que el software suministrado es utilizado por los usuarios.
- b) **Plataforma como servicio** (PaaS), en la que las aplicaciones se implementan en la administración de la nube mediante la personalización del cliente.
- c) **Infraestructura como servicio** (IaaS), en la que los usuarios hábiles ejecutan sus programas para aprovechar al máximo la capacidad de computación disponible y es a este tipo de servicio en nube la cual se eligió debido que elegirá un software open source que ya está desarrollado, pero previamente hay que realizar configuraciones para la implementarlo.

Figura 2

Arquitectura de la computación en nube



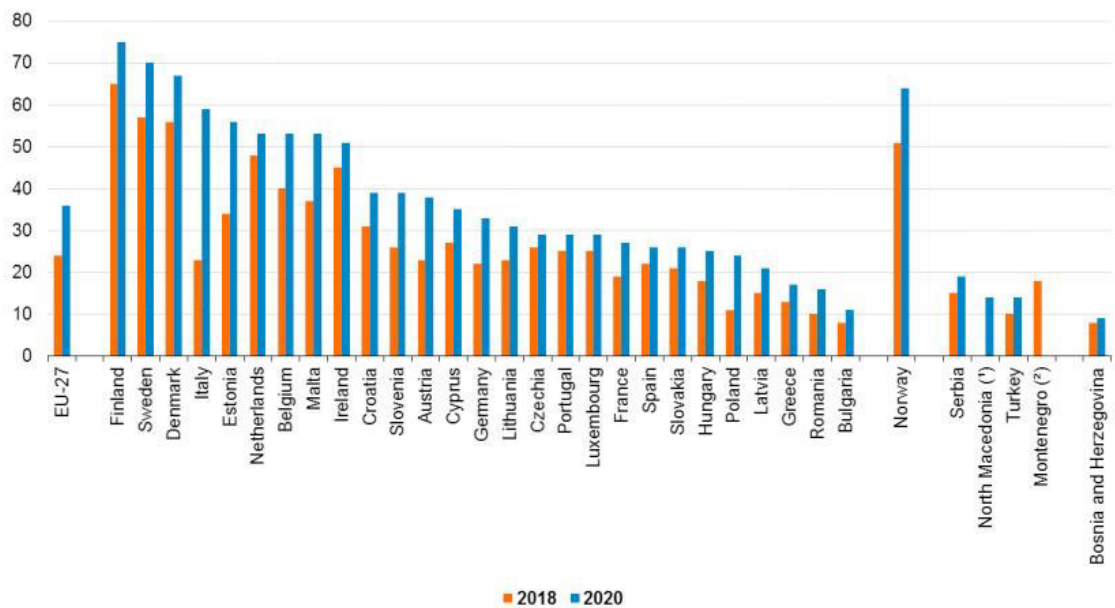
Nota: Recursos gestionados en cada nivel de una solución en nube.

Según la investigación de Eurostat, el uso de servicios de computación en la nube en toda la UE aumentó entre 2018 y 2020 del 24% al 36% de las empresas (Figura N°3). En el mismo período, Polonia registró una dinámica de crecimiento aún mayor, del 11% al 24% de las empresas. Plantea nuevos problemas a los gestores que deben tomar decisiones sin ser plenamente conscientes de los criterios que deben tenerse en cuenta.

Figura 3

Investigación de Eurostat en el uso de servicios de computación en la nube

Use of cloud computing services, 2018 and 2020
(% of enterprises)



(*) North Macedonia: 2018 not available

(*) Montenegro: 2020 unreliable

Note: Iceland: data not available

Source: Eurostat (online data code: isoc_cicce_use)

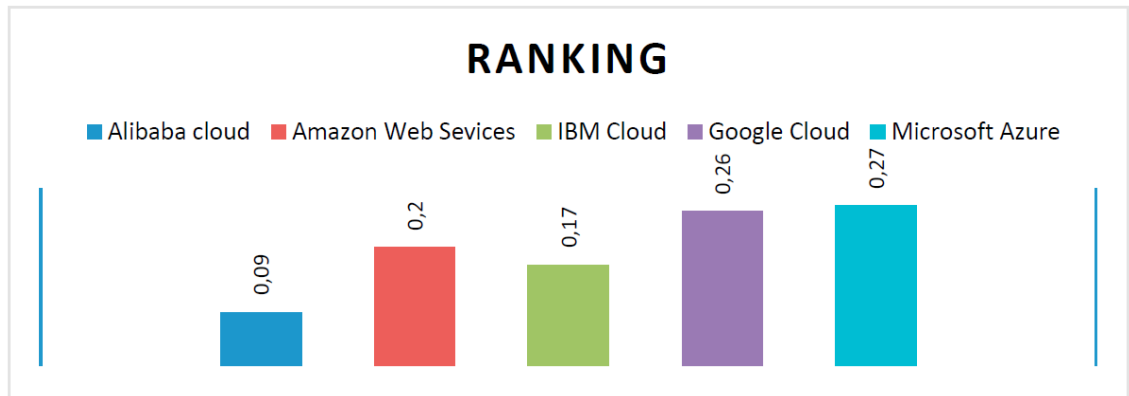
eurostat

Nota: Gráfico que representa el uso de la computación en nube en la Unión Europea desde el 2018 al 2020

Basándose en el artículo “The use of the multi-criteria AHP method to select a cloud computing provider” se observa que Amazon Web Service presenta un porcentaje favorable (Figura N° 4) para su elección como solución en la nube. En este artículo se realizó un estudio de 5 proveedores de soluciones cloud basado en la confiabilidad y número de servidores disponibles (Figura N°5).

Figura 4

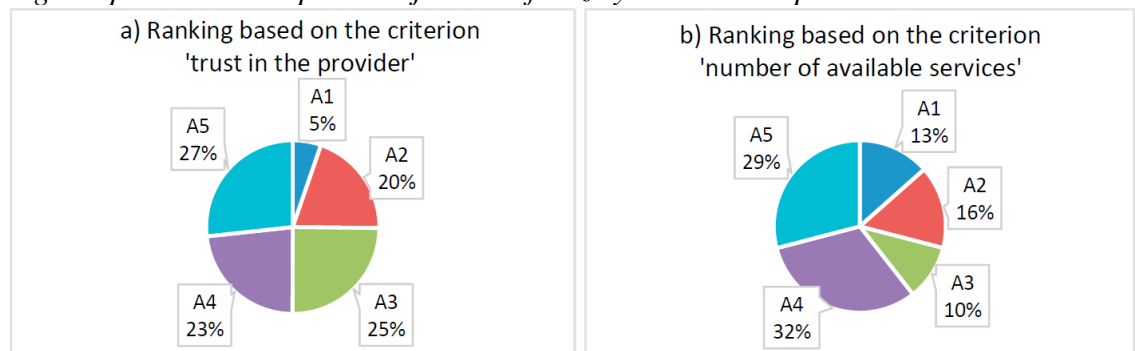
Clasificación utilizando las puntuaciones medias de todos los criterios.



Nota: Figura que muestra el porcentaje de demanda de 5 proveedores de soluciones Cloud en la UE entre el 2018 y el 2020.

Figura 5

Figura que muestra el porcentaje de confianza y servicios disponibles.



Nota: Clasificación basada en los criterios seleccionados: a) "confianza en el proveedor" y b) "número de servicios disponibles" de 5 proveedores de soluciones cloud en la UE entre el 2018 y el 2020.

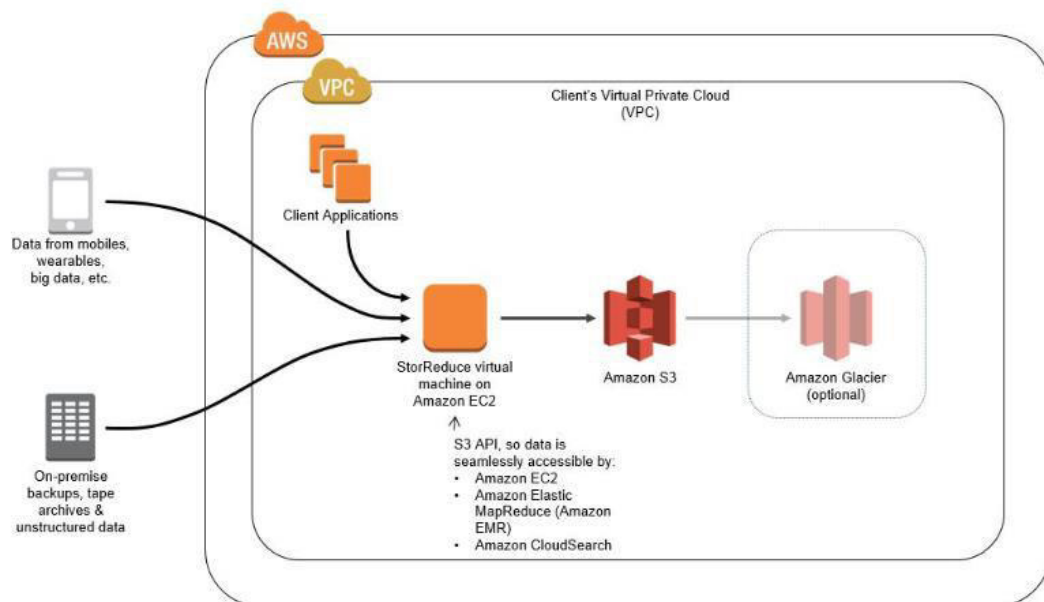
3.2.4.2 Amazon Web Services (AWS).

Es un conjunto de servicios de computación en la nube, según el artículo “Benefits of AWS in Modern Cloud” AWS ofrece múltiples opciones de almacenamiento, como **Amazon Glacier** que es un almacenamiento a largo plazo muy seguro y duradero, **Amazon S3** que es para almacenar los archivos estándar que son seguros, duraderos y escalables, **Amazon EC2 Instance Storage** que ofrece almacenamiento temporal a nivel de bloque para

las instancias, tal como se detalla en la Figura N°6. Una **instancia EC2** de AWS proporciona una capacidad informática escalable que elimina la necesidad de que una empresa, especialmente las que están empezando, invierta en dispositivos de hardware por adelantado. También viene con imágenes de máquina que empaquetan todo lo necesario para un servidor, incluido el sistema operativo. Varias imágenes de máquina ahora también incluyen marcos de aprendizaje profundo como Caffe y Mxnet. Se pueden configurar otros parámetros como la CPU, la memoria y la capacidad de la red. La tarea de anotación es una de las partes vitales para hacer innovaciones que impliquen inteligencia artificial.

Figura 6

Flujo de trabajo de StorReduce.



Nota: Estructura de la nube privada virtual del cliente

3.2.4.3 Plataforma de respuesta a incidentes de seguridad.

Las organizaciones quieren minimizar los riesgos de seguridad causados por adversarios como hackers, actores estatales u organizaciones criminales. En

2019, el 88% de las organizaciones se enfrentaron al spear phishing mientras que entre 2005 y 2020 se han registrado más de 10.000 violaciones de datos notificadas públicamente. Debido a esto, las organizaciones empresariales están adquiriendo plataformas comerciales de gestión de incidentes de seguridad (SIR), de información y eventos de seguridad (SIEM) y de orquestación, automatización y respuesta de seguridad (SOAR). Con estas plataformas las organizaciones aumentan el control, la visibilidad y el tiempo de respuesta más rápido para su dominio de seguridad. La mayoría de estas plataformas son de código cerrado ya que se comercializan.

3.2.4.4 *TheHive.*

Es una plataforma no comercializada de respuesta a incidentes de seguridad (SIR) de código abierto lanzada en 2016. El proyecto afirma ser una plataforma diseñada para facilitar la vida de los SOC, CSIRT, CERT e InfoSec al permitir un flujo de trabajo centralizado y organizado. TheHive permite crear fácilmente tareas para los miembros del equipo y una ubicación central para mostrar y cruzar los hallazgos. También afirma ser capaz de integrarse con MISP, para garantizar las investigaciones de los eventos de MISP, y Cortex, para analizar fácilmente los observables. Por otro lado, surgen nuevos proyectos que pretenden integrarse con TheHive para garantizar la automatización, como Shuffle SOAR. Si se combinan todos estos hechos, TheHive Project puede considerarse un posible sustituto de las costosas plataformas SIR o una alternativa a las plataformas SIEM y SOAR.

En el artículo “TheHive Project: The maturity of an open-source Security Incident Response platform” se realiza una investigación para determinar el grado de madurez de TheHive como plataforma de respuesta a incidentes de seguridad (SIRP) open source en el cual se ven cinco puntos principales del marco ad-hoc son: Gestión de casos y flujo de trabajo, Diario y apoyo probatorio, Inteligencia de amenazas y análisis de rutas de ataque, Generación automática de incidentes, Análisis y apoyo forense; los resultados muestran que tres de los escenarios satisfacen los requisitos del marco ad hoc, mientras que los dos restantes revelan pequeños defectos. El primer defecto es la falta de una conservación elaborada y segura de las

pruebas por defecto, La segunda falla que se descubrió, fue la falta de soporte forense.

3.2.5 Implementación De Las Áreas, Procesos, Sistemas Y Buenas Prácticas

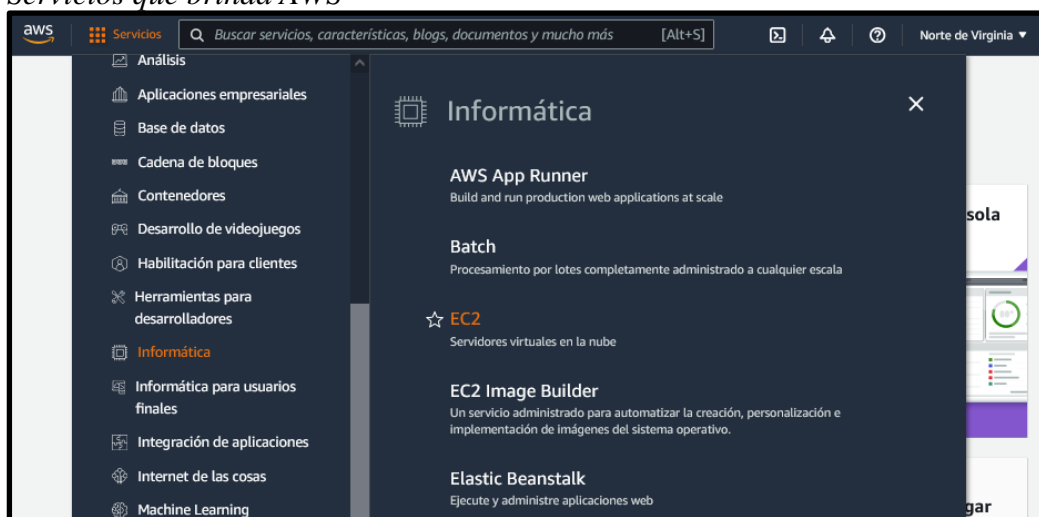
Lo primero a realizar es la creación e instancia de la máquina virtual en AWS con EC2 en la cuenta de prueba, después se procede con la instalación y configuración de los pre-requisitos de TheHive, finalmente se ejecuta la instalación y configuración de TheHive, la diferentes configuraciones e instalaciones se realizan según lo indicado en la documentación oficial de TheHive en su versión 4.x, adicionalmente se elaboró un informe con todos estos procedimientos.

3.2.5.1 Creación de una máquina virtual.

Para la creación de máquinas virtuales vamos a servicios, informática y finalmente EC2

Figura 7

Servicios que brinda AWS

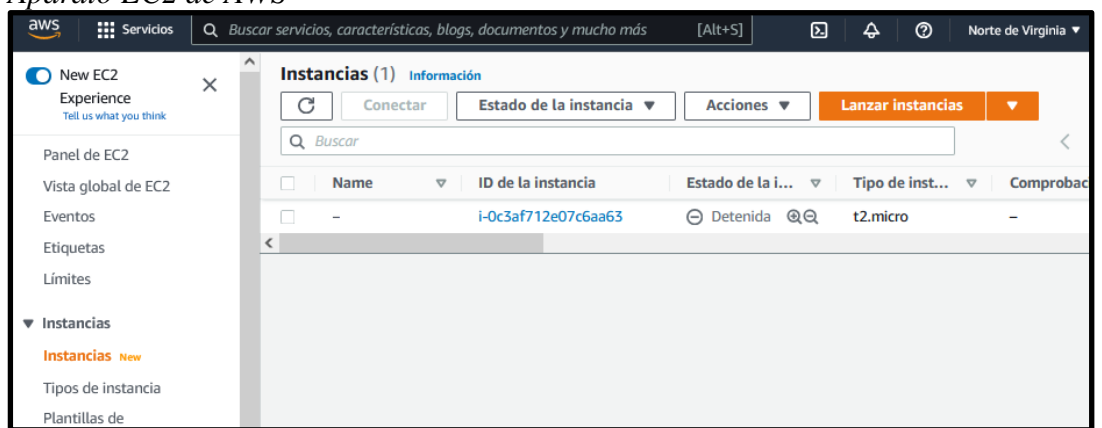


Nota: La imagen muestra como entrar al apartado EC2 de AWS

Nos saldrá la siguiente ventana en la cual seleccionamos instancias y después lanzar instancias:

Figura 8

Aparato EC2 de AWS

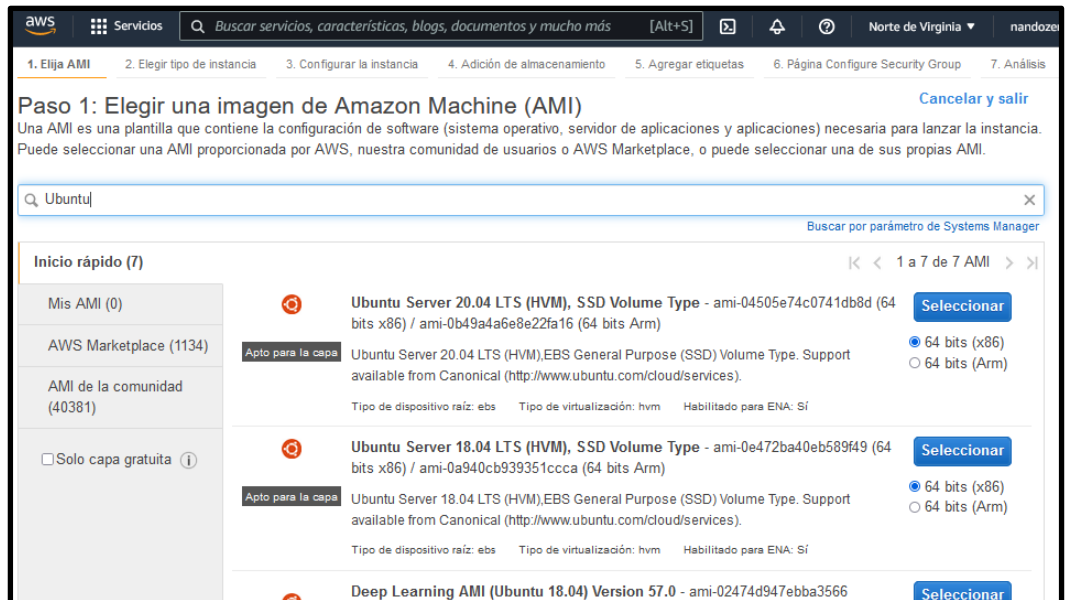


Nota: La figura muestra las diferentes opciones de EC2

En la siguiente buscamos ubuntu y seleccionamos Ubuntu server 20

Figura 9

Apartado donde se elige una imagen de Amazon Machine (AMI)

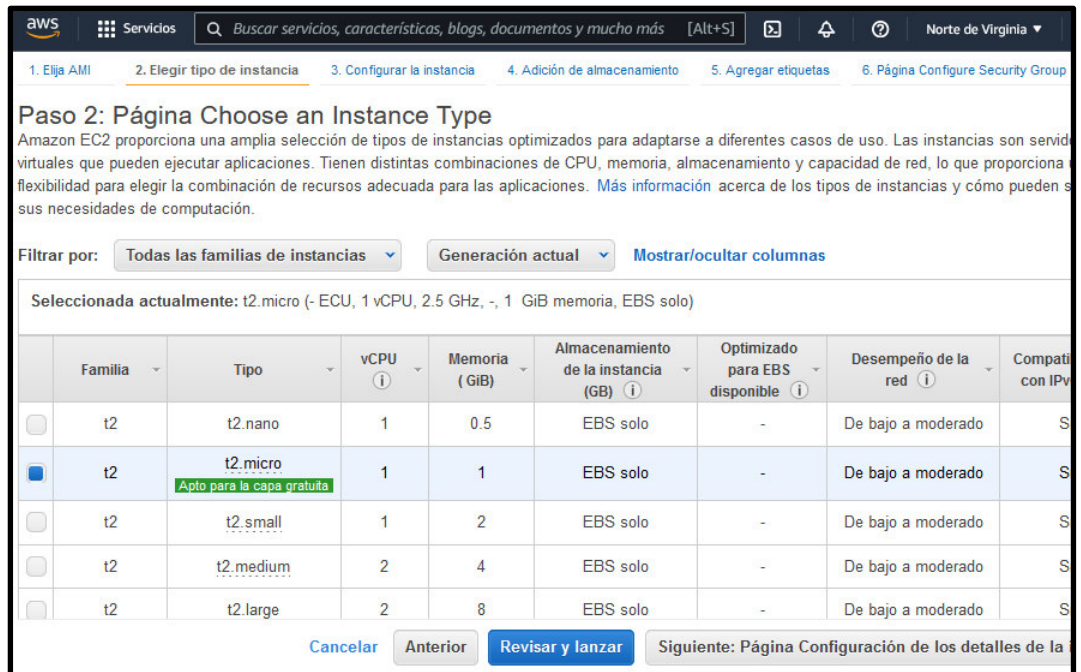


Nota: La figura muestra diferente AMI tanto de paga en el Marketplace como gratuitos hechos por la comunidad.

Seleccionamos la máquina virtual que va acorde a lo que necesitamos y le damos en revisar y lanzar

Figura 10

Apartado donde se elige el tipo de instancia.

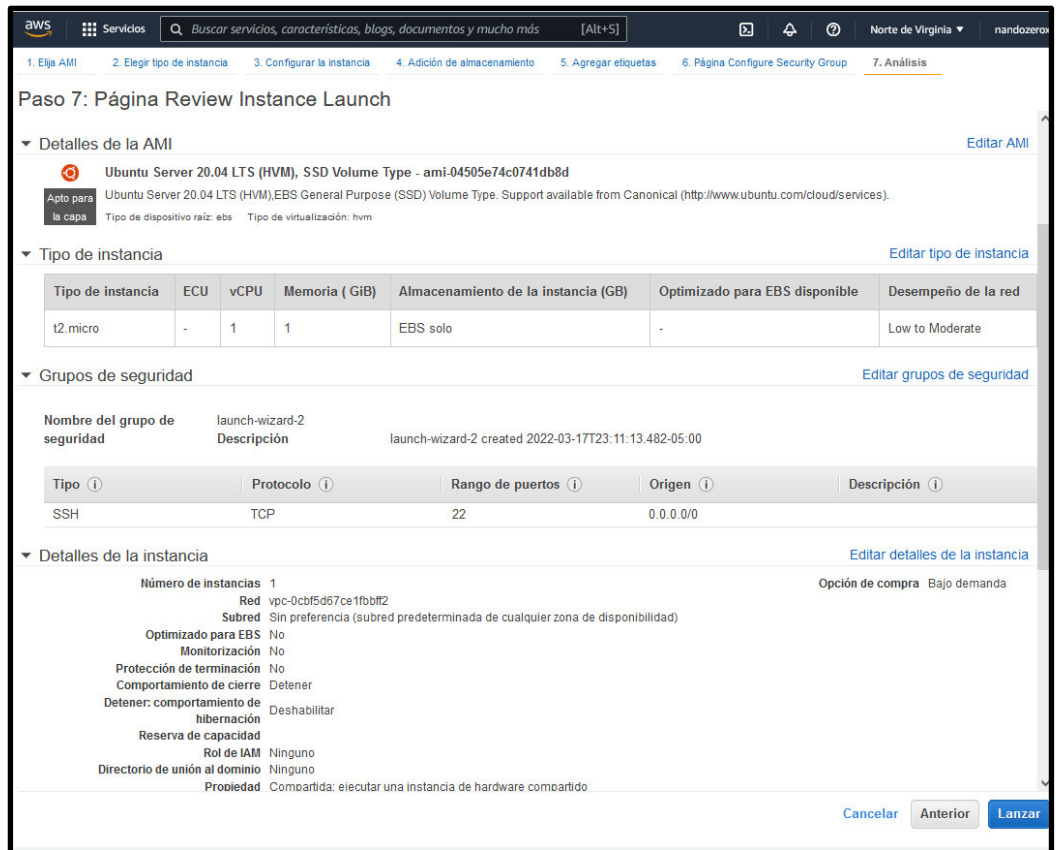


Nota: Figura que nos muestra la elección de las diferentes configuraciones de una máquina virtual.

Nos saldrá el detalle de la configuración de la máquina virtual, le damos en lazar

Figura 11

Apartado donde muestra un resumen de las configuraciones elegidas.

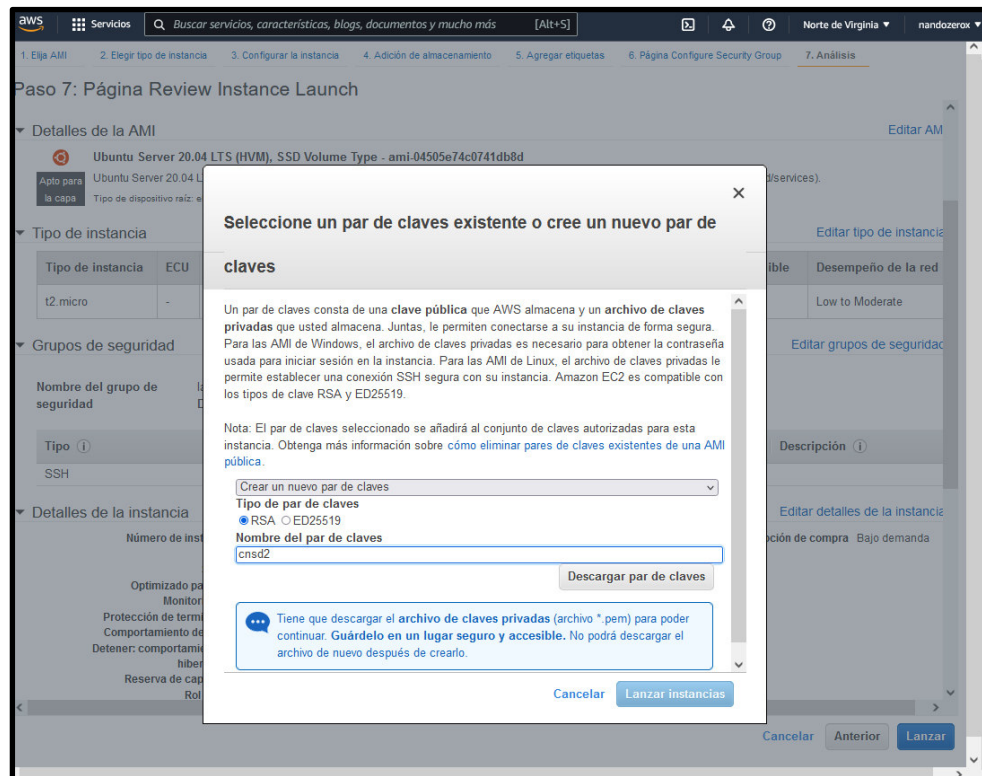


Nota: En este apartado podemos confirmar las configuraciones elegidas.

Seleccionamos crear un nuevo par de claves del tipo RSA, le asignamos un nombre y le damos en descargar par de claves:

Figura 12

Apartado donde podemos crear una key tipo RSA o ED25519

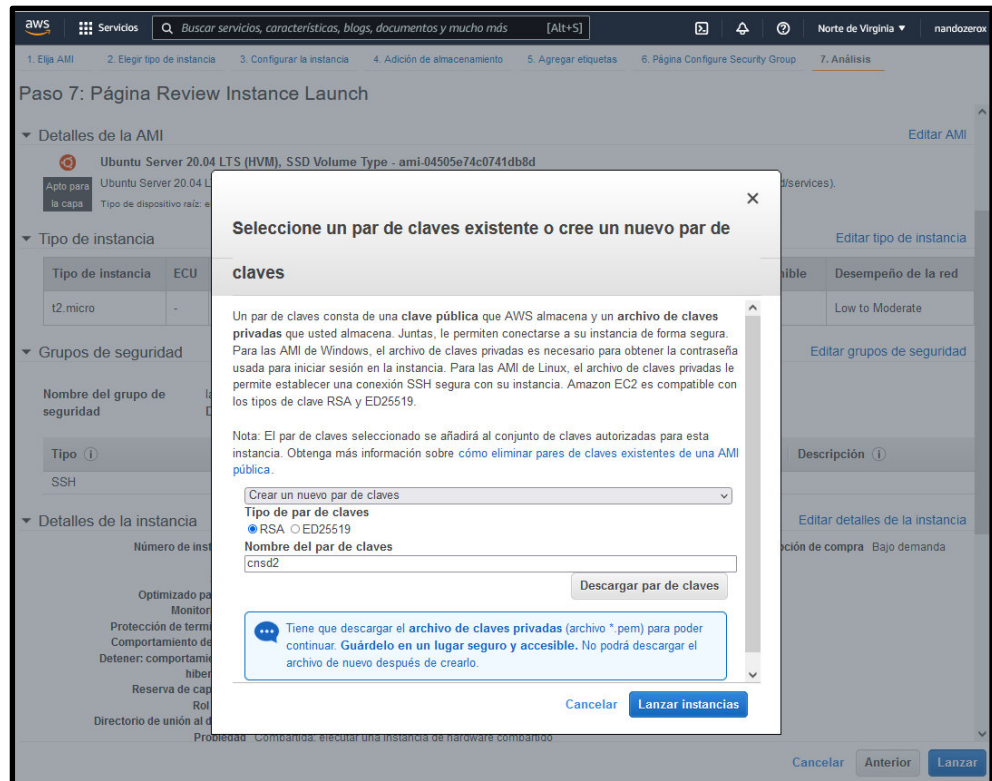


Nota: Aquí podemos descargar las key para conectarnos remotamente a la máquina virtual por SSH

Después de ellos se habilita el botón lanzar instancia y damos click sobre ella.

Figura 13

Figura que muestra el lanzamiento de la instancia



Nota: Una vez descargada la key podemos lanzar la instancia.

Nos saldrá una ventana con la confirmación del lanzamiento de la instancia:

Figura 14

La imagen muestra el lanzamiento de la instancia

Página Launch Status

Se está lanzando su instancia
 Se ha iniciado el siguiente lanzamiento de instancia: [i-0239707afbd4d435](#) [Ver log de lanzamiento](#)

Recibir notificaciones de los cargos estimados
[Crear alertas de facturación](#) para obtener una notificación por correo electrónico cuando los cargos estimados de su factura de AWS superen el importe definido (por ejemplo, cuando se excede la capa de uso gratuita).

Cómo conectarse a la instancia

Se está lanzando su instancia. Pueden transcurrir unos minutos hasta que tenga el estado **en ejecución**, momento en el cual estará lista para poder usarla. Las horas de uso de la nueva instancia comenzarán inmediatamente y seguirán devengando gastos hasta que detenga o termine la instancia.

Haga clic en [Ver las instancias](#) para monitorizar el estado de su instancia. Cuando la instancia tenga el estado **en ejecución**, podrá [conectarse](#) a ella desde la pantalla Instancias. [Más información](#) cómo conectarse a la instancia.

▼ Aquí tiene algunos recursos útiles que le ayudarán a comenzar

- [Cómo conectarse a la instancia Linux](#)
- [Amazon EC2: Guía del usuario](#)
- [Más información sobre la capa de uso gratuita de AWS](#)
- [Amazon EC2: Foro de debate](#)

Mientras se están lanzando sus instancias, también puede

- [Crear alarmas de comprobación de estado](#) recibir notificaciones cuando estas instancias no superen las comprobaciones de estado. (Podrían aplicarse cargos adicionales)
- [Crear y asociar volúmenes de EBS adicionales](#) (Podrían aplicarse cargos adicionales)
- [Administrar grupos de seguridad](#)

Ver instancias

Nota: La figura muestra los detalles del lanzamiento de la instancia.

Le damos en ver instancias y nos aparecerá las instancias creadas:

Figura 15

La figura muestra la nueva instancia en el apartado de EC2

The screenshot shows the AWS Management Console interface for EC2 Instances. The left sidebar contains navigation links for 'New EC2 Experience', 'Panel de EC2', 'Vista global de EC2', 'Eventos', 'Etiquetas', 'Límites', and 'Instancias'. The main content area is titled 'Instancias (2)' and includes a search bar, a filter for 'Estado de la instancia (cliente) != running', and a table of instances.

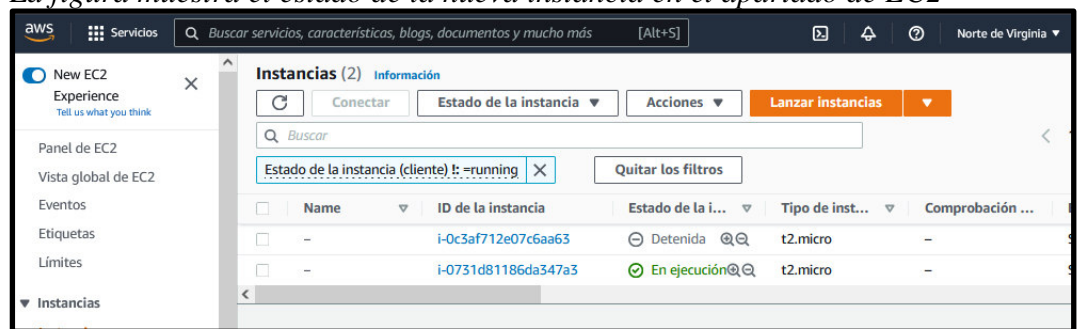
	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Es
☐	-	i-0c3af712e07c6aa63	Detenida	t2.micro	-	Si
☐	-	i-0731d81186da347a3	Pendiente	t2.micro	-	Si

Nota: Aquí veremos si las instancias están en ejecución o están detenidas.

Aquí tenemos que esperar unos minutos ya que la instancia comenzará en pendiente y pasará en ejecución:

Figura 16

La figura muestra el estado de la nueva instancia en el apartado de EC2



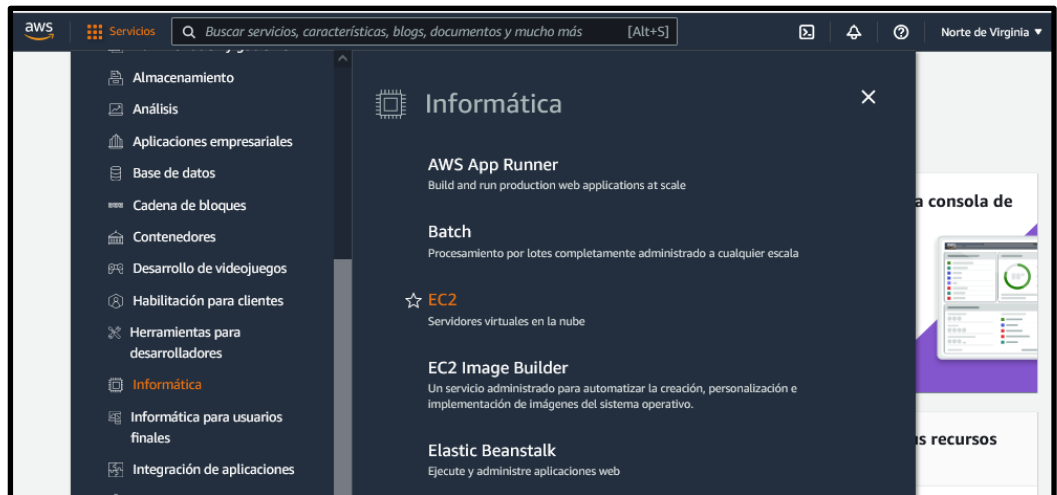
Nota: La nueva instancia se encuentra en ejecución

3.2.5.2 Conexión a la máquina remota por medio del EC2.

Nos dirigimos a servicios, informática y EC2

Figura 17

La imagen recalca cómo ingresar al EC2 de AWS

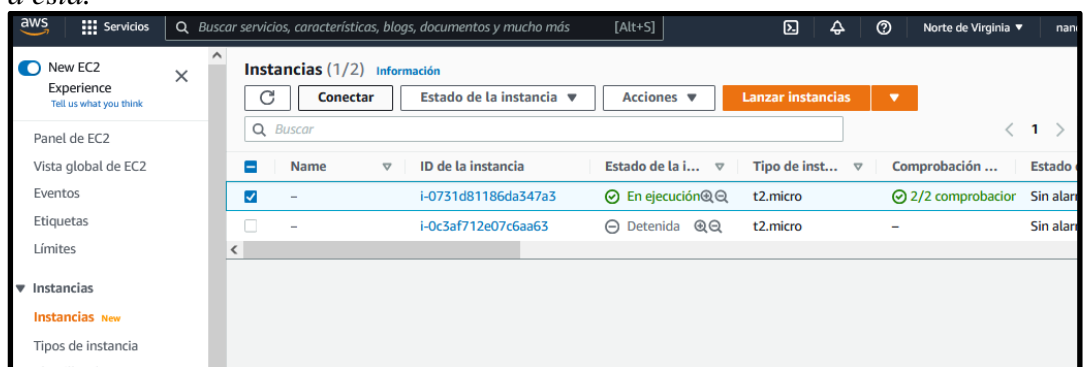


Nota: La figura muestra la lista de servicios AWS

Ingresamos instancia, seleccionamos la máquina virtual a la que nos queremos conectar, esta máquina debe estar en ejecución, seleccionamos conectar

Figura 18

La imagen muestra la selección de una instancia y el botón para conectar a esta.

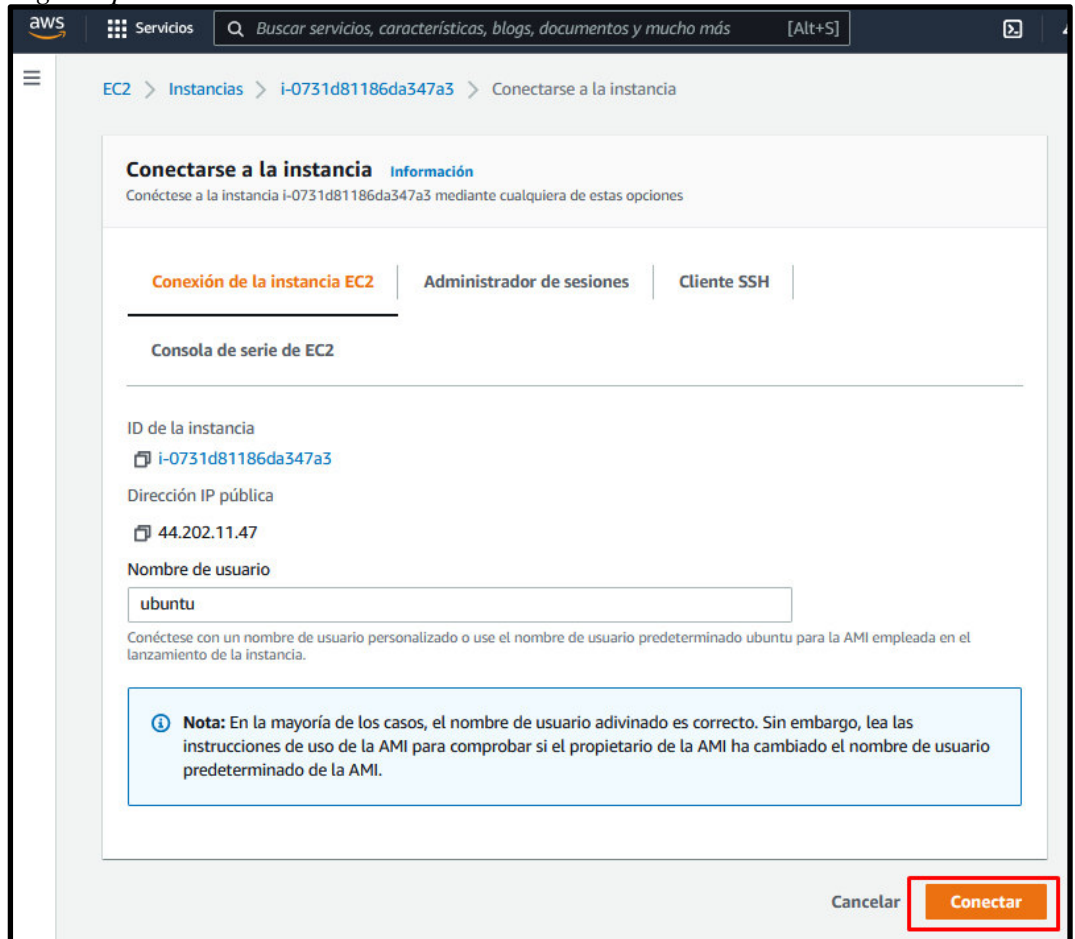


Nota: En la imagen muestra las instancias que se encuentra en ejecución

Aparecerá la siguiente ventana, le damos click en conectar:

Figura 19

Figura que muestra la conexión con una instancia.



Nota: La imagen muestra los datos de la instancia a conectarse.

Internamente se realizará la conexión a la máquina remota y nos aparecerá la siguiente ventana:

Figura 20

La figura muestra la conexión a una instancia.

```
welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.11.0-1022-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Fri Mar 18 10:40:18 UTC 2022

System load:  0.08               Processes:            99
Usage of /:   18.5% of 7.69GB    Users logged in:     0
Memory usage: 20%               IPv4 address for eth0: 172.31.93.149
Swap usage:   0%

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-93-149:~$
```

Nota: La imagen muestra algunas configuraciones de la máquina virtual.

3.2.5.3 Instalación del L.A.M.P.

Ingresamos a la máquina virtual remotamente y actualizamos las listas de paquetes para ello ponemos el siguiente comando:

sudo apt update

Figura 21

Figura que muestra el comando para actualizar ubuntu.

```

https://ubuntu.com/aws/pro
107 updates can be applied immediately.
65 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Fri Mar 18 11:26:03 2022 from 18.206.107.26
ubuntu@ip-172-31-93-149:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease [114
kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports InRelease [1
08 kB]
Hit:4 http://ppa.launchpad.net/ondrej/php/ubuntu focal InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Fetched 222 kB in 0s (479 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-93-149:~$ █

```

Nota: La imagen muestra el proceso de actualización de Ubuntu 20.04

Para la configuración de PHP ingresamos:

sudo apt install software-properties-common

Figura 22

La Figura muestra la instalación previa de algunas herramientas.

```

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Mar 18 10:40:19 2022 from 18.206.107.24
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-93-149:~$ sudo apt install software-properties-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
software-properties-common is already the newest version (0.99.9.8).
software-properties-common set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
ubuntu@ip-172-31-93-149:~$ █

```

Nota: La imagen muestra el proceso de instalación de herramientas necesarias

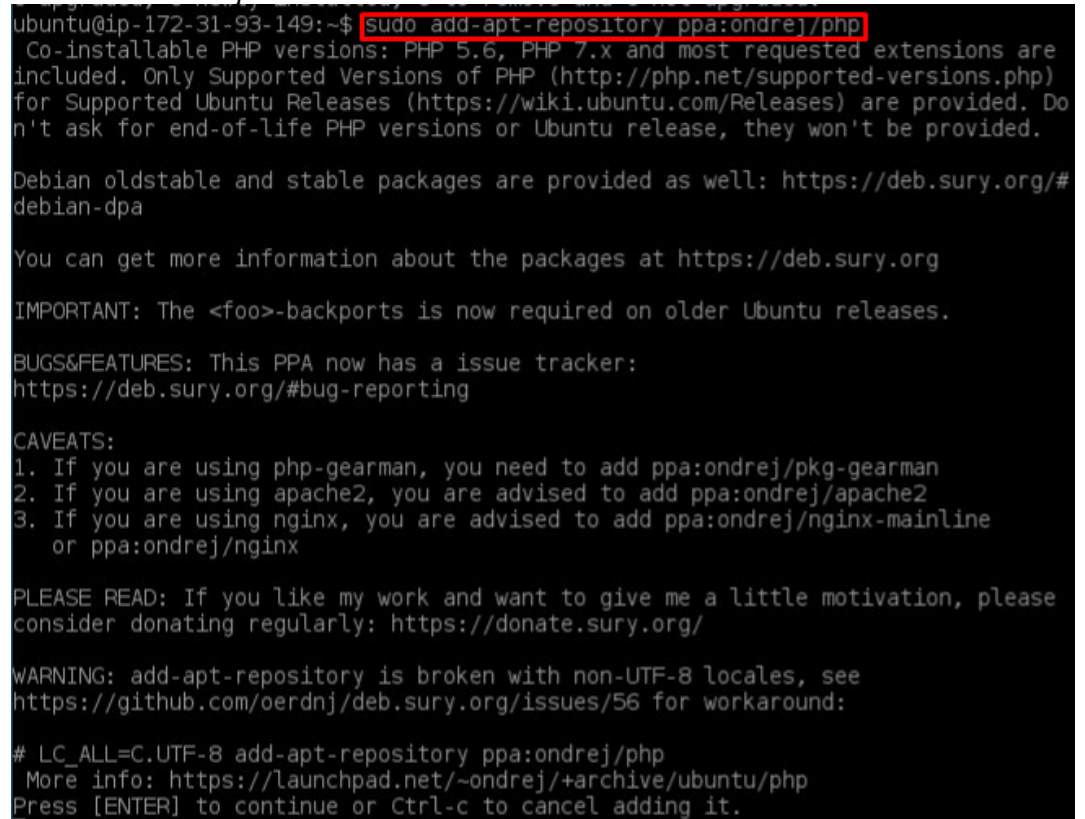
Se instala el repositorio ingresando el comando:

sudo add-apt-repository ppa:ondrej/php

Aparecerá los siguientes mensajes y damos Enter y comenzará la instalación

Figura 23

Instalación del repositorio.

A terminal window showing the execution of the command 'sudo add-apt-repository ppa:ondrej/php'. The output includes information about supported PHP versions, Debian packages, and a list of caveats for using php-gearman, apache2, and nginx. It also mentions a donation link and a warning about non-UTF-8 locales.

```
ubuntu@ip-172-31-93-149:~$ sudo add-apt-repository ppa:ondrej/php
Co-installable PHP versions: PHP 5.6, PHP 7.x and most requested extensions are
included. Only Supported Versions of PHP (http://php.net/supported-versions.php)
for Supported Ubuntu Releases (https://wiki.ubuntu.com/Releases) are provided. Do
n't ask for end-of-life PHP versions or Ubuntu release, they won't be provided.

Debian oldstable and stable packages are provided as well: https://deb.sury.org/#
debian-dpa

You can get more information about the packages at https://deb.sury.org

IMPORTANT: The <foo>-backports is now required on older Ubuntu releases.

BUGS&FEATURES: This PPA now has a issue tracker:
https://deb.sury.org/#bug-reporting

CAVEATS:
1. If you are using php-gearman, you need to add ppa:ondrej/pkg-gearman
2. If you are using apache2, you are advised to add ppa:ondrej/apache2
3. If you are using nginx, you are advised to add ppa:ondrej/nginx-mainline
   or ppa:ondrej/nginx

PLEASE READ: If you like my work and want to give me a little motivation, please
consider donating regularly: https://donate.sury.org/

WARNING: add-apt-repository is broken with non-UTF-8 locales, see
https://github.com/oerdnj/deb.sury.org/issues/56 for workaround:

# LC_ALL=C.UTF-8 add-apt-repository ppa:ondrej/php
More info: https://launchpad.net/~ondrej/+archive/ubuntu/php
Press [ENTER] to continue or Ctrl-c to cancel adding it.
```

Nota: La imagen muestra la instalación del repositorio.

Después actualizamos la lista de paquetes con:

sudo apt update

Figura 24

Actualización de repositorios.

```
ubuntu@ip-172-31-93-149:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://ppa.launchpad.net/ondrej/php/ubuntu focal InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
94 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-93-149:~$
```

Nota: Proceso de actualización de repositorios

Ahora se instalará los paquetes que componen los distintos elementos de la pila LAMP para Ubuntu 20.04 ingresando el siguiente comando para PHP 7.4:

```
sudo apt install -y apache2 libapache2-mod-php7.4 php7.4-mysql mariadb-server
```

Figura 25

Instalación de PHP 7.4.

```
ubuntu@ip-172-31-83-72:~$ sudo apt install -y apache2 libapache2-mod-php7.4 php7.4-mysql mariadb-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils galera-3 libapr1 libaprutil1 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libfcgi-fast-perl libfcgi-pm-perl libconfig-inifiles-perl libdbd-mysql-perl
  libdbi-perl libencode-locale-perl libfcgi-perl libhtml-parser-perl libhtml-tagset-perl
  libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl libjansson4 liblua5.2-0
  liblwp-mediatypes-perl libmysqlclient21 libpcre2-8-0 libsnappy1v5 libterm-readkey-perl
  libtimedate-perl liburi-perl mariadb-client-10.3 mariadb-client-core-10.3 mariadb-common
  mariadb-server-10.3 mariadb-server-core-10.3 mysql-common php-common php7.4-cli php7.4-common
  php7.4-json php7.4-opcache php7.4-readline socat ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser php-pear libclone-perl
  libmldbm-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl libipc-sharedcache-perl
  libwww-perl mailx mariadb-test tinycat openssl-blacklist
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils galera-3 libapache2-mod-php7.4 libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libfcgi-fast-perl libfcgi-pm-perl libconfig-inifiles-perl
  libdbd-mysql-perl libdbi-perl libencode-locale-perl libfcgi-perl libhtml-parser-perl
  libhtml-tagset-perl libhtml-template-perl libhttp-date-perl libhttp-message-perl libio-html-perl
  libjansson4 liblua5.2-0 liblwp-mediatypes-perl libmysqlclient21 libsnappy1v5 libterm-readkey-perl
  libtimedate-perl liburi-perl mariadb-client-10.3 mariadb-client-core-10.3 mariadb-common
  mariadb-server-10.3 mariadb-server-core-10.3 mysql-common php-common php7.4-cli php7.4-common
  php7.4-json php7.4-opcache php7.4-readline socat ssl-cert
```

Nota: Proceso de instalación de PHP 7.4

Comprobamos el estado de los servidores con:

systemctl status apache2 mariadb

Figura 26

Comprobación del estado de servicios

```
ubuntu@ip-172-31-93-149:~$ systemctl status apache2 mariadb
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: en
   Active: active (running) since Fri 2022-03-18 11:57:01 UTC; 9min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 13801 (apache2)
     Tasks: 6 (limit: 1147)
    Memory: 12.9M
    CGroup: /system.slice/apache2.service
            └─13801 /usr/sbin/apache2 -k start
              └─13804 /usr/sbin/apache2 -k start
                └─13805 /usr/sbin/apache2 -k start
                  └─13806 /usr/sbin/apache2 -k start
                    └─13807 /usr/sbin/apache2 -k start
                      └─13808 /usr/sbin/apache2 -k start

Mar 18 11:57:01 ip-172-31-93-149 systemd[1]: Starting The Apache HTTP Server...
Mar 18 11:57:01 ip-172-31-93-149 systemd[1]: Started The Apache HTTP Server.
```

Nota: Proceso de comprobación del estado de servicios

3.2.5.4 Configurar el firewall UFW de Ubuntu 20.04 para la pila LAMP.

Para permitir el acceso HTTP estándar:

sudo ufw allow http

Figura 27

permitir el acceso de HTTP

```
ubuntu@ip-172-31-93-149:~$ sudo ufw allow http
Rules updated
Rules updated (v6)
ubuntu@ip-172-31-93-149:~$
```

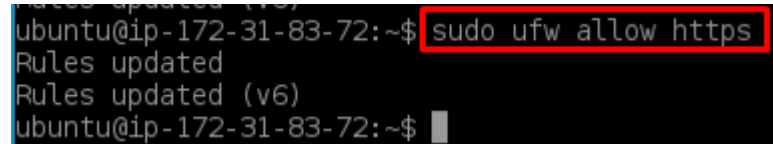
Nota: proceso para permitir el acceso de HTTP

Para permitir el acceso HTTPS:

sudo ufw allow https

Figura 28

Permisos de acceso HTTPS



```
ubuntu@ip-172-31-83-72:~$ sudo ufw allow https
Rules updated
Rules updated (v6)
ubuntu@ip-172-31-83-72:~$
```

Nota: Proceso d permisos de acceso HTTPS

3.2.5.5 Configurar los componentes de la pila LAMP en Ubuntu 20.04.

Para evitar alertas y eventos en los registros asignar un valor a la variable

ServerName ingresando el siguiente comando:

sudo nano /etc/apache2/apache2.conf

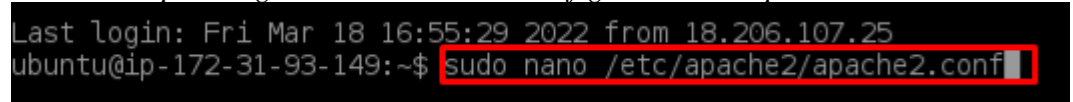
Esto nos permitirá editar el archivo conf, ingresamos la siguiente línea:

ServerName ubuntu2004.local.lan:80

Guardamos los cambios.

Figura 29

Comando para ingresar al archivo de configuración de apache



```
Last login: Fri Mar 18 16:55:29 2022 from 18.206.107.25
ubuntu@ip-172-31-93-149:~$ sudo nano /etc/apache2/apache2.conf
```

Nota: Proceso para ingresar al archivo de configuración de apache.

Figura 30

Ingresando directiva en la configuración de apache.

```
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE! If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the Mutex documentation (available
# at <URL:http://httpd.apache.org/docs/2.4/mod/core.html#mutex>);
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
#ServerRoot "/etc/apache2"
ServerName ubuntu2004.local.lan:80
```

Nota: Ingresando la directiva en la configuración de apache.

Recargamos la configuración con:

sudo systemctl reload apache2

Figura 31

Comando para recargar la configuración de apache.

```
ubuntu@ip-172-31-93-149:~$ sudo systemctl reload apache2
ubuntu@ip-172-31-93-149:~$
```

Nota: Recarga de la configuración de apache.

3.2.5.6 Configuración de PHP.

Ingresamos el siguiente comando:

sudo nano /etc/php/7.4/apache2/php.ini

Figura 32

Ingresando a la configuración de PHP.

```
ubuntu@ip-172-31-83-72:~$ sudo nano /etc/php/7.4/cli/php.ini
```

Nota: Proceso para ingresar a la configuración de PHP.

Con esto se nos abrirá el documento y agregamos zona horaria y guardamos los cambios

Figura 33

Directiva de la zona horaria.

```
[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
date.timezone = America/Lima
```

Nota: Proceso para ingresar la directiva de la zona horaria

Recargamos la configuración del servicio web

sudo systemctl reload apache2

Figura 34

Comando para recargar la configuración.

```
ubuntu@ip-172-31-93-149:~$ sudo systemctl reload apache2
ubuntu@ip-172-31-93-149:~$
```

Nota: Proceso para recargar la configuración.

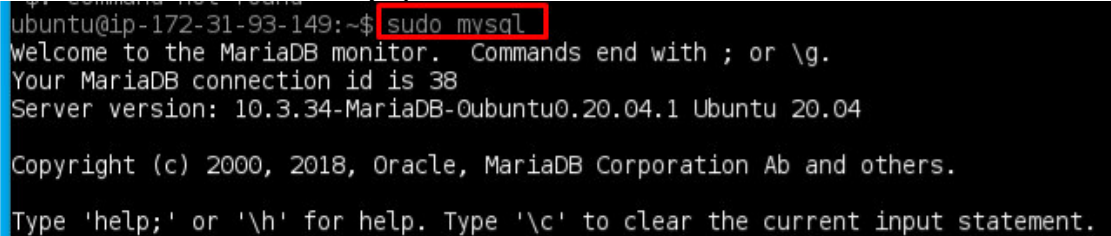
3.2.5.7 Configuración de MariaDB.

Usar el comando:

sudo mysql

Figura 35

Lanzamiento del cliente de mysql.

A terminal window with a black background and white text. The prompt is 'ubuntu@ip-172-31-93-149:~\$'. The command 'sudo mysql' is entered and highlighted with a red box. The output shows the MariaDB monitor welcome message, connection ID 38, server version 10.3.34-MariaDB-0ubuntu0.20.04.1, and copyright information. The prompt changes to 'mysql>'.

```
ubuntu@ip-172-31-93-149:~$ sudo mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.3.34-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

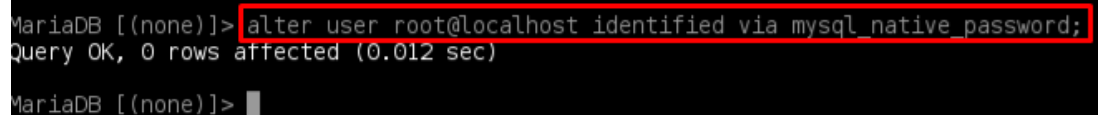
Nota: Proceso para lanzar el cliente de mysql

Para acceder una contraseña ingresamos:

alter user root@localhost identified via mysql_native_password;

Figura 36

Comando para cambiar la forma de autenticación.

A terminal window with a black background and white text. The prompt is 'MariaDB [(none)]>'. The command 'alter user root@localhost identified via mysql_native_password;' is entered and highlighted with a red box. The output shows 'Query OK, 0 rows affected (0.012 sec)'. The prompt changes to 'MariaDB [(none)]>'.

```
MariaDB [(none)]> alter user root@localhost identified via mysql_native_password;
Query OK, 0 rows affected (0.012 sec)

MariaDB [(none)]>
```

Nota: Proceso para cambiar la forma de autenticación.

alter user root@localhost identified by 'XXXXXXXXX';

Figura 37

Registrando contraseña.

```
MariaDB [(none)]> alter user root@localhost identified by 'XXXXXXXX';
```

Nota: Proceso para registrar la contraseña.

Ingresamos:

flush privileges;

Figura 38

Actualización de la tabla de privilegios.

```
MariaDB [(none)]> flush privileges;  
Query OK, 0 rows affected (0.004 sec)  
MariaDB [(none)]>
```

Nota: Proceso de actualización de la tabla de privilegios.

Finalmente ingresamos:

exit

Figura 39

Comando para cerrar la conexión a la base de datos.

```
MariaDB [(none)]> exit  
Bye  
ubuntu@ip-172-31-93-149:~$
```

Nota: Proceso para cerrar la conexión a la base de datos.

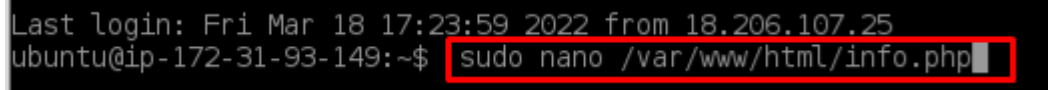
3.2.5.8 Probar la pila LAMP.

Para probar la pila LAMP en Ubuntu 20.04 crearemos un pequeño script en PHP:

sudo nano /var/www/html/info.php

Figura 40

Creando Script en PHP para probar la pila LAMP.

A terminal window with a black background. The text 'Last login: Fri Mar 18 17:23:59 2022 from 18.206.107.25' is at the top. Below it, the prompt 'ubuntu@ip-172-31-93-149:~\$' is followed by the command 'sudo nano /var/www/html/info.php' which is highlighted with a red rectangular box.

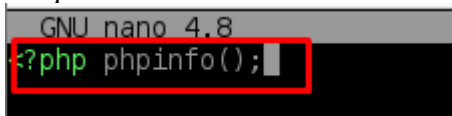
Nota: Creación de script en PHP.

Ingresamos la siguiente línea y guardamos los cambios:

<?php phpinfo();

Figura 41

Script PHP.

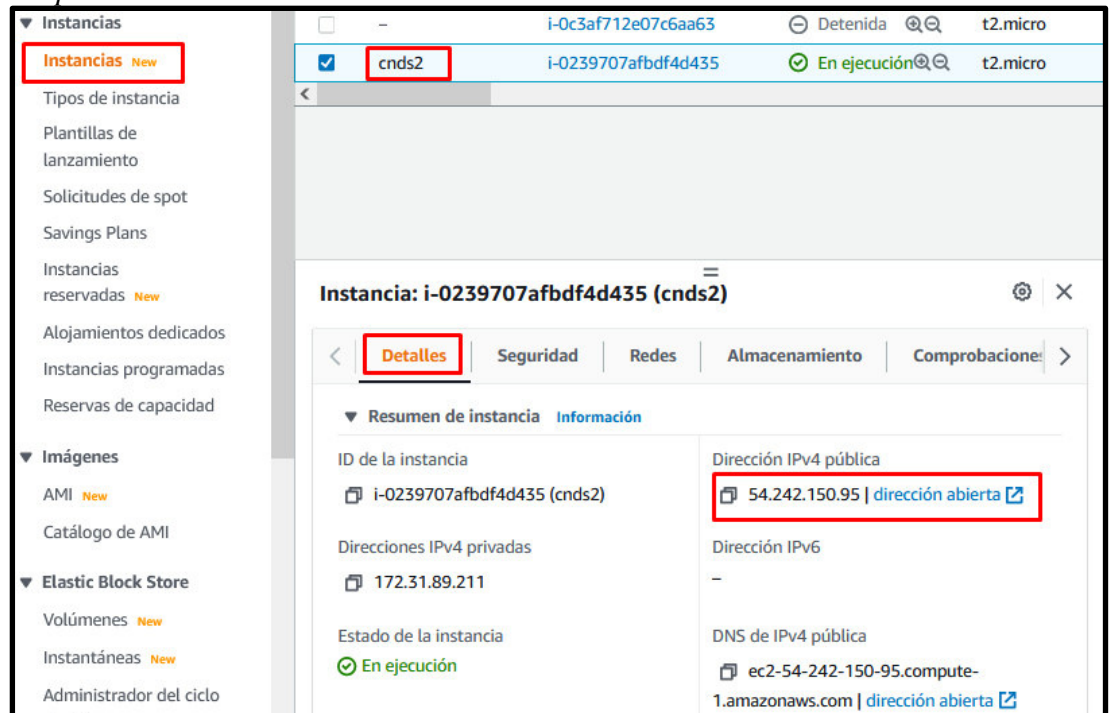
A terminal window showing the nano text editor. The title bar says 'GNU nano 4.8'. The text '<?php phpinfo();' is entered and highlighted with a red rectangular box.

Nota: Script PHP.

Nos dirigimos a EC2 a apartado de instancias y seleccionamos la máquina virtual en donde hemos realizado la configuración y a apuntamos la dirección pública que se nos ha asignado:

Figura 42

Propiedades de la instancia.

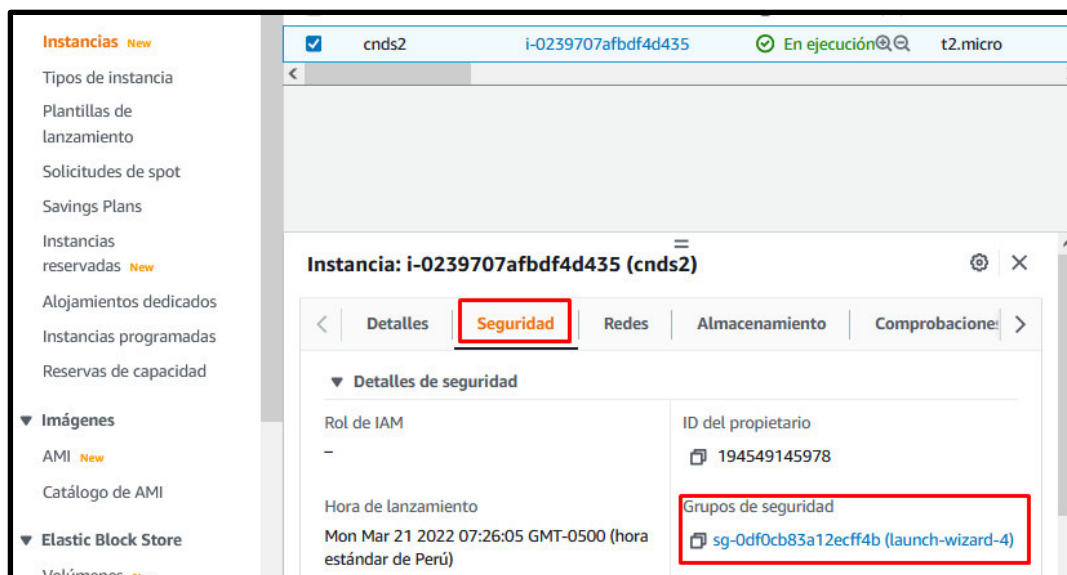


Nota: Detalles de la instancia creada.

Después ingresamos a seguridad y a grupo de seguridad

Figura 43

Apartado de seguridad de una instancia.

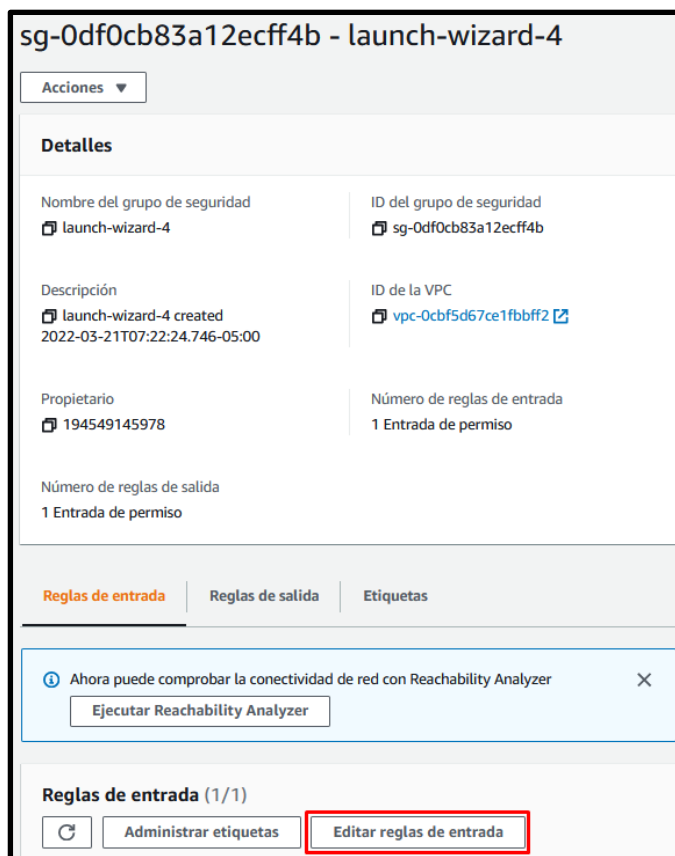


Nota: Grupo de seguridad de una instancia.

Nos aparecerá la siguiente ventana y entramos en editar parámetros de entrada

Figura 44

Reglas de entrada de la instancia.



Nota: Ediciones de reglas de entrada.

Nos aparecerá la siguiente ventana e ingresamos a agregar regla

Figura 45

Edición de reglas de entrada.

Editar reglas de entrada Información

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

Reglas de entrada Información

Regla de entrada 1 Eliminar

ID de la regla del grupo de seguridad: sgr-001a2fc7e842a578e

Tipo: SSH Información

Protocolo: TCP Información

Intervalo de puertos: 22 Información

Tipo de origen: Personalizada Información

Origen: 0.0.0.0/0 Información

Descripción: opcional Información

Agregar regla

Cancelar Previsualizar los cambios Guardar reglas

Nota: Formulario para ingresar nuevas reglas de entrada.

Agregamos las siguientes las siguientes reglas para HTTP y HTTPS y guardamos los cambios

Figura 46

Ingresando las reglas de entrada HTTP y HTTPS.

Editar reglas de entrada Información

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

Reglas de entrada Información

ID de la regla del grupo de seguridad	Tipo Información	Protocolo Información	Intervalo de puertos Información	Origen Información	Descripción: opcional Información	
sgr-001a2fc7e842a578e	SSH	TCP	22	Person...		Eliminar
-	HTTP	TCP	80	Anywh...		Eliminar
-	HTTPS	TCP	443	Anywh...		Eliminar

Agregar regla

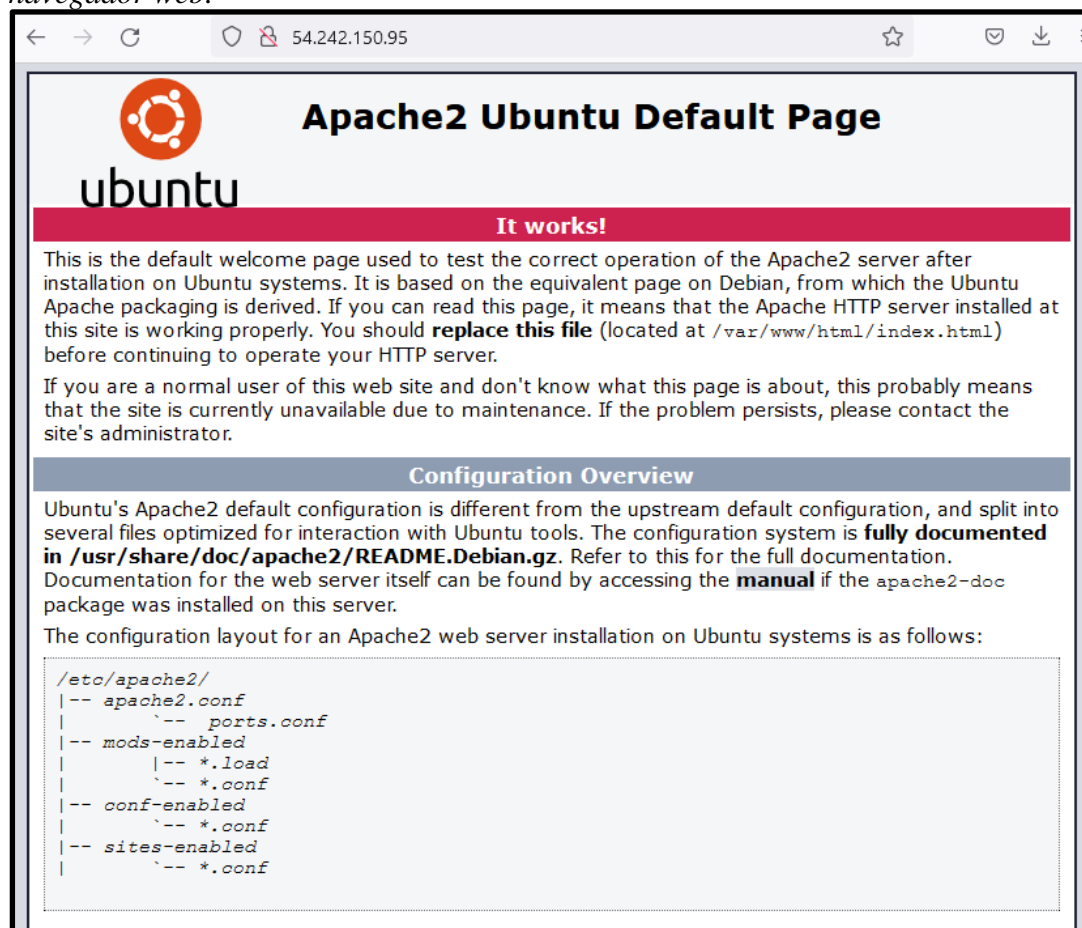
Cancelar Previsualizar los cambios Guardar reglas

Nota: Ingresando las nuevas reglas de entrada.

Después ingresamos la IP pública de nuestra máquina a un navegador de internet y deberá mostrarse lo siguiente para validar la instalación de apache:

Figura 47

Ingresando a la dirección pública de la instancia por medio de un navegador web.

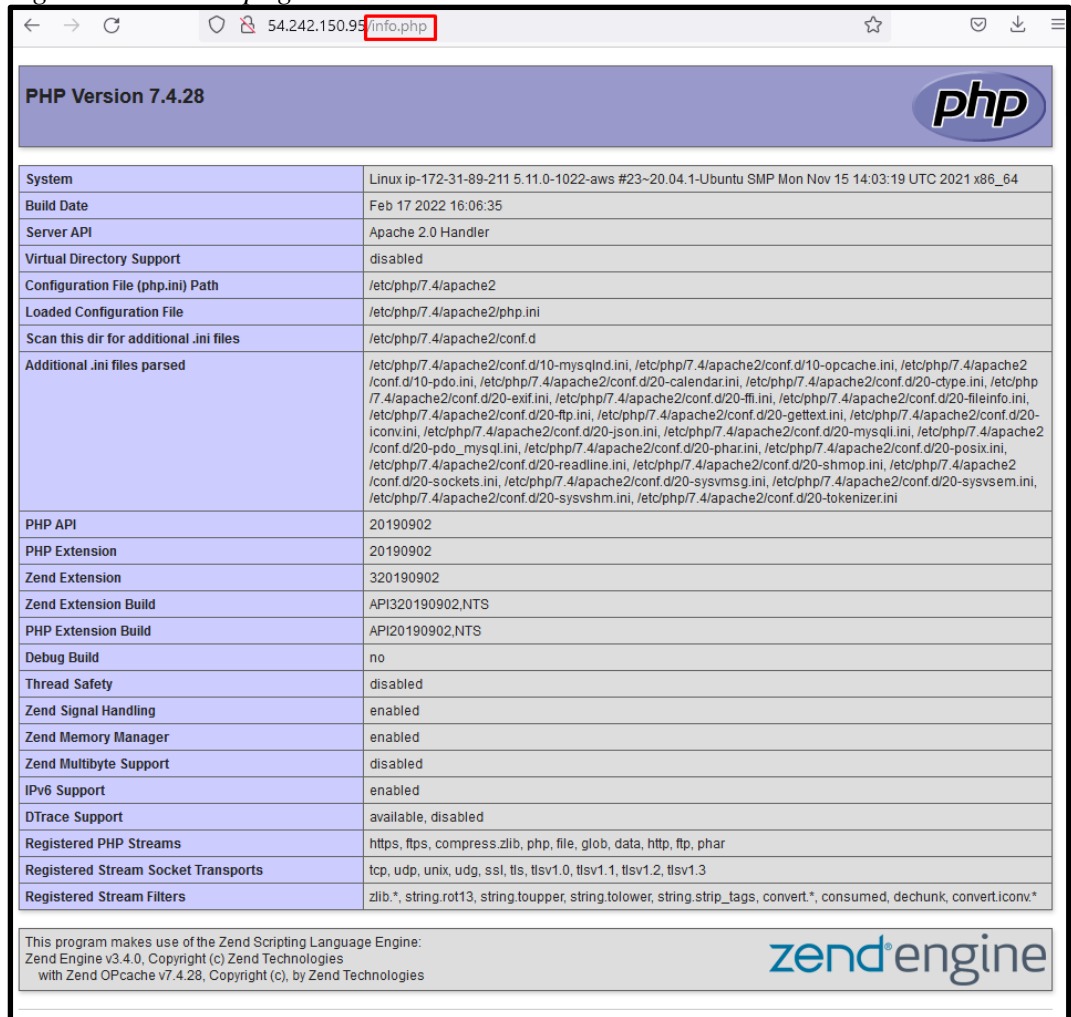


Nota: Probando el servicio expuesto de la máquina virtual ingresando a la IP pública de la instancia.

Para validar la instalación de PHP agregamos /info.php en el navegador de internet

Figura 48

Ingresando al Script generada.



PHP Version 7.4.28 	
System	Linux ip-172-31-89-211 5.11.0-1022-aws #23~20.04.1-Ubuntu SMP Mon Nov 15 14:03:19 UTC 2021 x86_64
Build Date	Feb 17 2022 16:06:35
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqld.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-syssem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*
This program makes use of the Zend Scripting Language Engine: Zend Engine v3.4.0, Copyright (c) Zend Technologies with Zend OPcache v7.4.28, Copyright (c), by Zend Technologies 	

Nota: Validando el ingreso al script ingresado al servicio.

3.2.5.9 Pre-requisitos para la instalación TheHive.

Primero eliminemos las actualizaciones y los repositorios para el resto del proceso de instalación:

sudo apt update -y && sudo apt upgrade -y

Figura 49

Actualizamos todos los repositorios.

```
ubuntu@ip-172-31-92-82:~$ sudo apt update -y && sudo apt upgrade -yls
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
```

Nota: Comando todos los repositorios.

***curl -fsSL https://www.apache.org/dist/cassandra/KEYS | sudo apt-key
add -***

Figura 50

Gestionado la lista de claves APT.

```
ubuntu@ip-172-31-92-82:~$ curl -fsSL https://www.apache.org/dist/cassandra/KEYS | sudo apt-key add -
OK
```

Nota: Comando para gestionar la lista de claves APT.

***echo "deb http://www.apache.org/dist/cassandra/debian 311x main" |
sudo tee -a /etc/apt/sources.list.d/cassandra.sources.list***

Figura 51

Agregando repositorio para Apache Cassandra.

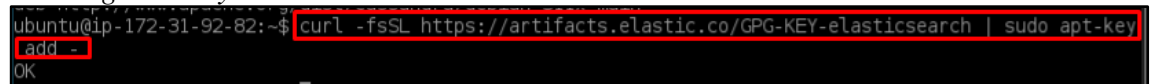
```
ubuntu@ip-172-31-92-82:~$ echo "deb http://www.apache.org/dist/cassandra/debian 311x main" | sudo tee  
-a /etc/apt/sources.list.d/cassandra.sources.list
deb http://www.apache.org/dist/cassandra/debian 311x main
```

Nota: Agregando repositorios para Apache Cassandra.

curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

Figura 52

Descargando key APT de elasticsearch.



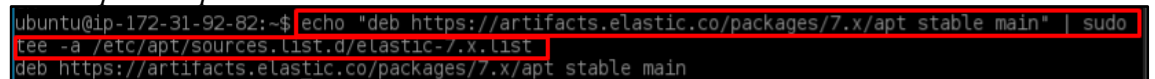
```
ubuntu@ip-172-31-92-82:~$ curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
```

Nota: comando para descargar key APT de elasticsearch

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

Figura 53

Pre-requisitos para elasticSearch.



```
ubuntu@ip-172-31-92-82:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
deb https://artifacts.elastic.co/packages/7.x/apt stable main
```

Nota: Pre-requisitos para elasticSearch.

curl https://raw.githubusercontent.com/TheHive-Project/TheHive/master/PGP-PUBLIC-KEY | sudo apt-key add -

Figura 54

Pre-requisitos para TheHive.

```
ubuntu@ip-172-31-92-82:~$ curl https://raw.githubusercontent.com/TheHive-Project/TheHive/master/PGP-PUBKEY.asc | sudo apt-key add -
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 3136 100 3136 0 0 41263 0 --:--:-- --:--:-- --:--:-- 41263
OK
```

Nota: Pre-requisitos para TheHive.

```
echo 'deb https://deb.thehive-project.org release main' | sudo tee -a
/etc/apt/sources.list.d/thehive-project.list
```

Figura 55

Pre-requisitos para TheHive.

```
ubuntu@ip-172-31-92-82:~$ echo 'deb https://deb.thehive-project.org release main' | sudo tee -a /etc/a
pt/sources.list.d/thehive-project.list
deb https://deb.thehive-project.org release main
```

Nota: Pre-requisitos para TheHive.

```
sudo apt update -y && sudo apt upgrade -y
```

Figura 56

Actualización de todos los repositorios.

```
ubuntu@ip-172-31-92-82:~$ sudo apt update -y && sudo apt upgrade -y
Hit:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease
Hit:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports InRelease
```

Nota: Actualización de todos los repositorios.

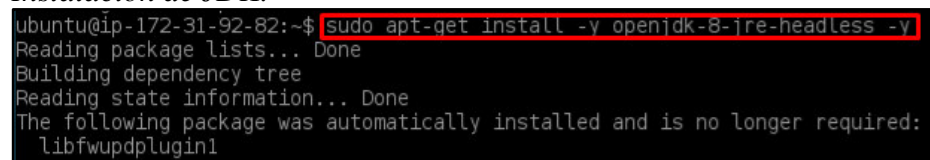
3.2.5.10 Instalar el entorno de tiempo de ejecución de Java

Se requiere JRE 8 para esta instalación ingrese los siguientes comandos:

```
sudo apt-get install -y openjdk-8-jre-headless -y
```

Figura 57

Instalación de JDK.

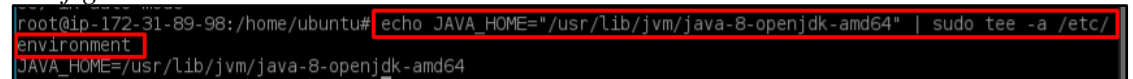
A terminal window showing the command 'sudo apt-get install -y openjdk-8-jre-headless -y' being executed. The output shows 'Reading package lists... Done', 'Building dependency tree', 'Reading state information... Done', and a message that the package was automatically installed and is no longer required, listing 'libfwupdplugin1'.

Nota: Instalación de JDK

```
echo JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64" | sudo tee -a  
/etc/environment
```

Figura 58

Configuración de JDK.

A terminal window showing the command 'echo JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64" | sudo tee -a /etc/environment' being executed. The output shows 'JAVA_HOME=/usr/lib/jvm/java-8-openjdk-amd64'.

Nota: Configuración de JDK.

```
export JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64"
```

Figura 59

Configuración de JDK.

```
ubuntu@ip-172-31-92-82:~$ export JAVA_HOME="/usr/lib/jvm/java-8-openjdk-amd64"
```

Nota: Configuración de JDK.

3.2.5.11 *Instalación de Cassandra.*

Para la instalación y configuración de cassandra ingresamos:

sudo apt install cassandra -y

Figura 60

Instalación de Cassandra.

```
ubuntu@ip-172-31-92-82:~$ sudo apt install cassandra -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is
```

Nota: Instalación de Cassandra.

sudo apt install net-tools

Figura 61

Instalación de net-tools.

```
ubuntu@ip-172-31-92-82:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and
  libfwupdplugin1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
```

Nota: Instalación de net-tools.

cqlsh localhost 9042

Figura 62

Configurando Cassandra con cqlsh.

```
root@ip-172-31-46-16:/home/ubuntu# cqlsh localhost 9042
Connected to Test Cluster at localhost:9042.
[cqlsh 5.0.1 | Cassandra 3.11.12 | CQL spec 3.4.4 | Native protocol v4]
Use HELP for help.
```

Nota: Configurando Cassandra con cqlsh.

Ahora tendrá que entrar por consola en Cassandra para realizar un cambio de configuración. Realice lo siguiente de forma interactiva dentro de CQLSH.

UPDATE system.local SET cluster_name = 'thp' where key='local';

Figura 63

Actualizando el nombre de cluster.

```
cqlsh> UPDATE system.local SET cluster name = 'thp' where key='local';
```

Nota: Actualizar el nombre del cluster.

exit;

Figura 64

Saliendo del cqlsh.

```
cqlsh> exit;
```

Nota: saliendo del cqlsh.

Luego realice una descarga usando lo siguiente desde la consola...

nodetool flush

Figura 65

nodetool flush.

```
svrthehive@svrthehive:~$ nodetool flush
```

Nota: Nodetool Flush.

luego edite /etc/cassandra/cassandra.yaml para reflejar los siguientes requisitos:

sudo nano /etc/cassandra/cassandra.yaml

Figura 66

Ingresando al yaml de Cassandra.

```
svrthehive@svrthehive:~$ sudo nano /etc/cassandra/cassandra.yaml
```

Nota: Ingresando al yaml de Cassandra.

Figura 67

Configuración para agregar al yaml de Cassandra.

```

cluster_name: 'thp'
listen_address: '127.0.0.1' # address for nodes
rpc_address: '127.0.0.1' # address for clients
seed_provider:
  - class_name: org.apache.cassandra.locator.SimpleSeedProvider
    parameters:
      # Ex: "<ip1>,<ip2>,<ip3>"
      - seeds: '127.0.0.1' # self for the first node
data_file_directories:
  - '/var/lib/cassandra/data'
commitlog_directory: '/var/lib/cassandra/commitlog'
saved_caches_directory: '/var/lib/cassandra/saved_caches'
hints_directory:
  - '/var/lib/cassandra/hints'

```

Nota: Configuración para agregar al yaml de Cassandra.

Figura 68

Cluster_name para yaml de Cassandra.

```

# The name of the cluster. This is mainly u
# one logical cluster from joining another.
cluster_name: 'thp'

```

Nota: Cluster_name para el yaml de Cassandra.

Figura 69

listen_address para el yaml de Cassandra.

```

listen_address: '127.0.0.1'

```

Nota: Listen_address para el yaml de Cassandra.

Figura 70

rpc_address para el yaml de Cassandra.

```

rpc_address: '127.0.0.1'

```

Nota: rpc_address para el yaml de Cassandra.

Figura 71

Seed_provider para el yaml de Cassandra.

```
seed_provider:  
  # Addresses of hosts that are deemed contact points.  
  # Cassandra nodes use this list of hosts to find each other and learn  
  # the topology of the ring.  You must change this if you are running  
  # multiple nodes!  
  - class_name: org.apache.cassandra.locator.SimpleSeedProvider  
    parameters:   
      # seeds is actually a comma-delimited list of addresses.  
      # Ex: "<ip1>,<ip2>,<ip3>"  
      - seeds: "127.0.0.1"
```

Nota: Seed_provider para el yaml de Cassandra.

Figura 72

Data_file_directories para el yaml de Cassandra.

```
# the configured compaction strategy.  
# If not set, the default directory is $CASSANDRA_HOME/data/data.  
data_file_directories:  
  - /var/lib/cassandra/data
```

Nota: Data_file_directories para el yaml de Cassandra.

Figura 73

Commitlog_directory para el yaml de Cassandra.

```
# separate spindle than the data directories.  
# If not set, the default directory is $CASSANDRA_HOME/data/commitlog.  
commitlog_directory: /var/lib/cassandra/commitlog
```

Nota: Commitlog_directory para el yaml de Cassandra.

Figura 74

Saved_caches_directory para el yaml de Cassandra.

```
# If not set, the default directory is $CASSANDRA_HOME/data/saved_caches  
saved_caches_directory: /var/lib/cassandra/saved_caches
```

Nota: Saved_caches_directory para el yaml de Cassandra.

Figura 75

Hints_directory para el yaml de Cassandra.

```
# Directory where Cassandra should store hints.  
# If not set, the default directory is $CASSANDRA_HOME/data/hints.  
hints_directory: /var/lib/cassandra/hints
```

Nota: Hints_directory para el yaml de Cassandra.

Guarde los cambios en su editor favorito y luego reinicie Cassandra.

sudo systemctl restart cassandra

Figura 76

Reiniciar Cassandra.

```
root@ip-172-31-46-16:/home/ubuntu# sudo systemctl restart cassandra
```

Nota: Reiniciar Cassandra.

sudo systemctl enable cassandra

Figura 77

Habilitar Cassandra.

```
root@ip-172-31-46-16:/home/ubuntu# sudo systemctl enable cassandra  
cassandra.service is not a native service, redirecting to systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable cassandra
```

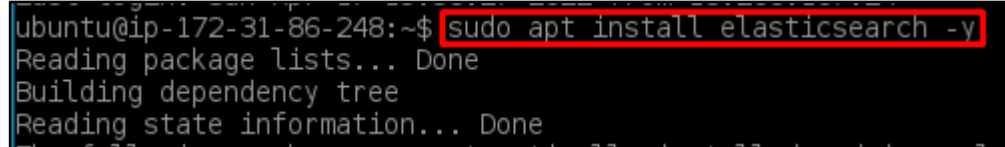
Nota: Habilitar Cassandra.

3.2.5.12 Instalar Elasticsearch.

sudo apt install elasticsearch -y

Figura 78

Instalar elasticsearch.



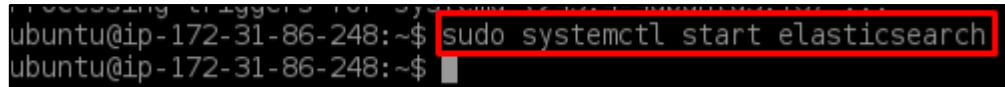
```
ubuntu@ip-172-31-86-248:~$ sudo apt install elasticsearch -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Nota: Instalación de elasticsearch.

sudo systemctl start elasticsearch

Figura 79

Iniciando elasticsearch.



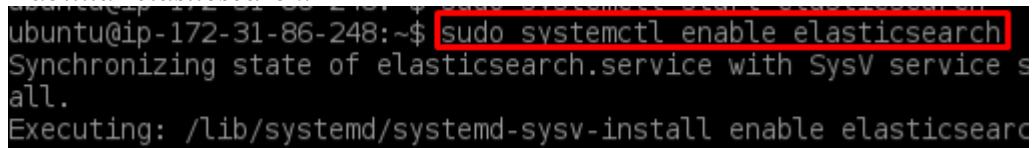
```
ubuntu@ip-172-31-86-248:~$ sudo systemctl start elasticsearch
ubuntu@ip-172-31-86-248:~$
```

Nota: Inicializando elasticsearch.

sudo systemctl enable elasticsearch

Figura 80

Habilitar elasticsearch.



```
ubuntu@ip-172-31-86-248:~$ sudo systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service s
all.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
```

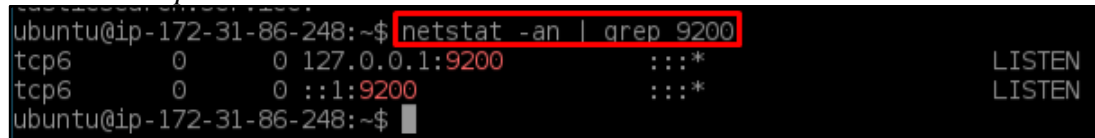
Nota: Habilitar elasticsearch.

Después de un período de aproximadamente 30 segundos, Elasticsearch debería anunciar el puerto 9200 en el host local. Puede verificar que ha ocurrido a través del siguiente comando:

netstat -an | grep 9200

Figura 81

Probando el puerto 9200.



```
ubuntu@ip-172-31-86-248:~$ netstat -an | grep 9200
tcp6      0      0 127.0.0.1:9200          :::*           LISTEN
tcp6      0      0 :::1:9200              :::*           LISTEN
ubuntu@ip-172-31-86-248:~$
```

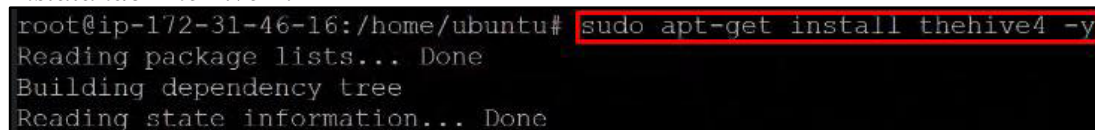
Nota: Probando el puerto 9200.

3.2.5.13 Instalar TheHive.

sudo apt-get install thehive4 -y

Figura 82

Instalando TheHive 4.



```
root@ip-172-31-46-16:/home/ubuntu# sudo apt-get install thehive4 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Nota: Instalación TheHive 4

sudo mkdir /opt/thp/thehive/index

Figura 83

Comando de configuración de TheHive.

```
root@ip-172-31-46-16:/home/ubuntu# sudo mkdir /opt/thp/thehive/index
```

Nota: Comando de configuración de TheHive.

sudo mkdir /opt/thp/thehive/files

Figura 84

Comando de configuración de TheHive.

```
root@ip-172-31-46-16:/home/ubuntu# sudo mkdir /opt/thp/thehive/files
```

Nota: Comando de configuración de TheHive.

sudo chown thehive:thehive -R /opt/thp/thehive/index

Figura 85

Comando de configuración de TheHive.

```
vrthehive@svrthehive:~$ sudo chown thehive:thehive -R /opt/thp/thehive/index
```

Nota: Comando de configuración de TheHive.

sudo chown thehive:thehive -R /opt/thp/thehive/files

Figura 86

Comando de configuración de TheHive.

```
svrthehive@svrthehive:~$ sudo chown thehive:thehive -R /opt/thp/thehive/files
```

Nota: Comando de configuración de TheHive.

3.2.5.14 Configurar TheHive y reiniciar.

Ahora podemos configurar TheHive editando el archivo de configuración apropiadamente. Esta será una configuración básica al principio, las integraciones avanzadas vienen más adelante bajo los encabezados de Integración.

En el editor, actualice las siguientes variables en
/etc/thehive/application.conf

nano/etc/thehive/application.conf

Figura 87

Ingresando al archivo de configuración de TheHive.

```
root@ip-172-31-46-16:/home/ubuntu# nano /etc/thehive/application.conf
```

Nota: Ingresado al archivo de configuración de TheHive.

Figura 88

Configuración para agregar a TheHive.

```

## Database configuration
storage {
  ## Cassandra configuration
  # More information at https://docs.janusgraph.org/basics/configuration-reference/#storagecql
  backend: cql
  hostname: ["127.0.0.1"]
  # Cassandra authentication (if configured)
  // username: "thehive"
  // password: "password"
  cql {
    cluster-name: thp
    keyspace: thehive
  }
  index.search {
    backend: elasticsearch
    hostname: ["127.0.0.1"]
    index-name: thehive
  }
}

## Attachment storage configuration
storage {
  ## Local filesystem
  provider: localfs
  localfs.location: /opt/thp/thehive/files
  ## Hadoop filesystem (HDFS)
  // provider: hdfs
  // hdfs {
  //   root: "hdfs://localhost:10000" # namenode server hostname
  //   location: "/thehive" # location inside HDFS
  //   username: thehive # file owner
  // }
}

```

Nota: Configuración para agregar a TheHive.

Figura 89

Agregar configuración a TheHive.

```

## Database configuration
db.janusgraph {
  storage {
    ## Cassandra configuration
    # More information at https://docs.janusgraph.org/basics/configuration-reference/#storagecql
    backend: cql
    hostname: ["127.0.0.1"]
    # Cassandra authentication (if configured)
    // username: "thehive"
    // password: "password"
    cql {
      cluster-name: thp
      keyspace: thehive
    }
  }
  index.search {
    // backend: lucene
    // directory: /opt/thp/thehive/index
    # If TheHive is in cluster Elasticsearch must be used:
    backend: elasticsearch
    hostname: ["127.0.0.1"]
    index-name: thehive
  }
}

```

Nota: Agregar configuración a TheHive.

Figura 90

Agregar configuración a TheHive.

```
## Attachment storage configuration
storage {
    ## Local filesystem
    provider: localfs
    localfs.location: /opt/thp/thehive/files

    ## Hadoop filesystem (HDFS)
    // provider: localfs
    // hdfs {
    //     root: "hdfs://localhost:10000" # namenode server hostname
    //     location: "/thehive" # location inside HDFS
    //     username: thehive # file owner
    // }
}
```

Nota: Agregar configuración a TheHive.

Guarde los cambios de configuración y luego inicie TheHive desde la consola

sudo systemctl start thehive

Figura 91

Inicializando TheHive.

```
root@ip-172-31-46-16:/home/ubuntu# sudo systemctl start thehive
```

Nota: Inicializando TheHive.

sudo systemctl enable thehive

Figura 92

Habilitar TheHive.

```
root@ip-172-31-46-16:/home/ubuntu# sudo systemctl enable thehive
```

Nota: Habilitar TheHive.

sudo apt-mark hold elasticsearch

Figura 93

Configuración para elasticsearch.

```
root@ip-172-31-46-16:/home/ubuntu# sudo apt-mark hold elasticsearch  
elasticsearch set on hold.
```

Nota: Configuración de elasticsearch.

sudo apt-mark hold thehive4

Figura 94

Configuración de TheHive.

```
root@ip-172-31-46-16:/home/ubuntu# sudo apt-mark hold thehive4  
thehive4 set on hold.
```

Nota: Configuración de TheHive

netstat -an | grep 9200

Figura 95

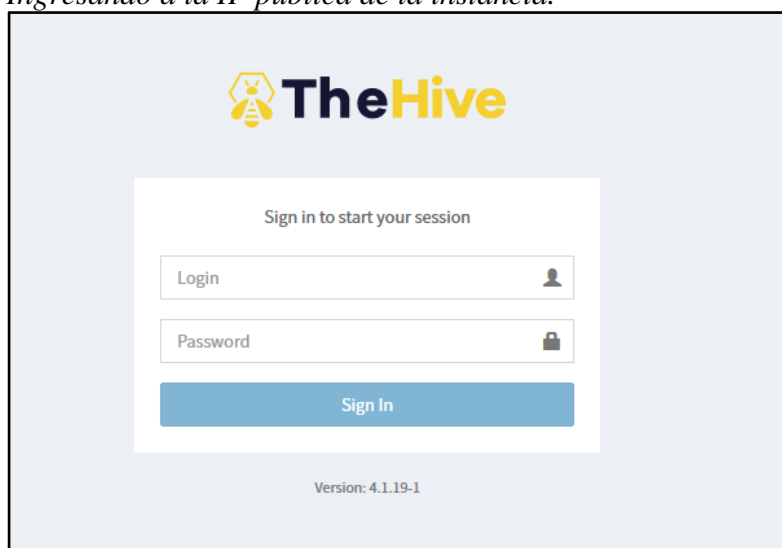
Probando el puerto 9000.

```
root@ip-172-31-46-16:/home/ubuntu# netstat -an | grep 9000
tcp6      0      0 :::9000          :::*              LISTEN
```

Nota: Probado el puerto 9000.

Figura 96

Ingresando a la IP pública de la instancia.



Nota: Ingresando a la IP pública de la instancia.

Una vez aprobado el informe se replica la instalación y configuración en la cuenta AWS donde se tiene los servidores para su uso en producción.

3.3 Evaluación

3.3.1 Evaluación Económica / Evaluación Costo-Beneficio

Para ello se realiza una estimación de costo por medio de la calculadora de AWS para Amazon EC2 con las siguientes configuraciones:

Tabla 4

Configuración para la instancia EC2

Configuración	Especificación
Región	EE. UU. Este (Norte de Virginia)
S.O.	Linux (Ubuntu 20.04)
VCPU	4
Memoria (GiB)	16
Instancias	1
Modelo de precios	EC2 Instance Savings Plans
Plazo de reserva	1 años
Opciones de pago	Sin pagos iniciales

Nota: Especificaciones para configuración de EC2

Con el cual se estaría pagando un costo anual de: 689.41 USD

Figura 97

Estimación de costos con calculadora de AWS

▼ **Mostrar cálculos**

Conversión de unidades

EC2 Instance Savings Plans rate for t4g.xlarge in the US East (N. Virginia) for 1 Year term and All Upfront is 0.0787 USD

Hours in the commitment: 365 days * 24 hours * 1 year = 8760.0000 hours

Total Commitment: 0.0787 USD * 8760 hours = 689.4120 USD

Upfront: All Upfront (100% of 689.412) = 689.4120 USD

Hourly cost for EC2 Instance Savings Plans = (Total Commitment - Upfront cost)/Hours in the term: (689.412 - 689.412)/8760 = 0.0000 USD

*Please note that you will pay an hourly commitment for Savings Plans and your usage will be accrued at a discounted rate against this commitment.

Cálculos de precios

1 instancias x 689,412 USD = 689,41 USD (costo inicial)

Instancia de Amazon EC2 (inicial): 689.41 USD

Nota: Estimación de costo mensual

La configuración para el almacenamiento por instancia sería:

Tabla 5

Configuración de almacenamiento

Configuración	Especificación
tipo de almacenamiento en volumen de EBS	SSD de uso general (gp2)
Cantidad de almacenamiento	30GB

Con el cual se estaría pagando un costo mensual de: 3 USD

Figura 98

Estimación de costos de almacenamiento

▼ **Mostrar cálculos**

30 GB x 0,10 USD x 1 instancias = 3,00 USD (costo de almacenamiento de EBS)

Costo del almacenamiento de EBS: 3,00 USD

Precios de Amazon Elastic Block Storage (EBS) (mensual): 3.00 USD

Nota: Estimación de costo mensual de alquiler de almacenamiento

Resumiendo, se tendría el siguiente costo mensual y anual:

Figura 99

Estimación de costos de almacenamiento

Resumen de la estimación [Información](#)

Costo inicial	Costo mensual	Costo total de 12 meses
689,41 USD	3,00 USD	725,41 USD
		Incluye el costo inicial

Nota: Estimación de costo anual

3.3.2 Interpretación Del Van Y Del Tir

Dado la obtención del costo anual mencionado en el punto anterior se realiza el análisis de la viabilidad del proyecto.

Tabla 6

Inversión y Tasa de descuento

Datos	Inversión inicial	\$	725.41
	Tasa de descuento		8%

Nota: Inversión inicial y tasa de descuento

Para realizar los cálculos se asume una tasa de descuento del 8%, en el caso de los ingresos a futuro se asume una ganancia inicial de \$740 con un aumento del 15% en los años posteriores.

Tabla 7

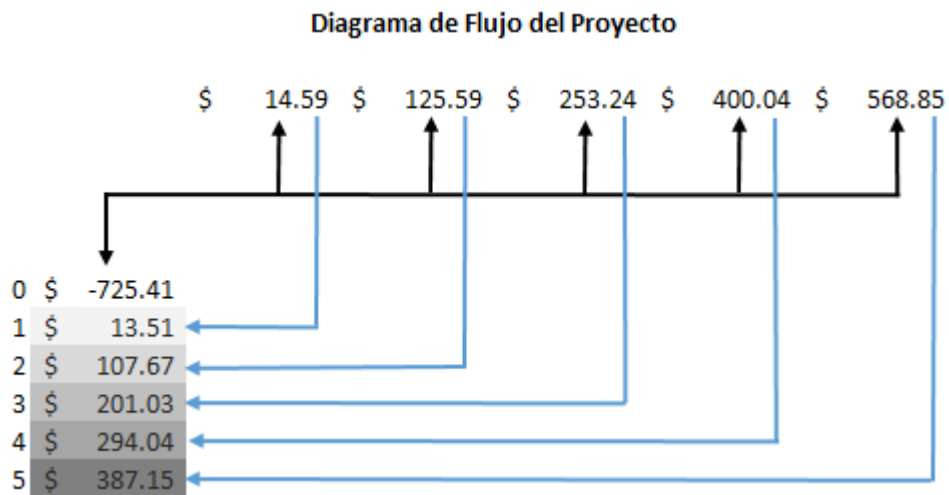
Cuadro de ingresos y egresos

Periodo	Ingreso	Egreso	Flujo de efectivo Neto	Valor Presente
0			\$ -725.41	\$ -725.41
1	\$ 740.00	\$ 725.41	\$ 14.59	\$ 13.51
2	\$ 851.00	\$ 725.41	\$ 125.59	\$ 107.67
3	\$ 978.65	\$ 725.41	\$ 253.24	\$ 201.03
4	\$ 1,125.45	\$ 725.41	\$ 400.04	\$ 294.04
5	\$ 1,294.26	\$ 725.41	\$ 568.85	\$ 387.15

Nota: Cálculo de los egresos al valor presente

Figura 100

Diagrama de Flujo del Proyecto



Nota: Gráfica que muestra el valor de los egresos al valor presente

Con los datos obtenidos en el valor presente se realizan los cálculos del VAN y del TIR.

Tabla 8

Resultado del VAN y TIR

Valor presente de los flujo actualizados:	\$ 1,003.40
Valor Actual Neto (VAN)	\$ 277.99
Tasa Interna de Retorno (TIR)	17%
Indice de rentabilidad o Razón Beneficio/Costo	1.38

Nota: Resultado de la evaluación costo beneficio.

Dado los resultados se observa que el proyecto es rentable con IR de 1.38.

CAPÍTULO IV. REFLEXIÓN CRÍTICA DE LA EXPERIENCIA

Inicialmente se buscó una imagen docker donde TheHive se encuentre instalado y configurado, se encontró imágenes de TheHive de versiones muy antiguas y estas eran inestables causando errores al momento de su ejecución por lo que se optó por una instalación y configuración desde cero.

Para la implementación de TheHive en la una cuenta de prueba se utilizó la documentación oficial de su sitio web, pero está no contenía información detallada sobre la implementación por lo que se investigó en otras fuentes de información y basándose en la experiencia del autor se logró concluir la instalación y configuración de TheHive.

Gracias a este proyecto el autor reforzó y actualizo su conocimiento de las soluciones en nube en especial de AWS ampliando los conocimientos sobre Amazon EC2, generando servidores virtuales y aprendiendo una nueva modalidad para conectarse a ellos, ya que habitualmente la conexión lo realizaba por medio de SSH con la herramienta Putty la cual se tiene que configurar y generar Key RSA para la conexión.

Referente a lo desarrollado durante el proyecto me siento grato al haber adquirido mayor experiencia y conocimientos sobre el avance de las soluciones en nube.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- De acuerdo con el objetivo general, se implementó un sistema para la gestión de registro de incidentes de seguridad digital del Centro Nacional de Seguridad Digital del Perú.
- De acuerdo al primer objetivo específico, se tiene un seguimiento del ciclo de vida de los incidentes tecnológicos registrados, permitiéndonos llevar un control y monitoreo adecuado debido a la implementación del sistema TheHive.
- De acuerdo al segundo objetivo específico, se puede clasificar los incidentes de acuerdo a su criticidad.

5.2 Recomendaciones

- Se recomienda realizar la Integración con MISP para garantizar las investigaciones de eventos.
- Realizar la integración con Cortex para utilizarlo como un motor de análisis por medio de los observables.
- Se recomienda estar pendiente de futuras actualizaciones que tenga TheHive para un mejor rendimiento y desempeño de la herramienta implementada.

- Se recomienda estar pendiente sobre futuras integraciones con TheHive a través de su página oficial para aprovechar los beneficios de estas integraciones.

5.3 Fuentes De Información

Plataforma digital única del Estado peruano, PCM. (2022). Organigrama de la PCM, recuperado de <https://www.gob.pe/institucion/pcm/informes-publicaciones/2078344-organigrama-institucional>

Davy Preuveneers y Wouter Joosen (2021, 18 de enero). The use of the multi-criteria AHP method to select a cloud computing provider, recuperado de <https://www.mdpi.com/2624-800X/1/1/8>

Department of Software Engineering, Firat University, Elazig, Turkey (2019, 10 de junio). Advantages to Disadvantages of Cloud Computing for Small-Sized Business, recuperado de <https://ieeexplore.ieee.org/abstract/document/8757549>

Piotr Niemcewicz (2021, 1 de octubre). The use of the multi-criteria AHP method to select a cloud computing provider, recuperado de <https://www.sciencedirect.com/science/article/pii/S1877050921017622>

Sourav Mukherjee (2019, 18 de marzo). Benefits of AWS in Modern Cloud, recuperado de <https://arxiv.org/abs/1903.03219>

Proofpoint (2022). State of the Phish, An in-depth look at user awareness, vulnerability and resilience, recuperado de https://www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf

Idtheftcenter (2020). Identity Theft Resource Center®'s Annual End-of-Year Data

Breach Report Reveals 17 Percent Increase in Breaches over 2018, recuperado de <https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/>

Anand Groenewegen y Joris Shuko Janssen (2021, 21 de julio). TheHive Project: The maturity of an open-source Security Incident Response platform, recuperado de https://www.researchgate.net/profile/Anand-Groenewegen/publication/352715439_TheHive_Project_The_maturity_of_an_open-source_Security_Incident_Response_platform/links/60ec1014b8c0d5588cef0c92/TheHive-Project-The-maturity-of-an-open-source-Security-Incident-Response-platform.pdf

María Salas Zárate y Luis Colombo Mendoza (2011, 17 de octubre). Cloud Computing: A Review Of Paas, Iaas, Saas Services And Providers, recuperado de <https://dialnet.unirioja.es/servlet/articulo?codigo=4490150>

Thehive-project (2022), TheHive Project Documentation, recuperado de <https://docs.thehive-project.org/thehive/installation-and-configuration/>

Amazon Web Service (2022). AWS Pricing Calculator, recuperado de <https://calculator.aws/#/createCalculator/EC2>

5.4 Glosario

- Security Incident Response (SIR), Respuesta a Incidentes de Seguridad.
- Security Incident Response Platform (SIRP), Plataforma diseñada para procesar incidentes de seguridad de forma eficiente y centralizada.
- Malware Information Sharing Platform (MISP), Plataforma de inteligencia contra amenazas.

- Security Information and Event Management (SIEM), Gestión de Información y Eventos de Seguridad.
- Security Orchestration, Automation and Response (SOAR), Orquestación, Automatización y Respuesta de Seguridad
- Indicators of Compromises (IoC), Indicadores de compromiso, son uno o más observables que potencialmente forman un patrón que podría indicar una intrusión.
- Computer Emergency Response Team (CERT), Equipo de respuestas de emergencias informáticas.
- Computer Emergency Response Team (CSIRT), Equipo de respuestas a incidentes informáticas.