

## Ampliación de Red y Seguridad para el I.E.S El Rincón

# Proyecto **Final de Ciclo**

Javier Henríquez Santana

# ÍNDICE

<b>Resumen.....</b>	<b>3</b>
<b>INTRODUCCIÓN.....</b>	<b>4</b>
Introducción a la cuestión.....	4
Objeto de Estudio y Justificación.....	5
Importancia del proyecto.....	5
La Red y su importancia.....	5
La Ciberseguridad en la Actualidad.....	6
Objetivos Principales.....	8
Objetivos Secundarios.....	9
Estructura de la Memoria.....	9
<b>Estado de la Cuestión.....</b>	<b>10</b>
<b>MARCO TEÓRICO.....</b>	<b>11</b>
HERRAMIENTAS UTILIZADAS.....	11
Cisco Packet Tracer.....	11
VirtualBox.....	12
Docker.....	13
Moodle.....	14
Proxy Squid.....	16
Wazuh - SIEM.....	17
<b>DISEÑO DE LA INVESTIGACIÓN Y METODOLOGÍA.....</b>	<b>18</b>
Metodología.....	20
1.0 Topología.....	20
1.1 Dispositivos a utilizar.....	21
2.0 Virtualización de Equipos.....	23
2.1 SERVIDOR MOODLE - PROXY.....	23
2.2 Configuración del Servidor.....	23
2.3 Servidor Router.....	24
2.4 Configuración en Modo Router.....	25
2.5 NAT MASQUERADE.....	25
2.6 Equipos de los Profesores y Alumnos.....	26
2.7 CONFIGURACIÓN MÁQUINAS VIRTUALES CLIENTES EN VIRTUALBOX.....	26
2.8 Comprobación de Conectividad a Internet.....	27
- 3.0 Configuración de Servicios.....	28
3.1 Moodle en Docker.....	28
3.2 INSTALACIÓN DE MOODLE.....	28
3.3 Configuración Moodle.....	29
3.3.1 CATEGORÍAS.....	29
3.3.2 Asignaturas.....	29
3.3.3 Usuarios.....	29
3.3.4 MATRICULAR ALUMNOS EN ASIGNATURAS.....	30
3.4 Comprobación de Uso.....	30
- 4.0 Servidor Proxy Squid.....	31
4.1 Configuración del Servidor Squid.....	31
4.2 CONFIGURACIÓN CLIENTES.....	32

4.3 Comprobación del funcionamiento del Servicio.....	32
- 5.0 Implementación del SIEM - Wazuh.....	33
5.1 Habilitar Detección de Vulnerabilidades.....	34
5.2 Integración de VirusTotal en Wazuh.....	34
<b>CONCLUSIONES.....</b>	<b>36</b>
<b>LIMITACIONES DEL ESTUDIO Y FUTURAS LÍNEAS DE INVESTIGACIÓN.....</b>	<b>37</b>
<b>Anexos.....</b>	<b>39</b>
Anexo I.....	39
Anexo II.....	43
Anexo III.....	55
Anexo IV.....	67
Anexo V.....	74

## Resumen

Como empresa se nos contrata para abordar un proyecto para el I.E.S El Rincón. Este proyecto se basará en que el instituto, debido a la amplia demanda para ingresar en los estudios de ciclo formativo de la rama de informática, tiene que realizar una **ampliación del centro en dos clases** nuevas que deberán estar debidamente preparadas y configuradas para su uso.

Primeramente, se llevará a cabo una **topología de red** para poder llevar a cabo la posterior instalación y configuración de los dispositivos necesarios para que cada clase funcione correctamente. Además, se



recomendarán dispositivos los cuales puedan encajar en el proyecto debido a sus capacidades y especificaciones. Además, se creará un espacio dedicado para un rack el cual alojará un servidor de **alta disponibilidad**.

A través de la virtualización, se simularán los equipos físicos de la topología anterior para su posterior instalación en un entorno real. Cada clase nueva tendrá una red para cada una. Para la simulación se **virtualizarán** siete ordenadores, es decir; dos equipos para cada uno de los profesores en cada aula, cuatro alumnos (dos por cada red), un servidor y un router.

Se configurará el servidor para que aloje una **Moodle** a través de contenedores de **Docker**. Esta Moodle será de índole educativa la cual simulará un entorno real donde cada clase tendrá su entorno dependiendo de qué curso se imparte en ella. Además, la Moodle estará configurada para que existan usuarios profesores y usuarios alumnos. Estos usuarios tendrán acceso a través de contraseñas las cuales seguirán unos estándares del **INCIBE** (Instituto Nacional de Ciberseguridad) para la creación de **contraseñas seguras**.

En este servidor también se aloja un **PROXY** el cual nos servirá para impedir que los usuarios de la red puedan acceder a ciertas páginas web que puedan contener contenido sexual o que puedan ser maliciosas.

Finalmente, se instalará un **SIEM** (Security Information Event Management) el cual servirá para que el administrador de la red del centro pueda monitorizar los eventos que ocurran en esta misma red. Se integrarán algunas herramientas a este **SIEM** para hacer la red más segura.

## INTRODUCCIÓN

### Introducción a la cuestión

La presente memoria detalla un proyecto integral destinado a **abordar las necesidades de expansión tecnológica** del Instituto de Educación Secundaria El Rincón. La creciente demanda de estudiantes interesados en los programas de informática ha generado la necesidad de ampliar la infraestructura tecnológica del centro. En respuesta a este desafío, se propone un proyecto que incluye la creación de dos nuevas aulas completamente equipadas y configuradas para su uso, así como la implementación de una serie de soluciones tecnológicas para **mejorar la educación y la seguridad** en el centro.

### Objeto de Estudio y Justificación

El objeto de estudio de este proyecto es proporcionar al Instituto El Rincón una **infraestructura tecnológica moderna** y funcional que satisfaga las demandas educativas y de seguridad de la comunidad escolar. La ampliación de las aulas y la implementación de soluciones como **Moodle**, un **servidor proxy** y un **SIEM** son fundamentales para mejorar la calidad de la educación y garantizar un entorno digital seguro para estudiantes y profesores.

La justificación de este proyecto radica en la necesidad de **adaptar la infraestructura tecnológica del Instituto** El Rincón a las demandas actuales de la educación digital. La

creación de nuevas aulas equipadas con tecnología avanzada y la implementación de plataformas educativas y herramientas de seguridad contribuirán significativamente a mejorar el proceso de enseñanza-aprendizaje y a proteger la integridad de la red escolar.

## Importancia del proyecto

La Red y su importancia.

La importancia de tener una red bien segmentada, configurada y la relevancia de hospedar su propio servidor radica en varios factores críticos que afectan la seguridad, eficiencia y control sobre la infraestructura de TI de una organización.

En primer lugar, la segmentación de red es fundamental para garantizar la seguridad de los datos y la protección contra posibles ataques cibernéticos. Al dividir la red en segmentos más pequeños o subredes, se pueden aplicar políticas de seguridad específicas a cada segmento, limitando el alcance de posibles brechas de seguridad y mitigando el impacto de ataques internos o externos. Esto ayuda a prevenir la propagación de amenazas y a proteger datos sensibles y críticos para la organización.

Además, una red bien segmentada facilita la administración y el monitoreo de la red, ya que permite una mejor organización y gestión de los recursos de red. Los equipos y servicios pueden agruparse en segmentos lógicos según su función o departamento, lo que simplifica la administración y facilita la identificación y resolución de problemas.

Por otro lado, la configuración adecuada de la red es esencial para garantizar su rendimiento, disponibilidad y confiabilidad. Esto incluye la optimización de la configuración de los dispositivos de red, como routers, switches y firewalls, para garantizar un flujo de datos eficiente y minimizar los tiempos de inactividad. Una configuración adecuada también implica la implementación de políticas de calidad de servicio (QoS) para priorizar el tráfico crítico y garantizar un rendimiento óptimo de las aplicaciones y servicios.

Además de la seguridad y el rendimiento, la decisión de hospedar su propio servidor ofrece una serie de beneficios adicionales. Al alojar su propio servidor, la organización tiene un mayor control sobre sus datos y aplicaciones, lo que le permite personalizar y adaptar el

entorno de servidor según sus necesidades específicas. Esto también proporciona una mayor flexibilidad y escalabilidad, ya que la organización puede agregar o modificar recursos según sea necesario sin depender de terceros proveedores de servicios.

Además, alojar su propio servidor puede resultar más económico a largo plazo, ya que elimina la necesidad de pagar tarifas de suscripción mensuales o anuales a proveedores de servicios en la nube u otros proveedores de alojamiento. Si bien puede requerir una inversión inicial en infraestructura y recursos, a largo plazo puede resultar en ahorros significativos y un mayor retorno de la inversión.

En resumen, tener una red bien segmentada, configurada y hospedar su propio servidor son elementos fundamentales para garantizar la seguridad, eficiencia y control sobre la infraestructura de TI de una organización. Estas prácticas no solo protegen los datos y los activos de la organización, sino que también proporcionan flexibilidad, escalabilidad y control sobre los recursos de red y de servidor.

## La Ciberseguridad en la Actualidad

La **importancia** de la **ciberseguridad** en la actualidad es **indiscutible**, ya que vivimos en una era digital donde la información y los sistemas tecnológicos son fundamentales para el funcionamiento de prácticamente todas las organizaciones y actividades de la vida cotidiana. La ciberseguridad se refiere al conjunto de prácticas, herramientas y medidas diseñadas para proteger los sistemas informáticos, redes, datos y dispositivos contra amenazas cibernéticas como virus, malware, ataques de hackers, robo de datos y otros riesgos relacionados con la seguridad en línea.

En el contexto de los entornos educativos, la **ciberseguridad** adquiere una importancia aún mayor debido a varios factores específicos:

- 1. Protección de datos sensibles:** Los entornos educativos manejan una gran cantidad de datos sensibles, incluida la información personal y académica de estudiantes y profesores, registros financieros, planes de estudio, materiales de enseñanza y más. Es fundamental proteger esta información para garantizar la privacidad, confidencialidad e integridad de los datos.

**2. Continuidad del aprendizaje:** En la era digital, gran parte del proceso de aprendizaje se ha trasladado a entornos en línea y plataformas educativas. La interrupción de estos sistemas debido a un ataque cibernético podría afectar gravemente la continuidad del aprendizaje de los estudiantes y tener un impacto negativo en su educación.

**3. Seguridad de las infraestructuras tecnológicas:** Los centros educativos dependen cada vez más de infraestructuras tecnológicas como redes de computadoras, servidores, sistemas de gestión de aprendizaje (LMS), sistemas de gestión de la información estudiantil (SIS) y otros sistemas críticos. Garantizar la seguridad de estas infraestructuras es esencial para proteger la disponibilidad, integridad y confidencialidad de los recursos tecnológicos.

**4. Protección contra amenazas emergentes:** El panorama de amenazas cibernéticas está en constante evolución, con nuevos tipos de malware, técnicas de ataque y vulnerabilidades que surgen regularmente. Los entornos educativos deben estar preparados para hacer frente a estas amenazas emergentes y adoptar medidas proactivas para protegerse contra ellas.

**5. Educación en ciberseguridad:** Además de proteger los sistemas y datos, es importante educar a estudiantes, profesores y personal administrativo sobre las mejores prácticas de seguridad en línea y concientizar sobre los riesgos asociados con el uso de la tecnología. La educación en ciberseguridad puede ayudar a prevenir incidentes de seguridad y promover un entorno en línea seguro y saludable.

La **ciberseguridad** es un aspecto crucial en los entornos educativos debido a la naturaleza sensible de los datos manejados, la dependencia de las infraestructuras tecnológicas y la necesidad de garantizar la continuidad del aprendizaje. Al adoptar medidas de seguridad adecuadas y promover la conciencia sobre la ciberseguridad, los centros educativos pueden proteger sus activos digitales y proporcionar un entorno en línea seguro y protegido para estudiantes, profesores y personal administrativo.

## Objetivos Principales

Estos son los objetivos principales del proyecto:

- Crear dos nuevas aulas completamente equipadas y configuradas para su uso, que cumplan con los estándares de tecnología educativa y seguridad.
- Diseñar e implementar una topología de red adecuada que garantice un funcionamiento óptimo de los dispositivos y servicios tecnológicos en el Instituto El Rincón.
- Virtualizar los equipos físicos necesarios para las nuevas aulas, utilizando tecnología de virtualización para optimizar recursos y flexibilidad.
- Configurar un servidor Moodle para proporcionar un entorno educativo interactivo y personalizado para estudiantes y profesores.
- Implementar un servidor proxy para controlar y filtrar el acceso a Internet, garantizando un entorno seguro y protegido para los usuarios de la red.
- Instalar un sistema SIEM para monitorear y gestionar eventos de seguridad en la red del Instituto El Rincón, fortaleciendo la seguridad cibernética del centro.

## Objetivos Secundarios

- Capacitar al personal del Instituto El Rincón en el uso y mantenimiento de la nueva infraestructura tecnológica.
- Establecer políticas de seguridad de la información y protocolos de respuesta a incidentes para proteger la red escolar contra amenazas cibernéticas.
- Evaluar el impacto del proyecto en el proceso de enseñanza-aprendizaje y en la productividad del personal docente y administrativo.
- Proporcionar soporte técnico continuo y mantenimiento preventivo para garantizar el rendimiento óptimo de la infraestructura tecnológica a lo largo del tiempo.

## Estructura de la Memoria

La **memoria** del proyecto está estructurada de la siguiente manera:

- **Introducción:** Presentación del proyecto, objeto de estudio, justificación, objetivos y estructura de la memoria.
- **Análisis de Requisitos:** Descripción detallada de los requisitos técnicos, educativos y de seguridad del proyecto.
- **Diseño de la Solución:** Propuesta de diseño para las nuevas aulas, topología de red, configuración de servidores y sistemas de seguridad.
- **Implementación:** Detalle de las etapas de implementación del proyecto, incluyendo la instalación de equipos, configuración de software y pruebas de funcionamiento.
- **Resultados y Conclusiones:** Evaluación de los resultados obtenidos y conclusiones sobre el impacto del proyecto en el Instituto El Rincón.
- **Recomendaciones y Futuras Mejoras:** Sugerencias para futuras mejoras y recomendaciones para mantener y actualizar la infraestructura tecnológica del centro.

## Estado de la Cuestión

En el marco del desarrollo del presente proyecto, es relevante contextualizarlo dentro del entorno educativo y las prácticas realizadas en el ciclo formativo de Administración de Sistemas Informáticos en Red. Se han integrado conocimientos adquiridos en diversas asignaturas, las cuales han contribuido significativamente al desarrollo y ejecución de este proyecto.

Las prácticas realizadas en clase han proporcionado una base sólida de conocimientos y habilidades técnicas necesarias para abordar los desafíos planteados en el proyecto. Estas prácticas abarcan una variedad de temas, como configuración de redes, virtualización,

administración de sistemas operativos, seguridad informática y gestión de servicios en entornos empresariales.

En particular, las prácticas relacionadas con la configuración de redes y la planificación de topologías han sido fundamentales para diseñar la infraestructura de red del proyecto. Se han aplicado conceptos de segmentación de redes, direccionamiento IP, configuración de routers y switches, así como la implementación de servicios de red como DHCP y DNS.

La **virtualización** ha desempeñado un papel crucial en la simulación de la infraestructura de red propuesta. Mediante el uso de herramientas como **Cisco Packet Tracer** y software de virtualización como **VirtualBox**, se han creado entornos virtuales para probar y validar la configuración de los dispositivos de red y servidores antes de su implementación en un entorno real.

Asimismo, las prácticas relacionadas con la administración de sistemas operativos, especialmente en entornos basados en Linux como **Ubuntu Server**, han sido de gran utilidad para configurar y gestionar los servidores que forman parte de la infraestructura del proyecto. Se han adquirido habilidades en la instalación y configuración de servicios como **Apache**, **MySQL**, **Docker**, **Squid Proxy**, entre otros.

En el ámbito de la **seguridad informática**, se han realizado prácticas enfocadas en la implementación de medidas de seguridad para proteger la red y los sistemas contra amenazas cibernéticas. Se han explorado técnicas de **filtrado de contenido web**, detección de intrusiones y gestión de eventos de seguridad mediante herramientas como Suricata y **Wazuh**.

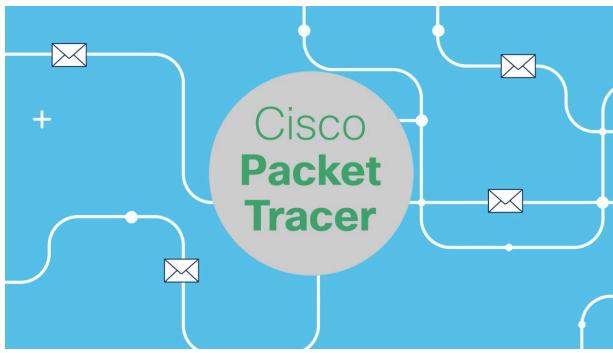
## MARCO TEÓRICO

## HERRAMIENTAS UTILIZADAS

### Cisco Packet Tracer

He utilizado la herramienta Cisco Packet Tracer para diseñar y simular las topologías de red requeridas en el proyecto. Con esta herramienta, he podido crear entornos virtuales que representan la infraestructura de red del Instituto El Rincón, incluyendo routers, switches, servidores y estaciones de trabajo. Esto me ha permitido simular el funcionamiento de la red

y validar la configuración antes de implementarla en un entorno real. Cisco Packet Tracer ha sido una herramienta invaluable para visualizar y probar las soluciones de red propuestas en el proyecto.



### ¿Qué es Cisco Packet Tracer y para qué sirve?

Cisco Packet Tracer es una herramienta de simulación de redes desarrollada por Cisco Systems. Está diseñada para permitir a los estudiantes y profesionales de redes diseñar, configurar y solucionar problemas de redes informáticas de manera virtual. Algunas de sus **características** principales incluyen:

- **Simulación de dispositivos de red:** Permite simular una amplia gama de dispositivos de red, incluidos routers, switches, PCs, servidores y dispositivos IoT.
- **Creación de topologías:** Los usuarios pueden crear y configurar topologías de red complejas para simular entornos de red del mundo real.
- **Configuración de dispositivos:** Permite configurar parámetros de dispositivos de red, como direcciones IP, enrutamiento, VLANs, seguridad, entre otros.
- **Análisis y solución de problemas:** Proporciona herramientas para analizar el tráfico de red, detectar problemas y solucionarlos.
- **Entorno de aprendizaje interactivo:** Ofrece actividades y laboratorios interactivos que ayudan a los estudiantes a comprender los conceptos de redes y a desarrollar habilidades prácticas.

## VirtualBox

Para la simulación de los equipos y la creación de entornos virtuales, he utilizado **VirtualBox**, una plataforma de virtualización de software que permite crear y ejecutar máquinas virtuales en un sistema operativo host. Con VirtualBox, pude crear múltiples máquinas virtuales para representar los diferentes dispositivos de la red, como servidores, routers y equipos de usuario. Esto me permitió probar configuraciones de red, software y servicios sin afectar a mi sistema operativo principal. Además, VirtualBox ofrece una **interfaz intuitiva** y herramientas de gestión que facilitaron la configuración y el control de las máquinas virtuales, lo que resultó fundamental para el desarrollo y la implementación del proyecto.



### ¿Qué es VirtualBox y para qué sirve?

VirtualBox es una plataforma de virtualización de software que permite a los usuarios crear y ejecutar máquinas virtuales en sus sistemas operativos host. Algunas de las **ventajas y usos principales** de VirtualBox son:

- **Virtualización de Sistemas Operativos:** VirtualBox permite crear máquinas virtuales que ejecutan sistemas operativos completos dentro de un entorno virtualizado. Esto es útil para probar diferentes sistemas operativos, configuraciones de red y software sin afectar al sistema operativo principal del host.
- **Entrenamiento y Aprendizaje:** VirtualBox es una herramienta útil para estudiantes y profesionales que desean aprender sobre sistemas operativos y redes informáticas. Permite crear entornos virtuales para practicar y experimentar sin riesgo de dañar equipos reales.

- **Portabilidad:** Las máquinas virtuales creadas en VirtualBox son archivos independientes que se pueden transferir y ejecutar en diferentes sistemas host que tengan instalado VirtualBox. Esto facilita la portabilidad y la distribución de entornos de desarrollo y aplicaciones.

## Docker

He utilizado la tecnología **Docker** para desplegar los distintos servicios requeridos en el proyecto, como Moodle. Docker me ha permitido **encapsular** cada servicio en contenedores virtuales, lo que facilita su distribución, implementación y gestión. Con Docker, he podido crear entornos aislados para cada servicio, lo que garantiza la independencia y la portabilidad de las aplicaciones. Además, Docker ofrece una forma sencilla de gestionar los recursos y las dependencias de cada servicio, lo que simplifica el proceso de despliegue y mantenimiento de la infraestructura de red. En resumen, Docker ha sido una herramienta fundamental para implementar de manera eficiente y escalable los servicios necesarios en la red del Instituto El Rincón.



### ¿Qué es Docker y para qué sirve?

**Docker** es una plataforma de **código abierto** que permite a los desarrolladores **empaquetar, distribuir y ejecutar** aplicaciones en contenedores. Aquí hay un resumen de sus **características** principales:

- **Contenedores:** Docker utiliza contenedores para encapsular aplicaciones y todas sus dependencias, lo que permite que se ejecuten de manera consistente en cualquier entorno.
- **Portabilidad:** Los contenedores Docker son portátiles y pueden ejecutarse en cualquier sistema operativo que admita Docker, lo que facilita la migración de aplicaciones entre entornos de desarrollo, pruebas y producción.

- **Eficiencia:** Los contenedores Docker comparten el mismo kernel del sistema operativo del host, lo que los hace más ligeros y eficientes en términos de recursos que las máquinas virtuales tradicionales.
- **Construcción rápida:** Docker utiliza un sistema de imágenes y capas para construir contenedores, lo que permite la creación rápida y eficiente de entornos de desarrollo y pruebas.
- **Gestión de imágenes:** Docker proporciona un registro público y privado de imágenes que permite a los desarrolladores compartir y distribuir fácilmente sus aplicaciones y servicios.
- **Orquestación de contenedores:** Docker Swarm y Kubernetes son herramientas populares para orquestar y gestionar contenedores en clústeres de servidores, lo que permite escalar y gestionar aplicaciones de manera eficiente

## Moodle

He utilizado **Moodle** para simular un entorno educativo en el proyecto, configurando dos cursos que reflejan el contenido y las actividades que se impartirán en las nuevas clases del **Instituto El Rincón**. Moodle proporciona una plataforma flexible y robusta para la gestión del aprendizaje en línea, lo que ha permitido diseñar y organizar los cursos de manera eficiente. Mediante Moodle, se han creado **entornos virtuales interactivos** donde los usuarios, tanto profesores como alumnos, pueden acceder a materiales educativos, participar en actividades y realizar evaluaciones. La configuración de dos cursos en Moodle representa la oferta educativa que se ofrecerá en las nuevas clases del instituto, brindando una experiencia de aprendizaje en línea completa y personalizada.

### ¿Qué es Moodle y para qué sirve?

**Moodle** es una plataforma de aprendizaje en línea de código abierto que ofrece una amplia gama de herramientas y recursos para la creación, gestión y entrega de cursos en línea. Aquí hay un resumen de sus características principales:

- **Gestión de cursos:** Moodle permite a los educadores crear cursos en línea con una variedad de recursos multimedia, actividades interactivas y herramientas de evaluación.
- **Personalización:** Los educadores pueden personalizar fácilmente la apariencia y el contenido de sus cursos para adaptarse a las necesidades específicas de sus estudiantes.
- **Interactividad:** Moodle ofrece una amplia gama de actividades interactivas, como foros de discusión, tareas, cuestionarios, wikis y encuestas, que fomentan la participación y el compromiso de los estudiantes.
- **Evaluación:** Los educadores pueden crear cuestionarios y exámenes en línea, realizar un seguimiento del progreso del estudiante y generar informes detallados sobre el rendimiento del curso.
- **Colaboración:** Moodle facilita la colaboración entre estudiantes y profesores a través de herramientas de comunicación, como mensajes privados, salas de chat y grupos de trabajo.
- **Accesibilidad:** Moodle cumple con los estándares de accesibilidad web y ofrece opciones de personalización para adaptarse a las necesidades de los estudiantes con discapacidades.
- **Comunidad y soporte:** Moodle cuenta con una gran comunidad de usuarios y desarrolladores que ofrecen soporte técnico, recursos de aprendizaje y complementos adicionales para ampliar las funcionalidades de la plataforma.



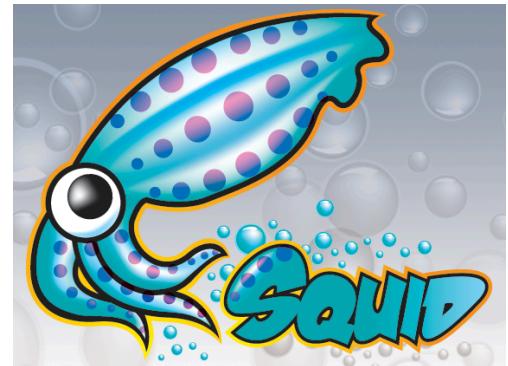
### Proxy Squid

En el proyecto, he implementado el servicio de **proxy Squid** para mejorar la **seguridad** y el **control del acceso** a Internet en la red del Instituto El Rincón. Squid se ha configurado con un archivo que contiene una lista de dominios recomendados por la comunidad para su no

visita, lo que permite bloquear el acceso a sitios web no deseados o potencialmente peligrosos. Esta medida contribuye a promover un entorno de navegación seguro y protegido para los usuarios de la red, evitando el acceso a contenido inapropiado o malicioso. Squid actúa como una capa adicional de seguridad al filtrar las solicitudes de los usuarios y bloquear el acceso a los dominios incluidos en la lista, garantizando así un ambiente de trabajo más seguro y productivo.

## ¿Qué es y para qué sirve?

**Squid** es un servidor proxy de **código abierto** y una herramienta de caché web que ofrece una serie de características importantes para mejorar el rendimiento y la seguridad en entornos de red. Aquí hay un resumen de sus características principales:



- **Caché web:** Squid almacena copias locales de las páginas web solicitadas por los clientes, lo que permite acelerar los tiempos de carga y reducir el ancho de banda utilizado para acceder a sitios web populares y recurrentes.
- **Control de acceso:** Squid proporciona una amplia gama de opciones de control de acceso para restringir el acceso a sitios web específicos, basándose en direcciones IP, nombres de dominio, encabezados HTTP y otros criterios.
- **Filtrado de contenido:** Squid puede filtrar el tráfico web para bloquear o permitir el acceso a ciertos tipos de contenido, como sitios web maliciosos, contenido para adultos o descargas de archivos específicos.
- **Autenticación de usuarios:** Squid puede integrarse con sistemas de autenticación externos, como LDAP, Active Directory o bases de datos SQL, para autenticar a los usuarios antes de permitirles acceder a Internet a través del proxy.
- **Registro y monitoreo:** Squid registra todas las solicitudes y respuestas de tráfico web, lo que permite a los administradores monitorear y analizar el uso de Internet, identificar posibles problemas de seguridad y cumplir con los requisitos de auditoría.

- **Balanceo de carga:** Squid puede distribuir el tráfico web entrante entre varios servidores proxy para mejorar el rendimiento y la disponibilidad del servicio.
- **SSL/TLS:** Squid puede actuar como un intermediario SSL/TLS para cifrar el tráfico web entre los clientes y los servidores de destino, proporcionando así una capa adicional de seguridad y privacidad.

## Wazuh - SIEM

Se ha integrado una herramienta **SIEM** (Security Information and Event Management) llamada Wazuh para **fortalecer la seguridad y la monitorización de la red del Instituto El Rincón**. Wazuh proporciona capacidades avanzadas de detección de amenazas, análisis de logs y gestión de incidentes, lo que permite identificar y responder de manera proactiva a posibles amenazas y vulnerabilidades en la red. Además, he integrado una API llamada VirusTotal, la cual escanea los archivos descargados de Internet en busca de posibles amenazas y los elimina automáticamente si se detecta que son maliciosos. Esta integración añade una capa adicional de protección contra malware y ataques cibernéticos, garantizando así la seguridad e integridad de los sistemas informáticos del instituto.

### ¿Qué es Wazuh y para qué sirve?

**Wazuh SIEM** (Security Information and Event Management) es una plataforma de código abierto diseñada para proporcionar una visión completa de la seguridad de la red y la infraestructura de TI. Esta herramienta combina la funcionalidad de detección de amenazas, análisis de logs, gestión de incidentes y correlación de eventos para ofrecer una solución integral de seguridad.



Entre sus **características** principales, **Wazuh SIEM** ofrece:

- **Detección avanzada de amenazas:** Utiliza reglas predefinidas y personalizables para detectar actividades sospechosas y amenazas en tiempo real.

- **Análisis de logs y eventos:** Recopila, normaliza y analiza logs y eventos de sistemas, aplicaciones y dispositivos en toda la red.
- **Gestión de incidentes:** Facilita la gestión y respuesta a incidentes de seguridad de manera eficiente, permitiendo una rápida acción ante posibles amenazas.
- **Correlación de eventos:** Identifica relaciones entre eventos aparentemente no relacionados para detectar patrones de comportamiento malicioso.
- **Integración con fuentes de inteligencia de amenazas:** Se integra con fuentes de inteligencia de amenazas externas para enriquecer la detección de amenazas.

## DISEÑO DE LA INVESTIGACIÓN Y METODOLOGÍA

El diseño de la investigación y metodología es una etapa crucial en cualquier proyecto, ya que define cómo se llevará a cabo el trabajo, qué pasos se seguirán y qué herramientas y técnicas se utilizarán. En el caso del proyecto para el I.E.S El Rincón, se han definido varias fases y procesos que permitirán alcanzar los objetivos establecidos de manera eficiente y efectiva.

**Definición de Metodología:** Se ha optado por una metodología de trabajo basada en la planificación detallada de cada fase del proyecto, la utilización de herramientas y técnicas específicas, y la asignación de recursos adecuados para cada tarea.

### Fases del Proyecto:

- 1. **Planificación Inicial:** En esta fase se establecieron los objetivos del proyecto, se definieron los requisitos y se elaboró un plan detallado de trabajo.
- 2. **Diseño de la Topología de Red:** Se llevó a cabo la planificación de la topología de red, considerando las necesidades específicas del centro educativo y la distribución de los dispositivos.
- 3. **Virtualización de Equipos:** Se procedió a la virtualización de los equipos físicos, simulando el entorno de red en un entorno virtual para su posterior implementación.
- 4. **Configuración de Servicios:** Se configuraron los servicios necesarios, como el servidor Moodle, el proxy Squid y el SIEM Wazuh, siguiendo las mejores prácticas de seguridad y rendimiento.

- **5. Pruebas y Validación:** Se realizaron pruebas exhaustivas para validar el funcionamiento correcto de los servicios configurados y asegurar la estabilidad y seguridad del entorno.
- **6. Documentación:** Se elaboró documentación detallada de todo el proceso, incluyendo manuales de usuario, informes de pruebas y procedimientos de mantenimiento.
- **7. Propuesta y Planificación:** Se propuso un plan detallado para la ejecución del proyecto, definiendo los plazos, recursos y responsabilidades de cada miembro del equipo. Se establecieron hitos importantes para medir el progreso y asegurar el cumplimiento de los objetivos.
- **8. Materiales y Herramientas:** Se utilizaron diversos materiales y herramientas durante la ejecución del proyecto, como software de virtualización, contenedores Docker, herramientas de configuración de red, entre otros.
- **9. Técnicas y Métodos:** Se aplicaron técnicas de planificación de proyectos, virtualización de redes, configuración de servicios, pruebas de rendimiento y seguridad, así como métodos de documentación y seguimiento.
- **10. Muestra:** La muestra del estudio consistió en el centro educativo I.E.S El Rincón, donde se implementaron las soluciones propuestas para la ampliación y mejora de la infraestructura de red y servicios.

## Metodología

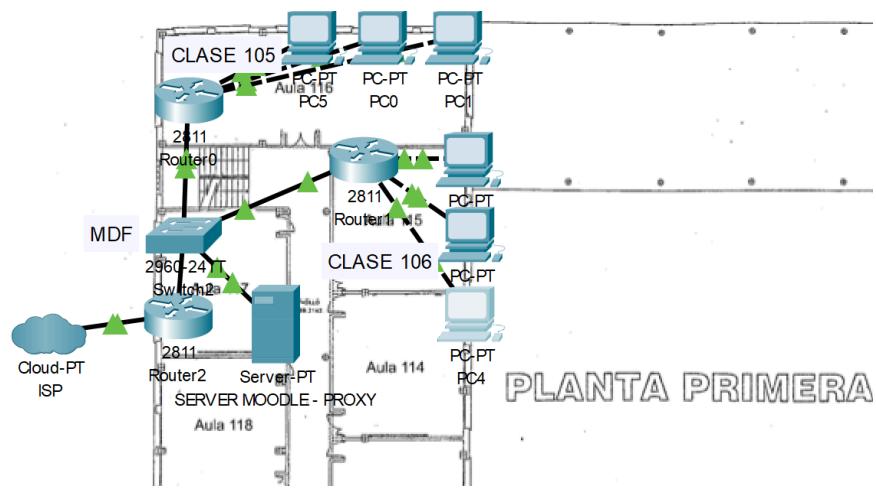
### 1.0 Diseño de la topología de red.

La planificación de la topología de red constituyó un paso crucial en el desarrollo del proyecto, ya que permitió establecer las bases para la posterior implementación y configuración de la infraestructura tecnológica en el **I.E.S El Rincón**. En esta fase, se consideraron detalladamente las necesidades específicas del centro educativo, así como la distribución óptima de los dispositivos para garantizar un funcionamiento eficiente y fiable de la red.

Se llevaron a cabo análisis exhaustivos para determinar la disposición de los equipos, la conectividad entre ellos y la segmentación de la red en redes adecuadas. Se tuvo en cuenta la ubicación de las nuevas clases, los requerimientos de conectividad de los profesores y alumnos, así como la integración de servicios adicionales como servidores y routers.

La topología de red diseñada se caracterizó por su **escalabilidad, flexibilidad y seguridad**, aspectos fundamentales para satisfacer las demandas de un entorno educativo en constante evolución. Se emplearon herramientas de modelado y simulación para visualizar y validar la configuración propuesta, asegurando su viabilidad y optimización.

# Topología Física



Como topología de red física tenemos la siguiente representación.

Como podemos observar en la imagen, cada una de las clases se encuentra en una red distinta. ¿estos qué ventajas nos aporta?

El hecho de tener cada clase en una red distinta ofrece varias ventajas en términos de seguridad, rendimiento y administración de la red. Algunas de estas ventajas son:

- **Seguridad:** Al separar cada clase en redes distintas, se limita la visibilidad y accesibilidad entre ellas. Esto significa que los dispositivos y recursos de una clase no están directamente expuestos a los dispositivos de otra clase, lo que reduce el riesgo de accesos no autorizados y la propagación de amenazas de seguridad.
  - **Control de tráfico:** Al segmentar la red en subredes separadas para cada clase, se puede gestionar de manera más efectiva el tráfico de red. Esto permite priorizar

certos tipos de tráfico, aplicar políticas de acceso específicas y optimizar el rendimiento de la red para cada entorno de clase.

- **Rendimiento:** Al distribuir el tráfico de red en redes separadas, se evita la congestión de la red que puede ocurrir cuando se comparten recursos entre múltiples clases. Esto garantiza un rendimiento óptimo de la red para cada grupo de usuarios y aplicaciones.
- **Facilidad de administración:** Al tener cada clase en una red separada, se simplifica la administración y la resolución de problemas de red. Los administradores pueden gestionar y monitorear cada red de manera independiente, lo que facilita la identificación y solución de problemas específicos de cada entorno de clase.

### **Dispositivos a utilizar**

Para una topología de red en un instituto, la marca Cisco ofrece una amplia gama de routers y switches que pueden adaptarse a diferentes necesidades y tamaños de red. Aquí te recomendaré algunos modelos que podrían ser adecuados dependiendo del tamaño y la complejidad de la red del instituto:

#### **Router Cisco elegido:**

Cisco ISR 4000 Series: Estos routers modulares son adecuados para redes de tamaño mediano a grande. Ofrecen una variedad de funciones de enrutamiento, seguridad y administración de servicios. Su precio es de 1.150,99 euros.

#### **Switches Cisco:**

Cisco Catalyst 9000 Series: Estos switches de acceso y agregación ofrecen alto rendimiento, seguridad avanzada y capacidades de administración simplificadas. Son ideales para redes de campus y sucursales. Su precio es de 5.756,30 euros.

Servidor:

#### **Cisco UCS C220 M5 Rack Server:**

Este servidor es parte de la serie Cisco Unified Computing System (UCS) y es una opción popular para cargas de trabajo empresariales y aplicaciones de servidor.

Ofrece un alto rendimiento y una capacidad de expansión flexible, lo que lo hace adecuado para alojar aplicaciones como **Moodle** y actuar como **servidor proxy**.

La arquitectura unificada de **Cisco UCS** proporciona una gestión centralizada y simplificada del servidor, lo que facilita su administración y operación.

### **Partes del Rack del Servidor:**

- Servidores redundantes: Instala al menos dos servidores idénticos con la misma configuración y aplicaciones. Estos servidores trabajarán en conjunto para distribuir la carga de trabajo y proporcionar redundancia en caso de fallo de uno de ellos.
- Sistema de alimentación ininterrumpida (UPS): Un UPS garantiza que los servidores estén protegidos contra cortes de energía y les proporciona tiempo suficiente para apagar correctamente en caso de una interrupción prolongada.
- Dispositivo de almacenamiento compartido: Implementa un almacenamiento compartido, como un sistema de almacenamiento en red (NAS) o un sistema de almacenamiento de área de almacenamiento (SAN), para que los servidores tengan acceso a los mismos datos y aplicaciones. Esto garantiza la coherencia de los datos y facilita la conmutación por error entre servidores.

## **Inversión final**

Para este supuesto caso habría que comprar dos routers y dos switches y un servidor, el coste total de estos dispositivos sería de 17.024. Teniendo en cuenta que cada dos metros de cable son 4,10, y que cada equipo necesita un cable, teniendo en cuenta que cada clase tendrá 20 equipos, el cableado será una inversión de 164 euros. A esto hay que sumarle el precio de las distintas partes del rack como el sistema NAS y el UPS.

La inversión total final sería de **17.188**, sin tener en cuenta el costo de cada uno de los equipos de los alumnos.

## Virtualización de Equipos

### SERVIDOR MOODLE - PROXY

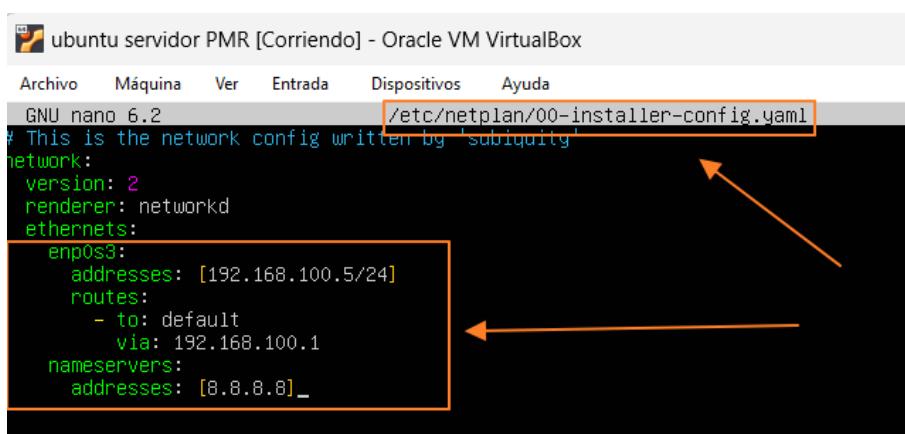
Para nuestro servidor hemos utilizado el sistema operativo de **Ubuntu Server 22.04 LTS**, para instalarlo simplemente hacemos uso de la ISO que podemos descargar directamente desde la página web oficial de Ubuntu.

#### ¿Por qué Ubuntu y no Windows?

La elección de **Ubuntu Server** sobre **Windows Server** para este proyecto se basa en varios factores clave. En primer lugar, Ubuntu Server es de código abierto y gratuito, lo que reduce los costos de licencia. Además, ofrece una gran flexibilidad y opciones de personalización, lo que permite adaptar el sistema operativo a las necesidades específicas del proyecto. Ubuntu Server es conocido por su seguridad y estabilidad, con actualizaciones regulares de seguridad y parches proporcionados por la comunidad de código abierto. También tiene una sólida compatibilidad con tecnologías de contenedores como Docker, lo que facilita la implementación y gestión de aplicaciones en contenedores. Además, cuenta con una amplia comunidad de usuarios y una abundante documentación en línea, lo que facilita la resolución de problemas y la obtención de soporte técnico. En general, Ubuntu Server puede ofrecer un mejor rendimiento y eficiencia en comparación con Windows Server en muchos casos, lo que lo convierte en una opción atractiva para este proyecto.

#### Configuración del Servidor

En este apartado, la única configuración realizada al tener instalado el sistema operativo, será modificar la configuración de red, tal y como se puede ver en la foto.



```
ubuntu servidor PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 6.2
/etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses: [192.168.100.5/24]
      routes:
        - to: default
          via: 192.168.100.1
      nameservers:
        addresses: [8.8.8.8]
```

## Servidor Router

Para este equipo también se ha utilizado el sistema operativo de Ubuntu Server 22.04 LTS y al igual que con el equipo servidor, la configuración modificada será la configuración de red. Este equipo contará con 3 interfaces de red, cada interfaz equivale a una red.

Como podemos observar en la captura de pantalla, se muestra la configuración adecuada para que el equipo funcione como router. Podemos ver como la interfaz `enp0s3` está dentro del rango de IP de la red donde se encontrará el servidor Proxy - Moodle (192.168.100.0/24). La interfaz `enp0s8` se encargará de ser la puerta de enlace para los equipos de la red de la clase 1 (192.168.105.0/24). Y finalmente la interfaz `enp0s9` será la puerta de enlace para los equipos de la clase 2 (192.168.106.0/24).

```

GNU nano 6.2                               /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses: [192.168.100.2/24]
      routes:
        - to: default
          via: 192.168.100.1
      nameservers:
        addresses: [8.8.8.8]
    enp0s8:
      addresses: [192.168.105.1/24]
      routes:
        - to: default
          via: 192.168.100.1
      nameservers:
        addresses: [8.8.8.8]
    enp0s9:
      addresses: [192.168.106.1/24]
      routes:
        - to: default
          via: 192.168.100.1
      nameservers:
        addresses: [8.8.8.8]

```

[ .. is a directory ]

Help Write Out Where Is Cut Execute Location Undo  
Exit Read File Replace Paste Justify Go To Line Redo

## Configuración en Modo Router

Para que este equipo funcione correctamente como un router deberemos hacer la configuración del **reenvío de paquetes entre interfaces**. Para ello deberemos descomentar la siguiente línea de configuración en el fichero `/etc/sysctl.conf`.

```

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

```

## NAT MASQUERADE

Para que los paquetes puedan salir al exterior debemos configurar una regla de iptables habilitando el **NAT MASQUERADE**.

```
ubuntu router PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
outer-pmr@router-pmr:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

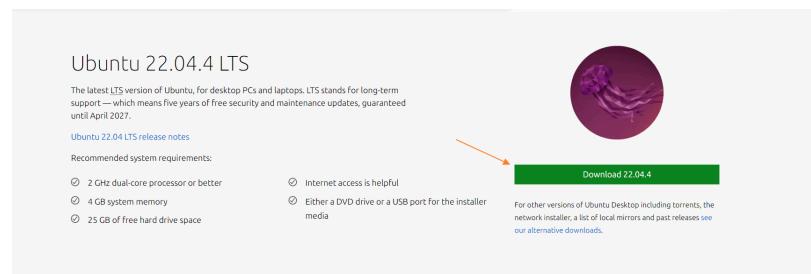
Además, deberemos instalar el siguiente paquete en el equipo router para que los cambios que hagamos en iptables se queden guardados de manera permanente.

```
ubuntu router PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
outer-pmr@router-pmr:~$ sudo apt install iptables-persistent
```

## Equipos de los Profesores y Alumnos.

Los equipos de los alumnos dispondrán del sistema operativo **Ubuntu 22.04 LTS**.

La elección se basa en varias consideraciones importantes. En primer lugar, Ubuntu es una distribución de Linux ampliamente utilizada y bien establecida, conocida por su facilidad de uso y su amplia gama de aplicaciones disponibles. La versión **LTS** (Long-Term Support) ofrece soporte a largo plazo, lo que significa que recibirá actualizaciones de seguridad y mantenimiento durante varios años, brindando estabilidad y confiabilidad a los usuarios.



## CONFIGURACIÓN MÁQUINAS VIRTUALES CLIENTES EN VIRTUALBOX

Como ya hemos mencionado, el software que usaremos para la virtualización de los equipos será **VirtualBox**.

### Router:

Para el equipo que va a actuar como router le daremos unos recursos mínimos, ya que no tendrá que realizar ninguna función más que la de actuar como router. Estas son las especificaciones:

- Se le asignan 3 GBs de memoria RAM.
- En cuanto a los procesadores, se le asignan 3.
- Para el almacenamiento se le asignan 15 GBs.
- Este equipo contará con 3 adaptadores de red.

### Servidor:

Para el equipo servidor deberemos asignarle una gran cantidad de los recursos disponibles ya que este será el equipo en el que estarán disponibles los distintos servicios que se van a instalar. Las especificaciones de la máquina son las siguientes:

- En el equipo servidor, he asignado 8 GBs de memoria RAM.
- En cuanto procesadores, este equipo contará con 4 procesadores.
- Contará con un disco duro de 50 GBs de capacidad.
- Y solo contará con un adaptador de red.

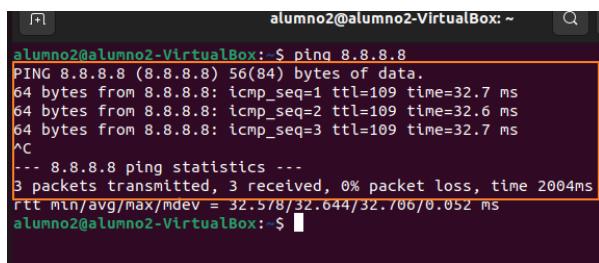
### Equipos de los Usuarios:

Los equipos de los usuarios de la red contarán con los recursos necesarios para las distintas funciones que llevarán a cabo. Los seis equipos usuarios contarán con los mismos recursos, estos son:

- Los equipos contarán con 3 GBs de memoria RAM.
- Contarán con 2 procesadores cada uno.
- Tendrán 1 disco duro de 15 GBs de almacenamiento.
- Y 1 solo adaptador de red

## Comprobación de Conectividad a Internet.

Como podemos observar en esta captura de pantalla, vemos como los equipos consiguen tener internet gracias a la configuración de reenvío de paquetes y nat masquerade que montamos en el equipo router.



```
alumno2@alumno2-VirtualBox: ~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=32.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=32.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=32.7 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 32.578/32.644/32.706/0.052 ms
alumno2@alumno2-VirtualBox: ~$
```

## - 3.0 Configuración de Servicios

### 3.1 Moodle en Docker.

Para este apartado haremos uso de la herramienta **Docker**.

Como podemos observar, en nuestro caso usaremos la última versión de la herramienta.



```
servidor-pmr@servidor-pmr: ~$ docker -v
Docker version 25.0.3, build 4debf41
servidor-pmr@servidor-pmr: ~$ _
```

## 3.2 INSTALACIÓN DE MOODLE

```
ubuntu servidor PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 6.2 docker-compose.yml
version: '3'
services:
  mariadb:
    image: mariadb
    environment:
      - MYSQL_ROOT_PASSWORD=moodle
      - MYSQL_ROOT_USER=root
      - MYSQL_DATABASE=moodle
  moodle:
    image: bitnami/moodle:latest
    ports:
      - 8080:8080
      - 8443:8443
    environment:
      - MOODLE_DATABASE_HOST=mariadb
      - MOODLE_DATABASE_USER=root
      - MOODLE_DATABASE_PASSWORD=moodle
      - MOODLE_DATABASE_NAME=moodle
      - MOODLE_USERNAME=javierh
      - MOODLE_PASSWORD=javierh
    depends_on:
      - mariadb
    links:
      - mariadb:mariadb
```

Para poder usar moodle tendremos que hacer uso de un archivo llamado **Docker Compose**. Docker Compose es una herramienta que permite definir y ejecutar aplicaciones Docker de manera multi-contenedor de una manera sencilla y declarativa. Permite describir las relaciones entre diferentes servicios, como contenedores, redes y volúmenes, en un archivo YAML llamado `docker-compose.yml`. Con Docker Compose, puedes definir la configuración de tu aplicación una vez y luego utilizar un solo comando para

crear y arrancar todos los servicios definidos en tu archivo `docker-compose.yml`.

## 3.3 Configuración Moodle

The screenshot shows the Moodle 'Manage courses and categories' page. It displays three course categories: 'Category 1', '2º ASIR Tardé' (which is highlighted with a red box), and '1º DAM Tardé'. Below the categories, there are buttons for 'Create new category', 'Move selected courses to...', and 'Choose'. On the left, there's a sidebar with 'Course categories and courses' and 'Selected categories' dropdowns.

### 3.3.1 CATEGORÍAS

Ayuda a **organizar los cursos** y recursos de manera lógica y estructurada, lo que facilita la navegación y la búsqueda de contenido para los usuarios.

### 3.3.2 Asignaturas

The screenshot shows the Moodle 'My courses' page with a 'Course overview' section. It lists six courses in a grid: 'Administración de sistemas gestores de base de datos 2º ASIR Tardé', 'Administración de sistemas operativos 2º ASIR Tardé', 'Empresa e iniciativa emprendedora 2º ASIR Tardé', 'Implantación de aplicaciones web 2º ASIR Tardé', 'Seguridad y alta disponibilidad 2º ASIR Tardé', and 'Servicios de red e internet 2º ASIR Tardé'.

Al crear materias, se establece una **estructura organizada** que facilita la administración y la navegación de los cursos. Cada materia representa una unidad temática

o un área específica de estudio, lo que ayuda a los estudiantes a encontrar fácilmente el contenido relacionado.

### 3.3.3 Usuarios



Permite a los estudiantes, profesores y administradores acceder a la plataforma **Moodle** de manera personalizada, utilizando credenciales únicas que les identifican en el sistema. Además, los usuarios pueden tener diferentes roles dentro de Moodle, como estudiante, profesor, tutor o administrador. La creación de usuarios permite asignar roles específicos a cada persona, lo que determina sus permisos y funciones dentro del entorno de aprendizaje.

En adición a lo anterior, las **contraseñas** de los usuarios han sido creadas según las pautas para la creación de una contraseña segura según el **INCIBE** (Instituto Nacional de Ciberseguridad).

First name / Last name	Email address	City/town	Country
Admin User	user@example.com		
alejandro monroy	alejandromonroy@alumno.ieselrincon.es		
francisco hernandez	francish@profesor.ieselrincon.es		
iker suarez	ikersuarez@alumno.ieselrincon.es		
manuel benitez	manuelbenitez@profesor.ieselrincon.es		
mario suarez	mariosuarez@alumno.ieselrincon.es		
ruben romero	ruberromero@alumno.ieselrincon.es		

### 3.3.4 MATRICULAR ALUMNOS EN ASIGNATURAS

Para ello iremos a los cursos y en **“participantes”** añadiremos los usuarios de la cohorte correspondiente. Además, le asignaremos el **rol de estudiante** a estos usuarios.

### 3.4 Comprobación de Uso

Como podemos observar, si entramos a la **Moodle** con un usuario solo nos saldrán las asignaturas en las que ese usuario esté matriculado.

### - 4.0 Servidor Proxy Squid

Utilizaremos la última versión del servicio. Como vemos es la **versión 5.7**.

```
router-pmr@router-pmr:~$ squid -v
Squid Cache: Version 5.7
Service Name: squid
Ubuntu linux
```

### 4.1 Configuración del Servidor Squid.

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
acl localnet src 0.0.0.1-255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0/8 # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CEN)
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-nt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
http_access deny all
http_port 3128
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\.?) 0 0% 0
refresh_pattern \/(Packages|Sources)([|\\].bz2|[|\\].gz|[|\\].xz)$ 0 0% 0 refresh-ims
refresh_pattern \/Release(|\\).pgp$ 0 0% 0 refresh-ims
refresh_pattern \/InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)([|\\].bz2|[|\\].gz|[|\\].xz)$ 0 0% 0 refresh-ims
refresh_pattern . 0 20% 4320
"squid.conf" 36L, 1626B
```

Podemos ver distintos elementos de configuración como las **ACL** de redes privadas, elementos de puertos seguros y las listas de bloqueo de acceso.

Para configurar correctamente el servidor proxy squid deberemos acceder al fichero de configuración **conf.d** y habilitar la ruta hacia otro fichero que crearemos posteriormente con todas las reglas pertinentes.

Antes de realizar la configuración, existen listas de dominios ya preconfiguradas, las cuales podemos descargar y usar para nuestro servidor squid.

Estas listas son muy útiles ya que recogen sitios no recomendados por la comunidad.

En nuestro caso usaremos la lista **blackweb.txt**. El archivo "**blackweb.txt**" contiene una lista de **dominios o direcciones URL** asociadas con contenido considerado inapropiado, **malicioso o no deseado**. Es común que este tipo de archivos se utilicen en configuraciones de filtros de contenido o sistemas de seguridad para bloquear el acceso a sitios web que pueden representar riesgos para la seguridad o la productividad.

El nombre "**blackweb**" sugiere que estos dominios están relacionados con la parte oscura o no ética de Internet, como sitios de phishing, malware, contenido para adultos, juegos de azar, entre otros. Estos dominios pueden ser bloqueados o filtrados para proteger a los usuarios finales de acceder inadvertidamente a ellos y para mantener la integridad y seguridad de la red.

Finalmente, las ACLs que configuraremos en nuestro servidor son las siguientes:

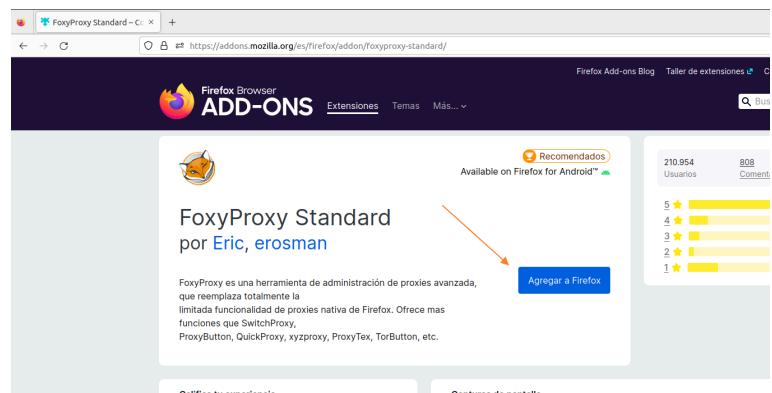
```
acl red1 src 192.168.105.0/24
acl red2 src 192.168.106.0/24

acl blackweb dstdomain "etc/squid/conf.d/blackweb.txt"

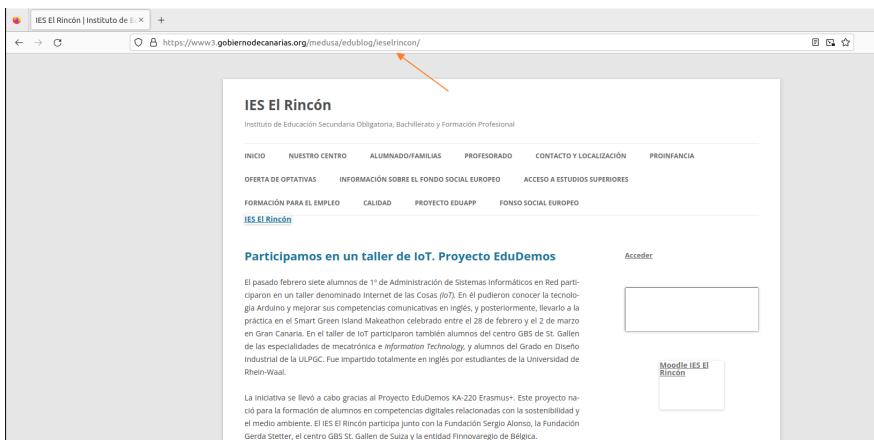
http_access deny blackweb
http_access allow red1
http_access allow red2
```

## 4.2 CONFIGURACIÓN CLIENTES

Al instalar **FoxyProxy** en los equipos de los alumnos, se les brinda una herramienta flexible para administrar su conexión a Internet, garantizando un acceso seguro, controlado y, en algunos casos, mejorado a los recursos en línea.

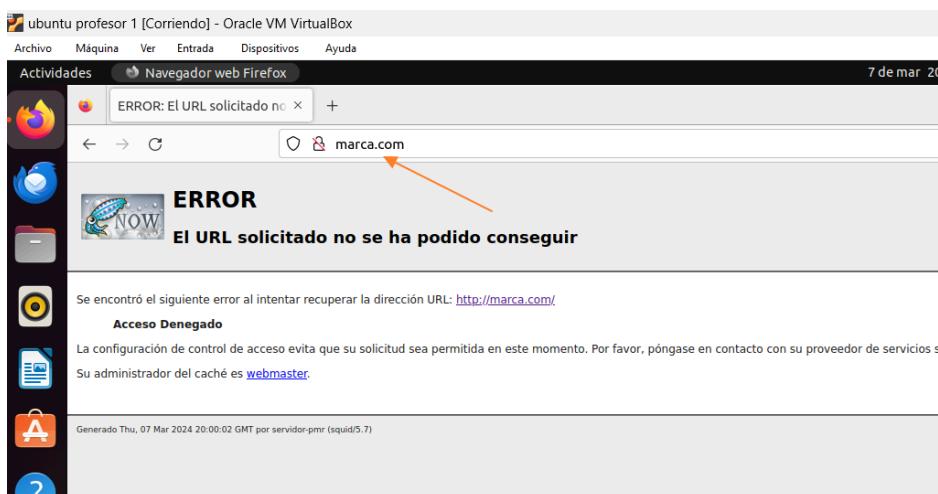


## 4.3 Comprobación del funcionamiento del Servicio.



Como podemos observar en la captura de pantalla, podemos acceder a la página del centro.

Pero no podremos acceder a la página del diario deportivo Marca.



## - 5.0 Implementación del SIEM - Wazuh

El **Sistema de Gestión de Información y Eventos de Seguridad (SIEM)** desempeña un papel fundamental en la ciberseguridad de una organización al proporcionar una plataforma integral para la recopilación, correlación, análisis y respuesta a eventos de seguridad en toda la infraestructura de TI.

El **SIEM Wazuh** es una herramienta esencial para fortalecer la postura de seguridad de una organización al proporcionar visibilidad, detección temprana y respuesta efectiva a amenazas cibernéticas. Su capacidad para recopilar, analizar y correlacionar eventos de seguridad ayuda a proteger los activos críticos de la organización y a mantener la integridad, confidencialidad y disponibilidad de la información.

Al ingresar con el usuario y contraseña que se nos facilitó durante la instalación de la herramienta, nos aparecerá el dashboard de la herramienta.

The screenshot shows the Wazuh dashboard with the following sections:

- Top Metrics:** Total agents (0), Active agents (0), Disconnected agents (0), Pending agents (0), Never connected agents (0).
- SECURITY INFORMATION MANAGEMENT:**
  - Security events:** Browse through your security alerts, identifying issues and threats in your environment.
  - Integrity monitoring:** Alerts related to file changes, including permissions, content, ownership and attributes.
- AUDITING AND POLICY MONITORING:**
  - Policy monitoring:** Verify that your systems are configured according to your security policies baseline.
  - System auditing:** Audit users behavior, monitoring command execution and alerting on access to critical files.
- THREAT DETECTION AND RESPONSE:**
  - Vulnerabilities:** Discover what applications in your environment are affected by well-known vulnerabilities.
  - MITRE ATT&CK:** Security events from the knowledge base of adversary tactics and techniques based on real-world observations.
- REGULATORY COMPLIANCE:**
  - PCI DSS:** Global security standard for entities that process, store or transmit payment cardholder data.
  - NIST 800-53:** National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

### 5.1 Habilitar Detección de Vulnerabilidades.

Se habilitará la integración de detección de vulnerabilidades de la herramienta **Wazuh** porque es una práctica recomendada para fortalecer la seguridad del sistema, proteger los

datos y cumplir con los requisitos de seguridad establecidos por las regulaciones y estándares de la industria.

## 5.2 Integración de VirusTotal en Wazuh.

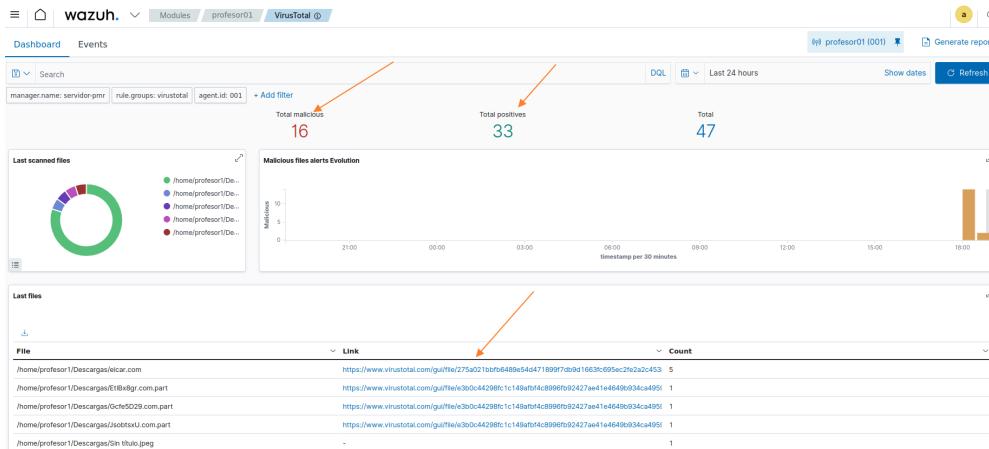
Se implementará **VirusTotal** para **escanear y eliminar archivos maliciosos** descargados por los usuarios. Este enfoque integral garantiza un entorno educativo seguro y funcional, adaptado a las necesidades del centro y en línea con las mejores prácticas de ciberseguridad.

Time	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
> Mar 12, 2024 @ 18:18:38.369	/home/profesor1/Descargas/eicar.com	deleted	File deleted.	7	553
> Mar 12, 2024 @ 18:18:34.961	/home/profesor1/Descargas/eicar.com	modified	File modified in /root directory.	7	100200
> Mar 12, 2024 @ 18:18:33.893	/home/profesor1/Descargas/Et10x8gr.com.part	deleted	File deleted.	7	553
> Mar 12, 2024 @ 18:18:33.882	/home/profesor1/Descargas/eicar.com	added	File added to /root directory.	7	100201
> Mar 12, 2024 @ 18:18:33.871	/home/profesor1/Descargas/Et10x8gr.com.part	added	File added to /root directory.	7	100201
> Mar 12, 2024 @ 18:15:45.845	/home/profesor1/Descargas/eicar.com	deleted	File deleted.	7	553
> Mar 12, 2024 @ 18:15:40.826	/home/profesor1/Descargas/eicar.com	modified	File modified in /root directory.	7	100200
> Mar 12, 2024 @ 18:15:40.820	/home/profesor1/Descargas/eicar.wRM2jdC.com.part	deleted	File deleted.	7	553

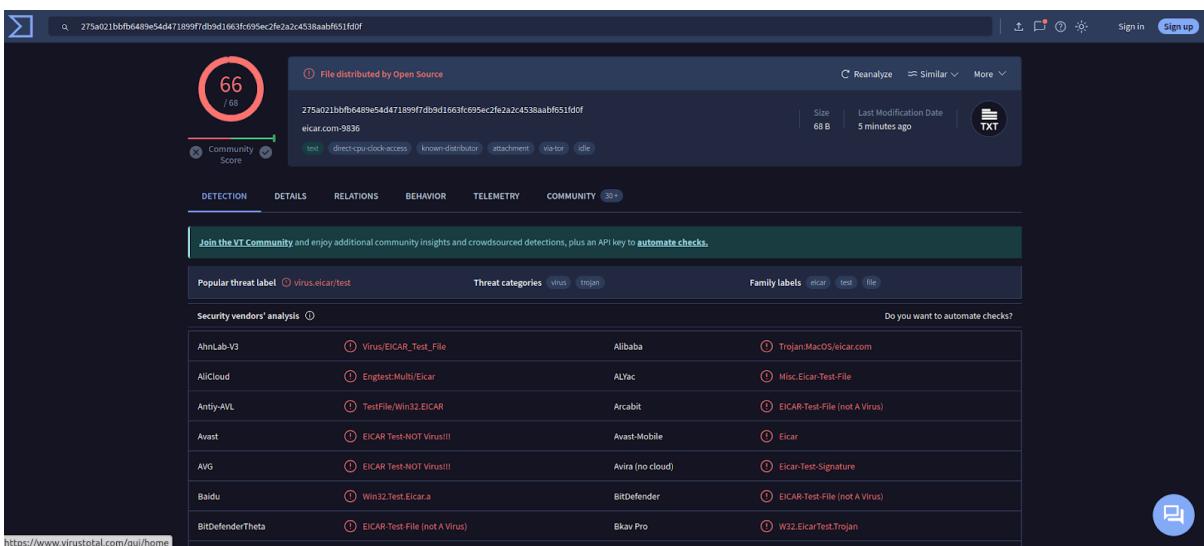
## ¿Qué es VirusTotal?

**VirusTotal** es un servicio en línea que ofrece un análisis gratuito de archivos y URL para detectar malware y otras amenazas en la seguridad informática. Utiliza una amplia variedad de motores antivirus y herramientas de escaneo para realizar un análisis exhaustivo de archivos y direcciones web, proporcionando resultados detallados sobre la presencia de cualquier amenaza conocida. VirusTotal es ampliamente utilizado por usuarios individuales, empresas y organizaciones de seguridad para verificar la seguridad de

archivos sospechosos antes de su ejecución o descarga. Su integración en sistemas informáticos y de red permite una capa adicional de protección contra amenazas ciberneticas.



Además, gracias a la integración de **VirusTotal** en **Wazuh** podemos acceder al análisis del archivo desde el dashboard de la herramienta.



## CONCLUSIONES

En el desarrollo del proyecto se han alcanzado satisfactoriamente los objetivos planteados inicialmente, los cuales incluían la ampliación del centro educativo con dos nuevas clases debidamente preparadas y configuradas, así como la implementación de una topología de red adecuada y la adopción de medidas de seguridad para proteger la infraestructura informática.

Se ha logrado diseñar y configurar una **topología de red** que permite la comunicación eficiente entre los distintos dispositivos y usuarios, garantizando un acceso seguro a los recursos compartidos. La virtualización de los equipos ha permitido simular los entornos de aula de manera efectiva, facilitando la gestión y administración de los recursos informáticos.

La implementación de servicios como Moodle para la gestión educativa, **Proxy Squid** para el filtrado de contenido web y **SIEM Wazuh** para la monitorización de la seguridad ha contribuido significativamente a mejorar la calidad y seguridad de la red. Además, la integración de VirusTotal para la detección de archivos maliciosos ha fortalecido aún más las medidas de protección.

Sin embargo, a pesar de los esfuerzos realizados, no se logró integrar el servicio **Veyon** para el monitoreo y gestión de los equipos de los alumnos. Aunque esta funcionalidad no pudo ser implementada, el resto de los servicios y medidas de seguridad han sido desplegados con éxito, proporcionando un entorno de aprendizaje eficiente y protegido para la comunidad educativa.

## LIMITACIONES DEL ESTUDIO Y FUTURAS LÍNEAS DE INVESTIGACIÓN

Durante el desarrollo del proyecto, se encontraron algunas **limitaciones** que afectaron la consecución de ciertos objetivos:

1. **Integración de Veyon:** A pesar de los esfuerzos realizados, no se logró integrar completamente el servicio Veyon para la administración conjunta de los equipos de las aulas. Se encontraron dificultades técnicas que requieren un mayor tiempo de investigación y configuración para su implementación exitosa.



En cuanto a las **futuras líneas de investigación y mejoras del proyecto**, se pueden considerar las siguientes:



#### 1. Implementación de Directorio Activo:

Para una administración más eficiente de los equipos de las aulas, se puede investigar y añadir un Directorio Activo que permita gestionar centralizadamente los usuarios, equipos y políticas de seguridad. Este objetivo se podría conseguir implementando herramientas como OpenLDAP.



2. Refuerzo de la Seguridad con Firewall:

Se puede estudiar la incorporación de un firewall para fortalecer la seguridad de la red, estableciendo reglas de filtrado de tráfico y protegiendo los equipos contra posibles amenazas externas. Herramientas como Suricata pueden encajar en el proyecto.



3. Servidor DHCP para Asignación de IP Dinámicas:

Para simplificar la gestión de direcciones IP en las clases, se puede implementar un servidor DHCP que proporcione direcciones IP de manera dinámica a los equipos, facilitando la conectividad de los

dispositivos a la red de forma automática y organizada. Esta configuración se podría realizar en los dispositivos de red de la marca Cisco.

## REFERENCIAS BIBLIOGRÁFICAS

1. Al-Fares, M., Loukissas, A., & Vahdat, A. (2008). A scalable, commodity data center network architecture. *ACM SIGCOMM Computer Communication Review*, 38(4), 63-74.
2. Cisco Systems. (2017). CCNA Routing and Switching Portable Command Guide. Cisco Press.
3. Comer, D. (2005). Interconexión de redes con TCP/IP. Pearson Educación.
4. Forouzan, B. A. (2006). Comunicaciones y redes de computadores. McGraw-Hill.
5. Gómez, L., & Garcerá, G. (2005). Administración de redes con GNU/Linux. Alfaomega Grupo Editor.
6. Kim, B. H., Choi, J., Lee, S., & Kim, H. J. (2018). Research on efficient management for information security events based on SIEM system. *Security and Communication Networks*, 2018.
7. Páginas web adicionales:
  - Documentación oficial de Squid: <https://www.squid-cache.org/Doc/>
  - Documentación oficial de Wazuh: <https://documentation.wazuh.com/current/index.html>
  - Docker Documentation. (s.f.). Docker Documentation. Recuperado de <https://docs.docker.com/>
8. Roesch, M. (1999). Snort: Lightweight Intrusion Detection for Networks. In LISA (Vol. 99, pp. 229-238).
9. Stallings, W. (2017). Redes e Internet de alta velocidad: Protocolos, rendimiento y control. Pearson Educación.
10. Tanenbaum, A. S., & Wetherall, D. J. (2011). Redes de computadoras. Pearson Educación.
11. Bejtlich, R. (2005). The Tao of Network Security Monitoring: Beyond Intrusion Detection. Pearson Education.

## Anexos

### Anexo I

#### Topología

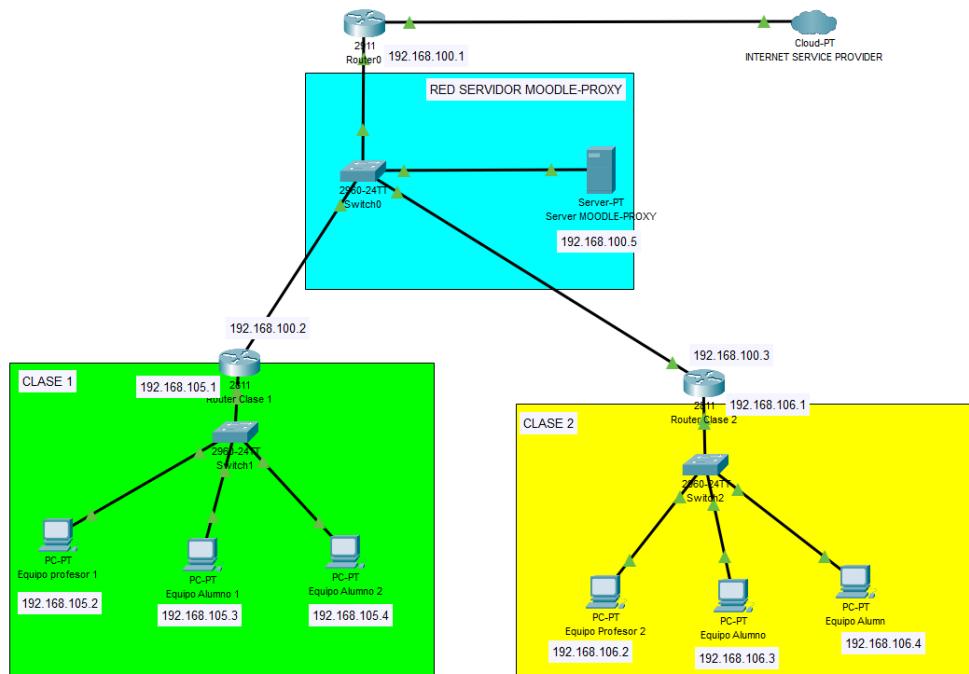
##### **Diseño de la Topología de Red:**

La planificación de la topología de red constituyó un paso crucial en el desarrollo del proyecto, ya que permitió establecer las bases para la posterior implementación y configuración de la infraestructura tecnológica en el I.E.S El Rincón. En esta fase, se consideraron detalladamente las necesidades específicas del centro educativo, así como la distribución óptima de los dispositivos para garantizar un funcionamiento eficiente y fiable de la red.

Se llevaron a cabo análisis exhaustivos para determinar la disposición de los equipos, la conectividad entre ellos y la segmentación de la red en subredes adecuadas. Se tuvo en cuenta la ubicación de las nuevas clases, los requerimientos de conectividad de los profesores y alumnos, así como la integración de servicios adicionales como servidores y routers.

La **topología de red** diseñada se caracterizó por su escalabilidad, flexibilidad y seguridad, aspectos fundamentales para satisfacer las demandas de un entorno educativo en constante evolución. Se emplearon herramientas de modelado y simulación para visualizar y validar la configuración propuesta, asegurando su viabilidad y optimización.

Como topología lógica de **red lógica** tenemos la siguiente.



Como podemos observar en la imagen, cada una de las clases se encuentra en una red distinta. ¿esto qué ventajas nos aporta?

El hecho de tener cada clase en una red distinta ofrece varias ventajas en términos de seguridad, rendimiento y administración de la red. Algunas de estas ventajas son:

**Seguridad:** Al separar cada clase en redes distintas, se limita la visibilidad y accesibilidad entre ellas. Esto significa que los dispositivos y recursos de una clase no están directamente expuestos a los dispositivos de otra clase, lo que reduce el riesgo de accesos no autorizados y la propagación de amenazas de seguridad.

**Control de tráfico:** Al segmentar la red en subredes separadas para cada clase, se puede gestionar de manera más efectiva el tráfico de red. Esto permite priorizar ciertos tipos de

tráfico, aplicar políticas de acceso específicas y optimizar el rendimiento de la red para cada entorno de clase.

**Rendimiento:** Al distribuir el tráfico de red en redes separadas, se evita la congestión de la red que puede ocurrir cuando se comparten recursos entre múltiples clases. Esto garantiza un rendimiento óptimo de la red para cada grupo de usuarios y aplicaciones.

**Facilidad de administración:** Al tener cada clase en una red separada, se simplifica la administración y la resolución de problemas de red. Los administradores pueden gestionar y monitorear cada red de manera independiente, lo que facilita la identificación y solución de problemas específicos de cada entorno de clase.

## Dispositivos a usar

Para una topología de red en un instituto, la marca **Cisco** ofrece una amplia gama de routers y switches que pueden adaptarse a diferentes necesidades y tamaños de red. Aquí te recomendaré algunos modelos que podrían ser adecuados dependiendo del tamaño y la complejidad de la red del instituto:

### Routers Cisco:

**Cisco ISR 4000 Series:** Estos routers modulares son adecuados para redes de tamaño mediano a grande. Ofrecen una variedad de funciones de enrutamiento, seguridad y administración de servicios. Su precio es de 1.150,99 euros.

The screenshot shows a product listing for the Router Cisco ISR4221/K9 (ISR4221/K9) from Bechtle. The page includes the following details:

- Router Cisco ISR4221/K9 (ISR4221/K9)**
- Nº del fabricante: ISR4221/K9
- N.º Bechtle: 4144125-12
- Puertos: 4 x LAN
- 1.150,99** (Price highlighted with an orange arrow)
- Categoría: Más productos para La red
- Precio bruto: 1.392,70 € incluye 241,71 € en concepto de IVA
- Gastos de envío

### Switches Cisco:

- **Cisco Catalyst 9000 Series:** Estos switches de acceso y agregación ofrecen alto rendimiento, seguridad avanzada y capacidades de administración simplificadas. Son ideales para redes de campus y sucursales. Su precio es de 5.756,30 euros.

The screenshot shows a product listing for the Cisco Catalyst 9200L48-PortPoE+ Cptn switch. The price is highlighted in a blue box at 5.756,30 €. Payment terms are shown as 208,66 €/mes over 18 months with a 4,95 € first payment. The item is labeled as 'Últimas unidades en stock' (last units in stock) and 'Reacondicionado' (refurbished). Delivery information indicates it can be delivered before 20 hours and 26 minutes, with collection between Wednesday 6 and Friday 8 via Correos Express/GLS Almacén 31.

### Servidor:

#### Cisco UCS C220 M5 Rack Server:

Este servidor es parte de la serie **Cisco Unified Computing System** (UCS) y es una opción popular para cargas de trabajo empresariales y aplicaciones de servidor.

Ofrece un alto rendimiento y una capacidad de expansión flexible, lo que lo hace adecuado para alojar aplicaciones como Moodle y actuar como servidor proxy.

Viene con procesadores **Intel Xeon** escalables de última generación, opciones de memoria de alta capacidad y almacenamiento escalable para adaptarse a las necesidades de tu aplicación.

La arquitectura unificada de **Cisco UCS** proporciona una gestión centralizada y simplificada del servidor, lo que facilita su administración y operación.

Lanzamiento de Cisco: 11 de mayo de 2022						
Número	Producto	Descripción	Precio de lista (USD)	Nuestro precio		Citar
1	UCSC-DBUN-C220-113	UCS C220 M3 SFF, 1xE5-2609, 1x8GB, ROM55, 2x650W, SD, RAILS.	\$3,212.00		<button>Citar</button>	<input type="checkbox"/>
2	UCSC-DBUN-C220-112	UCS C220 M3 SFF, 1xE5-2620, 1x8GB, ROM55, 2x650W, SD, RAILS.	\$3,499.00		<button>Citar</button>	<input type="checkbox"/>
3	UCSC-DBUN-C220-111	UCS C220 M3 SFF, 1xE5-2640, 1x8GB, ROM55, 2x650W, SD, RAILS.	\$4,625.00		<button>Citar</button>	<input type="checkbox"/>
4	UCSC-RAID-ROM5	Embedded SW RAID 0/1/10, 8 ports SAS/SATA.	\$35.00		<button>Citar</button>	<input type="checkbox"/>



4,20 euros.

## Cableado y Dispositivos del Rack:

El cable de parche Cat 6A S/FTP con conectores RJ45 es una opción robusta y de alto rendimiento para redes Ethernet que requieren velocidades de transferencia de datos de hasta 10 Gbps y un rendimiento consistente en entornos con altos niveles de interferencia electromagnética y radiofrecuencia. Tres metros de cable equivalen a

Esta es la opción para el sistema NAS.

Y este para el UPS.

## Inversión final

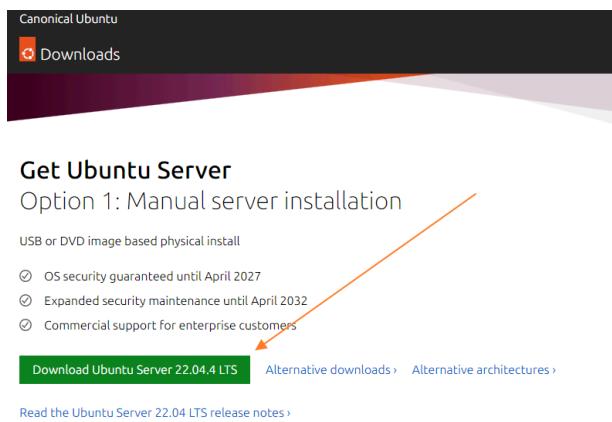
Para este supuesto caso habría que comprar dos routers y dos switches y un servidor, el coste total de estos dispositivos sería de 17.024. Teniendo en cuenta que cada dos metros de cable son 4,10, y que cada equipo necesita un cable, teniendo en cuenta que cada clase tendrá 20 equipos, el cableado será una inversión de 164 euros.

La inversión total final sería de 17.188, sin tener en cuenta el costo de cada uno de los equipos de los alumnos.

## Anexo II

### SERVIDOR MOODLE - PROXY

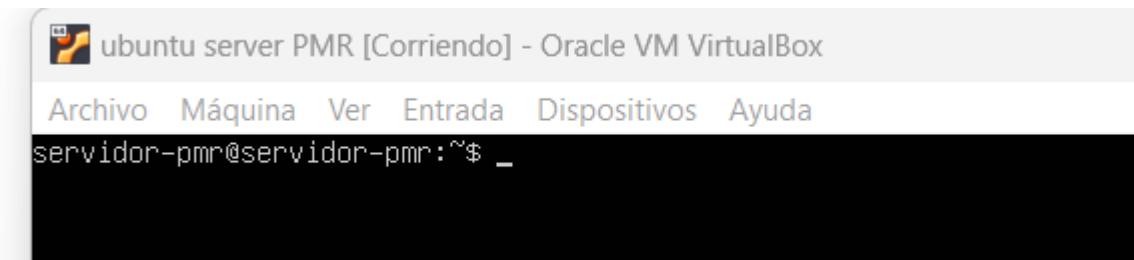
Para nuestro servidor hemos utilizado el sistema operativo de Ubuntu Server, para instalarlo simplemente hacemos uso de la ISO que podemos descargar directamente desde la pagina web oficial de Ubuntu.



Le asignamos un nombre al equipo servidor.



Una vez instalado el sistema operativo, quedaría de la siguiente manera. Al ser un Ubuntu Server, no tiene escritorio.



Lo siguiente que debemos hacer es configurar una dirección IP estática. Configuraremos el fichero de configuración **/etc/netplan/00-installer-config.yaml**.

```
ubuntu servidor PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 6.2          /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses: [192.168.100.5/24]
      routes:
        - to: default
          via: 192.168.100.1
      nameservers:
        addresses: [8.8.8.8]
```

Como podemos observar, al equipo solo tener una interfaz de red, solo debemos configurar dicha interfaz.

Para confirmar los cambios realizados en la interfaz de red usamos el siguiente comando.

```
servidor-pmr@servidor-pmr:~$ sudo netplan apply  
[sudo] password for servidor-pmr:  
servidor-pmr@servidor-pmr:~$
```

En este servidor instalaremos los servicios necesarios para este proyecto en pasos posteriores.

## ROUTER

The screenshot shows the Canonical Ubuntu download page. At the top, there's a dark header with 'Canonical Ubuntu' and a search icon. Below it, a navigation bar has 'Downloads' highlighted. The main content area is titled 'Get Ubuntu Server' and includes a sub-section 'Option 1: Manual server installation'. It features a 'Download Ubuntu Server 22.04 LTS' button in a green box. To the right of the download button, there's a note about security guarantees until April 2027, 2032, and 2034, followed by a link to 'Read the Ubuntu Server 22.04 LTS release notes'.

En este apartado veremos como instalar y configurar un Ubuntu Server para que funcione como **router**.

Como ya hemos comentado, el sistema operativo que se va a utilizar para este equipo es **Ubuntu Server**.

El siguiente equipo que configuraremos será el Ubuntu Server que hará de router.



Una vez instalado, de la misma manera que el servidor anterior, pasaremos a configurar las interfaces de red. Para ellos editaremos el fichero de configuración de netplan **/etc/netplan/00-installer-config.yaml**.

```

GNU nano 6.2                               /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s10:
      dhcp4: true
      ...

```

Como el router va a tener **3 interfaces**, la configuraremos de la siguiente manera.

```

GNU nano 6.2                               /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses: [192.168.100.2/24]
      routes:
        - to: default
          via: 192.168.100.1
          nameservers:
            addresses: [8.8.8.8]
    enp0s8:
      addresses: [192.168.105.1/24]
      routes:
        - to: default
          via: 192.168.100.1
          nameservers:
            addresses: [8.8.8.8]
    enp0s9:
      addresses: [192.168.106.1/24]
      routes:
        - to: default
          via: 192.168.100.1
          nameservers:
            addresses: [8.8.8.8]

```

Como podemos observar en la captura de pantalla, se muestra la configuración adecuada para que el equipo funcione como router. Podemos ver como la interfaz **enp0s3** está dentro del rango de IP de la red donde se encontrará el servidor Proxy - Moodle (192.168.100.0/24). La interfaz enp0s8 se encargará de ser la puerta de enlace para los equipos de la red de la clase 1 (192.168.105.0/24). Y finalmente la interfaz **enp0s9** será la puerta de enlace para los equipos de la clase 2 (192.168.106.0/24).

## Reenvío de Paquetes

Además, para que este equipo funcione correctamente como un router deberemos hacer la configuración del reenvío de paquetes entre interfaces. Para ello deberemos descomentar la siguiente línea de configuración en el fichero **/etc/sysctl.conf**.

```

GNU nano 6.2                               /etc/sysctl.conf
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

```

Aplicamos los cambios del paso anterior con el siguiente comando. Como podemos observar, el valor ha cambiado a **1** que es igual a **true**.

```
ubuntu router PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
router-pmr@router-pmr:~$ sudo sysctl -p /etc/sysctl.conf
net.ipv4.ip_forward = 1
router-pmr@router-pmr:~$ _
```

## NAT MASQUERADE

Para que los paquetes puedan salir al exterior debemos configurar una regla de **iptables** habilitando el **NAT MASQUERADE**. Para ello usaremos el siguiente comando.

```
ubuntu router PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
router-pmr@router-pmr:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

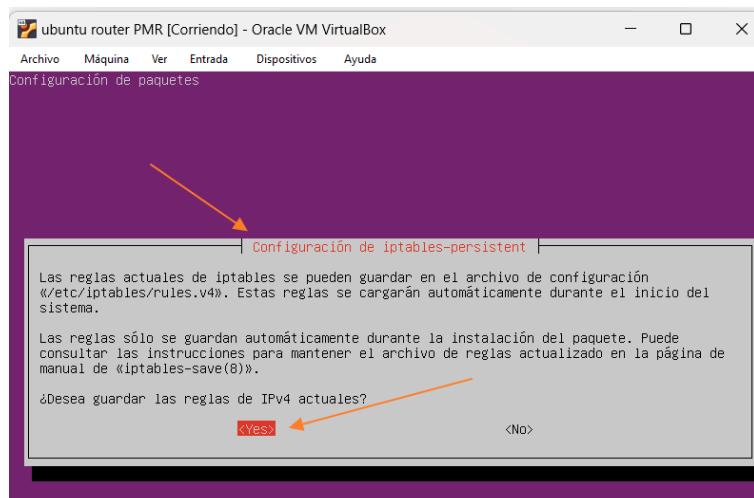
Como podemos observar, la regla aplicando el **enmascaramiento de red** se ha aplicado correctamente.

```
router-pmr@router-pmr:~$ sudo iptables -L -nv -t nat
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in     out      source          destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in     out      source          destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in     out      source          destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in     out      source          destination
    5   320 MASQUERADE  all  --  *      enp0s3  0.0.0.0/0           0.0.0.0/0
router-pmr@router-pmr:~$ _
```

Además, deberemos instalar el siguiente paquete en el equipo router para que los cambios que hagamos en iptables se queden guardados de manera permanente.

```
ubuntu router PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@router-pmr:~$ sudo apt install iptables-persistent
```

Nos saldrá la siguiente pantalla en la cual nos preguntará si queremos guardar las reglas de iptables ipv4 actuales, seleccionamos el “**yes**”.



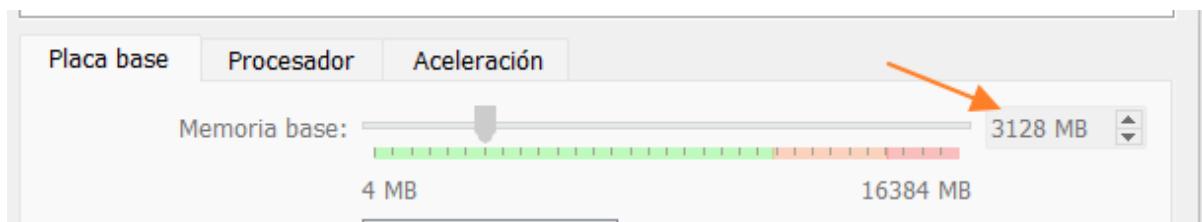
Con lo realizado ya podríamos tener la seguridad de que si reiniciamos el equipo, las reglas de **iptables** estarán configuradas de la manera correcta.

## CONFIGURACIÓN MÁQUINAS VIRTUALES CLIENTES EN VIRTUALBOX

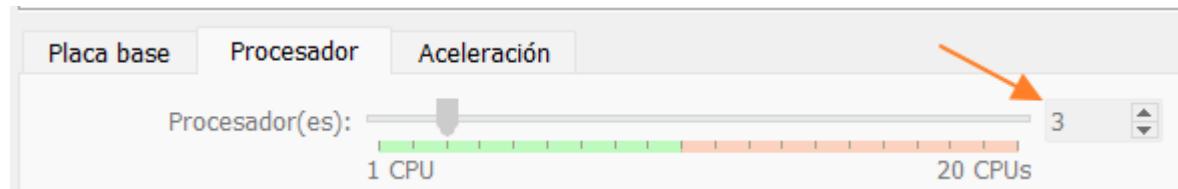
Como ya hemos mencionado, el software que usaremos para la virtualización de los equipos será VirtualBox.

Para el equipo que va a actuar como router le daremos unos recursos mínimos, ya que no tendrá que realizar ninguna función más que la de actuar como router.

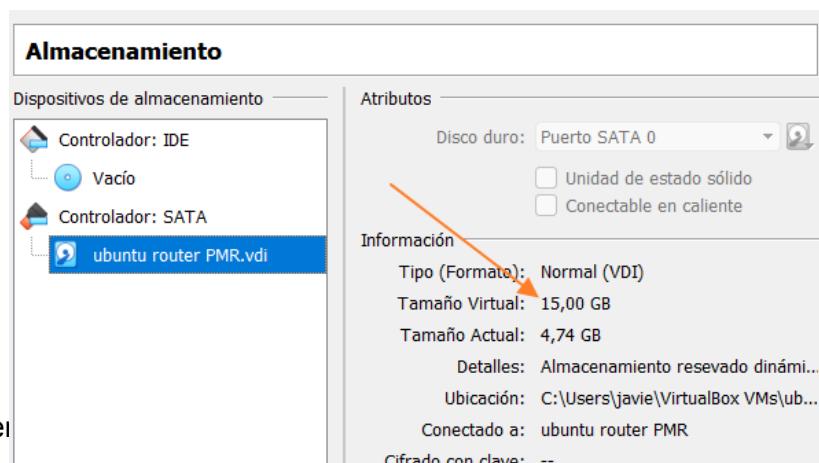
Se le asignan **3 GBs** de memoria **RAM**.



En cuanto a los **procesadores**, se le asignan **3**.

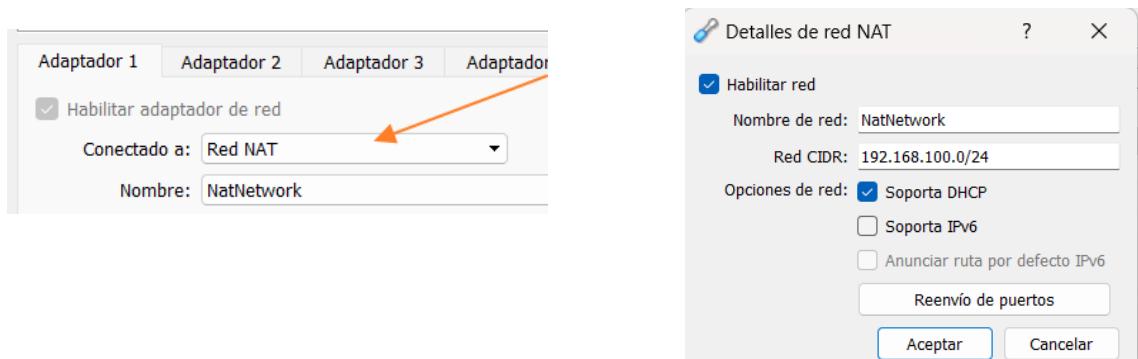


Para el **almacenamiento** se le asignan **15 GBs**.

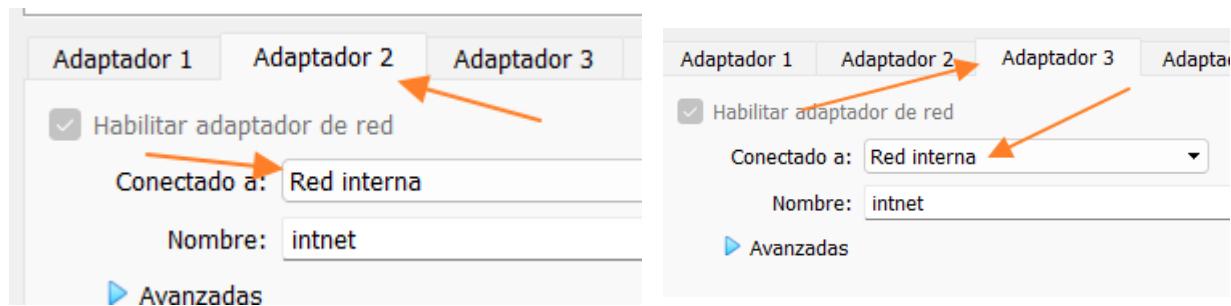


Y finalmente, el **red NAT** se configura en la sección **Adaptadores**.

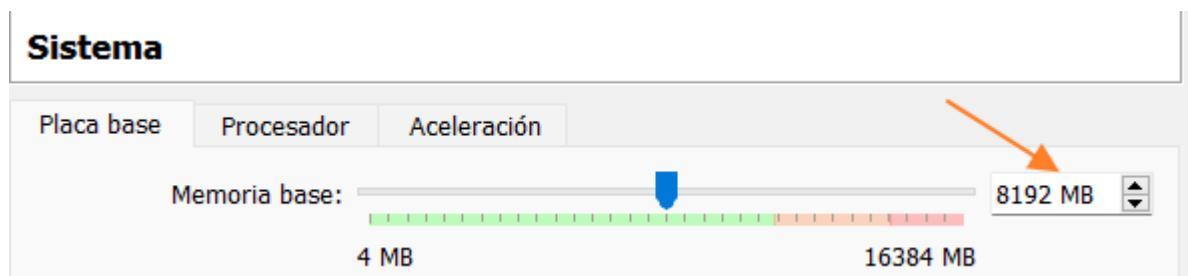
Uno de ellos será de tipo **red nat**, la cual será configurada de la siguiente manera.



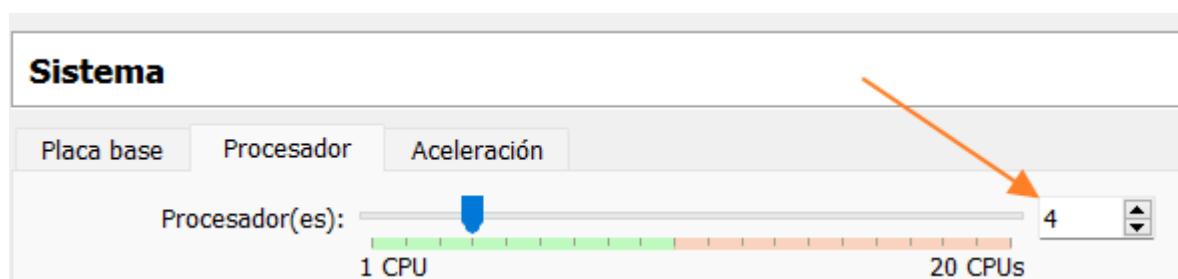
Los otros dos adaptadores se encontrarán en **red interna**.



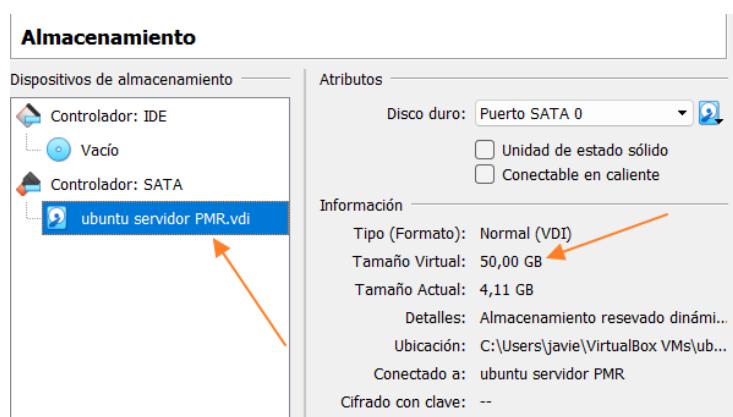
En el equipo servidor, he asignado **8 GBs** de memoria RAM.



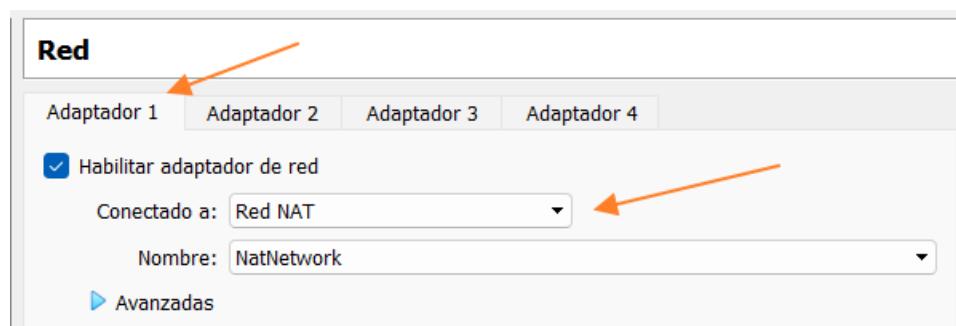
En cuanto procesadores, este equipo contará con **4 procesadores**.



Contará con un disco duro de **50 GBs de capacidad**.

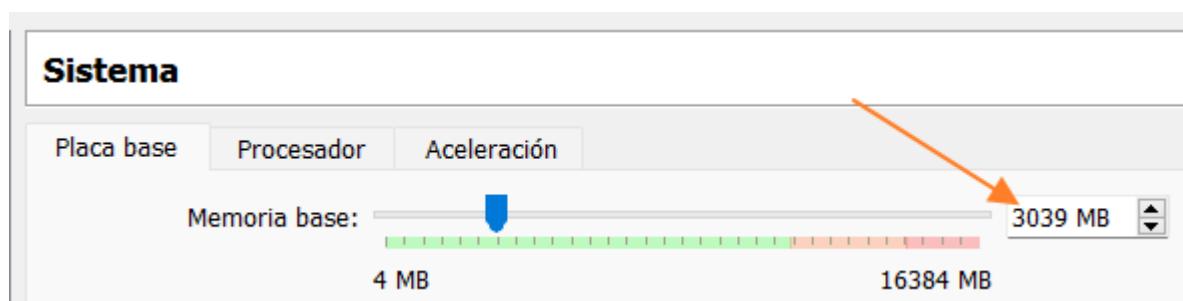


Y solo contará con un **adaptador de red** el cual será de tipo **red nat.**

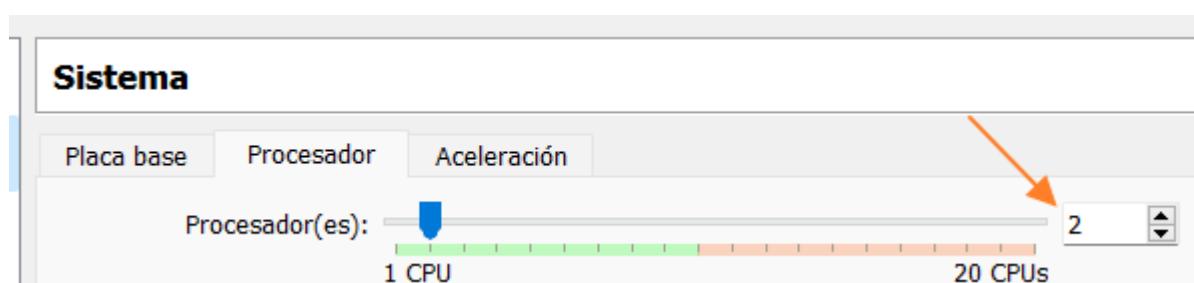


Para los equipos de los usuarios de la red, los **6 equipos** contarán con los **mismos recursos**.

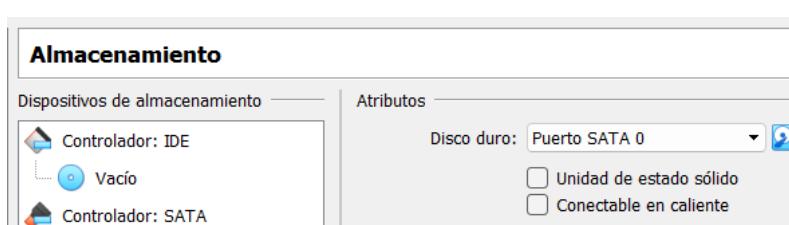
Todos los equipos contarán con **3 GBs de memoria RAM**.



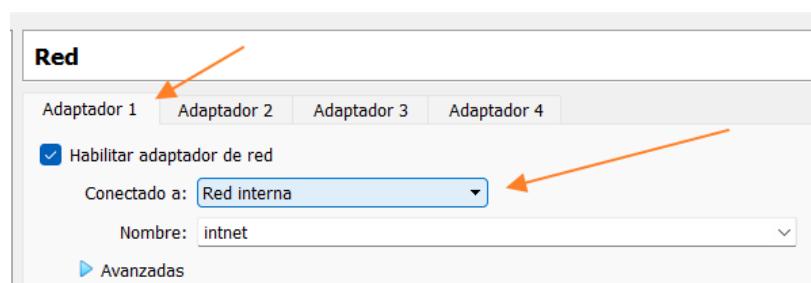
Contarán con **2 procesadores** cada uno.



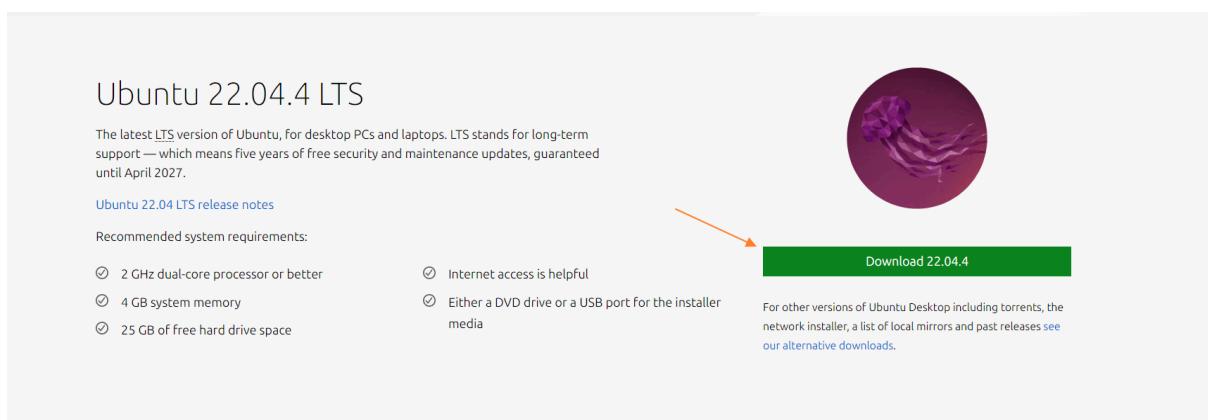
Tendrán 1 disco duro de **15 GBs** de almacenamiento.



Y 1 solo adaptador de red en tipo **red interna**.



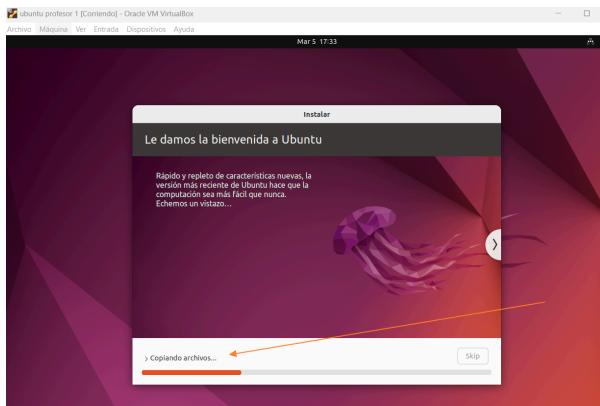
Como sistema operativo, estos equipos usarán **Ubuntu 22.04**.



Como ejemplo de instalación usaremos el equipo del profesor de la clase 1.

Introducimos nombre de usuario y contraseña para este usuario.





Y como podemos observar, se instalará automáticamente.

Una vez instalado, pasaremos a configurar el archivo de configuración de interfaces **/etc/netplan/01-network-manager-all.yaml**. Como los equipos de los profesores y alumnos solo tienen una interfaz, simplemente configuraremos una interfaz con su dirección IP y puerta de enlace correspondiente.

A screenshot of a terminal window on a Linux desktop. The title bar says 'ubuntu profesor 1 [Corriendo] - Oracle VM VirtualBox'. The terminal shows the command 'profesor1@profesor1-VirtualBox: ~' followed by the path '/etc/netplan/01-network-manager-all.yaml'. The file content is displayed in a code editor window:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      addresses: [192.168.105.2/24]
      routes:
        - to: default
          via: 192.168.105.1
      nameservers:
        addresses: [8.8.8.8]
```

Two orange arrows point from the text 'Y como podemos observar, se instalará automáticamente.' to the terminal window: one arrow points to the file path '/etc/netplan/01-network-manager-all.yaml', and another arrow points to the configuration block for the 'enp0s3' interface.

Siguiendo este mismo procedimiento, realizamos la instalación de las demás máquinas virtuales de profesores y alumnos.

### Alumno 1 clase 1

```
alumno1@alumno1-VirtualBox: ~
$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    queueing discipline: pfifo_fast
    link/ether 08:00:27:ba:19:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.105.3/24 brd 192.168.105.255 scope global noprefixroute
        valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:feba:1914/64 scope link
            valid_lft forever preferred_lft forever
alumno1@alumno1-VirtualBox: ~
```

### Alumno 2 clase 1

```
alumno2@alumno2-VirtualBox: ~
$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    queueing discipline: pfifo_fast
    link/ether 08:00:27:bb:fa:ba brd ff:ff:ff:ff:ff:ff
    inet 192.168.105.4/24 brd 192.168.105.255 scope global noprefixroute
        valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:febba:64/64 scope link
            valid_lft forever preferred_lft forever
alumno2@alumno2-VirtualBox: ~
```

```
profesor2@profesor2-VirtualBox: ~
$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
    queueing discipline: pfifo_fast
    link/ether 08:00:27:5a:e4:33 brd ff:ff:ff:ff:ff:ff
    inet 192.168.106.2/24 brd 192.168.106.255 scope global noprefixroute
        valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe5ae433/64 scope link
            valid_lft forever preferred_lft forever
profesor2@profesor2-VirtualBox: ~
```

### Alumno 1 clase 2

```
alumno1@alumno1-VirtualBox:~$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ae:db:d1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.106.3/24 brd 192.168.106.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feae:dbd1/64 brd fe80::ff:ffff:ffff:ffff scope link
        valid_lft forever preferred_lft forever
alumno1@alumno1-VirtualBox:~$
```

## Alumno 2 clase 2

```
alumno2@alumno2-VirtualBox:~$ ip ad
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 00:00:00:00:00:00 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 00:00:00:00:00:00 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e5:b8:6c brd ff:ff:ff:ff:ff:ff
    inet 192.168.106.4/24 brd 192.168.106.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fee5:b86c/64 brd fe80::ff:ffff:ffff:ffff scope link
        valid_lft forever preferred_lft forever
alumno2@alumno2-VirtualBox:~$
```

Y además, como podemos observar en esta captura de pantalla, vemos como los equipos consiguen tener internet gracias a la configuración de reenvío de paquetes y nat masquerade que montamos en el equipo router.

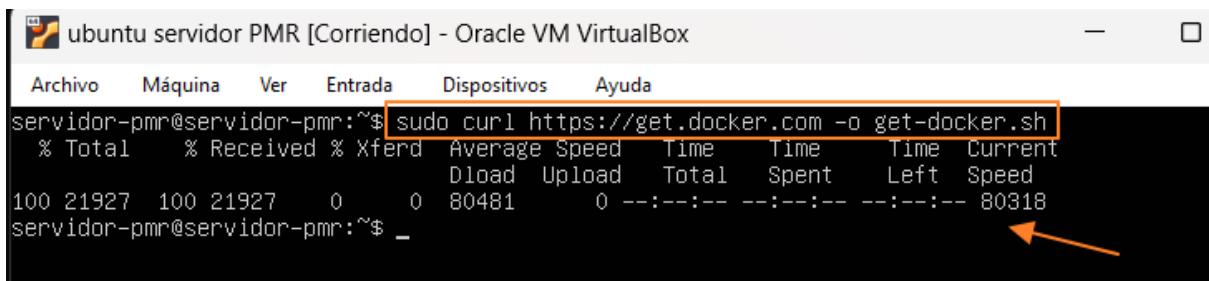
```
alumno2@alumno2-VirtualBox:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=32.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=32.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=32.7 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 32.578/32.644/32.706/0.052 ms
alumno2@alumno2-VirtualBox:~$
```

## Anexo III

### INSTALACIÓN DE LA HERRAMIENTA DOCKER

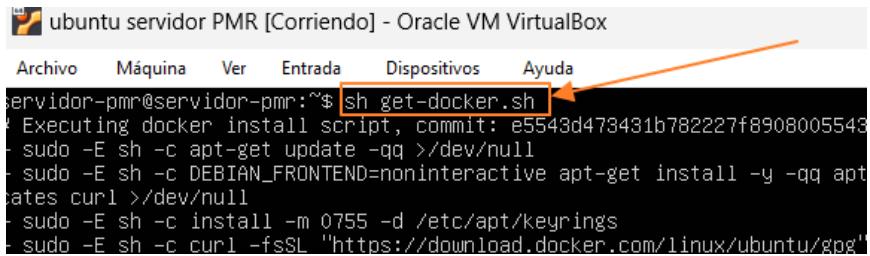
Para este apartado haremos uso de la herramienta **Docker**.

Para instalar la herramienta utilizaremos el siguiente comando.



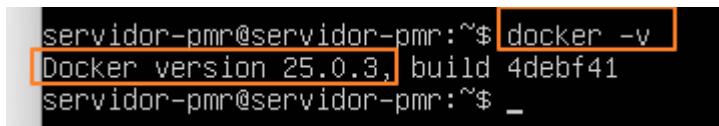
A screenshot of a terminal window titled "ubuntu servidor PMR [Corriendo] - Oracle VM VirtualBox". The window shows a command being run: "sudo curl https://get.docker.com -o get-docker.sh". The output shows the progress of the download, including the total size (100), received bytes (21927), and speed (80481). An orange arrow points from the text "Como vemos, se nos ha descargado un script de instalación el cual correremos de la siguiente manera." to the command line.

Como vemos, se nos ha descargado un script de instalación el cual correremos de la siguiente manera.



A screenshot of a terminal window titled "ubuntu servidor PMR [Corriendo] - Oracle VM VirtualBox". The window shows the command "sh get-docker.sh" being run. An orange arrow points from the text "Como podemos ver, se nos ha descargado la versión de docker 25.0.3." to the command line.

Como podemos ver, se nos ha descargado la versión de **docker 25.0.3**.



A screenshot of a terminal window titled "ubuntu servidor PMR [Corriendo] - Oracle VM VirtualBox". The window shows the command "docker -v" being run, which outputs "Docker version 25.0.3, build 4debf41". An orange arrow points from the text "Para poder usar moodle tendremos que hacer uso de un archivo llamado Docker Compose." to the command line.

### INSTALACIÓN DE MOODLE

Para poder usar moodle tendremos que hacer uso de un archivo llamado **Docker Compose**. Docker Compose es una herramienta que permite definir y ejecutar aplicaciones Docker de manera multi-contenedor de una manera sencilla y declarativa. Permite describir

las relaciones entre diferentes servicios, como contenedores, redes y volúmenes, en un archivo YAML llamado docker-compose.yml. Con Docker Compose, puedes definir la configuración de tu aplicación una vez y luego utilizar un solo comando para crear y arrancar todos los servicios definidos en tu archivo docker-compose.yml.

Crearemos el archivo llamado **docker-compose.yaml**.

```
servidor-pmr@servidor-pmr:~$ sudo touch docker-compose.yaml
[sudo] password for servidor-pmr:
servidor-pmr@servidor-pmr:~$
```

```
GNU nano 6.2
version: '3'
services:
  mariadb:
    image: mariadb
    environment:
      - MYSQL_ROOT_PASSWORD=moodle
      - MYSQL_ROOT_USER=root
      - MYSQL_DATABASE=moodle
  moodle:
    image: bitnami/moodle:latest
    ports:
      - 8080:8080
      - 8443:8443
    environment:
      - MOODLE_DATABASE_HOST=mariadb
      - MOODLE_DATABASE_USER=root
      - MOODLE_DATABASE_PASSWORD=moodle
      - MOODLE_DATABASE_NAME=moodle
      - MOODLE_USERNAME=javierh
      - MOODLE_PASSWORD=javierh
    depends_on:
      - mariadb
    links:
      - mariadb:mariadb
```

Una vez creado el archivo de docker compose, lo que deberemos hacer es editarla y añadir las siguientes líneas de configuración.

Este archivo es un ejemplo de un archivo de configuración de Docker Compose. Aquí hay una explicación de cada parte:

**version: '3'**: Esta línea especifica la versión de la sintaxis de Docker Compose que se está utilizando. En este caso, es la versión 3.

**services**: Esta sección define los servicios que se ejecutarán como contenedores Docker.

**mariadb**: Este es el servicio para la base de datos MariaDB. Utiliza la imagen mariadb del Docker Hub.

**environment:** Aquí se definen variables de entorno para configurar la base de datos MariaDB, como la contraseña de root, el usuario root y el nombre de la base de datos Moodle.

**moodle:** Este es el servicio para la aplicación Moodle. Utiliza la imagen bitnami/moodle:latest del Docker Hub.

**ports:** Esta línea mapea los puertos 8080 y 8443 del contenedor al mismo número de puertos en el host. Esto permite acceder a Moodle a través de estos puertos en el host.

**depends\_on:** Esta línea especifica que el servicio de Moodle depende del servicio de MariaDB, lo que significa que Docker Compose garantizará que el servicio de MariaDB esté en funcionamiento antes de iniciar el servicio de Moodle.

**links:** Esta línea establece un enlace entre el servicio de Moodle y el servicio de MariaDB, lo que permite que Moodle se comunique con la base de datos.

Guardamos el contenido del archivo, y para hacer que funcione el contenedor simplemente hacemos uso del siguiente comando.

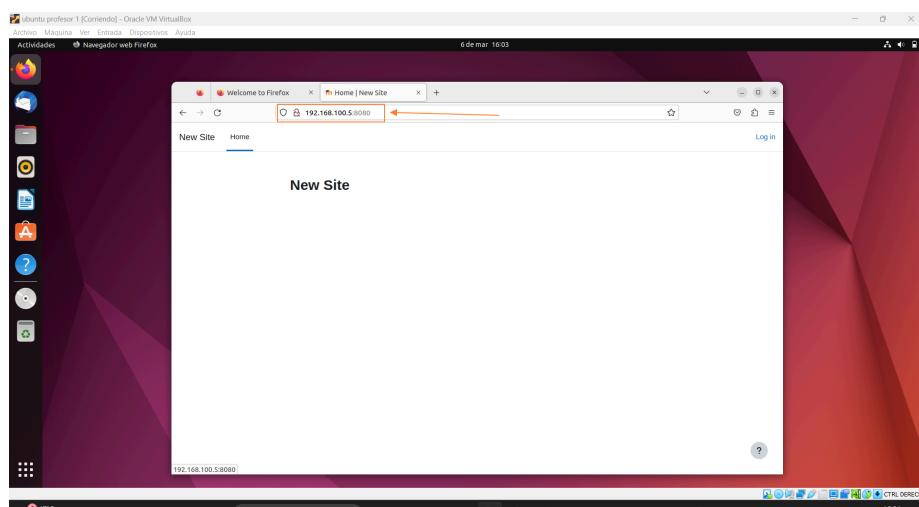
Como podemos observar, al no tener los paquetes de los servicios instalados, docker los descarga automáticamente.

```
ubuntu servidor PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
servidor-pmr@servidor-pmr:~$ sudo docker-compose up
[+] Running 10/11
  $ moodle 1 layers [+] 0B/0B Pulling
  $ 9a072f9f1de0 Download complete
  $ mariadb 8 layers [*****]
  $ bcccd10f490ab Pull complete
  $ d9d8e1823c6f Pull complete
  $ 4b658f15686b Pull complete
  $ 153080ffccddf Pull complete
  $ fc85f7aae1e5 Pull complete
  $ 59efdf043a883 Pull complete
  $ 676a7ad9f737 Pull complete
  $ 335ef3100b9e Pull complete
```

Como podemos observar, nuestro contenedor de **Moodle** y **Mariadb** está funcionando correctamente.

```
servidor-pmr-mariadb-1 | 2024-03-06 15:59:28 0 [Note] InnoDB: Loading buffer pool(s) from /var/lib/mysql/ib_buffer_pool
servidor-pmr-mariadb-1 | 2024-03-06 15:59:28 0 [Note] InnoDB: Buffer pool(s) load completed at 2403
06 15:59:28
servidor-pmr-mariadb-1 | 2024-03-06 15:59:28 0 [Note] Server socket created on IP: '0.0.0.0'.
servidor-pmr-mariadb-1 | 2024-03-06 15:59:28 0 [Note] Server socket created on IP: '::'.
servidor-pmr-mariadb-1 | 2024-03-06 15:59:28 0 [Note] mariadb: Event Scheduler: Loaded 0 events
servidor-pmr-mariadb-1 | 2024-03-06 15:59:28 0 [Note] mariadb: ready for connections.
servidor-pmr-mariadb-1 | Version: '11.3.2-MariaDB-1:11.3.2+maria' 'ubuntu2204' socket: '/run/mysqld/mysqld.sock' port: 3306
mariadb.org binary distribution
Certificate request self-signature ok
subject=
CN =
e
x
m
a
p
l
e
.
c
om
realpath: /bitnami/apache/conf: No such file or directory
moodle 15:59:29.44 INFO => Configuring Apache ServerTokens directive
moodle 15:59:29.46 INFO => Configuring PHP options
moodle 15:59:29.47 INFO => Setting PHP expose_php option
moodle 15:59:29.48 INFO => Setting PHP output_buffering option
moodle 15:59:29.49 INFO => Validating settings in MYSQL_CLIENT_* env vars
servidor-pmr-moodle-1 | moodle 15:59:29.50 INFO => Validating settings in POSTGRESQL_CLIENT_* env vars
servidor-pmr-moodle-1 | moodle 15:59:29.56 INFO => Ensuring Moodle directories exist
servidor-pmr-moodle-1 | moodle 15:59:29.58 INFO => Trying to connect to the database server
servidor-pmr-moodle-1 | moodle 15:59:29.59 INFO => Running Moodle install script
```

Como podemos observar, podemos acceder a la Moodle desde un equipo usuario.



## CONFIGURACIÓN DE LA MOODLE

### CREACIÓN DE CATEGORÍAS

Para crear las categorías nos dirigimos a la parte de **administración del moodle**.

Una vez dentro del apartado de administración, nos dirigimos al apartado de “**cursos**”.

Para crear las categorías, vamos al apartado de “**crear categoría**”.

The screenshot shows the Moodle Site administration interface. The 'Courses' tab is selected. On the right, there is a sidebar titled 'Manage courses and categories' with several options: 'Add a category' (which is highlighted with a red arrow), 'Add a new course', 'Restore course', 'Download course content', 'Course request', 'Pending requests', and 'Upload courses'. The URL in the browser is 192.168.100.5:8080/admin/search.php#linkcourses.

Le asignamos un **nombre** a la categoría.

The screenshot shows the 'Add new category' form under the 'New Site' section. The 'Category name' field is highlighted with a red arrow and contains the text '2º ASIR Tardé'. Other fields include 'Parent category' (set to 'Top'), 'Category ID number' (empty), and 'Description' (empty). The URL in the browser is 192.168.100.5:8080/course/editcategory.php?parent=0.

Y como podemos comprobar, las dos categorías(cursos) se han creado correctamente.

The screenshot shows the Moodle administration interface for the '1º DAM Tarde' site. Under 'Course categories', there are three entries: 'Category 1', '2º ASIR Tarde', and '1º DAM Tarde'. The '2º ASIR Tarde' category is highlighted with a red box and an orange arrow pointing from the explanatory text above. The '1º DAM Tarde' category is also highlighted with a blue box.

## CREACIÓN DE LAS MATERIAS DE LAS CATEGORÍAS

Para crear las materias, simplemente accedemos a “**mis cursos**” en el panel superior de moodle.

Y hacemos clic en “**crear curso**”.

The screenshot shows a Linux desktop with a Unity interface. A Firefox window is open to the URL '192.168.100.5:8080/my/courses.php'. The browser title bar says 'My courses | New Site'. On the left, there's a vertical dock with icons for Dash, Home, Dashboards, My courses, and Site administration. An orange arrow points from the explanatory text to the 'Create your first course' button at the bottom of the Moodle page.

Le asignamos un **nombre, unas siglas** y le asignamos la **categoría correspondiente**.

The screenshot shows the Moodle 'Add a new course' interface. The course name is 'Administración de sistemas operativos'. The short name field is empty, indicated by a red error message: '- Missing short name'. The category is set to '2º ASIR Tarde'. The visibility is set to 'Show'. Arrows from the text explain the fields: one arrow points to the 'Course full name' input field, another to the 'Course short name' input field, and a third to the 'Course category' dropdown.

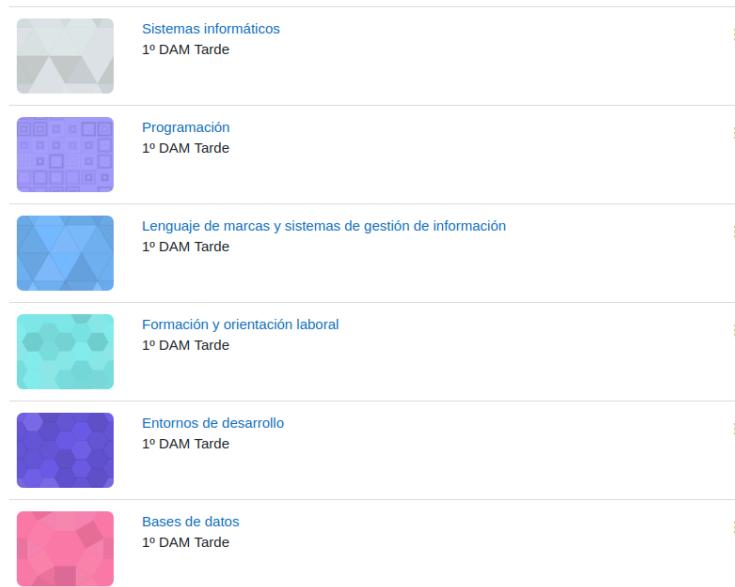
Siguiendo este proceso, creamos todas las asignaturas de los dos cursos correspondientes.

Estas son las asignaturas de **2ºASIR Tarde**.

The screenshot shows the Moodle 'My courses' page with six course cards:

- Administración de sistemas gestores de base de datos 2º ASIR Tarde
- Administración de sistemas operativos 2º ASIR Tarde
- Empresa e iniciativa emprendedora 2º ASIR Tarde
- Implantación de aplicaciones web 2º ASIR Tarde
- Seguridad y alta disponibilidad 2º ASIR Tarde
- Servicios de red e internet 2º ASIR Tarde

Y estas son las asignaturas de **1º DAM Tarde**.



## CREACIÓN DE USUARIOS

Para crear los usuarios accedemos a la **administración del sitio**, luego accedemos a “**usuarios**” y finalmente hacemos clic en “**añadir un nuevo usuario**”.

A screenshot of a Moodle site's 'Site administration' section, specifically the 'Users' page. An orange arrow points from the 'Users' tab in the navigation bar to the 'Add a new user' link in the sidebar menu.

The screenshot shows the following interface elements:

- Top Bar:** Shows the browser title 'ubuntu profesor 1 [Corriendo] - Oracle VM VirtualBox', the address bar '192.168.100.5:8080/admin/search.php#linkusers', and the date/time '6 de mar 18:16'.
- Left Sidebar:** Includes icons for File Manager, Control Panel, Home, Dashboard, My courses, and Site administration.
- Main Navigation:** 'Site administration' menu with tabs: General, Courses, Grades, Plugins, Appearance, Server, Reports, Development. The 'Users' tab is highlighted with a blue box and an orange arrow pointing to it.
- Sub-navigation:** 'Accounts' section with links: Browse list of users, Bulk user actions, Add a new user (highlighted with an orange arrow), User management, User default preferences, User profile fields, Cohorts, Cohort custom fields, Upload users, and Upload user pictures.

Nos pedirá la siguiente información, un nombre de usuario, un método de autenticación, una contraseña, nombre, apellidos y un correo electrónico.

The screenshot shows the 'Create user' page in Moodle. The 'General' tab is selected. The fields filled are:

- Username: francish
- Choose an authentication method: Manual accounts
- New password: Click to enter text (with a red arrow pointing to it)
- First name: francisco
- Last name: hernandez
- Email address: francish@profesor.ieselincon.es (with a red arrow pointing to it)
- Email visibility: Visible to course participants

Para las contraseñas seguiremos un **manual de creación de contraseñas** seguras creado por el **Instituto Nacional de Ciberseguridad (INCIBE)**.



Como vemos, se ha creado correctamente el usuario. Siguiendo el mismo procedimiento, creamos los usuarios restantes.

Accounts / Browse list of users

### I.E.S El Rincón

General Users Courses Grades Plugins Appearance Server Reports Development

#### 7 Users

✓ New filter

User full name  contains

Show more...  Add filter

First name / Last name	Email address	City/town	Country
Admin User	user@example.com		
alejandro monroy	alejandromonroy@alumno.ieselrincon.es		
francisco hernandez	franchis@profesor.ieselrincon.es		
iker suarez	ikersuarez@alumno.ieselrincon.es		
manuel benitez	manuelbenitez@profesor.ieselrincon.es		
mario suarez	mariosuarez@alumno.ieselrincon.es		
ruben romero	rubenromero@alumno.ieselrincon.es		

Add a new user

## CONFIGURACIÓN COHORTE

Los usuarios alumnos deberían solo ver las asignaturas en las que se supone que están matriculados, para esto hay que crear cohortes y añadir los usuarios. Para ello nos dirigimos a “**administración del sitio**” y luego a “**usuarios**”. En este apartado nos aparecerá la opción de “**cohorte**”.

Navegador web Firefox

Welcome to Firefox | Search | Administration | +

192.168.100.5:8080/admin/search.php#linkusers

El Rincón Home Dashboard My courses Site administration

Site administration

General Users Courses Grades Plugins Appearance Server Reports Development

Users

Accounts

- Browse list of users
- Bulk user actions
- Add a new user
- User management
- User default preferences
- User profile fields
- Cohorts
- Cohort custom fields
- Upload users
- Upload user pictures

Le asignamos un **nombre** al cohorte y le asignamos la **categoría correspondiente**.

ubuntu profesor 1 [Corriendo] - Oracle VM VirtualBox

Archivo Maquina Ver Entrada Dispositivos Ayuda

Actividades Navegador web Firefox

Welcome to Firefox | Add new cohort | El Rincón | +

192.168.100.5:8080/cohort/edit.php?contextid=1

El Rincón Home Dashboard My courses Site administration

Accounts / Cohorts / Add new cohort

I.E.S El Rincón

General Users Courses Grades Plugins Appearance Server Reports Development

Para asignar alumnos a las cohortes haremos clic en “**asignar**”.

Category	Name	Cohort ID	Description	Cohort size	Source
1º DAM Tardé	1º DAM Tardé			0	Created manually
2º ASIR Tardé	2º ASIR Tardé			0	Created manually

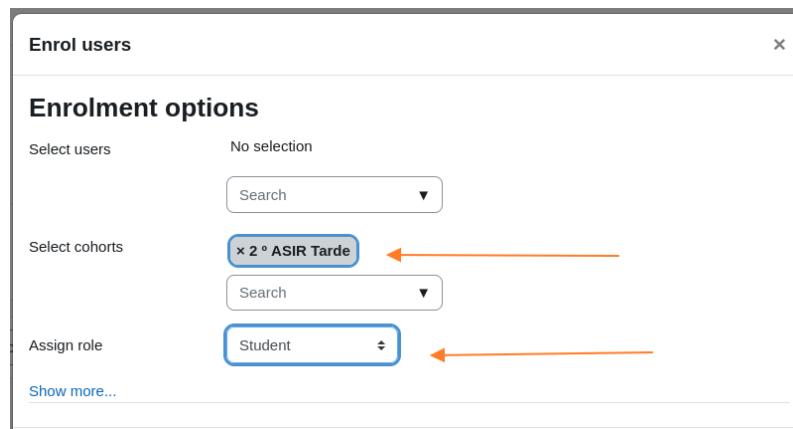
Y añadimos los **usuarios** que queremos asignar a esa **cohorte**.

Category	Settings	More
<b>Cohort '1º DAM Tardé' members</b>		
Removing users from a cohort may result in unenrolling of users from multiple courses which includes deleting of user settings, grades, group membership and other user information from affected courses.		
<b>Current users (2)</b> alejandro monroy (alejandromonroy@alumno.ieselrincon.es) ruben romero (rubenromero@alumno.ieselrincon.es)	<b>Potential users (9)</b> manuel benito (manuelbenito@profesor.ieselrincon.es) francisco hernandez (francky@profesor.ieselrincon.es) iker suarez (kersuarez@alumno.ieselrincon.es) mario suarez (manosuarez@alumno.ieselrincon.es) Admin User (user@example.com)	<b>Add</b> <b>Remove</b>

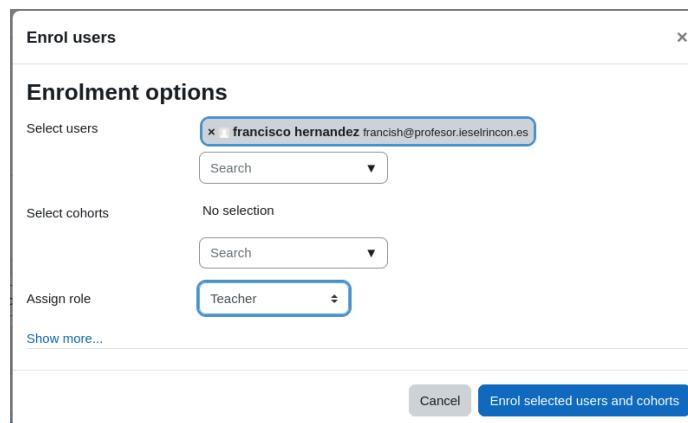
Y así con las dos cohortes creadas.

## MATRICULAR ALUMNOS EN ASIGNATURAS

Para ello iremos a los cursos y en “**participantes**” añadiremos los usuarios de la cohorte correspondiente. Además, le asignaremos el **rol** de estudiante a estos usuarios.



Ahora, asignaremos a los profesores sus asignaturas correspondientes. Para ello seguimos el mismo procedimiento que con los usuarios estudiantes, pero en nuestro caso seleccionamos el usuario en concreto y el rol de profesor.



Como podemos observar, si entramos a la Moodle con un usuario de la clase 2º ASIR Tarde, solo nos aparecerán las asignaturas correspondientes con el curso 2º ASIR.

Lo mismo sucede con un usuario de la clase 1º DAM tarde.

The screenshot shows a Moodle 'My courses' page with six course cards arranged in two rows of three. The cards are titled: 'Bases de datos 1º DAM Tarde', 'Entornos de desarrollo 1º DAM Tarde', 'Formación y orientación laboral 1º DAM Tarde', 'Lenguaje de marcas y sistemas de gestión de ... 1º DAM Tarde', 'Programación 1º DAM Tarde', and 'Sistemas informáticos 1º DAM Tarde'. Each card has a three-dot menu icon at the bottom right. The top right corner of the slide features orange arrows pointing towards the search bar, sort dropdown, and card dropdown. The bottom right corner features an arrow pointing towards the toolbar.

En cambio si entramos con un usuario profesor, nos saldrán las asignaturas en las que ese profesor de clase, independientemente del curso.

This screenshot shows a Moodle 'My courses' page with only two course cards visible: 'Entornos de desarrollo 1º DAM Tarde' and 'Implantación de aplicaciones web 2º ASIR Tarde'. The top right corner of the slide features orange arrows pointing towards the search bar, sort dropdown, and card dropdown. The bottom right corner features an arrow pointing towards the toolbar.

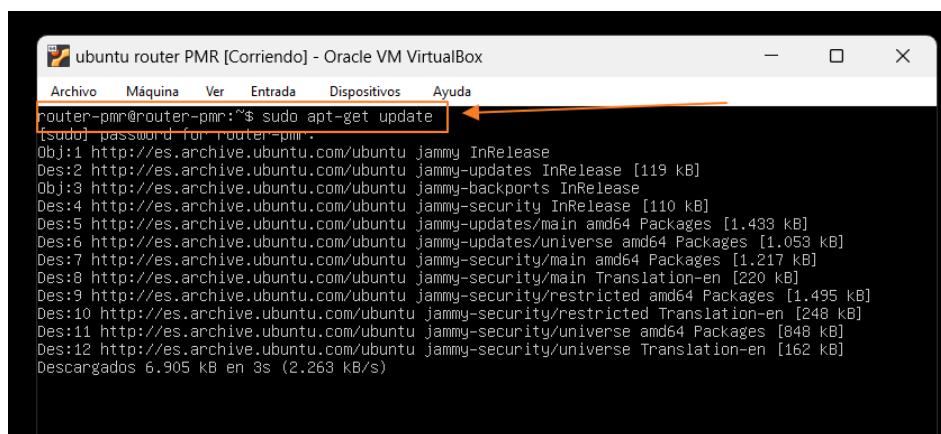
Para cerrar los contenedores de Docker sin que se pierda el progreso de la Moodle se pierda, usaremos el siguiente comando en el servidor.

```
servidor-pmr@servidor-pmr:~$ sudo docker-compose stop
[+] Stopping 2/2
  ⬤ Container servidor-pmr-moodle-1    Stopped
  ⬤ Container servidor-pmr-mariadb-1   Stopped
servidor-pmr@servidor-pmr:~$
```

## Anexo IV

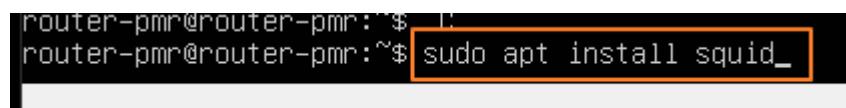
### INSTALAR PROXY SQUID

Lo primero que haremos en este apartado será actualizar los repositorios del sistema operativo.



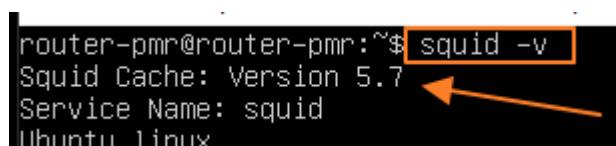
```
ubuntu router PMR [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
router-pmr@router-pmr:~$ sudo apt-get update
[sudo] password for router-pmr:
Obj:1 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Obj:3 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
Des:4 http://es.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1.433 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1.053 kB]
Des:7 http://es.archive.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1.217 kB]
Des:8 http://es.archive.ubuntu.com/ubuntu jammy-security/main Translation-en [220 kB]
Des:9 http://es.archive.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [1.495 kB]
Des:10 http://es.archive.ubuntu.com/ubuntu jammy-security/restricted Translation-en [248 kB]
Des:11 http://es.archive.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [848 kB]
Des:12 http://es.archive.ubuntu.com/ubuntu jammy-security/universe Translation-en [162 kB]
Descargados 6.905 kB en 3s (2.263 kB/s)
```

Lo siguiente que haremos será el servicio de SQUID con el siguiente comando.



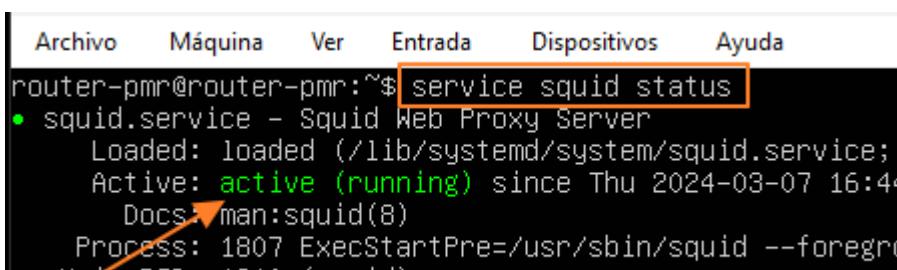
```
router-pmr@router-pmr:~$ sudo apt install squid
```

El siguiente comando nos devolverá la versión que se ha instalado de squid. Como vemos es la versión 5.7.



```
router-pmr@router-pmr:~$ squid -v
Squid Cache: Version 5.7
Service Name: squid
Ubuntu linux
```

Finalmente, podemos observar que el servicio está activo, lo revisamos con el siguiente comando.



```
Archivo Máquina Ver Entrada Dispositivos Ayuda
router-pmr@router-pmr:~$ service squid status
● squid.service - Squid Web Proxy Server
  Loaded: loaded (/lib/systemd/system/squid.service;
  Active: active (running) since Thu 2024-03-07 16:48:41
    Docs: man:squid(8)
  Process: 1807 ExecStartPre=/usr/sbin/squid --foreground
          └─ 1807 /usr/sbin/squid --foreground
```

## QUE ES UNA ACL Y COMO SE DEFINE

Los elementos ACL nos permiten definir los grupos de equipos, dominios y horarios. Y las listas de ACL son

las que nos permiten elegir los elementos y le daremos la orden de si queremos permitir o denegar el acceso.

La sintaxis de una ACL se compone de los siguientes elementos “acl aclname(nombre del elemento) acctype

(tipo de acl)argument(acción a realizar)”

## CONFIGURACIÓN POR DEFECTO SQUID

En este apartado observaremos que configuración viene por defecto en el servidor squid, para ello primero nos colocaremos en el directorio /etc/squid/ y listamos los archivos.

```
router-pmr@router-pmr:/etc/squid$ cd /etc/squid/
router-pmr@router-pmr:/etc/squid$ ls -l
total 344
drwxr-xr-x 2 root root    4096 mar  7 16:44 conf.d
-rw-r--r-- 1 root root    1800 ene 17 04:01 errorpage.css
-rw-r--r-- 1 root root 342138 ene 17 04:01 squid.conf
router-pmr@router-pmr:/etc/squid$
```



Lo primero que deberemos hacer es hacer una copia de seguridad del archivo de configuración.

```

Archivo Máquina Ver Entrada Dispositivos Ayuda
router-pmr@router-pmr:/etc/squid$ sudo cp squid.conf squid.conf.backup
router-pmr@router-pmr:/etc/squid$ ls -la
total 688
drwxr-xr-x 3 root root 4096 mar  7 16:57 .
drwxr-xr-x 99 root root 4096 mar  7 16:44 ..
drwxr-xr-x 2 root root 4096 mar  7 16:44 conf.d
-rw-r--r-- 1 root root 1800 ene 17 04:01 errorpage.css
-rw-r--r-- 1 root root 342138 ene 17 04:01 squid.conf
-rw-r--r-- 1 root root 342138 mar  7 16:57 squid.conf.backup
router-pmr@router-pmr:/etc/squid$ _

```

Eliminaremos todos los comentarios y las líneas con espacios del archivo de configuración primario con las instrucciones siguientes, accediendo a él con el comando sudo vim squid.conf.

Las instrucciones son las siguientes:

- :g/^#d - Para borrar los comentarios.
- :g/^\$/d - Para borrar las líneas sobrantes.

El archivo quedaría de la siguiente manera:

```

Archivo Máquina Ver Entrada Dispositivos Ayuda
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8      # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10    # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16   # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12    # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16   # RFC 1918 local private network (LAN)
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-ssl
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
http_access deny all
http_port 3128
coredump_dir /var/spool/squid
refresh_pattern ^ftp:           1440    20%    10080
refresh_pattern ^gopher:        1440    0%     1440
refresh_pattern -i ((/cgi-bin/|\.?)|(\.bz2|\.gz|\.xz)$) 0 0% 0 refresh-ims
refresh_pattern /Release(\.|\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern /InRelease$ 0 0% 0 refresh-ims
refresh_pattern /Translation-(*) (\.|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern .               0      20%    4320

```

En el que podemos ver que quedan solo las ACL de redes privadas, elementos de puertos seguros y las listas de bloqueo de acceso.

## COMPROBAR FUNCIONAMIENTO PROXY SQUID

Para comprobar el funcionamiento del proxy SQUID haremos uso del comando curl desde una terminal de una máquina no conectada al servidor.

El parámetro “-x” nos sirve para indicar que es una consulta a través de un servidor proxy. Y con el parámetro “-I” le indicamos que solo no muestre el encabezado.

Al introducir el comando de la imagen, nos mostrará que el acceso está restringido a esa página y nos devolverá desde qué dispositivo estamos realizando la conexión, en mi caso desde el servidor squid 5.7.

```
connect to server
profesor1@profesor1-VirtualBox:~$ curl -x http://192.168.100.2:3128 -I http://www.google.com/
HTTP/1.1 403 Forbidden
Server: squid/5.7
Mime-Version: 1.0
Date: Thu, 07 Mar 2024 17:14:45 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3514
X-Squid-Error: ERR_ACCESS_DENIED 0
Vary: Accept-Language
Content-Language: en
X-Cache: MISS from router-pmr
X-Cache-Lookup: NONE from router-pmr:3128
Via: 1.1 router-pmr (squid/5.7)
Connection: keep-alive
```

## CONFIGURAR PROXY SQUID

Para configurar correctamente el servidor proxy squid deberemos acceder al fichero de configuración **conf.d** y habilitar la ruta hacia otro fichero que crearemos posteriormente con todas las reglas pertinentes.

```
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/myrules.conf_
http_access allow localhost
http_access deny all
http_port 3128
```

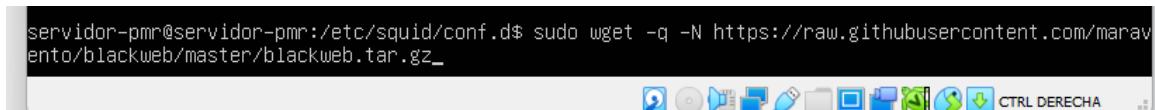
Creamos el fichero con el comando touch.

```
ARCHIVO  IMAGINA  VAI  LIMPIA  DISPOSITIVOS  Ayuda
router-pmr@router-pmr:/etc/squid/conf.d$ sudo touch myrules.conf
router-pmr@router-pmr:/etc/squid/conf.d$
```

Antes de realizar la configuración, existen listas de dominios ya preconfiguradas, las cuales podemos descargar y usar para nuestro servidor squid.

Estas listas son muy útiles ya que recogen sitios no recomendados por la comunidad.

Nos descargamos la siguiente lista y en la posterior configuración de reglas ACL la aplicaremos, para ello usaremos el siguiente comando.



```
servidor-pmr@servidor-pmr:/etc/squid/conf.d$ sudo wget -q -N https://raw.githubusercontent.com/maravento/blackweb/master/blackweb.tar.gz
```

Una vez descargada la lista de dominios, debemos configurar las ACLs.

Lo haremos de la siguiente manera.



```
acl red1 src 192.168.105.0/24
acl red2 src 192.168.106.0/24

acl blackweb dstdomain "etc/squid/conf.d/blackweb.txt"

http_access deny blackweb
http_access allow red1
http_access allow red2
```

En las dos primeras ACLs estamos declarando las redes de las clases.

En la tercera ACL estamos indicando la ruta del archivo que contiene los dominios que queremos bloquear.

En la siguiente línea, mediante el parámetro “http\_access deny” estamos denegando el acceso http a los dominios de blackweb.

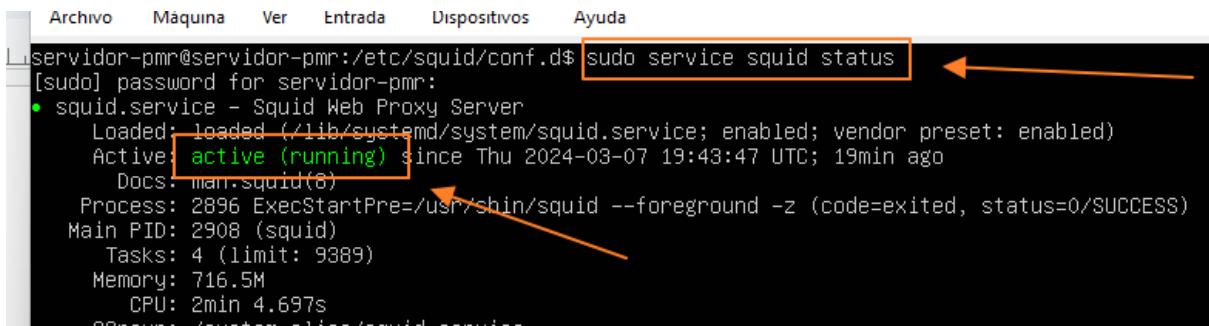
Y finalmente, en las dos últimas líneas, habilitamos la navegación por http a ambas redes.

Para aplicar los cambios utilizaremos el comando mostrado en la captura.



```
Lservidor-pmr@servidor-pmr:/etc/squid/conf.d$ sudo service squid restart
```

Como podemos observar, el servicio está funcionando correctamente.

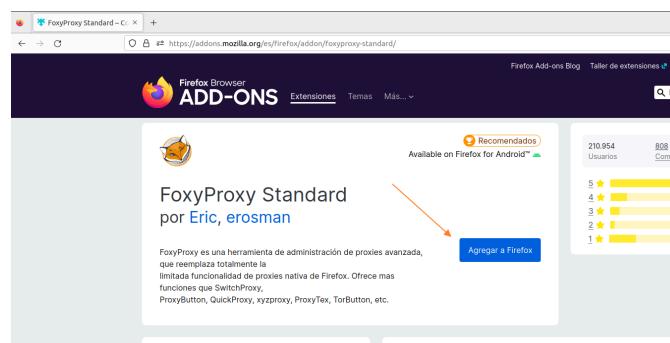


```
Lservidor-pmr@servidor-pmr:/etc/squid/conf.d$ sudo service squid status
[sudo] password for servidor-pmr:
● squid.service - Squid Web Proxy Server
  Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2024-03-07 19:43:47 UTC; 19min ago
    Docs: man:squid(8)
   Process: 2896 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 2908 (squid)
   Tasks: 4 (limit: 9389)
  Memory: 716.5M
     CPU: 2min 4.697s
    CGroup: /system.slice/squid.service
```

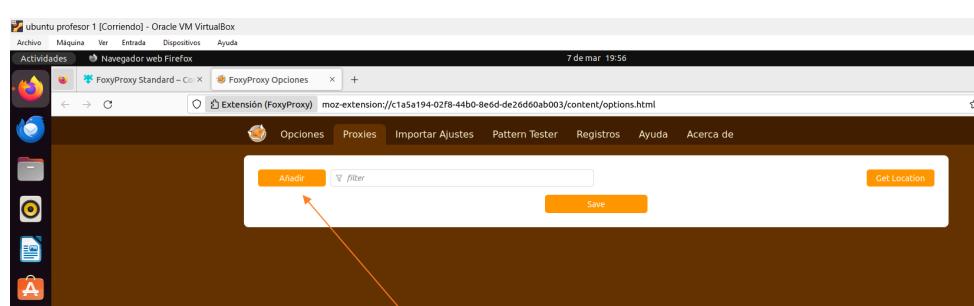
## CONFIGURACIÓN CLIENTES

Este apartado deberemos realizarlo en todos los equipos usuarios de la red.

En el navegador firefox, descargamos la extensión FoxyProxy.



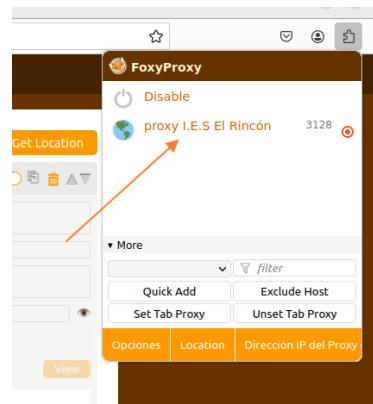
Una vez instalada dicha extensión, deberemos añadir el servidor proxy en la configuración, haciendo clic en “añadir”.



Añadiremos un nombre, que tipo de servidor proxy va a ser, en nuestro caso **HTTP**, y finalmente la **dirección IP** de dicho servidor, para guardar los cambios hacemos clic en “**save**”.



Finalmente activamos dicha configuración en la extensión.



Como podemos observar en la captura de pantalla, podemos acceder a la página del centro.

Pero no podremos acceder a la página del diario deportivo Marca.



## Anexo V

### Descarga de Wazuh - SIEM

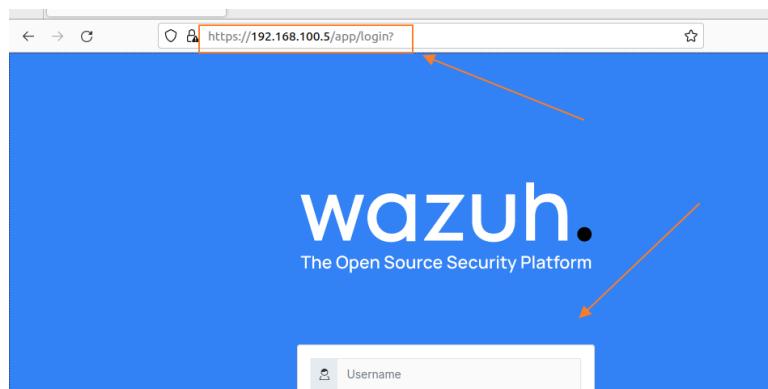
Para descargar la herramienta Wazuh usaremos el siguiente comando.

```
bash: ./wazuh-install.sh: No such file or directory
a|servidor-pmr@servidor-pmr:~$ curl -s0 https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash
/wazuh-install.sh -a
08/03/2024 17:23:43 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.3
08/03/2024 17:23:43 INFO: Verbose logging redirected to /var/log/wazuh-install.log
d t08/03/2024 17:23:51 INFO: Wazuh web interface port will be 443.
08/03/2024 17:23:56 INFO: Wazuh repository added.
08/03/2024 17:23:56 INFO: Configuration files
```

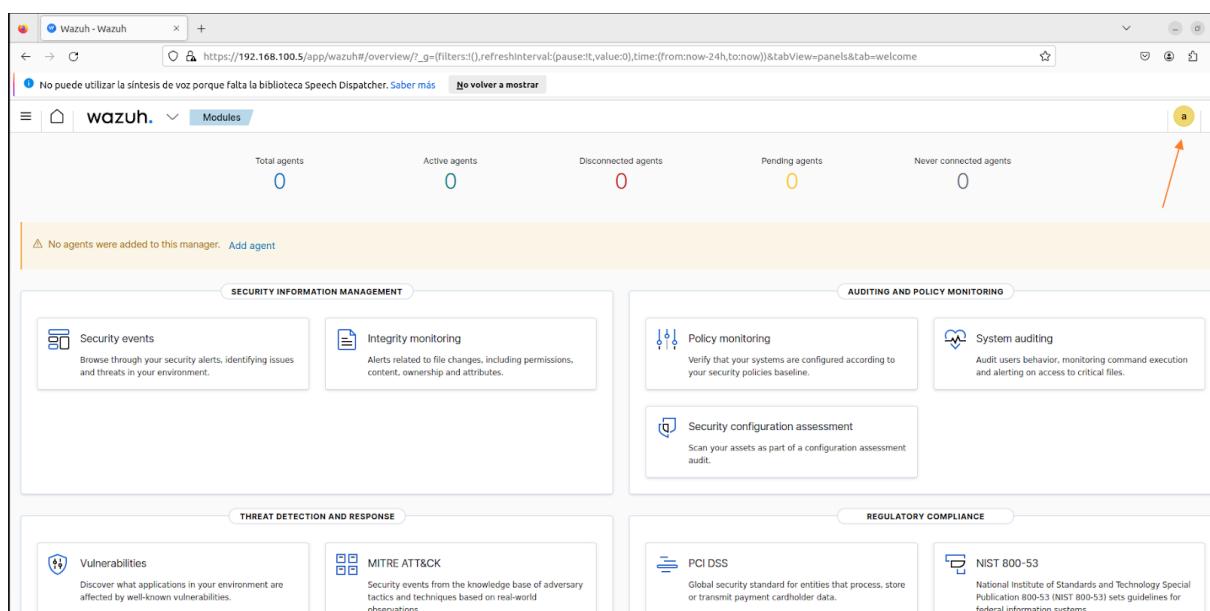
Cuando el proceso de instalación nos devolverá un usuario, contraseña y url para poder acceder a la interfaz.

```
08/03/2024 17:32:08 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: utotj4AzjG1cZaiONGV+MA04V+fkth8a
08/03/2024 17:32:08 INFO: Installation finished.
servidor-pmr@servidor-pmr:~$ _
```

Como podemos observar, si accedemos desde un navegador a esa url, nos aparecerá la interfaz para ingresar con un usuario.



Al ingresar con el usuario y contraseña que se nos facilitó durante la instalación, nos aparecerá el dashboard de la herramienta.



## AÑADIR AGENTES

Los agentes no son más que los equipos que queremos que dirija los logs la herramienta. Para ello simplemente hacemos clic en “**add agent**”.

Total agents: 0      Active agents: 0      Disconnected agents: 0

⚠️ No agents were added to this manager. [Add agent](#)

Seleccionamos la arquitectura del sistema operativo, y le añadimos la dirección IP del servidor.

Select the package to download and install on your system:

- LINUX** (selected)
  - RPM amd64
  - RPM aarch64
  - DEB amd64**
  - DEB aarch64
- WINDOWS**
  - MSI 32/64 bits
- macOS**
  - Intel
  - Apple silicon

For additional systems and architectures, please check our documentation [ct](#).

**Server address:**  
This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address: [ct](#)  
192.168.100.5

**Optional settings:**  
By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Le asignamos un nombre al agente, en nuestro caso estamos haciendo el ejemplo con el equipo del profesor de la clase 1.

**Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: [ct](#)  
profesor01

⚠️ The agent name must be unique. It can't be changed once the agent has been enrolled. [ct](#)

Lo siguiente que deberemos hacer es usar este comando que se nos administra en el equipo agente, es decir; en el equipo del profesor.

#### 4 Run the following commands to download and install the agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.3-1_amd64.deb &&
sudo WAZUH_MANAGER='192.168.100.5' WAZUH_AGENT_NAME='profesor01' dpkg -i ./wazuh-
agent_4.7.3-1_amd64.deb
```



##### ① Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

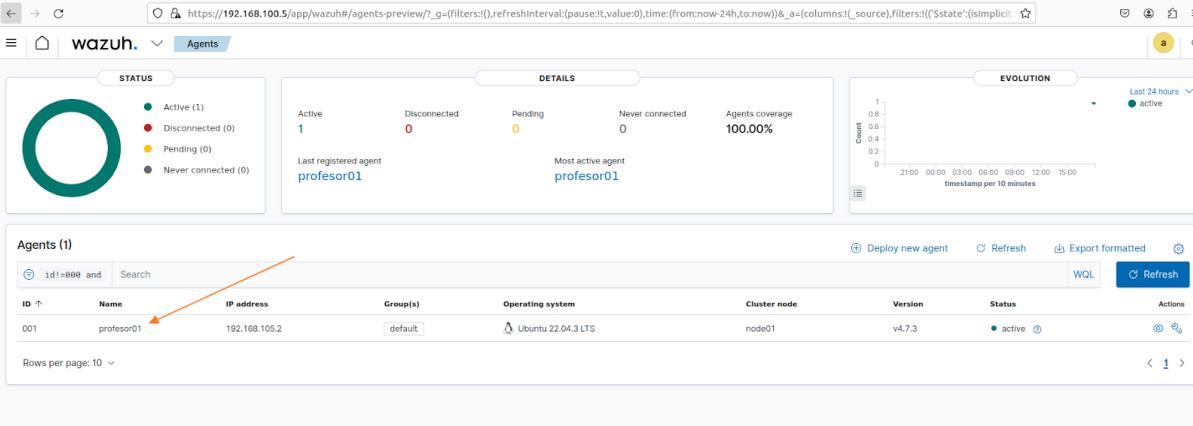
Y con el siguiente comando habilitamos el agente.

#### Start the agent:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```



Y como vemos, ya nos aparece disponible el agente “profesor01”.



ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	profesor01	192.168.105.2	default	Ubuntu 22.04.3 LTS	node01	v4.7.3	active	

Tendremos que seguir este procedimiento en todos los equipos de la red.

Como podemos observar, ya tenemos añadidos todos los equipos de la red.

Además de la información del equipo como la **dirección IP**, también nos aparecerá si los equipos están **activos o no activos**.

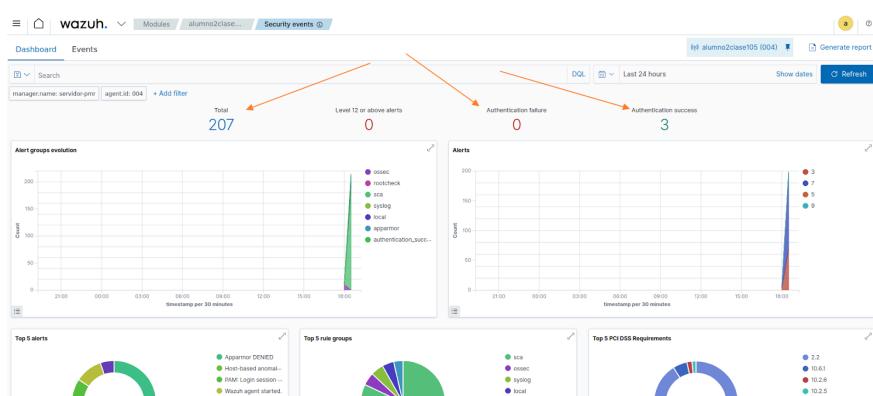
The screenshot shows the Wazuh Agents dashboard. At the top, there's a status summary: Active (2), Disconnected (4), Pending (0), Never connected (0), and Agents coverage 33.33%. Below this, it displays the last registered agent (alumno2clase106) and the most active agent (alumno2clase106). A table lists 6 agents with their details: ID, Name, IP address, Group(s), Operating system, Cluster node, Version, and Status. The status column includes icons for active, disconnected, and pending. An orange arrow points from the 'Status' section at the top to the status column in the table. Another orange arrow points from the status icons in the table to the detailed status icons shown in a legend below the table.

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	profesor01	192.168.105.2	default	Ubuntu 22.04.3 LTS	node01	v4.7.3	<span>active</span>	<span>Deploy new agent</span>
002	profesor02	192.168.106.2	default	Ubuntu 22.04.3 LTS	node01	v4.7.3	<span>disconnected</span>	<span>Refresh</span>
003	alumno1clase105	192.168.105.3	default	Ubuntu 22.04.3 LTS	node01	v4.7.3	<span>disconnected</span>	<span>Export formatted</span>
004	alumno2clase105	192.168.105.4	default	Ubuntu 22.04.3 LTS	node01	v4.7.3	<span>active</span>	<span>WQL</span>
005	alumno1clase106	192.168.106.3	default	Ubuntu 22.04.3 LTS	node01	v4.7.3	<span>disconnected</span>	<span>Refresh</span>
006	alumno2clase106	192.168.106.4	default	Ubuntu 22.04.3 LTS	node01	v4.7.3	<span>disconnected</span>	<span>Deploy new agent</span>

## EVENTOS DE SEGURIDAD

Como podemos observar, podemos ver distintos eventos de seguridad en el módulo de **“security events”**.

Como podemos observar, el dashboard de eventos de seguridad muestra los eventos totales relacionados con la seguridad de los equipos, intentos de autenticación fallidos e intentos de autenticación con éxito.



## INTEGRACIÓN VIRUSTOTAL-WAZUH

## Configuración en Agente

Busca el bloque `<syscheck>` en el archivo de configuración del agente Wazuh ubicado en `/var/ossec/etc/ossec.conf`.

Asegúrate de que `<disabled>` esté configurado en “**no**”. Esto activa el módulo de Integridad de Archivos de Wazuh para que monitoree los cambios en directorios.

Agrega una entrada dentro del bloque `<syscheck>` para configurar un directorio que se monitorizará en tiempo real. En este caso, estás monitoreando el directorio **Descargas..**

```
<scan_on_start>yes</scan_on_start>

<!-- Directories to check (perform all possible verifications) -->
<directories>/etc,/usr/bin,/usr/sbin</directories>
<directories>/bin,/sbin,/boot</directories>
<directories realtime="yes">/home/profesor01/Descargas</directories>

<!-- Files/directories to ignore -->
```

Buscamos el directorio `/var/ossec/active-response/bin/` y añadimos el **script** para eliminar los archivos.

```
root@profesor1-VirtualBox:/var/ossec/active-response/bin# ls
default-firewall-drop  firewall-drop  ipfw          npf          restart-wazuh
disable-account        host-deny     kaspersky    pf          route-null
firewalld-drop         ip-customblock kaspersky.py restart.sh  wazuh-slack
root@profesor1-VirtualBox:/var/ossec/active-response/bin#
```

```
#!/bin/bash
# LOCAL dirname $0
cd $LOCAL
cd ..
PWD=$(pwd)

read INPUT_JSON
FILENAME=$(echo $INPUT_JSON | jq -r .parameters.alert.data.virustotal.source.file)
COMMAND=$(echo $INPUT_JSON | jq -r .command)
LOG_FILE="/tmp/$(date '+%Y/%m/%d %H:%M:%S')_remove-threat.log"

#----- Analyze command -----
if [ ${COMMAND} = "add" ]
then
    # Send control message to execd
    printf '{"version":1,"origin":{"name":"remove-threat","module":"active-response"},"command":"'${COMMAND}'","parameters":{"keys":[]}}\n'

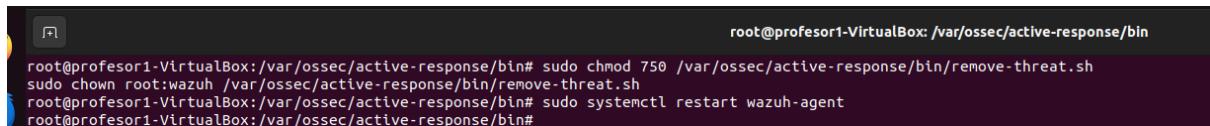
    read RESPONSE
    COMMAND2=$(echo $RESPONSE | jq -r .command)
    if [ ${COMMAND2} != "continue" ]
    then
        echo "date '+%Y/%m/%d %H:%M:%S' $0: ${INPUT_JSON} Remove threat active response aborted" >> ${LOG_FILE}
        exit 0;
    fi
fi

# Removing file
rm -f $FILENAME
if [ ! -f $FILENAME ]; then
    echo "date '+%Y/%m/%d %H:%M:%S' $0: ${INPUT_JSON} Successfully removed threat" >> ${LOG_FILE}
else
    echo "date '+%Y/%m/%d %H:%M:%S' $0: ${INPUT_JSON} Error removing threat" >> ${LOG_FILE}
fi

exit 0;
```

Creamos el fichero de extensión sh que contendrá el código en **bash**.

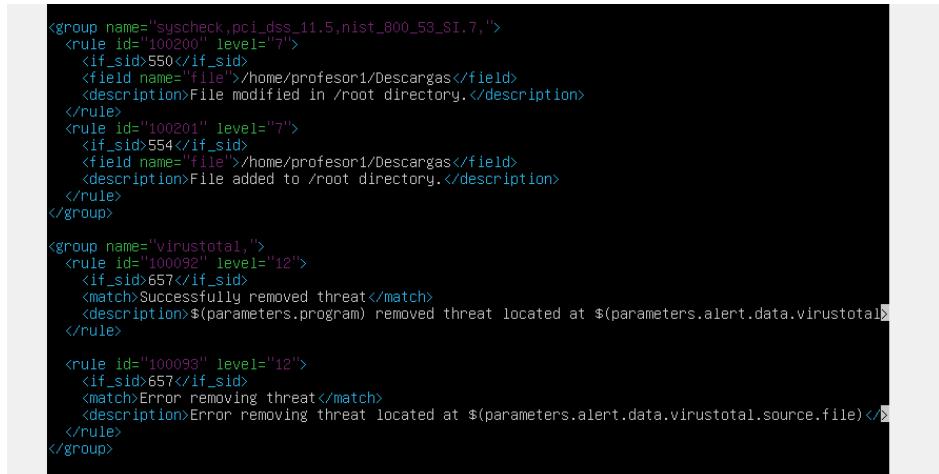
Le añadimos los **permisos** necesarios de ejecución al script y **reiniciamos** el servicio del agente.



```
root@profesor1-VirtualBox:/var/ossec/active-response/bin# sudo chmod 750 /var/ossec/active-response/bin/remove-threat.sh
sudo chown root:wazuh /var/ossec/active-response/bin/remove-threat.sh
root@profesor1-VirtualBox:/var/ossec/active-response/bin# sudo systemctl restart wazuh-agent
root@profesor1-VirtualBox:/var/ossec/active-response/bin#
```

## Configuración en Servidor

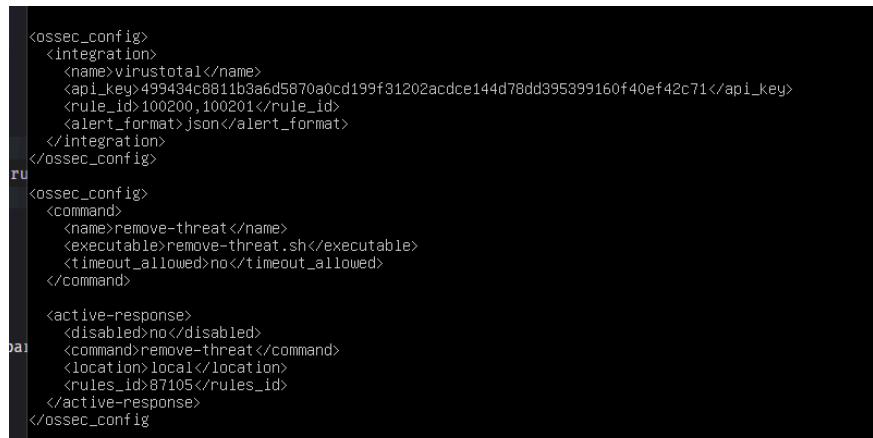
Añadimos las siguientes configuraciones al archivo **/var/ossec/etc/rules/local\_rules.xml**.



```
<group name="syscheck_pci_dss_11.5.nist_800_53_SI.7">
  <rule id="100200" level="7">
    <if_sid>550</if_sid>
    <field name="#file">/home/profesor1/Descargas</field>
    <description>File modified in /root directory.</description>
  </rule>
  <rule id="100201" level="7">
    <if_sid>554</if_sid>
    <field name="#file">/home/profesor1/Descargas</field>
    <description>File added to /root directory.</description>
  </rule>
</group>

<group name="virustotal">
  <rule id="100092" level="12">
    <if_sid>657</if_sid>
    <match>Successfully removed threat</match>
    <description>${parameters.program} removed threat located at ${parameters.alert.data.virustotal}</description>
  </rule>
  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at ${parameters.alert.data.virustotal.source.file}</description>
  </rule>
</group>
```

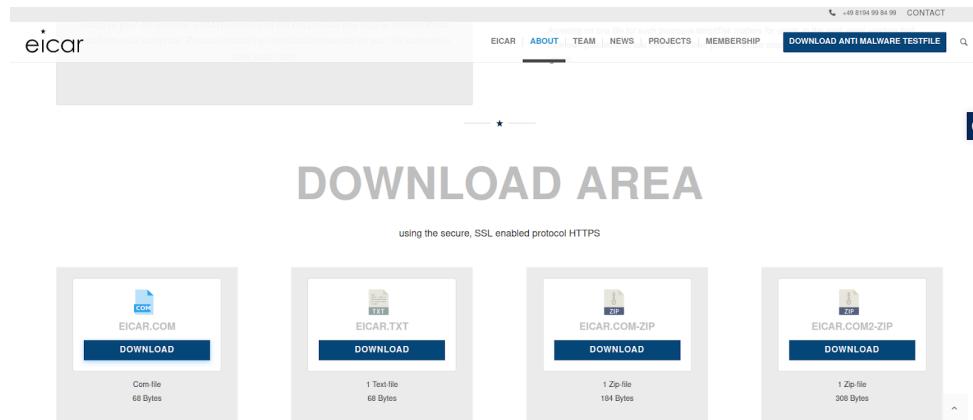
Y en el fichero **/var/ossec/etc/ossec.conf** añadimos las siguientes líneas de configuración para añadir la integración de VirusTotal a la herramienta. Necesitaremos la **API** de la integración, la cual podemos conseguir desde la página de **VirusTotal**.



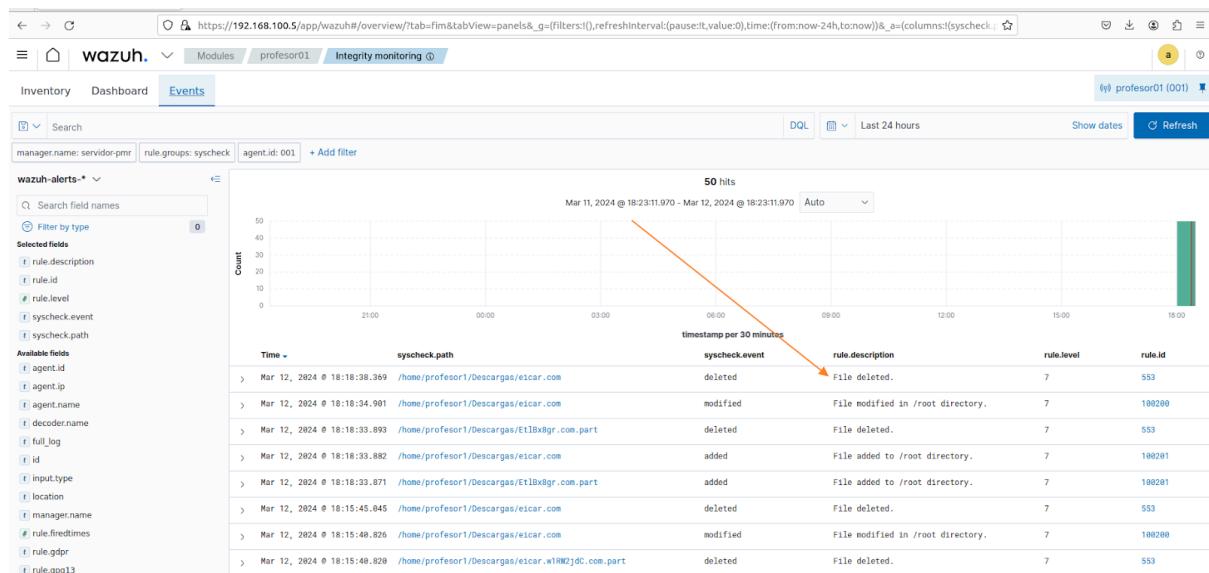
```
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key>499434c8811b3a6d5870a0cd199f31202acdce144d78dd395399160f40ef42c71</api_key>
    <rule_id>100200,100201</rule_id>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>
<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.sh</executable>
    <timeout_allowed>no</timeout_allowed>
  </command>
  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>
```

## Comprobación del Funcionamiento

Nos descargamos desde el equipo configurado como agente el siguiente archivo, el cual es un **sample de malware** que se utiliza para realizar pruebas.



Como podemos observar, desde el dashboard de eventos de seguridad del equipo, nos saldrá que **ha borrado** el archivo.



Además, podremos investigar el **análisis** que realiza VirusTotal sobre el archivo, donde podemos confirmar que se trata de un **malware**.

File distributed by Open Source

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f  
eicar.com-9836

Community Score: 66 / 68

REANALYZE SIMILAR MORE

Size: 68 B | Last Modification Date: 5 minutes ago | TXT

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: virus.eicar/test Threat categories: virus, trojan Family labels: eicar, test, file

Security vendors' analysis

Vendor	Analysis
AhnLab-V3	Virus/EICAR_Test_File
AliCloud	EngestMulti/Eicar
Anti-AVL	TestFile/Win32.EICAR
Avast	EICAR Test-NOT Virus!!!
AVG	EICAR Test-NOT Virus!!!
Baidu	Win32.Test.Eicar.a
BitDefenderTheta	EICAR-Test-File (not A Virus)
Alibaba	Trojan:MacOS/eicar.com
AliNac	Misc_Eicar-Test-File
Arcabit	EICAR-Test-File (not A Virus)
Avast-Mobile	Eicar
Avira (no cloud)	Eicar-Test-Signature
BitDefender	EICAR-Test-File (not A Virus)
Bkav Pro	W32.EicarTest.Trojan

Do you want to automate checks?