Escuela Politécnica Superior de Jaén
Grado en Ingeniería Informática

Universidad de Jaén
Escuela Politécnica Superior
de Jaén

TRABAJO FIN DE GRADO

EVALUACIÓN DE HERRAMIENTAS PARA LA CONEXIÓN REMOTA DEL ALUMNADO EN MODELOS DE DOCENCIA ON-LINE

Alumno

Sebastián Pulido Guerrero

Tutor

Rafael Jesús Segura Sánchez
(Departamento de Informática)

Febrero, 2022

(Página intencionalmente en blanco)

Universidad de Jaén

Departamento de Informática

Don Rafael Jesús Segura Sánchez, tutor del Trabajo Fin de Grado titulado: '**Evaluación de herramientas para la conexión remota del alumnado en modelos de docencia on-line**', que presenta Don Sebastián Pulido Guerrero, otorga el visto bueno para su entrega y defensa en la Escuela Politécnica Superior de Jaén.

Jaén, febrero de 2022

El alumno: El tutor:

Sebastián Pulido Guerrero Rafael Jesús Segura Sánchez

(Página intencionalmente en blanco)

Agradecimientos

Para comenzar, me gustaría agradecer la labor de mi tutor, Rafael Jesús Segura Sánchez. En todo momento he contado con su atención y ayuda en el desarrollo de este Trabajo Fin de Grado ofreciéndome todas las facilidades posibles.

Transmitir, igualmente, mis agradecimientos a Carlos Javier Ogayar Anguita (profesor del Departamento de Informática), Pedro López Cruz (miembro del Servicio de Informática) y, a mis compañeros Juan Pedro y Miki, por su colaboración desinteresada.

Y, por último, a mi mujer e hijas. Sin su apoyo constante, todo esto hubiera sido muy difícil. No olvidéis nunca que sois mi motor.

De verdad, gracias.

FICHA DEL TRABAJO FIN DE TÍTULO	
Titulación	Grado en Ingeniería Informática
Modalidad	Estudio Técnico
Especialidad (solo TFG)	Ingeniería del Software
Mención (solo TFG)	General
Idioma	Español
Tipo	General
TFT en equipo	No
Autor/a	Sebastián Pulido Guerrero
Fecha de asignación	02/03/2021
Descripción corta	Estudio y análisis de las diferentes herramientas de conexión remota disponibles para el uso por parte del alumnado en los modelos de docencia online. Presentación previa del entorno actual de trabajo donde los alumnos realizan sus prácticas. Instalación de la aplicación de Escritorio remoto que, según dicho estudio, más se adecue a los requerimientos del Departamento de Informática, y su evaluación, comprobando aspectos de seguridad, rendimiento, facilidad de uso, etc.

NORMAS APLICADAS EN ESTE DOCUMENTO	
LOCALES	
TFT-UJA:2017	Normativa de Trabajos Fin de Grado, Fin de Máster y otros Trabajos Fin de Título de la Universidad de Jaén (Normativa marco UJA aprobada en Consejo de Gobierno)
TFT-EPSJ:2017	Normativa sobre Trabajos Fin de Grado y Fin de Máster en la Escuela Politécnica Superior de Jaén (Normativa EPSJ aprobada en Junta de Escuela)
TFT-EPSJ	Criterios de evaluación y normas de estilo para TFG y TFM de la Escuela Politécnica Superior de Jaén
NACIONALES E INTERNACIONALES	
ISO 2145:1978	Documentación - Numeración de divisiones y subdivisiones en documentos escritos
UNE 50132:1994	Traducción de la ISO 2145
APA 6ª edición	Estilo de referencias y citas de APA (American Psychological Association)

NORMAS UTILIZADAS COMO BASE O REFERENCIA	
NACIONALES	
UNE 157001:2014	Criterios generales para la elaboración formal de los documentos que constituyen un proyecto técnico
UNE 157801:2007	Criterios generales para la elaboración de proyectos de sistemas de información
*Estas normas se han utilizado **como base o referencia** para la inclusión de algunos contenidos y definiciones sobre elaboración de proyectos, entendiendo como **proyecto** la documentación consensuada entre una empresa y un cliente, que da lugar al perfeccionamiento de un contrato para la elaboración de una obra o la prestación de un servicio. Por consiguiente, no debe esperarse la aplicación de estas normas en cuanto a la completitud de los contenidos ni a la organización de los mismos.*	

Contenido

Índice de ilustraciones

Índice de tablas

1 ESPECIFICACIÓN DEL TRABAJO

En este capítulo se presenta la especificación del trabajo, con una estructura y contenidos **inspirados** en los criterios y recomendaciones que establece la norma UNE 157801:2007 - "*Criterios Generales para la elaboración de proyectos de Sistemas de Información*".

A lo largo del documento se utilizarán términos y acrónimos cuya descripción aparecen en el apartado 6 (Definiciones y abreviaturas).

1.1 Introducción

La crisis sanitaria provocada por el COVID-19 ha tenido un enorme impacto en el desarrollo de la actividad académica, y las limitaciones derivadas del estado de alarma aceleraron el uso de las nuevas tecnologías haciendo que nos "abrazáramos" a la pantalla como solución para poder continuar con nuestras funciones laborales, educativas e incluso sociales.

Las instituciones de educación superior han tenido que implementar, con celeridad, nuevas lógicas y dinámicas educativas que no pierdan el compromiso con la calidad académica de las enseñanzas, realizando una rápida transición de una actividad docente principalmente presencial a una modalidad online y a distancia. Es por ello que el desarrollo de las clases prácticas de cada asignatura sea una de los apartados que más se ha visto afectado al no poder asistir físicamente los alumnos a los laboratorios específicos para la realización de las mismas. Esto se agrava en el caso especial del ámbito informático, aun contando el alumno con medios tecnológicos suficientes, ya que no sería posible el uso de software específico o de equipos de última generación con alta capacidad de computación que permite completar cierto tipo de tareas.

En el intento de minimizar estos inconvenientes sobrevenidos por el COVID-19, y a la vez potenciar el uso de los laboratorios de prácticas, este trabajo tiene como objetivo principal presentar las distintas herramientas de conexión a escritorio remoto que existen actualmente, haciendo una breve descripción de las mismas, mostrando sus características y analizando sus ventajas e inconvenientes. Así mismo, es también

objetivo del trabajo la implementación de alguna de ellas que permita al alumnado, de forma sencilla y segura, el acceso remoto al escritorio de cada uno de los ordenadores instalados en los diferentes laboratorios del Departamento de Informática de la Universidad de Jaén. Igualmente se llevará a cabo una detallada evaluación de los resultados que permitan justificar, o no, la implantación y uso de la herramienta por parte del alumnado y profesorado del Departamento, así como la presentación de un listado de mejoras / adaptaciones a desarrollar adicionalmente que pudieran integrar más aún a dicha herramienta en el día a día de la docencia e investigación realizada por los miembros del Departamento.

En este contexto, vamos a ver qué herramientas de este tipo existen en el mercado y cuál de ellas se ajustaría mejor a las necesidades actuales del Departamento de Informática de la Universidad de Jaén, y todo ello introduciendo una breve explicación de esta tecnología y detallando el entorno de trabajo que actualmente tiene instalado el Departamento de Informática para la realización de las prácticas de sus asignaturas.

1.2 Objetivos del trabajo

A continuación se presentan de forma más clara y precisa los objetivos introducidos en el punto anterior:

- Realizar un estudio que permita conocer el estado actual del entorno y condiciones de trabajo donde realizan sus prácticas los alumnos. Para ello se detallará los espacios e instalaciones de los que dispone el Departamento de Informática, así como las especificaciones de sus puestos de trabajo (hardware y software), conexiones, uso, nivel de ocupación, tipo de docencia, etc. Igualmente, dentro de este apartado, se hará referencia de forma breve a algunos aspectos de seguridad presentes en estos laboratorios de prácticas y en las conexiones realizadas desde y hacia la Universidad de Jaén.
- Presentación de las diferentes alternativas actuales de una aplicación de Escritorio Remoto con el análisis de sus principales características, ventajas e inconvenientes. Previamente serán expuestos los conceptos de acceso remoto y escritorio remoto para conocer esta tecnología y que permita una mejor lectura y comprensión de este tipo de aplicaciones.

- Implantación de alguna de las herramientas de Escritorio Remoto presentadas, obteniendo con ella una manera sencilla y controlada (tanto para los alumnos como para los administradores del servicio) para el acceso seguro a los ordenares de los laboratorios del Departamento de Informática. Dentro de los puntos a desarrollar con este objetivo se describirán:
  - Motivación.
  - Requisitos hardware y software.
  - Conocimientos previos.
  - Pasos para su instalación.
  - Manual de la aplicación.
  - Valoración económica.
- Evaluación de dicha aplicación una vez instalada que indique aspectos como los siguientes:
  - Seguridad de acceso.
  - Facilidad de uso.
  - Datos del monitoreo del consumo de red o ancho de banda.
  - Rendimiento en pruebas de carga.
  - Posible propuesta de mejora para su adaptación al Departamento.

1.3 Antecedentes y estado del arte

El propósito de este apartado es introducir el concepto de acceso remoto necesario para entender posteriormente el funcionamiento de las aplicaciones a analizar.

“Habitualmente, los usuarios desarrollan su labor interaccionando con su equipo local, pero cuando este equipo forma parte de una red, a veces se requieren diversas tareas que exigen el acceso a otro equipo distante. Por ejemplo, un usuario podría acceder a un equipo remoto para utilizar un recurso cuya adquisición le supone un elevado coste económico (aplicación informática), bien para ejecutar aplicaciones

muy exigentes en requerimientos hardware de los que su equipo carece o, simplemente, realizar tareas de administración sobre él [1, p. 153]".

Aunque inicialmente las conexiones remotas para trabajar en ordenadores o servidores ubicados en otros lugares permitían únicamente el acceso a interfaces basadas en texto debido principalmente a las restricciones de velocidad de las redes, el constante desarrollo de las comunicaciones y dispositivos de procesamiento ha permitido que en el presente se pueda acceder a entornos gráficos ejecutándose en el ordenador remoto, teniendo al alcance ya sea una simple aplicación o incluso todo el escritorio de trabajo de un usuario (Escritorio remoto).

Se puede definir el concepto de acceso remoto como el proceso que permite acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar, a través de una red local o externa (como Internet). En él se ven implicados protocolos (o un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red por medio de intercambio de mensajes), y programas (arquitectura cliente-servidor) en ambas computadoras que permitan recibir/enviar los datos necesarios. Además, deben contar con un fuerte sistema de seguridad (tanto la red, como los protocolos y los programas).

Remotamente se puede acceder prácticamente a cualquier recurso que ofrece una o más computadoras. Se pueden acceder a archivos, dispositivos periféricos (como impresoras), configuraciones, bases de datos, copias de seguridad, etc. Por ejemplo, se puede acceder a un servidor de forma remota para configurarlo, controlar el estado de sus servicios, transferir archivos, etc.

Existen multitud de programas y opciones que permiten controlar una computadora remotamente. A continuación, se citan en orden cronológico:

- TELNET [2] (Telematics Network): es el nombre de un protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero es una herramienta muy útil para administrar equipos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina. Su mayor problema es de seguridad y por esta razón ha sido sustituido por SSH, pero aún sigue teniendo cierta utilidad para los administradores de sistemas.

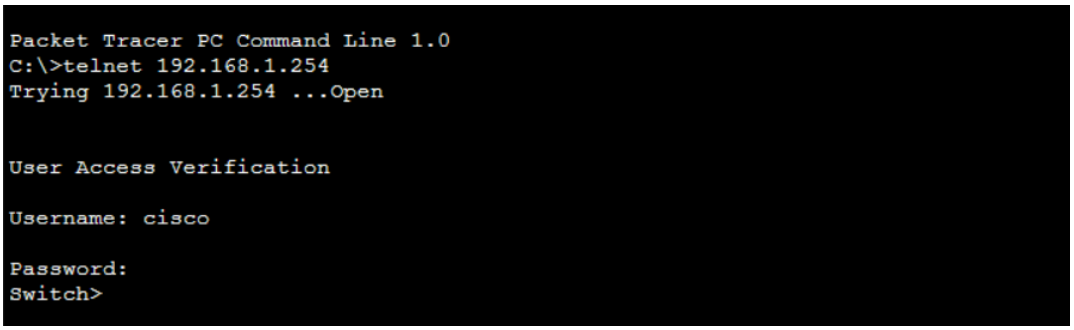

Ilustración 1.1. Acceso vía Telnet a un switch desde línea de comandos

- RLOGIN (Remote Login) es una aplicación TCP/IP que comienza una sesión de terminal remoto sobre el anfitrión especificado como host. Su funcionamiento es similar a Telnet con la salvedad de que los usuarios no tienen que introducir una contraseña para autenticarse antes de iniciar la sesión. Esta característica impide que las contraseñas sean capturadas por otros usuarios en la red.

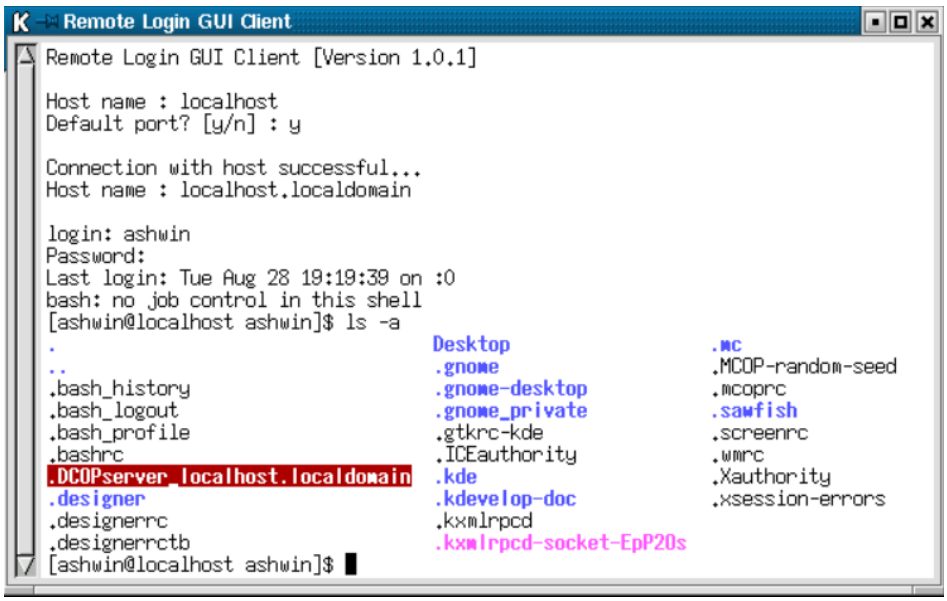

Ilustración 1.2. Acceso remoto con un cliente de RLogin

- SSH [3] (Secure Shell): Es el nombre de un protocolo y del programa que lo implementa y, al igual que los anteriores, sirve para acceder a máquinas remotas a través de una red mediante un intérprete de comandos, entre otras funciones, incluyendo mejoras en cuanto a seguridad. Cada vez que una computadora envía datos a la red, SSH los cifra (codifica) automáticamente.

Después, cuando los datos llegan a su destinatario, SSH los descifra (descodifica) automáticamente. El resultado es un cifrado transparente: los usuarios pueden trabajar con normalidad, sin saber que sus comunicaciones están cifradas de forma segura en la red.

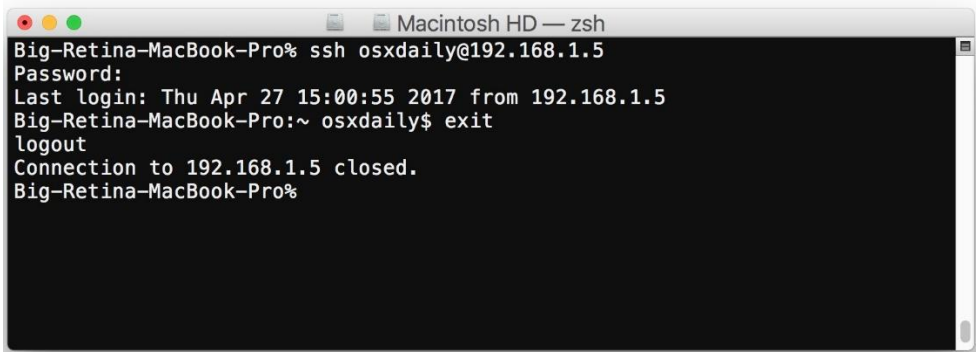

Ilustración 1.3. Acceso remoto por SSH en un terminal de Mac

- X-TERMINAL: servicio usado entre equipos GNU/Linux gracias al protocolo XDMCP (“X Display Manager Control Protocol” o Protocolo de Control de Administrador de la Pantalla X). Sus modos de funcionamiento son:
    - Sesión X Window remota: permite a un equipo GNU/Linux iniciar una sesión gráfica en un equipo remoto desde su máquina local, visualizando la pantalla de inicio de sesión remota. Una vez iniciada la sesión, el cliente tiene acceso al escritorio y aplicaciones del equipo remoto.
    - Aplicaciones X Window remotas: permite a un servidor GNU/Linux poner a disposición de un equipo cliente sus recursos hardware, de manera que pueda ejecutar aplicaciones gráficas.

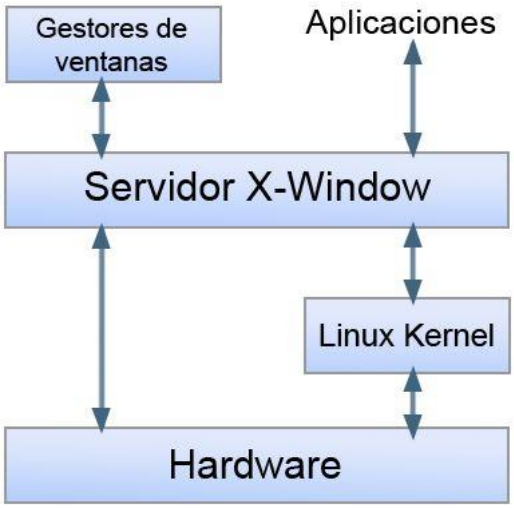

Ilustración 1.4. X-Window, interfaz gráfica utilizada por GNU/Linux[1]

- VNC [4] (Virtual Network Computing), que es uno de los más populares, basado en una estructura cliente-servidor, gratuito y libre. Hay veces en las que es necesario operar con el acceso remoto más allá de la línea de comandos. Es ahí donde aparece la necesidad de escritorios remotos, de ejecución remota de programas gráficos y la necesidad de cifrar esas conexiones. Una de las opciones que permite esto será VNC, es decir, controlar en modo gráfico otro equipo tanto de una red local como de otra externa (como Internet), teniendo el usuario la impresión de estar sentado delante del equipo remoto, con todas las ventajas que esto supone. Este programa no impone restricciones en el sistema operativo del ordenador servidor con respecto al del cliente. Un sistema de VNC se compone de un cliente, un servidor, y un protocolo de comunicación.
    - El VNC servidor es el programa en el equipo que comparte su pantalla. El servidor de forma pasiva permite al cliente tomar el control de la misma.
    - El VNC cliente (o espectador) es el programa que vigila, controla e interactúa con el servidor. El cliente controla al servidor.
    - El VNC protocolo (RFB) es muy simple, basado en una primitiva gráfica del servidor al cliente ("Put a rectangle of pixel data at the specified X,Y

[1] X.Org: sistema X Window, la interfaz gráfica (GUI) para sistemas UNIX http://recursostic.educacion.es/observatorio/version/v2/es/software/software-general/715-xorg-sistema-x-window

position", en español "Póngase un rectángulo de datos de píxel en la posición X,Y especificada) y mensajes de eventos desde el cliente al servidor.

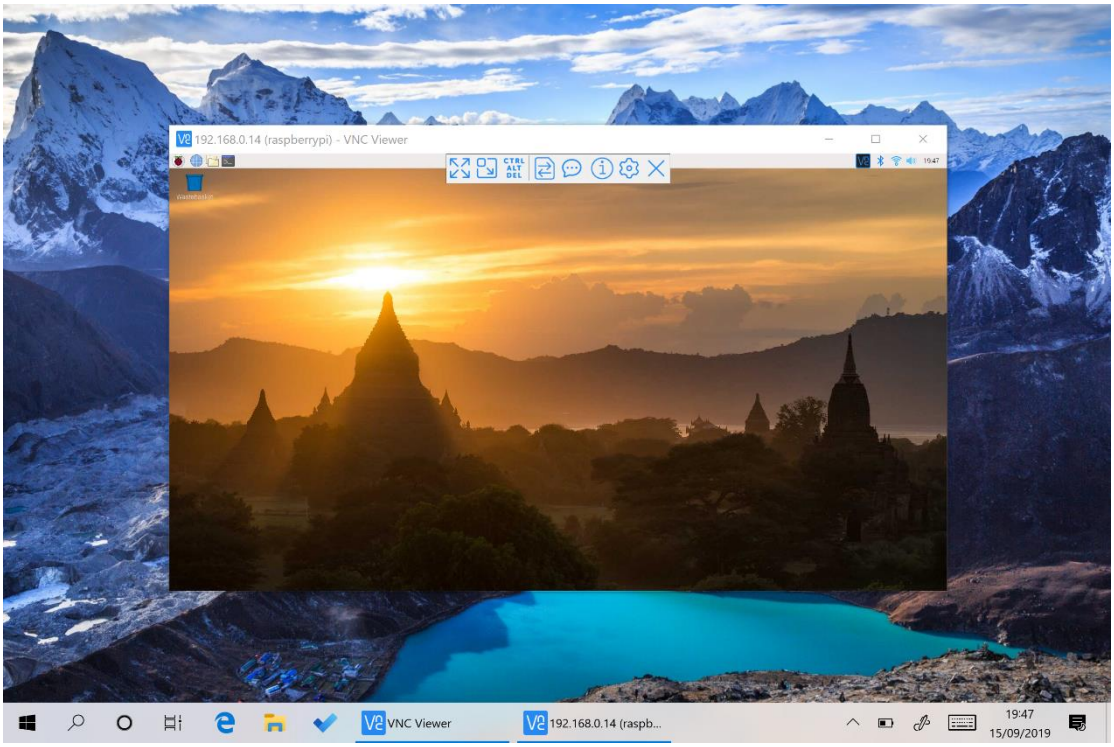

Ilustración 1.5. Cliente VNC conectado a una Raspberry desde un PC Windows

- Terminal Services [5] (servicios de terminal): actualmente conocidos como Servicios de Escritorio Remoto (del inglés Remote Desktop Services), son un componente de los sistemas operativos Windows que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso por red. Basados en el protocolo RDP (Remote Desktop Protocol [6]), protocolo propietario de Microsoft, que igual que el anterior permite el control de la interfaz gráfica del escritorio de la máquina remota. El modo de funcionamiento del protocolo es sencillo: la información gráfica que genera el servidor es convertida a un formato propio RDP y enviada a través de la red al terminal, que interpretará la información contenida en el paquete del protocolo para reconstruir la imagen a mostrar en la pantalla del terminal. En cuanto a la introducción de órdenes en el terminal por parte del usuario, las teclas que pulse el usuario en el teclado del terminal, así como los movimientos y pulsaciones de ratón son redirigidos al servidor, permitiendo el protocolo un

cifrado de los mismos por motivos de seguridad. El protocolo también permite que toda la información que intercambien cliente y servidor sea comprimida para un mejor rendimiento en las redes menos veloces. Microsoft proporciona el software cliente para todas las versiones de Windows 32 bits y para Mac OS X de Apple.

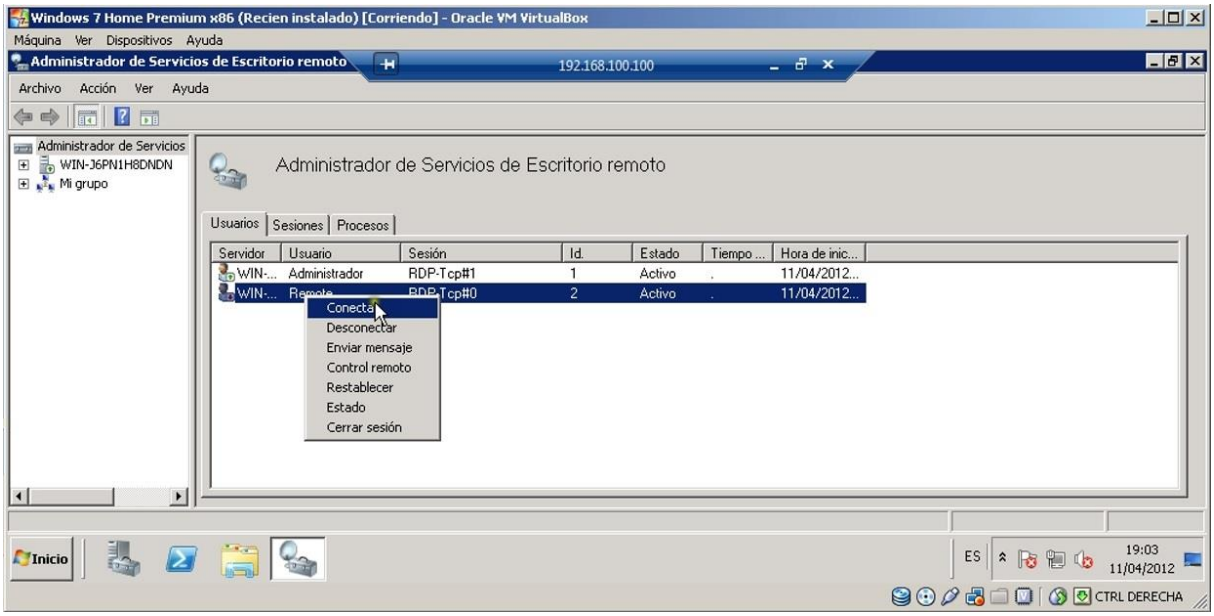

Ilustración 1.6. Acceso remoto con Terminal Services

- Aplicaciones web que permiten el acceso remoto a determinados recursos utilizando sólo un navegador web, ya sea a través de internet o cualquier otra red.

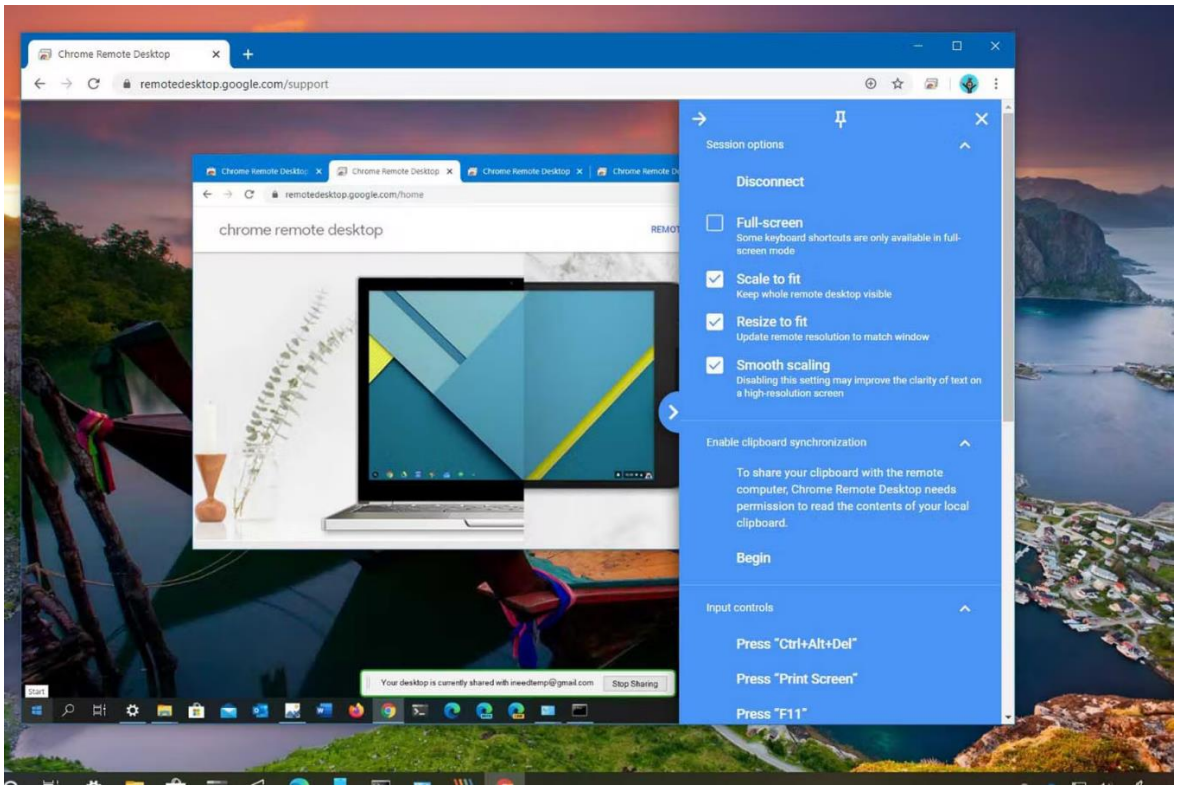

Ilustración 1.7. Conexión con un PC remoto a través del navegador Chrome

Básicamente, todas ellas tienen el mismo modo de funcionamiento en el que son necesarios un programa Servidor (ubicado y configurado en la máquina a la que queremos acceder) y un programa Cliente (encargado de manejar y mostrar los resultados de las operaciones realizadas en la máquina remota) conectados por Internet, VPN u otro tipo de red.

Este tipo de aplicaciones permiten, entre otras muchas cosas, visualizar la pantalla de otro PC en la pantalla del usuario. El programa permite el uso del ratón y del teclado para controlar otro computador remotamente. Esto quiere decir que se puede trabajar en un pc remoto como si se estuviese sentado frente a él desde cualquier ubicación.

La posibilidad de acceder al propio disco duro, ubicar un archivo en cualquier carpeta, ejecutar un programa específico, trabajar con la propia computadora, como si el operador estuviera en su oficina, y hasta escuchar la propia música almacenada en el disco duro, son algunos de los beneficios que brindan los programas de acceso remoto.

El único requisito es que la computadora a la que se quiera acceder esté encendida y conectada a Internet. Y lógicamente, que esté configurada para permitir

un acceso remoto, o tener software de acceso remoto instalado. El siguiente paso sólo será acceder a ella desde cualquier punto del mundo con conexión, utilizando un software o ingresando a una dirección Web para hacer el resto.

Los diversos sistemas de acceso remoto trabajan con mecanismos de seguridad de encriptación en la transmisión de datos, para desechar cualquier posibilidad de robo de información, lo cual vuelve a esta operación absolutamente segura. Otras características de seguridad ofrecidas habitualmente también por este tipo de software pueden ser:

- Límite en el número de usuarios que pueden conectarse.
- Protección con contraseña.
- Acceso privado.
- Lista negra de conexiones no deseadas.

Los beneficios que trae el acceso remoto al PC son enormes y su límite es la imaginación del usuario. Pero sin duda, facilita enormemente el acceso remoto a la información permitiendo trabajar a distancia con el consiguiente ahorro de tiempo, molestias y recursos económicos tanto en llamadas como en desplazamientos y evitando la necesidad del uso de copias de seguridad, discos portátiles, y ni siquiera pendrives. Además, por medio del control remoto se pueden ejecutar aplicaciones que el usuario no tiene instaladas en su equipo local, aunque sí en su PC remoto. Algunos sistemas van más allá, permitiendo a más de un usuario el acceso a un PC. Empleando esta tecnología se puede ser partícipe en un seminario web, realizar una reunión o clase online ... Pero la versatilidad no termina ahí, ya que algunos sistemas permiten el acceso remoto a PC desde dispositivos móviles. También se pueden copiar y pegar documentos entre el escritorio remoto y el equipo local, sincronizar y transferir archivos y hasta bloquear temporalmente su utilización. Y no podemos olvidar uno de sus usos principales como es la asistencia técnica a distancia.

Aunque no es objeto de este trabajo, cabe resaltar que en los últimos años la tecnología ha dado un paso más en el uso del Escritorio Remoto. Algunas empresas del sector TIC ofrecen los denominados “escritorios virtuales” (o DaaS “Desktop as a Service”, que traducido significa “Escritorio como servicio”), es decir, sistemas que también permiten a un usuario utilizar su escritorio de trabajo personal como si estuvieran físicamente en su mesa de la oficina. Pero, a diferencia de los escritorios

remotos, estos escritorios y aplicaciones no se encuentran en su propio equipo, sino que son servidos desde una infraestructura de virtualización implantada en servidores propios de la compañía o accesibles en modalidad Cloud.

El hecho de que ambos sistemas permitan trabajar a distancia puede generar cierta confusión, tendiendo a confundirlos, lo cual no es de extrañar si se tiene presente el sistema de escritorio remoto a través de la web. No obstante, son dos tecnologías diferentes, aunque compartan elementos comunes. Así, mientras que el escritorio remoto consiste en la interconexión de unos clientes con un host, en el cual se trabaja a distancia, la computación en la nube permite al usuario disponer de la información que necesite en el momento en el que la necesite. Esta información puede ser tanto archivos guardados como el acceso a programas a los que se tiene acceso desde un dispositivo conectado a Internet, entre otras muchas opciones. Por ello y por el ahorro de recursos que garantiza, el Cloud Computing se presenta como una herramienta más potente y versátil que la tecnología de escritorio remoto para determinadas tareas, toda vez que el escritorio remoto es el medio más eficaz para otras como el soporte técnico.

La virtualización de los puestos de trabajo es una opción cada vez más utilizada por grandes compañías y entidades, pero su aplicación en el terreno educativo resulta aún más llamativa, ya que permite que alumnos y/o profesores puedan trabajar con un mismo escritorio virtual a través del cual hacer uso de todas las aplicaciones educativas oportunas desde diferentes tipos de dispositivos digitales. Esto facilita la universalidad de la tecnología y aporta mayor accesibilidad para la implantación de las aulas TIC y las nuevas metodologías de enseñanza-aprendizaje, proporcionando un entorno compatible con cualquier sistema operativo y dispositivo. Es decir, la virtualización de escritorios consiste en que cuando un usuario trabaje desde su ordenador de sobremesa, su portátil, su tableta o su smartphone, todo su entorno de trabajo (incluidas aplicaciones, archivos, datos, etc.) sea recuperado desde la nube o desde un servidor propio.

Entre las ventajas y beneficios del uso de escritorios virtuales avanzados hay que destacar las siguientes:

- Reducción del coste general de los equipos: Utilizar escritorios virtuales no requiere de equipos de última generación o con gran capacidad de memoria, ya que las aplicaciones son ejecutadas realmente en los servidores de la plataforma, donde también se guardan los datos y archivos. Esto supone

una reducción de costes y a su vez una prolongación de la vida de los equipos informáticos, además de posibilitar la utilización de otros dispositivos de menor coste como tabletas o thin client. Asimismo, el uso de esta tecnología puede suponer un destacado ahorro en el consumo de energía.

- Disminución de soporte y mantenimiento técnico: Los costes de soporte y mantenimiento de los puestos de trabajo pueden verse reducidos drásticamente, gracias a la posibilidad de administración remota de los puestos de usuario a través de la Consola de Administración de la plataforma de virtualización. Además, el tiempo de respuesta ante una avería en un equipo puede quedar minimizado, ya que basta con llevar a cabo la sustitución del equipo para que este vuelva a tener disponible su entorno de trabajo personal de forma inmediata.
- Aumento de la seguridad de los escritorios: La gestión del parque informático, el control de las aplicaciones que son puestas a disposición de cada usuario y la configuración de la seguridad son efectuadas desde una única consola de administración central. Esto evita los problemas habituales que tienen las empresas a la hora de otorgar permisos a los usuarios y ofrecer a la vez un entorno de trabajo flexible que incorpore todas las funciones necesarias para que el adecuado desarrollo del trabajo.
- Mejora de la seguridad de los datos: El sistema de virtualización puede ser configurado para permitir el uso de los espacios de almacenamiento locales y/o remotos, lo que pone a disposición de los administradores de la plataforma todo un mundo de posibilidades para garantizar la seguridad y evitar el riesgo de pérdida de datos por robo de los equipos o dispositivos digitales. En el caso de que un equipo sea extraviado o sufra una rotura no existe ningún problema puesto que los documentos y datos son almacenados en la infraestructura del entorno de virtualización.

En definitiva, los escritorios virtuales avanzados ofrecen ventajas sólidas e importantes que justifican su uso en diferentes organizaciones y ámbitos de actividad, así como para los usuarios particulares en general.

Entre los principales proveedores de soluciones de escritorio virtual podemos encontrar los siguientes: “Nube V2”, “Amazon WorkSpaces (AWS), “Microsoft Azure”, “VMware Horizon Cloud”, “Citrix Virtual Apps and Desktops” …

1.4 Descripción de la situación de partida

Para describir de forma resumida la situación de la que parte la idea de este trabajo fin de grado habría que empezar conociendo el Departamento de Informática de la Universidad de Jaén, así como la estructura y gestión de sus laboratorios de docencia e investigación.

El Departamento de Informática [7] está situado en el edificio A3 (Escuela Politécnica Superior de Jaén) del Campus Las Lagunillas y en la Escuela Politécnica Superior de Linares del Campus Científico Tecnológico de Linares. Actualmente compuesto por más de 70 miembros entre los que se incluye a profesores, becarios y contratados con cargo a proyectos de investigación, y personal de administración de servicios organizados y repartidos en 3 áreas de conocimiento:

- Área de Arquitectura y Tecnología de Computadores.
- Área de Ciencias de la Computación e Inteligencia Artificial.
- Área de Lenguajes y Sistemas Informáticos.

Cada área de conocimiento imparte docencia a un conjunto de asignaturas de materia diferente que en algunos casos tienen también necesidades particulares en lo que se refiere a las prácticas en los laboratorios docentes.

Ilustración 1.8. Edificio A3

Además de la organización en áreas a efectos de implementar la actividad docente, los profesores también se organizan en 6 grupos de investigación:

- Grupo de Gráficos y Geomática de Jaén (GGGJ).
- Grupo de Sistemas Inteligentes de Acceso a la Información (SINAI).
- Grupo de Sistemas Inteligentes basados en Análisis de Decisión Difusos (SINBAD^2).
- Grupo de Sistemas Inteligentes y Minería de Datos (SIMIDAT).
- Grupo de Identificación por Radiofrecuencia en la UJA (RFIDUJA).
- Grupo en Avances en Sistemas Inteligentes y Aplicaciones (ASIA).

El Departamento de Informática imparte docencia de manera presencial en 6 centros de la Universidad de Jaén con más de 100 asignaturas pertenecientes a 20 Grados y 10 Másteres oficiales. Parte de esta docencia, y que es la que nos concierne, se desarrolla en los laboratorios docentes del Departamento.

Los laboratorios de docencia están destinados fundamentalmente a atender las prácticas de las asignaturas del Grado en Ingeniería Informática. No obstante también atiende las necesidades de algunas asignaturas específicas de otros Grados y de los Máster de Informática, Seguridad Informática, Secundaria, Ing. Mecatrónica, y pequeños cursos organizados por miembros del Departamento. Esto hace que el nivel de ocupación de estos laboratorios sea bastante elevado durante el periodo lectivo.

Tomando como referencia los datos correspondientes al segundo cuatrimestre de este curso académico 2021-22, el nivel de ocupación de los laboratorios docentes del Departamento de Informática es del 66% atendiendo a los horarios establecidos en cada uno de ellos (que se puede consultar en el sitio web del Departamento [7]).

UNIVERSIDAD DE JAÉN
Departamento de Informática

LABORATORIO 3 (Dep. A3-172, 25 puestos). SEGUNDO CUATRIMESTRE

HORA / DÍA	LUNES	MARTES	MIÉRCOLES	JUEVES	VIERNES
8:30-9:30	*Fund. bases de datos (1) [2º Gr. Informática]*	*Ingeniería de requisitos (1) [3º Gr. Informática]*	*Desarrollo ágil (1) [3º Gr. Informática]*	*Sistemas de información basados en web [1] [3º Gr. Informática]*	
9:30-10:30					
10:30-11:30	*Database Foundations (3)(EN) [2º Gr. Informática]*	*Calidad del software (1) [3º Gr. Informática]*	*Auditoría informática (1) [3º Gr. Informática]*	*BBDD distribuidas (1) [3º Gr. Informática]*	*Diseño de algoritmos (6) [2º Gr. Informática]*
11:30-12:30					
12:30-13:30	*Fund. bases de datos (2) [2º Gr. Informática]*	*Calidad del software (EN) [3º Gr. Informática]*		*Sistemas de recuperación de información (1) [3º Gr. Informática]*	*Bases de datos (1) [1º Gr. Ing. Geom. Topog.]*
13:30-14:30					
14:30-15:30					
15:30-16:30	*Fund. bases de datos (4) [2º Gr. Informática]*	*Técn. avanzadas de seguridad (1) [4º Gr. Informática]*	*Web semántica y social (T) [4º Gr. Informática]*	*Máster en Seg. Informática*	*Máster en Seg. Informática*
16:30-17:30			*Web semántica y social (1) [4º Gr. Informática]*		
17:30-18:30	*Fund. bases de datos (5) [2º Gr. Informática]*	*Técn. avanzadas de seguridad (2) [4º Gr. Informática]*	*Diseño y programación de sistemas embebidos (1)[1] [Máster Univ. Ing. Mecatrónica]*	*Máster en Seg. Informática*	*Máster en Seg. Informática*
18:30-19:30					
19:30-20:30	*Web semántica y social (T) [4º Gr. Informática]*			*Diseño y programación de sistemas embebidos (1)[1] [Máster Univ. Ing. Mecatrónica]*	
20:30-21:30	*Web semántica y social (1) [4º Gr. Informática]*				

Ilustración 1.9. Horario del laboratorio 3 (A3-172) – 2º cuatrimestre curso 2021-22

A esta ocupación fija y semanal hay que sumarle las múltiples reservas puntuales que a lo largo del curso solicita el personal docente para cursos internos de la Universidad, exámenes y pruebas, visitas guiadas, presentaciones, etc.

A continuación, se muestra una imagen de la aplicación web de los técnicos de los laboratorios con la que gestionan las reservas de cada laboratorio y en la que se listan las reservas puntuales realizadas hasta abril en uno de ellos:

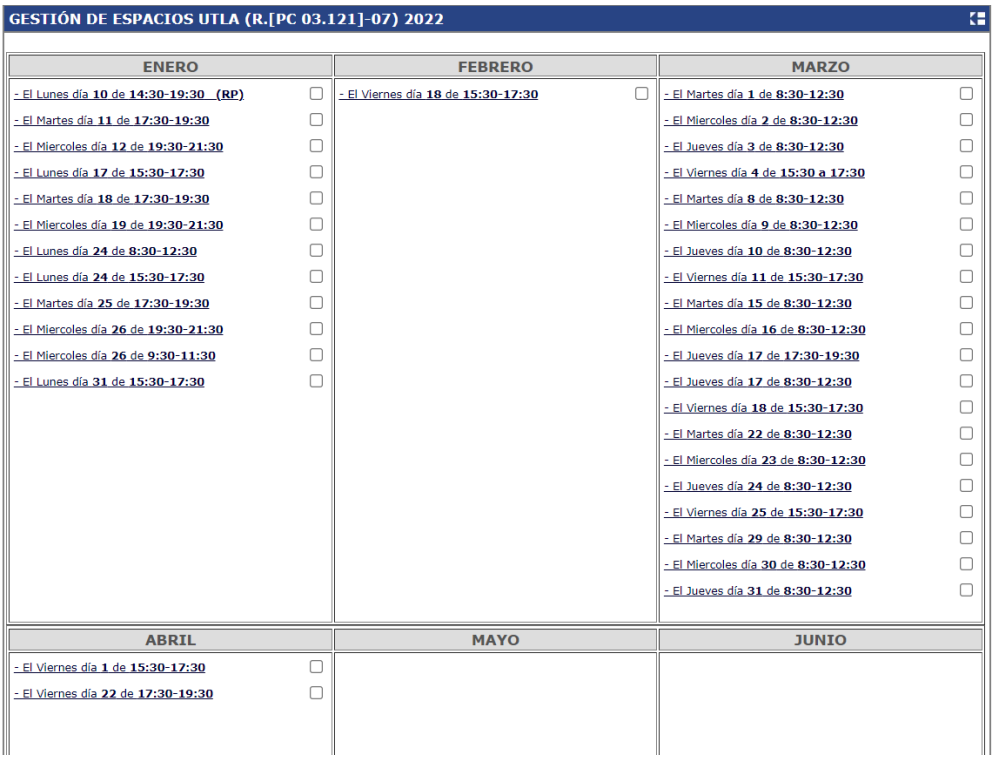

Ilustración 1.10. Lista de reservas adicionales del laboratorio 4

Como se puede observar, el grado de ocupación de los laboratorios es bastante alto y esto, unido a su uso únicamente de forma presencial, dificultó durante el estado de alarma (modo de docencia online y semipresencial) el desarrollo de las prácticas de las distintas asignaturas. El principal objetivo de este trabajo es el estudio e implantación de alguna solución que permita realizar conexiones de escritorio remoto contra los ordenadores de los laboratorios de prácticas que garantice de manera fácil y segura su utilización, minimizando así los inconvenientes ante posibles situaciones en las que los usuarios no puedan acceder físicamente a los laboratorios, o permitiendo incluso, potenciar su uso fuera de horario laboral o días no lectivos.

1.4.1 Descripción del entorno actual

El entorno actual de trabajo gestionado por el Departamento de Informática se compone de varios espacios. Además de los despachos de los profesores, personal de administración y técnicos de laboratorio, el departamento cuenta con dos seminarios (A3-153 y A3-104), tres laboratorios de investigación (A3-103, A3-154 y A3-155), una sala de servidores (A3-185) y seis laboratorios de docencia (A3-170, A3-

172, A3-174, A3-176, A3-183 y L-119) donde se imparten las prácticas de las diferentes asignaturas.

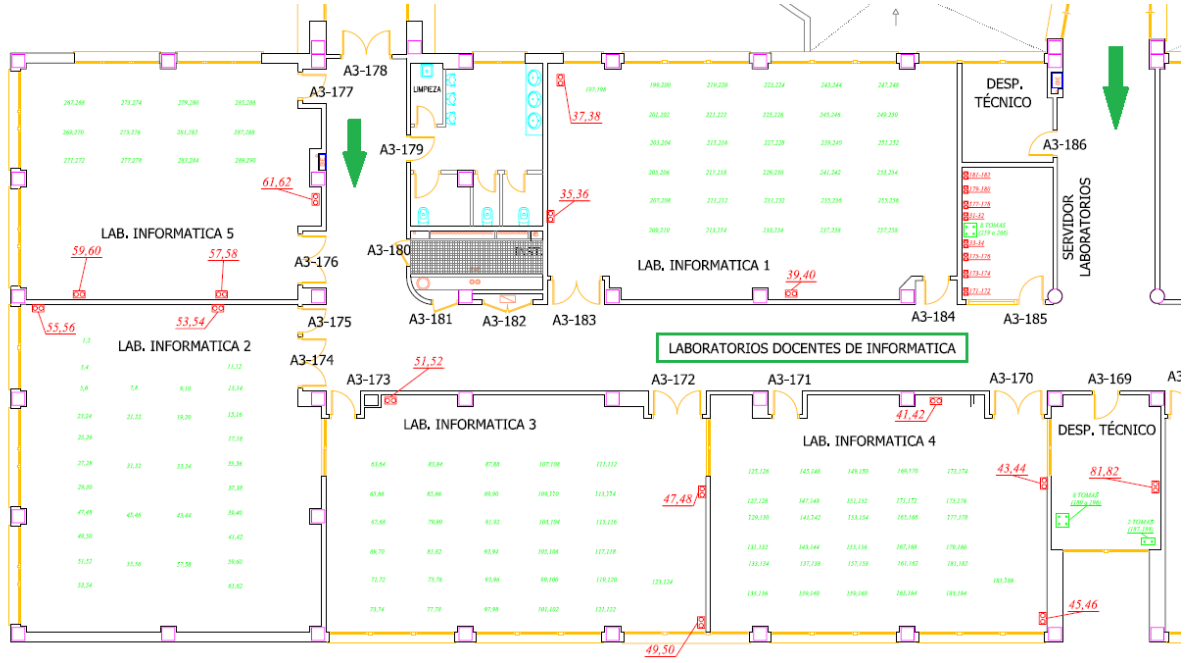

Ilustración 1.11. Plano de la zona de laboratorios del Departamento

En dos de estos espacios vamos a entrar algo más en detalle, puesto que son los que realmente se verán afectados en la implantación de alguna solución de escritorio remoto:

- Laboratorios de docencia: donde están instalados los ordenadores para realizar las prácticas de las asignaturas y contra los que se establecerán las conexiones remotas a sus diferentes escritorios.
- Sala de servidores: donde se ubicará el equipo servidor encargado de administrar y gestionar las conexiones a los diferentes puestos de trabajo con la instalación de alguna de las soluciones existentes en el mercado.

1.4.1.1 Laboratorios de docencia

Son los espacios del Departamento de Informática preparados y configurados para desarrollar e impartir la parte práctica de las asignaturas, entre otras, del Grado de Informática.

El equipamiento y uso de todos los laboratorios es similar. Cuenta con treinta puestos individuales más el del profesor equipados con el correspondiente ordenador

y conexión de red. Además, disponen de un cañón (o proyector de vídeo) conectado al equipo del profesor, y su pantalla de proyección.

Ilustración 1.12. Laboratorio 4 (A3-170)

La configuración de los ordenadores en cada laboratorio también es la misma. Todos cuentan con arranque múltiple, gestionados con GNU GRUB (GRand Unified Bootloader), que permite la selección del sistema operativo con el que se va a trabajar al arrancar el ordenador. Esto es, porque los equipos tienen instalados varios sistemas operativos que se usarán según las necesidades de que asignatura de prácticas. Actualmente, como mínimo, hay instalados 2 sistemas operativos en todos los ordenadores: Windows 10 y Ubuntu 20.04 LTS. La excepción se encuentra en el Laboratorio 4 en el que también está montado CentOS 7 (con sistema de ficheros ZFS) y Ubuntu 20.04 LTS (con sistema de ficheros ZFS), necesarios para el desarrollo de una asignatura porque permite deshacer todos los cambios realizados en el equipo de forma muy rápida y sencilla. Es decir, el acceso al escritorio remoto debe estar configurado para cualquiera de los sistemas operativos instalados en el PC.

El software instalado en estos sistemas operativos depende de cada asignatura y va cambiando de manera continua en función de las necesidades docentes, aunque

hay ciertas aplicaciones que, por su uso habitual, están siempre instaladas en los equipos en su última versión:

- Paquete ofimático Microsoft Office (Word, Excel, Powerpoint, Access, Publisher, OneNote y Outlook)
- Panda Dome (Antivirus)
- 7Zip (potente compresor y descompresor de archivos que soporta un gran número de formatos)
- Adobe Acrobat Reader (visor de ficheros PDF)
- Navegadores web Google Chrome y Firefox
- Gimp (herramienta de edición y retoque de imágenes)
- VLC (reproductor multimedia)
- VirtualBox (software de virtualización)
- Visual Studio Code (editor de código fuente)
- Entornos de desarrollo CodeBlocks y CLion
- Veyon (herramienta para monitorizar y controlar ordenadores)

La mayor parte de estas aplicaciones utilizadas son software libre o gratuito. Solamente el paquete Office y el antivirus requieren licencia para su uso.

En cuanto al hardware actual de los ordenadores, cabe destacar que todos ellos son ordenadores clónicos con tarjetas gráficas instaladas aparte para ampliar sus capacidades, a excepción del laboratorio 2 (también conocido como “aula Mac”), que cuenta con 31 equipos iMac de 27 pulgadas fruto de un acuerdo con Apple en el año 2011.

Ilustración 1.13. Laboratorio 2 (A3-174, aula Mac)

El uso prioritario (aunque no exclusivo) de esta aula va dirigido hacia la asignatura de “Desarrollo de software para dispositivos móviles”, de 3º del Grado de Ingeniería Informática, que requiere del uso de herramientas de desarrollo sobre Mac OS, y en general, de asignaturas relacionadas con el diseño o edición de imagen o video que usen herramientas específicas de Mac OS, o que aprovechen las características peculiares de estos ordenadores.

La siguiente tabla resume las características actuales de los equipos de los distintos laboratorios.

Laboratorio	Procesador	Memoria	Disco duro
1 (A3-183)	Intel Core i7-7700 3.60Ghz	16Gb	HD 2Tb
2 (A3-174)	Intel Core i7 2.93Ghz	16Gb	SSD 1Tb
3 (A3-172)	Intel Core i7-8700 3.20Ghz	16Gb	HD 1Tb
4 (A3-170)	Intel Core i7-8700 3.20GHz	16Gb	SSD 480Gb
5 (A3-176)	Intel Core i7- 10700F 2.9GHz	16Gb	SSD 480Gb
6 (L-119)	Intel Core i7-9700 3.0GHz	16Gb	SSD 480Gb

Tabla 1.1. Características técnicas de los PC de los laboratorios

Otra característica importante en cualquier tipo de organización, y que afectará al resultado del objetivo final de este trabajo, es la velocidad de red.

Las velocidades de red se rigen, entre otras cosas, tanto por las características de la tarjeta de red como por el tipo de cable usado. Todos los PC de los laboratorios cuentan con tarjetas de red (Ethernet) con una velocidad de 1Gbps (Gigabits por segundo), su cableado es de categoría 5e (o superior) y los switchs de conexión de los equipos admite también velocidades de transmisión de datos de 1Gbps.

Ilustración 1.14. Armario (o rack) de comunicaciones de la sala de servidores

Todas estas características del hardware actual permiten una conexión a Internet ideal proporcionando una buena experiencia de usuario al realizar una conexión de escritorio remoto desde el exterior de la UJA.

El esquema de red de los laboratorios se refleja en la siguiente imagen:

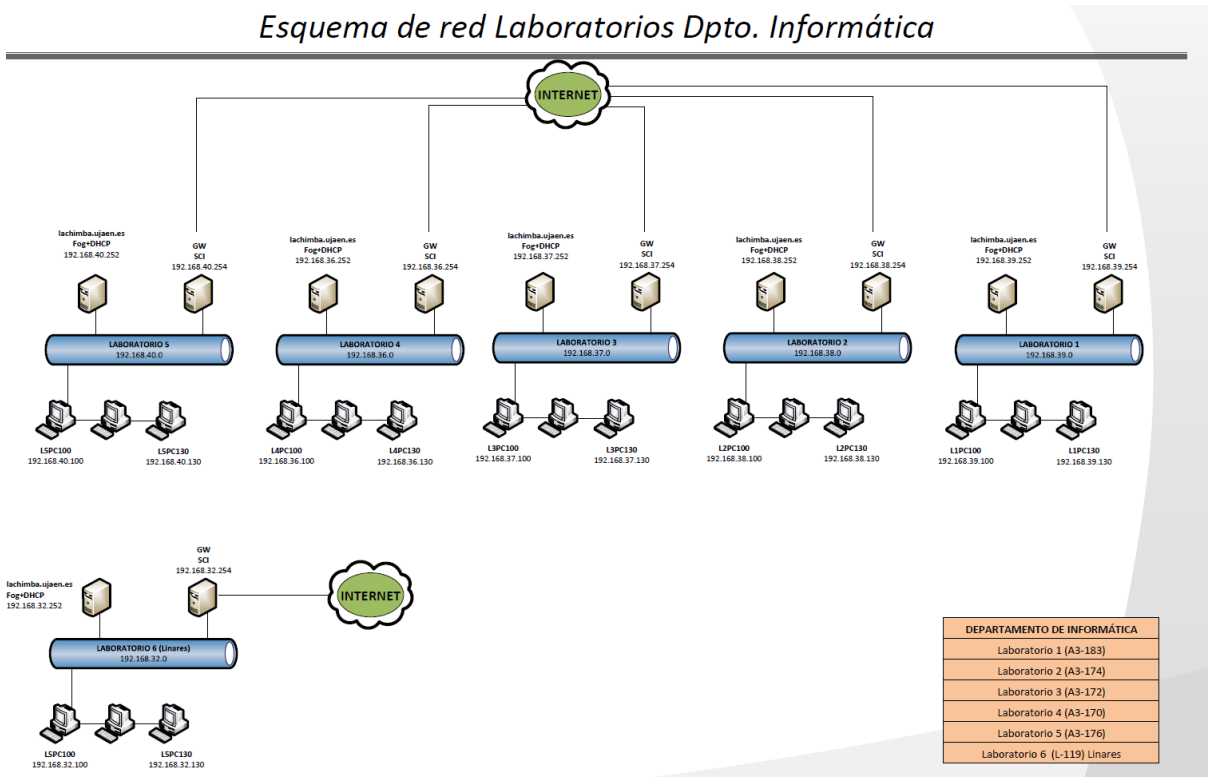

Ilustración 1.15. Esquema de red de los laboratorios

Como se observa en esta imagen, cada laboratorio cuenta con una subred interna independiente y un servidor de DHCP encargado de establecer de manera una dirección IP concreta a cada uno de los equipos. Esto es importante dado que para el establecimiento de cualquier conexión remota es imprescindible conocer la dirección IP del ordenador de destino.

Laboratorio	Subred
1 (A3-183)	192.168.39.0
2 (A3-174)	192.168.38.0
3 (A3-172)	192.168.37.0
4 (A3-170)	192.168.36.0
5 (A3-176)	192.168.40.0
6 (L-119)	192.168.32.0

Tabla 1.2. Lista de las subredes internas de los laboratorios

Para ello, cada laboratorio tiene creada una máquina virtual con el sistema operativo Ubuntu 20.04 LTS en el servidor del Departamento lachimba.ujaen.es

ubicado en la sala de servidores (A3-185). Dichas máquinas virtuales son las encargadas de dar servicio DHCP al laboratorio correspondiente de la siguiente manera:

- Asignación de dirección IP según dirección MAC. Cada puesto de trabajo de cada laboratorio tendrá asignada de forma automática una dirección IP fija en el rango de 192.168.XX.101-130 (siendo XX el valor correspondiente a la subred del laboratorio en cuestión). Por ejemplo: el puesto número 12 del laboratorio 3 tendrá asignada la IP 192.168.37.112. En el caso de los puestos del profesor siempre se asignará la IP 192.168.XX.100
- Rango de asignación dinámica de direcciones IP: 192.168.XX.132-199. Todos los laboratorios tienen, al menos, 2 tomas de red por cada ordenador. Estas tomas pueden ser utilizadas por los usuarios para conectar otros dispositivos en las prácticas de sus asignaturas (otro PC, portátiles, switch…)
- Asignación del resto de parámetros relativos a la configuración de red:
  - Máscara de subred: 255.255.255.0
  - Gateway (dirección IP): 192.168.XX.254
  - Servidor DNS (dirección IP): 150.214.170.15

Además del servicio DHCP, otra de las funciones de estas máquinas virtuales es gestionar el software instalado en los ordenadores con la ayuda de un sistema de gestión y clonado de imágenes: FOG [8], proyecto enfocado en facilitar la administración de imágenes de ordenadores y clonado de las mismas sobre ordenadores en una red haciendo uso de una interfaz web.

Cada una de estas 6 máquinas virtuales, con el objeto de evitar cuellos de botella durante la transferencia de las imágenes, sale al exterior por una tarjeta de red distinta conectada a la subred de cada uno de los laboratorios. La razón para la instalación de FOG en máquinas virtuales individuales es tener la flexibilidad de hacer diferentes operaciones al mismo tiempo en distintos laboratorios.

FOG permitirá configurar fácilmente todos y cada uno de los equipos de los laboratorios (mediante el clonado de imágenes con las opciones de “Escritorio Remoto” y “Compartir pantalla” activados) que permita el acceso a sus escritorios remotos que es el objetivo principal de este trabajo.

1.4.1.2 Sala de servidores

Los servidores para atender a las necesidades de docencia e investigación del departamento se encuentran en su mayoría en la dependencia A3-185. Ésta dispone de un sistema de refrigeración para mantener una temperatura constante y los correspondientes racks para acoger a los servidores.

A continuación, se muestra la lista de servidores existentes en esta dependencia en la actualidad:

Nombre	Marca	Modelo	Observaciones
Lachimba	Huawei	1288H V5	Servidor de virtualización
Lamella	HP	Proliant DL360p Gen8	Servidor Apache Guacamole
Keops	DELL	PowerEdge 1950	Servidor de virtualización
Kefren	DELL	PowerEdge 1950	Servidor de virtualización
Micerino	DELL	PowerEdge 1950	Fuera de servicio (Gitlab)
Pandera	DELL	PowerEdge R410	Servidor de virtualización
Almadén	Cofiman	-	Respaldo DHCP
Valdepeñas	HP	Proliant DL160 G5	Pruebas servicio CentOS 6
Aznaitin	Lenovo	EMC2 px4 300r	Servidor documental
Suleiman	Lenovo	SR650 ThinkSystem	Serv. Investigación Sinbad2
Serezade	HP	Proliant Dl165 G7	Serv. Investigación Sinbad2
Sinbad2	HP	Proliant Dl180 G6	Serv. Investigación Sinbad2
Pastira	Azken	-	Serv. Investigación GGGJ
Ararat	DELL	PowerEdge R715	Serv. Investigación SINAI
Titan	Clónico	-	Servidor de investigación
Tornasol	DELL	PowerEdge T110 II	Servidor de investigación
Custodes	Fujitsu	Primergy RX2530 M5	Serv. Investigación SIMIDAT

Tabla 1.3. Servidores del Departamento de Informática

Como se puede ver, existen tres tipos de equipos en esta sala:

- La mayoría son equipos servidores adquiridos por los grupos de investigación del Departamento, gestionados por estos mismos grupos.
- Servidores de virtualización, gestionados por los técnicos de laboratorio del Departamento y cuya función es ejecutar las máquinas virtuales solicitadas por los miembros del Departamento (para cursos internos, trabajos de fin de

Grado, trabajos de fin de Máster, sitios web, proyectos de investigación, etc.)

- Máquinas para apoyo a la docencia de los laboratorios: aznaitin (servidor documental y NAS para copias de seguridad), lamella (servidor Apache Guacamole, cuya función se describirá más adelante), lachimba (contiene las máquinas virtuales de FOG para el clonado de imágenes de los ordenadores) y Almadén (DHCP de respaldo).

A parte del listado anterior de servidores, en esta dependencia podemos encontrar otros equipos pertenecientes también a los grupos de investigación, varios dispositivos de almacenamiento (NAS) y el armario de comunicaciones de los laboratorios.

Ilustración 1.16. Sala de servidores del Departamento (A3-185)

La instalación y configuración de una de las posibles soluciones de escritorio remoto a cualquier ordenador de los laboratorios (Apache Guacamole) se realiza en uno de estos servidores que el Departamento cede temporalmente para la evaluación de la herramienta y los beneficios de la aplicación de la misma.

1.4.1.3 Red corporativa y seguridad en la Universidad de Jaén

La UJA dispone de una arquitectura de red multiservicio, que permite la convergencia de servicios y dispositivos. La red corporativa de la Universidad de Jaén

se denomina RIUJA (Red Informática de la Universidad de Jaén), y su infraestructura se compone de dos campus principales (Jaén y Linares), separados entre sí a una distancia de 50 Km y algunas otras sedes menores repartidas en Jaén capital.

En el campus principal existe un CPD que alberga la práctica totalidad de los servicios TIC ofrecidos. Todas las comunicaciones hacia y desde el exterior están soportadas por la electrónica de red correspondiente alojada en este CPD. Las comunicaciones internas están enfocadas a unir los conmutadores de todos los edificios con los conmutadores centrales del CPD, los cuales concentran las redes de usuarios y servidores.

Actualmente la topología de red de la UJA está dividida en sus distintas sedes:

- Campus de Las Lagunillas (Jaén). Es la sede central de la UJA. En este campus se encuentra la conexión con Internet a través de CICA/RedIRIS, el CPD y el grueso del equipamiento de red de la UJA. Se encuentra dividido en 21 edificios interconectados entre sí a través de una topología en estrella con dos núcleos principales, situados en el Edificio Zabaleta (D1) y en el Edificio de Ingeniería y Tecnología (A3).
- Campus Científico Tecnológico (Linares). Es el otro gran campus de la UJA. En él se encuentra la Escuela Politécnica Superior de Linares. Con un total de 6 edificios, es la infraestructura más grande de la UJA fuera de su sede central de Jaén.
- Un edificio en el centro de Jaén (Edificio de Magisterio).

Todas estas sedes se encuentran interconectadas a través del servicio MacroLAN de Telefónica con anchos de banda que oscilan entre los 100 Mbps y 1Gbps.

La seguridad perimetral es uno de los métodos más habituales de defensa de una red. Se basa en el establecimiento de elementos de seguridad en el perímetro de la red y en diferentes capas, lo que nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, denegando cualquier tipo de acceso al resto.

Algunos de los objetivos que persigue la seguridad perimetral son:

- Definir y proteger todo el perímetro de nuestra red, proporcionando un único punto de interconexión con el exterior.

- Permitir solo ciertos tipos de tráfico autorizados o entre determinados orígenes y destinos, denegando el resto.
- Redirigir el trafico entrante solo a los sistemas autorizados dentro de la red corporativa.
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet.
- Registrar y auditar el tráfico entre el exterior y el interior.
- Ocultar información de nuestra red al exterior: nombres de sistemas, topologías de red, tipos de dispositivos de red, cuentas de usuario, etc.

Se conoce como perímetro de la red a la frontera entre el exterior (generalmente Internet) y los equipos, servidores y dispositivos de nuestra red interna. Los elementos que lo componen son:

- Router frontera. Es un dispositivo situado entre la red interna y las redes de otros proveedores que intercambian el tráfico con nosotros y que se encarga de dirigir el tráfico de datos de un lado a otro. Es el ultimo router que controlamos antes de Internet. La primera y última línea de defensa que realiza el filtrado inicial y final.
- Cortafuegos (firewalls). Son los dispositivos más directamente relacionados con la seguridad perimetral. Son capaces de permitir, limitar, cifrar/descifrar, el tráfico entre equipos o redes sobre la base de un conjunto de políticas establecidas, además de otros criterios.
- Sistemas de Detección y Prevención de Intrusiones (IDS/IPS). Son sistemas y aplicaciones usadas para detectar y proteger un ordenador/servidor o una red frente a accesos no autorizados. Un IDS/IPS permite:
    - Detectar ataques en el momento que están ocurriendo o poco después.
    - Automatizar la búsqueda de nuevos patrones de ataque, gracias a herramientas estadísticas de búsqueda y análisis de trafico anómalo.

  - Automatizar tareas como la actualización de reglas, obtención y análisis de logs, configuración automática de políticas de firewalls, etc.
  - Monitorización y análisis de la actividad de los usuarios. De este modo se pueden conocer los servicios realmente en uso y estudiar el contenido del tráfico en busca de elementos anómalos (conexiones fuera de hora, reintentos de conexión fallidos y otros).
  - Auditoria de configuraciones y vulnerabilidades de determinados sistemas.
  - Descubrir sistemas con servicios que no deberían tener habilitados, mediante el análisis del tráfico y de logs.

- Redes Privadas Virtuales (VPN). Son redes privadas construidas sobre una infraestructura de red pública, generalmente Internet. Para ello se establece una conexión virtual punto a punto que cifra toda la comunicación, de forma que los usuarios tienen acceso seguro a la red corporativa de la organización como si estuvieran conectados directamente a ella. Las organizaciones usan VPNs para conectar de forma segura oficinas y usuarios remotos a través de accesos a Internet proporcionados por ISP, en lugar de usar líneas dedicadas. Las VPN proporcionan un alto nivel de seguridad y protegen los datos que transportan frente a accesos no autorizados.

Uno de los elementos fundamentales de la seguridad perimetral son los firewalls. Definidos como elementos de red que previenen accesos no autorizados desde Internet (o cualquier otra zona potencialmente insegura) a las redes de una organización. Generalmente operan sobre un dispositivo dedicado, conectado a la red corporativa, pero fuera de ella, en el perímetro. Todos los paquetes que entran y salen a través de los firewalls son filtrados o examinados para asegurar que el tráfico de red cumple con la política de seguridad establecida por la organización.

Los firewalls proporcionan una capa de aislamiento entre redes internas y externas. Se asume en este escenario que todas las amenazas vienen del exterior, aunque no siempre es así. Podemos tener amenazas desde dentro de nuestra propia red. El espacio protegido (perímetro de seguridad) suele ser propiedad de la

organización, y la protección se realiza contra una red externa no confiable, llamada zona de riesgo.

A la hora de implantar un firewall hay que definir qué se va a permitir y qué se va a denegar. Podemos optar por dos filosofías de actuación:

- Denegar todo el tráfico no permitido explícitamente: es la más segura y la más usada. Consiste en empezar con una red cerrada totalmente a cualquier tipo de tráfico externo, e ir abriendo únicamente los tipos de tráfico autorizados.
- Permitir todo el tráfico no denegado explícitamente: ésta es más cómoda, aunque menos segura, siendo útil en el caso de que deseemos protegernos sólo de algunos tipos de ataque.

Queda claro que la seguridad perimetral ofrecida por un firewall es una primera e importante línea de defensa. Pero siendo realista, si un atacante quiere acceder a nuestra red acabará encontrando algún modo de hacerlo. En ese caso hay que limitar lo más posible un ataque una vez tenemos al enemigo dentro de nuestra red, mediante la segmentación de la misma.

La segmentación [9] es una técnica de seguridad que divide una red física en distintos segmentos o subredes lógicas más pequeñas, permitiendo a los equipos y dispositivos estar compartimentados y aplicar controles de seguridad específicos a cada una de esas subredes y segmentos. Hace años, las redes tradicionales tenían una arquitectura plana con un único perímetro defensivo exterior. La segmentación, sin embargo, nos permite aplicar el principio de defensa en profundidad, mediante diferentes capas, dentro de unos límites manejables por los administradores de red. Este esquema aplica no solo a las amenazas externas, sino también a las internas, evitando que usuarios, que ya tienen acceso a determinadas zonas de nuestra red, tengan acceso a otras zonas a las que no están autorizados.

Para definir las zonas en las que segmentar la red corporativa, podemos usar múltiples criterios. Entre ellos, se proponen los siguientes:

- Segmentación en función de los procesos de negocio y qué información se intercambia. De esta forma podremos dar a los usuarios acceso exclusivamente a los datos que necesitan para su actividad y no a otros, siguiendo siempre el principio de mínimo privilegio (otorgar siempre el

mínimo privilegio al usuario e ir ampliando accesos según los vaya necesitando).

- Segmentación en función de la estructura organizativa, asignando diferentes VLAN y direccionamiento IP asociado a cada unidad que compone la Universidad: Departamentos, Servicios, Unidades, etc.
- Segmentación en función de los diferentes colectivos. Así, se pueden tener VLAN específicas para el personal de administración y servicios, para el personal docente e investigador, para estudiantes o para diferentes perfiles de conexión en el caso de la red WiFi (eduroam), por poner algunos ejemplos.
- Segmentación en función de grupos de tráfico de red con características especiales y significativas. De esta forma, en la UJA se definen VLAN y subredes específicas para diferentes perfiles de red wifi (personal de administración y servicios, personal docente e investigador, estudiantes, visitantes, invitados, etc.), perfiles de conexión VPN, sistemas de videovigilancia, etc.

El resultado final es una segmentación en subredes lo más granular posible (a mayor segmentación, mayor seguridad) en base a varios de los criterios anteriores, generalmente una combinación de varios.

1.4.1.4 Seguridad en los laboratorios y servidores

La seguridad en los laboratorios se implementa a varios niveles. En primer lugar, a nivel físico. Todos los equipos están protegidos frente al robo mediante un punto de anclaje Kensington (cuando éste está disponible), o usando cables y candados para este fin.

A nivel software, los laboratorios no cuentan con un sistema de congelación de equipos por los inconvenientes que éste puede generar: pérdida de trabajos o archivos, pérdida de configuraciones realizadas en el sistema (algo muy habitual en las asignaturas del Grado en Informática), imposibilidad de instalar (o desinstalar) aplicaciones, etc. En este caso, la seguridad a nivel de software está cubierta con FOG (sistema de administración y clonado de imágenes vía web) ya que permite restaurar rápidamente el sistema operativo (o el disco duro completo) de cualquier

puesto de trabajo si éste es modificado por un alumno de manera no autorizada. Además, los sistemas Windows instalados en los laboratorios disponen del antivirus Panda con la correspondiente licencia Campus universitaria.

Otro elemento de seguridad es el sistema de gestión de asistencia (https://aries.ujaen.es/asistencias/inicio.php) instalado en todas las aulas de informática de la UJA incluyendo, lógicamente, los laboratorios docentes del Departamento de Informática. Este sistema permite controlar los alumnos que han asistido a una sesión concreta, así como examinar los equipos que han utilizado en caso de que sea necesario.

Por último, tanto los laboratorios como los servidores del Departamento están sujetos a las políticas de seguridad globales establecidas por el Servicio de Informática para la red informática de la Universidad de Jaén (RIUJA), que bloquean la mayoría de puertos para evitar accesos no autorizados desde el exterior. Existe, no obstante, un procedimiento establecido por dicho servicio para, de una manera justificada, abrir los puertos en el firewall que se estimen necesarios para el correcto funcionamiento de una aplicación o servicio concretos.

1.4.2 Resumen de las deficiencias y carencias identificadas

Una vez descrita y analizada la situación actual en los laboratorios docentes del Departamento de Informática para la realización de las prácticas de las asignaturas, es posible definir las deficiencias identificadas en el desarrollo de éstas en el caso de no poderlo hacer en los espacios preparados para ello. El objetivo es tratar de superarlas o mejorarlas una vez sea implantada alguna solución para realizar conexiones de escritorio remoto contra los ordenadores de los laboratorios docentes. Serían las siguientes:

1. La imposibilidad del uso de ciertas herramientas software, disponibles únicamente en los laboratorios docentes (aun teniendo los estudiantes medios tecnológicos suficientes para el desarrollo de sus prácticas). Se trata de software de pago que requieren de licencia para su utilización.
2. En asignaturas concretas, ejecución de ciertas tareas que implican una alta potencia de computación.
3. Uso de sistemas operativos y software específicos. Es el caso de Mac OS, sistema operativo creado por Apple para sus propios equipos. Si bien es

técnicamente posible ejecutar Mac OS en alguna herramienta de virtualización, es ilegal para ejecutarlo en hardware que no sea de la compañía. Es decir, que mediante la ejecución de Mac OS en una máquina virtual se estarían violando los términos de servicio de Apple.

Además de esto, la posibilidad de conexión con los escritorios remotos de los laboratorios del Departamento, permitiría aumentar aún más el nivel de ocupación en situaciones específicas de los usuarios como pueden ser:

- Horarios especiales en la realización de las prácticas (incluso fuera del horario laboral).
- Uso en días no lectivos o fines de semana.
- Uso en periodo vacacional.
- Imposibilidad de desplazamiento al Campus de la UJA, o confinamientos temporales de los usuarios.

Lógicamente, para permitir el uso de los ordenadores en remoto en estas situaciones, la solución de escritorio remoto a implantar tiene que permitir establecer un control y gestión en la asistencia de los usuarios por parte de un administrador o responsable de la asignatura / proyecto.

1.5 Requisitos

Una conexión remota implica, al menos, dos computadoras:

- Un equipo local, o sea el cliente. Este es el ordenador que se controlará usando el software de acceso remoto.
- Un equipo remoto, también llamado servidor. Este es el ordenador donde se indicarán los comandos que queremos ejecutar en el equipo del cliente.

Partiendo de esta base, los requisitos mínimos necesarios, sin entrar en detalle, de cualquiera de las herramientas de conexión remota son los que se enumeran a continuación:

- Debe existir una conexión de red funcional.

- El acceso remoto debe estar habilitado y configurado en ambos equipos (Escritorio remoto de Windows, Software para conexión remota cliente/servidor, …)
- El equipo que se conecte (cliente) debe tener permiso para conectarse.
- Conocer la dirección IP del equipo al que queremos conectar.
- El equipo que recibirá la conexión (servidor) debe estar encendido y activado.

1.6 Alcance

El objetivo final de este trabajo fin de grado es implantar la herramienta software que mejor se ajuste a las necesidades del Departamento de Informática para cubrir las necesidades de acceso remoto a los puestos de trabajo de los laboratorios en situaciones específicas de docencia on-line que permitan el normal desarrollo de las clases prácticas.

Teniendo en cuenta esto, el listado de los entregables de este trabajo es el siguiente:

1. Memoria del trabajo fin de grado: fichero en formato PDF que desarrolla el estudio técnico de la evaluación de herramientas software actuales para la conexión remota de los usuarios, y de la implantación de alguna de las soluciones descritas.
2. Software: carpeta con todos los ficheros necesarios en el proceso de instalación de la herramienta elegida (igualmente descrito en la memoria anterior).
3. Dirección URL de la instalación de la solución (**https://lamella.ujaen.es**): el montaje se realizará en un servidor cedido de manera temporal por el Departamento de Informática para el uso y pruebas antes de su posible implantación definitiva. Es decir, únicamente usando un navegador web y desde cualquier PC con acceso a esta dirección, se podrá acceder a dicha aplicación.
4. Máquina virtual con la herramienta ya instalada: se entregará esta máquina en formato OVA, con el sistema operativo Ubuntu 20.04 y la solución

seleccionada. Permitirá su utilización en cualquier ordenador de forma local (con la ayuda de cualquier software de virtualización como pueden ser Oracle VM VirtualBox o VMWare WorkStation), o en cualquier red local para poder acceder a los ordenadores que tengan configurado el acceso remoto correspondiente.

5. Copia de la base de datos con toda la información y configuración de la aplicación de Escritorio remoto para el acceso remoto a un conjunto de ordenadores de cada uno de los laboratorios de prácticas del Departamento: usuarios, conexiones a los ordenadores, tipos de conexiones, puertos de acceso, etc.

1.7 Hipótesis y restricciones

Para la consecución del principal objetivo del trabajo de acceso seguro a los laboratorios de prácticas, a priori, contamos con todos los medios tecnológicos posibles (y cedidos por el Departamento de Informática) y de personal.

Así mismo, por su influencia en la elección y despliegue de alguna de las soluciones de escritorio remoto del mercado, hay que tener en cuenta las siguientes restricciones:

- Restricción económica: para reducir costes al máximo, el software a elegir para su implantación será gratuito o libre, en el que no existan limitaciones de ningún tipo (de tiempo de uso, número de conexiones, etc.), y que garantice los elementos para un acceso remoto fácil, seguro y controlado a todos los usuarios de este servicio.
- Restricciones de seguridad: establecidas e impuestas por el Servicio de Informática en sus políticas de seguridad globales para la red informática de la Universidad de Jaén (RIUJA), que bloquean la mayoría de puertos para evitar accesos no autorizados desde el exterior, con lo que la herramienta seleccionada debe utilizar puertos abiertos y accesibles según estas medidas o, en caso contrario, se necesitaría el uso de otro tipo de redes como una VPN que se saltara estas restricciones. Además, en el caso de instalación de alguna herramienta con interfaz web, es necesario el uso del protocolo HTTPs, así como redirección automática desde HTTP a HTTPs,

proporcionando el Servicio de Informática los certificados SSL necesarios para el servidor web. Se trata de aplicar tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envíe entre los dos extremos e impedir que pueda ser leída y modificada en su transmisión.

1.8 Estudio de alternativas y viabilidad

En este apartado se realiza un breve estudio de las herramientas software de Escritorio remoto más destacadas del mercado, con el análisis de sus principales características, ventajas e inconvenientes, así como la viabilidad para su instalación en el Departamento de Informática. Igualmente se justifica la elección de una de ellas que será la que se detalle más en profundidad en próximos apartados de este documento.

1.8.1 Escritorio remoto de Windows

También conocido como “Remote Desktop” [10], o RDP, es el programa que ofrece Microsoft en su sistema operativo para conectarnos de forma remota a cualquier ordenador, siempre y cuando se den las condiciones técnicas necesarias. En algunos casos puede incluso tener un acceso total al ordenador remoto, lo que depende del nivel de autorización.

Microsoft ofrece a los usuarios de Remote desktop un protocolo de red propio, el Remote Desktop Protocol (RDP). Por así decirlo, este protocolo es la herramienta de control de los servicios de terminal (Remote Desktop Services) y se ocupa de la ejecución de los comandos de escritorio remoto. RDP controla tanto el terminal servidor como el cliente y regula la transferencia de los contenidos de la pantalla y de las entradas del teclado y del ratón a través de la red.

Este software, proporcionado gratuitamente por Microsoft, no se tiene que descargar ni instalar. Simplemente tendremos que activarlo desde Configuración > Sistema > Escritorio Remoto para que quede listo para usarlo.

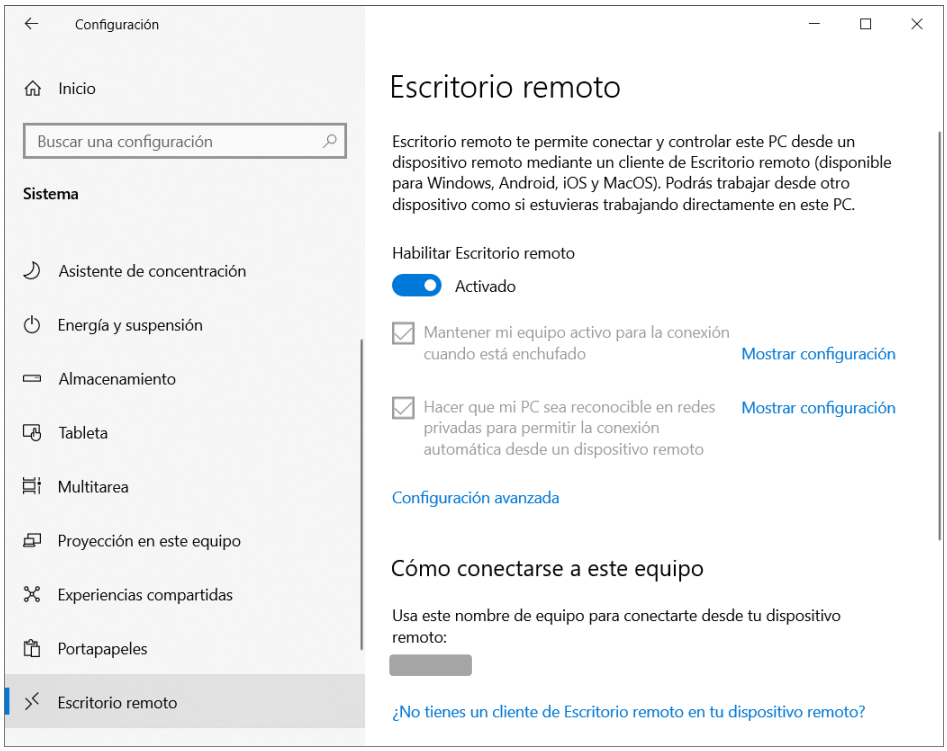

Ilustración 1.17. Activación del Escritorio remoto de Windows 10

A diferencia de otra variante de éste (asistencia remota de Windows), que veremos más adelante, el escritorio remoto permite que otra persona inicie sesión en el sistema host deseado sin necesidad de una "conexión" activa. El sistema local funciona en este caso como servidor que permite a los usuarios registrarse como usuarios "locales". Para iniciar sesión deben formar parte de la lista de usuarios del sistema local y disponer de una contraseña.

Entre sus principales características podemos destacar lo sencillo, fácil y rápido que es. Como se ha comentado anteriormente, no hay que hacer nada más que activarlo en el ordenador que queremos controlar, y después, desde uno de los muchos clientes que existen, conectarnos a nuestro PC a través de su IP o un DDNS. Los datos de acceso (usuario y contraseña) son los mismos que los datos de acceso a nuestro PC.

Ilustración 1.18. Escritorio remoto de Windows

Al igual que otras aplicaciones de este tipo, permite realizar el redireccionamiento del audio (permite al usuario ejecutar un programa de audio en ordenador remoto y escuchar el sonido en el local), redireccionamiento del sistema de ficheros, compartición del portapapeles, impresión remota, etc.

Sus dos principales desventajas son, en primer lugar, que se bloquea la sesión en el ordenador local mientras lo controlamos, por lo que no vemos qué se está haciendo en remoto. Y la segunda, que el servidor RDP solo está disponible (a partir de Windows 7) para los usuarios de Windows versión Professional, Enterprise o Ultimate. La edición Home no se puede controlar a través de este programa (aunque sí nos permite conectarnos a otros ordenadores como cliente).

Aunque la transmisión de datos entre cliente y servidor está cifrada, para mejorar aún más la seguridad del escritorio remoto de Windows se puede aplicar una serie de medidas como éstas:

- Mantener el software actualizado. La razón es que en muchas ocasiones pueden surgir vulnerabilidades que son aprovechadas por los piratas informáticos para llevar a cabo sus ataques. De ahí que debamos aplicar los parches y actualizaciones del sistema que haya disponibles con el objetivo de corregirlo lo antes posible.

- Utilizar contraseñas fuertes y autenticación en dos pasos. Ya que la aplicación nos obliga a logarnos en el sistema, algo esencial que debemos tener en cuenta en todo momento a la hora de proteger el escritorio remoto o cualquier servicio o herramienta que utilicemos es crear contraseñas que sean seguras.

- Cambiar el puerto por defecto. Así se evitan posibles atacantes que puedan apuntar hacia este puerto por defecto, que es el 3389.
- Limitar y controlar los usuarios que pueden acceder. Esto es posible hacerlo en el apartado de configuración del Escritorio Remoto. Igualmente, dentro de la configuración avanzada de este mismo apartado, permite configurar sólo el acceso de equipos con Autenticación a nivel de red (NLA). Cuando se habilita esta opción, los usuarios deben autenticarse en la red antes de conectarse a tu equipo.

Debido a que el RDP cuenta con un puerto propio (3389) para comunicarse con otros ordenadores, en el caso de comunicaciones fuera de la red como, por ejemplo, a través de Internet, entra en acción el firewall, lo que bloquea la conexión. Para poder usar el Remote desktop de Windows sería necesario modificar la configuración en la seguridad perimetral de la Universidad añadiendo reglas de exclusión en los ajustes del firewall. Asimismo, el router de la WLAN puede suponer otro impedimento para la conexión remota ya que habría que redireccionar puertos para poder usar esta aplicación. Estos posibles obstáculos nos hacen ver que no es la solución idónea para implantar como herramienta de conexión remota a los laboratorios del Departamento.

1.8.1.1 Escritorio remoto multisesión

El sistema operativo Windows, de forma predeterminada, no es multisesión. Es decir, únicamente puede haber una sesión de usuario conectada ya sea en modo local o en remoto. Cualquier acceso de un segundo usuario, desconectará al anterior.

En realidad, el número de conexiones RDP simultáneas está limitado más bien por la licencia. Por tanto, esta restricción no permite crear un servidor terminal RDP basado en la estación de trabajo que pueda ser utilizado por múltiples usuarios. La lógica de Microsoft es simple: si necesita un servidor de escritorio remoto, debe comprarse una licencia de Windows Server, RDS CAL, instalar y configurar la función de host de sesión de escritorio remoto (RDSH).

Desde un punto de vista técnico, cualquier versión de Windows con una cantidad suficiente de RAM puede soportar el funcionamiento simultáneo de varias docenas de usuarios remotos. En promedio, se requieren 150-200 MB de memoria para una sesión de usuario, sin tener en cuenta las aplicaciones iniciadas. Es decir, el

número máximo de sesiones RDP simultáneas en teoría está limitado solo por los recursos informáticos.

Existen básicamente 2 métodos para convertir un equipo de escritorio Windows en un entorno multisesión que si soporte varios usuarios remotos conectados de forma simultánea:

1. Utilizamos un Windows Server que si está preparado para esta situación de trabajo en entornos multiusuario. De forma predeterminada esta versión de Windows incluye 2 licencias de escritorio remoto válidas para tareas administrativas. Para el uso simultáneo de más usuarios se precisan licencias de Terminal Server adicionales.
2. Utilizar el entorno de escritorio remoto multisesión en la nube de Microsoft.

No es el objetivo de este trabajo este tipo de entornos, pero se trata de otra posibilidad más de esta aplicación.

1.8.1.2 Asistencia rápida (Quick Assist)

Quick Assist [11] es una nueva aplicación que ofrece Microsoft Windows 10 que reemplaza la funcionalidad heredada de “Windows Remote Assistance”. Técnicamente, es una aplicación de escritorio remoto, pero diseñada para ser más fácil de usar y más segura (al estilo de Team Viewer y herramientas similares).

Ilustración 1.19. Logo de Asistencia rápida (o Quick Assist)

A diferencia de la aplicación Escritorio remoto, no necesita habilitar “Escritorio remoto” o “Asistencia remota” a través de Propiedades del sistema, ni abrir un puerto de firewall. Sin embargo, se requieren dos personas (una en cada extremo) para compartir la pantalla de la computadora a través de una conexión remota. Fue diseñado de esta manera porque la aplicación fue creada para que una persona ayude a otra a resolver problemas en una computadora remota.

Para obtener asistencia remota en Windows 10, la persona que ofrece ayuda debe iniciar el proceso y la persona que recibe ayuda debe permitir la conexión. Estos son estos pasos:

1. Tanto el usuario que ayuda como el que comparte inician la aplicación Asistencia rápida.
2. El usuario que ayuda hace clic en el botón “Ayudar a otra persona” del apartado “Proporciona asistencia”. Después deberá iniciar sesión con su cuenta de Microsoft y una vez hecho esto aparecerá un código de seguridad de seis dígitos mismo que tendrá que compartir con la persona a la que va a ayudar. Por razones de seguridad ese código solo será válido durante 10 minutos.
3. El usuario que comparte para recibir ayuda deberá ingresar el código en el campo del apartado "Obtener asistencia". En ese momento la aplicación usa ese código para ponerse en contacto con el Servicio de asistencia remota y unirse a esa sesión remota específica.
4. El usuario que ayuda tiene que seleccionar Solo vista o Control total.
5. Se pide al usuario que comparte que confirme su permiso para compartir escritorio con el que ayuda. En la ventana aparecerá el nombre de usuario que la persona que ayuda tiene en su cuenta de Microsoft, y sólo habría que hacer clic en el botón "Permitir".
6. Quick Assist inicia el control del Protocolo de escritorio remoto (RDP) y se conecta a su servicio de retransmisión.
7. RDP comparte el vídeo con la persona que ayuda a través de https (puerto 443) mediante el servicio de retransmisión RDP al control RDP de la persona que ayuda. La entrada se comparte desde la persona que ayuda a la persona que comparte a través del servicio de retransmisión RDP. La aplicación también permite abrir una pequeña ventana de Chat para enviar indicaciones a la otra persona.

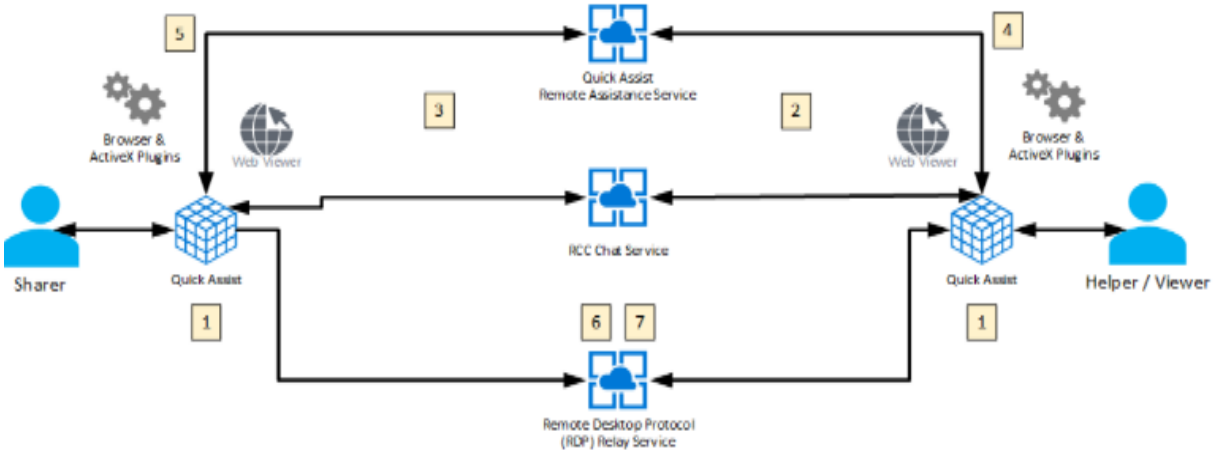

Ilustración 1.20. Flujo de conexiones de una sesión remota con Quick Assist[2]

La aplicación Quick Assist en Windows 10 es muy sencilla y fácil de usar. Si bien la computadora remota solo obtiene un conjunto simple de controles para detener el uso compartido de la pantalla y finalizar la conexión, la persona que brinda la asistencia (Administrador) obtiene acceso a algunas características interesantes, incluida la capacidad de seleccionar el monitor, anotar, ver el tamaño de pantalla real, reinicie la sesión remota e incluso abra el Administrador de tareas. Y también tiene el botón reconectar, pausar y finalizar para finalizar la conexión. Quien recibe ayuda puede detener la "Asistencia rápida" en cualquier momento.

Al estar esta herramienta muy orientada a la asistencia técnica en momentos puntuales, además de sólo poder ser utilizada en plataforma Windows, hace que no sea una herramienta candidata para la instalación en el Departamento. Igualmente, es necesario que ambos usuarios cuenten con una cuenta de Microsoft y que estén presentes en ambos extremos de la comunicación.

1.8.2 Teamviewer

Sin duda, Teamviewer [12] se trata de uno de los programas de control remoto más popular y usado. Es una aplicación multiplataforma y cuenta con funciones para compartir y controlar escritorios, reuniones en línea, videoconferencias, transferencia de archivos entre ordenadores, así como la posibilidad de acceder a otro equipo que se encuentre ejecutando TeamViewer con un navegador web.

[2] Microsoft: Asistencia rápida para ayudar a los usuarios
https://docs.microsoft.com/es-es/windows/client-management/quick-assist

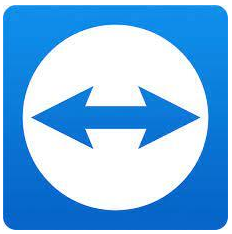

Ilustración 1.21. Logotipo de Teamviewer

TeamViewer conecta ordenadores, teléfonos inteligentes, servidores, dispositivos IoT, robots, etc. con conexiones rápidas y de alto rendimiento incluso en entornos de bajo ancho de banda.

No es necesaria su instalación (versión portable) para hacer conexiones puntuales para dar asistencia técnica, por ejemplo. El propio fichero ejecutable en su asistente de instalación nos ofrece esta posibilidad de sólo iniciar la aplicación. Sólo con esto, se podría realizar la conexión para permitir asistencia, o bien para ofrecerla, al estilo de la herramienta de Asistencia rápida de Windows (comentada anteriormente) compartiendo un código y una contraseña. Para una mejor experiencia también es posible crear una cuenta de Teamviewer que permite, entre otras cosas, administrar los equipos a los que nos conectamos y poderlos controlar y monitorizar desde cualquier otro dispositivo remoto.

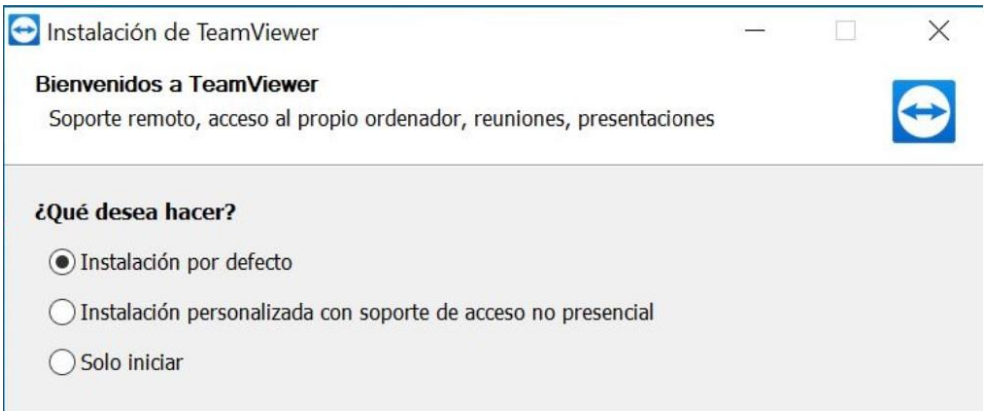

Ilustración 1.22. Asistente de instalación de Teamviewer

Tampoco es necesaria ninguna configuración específica en el firewall o router para su uso en conexiones de equipos conectados a través de Internet. TeamViewer prefiere establecer conexiones TCP y UDP salientes a través del puerto 5938, que es el principal puerto que utiliza y con el que TeamViewer tiene un mejor rendimiento.

Pero si TeamViewer no puede conectarse a través del puerto 5938, tratará de conectarse utilizando el puerto 443 TCP.

No obstante, las aplicaciones móviles de Teamviewer para Android, iOS y Windows Mobile no utilizan el puerto 443, con lo que, si no se puede conectar a través de los puertos 5938 o 443, probará con el puerto 80 TCP. La velocidad de conexión a través de este puerto es más lenta y menos fiable que a través de los otros puertos debido a la sobrecarga adicional que utiliza. Además, la conexión no se restablece automáticamente en caso de desconexión temporal. Por este motivo, el puerto 80 solo se utiliza como último recurso.

Una de sus principales características de esta aplicación es la seguridad (sin necesidad de una red VPN). La transferencia de datos tiene lugar, exclusivamente, a través de canales de datos seguros. TeamViewer incluye una codificación extremo a extremo basada en RSA (4096 bits) y AES (256 bits). De acuerdo con las declaraciones del fabricante, en principio no son posibles ataques de intermediarios (Man-in-the-Middle). Esto se garantiza mediante el intercambio firmado de dos pares de claves.

Otras características destacables que hacen que Teamviewer sea de las más usadas del mercado son:

- Pantalla negra para mantener tu privacidad durante el acceso remoto.
- Acceso permanente para dispositivos sin supervisión.
- Grabación de las sesiones.
- Encender un ordenador apagado o en modo de suspensión utilizando la función Wake-on-LAN.
- Permite realizar impresiones a distancia.

Los usuarios privados que utilizan TeamViewer con fines no comerciales pueden hacer uso del software de forma gratuita. Para el uso comercial del software hay que pagar la cuota correspondiente.

Tras este breve análisis se puede deducir que es una herramienta de acceso remoto muy completa y segura que cumpliría los requisitos para su despliegue en el Departamento. Sólo presenta el inconveniente que, además de no ser gratuita, supone la dificultad en la gestión y administración de acceso a los 180 puestos de trabajo repartidos en los 6 laboratorios docentes.

1.8.3 Supremo

Supremo [13] es software de escritorio remoto diseñado como una solución todo en uno, siendo gratuito para un uso no profesional o no continuo.

Ilustración 1.23. Logotipo aplicación SupRemo

Los pasos para hacer uso de este programa son simples, no es necesario instalar, solo descargar el archivo y ejecutarlo. Tampoco es preciso configurar nada extra en el ordenador, ni en el router, ni en el firewall, para que el programa funcione (utiliza los puertos habitualmente abiertos, 80 y 443, para las conexiones).

En el momento de realizar la conexión se requiere que el equipo que será controlado ejecute el programa y genere el ID que lo identifica y la contraseña. Para acceder al equipo remoto solo se deben insertar estos datos en la interfaz de Supremo Remote Desktop que estará visible en el dispositivo que funcionará como controlador.

TeamViewer y AnyDesk son productos similares, pero cabe destacar que Supremo es más intuitivo y sencillo. Una opción que sobresale como una de las ventajas principales es poder acceder de manera remota a varios equipos desde un solo dispositivo. Otra opción interesante es que al controlar un equipo se tiene acceso total a todos sus recursos, archivos y carpetas (incluso, es posible la impresión remota).

La aplicación cuenta internamente con un chat que permite intercambiar mensajes entre las personas conectadas en los distintos equipos. La transferencia de archivo entre dispositivos también es posible y muy simple hacerlo; el usuario solo debe arrastrar y soltar la carpeta que se quiera copiar. Los contactos registrados en la aplicación se pueden compartir para mejorar el sentido de cooperación.

En cuanto a la seguridad, la contraseña aleatoria generada por la aplicación para acceder a un equipo puede personalizarse estableciendo una más compleja. Para garantizar la privacidad y seguridad de los datos de los usuarios, toda la información que se intercambia entre dispositivos es cifrada de extremo a extremo con el algoritmo AES 256-bits.

Otras opciones interesantes pueden ser las plataformas en las que está disponible el uso de la aplicación, entre ellas Windows, GNU/Linux, Android y MacOS. Los asiduos a tener su propio sello pueden personalizar el ejecutable y darle un aspecto más afín a su gusto. No se debe pasar por alto que se recopila información relacionada con las conexiones para mejorar el funcionamiento del programa.

Entre sus principales desventajas destaca que es gratuito sólo para uso no profesional (incluso después de que expire el período de prueba de 21 días, y las sesiones tendrán una duración limitada). Después del periodo de prueba, para fines comerciales, el software sólo puede utilizarse con un plan de suscripción de pago.

Podemos concluir que se trata de una aplicación ligera y fácil de usar, pero sólo gratuita para uso personal o no continuado, es decir, no es la solución ideal para su implantación en el Departamento de Informática.

1.8.4 AnyDesk

Al igual que las dos anteriores, con AnyDesk [14] puede conectarse fácilmente desde cualquier lugar a cualquier dispositivo, sin importar el sistema operativo que utilice, ya sea un profesional de TI o un usuario particular.

Ilustración 1.24. Logotipo aplicación AnyDesk

Su funcionamiento y configuración es muy similar al de Teamviewer, aunque con licencia freeware (gratuito para uso personal y ofrece un conjunto limitado de funciones y asistencia). AnyDesk, por ahora, ofrece un uso más enfocado en el usuario particular. Sin embargo, TeamViewer puede ser usado tanto por aquellos con poca experiencia, así como por profesionales de TI.

1.8.5 Chrome Remote Desktop

Creada por Google, el escritorio remoto de Chrome [15] es otra de las herramientas a tener en muy cuenta para controlar de forma remota un equipo siempre que tengamos instalado Chrome en él. Gracias a esta aplicación es posible

conectarnos a un ordenador desde cualquier lugar, ya sea desde otro ordenador o desde un móvil con la aplicación oficial (y controlar el PC desde Android o iOS) usando internet en una conexión segura.

Todo funciona mediante una cuenta de Google, así como un PIN personal como medida extra de seguridad cuando se trata de una conexión remota a nuestros propios equipos, y depende de un código de acceso cuando se conecta con el ordenador de otro usuario que caducará al final de la sesión de Asistencia remota. Igualmente, un código no utilizado caducará después de unos minutos si no se usa, lo que brinda mayor protección. Además, toda la sesión remota está encriptada con AES a través de una conexión SSL segura, por lo que tanto los datos como el ordenador estarán seguros.

El escritorio remoto de Chrome es una herramienta totalmente gratuita, que permite el acceso no sólo al navegador Chrome sino a todo el ordenador, y compatible con varios sistemas operativos, incluidos Windows, Mac, Linux y Chromebook.

Ilustración 1.25. Logotipo del Escritorio Remoto de Chrome

Hay dos formas de usar Chrome Remote Desktop: para compartir la pantalla de usuario a usuario (Asistencia remota) o para acceder a nuestro propio equipo desde otra máquina. En cualquiera de los 2 casos es necesario iniciar sesión con una cuenta de Google.

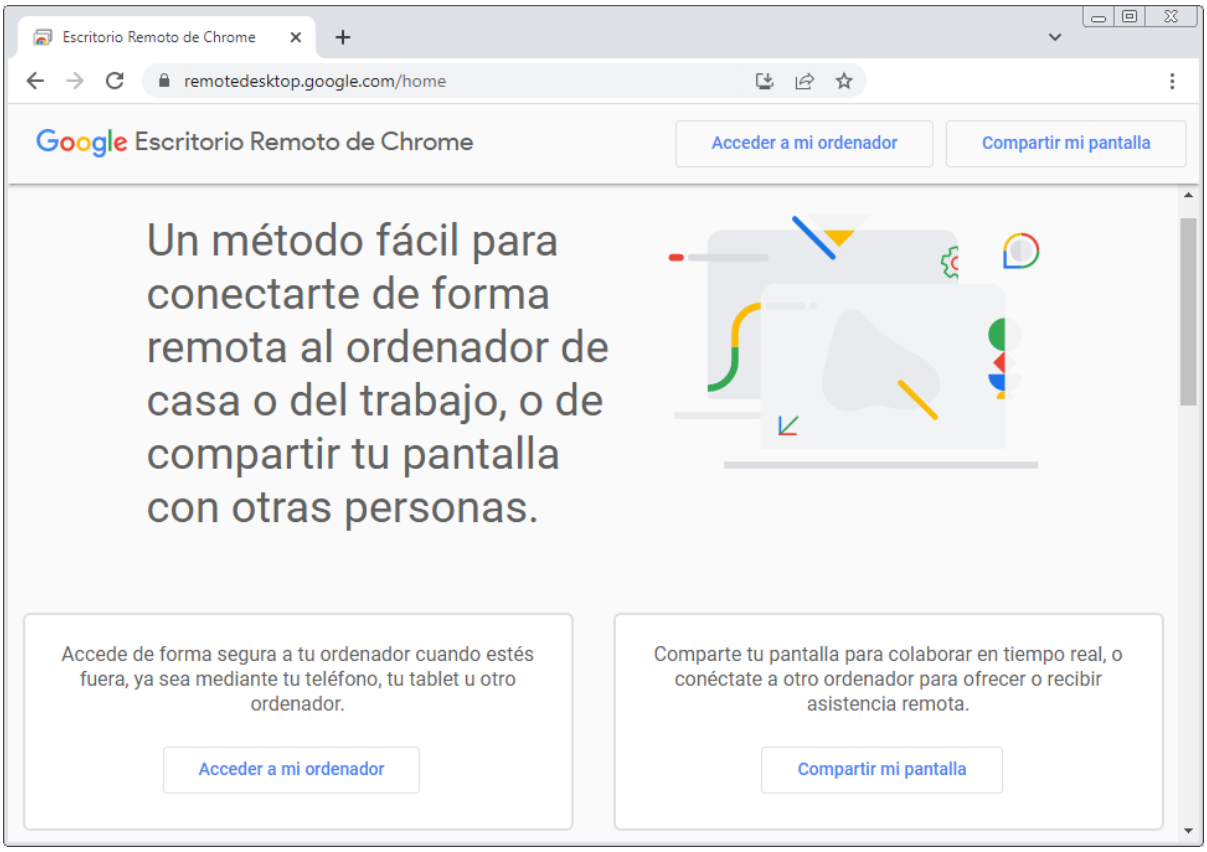

Ilustración 1.26. Página inicial del Escritorio Remoto de Chrome[3]

La primera de las utilidades de esta herramienta tiene la misma forma de funcionar que las aplicaciones anteriores.

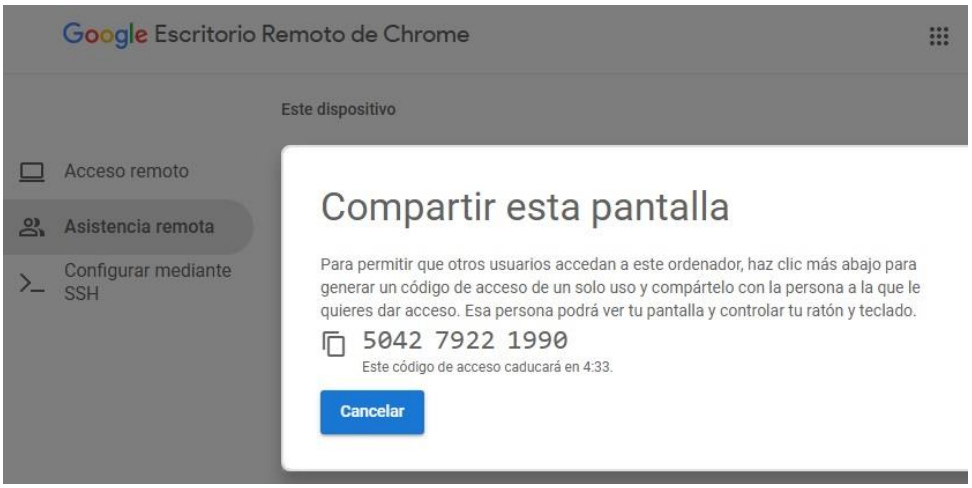

Ilustración 1.27. Logotipo del Escritorio Remote de Chrome

[3] https://remotedesktop.google.com/home

A partir de un código generado por el equipo que comparte, el ordenador que se conecta remotamente lo introduce, y en el primero se muestra un mensaje para que el usuario confirme, o no, la asistencia remota. En ese momento, el escritorio del ordenador compartido aparecerá en la pestaña del navegador Chrome del equipo que accede.

La segunda, y principal utilidad, es la que permite conectar con los equipos propios del usuario que están configurados en su cuenta de Gmail simplemente indicando el pin o contraseña establecidos.

Su instalación y configuración son muy sencillos, en uno y otro equipo de los extremos de la conexión remota. Para la conexión remota a otro ordenador para asistencia remota no es necesario instalar nada, simplemente entrar en la dirección url https://remotedesktop.google.com/support desde el navegador Chrome, iniciar sesión en una cuenta de Gmail e indicar el código generado por el equipo al que nos queremos conectar. Sin embargo, para poder compartir la pantalla del ordenador local o configurar el equipo para acceder a él de forma remota desde otro dispositivo, además de usar Chrome e iniciar sesión en una cuenta de Gmail hay que realizar estos pasos:

1. Añadir en el navegador la extensión “Chrome Remote Desktop” desde la “Chrome Web Store”.

2. Instalar el software de Escritorio Remoto de Chrome.

   Estos dos primeros pasos se realizan de forma automática al pulsar en el enlace “Descargar Escritorio Remoto de Chrome” y siguiendo las instrucciones que aparecen en pantalla para descargar e instalar. Cuando se pulse el botón, se abre una nueva página de Chrome que nos dirige a la extensión de Escritorio Remoto de Chrome. Dentro de esa página, pulsar en el botón Añadir a Chrome para instalar la extensión en el navegador. Aparecerá una ventana en la que se especifica que la extensión tendrá que acceder a casi todo en el ordenador, y habrá que aceptar las condiciones para proceder. Cuando vuelva a la ventana principal de Chrome donde se está realizando el proceso, el navegador también ha descargado un archivo ejecutable y necesario para que todo funcione. De hecho, Chrome ya lo ha detectado, y habrá que pulsar en el botón Aceptar e instalar de la página

para que proceda a instalar automáticamente el archivo sin que haya que hacer nada más.

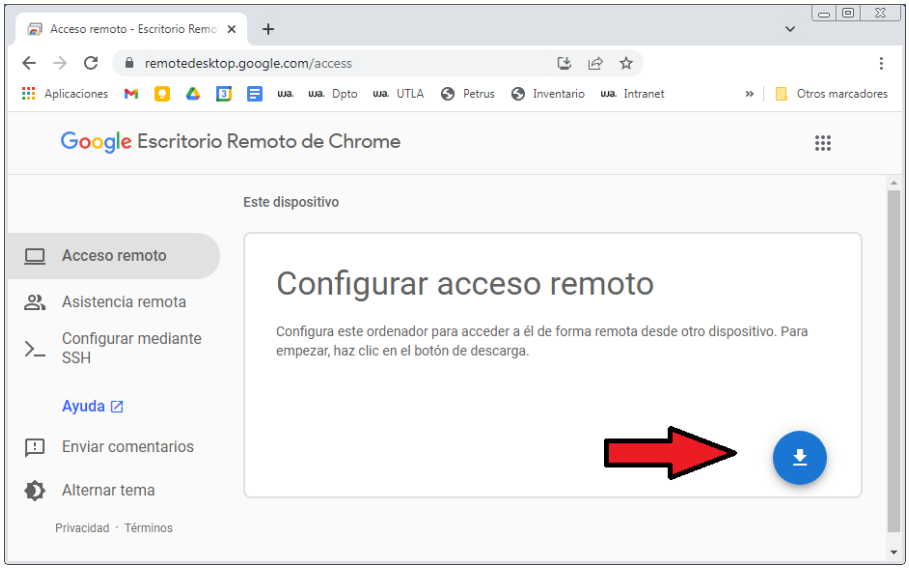

Ilustración 1.28. Instalación del Escritorio Remote de Chrome

3. Introducir un nombre para identificar al ordenador donde se está realizando la instalación.
4. Indicar un pin o contraseña de al menos 6 dígitos.

Utilizando la misma cuenta Gmail, este proceso se podrá repetir en cada ordenador al que se quiere acceder de forma remota. Esto creará, en dicha cuenta, una colección con todos los dispositivos remotos configurados para su acceso.

Además de las ventajas ya comentadas también se puede destacar las siguientes:

- Es gratuito tanto para uso personal como comercial (aunque las funciones pueden ser limitadas para fines empresariales).
- Acceso al host sin necesidad de ejecutar Chrome o de que el usuario inicie sesión en su cuenta.
- Opción de transferencia de archivos disponible.
- Posibilidad de incrementar la seguridad realizado la conexión remota a través de SSH. Para realizar esta configuración sólo habría que ejecutar en una terminal el comando que propone la propia aplicación del Escritorio Remoto de Chrome (tanto para Windows como para Linux).

- Podemos acceder a nuestros equipos sin conocer la dirección IP, al estar ya configurados y accesibles desde la aplicación, indicando sólo el pin o contraseña.
- Utiliza el puerto 443 (https) con lo que no es necesario realizar configuración alguna en los posibles firewalls a atravesar en la conexión remota.

Como inconvenientes, indicar que por ahora no contempla las opciones de chat ni de impresión remota.

Tras este breve análisis, indicar que se trata de una herramienta ideal de escritorio remoto si se trata de conexiones remotas a ordenadores personales o asistencia técnica puntual, pero no está diseñada para administrar un número grande de equipos como es el caso de los laboratorios de prácticas referidos en este trabajo.

1.8.6 Apple Remote Desktop

Al igual que Microsoft, Apple también tiene su propio sistema de acceso remoto desde hace años, el Apple Remote Desktop [16]. Aunque es una opción nativa de macOS tienes que comprarla a parte para desbloquearla.

Es una poderosa herramienta que le permite gestionar y administrar de forma remota otras Mac simultáneamente. La idea no es tanto la de permitirte acceder a tu ordenador de cualquier sitio como la de poder crear, administrar y controlar una red de ordenadores de la compañía de Apple.

Ilustración 1.29. Logotipo del Apple Remote Desktop

Los administradores de una red de muchos equipos Mac pueden encontrar que su gestión es una tarea increíblemente costosa en tiempo y dinero si se hace unidad a unidad. Apple Remote Desktop es la aplicación de gestión remota que incluye toda una suite de herramientas que te permite, sin moverte de tu sitio, acceder al escritorio de cada Mac de una red, solucionar problemas, reiniciarlo o apagarlo, enviar

comandos, generar informes, realizar instalaciones de software o configurar su comportamiento. Incluye características que te permiten automatizar tareas frecuentes. También hay plantillas de tareas que puedes reutilizar.

Su diseño, además de no ser gratuita, no encaja como solución a aplicar para el acceso a los escritorios remotos de cualquier sistema operativo instalado en los PC de prácticas.

1.8.7 RealVNC (o VNC Connect)

RealVNC, ahora conocida como VNC Connect [17], es una de las herramientas de control remoto de ordenadores más utilizadas, junto a TeamViewer y Microsoft Remote Desktop. Esta herramienta multiplataforma utiliza la tecnología de VNC, basada en el concepto de cliente-servidor, para conectarnos de forma remota a nuestro ordenador a través de Internet y tener control completo sobre él.

Ilustración 1.30. Logotipo de RealVNC

Consta de una aplicación VNC Server para el equipo que desea controlar y los programas de apoyo, y un cliente VNC Viewer para ejercer el control desde cualquier plataforma.

Nos permite unirnos a la nube de la compañía de manera que podamos conectarnos a los ordenadores de nuestra red directamente a través de ella en lugar de tener que introducir nuestra dirección IP, de forma muy similar a como permite su rival TeamViewer. Además, gracias a la nube, va a ser posible guardar una lista con los ordenadores a los que nos solamos conectar en la libreta de direcciones de VNC, la cual se mantendrá siempre sincronizada tanto con la nube como con el resto de equipos con VNC Connect que tengamos iniciados con nuestra cuenta de usuario.

RealVNC utiliza por defecto el puerto TCP 5900 para realizar la conexión del escritorio remoto. Además, utiliza el protocolo RFB (Remote Frame Buffer) el cual, debido a su simplicidad y diseño, es aplicable a todos los sistemas de ventanas y aplicaciones.

Se trata de una aplicación que cubre todas las necesidades de acceso remoto, pero presenta tres inconvenientes que no la hacen idónea para el acceso a los

escritorios remotos de los equipos de los laboratorios de prácticas del Departamento de Informática:

- Al estar basado en el protocolo RFB, tiene un rendimiento más bajo que las herramientas anteriores que presentan una mejor comprensión del diseño gráfico subyacente. RFB solo envía los datos de píxel sin procesar, mientras que otros protocolos envían primitivas gráficas o comandos de alto nivel en una forma más simple (es decir, 'abrir ventana' por ejemplo). Esto se traduce también en un mayor ancho de banda necesario para soportar un alto número de conexiones remotas simultáneas, como es el caso.
- Apertura de puertos (uno por cada uno de los equipos) en los dispositivos del perímetro de seguridad, así como configurar el reenvío de dichos puertos para reenviar el puerto TCP 5900 (o el puerto personalizado correspondiente) a la dirección del equipo local si está oculto tras el enrutador NAT. Como alternativa, puede tunelar VNC mediante SSH, evitando la apertura de puertos adicionales y atravesando así automáticamente el enrutador NAT. SSH también proporciona cifrado adicional en la conexión entre el servidor y el cliente VNC.
- Es de pago, con diferentes precios según las necesidades. Sólo cuenta con una prueba gratuita de 30 días.

1.8.7.1 Otras aplicaciones basadas en VNC

- UltraVNC (también llamado uVNC) [18] es otro es un software libre de escritorio remoto bajo Microsoft Windows basado en VNC.

  Tiene un gran parecido a la versión libre de RealVNC, sin embargo, además de control remoto, el programa añade varias características, como un plugin de cifrado para hacer más segura la conexión cliente/servidor. También soporta la transferencia de archivos, el chat de texto y varios métodos de autentificación. El software es gratuito y se distribuye bajo los términos de la Licencia Pública General GNU.

  Por los mismos motivos que el anterior, además de otros, no es la herramienta que encaja en el Departamento de Informática para el acceso remoto a sus laboratorios.

- TightVNC [19] es una aplicación más de código abierto para administración remota multiplataforma que utiliza protocolo RFB de VNC para compartir tanto pantallas como archivos en remoto. Como característica diferenciadora presenta una 'codificación apretada' (tight encoding), que es una combinación de compresión JPEG y otros tipos de codificación, que mejora el rendimiento en las conexiones de bajo ancho de banda.

  De esta aplicación derivan otras como:

  - RemoteVNC, bifurcación del proyecto TightVNC incorporando atravesado automático de NAT y cortafuegos.
  - TurboVNC, basado en el código de esta aplicación incluye mejoras de rendimiento y características dirigidas a trabajos de dibujo y de vídeo 3D.
  - TigerVNC, otra bifurcación de TightVNC preocupada especialmente del desempeño y la función de mostrar pantalla (escritorio) remotamente.

1.8.8 NoMachine

NoMachine [20] es otra alternativa más para la administración remota que no utiliza un servidor de terceros lo cual le permite configurar su propia máquina de escritorio remoto para realizar la función de servidor, usando su propio ordenador y utilizando el rápido y eficiente protocolo de vídeo NX.

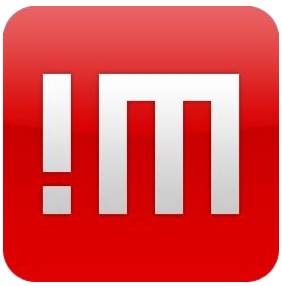

Ilustración 1.31. Logotipo de NoMachine

Como su nombre en inglés indica, “NoMachine” (ninguna máquina) significa que no hay servidores ni dispositivos entre tu ordenador y el ordenador al que quieres conectarte. La aplicación utiliza la tecnología más reciente que le permite compartir su

escritorio con la máxima calidad permitiendo trabajar con cualquier contenido (por ejemplo, retransmisión audio y vídeo) y, además, sin ninguna infraestructura.

Este programa brinda compatibilidad con dos protocolos: Uno es el clásico SSH, mientras que el otro es conocido como “NX” [21], una tecnología propietaria que ayuda a simplificar el proceso de autenticación, conservando un buen equilibrio entre seguridad y rendimiento.

Usar a NoMachine es muy sencillo. Hay un único fichero de instalación que proporciona todo lo necesario para dar acceso al propio ordenador de forma remota (actúa como un servidor), y también para poder conectarlo a otros ordenadores con NoMachine instalado (actúa como un cliente).

La instalación coloca un monitor (o servicio) en el sistema y, por otro lado, la interfaz principal para administrar todas las conexiones remotas a los distintos equipos. Esta interfaz detecta automáticamente a cualquier ordenador en la red LAN que esté listo para recibir una conexión, sólo hay que añadir las conexiones que se realicen a través de Internet.

Bajo una configuración estándar, NoMachine utiliza como nombre de usuario y contraseña en cada conexión las mismas credenciales que se encuentran activas en el ordenador remoto.

En cuanto a la seguridad, a parte de la comunicación segura protegida por criptografía SSL, en el servidor se puede habilitar el permiso de conexión o dejar el servidor abierto para que se conecte cualquiera. Además, es posible habilitar el permiso requerido para que el usuario remoto pueda interactuar con el escritorio remoto. Lo que significa que el usuario se conectará al servidor en modo de sólo vista por defecto. Hay algunas características de seguridad más, como que el programa dejará en blanco la pantalla física una vez que el cliente se haya conectado para que el usuario local no pueda utilizar el ordenador, o puede bloquear automáticamente el ordenador después de que el cliente se haya desconectado.

NoMachine es gratuito bajo uso personal, compatible con todos los sistemas operativos principales (Windows, Linux, OS X, Android, iOS y Raspberry Pi), y cuenta con múltiples opciones en licencias empresariales.

En cualquier caso, se trata de una magnifica herramienta de conexión remota, pero presenta, al igual que el Escritorio Remoto de Windows, un gran inconveniente para su instalación en los laboratorios de prácticas: no utiliza un puerto estándar para la conexión como son el 80 (http) y el 443 (https). Esto significa que las direcciones IP

internas de los equipos y los puertos no son accesibles desde el exterior sin la modificación de los cortafuegos de la Universidad de Jaén y el reenvío de puertos necesario en los enrutadores. Este es uno de los requisitos fundamentales en la elección de la herramienta de conexión remota del alumnado para sus diferentes usos en línea.

1.8.9 Otras aplicaciones del mercado

En los puntos anteriores se han presentado un conjunto de aplicaciones con diferentes tecnologías que son las más relevantes y usadas por los usuarios en la administración remota, pero el listado es mucho más amplio (algunas incluso muy famosas): LogMeIn, Splashtop, ShowMyPC, Zoho Assist, GoToMyPC, Iperius Remote, AeroAdmin, Ammyy Admine, etc. Todas ellas presentan un denominador común: no tienen una versión gratuita (o libre) que no tenga limitaciones (al menos para uso personal). Por esta razón, no son aplicaciones candidatas para su uso en el Departamento y, por tanto, tampoco son objeto de análisis de este estudio técnico.

En cualquier caso, el software de escritorio remoto gratuito nunca tendrá todas las funcionalidades que tiene una versión de pago. Puede estar limitado en cuanto a cuántos ordenadores puedes conectar, la interfaz, si necesitas que se instale en el host o no, cuánto tiempo tienes para la sesión remota, si puedes transferir archivos o puedes hablar con el agente por chat, etc. Es posible consultar una tabla comparativa con la gran mayoría de las aplicaciones mencionadas en la siguiente dirección url: https://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software.

El objetivo de este trabajo es encontrar la solución de escritorio remoto que, a la fecha de entrega del mismo, mejor encaje con los requerimientos del Departamento de Informática, con la mayor cobertura de funcionalidades y el menor coste posibles.

1.9 Descripción de la solución propuesta: Apache Guacamole

Como hemos visto anteriormente, existe una gran variedad de aplicaciones que permiten una conexión a un escritorio remoto, pero ninguna que cumpla con todos los requisitos mínimos iniciales para evaluar su implantación como herramienta de escritorio remoto instalada en los ordenadores de los laboratorios docentes del Departamento de Informática. Estos requisitos son los que deben asegurar una buena

experiencia de usuario, tanto al alumnado como a los profesores y administradores, en modelos de docencia on-line, en conexiones contraladas si hay disponibilidad del laboratorio o fuera del horario laboral:

- Acceso seguro.
- Facilidad de uso y configuración.
- Control y administración de múltiples conexiones remotas necesarias para todos los puestos de trabajo.
- Buen rendimiento.

Junto a las anteriores, también son características importantes a tener en cuenta las siguientes:

- Aplicación multiplataforma, que permita su funcionamiento en cualquier sistema o dispositivo.
- Software libre, que tenga la posibilidad personalizar o añadir cualquier funcionalidad, razones económicas a parte.

Una herramienta de administración remota que cumple con todos estos requerimientos es Apache Guacamole [22]. En su página web se define como una puerta de enlace de escritorio remoto sin cliente (llamado así porque no se requieren complementos ni software de cliente).

Ilustración 1.32. Logotipo de Apache Guacamole

Una vez que Apache Guacamole, a partir de ahora Guacamole, está instalado en un servidor, todo lo que los usuarios necesitan para acceder a sus escritorios es un navegador web que soporte HTML5 y JavaScript. Además, estos escritorios remotos a los que se accede a través de Guacamole no necesitan existir físicamente. Con Guacamole y un sistema operativo de escritorio alojado en la nube, se puede

combinar la conveniencia de esta herramienta con la flexibilidad de la computación en la nube.

Guacamole se trata de una aplicación web HTML5 que se encarga de realizar la conexión dentro de una red doméstica o de una organización por RDP, SSH, Telnet, VNC o Kubernetes, y servir esa conexión al exterior vía WEB (evitando el clásico esquema de conexión donde cada usuario tiene un acceso por VPN a la red por ejemplo de la organización y a su vez acceso a las máquinas X que le correspondan) para ofrecernos un acceso remoto centralizado bajo unas únicas credenciales para acceder a nuestros equipos.

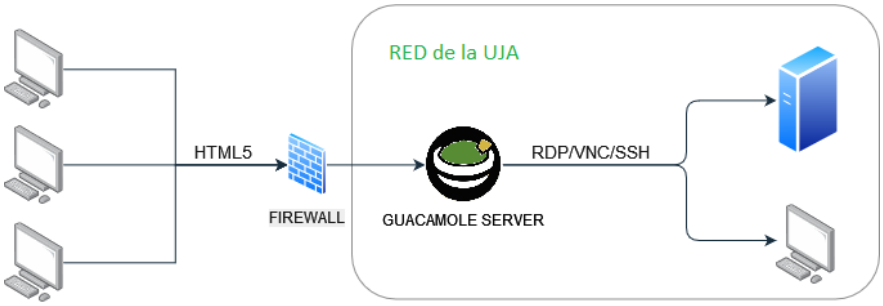

Ilustración 1.33. Esquema de Apache Guacamole

Esta arquitectura hace que podamos controlar de forma detallada quién se conecta a qué servicio sin tener que crear complejas reglas en el firewall ya que no se exponen puertos críticos directamente de los equipos de la organización, en principio para RDP -Remote Desktop Protocol- (3389), SSH -Secure SHell- (22), VNC -Virtual Network Computer- (5901) y Telnet (23). Al utilizar un navegador para la conexión al escritorio remoto, sólo serán necesarios tener abiertos los puertos HTTP (80) y HTTPS (443) en la configuración de los firewalls de la organización, en nuestro caso, la Universidad de Jaén.

Su gestión de usuarios centralizada, nos permite resolver y monitorizar los accesos particulares de cada uno y registrar sus operaciones manteniendo un fichero de registro. Además, como medidas de seguridad extra esta herramienta cuenta con la posibilidad de implementar:

- Acceso con doble factor.
- Permisos de acceso con horarios.
- Caducidad de los permisos.

- Grabación de las sesiones.
- sFTP para los accesos SSH (poder subir y bajar ficheros sin necesidad de otra conexión).
- Límites de conexiones concurrentes a máquinas.
- Wake-on-LAN (encender los equipos al levantar la sesión).
- Posibilidad de conectar con servicios de identificación de usuarios (en nuestro caso con SIDUJA, servicio de identidad de la Universidad de Jaén) a los usuarios y grupos de usuarios creados en Guacamole
- Posibilidad de balanceo de carga de usuarios entre grupos de máquinas.

Otras funcionalidades que presenta Apache Guacamole pueden ser la posibilidad de compartir la sesión con otras personas que no disponen de cuenta en el sistema, por ejemplo, para situaciones de docencia online, o similares.

Sus características permiten incluso que puedan ofrecerse funcionalidad para copiar y pegar de forma remota, transferir ficheros, emplear el audio remoto, impresión remota y/o local, etc. O bien, puede darse el caso en entornos más restrictivos para evitar filtraciones de información y donde no se desee que estas funcionalidades sean empleadas y se eliminen, evitando de esta forma tener que realizar operaciones directamente sobre los equipos remotos.

Sigue la filosofía de desarrollo del código abierto y es software libre. Ya que utiliza una licencia Apache en su versión 2.0, además de contar una gran comunidad de desarrolladores detrás.

Utiliza un conjunto de API que están ampliamente documentadas, incluyendo tutoriales básicos y descripciones conceptuales en su manual en línea. Es posible utilizar extensiones de terceros, por ejemplo, para modificar el portal de login con nuestro logo, o podemos crear nuestras propias extensiones si hay algo que no nos encaja.

En conclusión, es la herramienta que por sus características más se ajusta al entorno del Departamento de Informática y a las necesidades a resolver, además de tener la posibilidad de ampliar y personalizar su funcionalidad.

1.10 Material y métodos

Los medios de los que se ha dispuesto para este trabajo fin de grado han sido los descritos a continuación:

1. Fuentes bibliográficas y de documentación para la realización de esta memoria:
    - La biblioteca de la UJA, sobre todo sus libros electrónicos accesibles de forma on-line accediendo con la cuenta TIC de la Universidad.
    - Servicio de informática, que facilita también información genérica referente a la seguridad de la red informática de la Universidad de Jaén (RIUJA).
    - Internet, que ha sido la gran fuente de información para poder describir y evaluar las diferentes alternativas de herramientas de administración remota existentes en la actualidad.
2. Servidor del Departamento de Informática para la instalación de una de las soluciones:
    - Servidor HP modelo Proliant DL360p Gen8 ubicado en la sala de servidores del Departamento (A3-185).
    - Certificado SSL para el servidor web montado (lamella.ujaen.es) solicitado al Servicio de Informática.
    - Configuración por parte de Servicio de Informática en los conmutadores correspondientes para poder hacer bonding con la finalidad de tener un mayor ancho de banda en el equipo servidor.
3. Laboratorios docentes del Departamento de Informática:
    - Disponibilidad en el acceso a todos ellos para la realización de pruebas de conexión, configuración de los sistemas operativos, pruebas de carga, etc.
    - Configuración y activación de los servicios necesarios para habilitar las conexiones remotas por los diferentes protocolos de los sistemas operativos montados en los equipos de los laboratorios.

Así mismo, la metodología usada en el desarrollo de este estudio técnico se resume en estos puntos:

- Estudio bibliográfico de las soluciones existentes en la actualidad, previo desarrollo del estado del arte y sus antecedentes.
- Análisis de las características, ventajas e inconvenientes de las distintas herramientas seleccionadas.
- Instalación de la herramienta que cumpla mejor los requerimientos, una vez terminado el análisis.
- Evaluación del software seleccionado.
- Redacción de la memoria de resultados.

1.11 Tecnologías utilizadas

Guacamole no es una aplicación web independiente y se compone de muchas partes. La aplicación web en realidad está destinada a ser simple y mínima, con la mayoría del trabajo pesado realizado por componentes de nivel inferior.

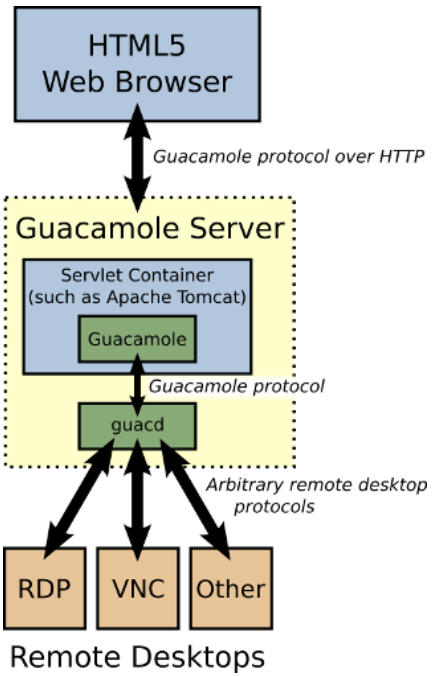

Ilustración 1.34. Arquitectura de Apache Guacamole[4]

[4] Apache Guacamole: implementación y arquitectura
https://guacamole.apache.org/doc/gug/guacamole-architecture.html

Se trata de una aplicación cliente/servidor. El servidor contiene todos los componentes nativos del lado del servidor requeridos por Guacamole para conectarse a escritorios remotos y el cliente que contiene todos los componentes Java y JavaScript de Guacamole. Estos componentes conforman la aplicación web que servirá al cliente HTML5 Guacamole a los usuarios que se conectan a su servidor.

En un entorno de alta disponibilidad, podremos separar dichos componentes en diferentes servidores para balancear las cargas de trabajo.

Los usuarios se conectan a un servidor de Guacamole con su navegador web. El cliente Guacamole, escrito en JavaScript, se sirve a los usuarios por un servidor web dentro del servidor Guacamole. Una vez cargado, este cliente se vuelve a conectar al servidor a través de HTTP utilizando el protocolo Guacamole.

La aplicación web implementada en el servidor de Guacamole lee el protocolo de Guacamole y lo reenvía a guacd, el proxy nativo de Guacamole. Este proxy, en realidad, interpreta el contenido del protocolo Guacamole, y se conecta a los servidores de escritorio remotos en nombre de los usuarios.

1.11.1 Protocolo de Guacamole

La aplicación web no interpreta ningún protocolo de escritorio remoto. No contiene soporte para VNC o RDP, o cualquier otro protocolo configurable en Guacamole. En realidad, solo comprende el protocolo Guacamole, que es un protocolo para la visualización remota y el transporte de eventos. Si bien un protocolo con esas propiedades naturalmente tendría las mismas capacidades que un protocolo de escritorio remoto, los principios de diseño detrás de un protocolo de escritorio remoto y el protocolo Guacamole son diferentes: el protocolo Guacamole no está diseñado para implementar las funciones de un entorno de escritorio específico.

Como protocolo de interacción y visualización remota, Guacamole implementa un amplio conjunto de protocolos de escritorio remoto existentes. Agregar soporte para un protocolo de escritorio remoto particular (como RDP) a Guacamole implica escribir una capa intermedia que "traduce" entre el protocolo de escritorio remoto y el protocolo Guacamole. La capa intermedia que maneja esta traducción es guacd.

1.11.2 Guacd

Es el corazón de Guacamole que carga dinámicamente el soporte para los protocolos de escritorio remoto (llamados "complementos de cliente") y los conecta a los escritorios remotos según las instrucciones recibidas de la aplicación web.

Guacd es un proceso demonio que se instala junto con Guacamole y se ejecuta en segundo plano, escuchando conexiones TCP desde la aplicación web. Guacd tampoco comprende ningún protocolo de escritorio remoto específico, sino que implementa sólo lo suficiente del protocolo Guacamole para determinar qué soporte de protocolo se debe cargar y qué argumentos se le deben pasar. Una vez que se carga un complemento de cliente, se ejecuta independientemente de guacd y tiene control total de la comunicación entre él y la aplicación web hasta que finaliza el complemento de cliente.

1.11.3 Aplicación Web

La aplicación web, implementada en Java, es la parte de Guacamole con la que un usuario realmente interactúa.

Como se mencionó anteriormente, no implementa ningún protocolo de escritorio remoto. Se basa en guacd e implementa nada más que una interfaz web elegante y una capa de autenticación.

1.12 Riesgos de este tipo de herramientas

Como no puede ser de otra manera, el principal riesgo que afecta a la instalación de un software de administración remota en una organización es el acceso no permitido a sus escritorios remotos, en este caso concreto, al de los equipos de los laboratorios de prácticas del Departamento de Informática y, en definitiva, el acceso a la red corporativa y recursos de la Universidad de Jaén.

Para evitar este riesgo, Apache Guacamole posibilita de una serie de medidas que dificultan cualquier ataque indeseado, además de no exponer puertos críticos directamente de los equipos a los que queremos conectar:

- Uso de certificado SSL en la aplicación web que encripte todo el tráfico entre el navegador del usuario y servidor web de Apache Guacamole, y que certifique la autenticidad del dominio web.

- Empleo de una VPN tanto para las conexiones seguras de los clientes remotos con Guacamole y de los equipos de la organización.
- Limitación del acceso según horario.
- Doble factor de autenticación de usuarios.
- Contraseñas robustas y temporales.

Otro posible riesgo, aunque no de seguridad, puede ser el que la herramienta elegida para los accesos remotos no ofrezca una experiencia de usuario suficiente que permita convertirlo en un servicio más ofrecido por el Departamento.

1.13 Organización y gestión

La idea de este TFG surge de una necesidad clara e impuesta por la situación sobrevenida provocada por el COVID-19. La imposibilidad de acceder al entorno habitual de trabajo y, sobre todo, en el caso de la realización de las prácticas de las asignaturas, aceleró el cambio del modelo de docencia presencial hacia un nuevo modelo on-line.

A partir de esta situación se inicia el estudio de las distintas posibilidades de acceso remoto a los laboratorios de prácticas que mejor se adaptara a las necesidades del Departamento de Informática y a su alumnado. En esa búsqueda precipitada, y de un comentario surgido en una reunión telemática, aparece Apache Guacamole como posible solución.

En ese momento, y viendo la tecnología web que usa este software, empiezan los contactos con la Dirección del Departamento (y su Comisión de Asuntos Económicos e Infraestructuras) para la cesión de uno de sus servidores para la implantación y evaluación de Guacamole.

Igualmente, al tratarse de un sitio web, se requiere cumplir una serie de medidas para garantizar la accesibilidad web, protección de datos y unas condiciones mínimas de seguridad (definidos en el Protocolo del Servicio Web de la Universidad de Jaén [23]). Por ello, también se contacta con el Servicio de Informática para que proporcionara un certificado SSL para el nuevo servicio web con el objetivo de autenticar la identidad del sitio web y habilitar una conexión cifrada que aumente la seguridad en la transmisión de información.

Destacar la total predisposición de todas las partes para realizar el desarrollo de este estudio, y comprobar si este software realmente puede ayudar a los alumnos en situaciones específicas de imposibilidad en el acceso a los laboratorios, o incluso para potenciar su uso en horarios especiales.

1.14 Estimación del tamaño y esfuerzo

Ya que el presente proyecto es un TFG, no existen restricciones de tipo económico, sino de tipo temporal (un número aproximado de horas). Por consiguiente, los cálculos de tamaño del proyecto están supeditados el tiempo disponible. En cuanto al esfuerzo, se dispone de tan un solo efectivo (la persona autora del trabajo).

1.15 Planificación temporal

Para enfocar mejor este trabajo fin de grado, la planificación temporal parte de la identificación inicial de las diferentes tareas y subtareas a abordar para la consecución de los objetivos de éste:

1. Revisión bibliográfica: búsqueda de la información necesaria para documentar el concepto y la evolución de las conexiones remotas, el entorno y condiciones de trabajo donde realizan sus prácticas los alumnos y las características de cada aplicación de escritorio remoto.
2. Análisis de las alternativas del mercado: estudio de una selección de aplicaciones de escritorio remoto, que usen las distintas tecnologías, para analizar sus características y viabilidad.
3. Instalación de la herramienta seleccionada.
    - Apache Guacamole: preparación del equipo servidor, montaje de todos los componentes e instalación. Configuración de Guacamole: usuarios, grupos de usuarios y conexiones RDP, VNC, SSH
    - Configuración de ordenadores de los laboratorios docentes: habilitar la conexión remota en cada sistema operativo montado en los ordenadores
        - Windows 10: escritorio remoto (RDP).
        - Ubuntu 20.04: compartir pantalla (VNC).

- MacOS: compartir pantalla (VNC).

4. Evaluación de la herramienta. Pruebas de carga.
5. Elaboración de la documentación.
    - Objetivos y Estado del arte.
    - Entorno actual de trabajo y seguridad.
    - Estudio de las alternativas de mercado.
    - Apache Guacamole.
        - Instalación.
        - Manual de la aplicación.
    - Resto de documentación: introducción, apéndices, glosario de términos, etc.

En la siguiente imagen se muestra la división del plan de trabajo en tareas y, según el caso, sus correspondientes subtareas.

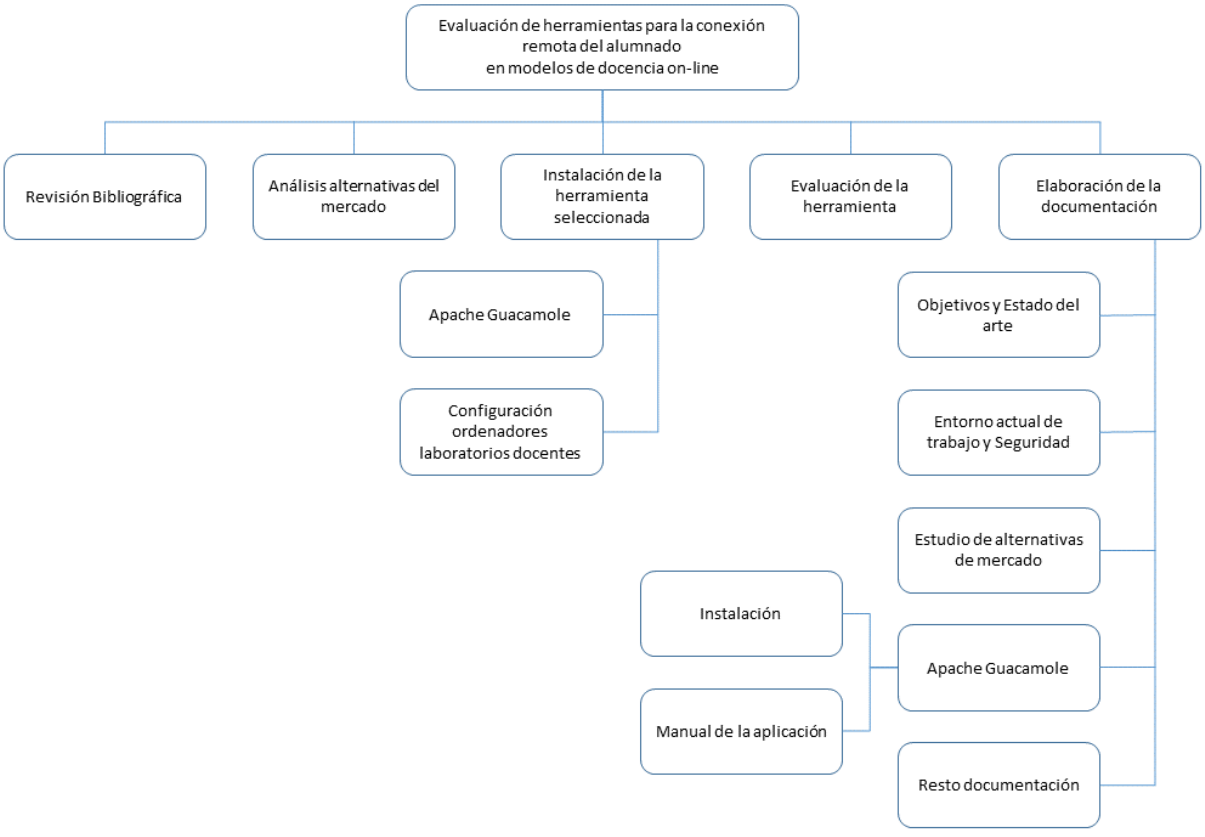

Ilustración 1.35. Estructura del plan de trabajo

En la siguiente tabla se asigna el esfuerzo a cada una de las tareas y subtareas anteriores.

Tarea	Duración en días
Revisión bibliográfica	**25**
Análisis de las alternativas del mercado	**30**
Instalación de la herramienta seleccionada	**35**
Apache Guacamole	30
Configuración de ordenadores de los laboratorios docentes	5
Evaluación de la herramienta	**10**
Elaboración de la documentación	**40**
Objetivos y Estado del arte	5
Entorno actual de trabajo y seguridad	5
Estudio de las alternativas de mercado	10
Apache Guacamole	
Instalación	5
Manual de la aplicación	5
Resto de documentación	10
Total	**140 días**

Tabla 1.4. Listado de tareas planificadas

Por último, se muestra el Diagrama de Gantt para reflejar esta planificación temporal del proyecto con comienzo el día 10 de enero y finalización el día 30 de mayo de 2022, que suman un total de 140 días (con una dedicación prevista de 3 horas diarias). Este diagrama es una forma fácil y rápida de tener una vista general de la dedicación prevista para las tareas programadas, además, nos permite realizar un seguimiento del progreso de cada uno de los hitos del proyecto.

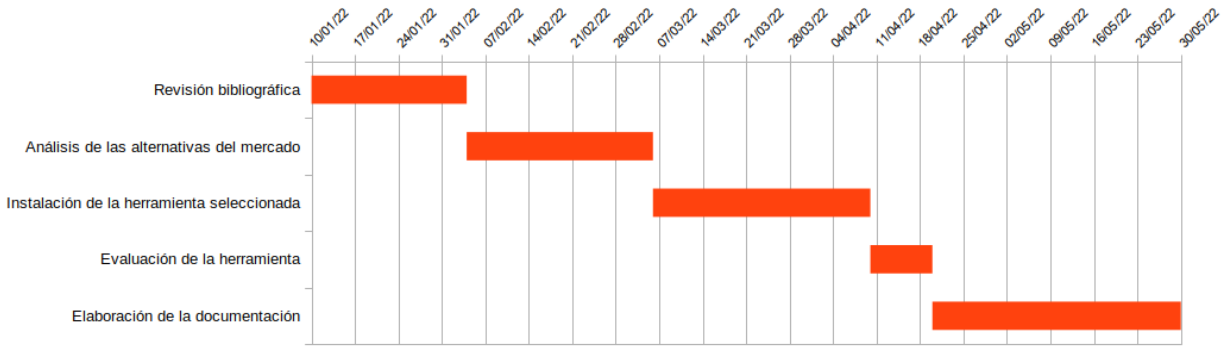

Ilustración 1.36. Diagrama de Gantt

1.16 Presupuesto

Realizar un estudio sobre el presupuesto necesario para poder llevar a cabo cualquier proyecto es un paso obligatorio antes de abordarlo, ya que si el coste total estimado es muy alto puede suponer la cancelación del mismo.

En el presupuesto que podemos observar en la siguiente tabla se valoran económicamente los costes que se necesitan para llevar a cabo este estudio técnico y la implantación de su resultado. En él se incluyen tanto los costes de análisis e investigación y elaboración de la memoria como los costes de hardware, despliegue de la herramienta de escritorio remoto y su configuración. No hay costes añadidos de licencias de software ya que todo el software usado para implementar la conexión remota centralizada a los equipos de los laboratorios es libre (y gratuito).

Concepto	Coste
Hardware (servidor Proliant DL360p Gen8) **[24]**	1.445,56€
Software	0,00€
Estudio y despliegue (420 horas a 12,08€/hora **[25]**)	5.073,60€
Costes indirectos (10%)	651,92€
Coste bruto	**7.171,08€**
IVA (21%)	**1.505,93€**
Coste total	**8.677,01€**

Tabla 1.5. Análisis de costes

En el caso de tratarse de una empresa u organización con ánimo de lucro habría que incrementar un 50% sobre el coste total (3.585,54€) como beneficio con lo que la cantidad final del proyecto ascendería a 10.756,62€ (IVA no incluido).

Igualmente, para el mantenimiento y actualización de la aplicación, una vez desplegada, se puede añadir al presupuesto un concepto opcional por un importe de 200€ por mes (IVA no incluido), correspondiente a 5 horas de trabajo semanales, para realizar estos trabajos de mantenimiento.

2 DESCRIPCIÓN DE LOS TRABAJOS

Es, en este punto, donde se desarrollan todos los pasos a seguir para el montaje y configuración de Apache Guacamole en su última versión (v1.4.0 en la fecha de entrega de este TFG), y sus ajustes para adaptarla como herramienta de conexión remota en los laboratorios docentes del Departamento de Informática.

2.1 Instalación y configuración de la aplicación web

El primer paso es la preparación del equipo donde se va a desplegar Apache Guacamole. Para ello, contamos con el siguiente servidor en formato rack (1U) de la marca HP (modelo Proliant DL360p Gen8), ubicado en la sala de servidores del Departamento, y con estas características:

- Procesador Intel Xeon E5-2620v2 2.10Ghz (16 núcleos).
- 32Gb de memoria RAM.
- 4 discos duros de 1Tb configurados en 2 discos virtuales RAID 0 (de 1,8Tb).
- 6 interfaces de red (1Gbps).

Ilustración 2.1. Servidor lamella.ujaen.es del Departamento de Informática

Como sistema operativo se utilizará Ubuntu Server 20.04 LTS que es una de las distribuciones de Linux más usada en servidores Linux con un gran rendimiento para servidores. Se trata de un Sistema Operativo sin entorno gráfico (aunque podemos instalarlo) lo que quiere decir que todas las acciones se realizan mediante consola. Esta versión LTS (Long Term Support, o soporte a largo plazo) de Ubuntu

Server tiene soporte completo de actualizaciones de seguridad y mantenimiento hasta el año 2025 y, además, soporte adicional de tres años para actualizaciones de seguridad.

El servidor se formatea en el proceso de instalación del sistema operativo desde un Live USB con la imagen ISO de Ubuntu Server 20.04 LTS descargada desde la web oficial [26]. Sólo se utiliza uno de los 2 discos virtuales y Ubuntu Server se monta sobre LVM en una partición de 1Tb de capacidad (quedando libres sin asignar unos 800Gb y otro disco de 1'8Tb). Esto nos permitirá, entre otras cosas, poder ampliar en un futuro la capacidad de la partición del sistema (punto de montaje /, en nuestro caso /dev/sda3).

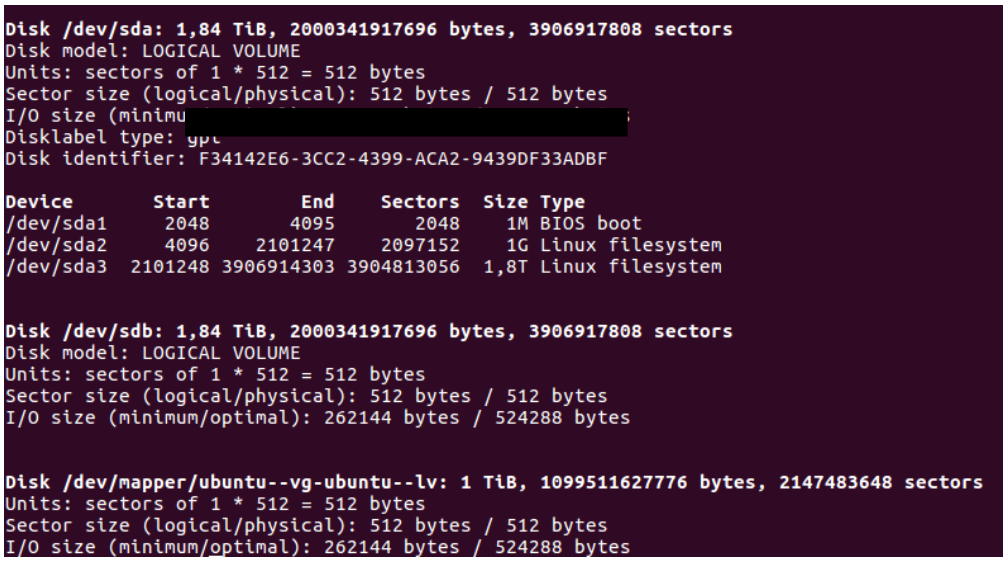

Ilustración 2.2. Particionado del servidor lamella.ujaen.es

Con el sistema operativo recién instalado, a continuación, se actualizan todos los paquetes y se configura la zona horaria con estos comandos:

```
apt update
apt upgrade
dpkg-reconfigure tzdata
```

Como configuración opcional, si el equipo posee más de una tarjeta de red, sería recomendable hacer bonding con ellas. Esto permite sumar el ancho de banda de cada una de las tarjetas de red de manera que las aplicaciones sólo verán una interfaz de red con un gran ancho de banda, necesario en el caso de un gran número

de conexiones remotas simultáneas. Para hacerlo se pueden seguir las instrucciones del apéndice correspondiente que se encuentra al final del documento.

Con esto, el servidor ya estaría listo para iniciar la instalación de Apache Guacamole. Todos los comandos indicados a partir de este momento (también se incluyen los 3 anteriores) se ejecutan como root, que es la cuenta superusuario en Linux, es decir, aquella que posee todos los privilegios y permisos para realizar cualquier acción sobre el sistema.

2.1.1 Instalación de guacamole-server

Guacamole se divide en dos partes: guacamole-server, que proporciona el proxy guacd y las bibliotecas relacionadas, y guacamole-client, que proporciona el cliente para ser atendido por su contenedor de servlet, generalmente Apache Tomcat. La instalación se realiza de forma nativa porque, aunque guacamole-client está disponible en forma binaria, guacamole-server no, y debe construirse desde el código fuente (aunque también lo haremos con guacamole-client).

guacamole-server contiene todos los componentes nativos del lado del servidor que requiere Guacamole para conectarse a escritorios remotos. Proporciona una biblioteca C común (libguac) de la que dependen todos los demás componentes nativos, así como bibliotecas para cada protocolo compatible, y guacd, el corazón de Guacamole.

guacd es el demonio proxy que se ejecuta en su servidor Guacamole, acepta las conexiones de los usuarios que se canalizan a través de la aplicación web Guacamole y luego se conecta a los escritorios remotos en su nombre.

Antes de iniciar el proceso de instalación, se instalan una serie de herramientas genéricas que son necesarias durante la compilación de estos componentes y para la propia ejecución de Apache Guacamole (utilidades de red, contenedor de servlets, Java JDK, compilador de C, control de versiones git, JavaScript entorno de ejecución del lado del servidor, etc.).

```
apt install -y net-tools tomcat9 maven make default-jdk git gcc
nodejs
```

Una vez instaladas, continuamos con el proceso de compilación de guacamole-server. Para ello comenzamos instalando las dependencias estrictamente necesarias.

Guacamole no se puede construir sin ellas. Entre paréntesis se indica el paquete correspondiente para las distribuciones de Ubuntu:

- El Cairo utilizado para la representación de gráficos (libcairo2-dev).
- libjpeg-turbo para brindar compatibilidad con JPEG (libjpeg-turbo8-dev).
- libpng para escribir imágenes PNG, el tipo de imagen principal utilizado por el protocolo Guacamole (libpng-dev).
- libtool se utiliza durante el proceso de compilación. libtool crea bibliotecas compiladas necesarias para Guacamole (libtool-bin).
- libuuid para asignar identificaciones internas únicas a cada usuario y conexión de Guacamole (uuid-dev).

El comando sería el siguiente:

```
apt install -y libcairo2-dev libjpeg-turbo8-dev libpng-dev
libtool-bin uuid-dev
```

Las dependencias opcionales de Guacamole dictan qué partes del servidor de guacamole se habilitarán. Esto incluye la compatibilidad con varios protocolos de escritorio remoto, así como cualquier característica adicional de esos protocolos (se puede consultar en detalle en la documentación del sitio web oficial [22]). En este caso se pretende poder compilar guacamole-server con todos los protocolos disponibles (actualmente RDP, VNC, SSH, Telnet y soporte de Kubernetes) pero algunas de las siguientes librerías no serían necesarias si no se necesitase algún protocolo o función:

```
apt install -y libavcodec-dev libavformat-dev libavutil-dev
libswscale-dev freerdp2-dev libpango1.0-dev libssh2-1-dev
libtelnet-dev libvncserver-dev libwebsockets-dev libpulse-dev
libssl-dev libvorbis-dev libwebp-dev
```

Procedemos a descargamos el paquete correspondiente al servidor en la carpeta `/root` y lo desempaquetamos:

```
cd /root/
wget
https://downloads.apache.org/guacamole/1.4.0/source/guacamole-
server-1.4.0.tar.gz
tar -xzf guacamole-server-1.4.0.tar.gz
```

Si desea el código más reciente y no le importa que el código no se haya probado tan rigurosamente como el código en versiones estables, también puede clonar el repositorio git del equipo de Guacamole en GitHub:

```
git clone git://github.com/apache/guacamole-server.git
```

Cambiamos al nuevo directorio creado y ejecutamos el script `configure` que determinará qué bibliotecas están disponibles en el sistema y seleccionará los componentes apropiados para compilar según lo que realmente haya instalado:

```
cd guacamole-server-1.4.0/
./configure --with-init-dir=/etc/init.d
```

El parámetro `--with-init-dir=/etc/init.d` que se muestra arriba prepara la compilación para instalar un script de inicio para guacd en el directorio `/etc/init.d`, de modo que se inicie automáticamente en el arranque.

En la siguiente imagen, una vez que finalice la ejecución de “configure”, se puede ver una lista de las bibliotecas que se encontraron y lo que ha determinado que se debe construir con la instrucción “make”:

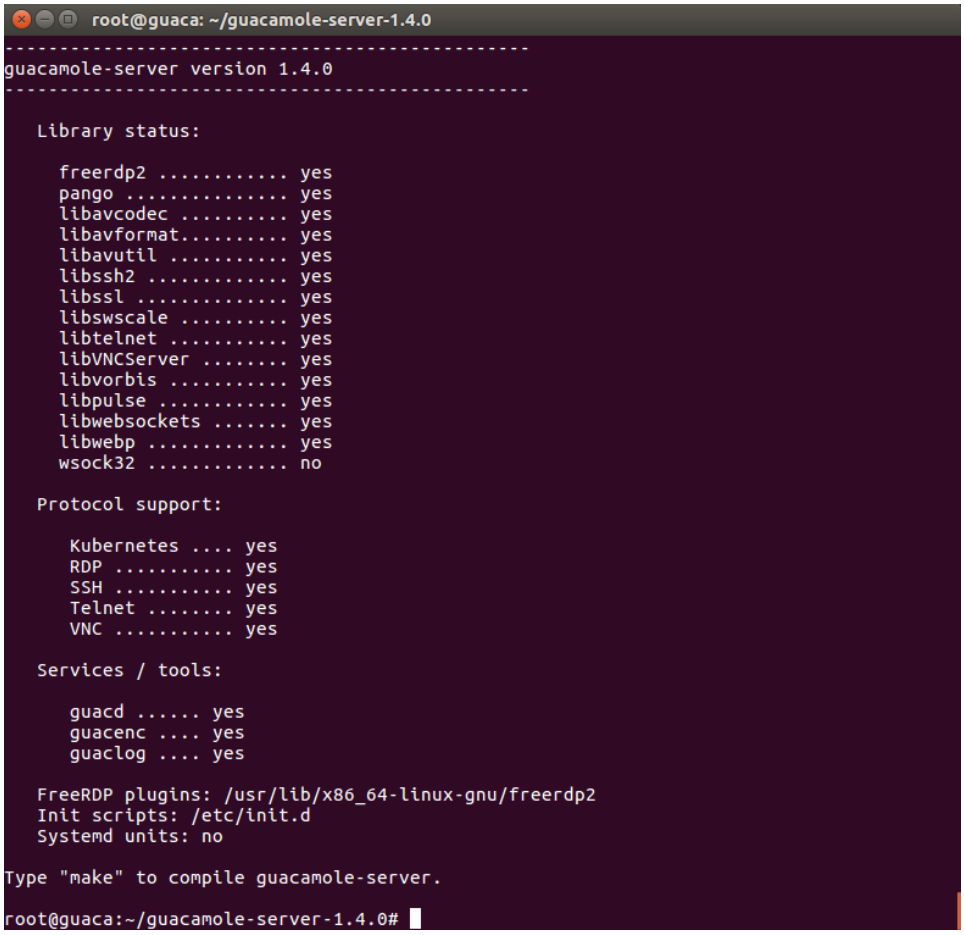

Ilustración 2.3. Resumen del configurador antes de compilar el servidor de Guacamole

Desde el mismo directorio, compilamos guacamole-server:

```
make
```

Procedemos a instalar guacamole-server:

```
make install
```

Una vez terminada la instalación, actualizamos las librerías instaladas en el sistema:

```
ldconfig
```

2.1.2 Instalación de guacamole-client

guacamole-client contiene todos los componentes Java y JavaScript de Guacamole. Estos componentes finalmente conforman la aplicación web que servirá el cliente HTML5 Guacamole a los usuarios que se conecten a su servidor. Esta aplicación web luego se conectará a guacd, parte de guacamole-server, en nombre de los usuarios conectados para brindarles cualquier escritorio remoto al que estén autorizados a acceder.

Para compilar guacamole-client, todo lo que se necesita es Apache Maven y una copia de Java JDK (ya instaladas anteriormente en el punto anterior).

Procedemos a la instalación del cliente, descargando el fichero desde su sitio web en la carpeta `/root` ().

```
cd /root/
wget
https://downloads.apache.org/guacamole/1.4.0/source/guacamole-client-1.4.0.tar.gz
tar -xzf guacamole-client-1.4.0.tar.gz
```

Al igual que con guacamole-server, si desea el código más reciente también puede clonar el repositorio git del equipo de Guacamole en GitHub:

```
git clone git://github.com/apache/guacamole-client.git
```

Para compilar el cliente hay que tener la variable JAVA_HOME establecida, así como la ruta del JDK en la variable PATH, y ejecutar `mvn package`. Esto invocará a

Maven para compilar y empaquetar automáticamente todos los componentes, produciendo un solo archivo .war que contiene toda la aplicación web completa.

```
cd guacamole-client-1.4.0/
echo JAVA_HOME="/usr/lib/jvm/java-11-openjdk-amd64/" >>
/etc/environment
source /etc/environment
export PATH=$PATH:/usr/lib/jvm/java-11-openjdk-amd64/bin
JAVA_HOME="/usr/lib/jvm/java-11-openjdk-amd64/" mvn package
```

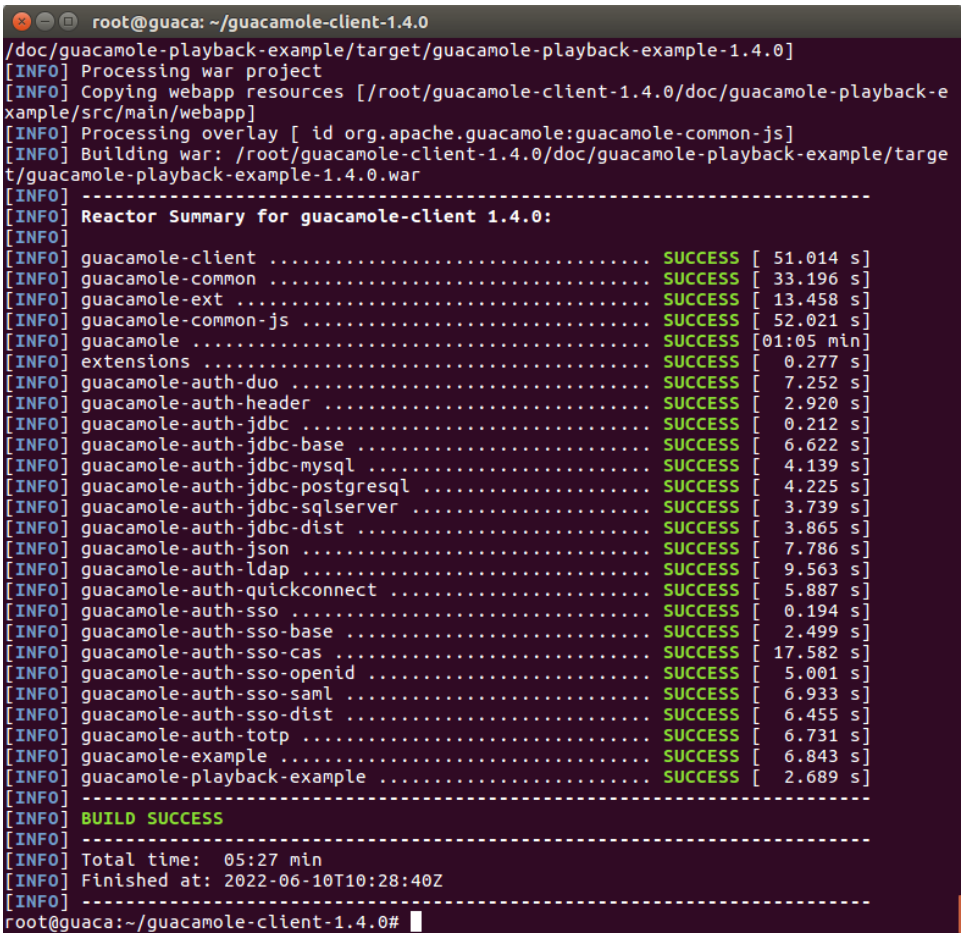

Ilustración 2.4. Compilación de guacamole-client

Una vez finalice la compilación con éxito, encontraremos el fichero .war en el directorio guacamole/target (estando dentro del directorio de guacamole-client-1.4.0). Se crean los directorios necesarios para la configuración de Guacamole, se renombra el fichero .war y lo copiamos en el directorio `/etc/guacamole` y enlazamos en el directorio webapps de Tomcat:

```
mkdir /etc/guacamole
```

```
mkdir /usr/share/tomcat9/.guacamole
cp guacamole/target/guacamole-1.4.0.war
/etc/guacamole/guacamole.war
ln -s /etc/guacamole/guacamole.war /var/lib/tomcat9/webapps
```

Una vez que el archivo .war esté en su ubicación, reiniciaremos tanto Tomcat para obligarlo a implementar la nueva aplicación web, como el demonio guacd:

```
service tomcat9 restart
/etc/init.d/guacd start
```

Después de reiniciar Tomcat e iniciar guacd, Guacamole estará disponible (pero no accesible). En su estado actual, está pendiente de configurar y se requieren más pasos para agregar al menos un usuario de Guacamole y algunas conexiones. Aun así, se puede comprobar el nuevo sitio web en la dirección url `http://<ip del servidor>:8080/guacamole/`

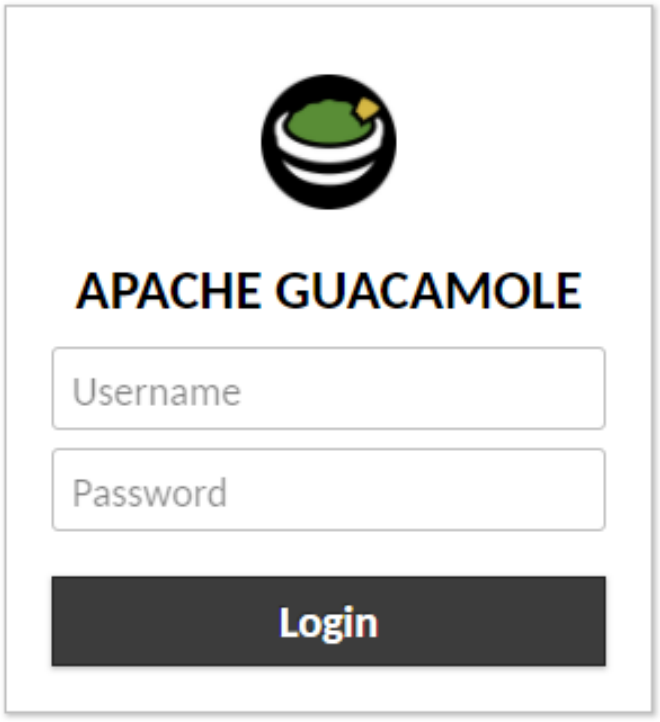

Ilustración 2.5. Página de inicio de Apache Guacamole

2.1.3 Configuración

Después de instalar Guacamole, hay que configurar los usuarios y las conexiones antes de que Guacamole pueda ser utilizado. En este punto se detalla el

método de autenticación predeterminado, que lee todos los usuarios y conexiones de un solo archivo llamado user-mapping.xml. Esta configuración suele ser suficiente para su uso con pocos usuarios y conexiones y también nos ayuda a verificar que Guacamole se ha instalado correctamente.

En el siguiente apartado se describe otro método de autenticación basado en el acceso a una base de datos.

En cualquier caso, la configuración de Guacamole siempre consta de dos partes principales:

- Directorio `GUACAMOLE_HOME`, que es la ubicación principal de búsqueda de archivos de configuración, extensiones (carpeta `extensions/`) y librerías requeridas por cualquiera de las extensiones (carpeta `lib/`).
- Fichero `guacamole.properties`, el archivo de configuración principal utilizado por Guacamole y sus extensiones.

Como primer paso vamos a crear este fichero en el directorio `GUACAMOLE_HOME` y un enlace simbólico al directorio `/usr/share/tomcat9/.guacamole/`.

```
cd /etc/guacamole
touch guacamole.properties
ln -s guacamole.properties /usr/share/tomcat9/.guacamole/
```

Se edita con el siguiente contenido:

```
     guacd-hostname: localhost
     guacd-port: 4822
     user-mapping: /etc/guacamole/user-mapping.xml
     auth-provider:
net.sourceforge.guacamole.net.basic.BasicFileAuthenticationProv
ider
     basic-user-mapping: /etc/guacamole/user-mapping.xml
```

Hay varias propiedades estándar que están disponibles para su uso en este fichero (y que se pueden consultar en la documentación del sitio web oficial [22]). Por ejemplo, la propiedad `api-session-timeout` establece la cantidad de tiempo, en minutos, para permitir que las sesiones de Guacamole sigan siendo válidas a pesar de la inactividad (por defecto caducan después de 60 minutos de inactividad). En este

caso, simplemente se indica el puerto y el equipo donde se ubica el demonio guacd, y el método de autenticación de los usuarios.

Continuamos con la configuración creando el fichero user-mapping.xml también en el directorio `GUACAMOLE_HOME` con el siguiente contenido:

```
nano user-mapping.xml
<user-mapping>
   <authorize
      username="usuario"
      password="f8032d5cae3de20fcec887f395ec9a6a"
      encoding="md5">
      <connection name="SSH">
         <protocol>ssh</protocol>
         <param name="hostname">192.168.1.112</param>
         <param name="port">22</param>
         <param name="username">usuario</param>
      </connection>
   </authorize>
</user-mapping>
```

En este fichero cada usuario se especifica con una etiqueta `<authorize>` y ésta contiene todas las conexiones autorizadas para ese usuario, cada una indicada con una etiqueta `<connection>`. Cada etiqueta `<connection>` contiene un protocolo concreto y un conjunto de parámetros específicos de configuración de dicho protocolo, especificados con las etiquetas `<protocol>` y `<param>` respectivamente. Estos parámetros suelen describir el nombre de host y el puerto del servidor de escritorio remoto, las credenciales que se utilizarán al conectarse, si las hay, y el tamaño y la profundidad de color de la pantalla. Si el protocolo admite la transferencia de archivos, también se proporcionarán opciones para habilitar esa funcionalidad. El listado completo de todos estos parámetros está detallado en la documentación publicada en el sitio web oficial [22].

En nuestro ejemplo:

- Etiqueta Authorize: define un usuario que iniciará sesión en la interfaz web, indicando el nombre de usuario, password y, en su caso, método de codificación. Por ejemplo, podemos obtener un password codificado (hash

md5) con la siguiente instrucción: `printf '%s' "<contraseña_usuario>" | md5sum`

- Etiqueta Connection: define el nombre de la conexión.
- Etiqueta Protocol: define los protocolos que el usuario podrá usar en cada conexión (VNC, RDP, SSH, etc.). En el ejemplo una conexión por SSH.
- Etiqueta Param: define el nombre o dirección IP del equipo al que se conectará, puerto a usar y usuario del sistema al que podrá conectarse.

Por último, modificamos permisos, propietario y grupo propietario del fichero `user-mapping.xml`:

```
chmod 600 user-mapping.xml
chown tomcat:tomcat user-mapping.xml
```

Y reiniciamos Tomcat y el demonio guacd, además de habilitar el servicio para que arranque al iniciar el sistema:

```
service tomcat9 restart
/etc/init.d/guacd restart
systemctl enable guacd.service
```

Una vez reinicie el equipo se puede realizar una prueba de funcionamiento. En un ordenador (en este caso de la misma red) nos vamos al navegador, escribimos la dirección url del servidor de Guacamole (`http://<ip del servidor>:8080/guacamole`) e introducimos usuario y contraseña definidos en el `tag authorize`:

Ilustración 2.6. Prueba de acceso remoto con Apache Guacamole

Al iniciar sesión en Apache Guacamole nos pedirá contraseña del usuario indicado en el apartado `connection`. Introducimos dicha contraseña y, según nuestro ejemplo, accederemos por SSH a su cuenta desde la terminal abierta en el navegador.

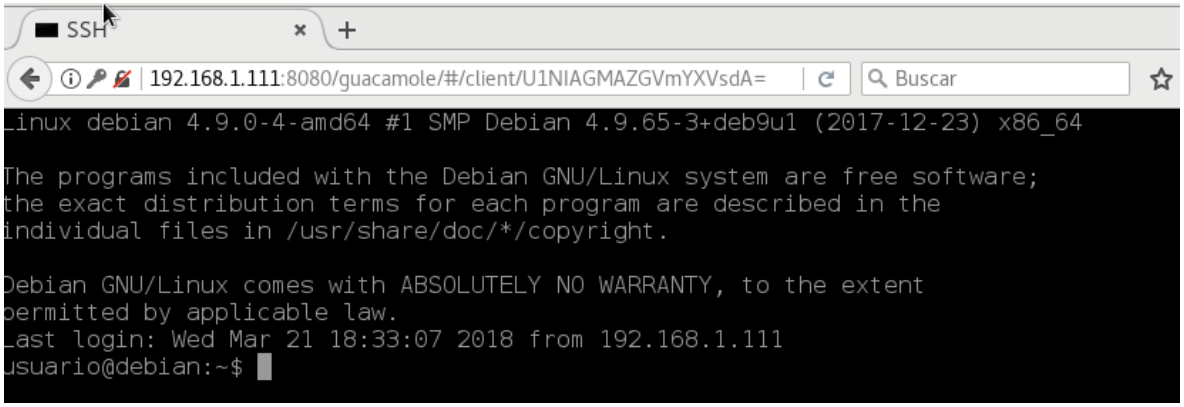

Ilustración 2.7. Ejemplo de conexión por SSH con Guacamole

2.1.4 Autenticación de base de datos

Hasta aquí hemos visto la autenticación de los usuarios basándonos en un fichero XML. El incorporar autentificación por base de datos, aporta muchas ventajas a nuestro sistema. No sólo el mantenimiento de usuarios y conexiones, que se podrá realizar usando una interfaz administrativa basada en web, sino que también

podremos añadir controles y estadísticas de usos de una forma fácil y cómoda. A diferencia del módulo de autenticación basado en el fichero XML predeterminado, todos los cambios en los usuarios y las conexiones surten efecto inmediatamente; los usuarios no necesitan cerrar la sesión y volver a iniciarla para ver nuevas conexiones.

Apache Guacamole admite la autenticación a través de bases de datos MySQL, PostgreSQL o SQL Server con las extensiones disponibles en el sitio web del proyecto. En este estudio vamos a configurar Guacamole con una base de datos MySQL. Su instalación se efectuaría con este comando:

```
apt install -y default-mysql-server default-mysql-client mysql-common
```

Seguidamente ejecutamos el script `mysql_secure_installation` que establece la contraseña para el usuario `root` y elimina algunos puntos vulnerables (como son la base de datos de prueba, usuarios anónimos o el acceso remoto con el usuario root) para agregar algo de seguridad a la base de datos:

```
mysql_secure_installation
```

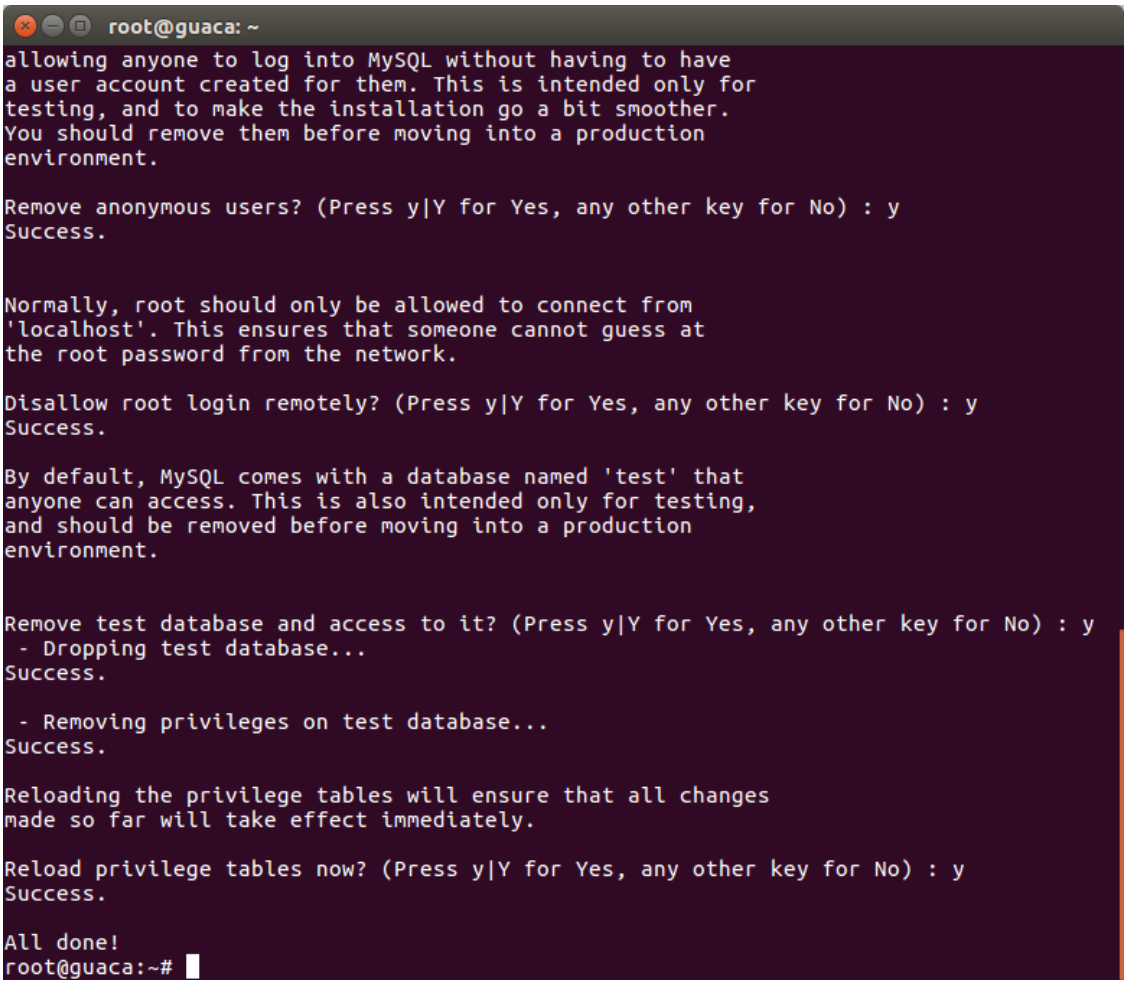

Ilustración 2.8. Ejecución del script mysql_secure_installation

En cualquier caso, lo idóneo es fortificar aún más la seguridad de la instalación de MySQL.

El siguiente paso sería descargar la extensión de autenticación de la base de datos y el controlador JDBC compatible con MySQL, que son imprescindibles para el acceso a la base de datos:

```
cd /root/
wget http://ftp.iij.ad.jp/pub/db/mysql/Downloads/Connector-J/mysql-connector-java-8.0.19.tar.gz
wget https://apache.org/dyn/closer.lua/guacamole/1.4.0/binary/guacamole-auth-jdbc-1.4.0.tar.gz
```

Creamos los directorios donde irán ubicados dentro de `GUACAMOLE_HOME`, descomprimimos los dos archivos descargados anteriormente y los copiamos en su directorio correspondiente.

```
mkdir /etc/guacamole/lib
mkdir /etc/guacamole/extensions
tar -xzf mysql-connector-java-8.0.19.tar.gz
tar -xzf guacamole-auth-jdbc-1.4.0.tar.gz
cp  mysql-connector-java-8.0.19/mysql-connector-java-8.0.19.jar
/etc/guacamole/lib
cp   guacamole-auth-jdbc-1.4.0/mysql/guacamole-auth-jdbc-mysql-
1.4.0.jar /etc/guacamole/extensions
```

El módulo de autenticación de la base de datos necesitará una base de datos para almacenar datos de autenticación y un usuario para usar solo para el acceso y la manipulación de datos. Para ello hay que ejecutar MySQL y, una vez dentro, lanzamos estas sentencias SQL para crear la base de datos (guacamole_db) y el usuario (guacauser) necesarios, y establecer los permisos de selección, inserción, actualización y borrado sobre todas las tablas de Guacamole:

```
mysql -u root -p
     mysql> create database guacamole_db;
     mysql> create user 'guacauser'@'localhost' identified by
"XXXXXXXX";
     mysql> GRANT SELECT,INSERT,UPDATE,DELETE ON guacamole_db.*
TO 'guacauser'@'localhost';
     mysql> flush privileges;
     mysql> exit;
```

donde XXXXXXXX se sustituye por la contraseña que se desee establecer para el usuario `guacauser` de la base de datos.

También será necesario ejecutar sobre esta base de datos (`guacamole_db`) los scripts acabados en “sql” que contiene el paquete `guacamole-auth-jdbc-1.4.0` y que provocará la creación de todas las tablas necesarias para el correcto funcionamiento de Apache Guacamole. Esto, precisamente, es lo que realiza el siguiente comando:

```
cat guacamole-auth-jdbc-1.4.0/mysql/schema/*.sql | mysql -u root
-p guacamole_db
```

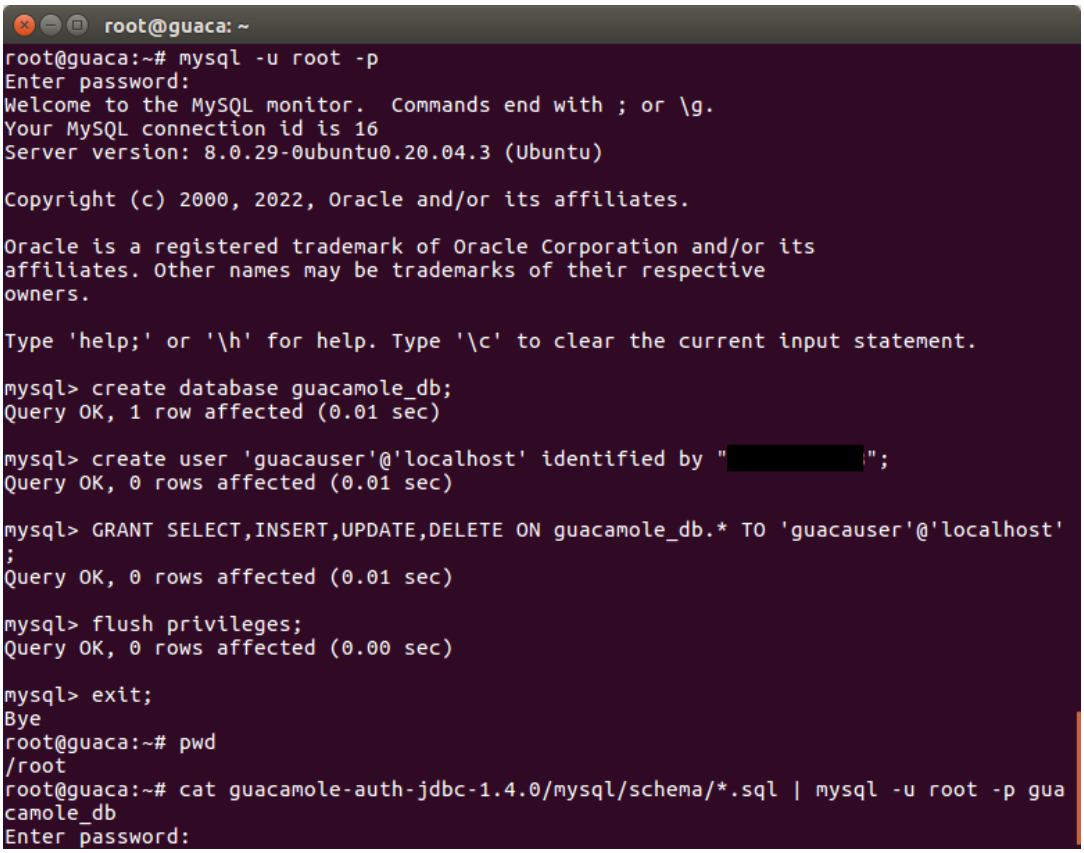

Ilustración 2.9. Creación de la base de datos de Guacamole en MySQL

Como paso final ya sólo queda editar el fichero `guacamole.properties` y modificar la configuración para poder conectar con la base de datos y que funcione correctamente la autenticación. Para esto habría que cambiar la propiedad `auth-provider` y añadir las 4 propiedades mínimas requeridas en este fichero:

```
nano /etc/guacamole/guacamole.properties

auth-provider:
net.sourceforge.guacamole.net.auth.mysql.MySQLAuthenticationPro
vider


# MySQL options
mysql-hostname: localhost
mysql-database: guacamole_db
mysql-username: guacauser
mysql-password: XXXXXXXX   #indicar el password correspondiente
```

Estas propiedades con su nombre se explican por sí mismas.

Lógicamente, existen más propiedades opcionales para controlar cómo se conecta Guacamole al servidor de la base de datos que se pueden configurar con el fichero `guacamole.properties`. Entre ellas podemos destacar propiedades para cambiar el puerto de conexión a la base de datos, para configurar la complejidad de las contraseñas de los usuarios y su cambio regular, para restringir el uso simultáneo de conexiones, etc. Todas estas propiedades se pueden consultar en la documentación de su sitio web, aunque tienen nombres muy descriptivos. Algunos ejemplos son:

```
mysql-port: 3306

mysql-user-password-min-length: 8
mysql-user-password-require-multiple-case: true
mysql-user-password-require-symbol: true
mysql-user-password-require-digit: true
mysql-user-password-prohibit-username: true

mysql-default-max-connections: 1
mysql-default-max-group-connections: 1
```

Para completar la instalación es necesario reiniciar el contenedor de servlets (Tomcat) ya que Guacamole sólo volverá a leer el fichero guacamole.properties y cargar las extensiones recién instaladas durante el inicio.

```
service tomcat9 restart
```

Probamos que todo funcione, tecleando en un navegador `http://<ip del servidor>:8080/guacamole`.

Es posible que el navegador presente un error al intentar acceder a la página de Guacamole. Esto es debido a un problema con la compatibilidad horaria entre el servidor y la base de datos. El log al consultar el estado del servicio de Tomcat muestra el mensaje:

> *"Error querying database. Cause: java.sql.SQLException: The server time zone value 'CEST' is unrecognized or represents more than one time zone. You must configure either the server or JDBC driver (via the serverTimezone configuration property) to use a more specifc time zone value if you want to utilize time zone support."*

La solución está en indicarle a MySQL la “timezone” que está utilizando el servidor ejecutando estos comandos como usuario `root`:

```
mysql_tzinfo_to_sql /usr/share/zoneinfo | mysql -u root -D mysql
-p
nano /etc/mysql/mysql.conf.d/mysql.cnf
      #añadir esta línea en [mysqld]
      default_time_zone=Europe/Madrid
systemctl restart mysql.service
```

Una vez ejecutadas estas instrucciones, para solucionar este posible error, ya podremos acceder a la página de inicio de sesión de Apache Guacamole.

El usuario predeterminado de Guacamole creado por los scripts SQL provistos es “guacadmin”, y su contraseña predeterminada “guacadmin”. Una vez que se ha verificado que la autenticación de la base de datos está funcionando, hay que proceder a cambiar esta contraseña de inmediato, ya que este es el usuario predefinido para la administración de la aplicación. Esta operación se puede realizar accediendo a “Configuración” y en la pestaña “Preferencias”

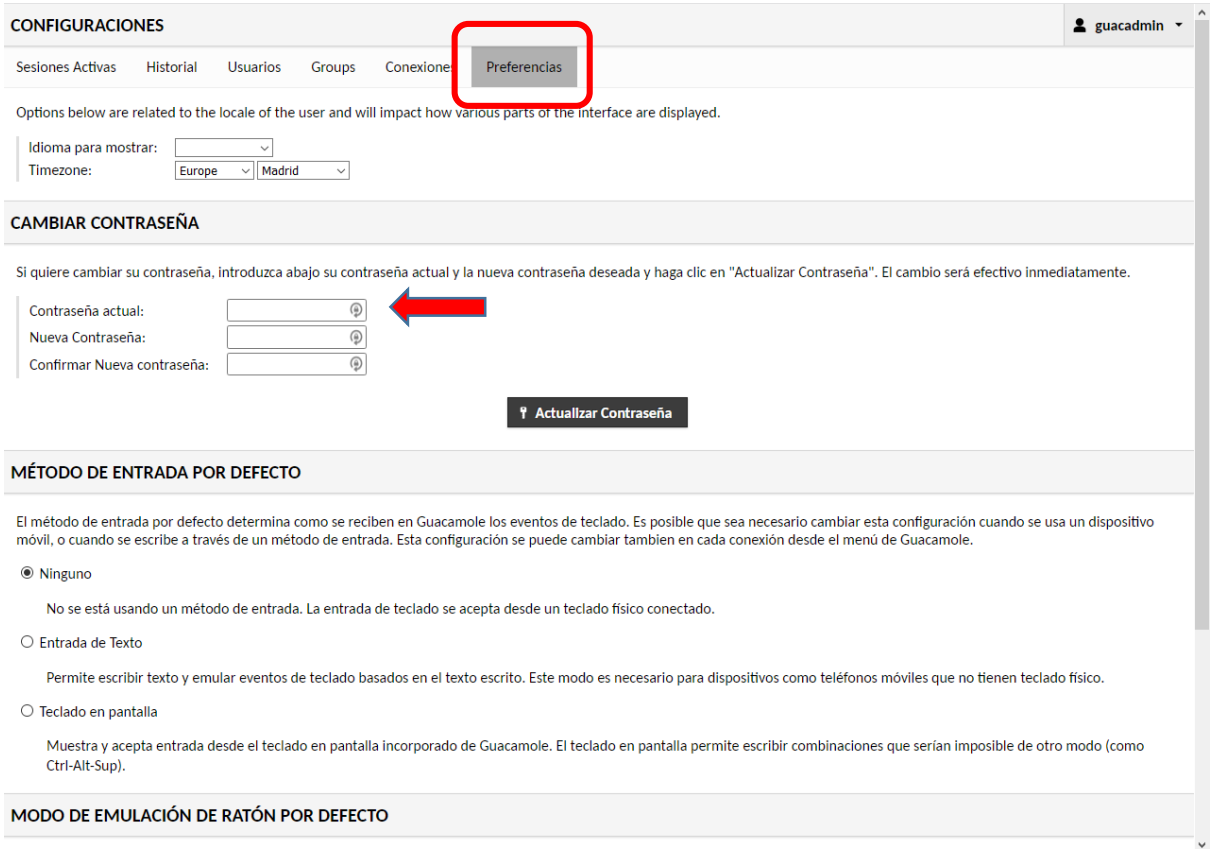

Ilustración 2.10. Cambio de contraseña por defecto del usuario de administración

2.1.5 Modificar la dirección url de inicio

Para hacer este cambio, y no tenemos más sitios web en el servidor, podemos hacer que la dirección url de inicio de la aplicación web sea simplemente `http://<ip del servidor>:8080`, y no haga falta añadir `/guacamole`, hay que ejecutar estos comandos como usuario `root`:

```
rm -rf /var/lib/tomcat9/webapps/ROOT
ln -s /var/lib/tomcat9/webapps/guacamole
/var/lib/tomcat9/webapps/ROOT
systemctl restart tomcat9.service
```

De este modo también se evita que cualquier usuario cargue la página web de inicio de Tomcat:

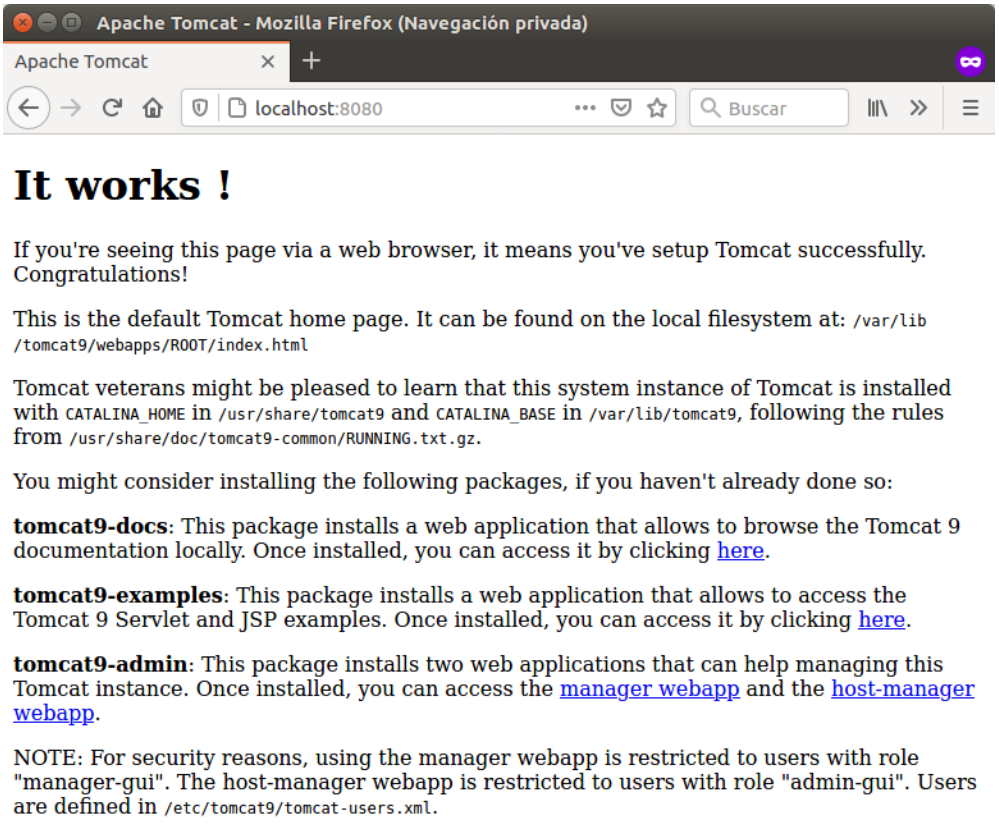

Ilustración 2.11. Página web de inicio de Tomcat

2.2 Configuración de los escritorios remotos

Hasta aquí sólo se ha detallado la instalación y configuración de la aplicación web en un servidor que va a ser el encargado de administrar las conexiones remotas de los usuarios contra los diferentes escritorios y sistemas de los equipos de los laboratorios docentes del Departamento de Informática.

Lógicamente, para poder tener acceso a todos estos escritorios a través de las tecnologías ya comentadas (RDP, VNC y SSH), también habrá que configurar las opciones específicas para ello en cada sistema operativo de cada equipo al que nos queremos conectar. Este punto dedica un apartado individual a cada sistema operativo montado en los equipos de los laboratorios docentes donde se describen los pasos para habilitar su acceso remoto.

Para replicar fácilmente, en todos los ordenadores, todas las configuraciones podemos hacer uso de la herramienta FOG mediante el clonado de imágenes con la configuración ya aplicada.

2.2.1 Windows 10

La conexión a este sistema operativo es a través de su protocolo de Escritorio Remoto (RDP), y su configuración es simple:

1. Seleccionar Inicio > Configuración > Sistema > Escritorio remoto y activar Habilitar escritorio remoto.

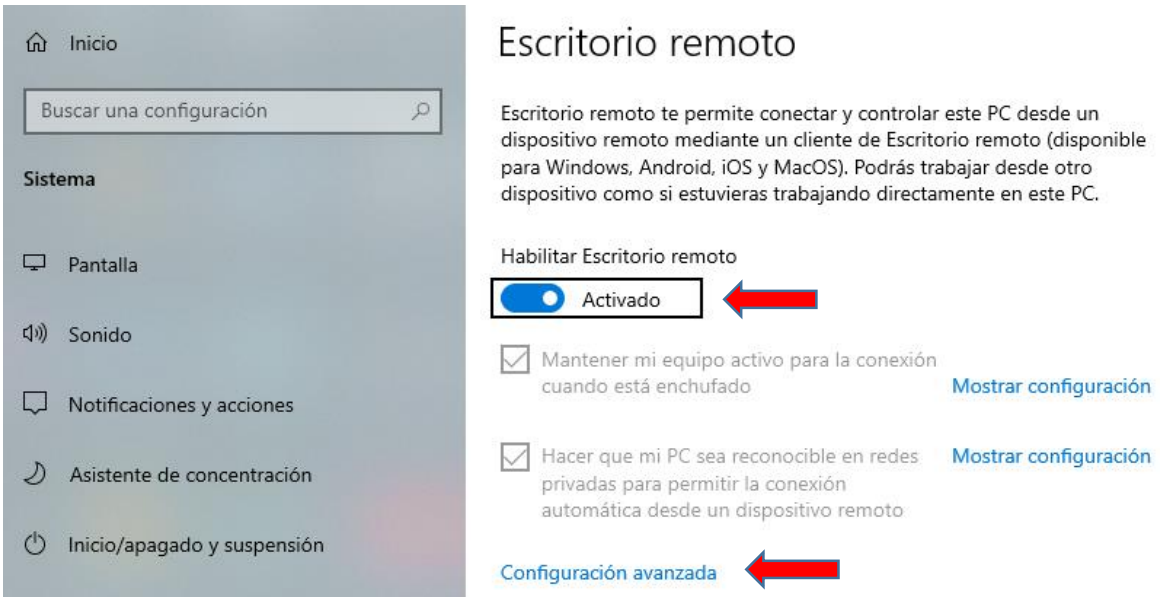

Ilustración 2.12. Configuración de Escritorio Remoto de Windows 10

2. Dentro de la Configuración avanzada, activar la opción “Requerir equipos usen autenticación a nivel de red para conectarse” (también denominada NLA).

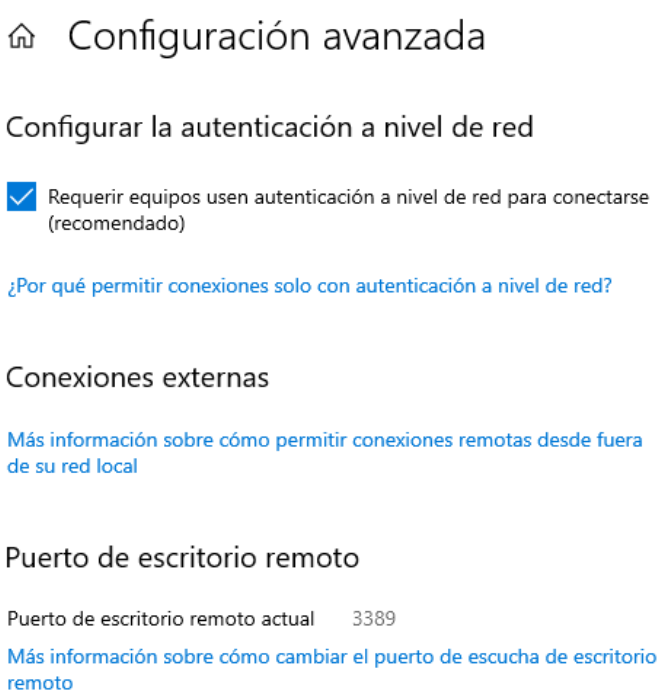

Ilustración 2.13. Configuración avanzada de Escritorio Remoto de Windows 10

3. El Escritorio remoto requiere un nombre de usuario y contraseña al abrir la ventana de terminal. Esto protege a cualquier ordenador de accesos no autorizados, aunque este requisito se podría eliminar modificando la directiva de seguridad local para que permita contraseñas en blanco.

   En cualquier caso, para grabar una contraseña en la cuenta del usuario hay que seleccionar Inicio > Configuración > Cuentas > Opciones de inicio de sesión y establecer una contraseña a la cuenta de usuario.

   No es necesario que el usuario tenga iniciada la sesión en Windows para permitir la conexión a su Escritorio remoto desde Guacamole.

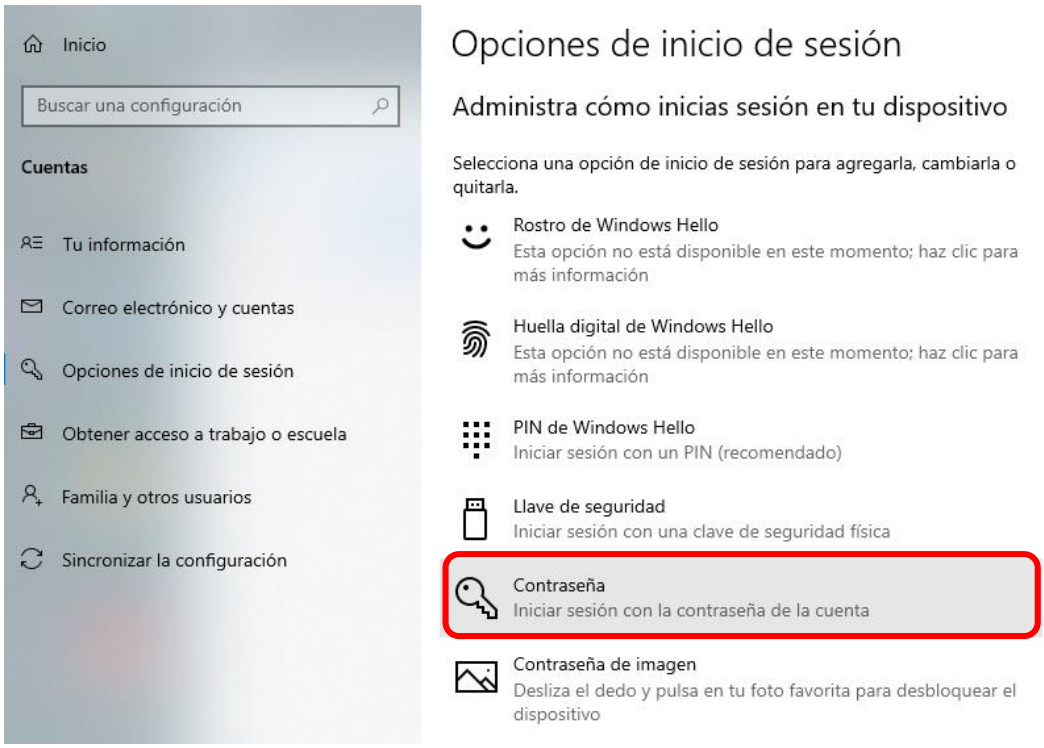

Ilustración 2.14. Inicio de sesión con contraseña en Windows 10

Aunque no es el caso que nos concierne, si deseamos realizar una conexión directa desde un equipo externo a la Universidad de Jaén, es decir, sin pasar la comunicación por Apache Guacamole, no sólo necesitaría aplicar la configuración comentada en el equipo al que nos conectamos, sino también sería necesario establecer previamente una conexión VPN-SSL a la Universidad de Jaén desde el equipo que queremos conectar. Para esto, es condición indispensable tener una cuenta de usuario de la UJA y nos permitiría atravesar todo su perímetro de seguridad.

2.2.2 Ubuntu 20.04

Con este sistema operativo la conexión remota se realizará a través de VNC y para ello sólo habría que activar la opción para compartir pantalla:

1. Seleccionar Configuración > Compartir > Activar (para que se habilite la opción de “Compartición de la pantalla”) > Compartición de la pantalla.

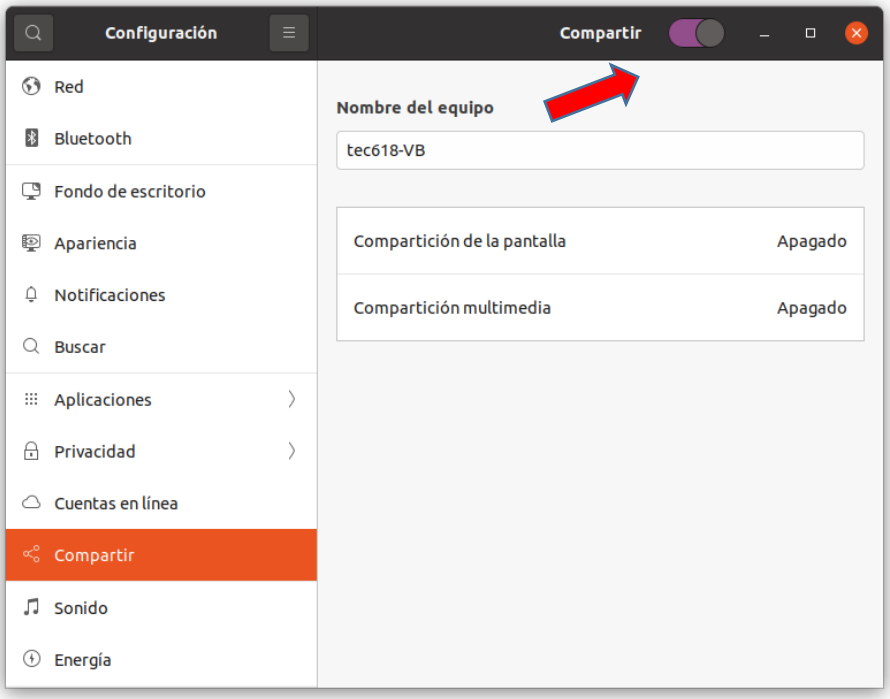

Ilustración 2.15. Compartir pantalla en Ubuntu 20.04

2. Activar Compartición de la pantalla (ubicado en la parte superior), “Permitir conexiones para controlar la pantalla” y “Solicitar una contraseña”.

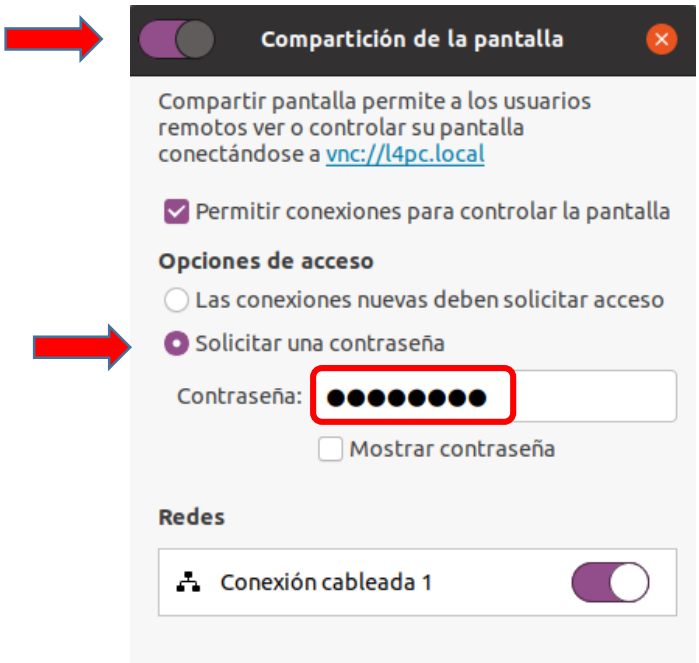

Ilustración 2.16. Configuración para compartir pantalla en Ubuntu 20.04

3. Seleccionar Configuración > Usuarios > Desbloquear (con las credenciales de administrador, para poder cambiar la configuración) y activar “Iniciar sesión automáticamente”. Apache Guacamole requiere con este sistema que esté iniciada la sesión de usuario para poder conectar con su escritorio.

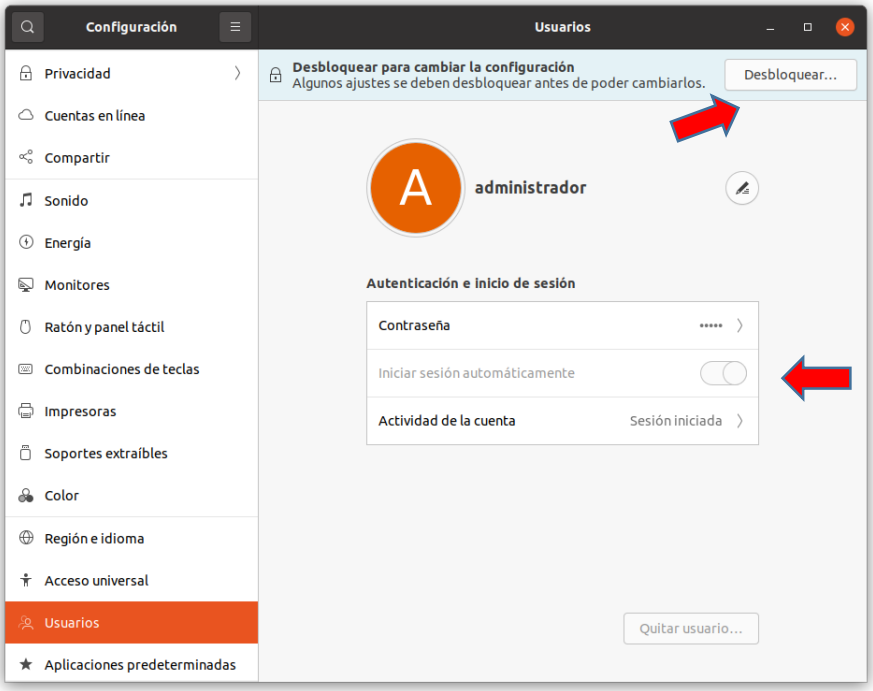

Ilustración 2.17. Inicio de sesión automático en Ubuntu 20.04

2.2.3 MacOS High Sierra

Como último sistema operativo, vamos a ver la configuración de MacOS en la versión High Sierra ya que está es la última versión cargada en los ordenadores iMac del aula Mac del Departamento (en otras versiones el procedimiento sería similar). Al igual que el anterior, la configuración de esta conexión remota también se realiza por VNC:

1. Seleccionar Preferencias del sistema > Compartir, y marcar estas opciones (una vez que las hayamos desbloqueado haciendo clic en el candado e introduciendo credenciales administrativas del sistema):

    - Compartir archivos, Sesión remota (en el caso de que realizar conexiones remotas a través de SSH), Gestión remota, Eventos Apple remotos.

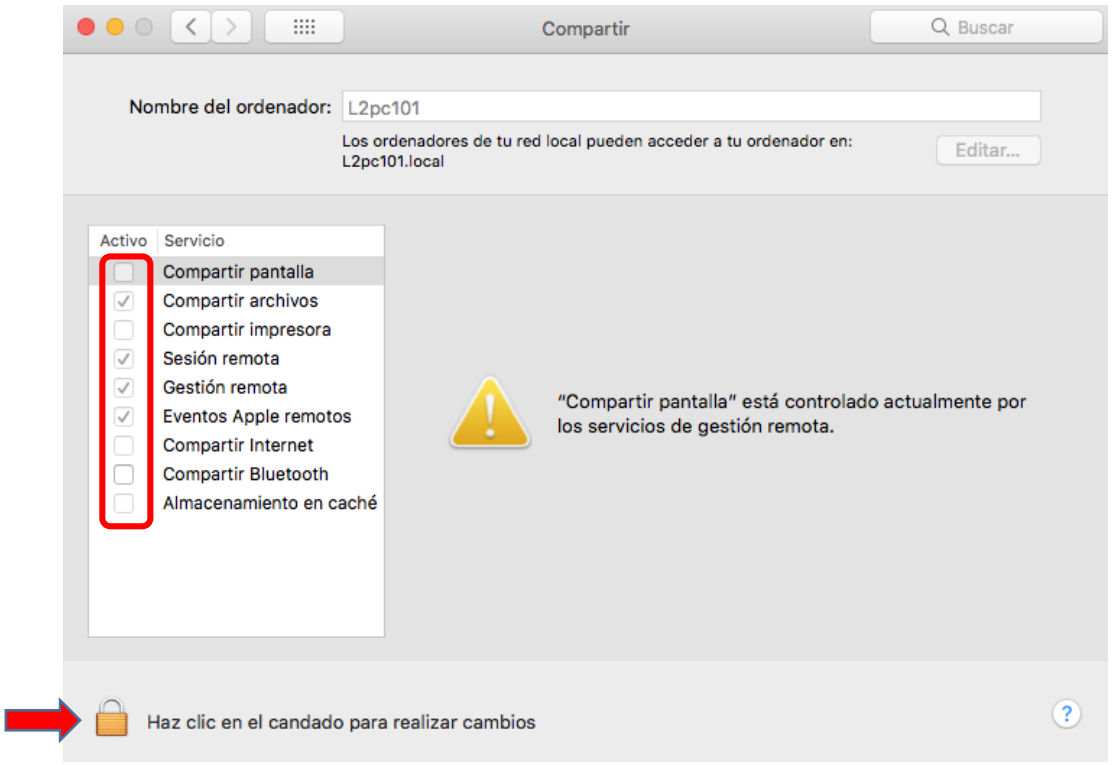

Ilustración 2.18. Configuración para compartir pantalla en MacOS

2. En la opción Gestión remota > Ajustes del ordenador, marcar:
    - Todos pueden pedir permiso para controlar la pantalla.
    - Los visores VNC pueden controlar la pantalla mediante contraseña > indicar el password de acceso.

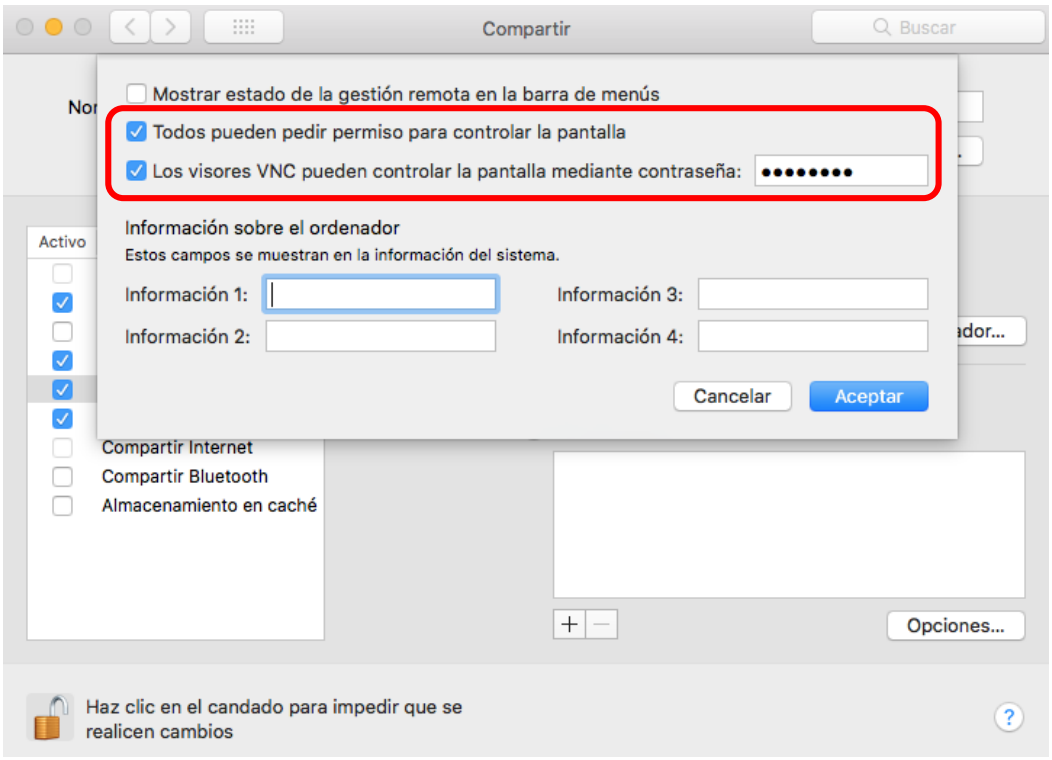

Ilustración 2.19. Configuración en Gestión remota en MacOS

3. En la opción Sesión remota, y en el caso de que realizar conexiones remotas a través de SSH > Activar una de estas 2 opciones en “Permitir acceso a”:
    - Todos los usuarios.
    - Añadir en la lista sólo a los usuarios del sistema con los cuales queremos establecer una conexión SSH.

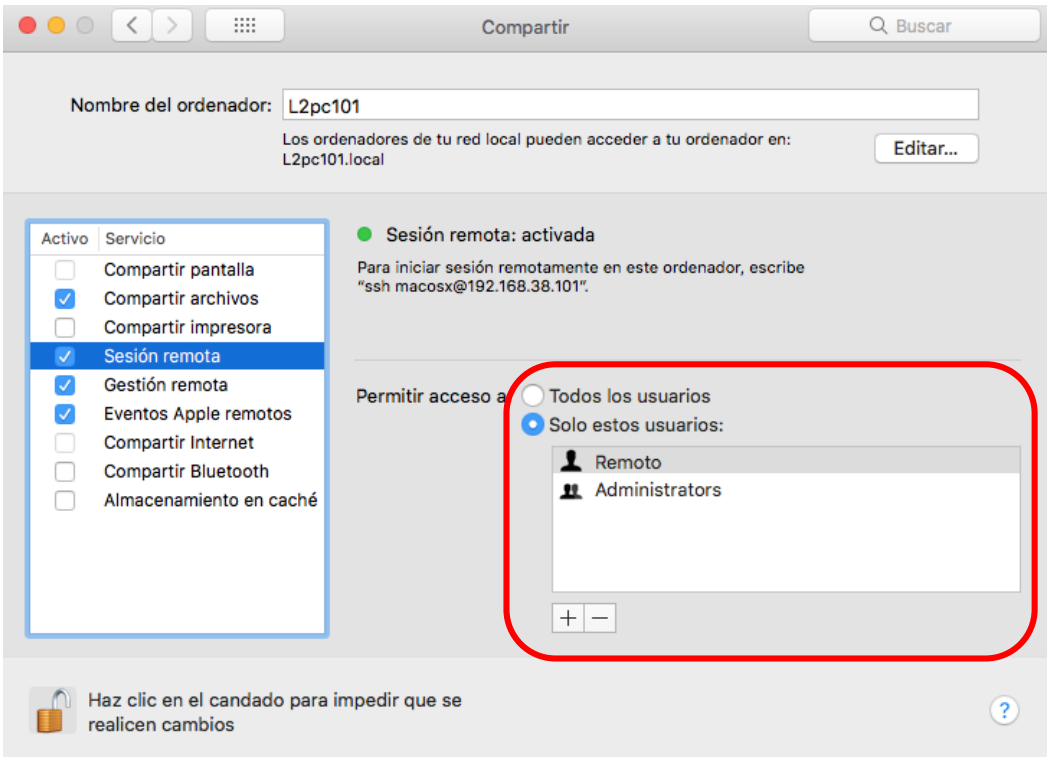

Ilustración 2.20. Configuración de conexión SSH en MacOS

2.3 Recomendaciones

De manera opcional, aunque muy recomendable, esta sección lista una serie de recomendaciones genéricas que permiten mejorar tanto la seguridad en nuestro servidor como la experiencia de usuario con la aplicación Apache Guacamole (o cualquier herramienta de escritorio remoto).

- Seguridad:
  - Actualización del sistema operativo y firmware. Para proteger al equipo frente a las vulnerabilidades de seguridad, eligiendo la opción de actualizaciones automáticas siempre que esté disponible.
  - Actualización del antivirus (si es el caso).
  - Uso de contraseñas robustas. No sólo en los usuarios del sistema y acceso a la base de datos, sino también en los usuarios definidos en Guacamole que son los que realmente ofrecen el acceso remoto desde el exterior de una organización. Las claves para una contraseña robusta son:
    - Que tenga al menos 8 caracteres.

        - Que combine letras, números y caracteres especiales.
        - Que use mayúsculas y minúsculas.
        - No incluir datos obvios, como nombre o fecha de nacimiento.
        - Cambiar la contraseña cada cierto tiempo.
    - Factor de doble autenticación. Es una mejora del punto anterior, que permite Guacamole y que añade una segunda capa de protección a la contraseña que empleamos para el acceso remoto. En otras palabras, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor de autenticación, por ejemplo, un código de seguridad que se envía mediante otro medio para así confirmar que realmente eres el propietario de la cuenta.
    - VPN (Red Privada Virtual). Utilizar una VPN tanto para las conexiones de los clientes como para el acceso a los equipos remotos.
    - Copias de seguridad. Se trata de una recomendación genérica pero muy efectiva ante cualquier ataque o fallo del sistema.
- Experiencia de usuario:
    - Para mejorar el rendimiento de la conexión a un escritorio remoto es conveniente configurar ciertos parámetros en el propio escritorio al que nos conectamos:
        - Tener un fondo de escritorio de un color sólido y no de una imagen.
        - Reducir la intensidad del color.
        - Desactivar la función de salvapantallas.
        - Desactivar todos los efectos visuales relacionados con minimizar las ventanas, transparencia y sombreado de éstas, etc.
    - Cambiar la resolución de la pantalla a aquella que mejor se adapte al monitor desde donde nos conectemos.

- En el navegador, a través del cual nos conectamos al equipo remoto, el uso de "Pantalla completa" permite una mejor definición de la pantalla remota.
- Es posible hacer uso del portapapeles para copiar o pegar texto en la máquina remota. Para ello hay que habilitar este permiso al conectarnos por primera vez al sitio web o en el navegador como podemos ver en la siguiente imagen del navegador Chrome:

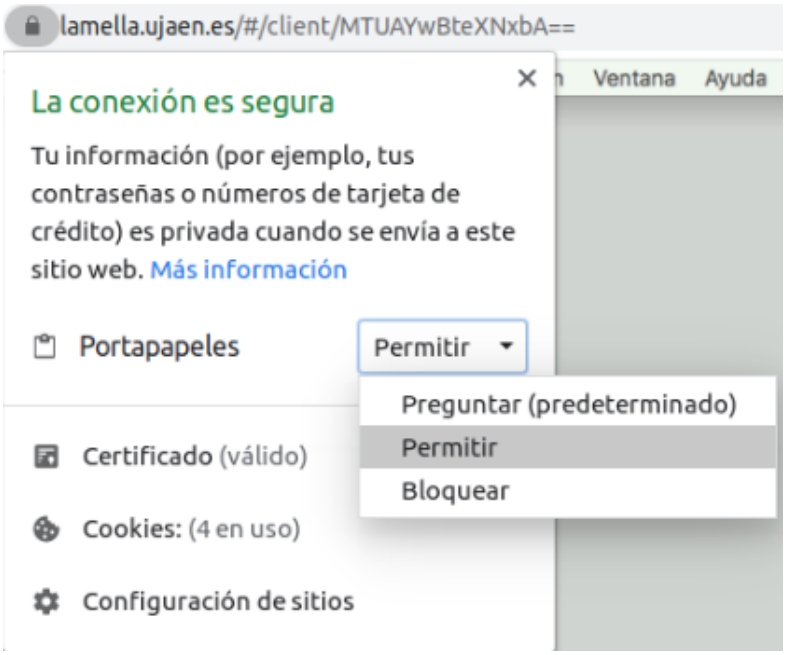

Ilustración 2.21. Habilitar portapapeles en la conexión remota con Apache Cuacamole

3 EVALUACIÓN

Llegados a este punto, es el momento de comprobar y evaluar los resultados que indiquen si Apache Guacamole cumple, o no, con el objetivo principal que motivó este trabajo fin de grado.

Es evidente que no se trata de una aplicación pensada para jugar o ver videos online por la carga gráfica que esto supone, aunque si se puede decir que permite trabajar al usuario perfectamente, por ejemplo, en el desarrollo normal de una sesión de prácticas de una asignatura, y con una usabilidad muy aceptable.

El rendimiento registrado en las pruebas de carga es otro de los datos a destacar. Para realizar esta evaluación se han realizado varias conexiones simultáneas a los ordenadores del laboratorio 2 (iMacs de Apple) ya que estos equipos son, por sus características, los menos habituales entre el alumnado y por ello se podría tratar de una prueba más real. Para medir los recursos consumidos por el servidor de Guacamole en la ejecución de las pruebas se ha utilizado una aplicación específica de terceros: sysmontask [27], un monitor de sistema para Linux que imita al Administrador de tareas de Windows 10, y que ofrece un mayor control y monitoreo que las propias herramientas del sistema.

Antes de iniciar esta simulación, era necesario montar en el servidor la interfaz gráfica de Ubuntu para así poder ejecutar la aplicación anterior, ya que el sistema operativo Ubuntu Server no instala por defecto el entorno gráfico de escritorio. Para ello, se ejecutan estos comandos con privilegios de administrador:

```
sudo apt install tasksel
sudo tasksel install ubuntu-desktop
reboot
```

Una vez montado el entorno gráfico de usuario, ejecutamos también estos comandos para la instalación de este monitor de sistema en Ubuntu:

```
sudo apt install python3-pip
sudo add-apt-repository ppa:camel-neeraj/sysmontask
sudo apt install sysmontask
sudo pip3 install -U psutil
```

Con la herramienta ya ejecución, iniciamos las pruebas de carga para ir capturando la información que nos ofrece el monitor. En el intento de realizar

conexiones remotas “exigentes”, los escritorios remotos visualizarán un video de Internet (usando el navegador y el sitio web Youtube) durante la conexión para que haya una gran transmisión de datos entre el equipo al que se conecta el usuario de Guacamole y el propio equipo del usuario.

La información recopilada es la que aparece en las siguientes imágenes que muestra porcentajes de uso y gráficos de monitorización del procesador (CPU), memoria RAM, disco y red en diferentes situaciones según el número de conexiones remotas simultáneas:

- Recursos con el servidor “en reposo” (sin conexiones remotas).

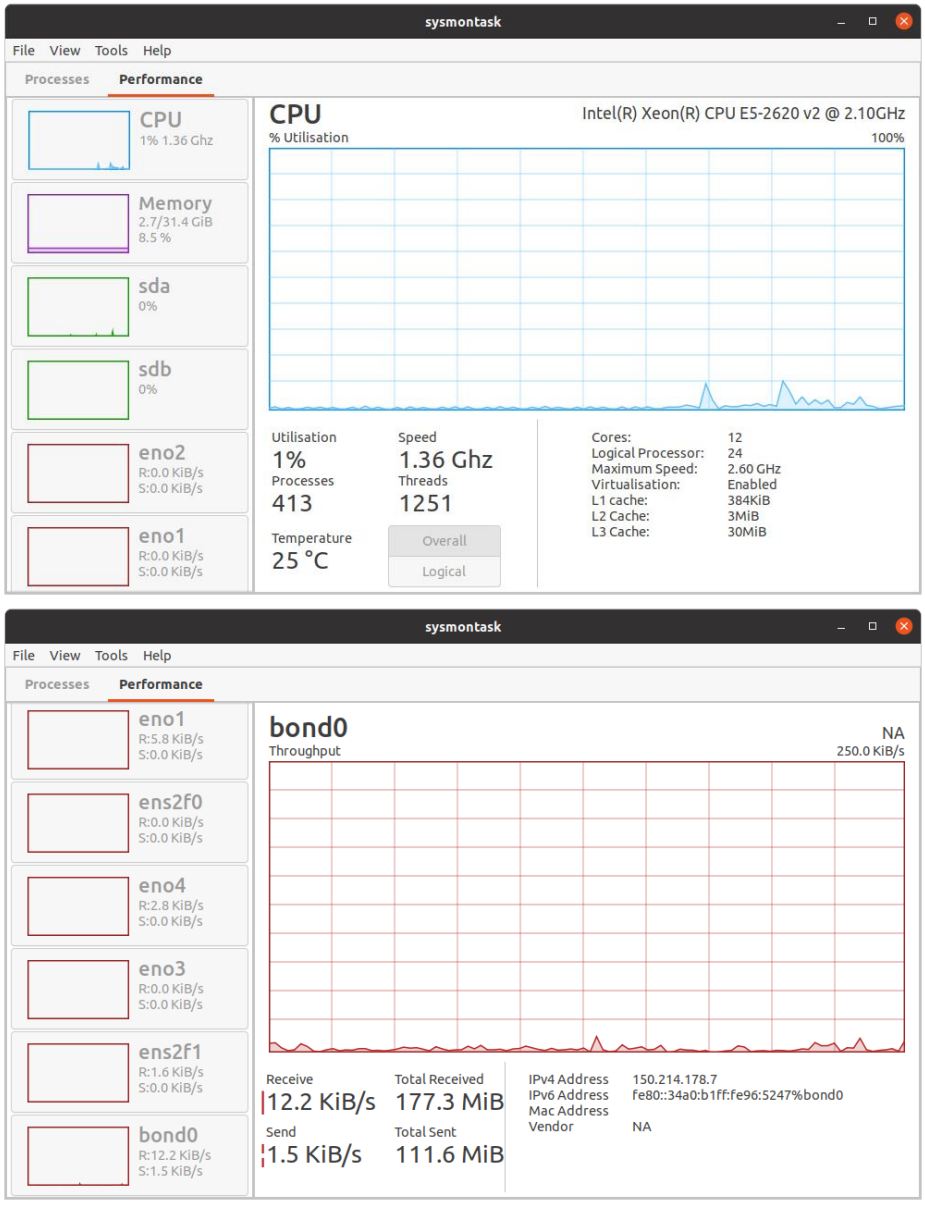

Ilustración 3.1. Recursos del sistema sin conexiones remotas

- Recursos consumidos por una sola conexión:

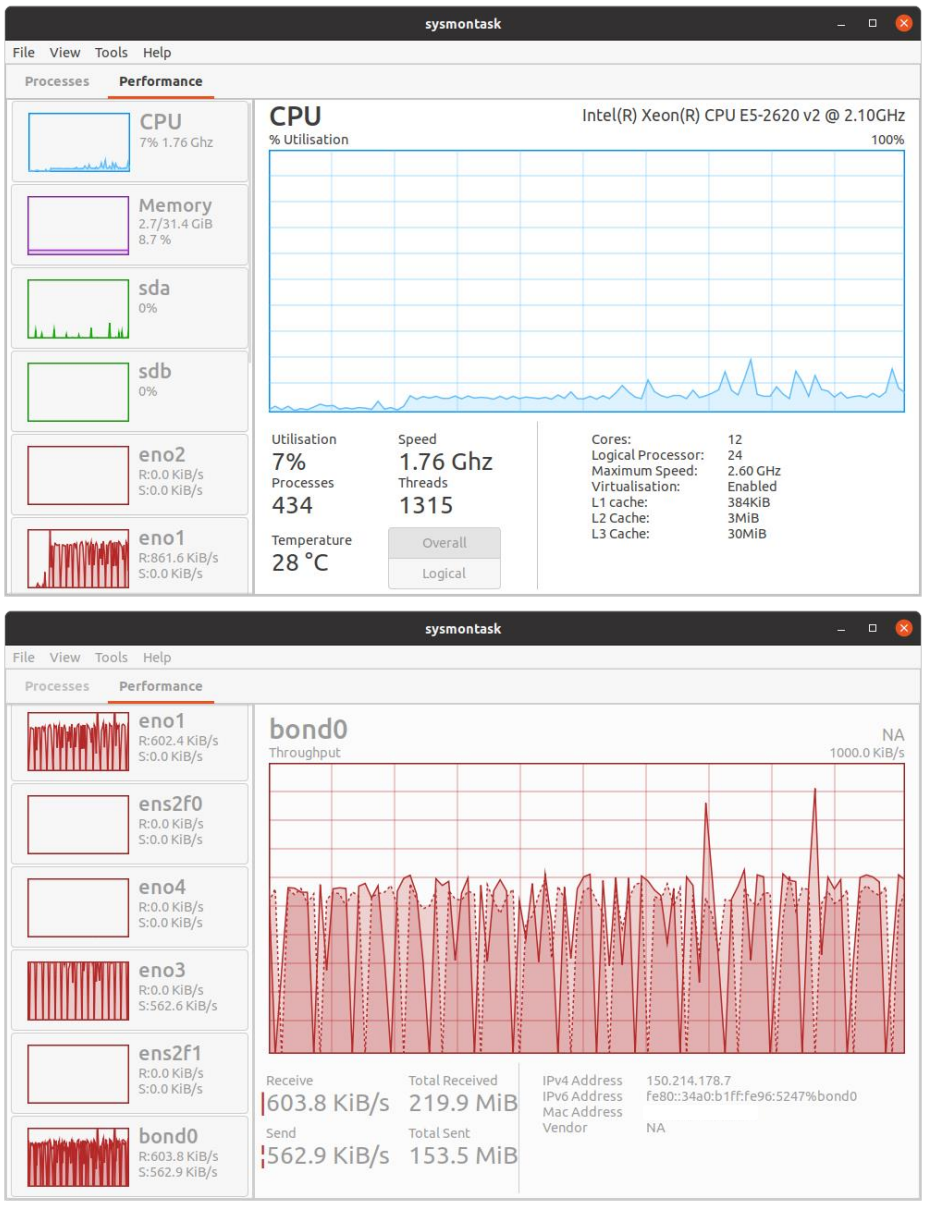

Ilustración 3.2. Recursos del sistema con una sola conexión remota

- Recursos consumidos por 5 conexiones simultáneas:

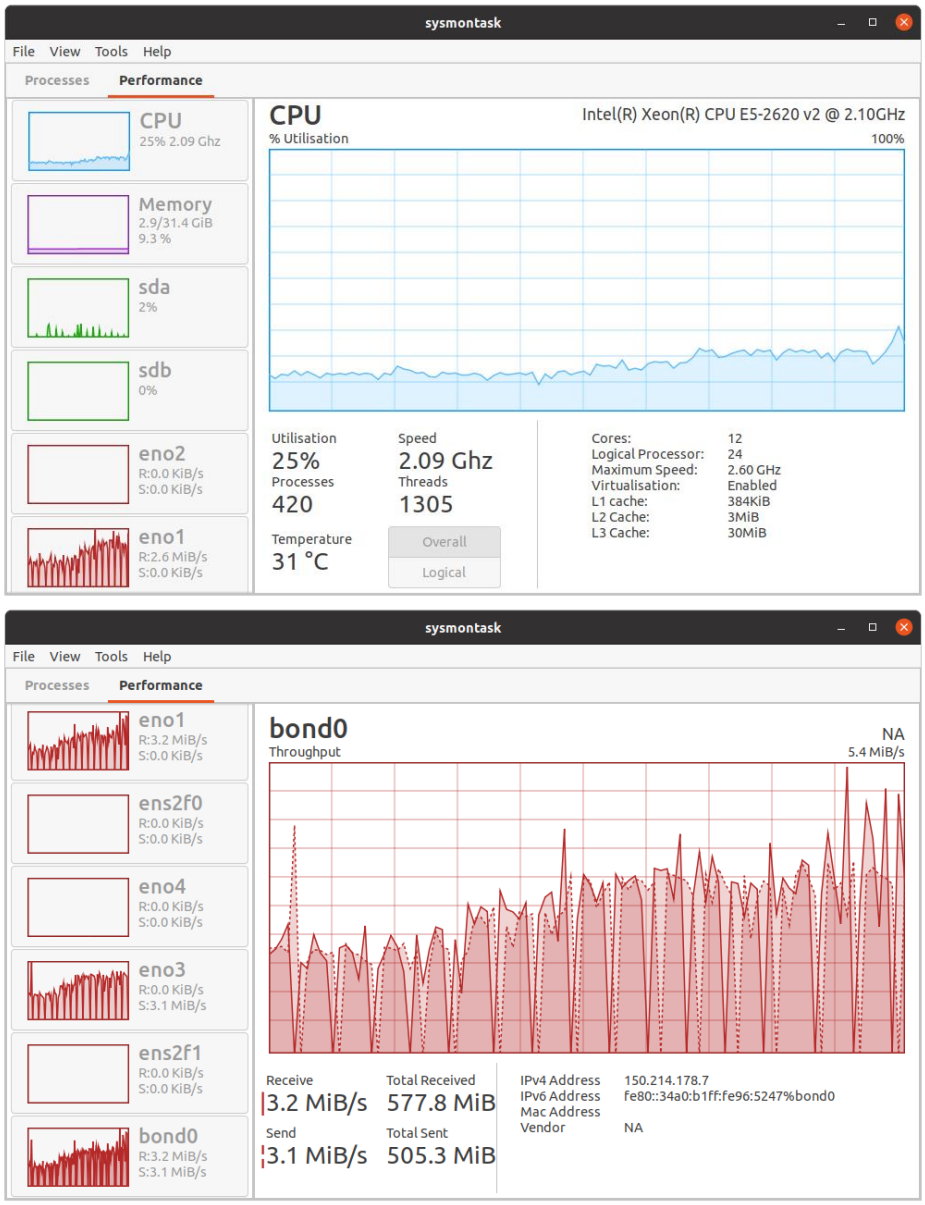

Ilustración 3.3. Recursos del sistema con 5 conexiones remotas simultáneas

- Recursos consumidos por 10 conexiones simultáneas:

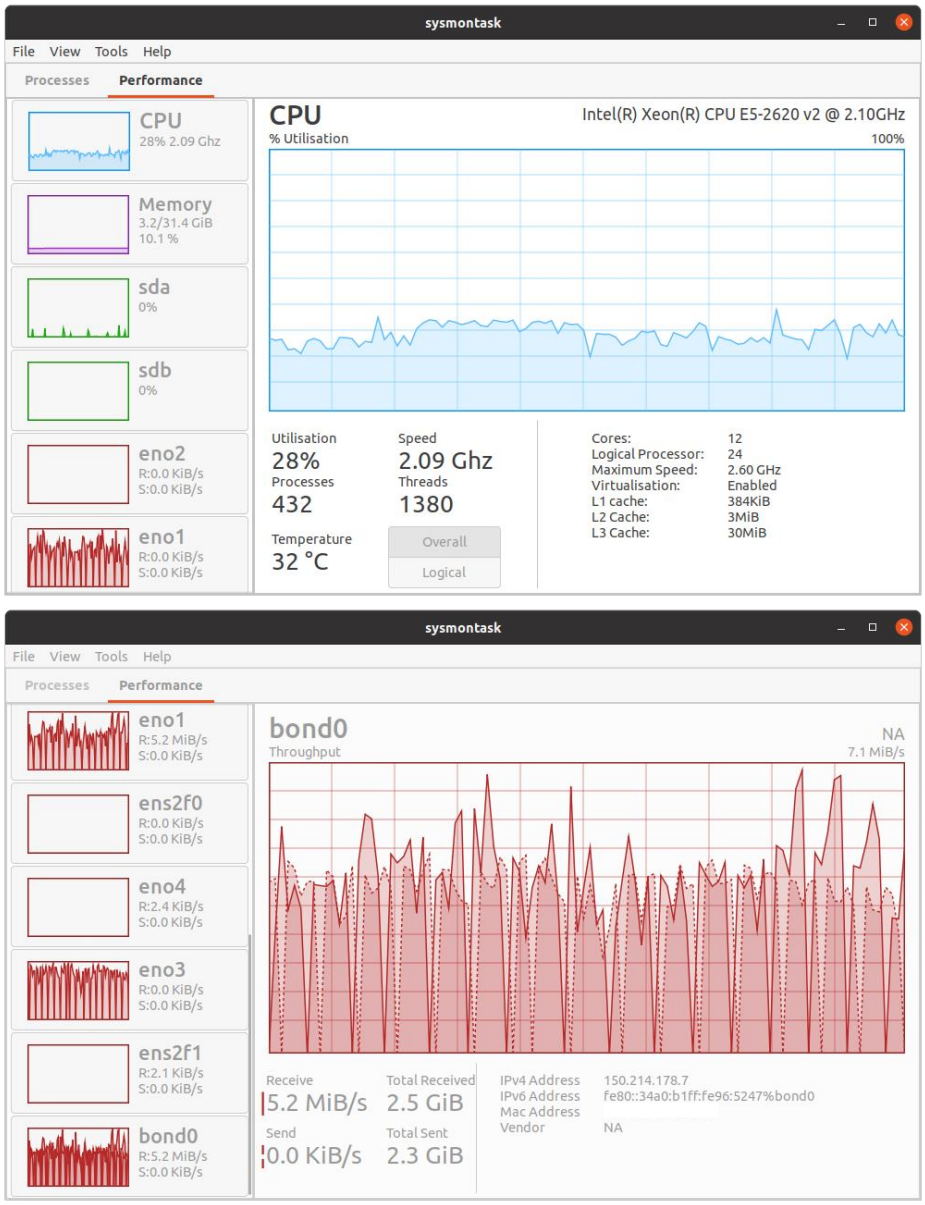

Ilustración 3.4. Recursos del sistema con 10 conexiones remotas simultáneas

Como se puede observar Guacamole no consume muchos recursos. Incluso con 10 conexiones remotas a la vez visualizando un video, el porcentaje de uso de la CPU no supera el 28%, y la memoria RAM apenas supera el 10%. Lógicamente, el tráfico de red es el dato más relevante ya que la transferencia de datos asciende a unos 7MiB/s que, convirtiéndolo a una velocidad de transferencia de datos más común, serían unos 60Mbps. No parece una velocidad alta tratándose de conexiones remotas con mucha carga gráfica, además de utilizar la interfaz bond0 sólo 2 de las tarjetas de red del servidor.

Por otro lado, evaluando la seguridad comprobamos los puertos que expone al exterior nuestro servidor una vez instalado y configurado con la ejecución de este comando:

```
ss –plnut
```

Siendo éste el resultado de los puertos abiertos: 22 (ssh), 53 (local), 4822 (local guacd), 8080 (local tomcat), 3306 (local mysql), 33060 (mysql), 80 y 443 (nginx). Es decir, sólo quedan expuestos los puertos estrictamente necesarios para el correcto funcionamiento de Apache Guacamole.

Como se puede consultar en el apéndice correspondiente al final del documento, el servidor web de la aplicación aplica más seguridad al tener instalado y configurado un certificado SSL para servir la aplicación web a través del protocolo HTTPS, encriptando la comunicación entre los navegadores de los usuarios y Apache Guacamole. A esto se le puede añadir las medidas de seguridad que ofrece la aplicación en cuanto a la autenticación de usuarios se refiere.

En resumen, podemos concluir con el gran rendimiento y usabilidad de Apache Guacamole y el bajo consumo de recursos del servidor, aportando la seguridad que este tipo de aplicaciones requiere por estar expuesta en Internet.

4 CONCLUSIONES Y TRABAJOS FUTUROS

Partiendo de la necesidad surgida e impuesta por la aparición del COVID19 y, analizado un conjunto representativo de todas las herramientas de conexión remota existentes en el mercado, podemos concluir que Apache Guacamole se trata de un software con muchas virtudes, que no sólo resuelve de manera sencilla el acceso remoto a las aulas de ordenadores, sino que también puede ser solución para ayudar a cualquiera empresa a implantar el teletrabajo, tan necesario en ocasiones y tan de moda en la época que vivimos.

En nuestro caso particular, Guacamole ofrece un acceso remoto seguro, sencillo, controlado y directo a los escritorios de cada uno de los 180 equipos ubicados en los laboratorios de prácticas del Departamento de Informática, permitiendo al alumnado desarrollar sus prácticas desde cualquier lugar con solo un navegador.

Además, se trata de una aplicación de software libre, lo que nos da la posibilidad de personalizar o añadir cualquier funcionalidad que mejore sus prestaciones actuales, pudiéndose ajustar aún más a las necesidades particulares de cada organización. Y como consecuencia de esto, podemos destacar como posibles mejoras a futuro las siguientes:

- Combinación de Apache Guacamole y un sistema cliente/servidor de VPN multiplataforma que nos permita conectar de forma más segura (mediante un túnel) a Internet o a los equipos remotos desde Microsoft Windows, GNU/Linux, MacOS, y por supuesto para Android y iOS en el caso de soluciones móviles.

- Con el objetivo de potenciar el uso de los laboratorios docentes en situaciones específicas y horarios especiales (por ejemplo, fuera del horario laboral o días no lectivos) se propone el desarrollo de una extensión de Apache Guacamole para gestionar reservas de sus puestos de trabajo. Esta funcionalidad se integraría en la interfaz web de la aplicación quedando reservado su uso a usuarios administradores. Cada reserva tendría un acceso limitado en el tiempo y con una clave única de acceso. Una vez finalizado el tiempo de reserva, la sesión finaliza automáticamente (desconectando al usuario) y se deshabilita la cuenta del usuario para impedir un nuevo acceso con esa clave.

5 APÉNDICES

5.1 Guía original del Trabajo Fin de Título

En este apartado se expone la propuesta de este TFG:

(Cód.: 21/22-3161) Evaluación de herramientas para la conexión remota de alumnado en modelos de docencia online

Tutor: RAFAEL JESÚS SEGURA SÁNCHEZ

Grado en Ingeniería Informática | Esp: Ingeniería del Software | Mención: General

Modalidad: Estudio Técnico | Tipo: TFG General

Número máximo de estudiantes: 1 (1 asignados)

Idioma: Castellano

La irrupción de la pandemia de COVID 19 ha provocado que las universidades y centros educativos deben adaptar en muy poco tiempo su docencia presencial hacia un modelo de docencia en la que el estudiante y el profesor se encuentran conectados de manera online, pero sin compartir el mismo espacio. Ello ya ha provocado que la realización de las prácticas en la mayoría de la disciplina, pero especialmente en el ámbito de la informática, hayan pasado por dificultades derivadas de la imposibilidad de que los estudiantes pudieran utilizar ciertas herramientas software, disponibles únicamente en los espacios educativos, aún a pesar de que el alumno contaba con los medios tecnológicos suficientes.

Este trabajo Fin de Grado pretende explorar las diferentes soluciones disponibles para realizar conexiones de escritorio remoto contra los ordenadores de los laboratorios de maneta que se garanticen elementos de seguridad y facilidad en la utilización de los recursos.

Conocimientos Previos

No tiene.

Objetivos del TFG

- Comprender los elementos de seguridad que deben mantenerse en organizaciones.
- Poner en práctica elementos implantaciones de software de servicio a través de Internet.
- Capacidad crítica del alumno/a la hora de evaluar entre diferentes alternativas de soluciones software.

Metodología a Desarrollar

- Revisión bibliográfica de soluciones.
- Análisis crítico de ventajas e inconvenientes de las diferentes herramientas seleccionadas.
- Implantación de prototipos de prueba.
- Evaluación de los prototipos implantados a partir de métricas comparables.
- Redacción de la memoria de resultados.

Documentos y Formatos de Entrega

- La memoria habrá de entregarse en PDF. Además, se entregará un disco con la instalación de las herramientas desarrolladas.

5.2 Manual de usuario

Apache Guacamole ofrece acceso a gran parte de la funcionalidad de un escritorio desde su navegador web, y tiene como objetivo convertirse en el medio principal para acceder a los escritorios, por lo que su interfaz debe ser lo más sencilla e intuitiva posible.

5.2.1 Pantalla de inicio

Una vez que el usuario inicie sesión, será llevado a la pantalla de inicio de Guacamole, donde se enumeran todas las conexiones disponibles, o directamente a una conexión, si solo tiene acceso a una conexión.

La pantalla de inicio contendrá una lista de todas las conexiones a las que tiene acceso (con un filtro para su búsqueda en el caso de tener muchas), junto con miniaturas de las conexiones activas o utilizadas recientemente.

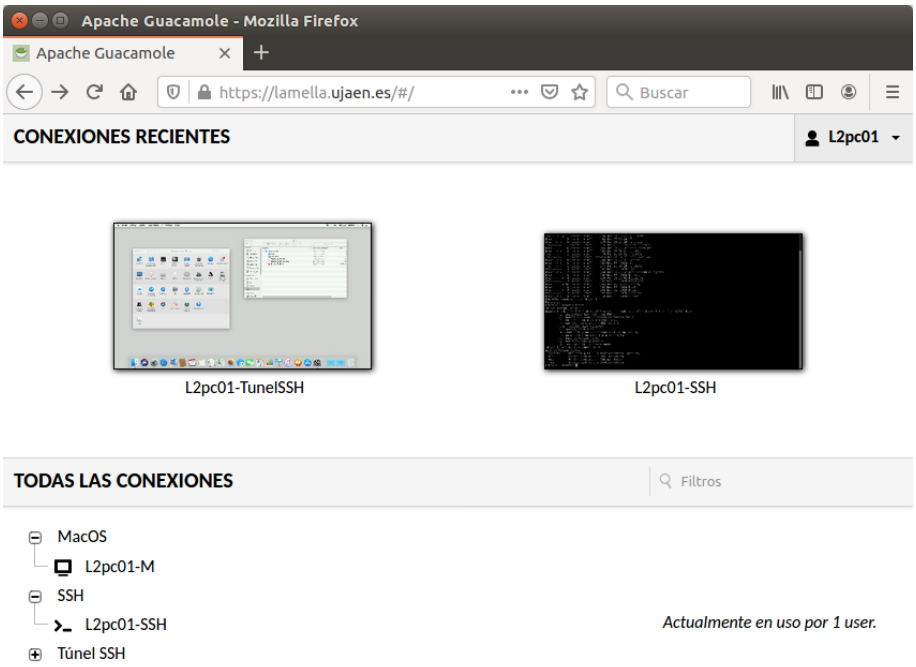

Ilustración 5.1. Pantalla de inicio de Apache Guacamole

Al hacer clic en cualquier conexión, se abrirá esa conexión dentro de la ventana o pestaña actual, pero se pueden usar varias conexiones simultáneamente. Puede volver fácilmente a la pantalla de inicio sin desconectarse usando el botón Atrás de su navegador o el botón "Inicio" en el menú Guacamole. Cada conexión que use permanecerá activa hasta que se desconecte explícitamente, o hasta que el usuario cierre su sesión.

5.2.1.1 Menú de usuario

A excepción de la pantalla del cliente cuando se abre una conexión, todas las pantallas de Guacamole contienen un menú en la esquina superior derecha llamado "menú de usuario". Este menú muestra su nombre de usuario y contiene varias opciones que dependen del nivel de acceso de su usuario:

- Inicio: para navegar de regreso a la pantalla de inicio (si sólo tiene acceso a una conexión, esta opción de menú se reemplaza con un enlace a esa conexión).

- Configuración: da acceso a las preferencias del usuario y, en el caso de tener acceso a funciones administrativas, también se encuentran dentro de la interfaz de configuración (que veremos más adelante).
- Cerrar sesión: supone el cierre de todas las conexiones actuales y finalizar la sesión de Guacamole.

5.2.2 Pantalla de cliente

Una vez que abra una conexión, veremos una vista en tiempo real de la pantalla remota. Puede interactuar con esta pantalla tal como lo haría con su escritorio normal. Su mouse y teclado funcionarán como si estuvieran conectados directamente a la máquina remota.

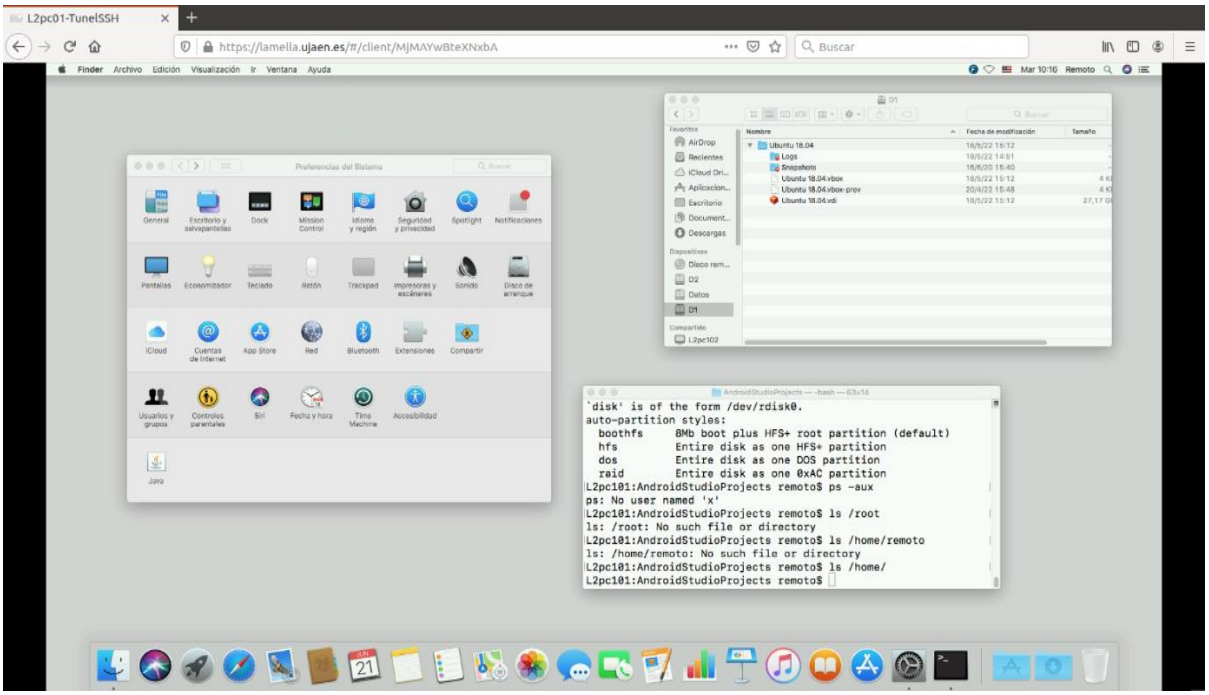

Ilustración 5.2. Pantalla de cliente de una conexión con Apache Guacamole

La pantalla remota ocupará toda la ventana del navegador, sin botones ni menús que perturben la vista. Con la intención de ofrecer una experiencia perfecta, las opciones específicas del escritorio remoto están ocultas dentro del menú Guacamole, que se puede abrir según sea necesario.

5.2.2.1 Menú de Guacamole

El menú Guacamole es una barra lateral que está oculta hasta que se muestra explícitamente. En un ordenador de escritorio (u otro dispositivo) con un teclado puede mostrar este menú presionando `Ctrl+Alt+Shift`. En cambio, si se utiliza un dispositivo móvil o de pantalla táctil que no tiene teclado, también es posible mostrar el menú deslizando el dedo hacia la derecha desde el borde izquierdo de la pantalla. Para ocultar el menú, presione nuevamente `Ctrl+Alt+Shift` o deslice hacia la izquierda en la pantalla.

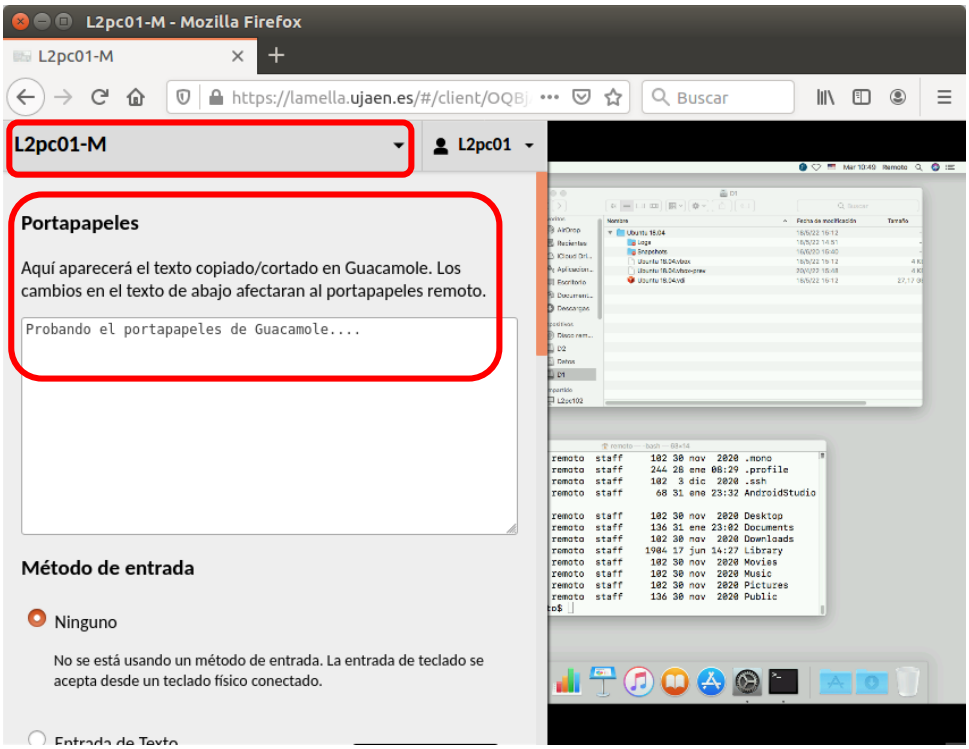

Ilustración 5.3. Menú Guacamole en una conexión

El menú Guacamole ofrece opciones para:

- Leer desde (y escribir en) el portapapeles del escritorio remoto. En la parte superior del menú Guacamole hay un área de texto llamada "portapapeles" que funciona como una interfaz entre el portapapeles remoto y el portapapeles local. El texto del portapapeles local se puede pegar en el área de texto, lo que hace que ese texto se envíe al portapapeles del escritorio remoto. De manera similar, si copia o corta texto dentro del escritorio remoto, verá ese texto dentro del área de texto y puede copiarlo manualmente en el portapapeles local si lo desea.

- Cambiar entre conexiones activas y mostrar varias conexiones a la vez. Si tiene acceso a más de una conexión, al hacer clic en el nombre de la conexión actual en la parte superior del menú Guacamole se abrirá un menú desplegable que contiene una lista de sus otras conexiones disponibles. Se podrá cambiar de conexión o, también, mostrar varias conexiones simultáneamente que se irán organizando automáticamente en mosaicos de igual tamaño que llenen el área disponible.

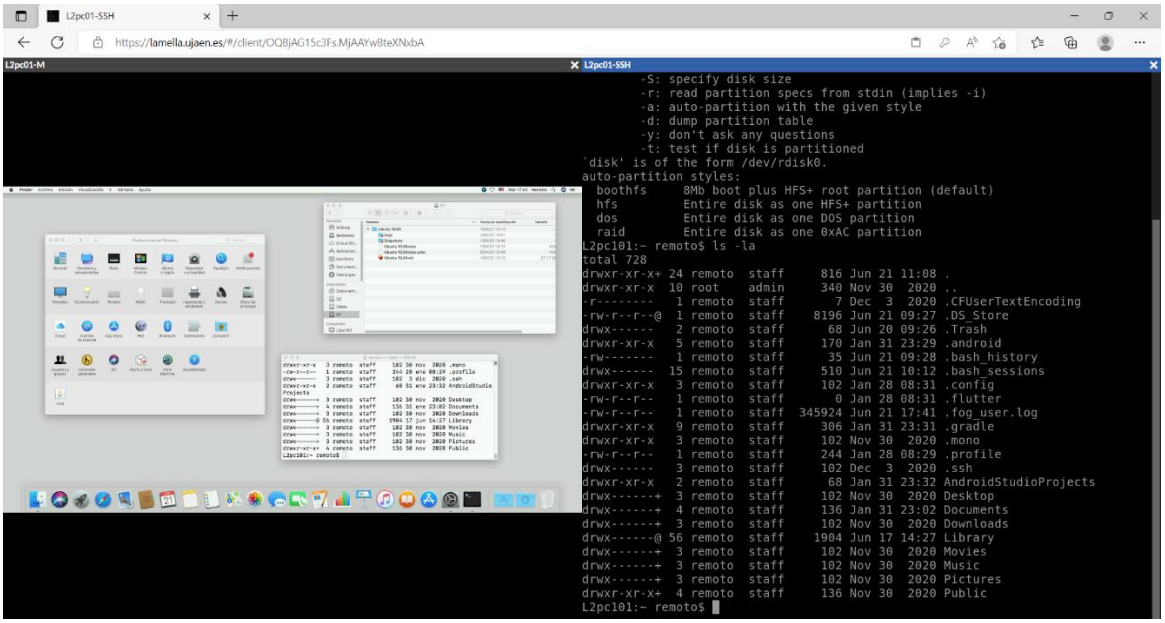

Ilustración 5.4. Mostrando varias conexiones simultaneas

- Navegación a la pantalla de inicio.
- Desconectarse completamente de la conexión actual. El menú de usuario dentro del menú Guacamole proporciona una opción adicional de "Desconectar" que le permite cerrar explícitamente sólo la conexión actual. Al hacer clic en "Cerrar sesión", también se desconectarán implícitamente todas las conexiones activas, incluida la conexión actual. En el caso de navegar de regreso a la pantalla de inicio o a la pantalla de configuración no se desconectarán, continuarán ejecutándose en segundo plano dichas conexiones.

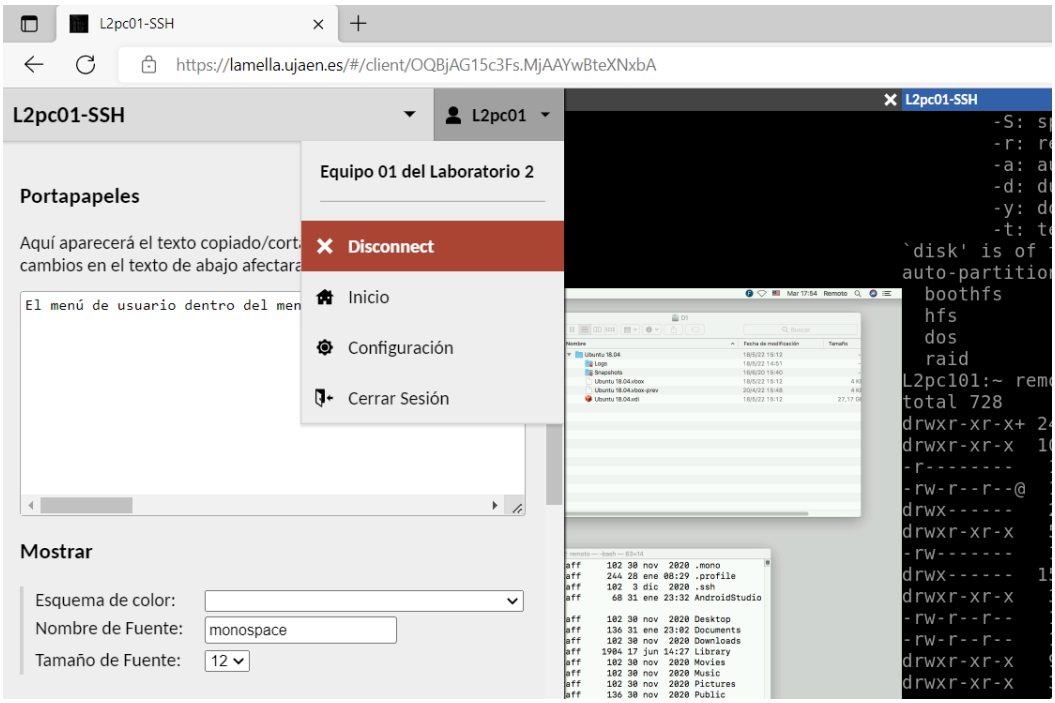

Ilustración 5.5. Desconectar la conexión actual

- Compartir la conexión actual. Si el servidor de Guacamole está configurado para permitir compartir la conexión y se le ha otorgado permiso para compartir la conexión actual, aparecerá un menú adicional "Compartir" junto a su nombre de usuario en el menú de Guacamole. Con esta opción se genera un enlace compartido único que se puede distribuir a cualquier persona, incluso a usuarios que no tienen cuentas en Guacamole, para ofrecer un acceso temporal a su conexión. Una vez que se cierra la conexión, el enlace deja de ser válido y todos los usuarios que compartan la conexión son automáticamente desconectados.
- Transferencia de archivos. Es posible transferir archivos de un lado a otro entre su ordenador local y el escritorio remoto si es compatible con el protocolo subyacente y está habilitado en la conexión. Actualmente, Guacamole admite la transferencia de archivos para VNC, RDP y SSH, ya sea mediante el soporte nativo de transferencia de archivos del protocolo o SFTP.
- Escalar la pantalla remota. Guacamole por defecto reducirá o expandirá la pantalla remota para que se ajuste exactamente a la ventana del navegador, pero esto no es necesariamente lo ideal, sobre todo si hablamos de

dispositivos móviles. Se puede escalar la pantalla en dispositivos táctiles mediante el conocido gesto de pellizcar o, si su dispositivo no tiene una pantalla táctil, también se puede controlar el nivel de zoom con los controles que se encuentran en la parte inferior del menú.

- Métodos alternativos para escribir o controlar el ratón, particularmente para usar en dispositivos móviles o con pantalla táctil.

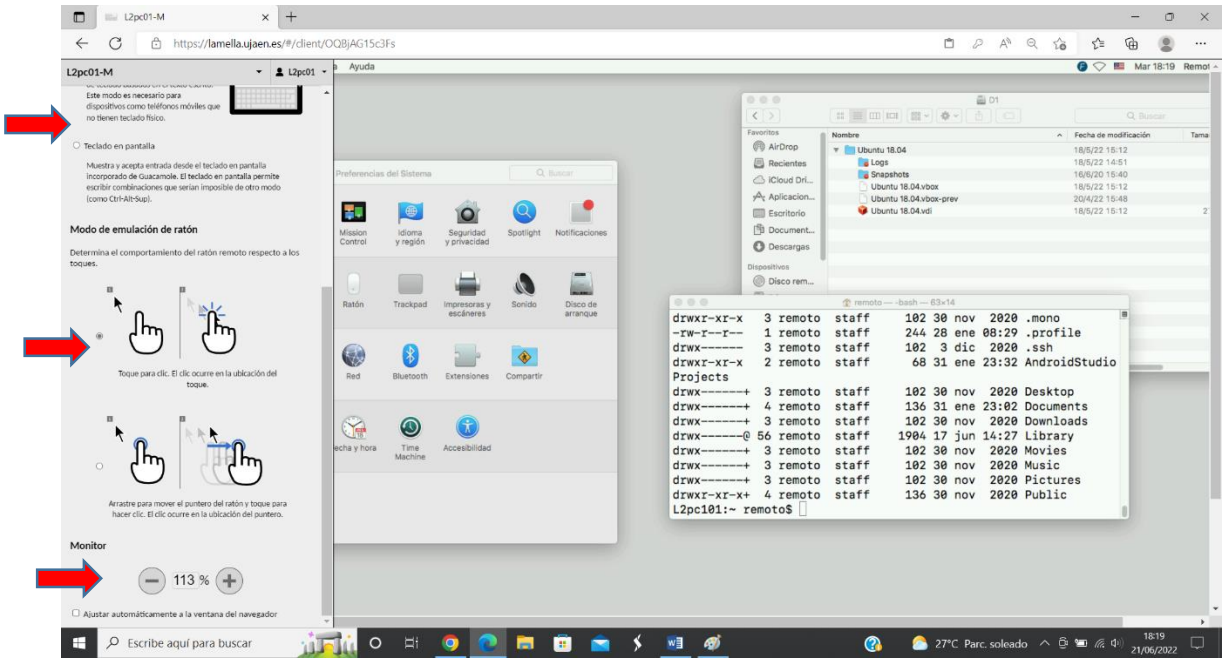

Ilustración 5.6. Opciones del menú Guacamole

5.2.3 Preferencias del usuario

Se pueden cambiar en la opción de configuración (en el menú de usuario). Estas preferencias se almacenan localmente dentro del navegador, por lo que, si se accede a Guacamole desde distintos dispositivos, puede tener diferentes configuraciones para cada ubicación. La pantalla de configuración permite a los usuarios cambiar el idioma de la interfaz de Guacamole, cambiar el método de entrada predeterminado utilizado por las conexiones de Guacamole y cambiar el modo de emulación del ratón predeterminado si se usa un dispositivo táctil. Si tiene suficientes permisos, también puede cambiar su contraseña (los administradores del sistema pueden restringir la capacidad de los usuarios individuales para cambiar sus propias contraseñas) o administrar el sistema.

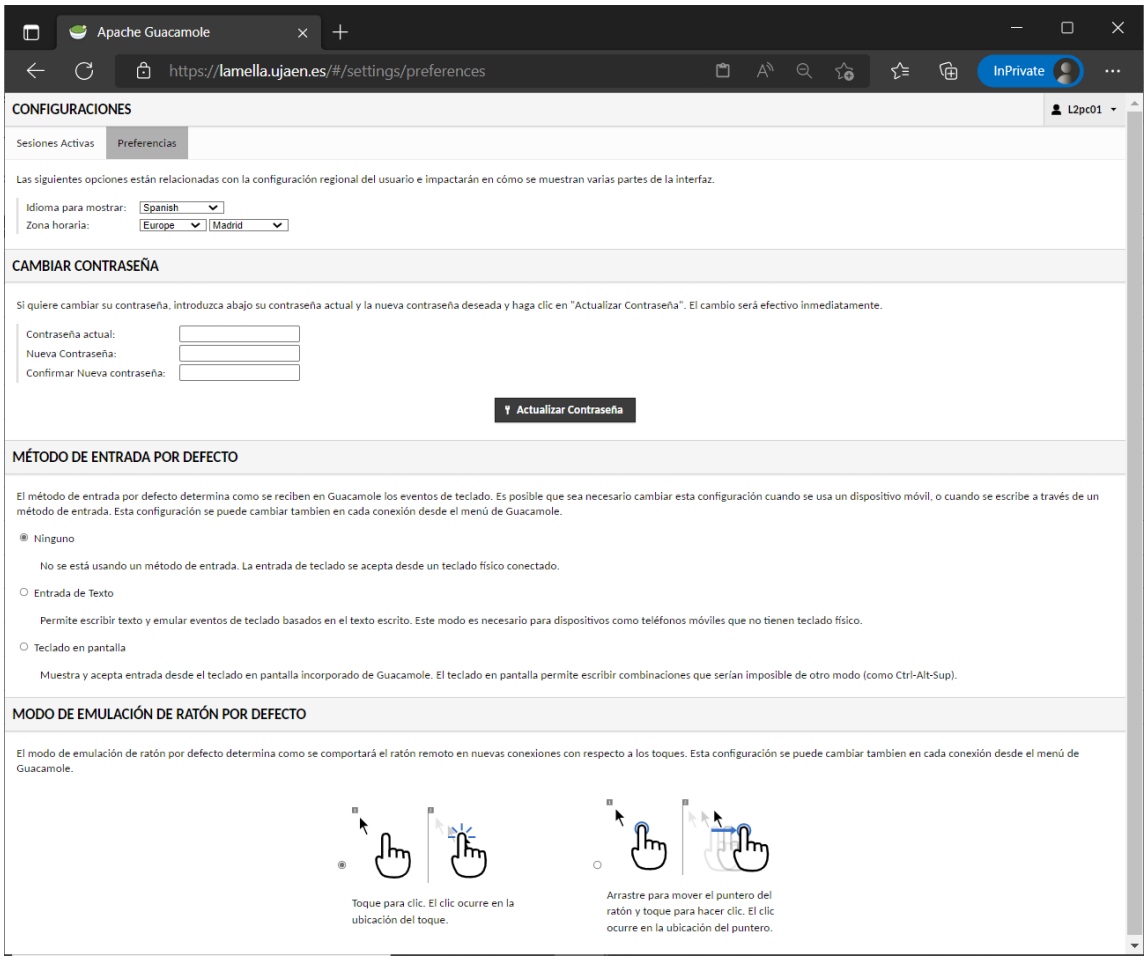

Ilustración 5.7. Preferencias del usuario

5.2.4 Administración

Los usuarios, grupos de usuarios, conexiones y sesiones activas se pueden administrar desde la interfaz web si el módulo de autenticación lo admite, actualmente sólo en el caso de autenticación a través de base de datos. Es decir, si está configurado el mecanismo de autenticación predeterminado (que lee todos los usuarios y conexiones del archivo `user-mapping.xml`) u otra extensión de autenticación, estas opciones de administración no estarán visibles en la interfaz de Guacamole.

Partiendo del caso de tener configurado uno de los proveedores de autenticación de la base de datos, si se inicia sesión como un usuario con suficientes privilegios, se podrán ver las secciones de administración enumeradas en la pantalla de configuración (además del apartado, ya comentado, de preferencias del usuario):

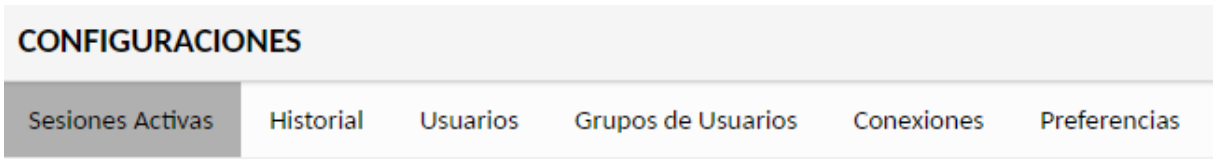

Ilustración 5.8. Opciones de administración en Guacamole

5.2.4.1 Administrar sesiones

En la pestaña "Sesiones activas" se muestra la pantalla de administración de sesiones. Ésta muestra todas las sesiones activas y permite a los administradores del sistema eliminarlas según sea necesario.

Cuando cualquier usuario accede a una conexión de escritorio remoto en particular, se crea una sesión única y aparecerá en la lista de sesiones activas en esta pantalla de administración de sesiones. Cada sesión activa muestra como información el nombre de usuario del usuario correspondiente, cuánto tiempo ha estado activa la sesión, la dirección IP de la máquina desde la que se conecta el usuario y el nombre de la conexión que se está utilizando. La información de esta tabla se puede reordenar simplemente haciendo clic en los encabezados de las columnas o ser filtrada introduciendo algún criterio de búsqueda con el campo específico para ello.

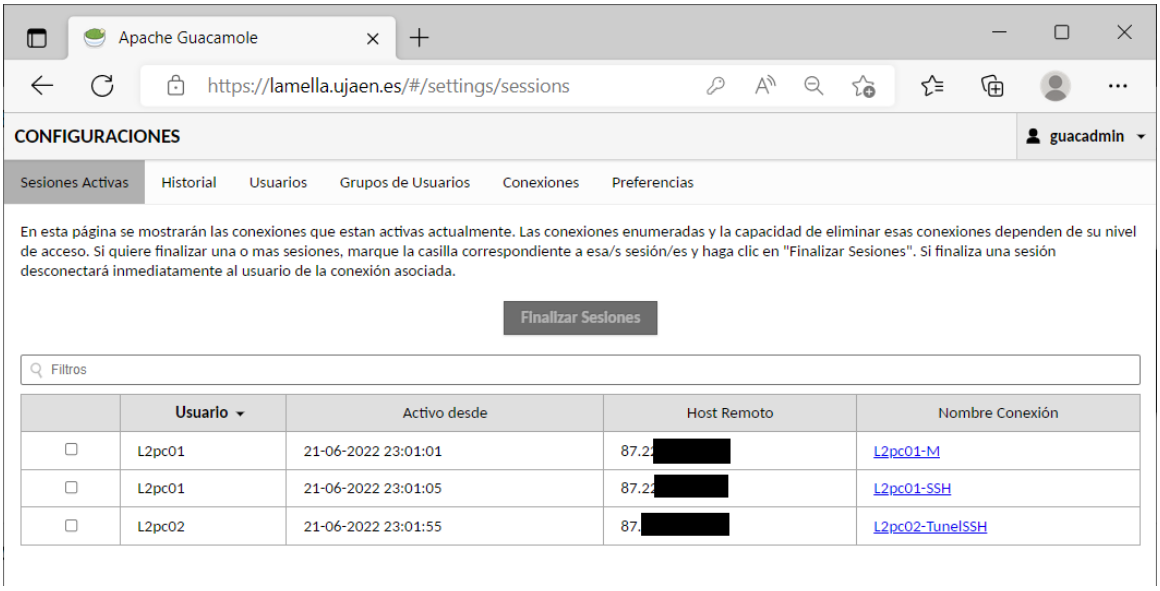

Ilustración 5.9. Sesiones activas en Apache Guacamole

Para eliminar una o más sesiones, hay que marcarlas haciendo clic en sus casillas de verificación. Una vez seleccionadas todas las sesiones a eliminar,

pulsamos en el botón "Finalizar sesiones", y el sistema desconectará inmediatamente a esos usuarios de la conexión asociada.

5.2.4.2 Historial de conexiones

La pantalla del historial de conexiones muestra una tabla de las conexiones más recientes, incluido el usuario que usó esa conexión, la hora en que comenzó la conexión y cuánto tiempo se usó.

Al igual que con la tabla de sesiones activas descrita anteriormente, la tabla de registros históricos se puede reordenar haciendo clic en los encabezados de las columnas o filtrar ingresando términos de búsqueda en el campo "Filtro".

5.2.4.3 Gestión de usuarios

Éste es un apartado de administración destacado ya que aquí podemos agregar nuevos usuarios, editar las propiedades y los privilegios de los usuarios existentes y ver las veces que cada usuario inició sesión por última vez. Si hay muchos usuarios creados en el sistema, también se podrá filtrar en la lista introduciendo términos de búsqueda por nombre de usuario dentro del campo "Filtro".

Para agregar un nuevo usuario, hacemos clic en el botón "Nuevo usuario". Esto nos llevará a una pantalla donde se podrá introducir los datos del nuevo usuario:

- Nombre de usuario y contraseña
- Datos del perfil: nombre completo, correo electrónico, organización y puesto.
- Restricciones de la cuenta. Todas ellas relacionadas con el acceso a la aplicación: deshabilitar la cuenta de usuario, obligar a modificar la contraseña en el siguiente inicio de sesión, permitir o no el acceso después de una hora / fecha determinadas.
- Permisos. Aquí se configuran los permisos administrativos del usuario: si puede crear nuevos usuarios, nuevos grupos, conexiones … o, incluso, si puede modificar su propia contraseña.
- Grupos. Establece los grupos de usuarios a los que pertenece el propio usuario.
- Conexiones. Habilita las conexiones a las que el usuario va a tener acceso.

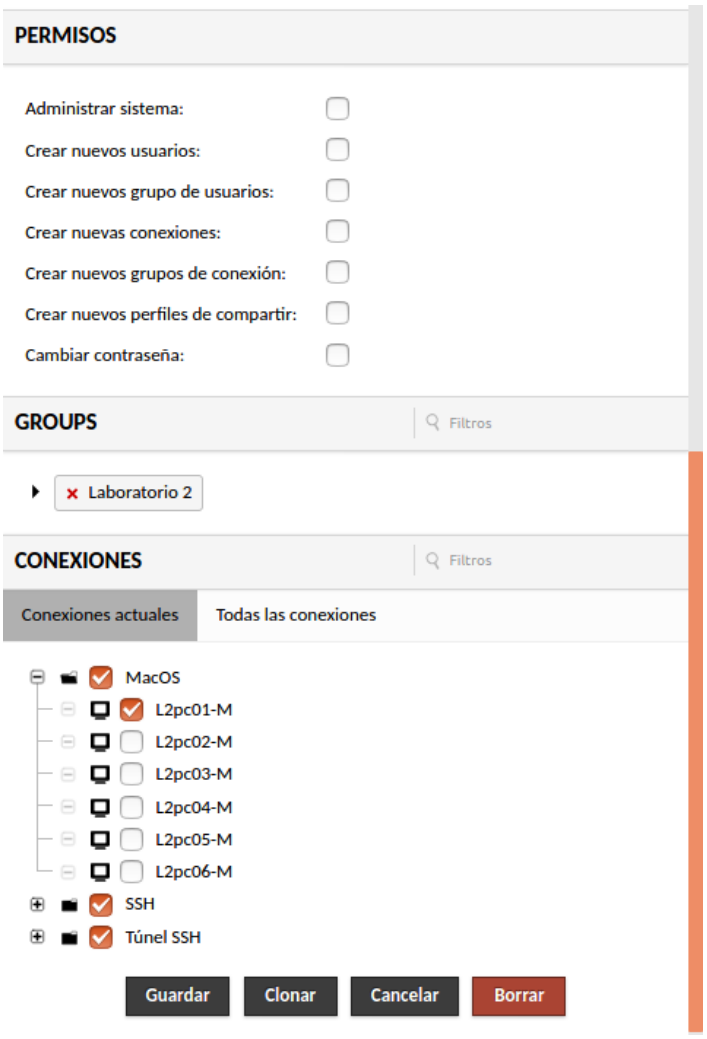

Ilustración 5.10. Interfaz de los usuarios de Apache Guacamole

Si se administra una gran cantidad de conexiones o grupos y, queremos reducir el tamaño de la lista que se muestra, podemos hacerlo especificando los términos de búsqueda en el campo "Filtro".

Si tiene permiso de eliminación en el usuario, también se verá un botón "Borrar". Al hacer clic en este botón, se eliminará permanentemente al usuario. Alternativamente, si sólo desea deshabilitar temporalmente la cuenta, habría que marcar "Inicio de sesión deshabilitado" y se logrará el mismo efecto sin eliminar al usuario por completo. Si el usuario intenta iniciar sesión, el intento será rechazado como si su cuenta no existiera.

5.2.4.4 Gestión de grupos de usuarios

Una de las formas más cómodas para gestionar los usuarios y sus permisos (en caso de que vayamos a tener más de un usuario y con diferentes permisos) son los grupos.

Pinchando en "Grupos" dentro de la lista de secciones de configuración, se accede a la pantalla de administración de grupos de usuarios. Desde esta pantalla puede agregar nuevos grupos y editar las propiedades y privilegios de los grupos ya existentes. Al igual que las anteriores interfaces, si tiene una gran cantidad de grupos de usuarios, también puede ingresar términos de búsqueda dentro del campo "Filtro" para filtrar la lista de grupos por nombre.

Ilustración 5.11. Grupos de usuarios en Apache Guacamole

Para crear o editar un grupo de usuarios, hacemos clic en el botón "Nuevo grupo" o pulsamos sobre el nombre del grupo ya existente. Esto nos lleva a una pantalla donde se permitirá configurar los detalles del grupo:

- Miembros del grupo.
- Permisos administrativos: se trata de los mismos permisos que tenemos a nivel de usuario.
- Agregar o quitar acceso a conexiones específicas (de la misma forma que a nivel de usuario).

- Compartir perfiles o grupos de conexión.
- Pertenencia del grupo a otros grupos.

Para eliminar de forma definitiva un grupo hay un botón específico para ello y, opcionalmente, existe también la posibilidad de deshabilitarlo temporalmente marcando en "Deshabilitado". Esta última opción logra el mismo efecto (sus miembros dejan de tener los permisos y acceso a las conexiones correspondientes), pero sin eliminar el grupo por completo.

Por último, hay que tener en cuenta que la extensión de autenticación de la base de datos implementa herencia recursiva completa de los permisos de grupo, es decir, los permisos establecidos a un grupo se otorgan a todos los miembros/descendientes de ese grupo.

5.2.4.5 Conexiones y grupos de conexiones

Las conexiones son, junto con los usuarios, parte fundamental de la configuración para el acceso remoto a los equipos. Al definir una conexión se establece el protocolo a usar para la conexión, nombre o dirección IP del equipo destino, puerto de conexión, datos de autenticación en el sistema, etc.

Por otro lado, existen también los grupos de conexiones que pueden ser "organizativos" o "de equilibrio". Cada grupo puede contener cualquier número de otras conexiones o grupos, pero la semántica del grupo cambia según el tipo:

- Un grupo organizacional se comporta exactamente como una carpeta o directorio en un sistema de archivos. Simplemente contiene conexiones y otros grupos, pero no proporciona ningún otro comportamiento.
- Un grupo de equilibrio se comporta como una conexión. Equilibra dinámicamente la carga entre las conexiones que contiene, eligiendo la conexión con la menor cantidad de usuarios activos. A diferencia de los grupos organizativos, al hacer clic en un grupo de equilibrio se abre una nueva conexión.

La pantalla de administración de conexiones permite a los administradores crear y editar conexiones, compartir perfiles y grupos de conexiones. Si hay definidas una cantidad alta de conexiones, también podemos filtrar en la lista por nombre o protocolo de la conexión.

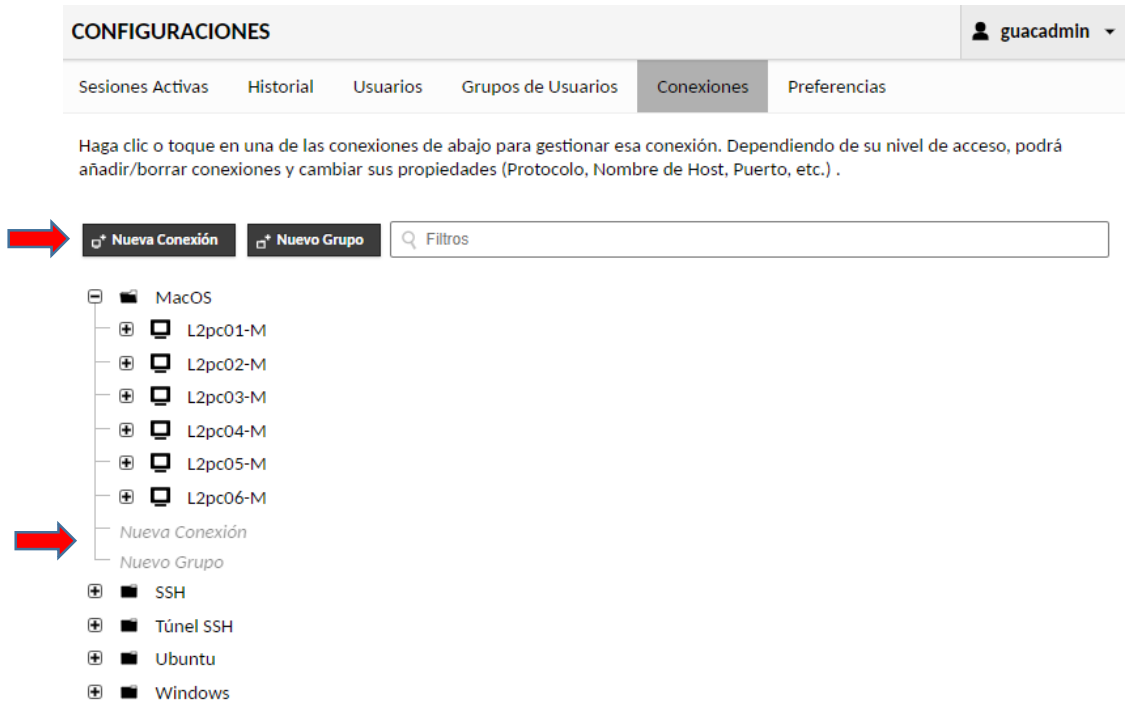

Ilustración 5.12. Conexiones en Apache Guacamole

Para crear una nueva conexión o grupo de conexiones, hacemos clic en el botón "Nueva conexión" o "Nuevo grupo", o en los marcadores de posición "Nueva conexión" o "Nuevo grupo" que aparecen cuando expande un grupo de conexiones existente. Estas opciones nos llevan a una pantalla donde se indican los detalles del nuevo objeto, como su ubicación dentro de algún grupo, parámetros y nombre. Este nombre debe ser descriptivo, pero también debe ser único con respecto a otros objetos en la misma ubicación.

Los parámetros de una conexión varían según el tipo de protocolo indicado al completar el formulario. Aunque hay ciertos datos fijos para cualquier conexión, la interfaz adapta el formulario para que se soliciten los parámetros correctos según el tipo de protocolo de la conexión.

Los campos fijos del formulario de una conexión son:

- Nombre, Ubicación (para encasillar dentro de algún grupo de conexiones) y protocolo. Estos 3 datos son obligatorios para crear una nueva conexión.
- Límites de concurrencia, en el que podemos establecer un número máximo de conexiones con el mismo usuario, o en general.
- Balanceo de carga, indicando el peso de la conexión para configuraciones con balanceo de carga.

- Parámetros del proxy de guacamole (guacd), en el caso de que está ubicado en otro equipo diferente al de la aplicación web.

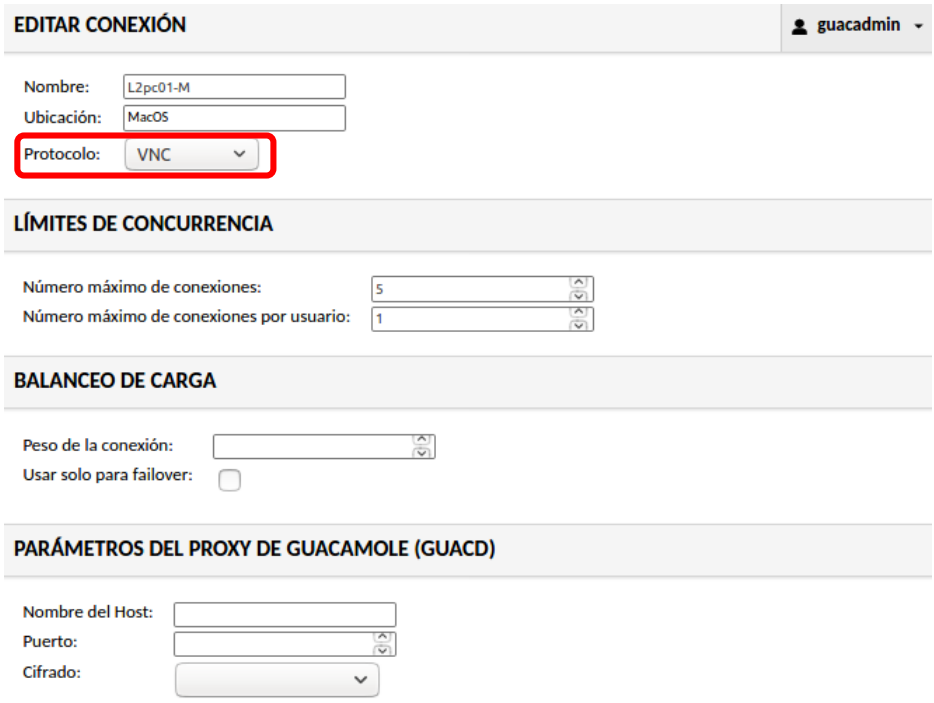

Ilustración 5.13. Formulario de una conexión en Apache Guacamole

Para completar una conexión hay que indicar también la información específica y relativa al protocolo seleccionado en esta primera parte del formulario. Por ejemplo, para una conexión a través de VNC se solicita la siguiente información:

- Red: nombre o IP del equipo al que queremos conectar y el puerto de conexión. Estos datos son obligatorios.
- Autenticación: usuario y contraseña para iniciar sesión de forma automática en el sistema operativo del equipo destino. Si no se rellena esta información nos la solicitará al iniciar la conexión.
- Monitor: aquí podemos indicar si la conexión es de sólo lectura (es decir, no permitirá operar en el equipo destino) profundidad de color, etc.
- Portapapeles: opciones de configuración del portapapeles.
- Repetidor VNC.

- Grabación pantalla: en el caso de grabar la sesión habría que completar estos datos. Para poder ver el video de la grabación, tendremos que codificar el archivo. Este es el comando para la codificación en .m4v:

```
guacenc [-s ANCHOxALTO] [-r BITRATE] [-f] [ARCHIVO]...
```

- SFTP: información para habilitar la transferencia segura de archivos.
- Audio: permite redireccionar el audio del equipo remoto y poder escuchar cualquier audio a través de nuestra conexión.
- Wake-on-Lan (WoL): en este apartado se encuentran los campos necesarios para configurar la conexión y poder “levantar” el equipo remoto al iniciar una conexión (si está suspendido o apagado).

Una vez cumplimentados estos datos (conexión o grupo de conexiones) hacemos clic en "Guardar" para crear el nuevo objeto, pero inicialmente solo lo podrán usar los administradores y su usuario actual. Para otorgar acceso a otro usuario a la nueva conexión o grupo de conexiones, debe editar ese usuario o un grupo de usuarios del que el usuario sea miembro, marcando la casilla correspondiente a la conexión o grupo de conexiones recién creada.

5.2.4.6 Compartir conexión

Teniendo Guacamole configurado con autenticación a través de base de datos, a partir de una conexión definida existe la posibilidad de compartir esta conexión a través de un enlace que podrá ser utilizado por cualquiera y sin necesidad de tener una cuenta en el sistema de Apache Guacamole.

Para esto se crea un perfil compartido para una conexión concreta. A diferencia de las conexiones y los grupos, en la pantalla de administración de conexiones no existe el botón "Nuevo perfil compartido". Los perfiles de uso compartido se crean haciendo clic en los marcadores de posición "Nuevo perfil de uso compartido" que aparecen cuando se expanden las conexiones. Así como expandir un grupo de conexiones revela las conexiones o grupos que contiene, expandir una conexión revela los perfiles compartidos asociados con esa conexión. Esto es válido tanto para la lista de conexiones en la pantalla de administración de conexiones como para la lista de conexiones en la edición de usuarios.

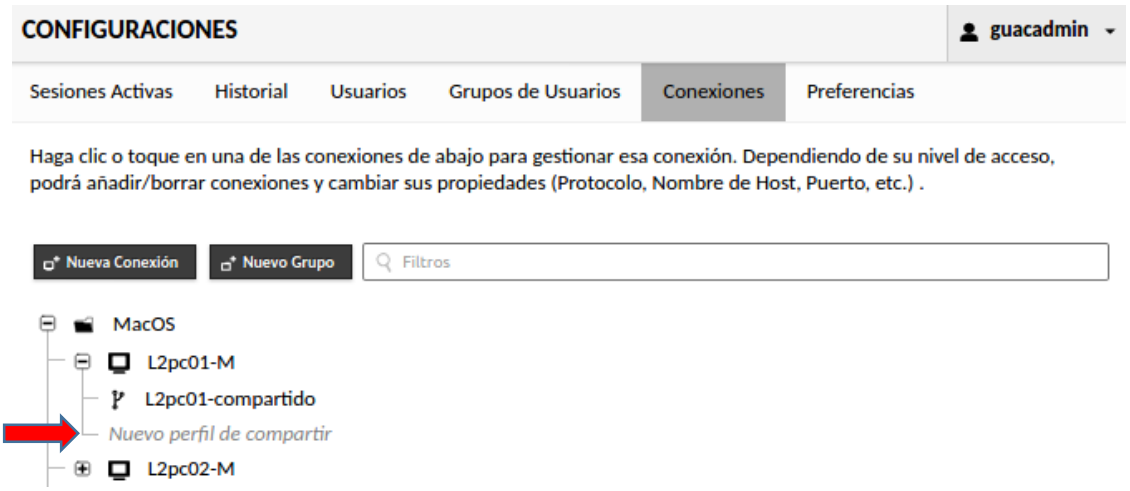

Ilustración 5.14. Conexiones y perfiles compartidos en Apache Guacamole

Al crear un nuevo perfil simplemente se solicita un nombre y el nivel de acceso que obtendrá usando este perfil: sólo lectura o acceso normal.

Ilustración 5.15. Nuevo perfil para compartir conexión en Apache Guacamole

Como último paso, los usuarios con acceso tanto a esa conexión como a ese perfil compartido podrán compartir la conexión con otros usuarios generando enlaces para compartir la conexión como se muestra en la siguiente imagen:

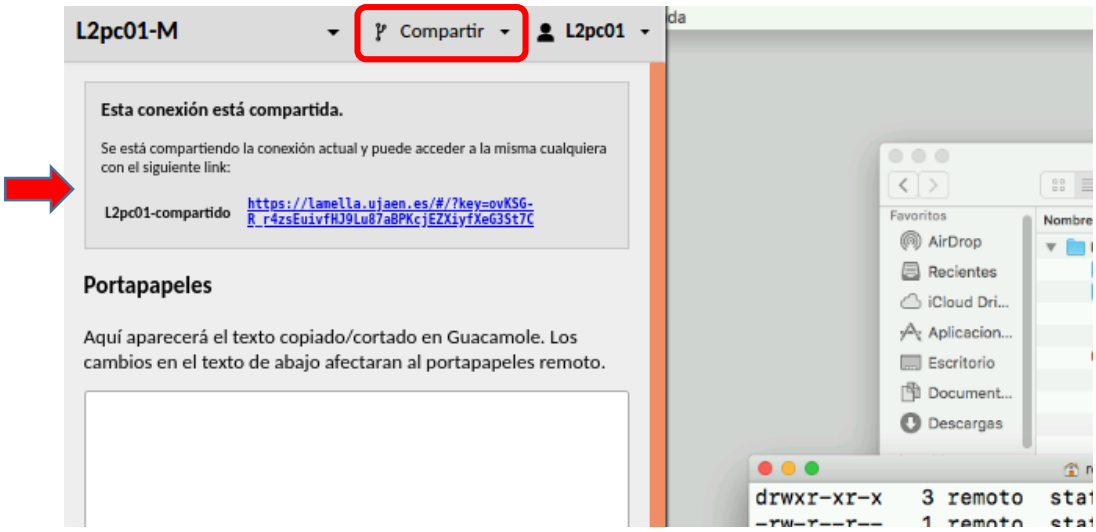

Ilustración 5.16. Compartir una conexión en Apache Guacamole

5.2.4.7 Configuración aplicada para el Departamento de Informática

Una vez descritas las diferentes secciones de la administración de Guacamole, este apartado describe un posible planteamiento para el uso de Guacamole como herramienta de conexión remota en el caso particular de los laboratorios docentes del Departamento de Informática de la Universidad de Jaén:

- Conexiones: Se agregará una conexión específica por cada sistema operativo de cada puesto de trabajo (Windows 10, Ubuntu 20.04 y MacOS High Sierra) con esta información:
  - Nombre LXpcNN-S: donde X es el número del laboratorio, NN es el número de puesto y S es el sistema operativo (W-Windows 10, U-Ubuntu 20.04 y M-MacOSx). Con esta nomenclatura se sabrá claramente a qué equipo y qué sistema se refiere cada conexión, y también facilitará las búsquedas utilizando el filtro de la pantalla de administración de las conexiones. Por ejemplo, L4pc06-U sería la conexión para Ubuntu del equipo número 6 del laboratorio 4.
  - Ubicación: indicará grupo de conexiones al que pertenece y que han sido creadas previamente (sólo se usará por tema organizativo).
  - Protocolo: VNC, RDP o SSH.
  - Nombre del host (o dirección IP interna del equipo): 192.168.XX.YYY, donde XX es la subred interna del laboratorio del equipo e YYY es el

número de puesto empezando por el 101 hasta el 130. Por ejemplo, la dirección IP 192.168.37.124 es el puesto número 24 del laboratorio 3.

- Puerto de conexión (según protocolo): 5900 (VNC), 3389 (RDP), 22 (SSH).
- Datos de autenticación en el sistema operativo: nombre, contraseña, etc.

En el caso particular del Laboratorio número 2 (aula Mac), que sólo tiene un sistema operativo, a parte de la conexión a su sistema MacOSx se definen 2 conexiones más por equipo:

- SSH: sólo hay 2 cambios con respecto a lo anterior (protocolo y puerto).
- Túnel SSH: esta conexión accede al equipo de forma gráfica a través VNC (no a la terminal) pero utilizando un túnel SSH. Esto encripta la comunicación entre el servidor Guacamole y el equipo, aplicando más seguridad a la conexión remota (aunque en el caso del Departamento de Informática no sería necesaria ya que ambos extremos de la comunicación están dentro de la red corporativa de la Universidad de Jaén). Para configurar esta conexión hay que realizar estos pasos:
  - Creación automática de un túnel SSH desde el servidor a cada uno de los equipos del laboratorio. Para ello:
    - Permitir el acceso por SSH.
    - Instalación de un par de claves pública y privada en el servidor de Guacamole y montar esta clave pública en los equipos destino. Esto hará que en la creación del túnel no se solicite la contraseña del usuario del sistema al que conecta por SSH.
    - Creación de un túnel SSH, y para que éste sea permanente y se cree al iniciar el sistema, usamos la utilidad “autossh” y, configuramos y habilitamos un

servicio systemd parametrizado que haga uso de autossh para crear el túnel SSH de cada puesto de trabajo del laboratorio 2. Es decir, iniciamos y habilitamos el mismo servicio por cada equipo indicando el número de puesto. Ejemplo del puesto 3:

```
systemctl start autossh-tunnel@3.service
systemctl enable autossh-tunnel@3.service
```

- En la creación de la conexión en Apache Guacamole tener en cuenta estas modificaciones:
  - Protocolo: VNC.
  - Nombre del host: localhost.
  - Puerto: 59XX, donde XX es el número del equipo del laboratorio docente.

  Esta configuración es debida a que el túnel SSH que genera el servicio del sistema comentado anteriormente, se crea desde el propio servidor (Localhost) por el puerto 59XX al puerto 5900 del equipo 192.168.38.1XX.

- Grupos de conexiones: se crea un grupo por cada tipo de conexión simplemente por temas organizativos y orden en la pantalla de administración (Windows, Ubuntu, MacOS…).
- Usuarios. Podríamos clasificar en 3 tipos los usuarios a definir:
  - Administrador (guacadmin): es el usuario principal con todos los privilegios de administración de Guacamole. Tiene acceso a todas las conexiones, administra todas las sesiones activas, crea, modifica y elimina los usuarios, conexiones, grupos… Se mantiene su configuración por defecto simplemente cambiamos su contraseña.
  - Puestos de trabajo: se crea un usuario por cada uno de los puestos de trabajo de los laboratorios docentes, todos ellos usando la misma nomenclatura LXpcNN (donde X es el número de laboratorio y NN el número de puesto). Esta manera de nombrar los usuarios nos

permitirá filtrar de forma sencilla, por ejemplo, los usuarios de un laboratorio concreto. Todos estos usuarios se definen sin ningún privilegio de administración y seleccionando sus conexiones correspondientes a su puesto. Así, cuando un alumno inicie sesión en Guacamole con el usuario de un puesto de trabajo se mostrará en pantalla todas las conexiones establecidas para conectar con los distintos sistemas operativos de ese puesto específico.

    - Laboratorios: usuario idéntico al anterior con la diferencia de que puede acceder a todos los equipos de un laboratorio concreto. Es decir, tiene configuradas todas las conexiones correspondientes a todos los puestos de trabajo de un laboratorio. Este tipo de usuario estaría pensado para el uso de los profesores y les permitiría conectarse en cualquier momento al equipo que lo requiera del laboratorio o finalizar sus sesiones.

- Grupos de usuarios. Se crea un grupo por cada laboratorio para gestionar de forma más cómoda los permisos administrativos de los usuarios del mismo, agregar conexiones, perfiles o grupos de conexión. También se crea otro grupo específico para los usuarios de los profesores que serían los usuarios de tipo laboratorio comentados anteriormente.

5.3 Instalación de un certificado SSL

Para darle una capa más de seguridad, habría que encriptar la comunicación entre los navegadores de los usuarios y Apache Guacamole. Esto implica instalar un proxy inverso como Nginx para configurar SSL y servir nuestra aplicación web a través de HTTPS. Un proxy inverso es un servidor que se sitúa delante de los servidores web y reenvía las solicitudes del cliente (por ejemplo, el navegador web) a esos servidores web. Suelen implementarse para ayudar a aumentar la seguridad, el rendimiento y la fiabilidad.

En Guacamole, el puerto de Tomcat por defecto es el 8080 pero para cambiar este puerto para que la aplicación web responda en el 80 (http) y el 443 (https) hay un problema: los puertos por debajo de 1024 en sistemas Linux son puertos que sólo pueden ser usados por usuarios con privilegios como `root`. Como solución, al igual

que la mayoría de las aplicaciones web, Guacamole se puede colocar detrás de un proxy inverso (Nginx). Es decir, el servidor Nginx se coloca por delante de Tomcat (puerto 80 y 443) y es el que redirige internamente a los puertos habilitados en Tomcat.

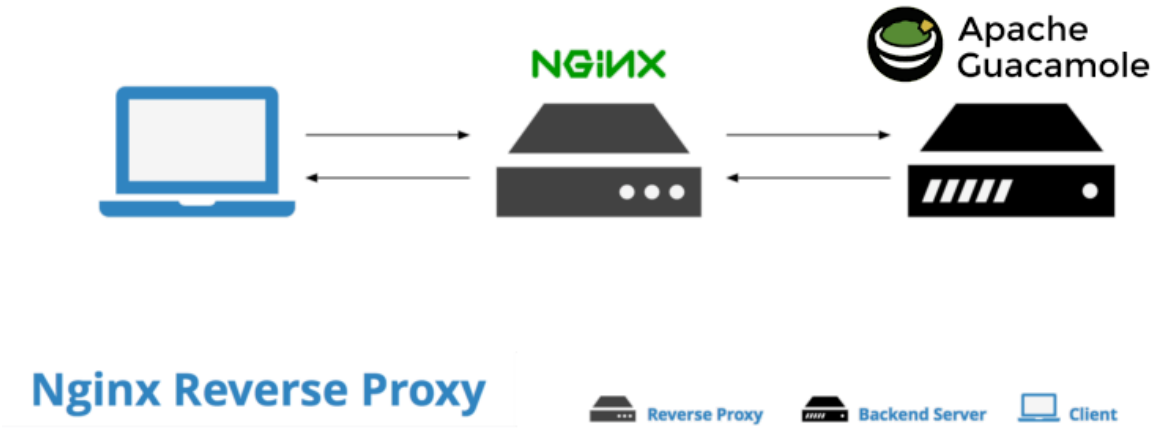

Ilustración 5.17. Proxy inverso con Apache Guacamole

La instalación del proxy inverso es sencilla:

```
apt install nginx
```

Por otro lado, para instalar un certificado SSL en Nginx, necesitaremos los siguientes ficheros:

- Certificado (`lamella_ujaen_es_cert.cer`)
- Clave privada (`lamella.ujaen.es_privatekey.pem`)
- Certificado intermediate (`lamella_ujaen_es_interm.cer`), que es el que proporciona la fiabilidad del certificado SSL.

Todos estos ficheros son suministrados por el Servicio de Informática (y la entidad certificadora SECTIGO) a través del correo electrónico para cada uno de los dominios de la Universidad de Jaén, en este caso particular para el servidor `lamella.ujaen.es` (donde va a ser montado Apache Guacamole).

Para instalar el certificado en el servidor habrá que ejecutar estos comandos (como usuario `root`):

```
cat lamella_ujaen_es_cert.cer lamella_ujaen_es_interm.cer > certificado-ssl.crt
```

Con éste se une en un solo fichero los ficheros del certificado y el certificado intermediate (intermediador), hecho que diferencia a Nginx con otros servidores.

A continuación, creamos dentro del directorio de configuración de Nginx la carpeta donde se ubicarán los ficheros del certificado y los copiamos en ella.

```
mkdir -p /etc/nginx/ssl/lamella_ujaen_es
mv certificado-ssl.crt /etc/nginx/ssl/lamella_ujaen_es/
cp lamella.ujaen.es_privatekey.pem
/etc/nginx/ssl/lamella_ujaen_es/
```

Seguidamente editamos el fichero de configuración del sitio web, dejándolo con este contenido que establece nuestro certificado SSL, configura el servidor para escuchar por el puerto seguro 443, redirige el puerto 80 al 443 (es decir, las peticiones que lleguen por http las redirige automáticamente al protocolo seguro https) y redirige las peticiones a los puertos que habilita Tomcat (8080). En negrita, los datos a personalizar según el caso.

```
nano /etc/nginx/sites-available/default
      #esto para redirigir del puerto 80 al 443
      server {
        listen 80 default_server;
        server_name _;
        return 301 https://$host$request_uri;
      }
      server {
        listen 443 ssl;
        listen [::]:443 ssl;

        server_name lamella.ujaen.es;
        ssl_certificate
/etc/nginx/ssl/lamella_ujaen_es/certificado-ssl.crt;
        ssl_certificate_key
/etc/nginx/ssl/lamella_ujaen_es/lamella.ujaen.es_privatekey.pem
;
        ssl_prefer_server_ciphers on;

        proxy_request_buffering off;
        proxy_buffering off;
```

```
        location / {
          proxy_pass http://127.0.0.1:8080;
          proxy_redirect off;
          proxy_set_header Host $host;
          proxy_set_header X-Real-IP $remote_addr;
          proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
          proxy_set_header X-Forwarded-Host $server_name;
        }
      }
```

También, para evitar problemas, hay que revisar el fichero `/etc/tomcat9/server.xml` y que la entrada del conector se vea así:

```
nano /etc/tomcat9/server.xml
     <Connector address="127.0.0.1" port="8080"
     protocol="HTTP/1.1"
     connectionTimeout="20000"
     URIEncoding="UTF-8"
     redirectPort="8443" />
```

Finalmente, se reinician los servicios de Tomcat y Nginx.

```
systemctl restart tomcat9.service
systemctl restart nginx.service
```

Probamos el resultado abriendo un navegador e indicando solamente la dirección del servidor (sin puertos), en nuestro caso, http://lamella.ujaen.es o https://lamella.ujaen.es. Será indiferente hacerlo por http o https ya que debe ejecutar la redirección al protocolo seguro de forma automática.

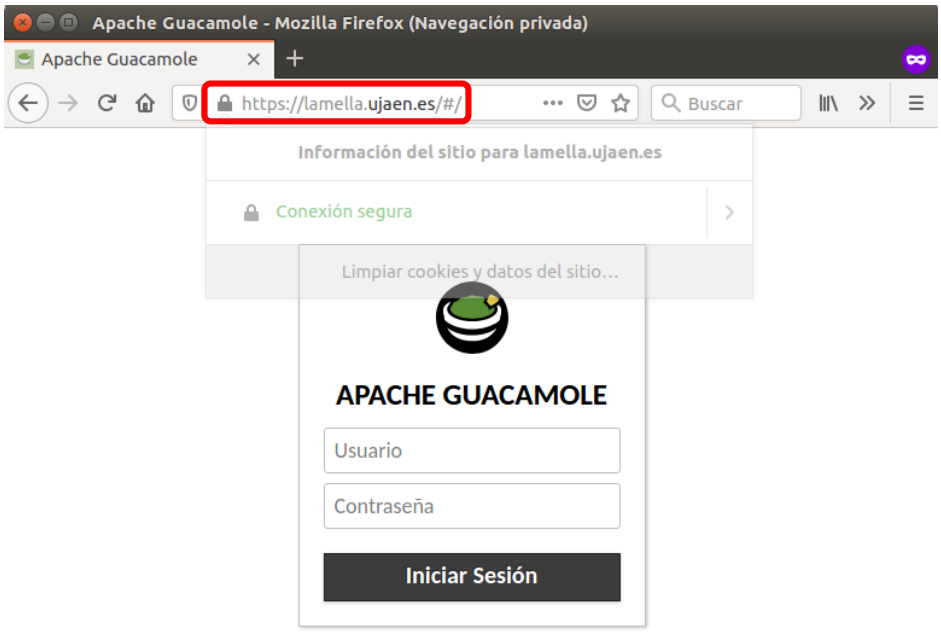

Ilustración 5.18. Apache Guacamole con conexión segura

5.3.1 Captura de la dirección IP remota del cliente

De forma predeterminada, cuando Tomcat está detrás de un proxy inverso, la dirección IP remota del cliente que ve es la del proxy en lugar del cliente original. Para permitir que las aplicaciones alojadas en Tomcat, como Guacamole, vean la dirección IP real del cliente, debemos editar el fichero `/etc/tomcat9/server.xml` y añadir lo siguiente en la sección host (ubicada al final del fichero):

```
nano /etc/tomcat9/server.xml
<Valve className="org.apache.catalina.valves.RemoteIpValve"
               internalProxies="127.0.0.1"
               remoteIpHeader="x-forwarded-for"
               remoteIpProxiesHeader="x-forwarded-by"
               protocolHeader="x-forwarded-proto" />
```

Una vez editado, reiniciamos el servicio de Tomcat.

```
systemctl restart tomcat9.service
```

Esta es una configuración muy recomendable debido a que la dirección IP remota en Guacamole se usa para auditar los inicios de sesión y las conexiones de los usuarios y podría usarse potencialmente para la autenticación. Igualmente se puede consultar la IP remota en la página que muestra las sesiones activas de los distintos usuarios.

5.4 Configuración de un bonding de las tarjetas de red

Como se comentó anteriormente, en el caso de desplegar Apache Guacamole en un equipo o servidor con varias tarjetas de red, es aconsejable utilizar la técnica llamada bonding que consiste en simular un dispositivo de red con gran ancho de banda uniendo varias tarjetas de red independientes, de manera que las aplicaciones solo verán una interfaz de red. Con esto podemos conseguir varias cosas:

- Mayor ancho de banda: el ancho de banda de la interfaz virtual será la suma de los anchos de banda de las interfaces reales.
- Balanceo de carga: tendremos balanceo de carga del tráfico de red entre todas las interfaces reales.
- Tolerancia a fallos: si falla una tarjeta de red los datos irán por las restantes que estén en buen estado.

Existen hasta 7 tipos de bonding combinando las características anteriores, aunque en nuestro caso, aplicaremos en la configuración el modo 4 ó 802.3ad (estándar IEEE 802.3ad, Dynamic link aggregation) también llamado “port trunking“, que ofrece alta disponibilidad y aumento de la velocidad, pero requiere que el módulo del kernel y el switch lo soporten (como es el caso).

A continuación, se indican las instrucciones a ejecutar para llevar a cabo esta configuración, empezando por la instalación de las utilidades de red y el paquete que permite establecer las tarjetas de red como esclavas.

```
apt install net-tools
apt install ifenslave
```

Comprobamos si está cargado el módulo de bonding en el kernel:

```
lsmod | grep bonding
```

Si esta instrucción no devuelve nada por pantalla significará que no está cargado. En ese caso, editamos el fichero `/etc/modules` y se añade al final del mismo la palabra bonding:

```
nano /etc/modules
     ...
     bonding
```

Reiniciamos el sistema y podemos comprobar que ya estará cargado este módulo.

Para finalizar esta configuración usaremos la herramienta de administración de red llamada `netplan` que incorpora nuestra versión de Ubuntu Server. Su archivo de configuración se encuentra en el directorio /etc/netplan y tiene extensión "`.yaml`".

Simplemente renombramos el fichero `.yaml` de dicho directorio con su mismo nombre y añadiendo al final "`.original`" y, creamos un nuevo fichero de nombre `bonding_servidor.yaml` (por ejemplo) con el siguiente contenido:

```
sudo mv /etc/netplan/00-installer-config.yaml /etc/netplan/00-installer-config-yaml.original
sudo touch /etc/netplan/bonding_servidor.yaml
sudo nano /etc/netplan/bonding_servidor.yaml
     network:
       version: 2
       ethernets:
         eports:
           match:
             name: en*
           optional: true
       bonds:
         bond0:
           interfaces: [eports]
           addresses: [150.214.178.7/24]
           gateway4: 150.214.178.1
           nameservers:
             addresses: [150.214.170.15]
           parameters:
             mode: 802.3ad
             lacp-rate: fast
             mii-monitor-interval: 100
```

Así se indican las tarjetas de red que forman parte del bonding (en este caso particular serían todas, es decir, 6), modo, nombre de la nueva interfaz de red (`bond0`), así como la dirección IP, puerta de enlace y servidores DNS.

Por último, ejecutamos el comando para aplicar estos cambios y reiniciamos.

```
netplan apply
```

```
reboot
```

Cuando inicie de nuevo el sistema se puede comprobar el estado de la nueva interfaz bonding:

```
cat /proc/net/bonding/bond0
ethtool bond0
```

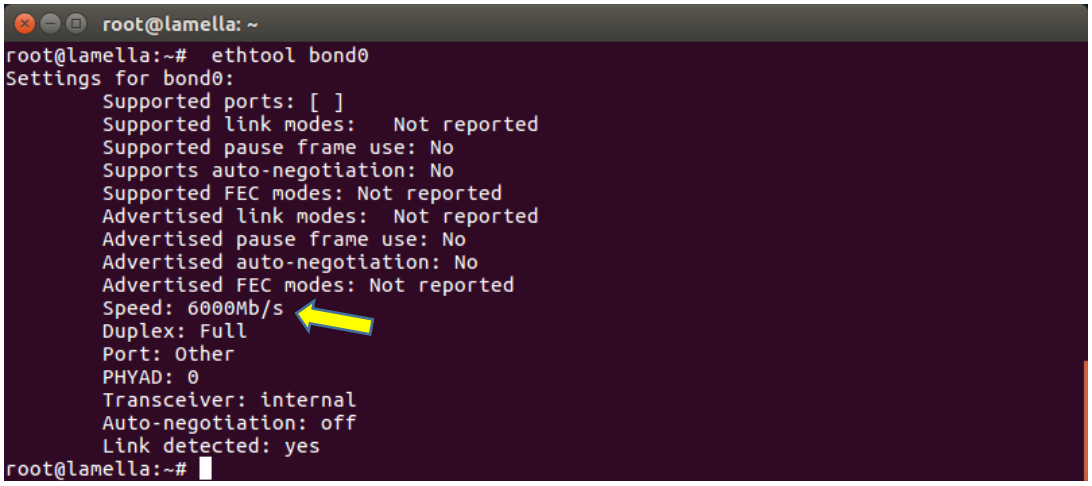

Ilustración 5.19. Estado de la interfaz bond0 del servidor lamella.ujaen.es

Se trata de una configuración opcional, aunque permitirá un mayor rendimiento a Guacamole, sobre todo, en casos de múltiples conexiones remotas simultáneas.

5.5 Máquina virtual de Apache Guacamole

Junto a la memoria de este TFG se entrega una máquina virtual con Guacamole ya instalado que nos permitirá realizar cualquier prueba de conexión remota. Ésta es su configuración:

- Sistema operativo: Ubuntu Server 20.04 LTS
- Memoria RAM: 2Gb.
- Disco duro: 50Gb.
- Aplicaciones: SSH, Apache Guacamole.
- Adaptador de red: NAT.
- Reenvío de puertos (de la máquina anfitriona a la máquina virtual):
    - 2222-->22.

  - 8080-->8080.

- Usuario del sistema: usuario.
- Contraseñas:
  - Usuario usuario de Ubuntu Server: guac@-pass
  - Usuario root de MySQL: guac@-R00t
  - Usuario guacamole_user de MySQL: guac@-Us3r
  - Usuario guacadmin de Apache Guacamole: guacadmin

Se entrega en un único fichero con formato OVA. Para su instalación y uso es necesaria la ayuda de un software de virtualización como por ejemplo Oracle VM VirtualBox (aunque poder ser cualquier otro). Simplemente haciendo doble clic en el fichero OVA la máquina virtual será importada en VirtualBox y estará disponible para su utilización:

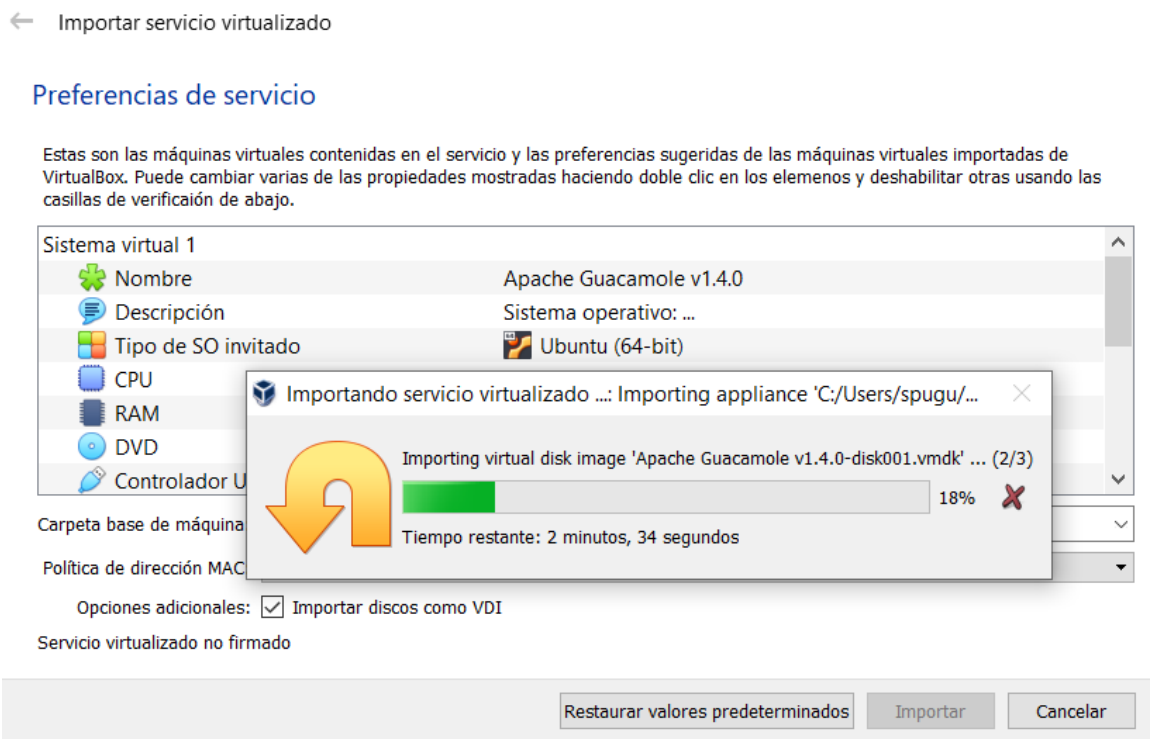

Ilustración 5.20. Importación de la máquina virtual (en VirtualBox)

La finalidad de esta máquina virtual es poder comprobar las características y funcionalidad de la aplicación Apache Guacamole accediendo, a través de ella, a los

ordenadores que tengan configurado el acceso remoto correspondiente. Todo esto antes de abordar su instalación definitiva en algún equipo físico.

Estas son las consideraciones a tener en cuenta para su uso una vez que ha sido importada en el software de virtualización:

- Si el equipo anfitrión dispone de, al menos, 8Gb de memoria RAM es aconsejable ampliar la memoria RAM de la máquina virtual a 4Gb en las opciones de configuración.
- Según la configuración indicada en el apartado de la tarjeta de red, dependerá la forma de acceder a la aplicación web de Guacamole (de la máquina virtual):

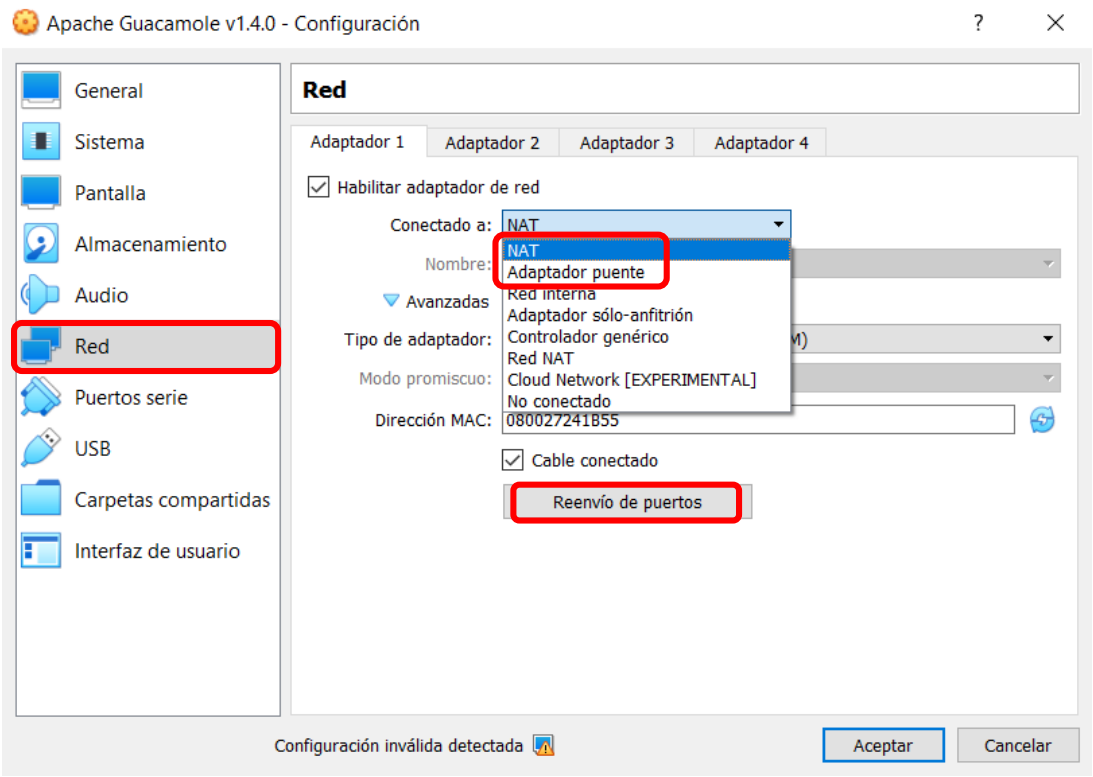

Ilustración 5.21. Configuración de la máquina virtual: interfaces de red

  - NAT. Esta es la configuración por defecto aplicada a la tarjeta de red en el fichero OVA de la máquina virtual. Este modo asigna a la interfaz de red una dirección IP interna para su salida a Internet, pero tiene la desventaja que la máquina virtual es invisible e inalcanzable fuera de su red y por lo tanto no podemos instalar un servidor de esta manera a menos que configuremos el reenvío de puertos.

- Reenvío de puertos. Necesario definirlo (en modo NAT) para poder acceder posteriormente a la aplicación de Apache Guacamole de la máquina virtual. La imagen muestra la configuración que viene, por defecto, en el fichero OVA. La primera regla es opcional, y sólo es necesaria para el acceso por SSH a la máquina virtual (ejemplo de comando de conexión: `ssh usuario@localhost -p 2222`), y la segunda regla es la que realmente permite el acceso a Guacamole en modo NAT y, por lo tanto, es obligatoria su definición.

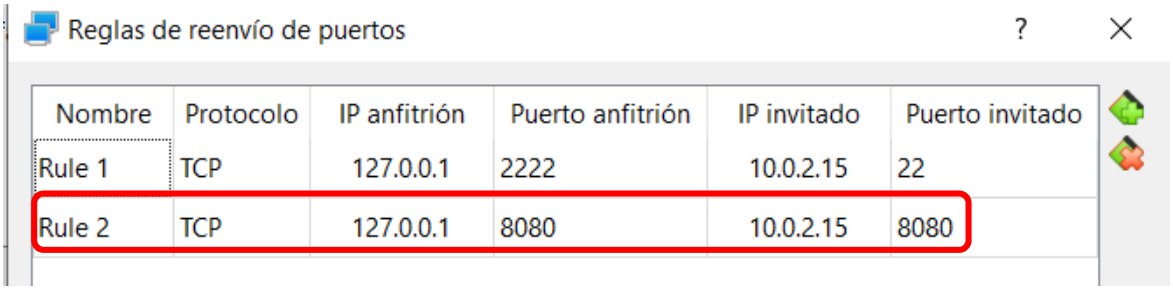

Ilustración 5.22. Configuración de la máquina virtual: reenvío de puertos

  - Adaptador puente. Este modo hace que la máquina virtual se conecte a la misma red que el equipo anfitrión, de tal forma que ésta se comportará como si fuera un PC más conectado a la red real. Para consultar la IP asignada, en el caso de tener activada la configuración para obtener una dirección IP automáticamente, podremos utilizar el comando `ifconfig` en la terminal de la máquina.

  Es posible usar cualquier de estas 2 opciones para configurar el adaptador de red, dependerá de las necesidades y el entorno que dispongamos para la prueba.

- Acceso a Apache Guacamole (ubicado en la máquina virtual):
  - `http://localhost:8080/guacamole` (modo NAT).
  - `http://ip_asignada:8080/guacamole` (modo Adaptador puente).
- Para utilizar la copia de la base de datos entregada también con esta máquina virtual, y que configura los usuarios y conexiones para el acceso a

los ordenadores de los laboratorios docentes, habrá que ejecutar el siguiente comando en la terminal de esta máquina:

```
mysql –u root – p guacamole_db < base_de_datos_guacamole.sql
```

Solicitará la contraseña del usuario root para la base de datos (antes indicada).

6 DEFINICIONES Y ABREVIATURAS

- **Acceso remoto**: proceso que permite acceder desde una computadora a un recurso ubicado físicamente en otra computadora que se encuentra geográficamente en otro lugar.
- **Android**: sistema operativo móvil basado en el núcleo Linux y otros software de código abierto. Fue diseñado para dispositivos móviles con pantalla táctil, como smartphones, tabletas, relojes inteligentes, etc.
- **Antivirus**: programa cuyo objetivo es detectar y eliminar virus informáticos. Con el paso del tiempo, los antivirus han evolucionado hacia programas más avanzados que además de buscar y detectar virus informáticos consiguen bloquearlos, desinfectar archivos y prevenir una infección de estos.
- **Apache**: servidor web HTTP de código abierto. Está desarrollado y mantenido por una comunidad de usuarios en torno a la Apache Software Foundation. Actualmente y desde el 1996 es el servidor web más usado en todo el mundo debido a su seguridad y estabilidad.
- **Arranque múltiple (o multiarranque)**: es la capacidad de un ordenador para poder tener más de un sistema operativo funcionando en un mismo disco rígido o equipo y arrancar con cualquiera de ellos.
- **Bonding**: tecnología que permite sumar dos o más interfaces de red independientes para aumentar el ancho de banda o la redundancia.
- **Cañón (o proyector de vídeo)**: aparato óptico que recibe una señal de vídeo y proyecta la imagen correspondiente en una pantalla de proyección usando un sistema de lentes, permitiendo así mostrar imágenes fijas o en movimiento.
- **Certificado SSL**: certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada.
- **Cliente-Servidor**: La arquitectura cliente-servidor es un modelo de diseño de software en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes. Un cliente realiza peticiones a otro programa, el servidor, quien le

da respuesta. Esta idea también se puede aplicar a programas que se ejecutan sobre una sola computadora, aunque es más ventajosa en un sistema operativo multiusuario distribuido a través de una red de computadoras.

- **Clónico**: equipo ensamblado a partir de piezas de cualquier fabricante. También son denominados ordenadores a medida.
- **Cloud Computing**: (computación en la nube) conocida también como servicios en la nube, informática en la nube, nube de cómputo o simplemente «la nube», es el uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software. En lugar de depender de un servicio físico instalado, se tiene acceso a una estructura donde el software y el hardware están virtualmente integrado.
- **Código fuente**: Básicamente, es el archivo o archivos con las instrucciones necesarias, realizadas en un lenguaje de programación, que sirve para compilar posteriormente un programa o programas para que puedan ser utilizados por el usuario de forma directa, tan sólo ejecutándolo.
- **Computación**: referido a la capacidad del ordenador para procesar datos y realizar cálculos complejos. Para ponerlo en perspectiva, un equipo portátil o de sobremesa con un procesador de 3 GHz puede realizar unos 3.000 millones de cálculos por segundo.
- **COVID-19**: enfermedad causada por el nuevo coronavirus conocido como SARS-CoV-2. La OMS tuvo noticia por primera vez de la existencia de este nuevo virus el 31 de diciembre de 2019, al ser informada de un grupo de casos de «neumonía vírica» que se habían declarado en Wuhan (República Popular China).
- **CPD**: (centro de proceso de datos) espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
- **DaaS**: El escritorio como servicio (DaaS, o “Desktop as a Service”) es una solución de informática de nube en la que un proveedor de servicios

suministra escritorios virtuales a los usuarios finales por Internet, bajo licencia de acuerdo con una suscripción por usuario. [28]

- **DDNS**: (o DNS dinámicos) servicio que nos permite asociar nuestra IP pública a un dominio, de manera que, en lugar de tener que memorizar los números de nuestra IP pública, podamos conectarnos a ella recordando ese dominio.
- **DHCP**: (Dynamic Host Configuration Protocol) protocolo de red tipo cliente / servidor que se encarga de asignar direcciones IP de forma dinámica, así como otros parámetros relativos a la configuración de red a cada uno de los dispositivos conectados.
- **Dirección IP**: es una etiqueta numérica, que identifica de manera lógica y jerárquica a un dispositivo en Internet o en una red local.
- **DNS**: (Domain Name Service) Servicio de Nombres de Dominio en español. Protocolo jerárquico distribuido para dar nombres a sistemas informáticos. Su objetivo es proporcionar una traducción textual y entendible por humanos a las direcciones IP numéricas que usan los ordenadores.
- **Entorno de desarrollo integrado**: (Integrated Development Environment, IDE) aplicación informática que proporciona servicios integrales para facilitarle al desarrollador o programador el desarrollo de software.
- **Escritorio remoto**: tecnología que permite a un usuario trabajar en una computadora a través de su escritorio gráfico desde otro dispositivo terminal ubicado en otro lugar. Se emplea en el terreno de la informática para nombrar a la posibilidad de realizar ciertas tareas en una computadora (ordenador) sin estar físicamente en contacto con el equipo.
- **Ethernet**: tecnología que permite que los dispositivos de redes de datos conectados por cable se comuniquen entre sí.
- **Firewall**: (o cortafuegos) es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas

- **Gateway**: (o puerta de enlace) dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores.
- **GNU GRUB (GNU GRand Unified Bootloader)**: es un cargador de arranque múltiple, desarrollado por el proyecto GNU que nos permite elegir qué Sistema Operativo arrancar de los instalados en el ordenador.
- **GNU/Linux**: sistema operativo tipo Unix (sistema operativo portable, multitarea y multiusuario, desarrollado en 1969) compuesto por software libre y de código abierto. Surge de las contribuciones de varios proyectos de software, entre los cuales destacan GNU (iniciado por Richard Stallman en 1983) y el kernel “Linux” (iniciado por Linus Torvalds en 1991).
- **Hardware**: se refiere a las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos. Los cables, así como los muebles o cajas, los periféricos de todo tipo, y cualquier otro elemento físico involucrado, componen el hardware o soporte físico.
- **Hash**: operación criptográfica que genera identificadores únicos e irrepetibles a partir de una información dada.
- **Host**: El término host o anfitrión se usa en informática para referirse a las computadoras u otros dispositivos (tabletas, móviles, portátiles) conectados a una red que proveen y utilizan servicios de ella.
- **HTML5**: es la quinta revisión importante del lenguaje básico de la World Wide Web, HTML.
- **HTTPs (Hyper Text Transfer Protocol Secure)**: protocolo seguro de transferencia de hipertexto.
- **iMac**: serie de computadoras de escritorio fabricados por Apple Inc. Está orientada al mercado doméstico y todos sus modelos se caracterizan por no necesitar una torre y el monitor, el teclado y el mouse son los únicos aparatos.

- **Imagen ISO**: también conocida como archivo ISO, es un tipo de archivo que se utiliza para almacenar una copia exacta de un sistema de ficheros de una unidad óptica.
- **Interfaz gráfica**: (en inglés, graphical user interface, GUI), programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz y que, principalmente, proporciona un entorno visual sencillo para permitir la comunicación con el sistema operativo de una máquina o computador.
- **Internet**: red informática descentralizada de alcance global. Se trata de un sistema de redes interconectadas mediante distintos protocolos que ofrece una gran diversidad de servicios y recursos.
- **iOS**: sistema operativo móvil de la multinacional Apple Inc. Originalmente desarrollado para el iPhone, después se ha usado en dispositivos como el iPod touch y el iPad.
- **IP**: (Internet Protocol) Es el protocolo principal utilizado para el intercambio de paquetes de datos a través de una red. IP permite la entrega de paquetes de datos mediante únicamente la dirección del destinatario.
- **JavaScript**: lenguaje de programación interpretado (sin necesidad de compilación) que funciona en los navegadores web de forma nativa.
- **JDBC**: estándar de conectividad de bases de datos de Java.
- **Kernel**: software que constituye una parte fundamental del sistema operativo, y se define como la parte que se ejecuta en modo privilegiado (conocido también como modo núcleo). En otras cosas, se encarga de conceder el acceso al hardware de forma segura para todo el software que lo solicita.
- **Kubernetes**: sistema de código abierto creado por Google para la gestión de aplicaciones en contenedores, un sistema de orquestación para contenedores Docker, permitiendo acciones como programar el despliegue, escalado y la monitorización de nuestros contenedores, entre muchas otras más.

- **Línea de comandos**: (en inglés, command-line interface, CLI) tipo de interfaz de usuario de computadora que permite a los usuarios dar instrucciones a algún programa informático o al sistema operativo por medio de una línea de texto simple.
- **Live USB**: es un dispositivo de almacenamiento extraíble (memoria USB) que alberga un sistema operativo en su totalidad y el cual es capaz de arrancar una computadora.
- **Log**: también denominado registro o historial, se refiere a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.)
- **LTS**: (en inglés, Long Term Support, o soporte a largo plazo) término informático usado para nombrar versiones o ediciones especiales de software diseñadas para tener soportes durante un período más largo que el normal.
- **LVM**: es una implementación de un gestor de volúmenes lógicos para el núcleo Linux, una capa de abstracción entre un dispositivo de almacenamiento (por ejemplo un disco) y un sistema de ficheros.
- **MAC**: (Media Access Control, o dirección física) identificador único que los fabricantes asignan a una tarjeta o dispositivo de red. Formada por 48 bits representados por 6 bloques de dos caracteres hexadecimales.
- **Mac OS**: (Macintosh Operating System) sistema operativo creado por Apple para su línea de computadoras Macintosh, y conocido por haber sido uno de los primeros sistemas dirigidos al gran público en contar con una interfaz gráfica compuesta por la interacción del mouse con ventanas, iconos y menús.
- **Máquina virtual**: software que simula un sistema de computación y puede ejecutar programas como si fuese una computadora real. Su característica esencial es que los procesos que ejecutan están limitados por los recursos y abstracciones proporcionados por ellas, no pudiendo escaparse de esta "computadora virtual".

- **Máscara de subred**: indica al sistema cuál es el esquema de particionamiento de subred. Tiene la misma apariencia que una dirección IP, pero en este caso, va a ser la que nos ayude a identificar si un equipo está dentro de una subred local o en una red remota.
- **MD5**: algoritmo de reducción criptográfico de 128 bits ampliamente usado.
- **MySQL**: sistema de gestión de bases de datos relacional que está considerada como la base de datos de código abierto más popular del mundo.
- **Navegador web**: programa que permite el acceso a la Web, interpretando la información de distintos tipos de archivos y sitios web para que estos puedan ser vistos.
- **NAS**: (Network Attached Storage, o almacenamiento conectado en red) tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador/ordenador (servidor) con computadoras personales o servidores clientes a través de una red.
- **OVA**: un archivo OVA es un dispositivo virtual utilizado por aplicaciones de virtualización como VMware Workstation y Oracle VM Virtualbox. Es decir, en este archivo se empaquetan todos los archivos necesarios para ejecutar la máquina virtual que contiene.
- **PC**: Ordenador personal (Personal Computer).
- **PDF**: (Portable Document Format) formato de almacenamiento para documentos digitales independientes de plataformas de software o hardware.
- **Protocolo**: conjunto de normas que permite la comunicación entre ordenadores, estableciendo la forma de identificación de estos en la red, la forma de transmisión de los datos y la forma en que la información debe procesarse.
- **Proxy**: servidor (software o dispositivo) que hace de intermediario en las peticiones de recursos que realiza un cliente a un servidor cuyas funciones básicas suelen ser: control de acceso, registro del tráfico, filtros de contenido, caché, etc.

- **Rack**: soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones.
- **RAID**: (Matriz Redundante de Discos Independientes) tecnología que permite a un equipo usar dos o más discos duros al mismo tiempo. RAID trata múltiples unidades como una unidad continua, ya sea mediante configuraciones de hardware o de software.
- **RDP**:(Remote Desktop Protocol) Protocolo desarrollado por Microsoft utilizado para ofrecer una interfaz gráfica a una máquina distinta, permitiendo el control remoto de la máquina. El protocolo es una extensión del protocolo estandarizado en ITU-T T.128 para el protocolo para compartir aplicaciones.
- **Red**: es un conjunto de equipos (nodos) y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.
- **Router**: dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino. Normalmente utilizado para conectarse a Internet.
- **Script**: documento que contiene una secuencia de instrucciones, escritas en algún lenguaje de programación.
- **Shell**: software que ofrece una interfaz para comunicarse con el núcleo del sistema operativo. Existen principalmente dos tipos de shell: interfaz de línea de comandos (CLI en inglés) e interfaz gráfica de usuario (GUI en inglés).
- **Sistema operativo**: conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software. Estos programas se ejecutan en modo privilegiado respecto al resto.
- **Software**: término informático que hace referencia a un programa o conjunto de programas de cómputo, así como datos, procedimientos y

pautas que permiten realizar distintas tareas en un sistema informático. Comúnmente se utiliza este término para referirse de una forma muy genérica a los programas de un dispositivo informático, sin embargo, el software abarca todo aquello que es intangible en un sistema computacional.

- **Software libre**: es aquel software que les da a sus usuarios la libertad de ejecutar, copiar, estudiar, modificar y distribuirlo.
- **SSH**: (Sechure SHell) Protocolo y programa que lo implementa, permite el acceso remoto a una máquina ofreciendo un intérprete de comandos y la transmisión de ventanas. La principal ventaja de ssh es que la conexión realizada es segura, siendo confidenciales los datos transmitidos gracias a los protocolos de cifrado que implementa.
- **SSL**: (Secure Sockets Layer, o capa de puertos seguros) protocolo criptográfico que proporciona comunicaciones seguras por una red, normalmente Internet.
- **Subred**: pequeña red dentro de una red más grande. Es una agrupación lógica de dispositivos de red conectados que tienden a estar ubicados en estrecha proximidad física entre sí en una red de área local. Son creadas para facilitar su administración y mejorar su rendimiento y seguridad.
- **Switch**: (o conmutador) dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet.
- **TCP/IP**: es un conjunto de protocolos de red en los que se basa internet y que permiten la transmisión de datos entre computadoras.
- **Thin Client**: literalmente traducido como cliente ligero, es un ordenador o software cliente en una arquitectura cliente-servidor, que depende primariamente del servidor central para las tareas de procesamiento, y se enfoca principalmente en transportar la entrada y la salida entre el usuario y el servidor remoto.
- **UJA**: Universidad de Jaén.

- **URL**: dirección única y específica que se asigna a cada uno de los recursos disponibles en Internet para que puedan ser localizados por el navegador y visitados por los usuarios.
- **Virtualización**: creación de una capa de abstracción entre el hardware de una máquina y un sistema operativo huésped, que crea una versión virtual de un dispositivo. Esta capa software se encarga de repartir los recursos físicos de la máquina, entre las máquinas virtuales ejecutadas sobre la máquina anfitrión real.
- **VLAN**: (virtual LAN, o red de área local virtual) método para crear redes lógicas independientes dentro de una misma red física.
- **VNC**: (Virtual Network Computing o Computación virtual en Red) es un programa de software libre basado en una estructura cliente-servidor que permite observar las acciones del ordenador servidor remotamente a través de un ordenador cliente. VNC no impone restricciones en el sistema operativo del ordenador servidor con respecto al del cliente.
- **VPN**: (red privada virtual o virtual private network) es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
- **ZFS**: es un sistema de archivos avanzado que, entre otras características, tiene la posibilidad de realizar y recuperar instantáneas (“foto” del estado del sistema de archivos en un determinado momento) de manera muy rápida.

7 BIBLIOGRAFÍA

[1] F. J. Molina Robles y E. Polo Ortega, Servicios de red e Internet, Madrid: RA-MA Editorial, 2015.

[2] Wikipedia, la enciclopedia libre: Telnet (Teletype Network). Disponible en: https://es.wikipedia.org/wiki/Telnet. [Último acceso: 7 Marzo 2022].

[3] D. J. Barret, R. G. Byrnes y R. E. Silverman, SSH, the secure shell : the definitive guide, O'Reilly, 2005.

[4] Wikipedia, la enciclopedia libre: VNC (Virtual Network Computing). Disponible en: https://es.wikipedia.org/wiki/VNC. [Último acceso: 7 Marzo 2022].

[5] Wikipedia, la enciclopedia libre: Remote Desktop Services (Servicios de Escritorio Remoto). Disponible en: https://es.wikipedia.org/wiki/Remote_Desktop_Services. [Último acceso: 7 Marzo 2022].

[6] Wikipedia, la enciclopedia libre: RDP (Remote Desktop Protocol). Disponible en: https://es.wikipedia.org/wiki/Remote_Desktop_Protocol. [Último acceso: 7 Marzo 2022].

[7] Universidad de Jaén: Departamento de Informática. Disponible en: https://www.ujaen.es/departamentos/dinformatica/. [Último acceso: 15 Marzo 2022].

[8] FogProject. Disponible en: https://fogproject.org/. [Último acceso: 29 04 2022].

[9] Redes zone: Para qué sirve la segmentación de redes y por qué es recomendable implementarla. Disponible en: https://www.redeszone.net/tutoriales/seguridad/segmentacion-red-vlan-que-es/. [Último acceso: 23 Mayo 2022].

[10] Microsoft: Cliente de Escritorio Remoto: configuración admitida. Disponible en: https://docs.microsoft.com/es-es/windows-server/remote/remote-desktop-services/clients/remote-desktop-supported-config. [Último acceso: 5 Mayo 2022].

[11] Microsoft: Usar asistencia rápida para ayudar a los usuarios. Disponible en: https://docs.microsoft.com/es-es/windows/client-management/quick-assist. [Último acceso: 5 Mayo 2022].

[12] Teamviewer: La solución para el acceso y el control remotos. Disponible en: https://www.teamviewer.com/es/. [Último acceso: 12 Mayo 2022].

[13] Nanosystems: SupRemo, acceso remoto de forma fácil y segura. Disponible en: https://www.supremocontrol.com/es. [Último acceso: 4 Mayo 2022].

[14] AnyDesk: Conexiones remotas rápidas con el escritorio remoto de AnyDesk. Disponible en: https://anydesk.com/es/solutions/remote-desktop. [Último acceso: 12 Mayo 2022].

[15] Google: Acceder a otro ordenador con Escritorio Remoto de Chrome. Disponible en: https://support.google.com/chrome/answer/1649523. [Último acceso: 20 Mayo 2022].

[16] Apple: Manual del usuario de Apple Remote Desktop. Disponible en: https://support.apple.com/es-es/guide/remote-desktop/welcome/mac. [Último acceso: 22 Mayo 2022].

[17] RealVNC: Software de acceso remoto para equipos de escritorio y dispositivos móviles. Disponible en: https://www.realvnc.com/es/. [Último acceso: 21 Mayo 2022].

[18] UltraVNC: Herramientas de acceso remoto. Disponible en: https://uvnc.com/. [Último acceso: 22 Mayo 2022].

[19] TightVNC: TightVNC Software. Disponible en: https://www.tightvnc.com/. [Último acceso: 22 Mayo 2022].

[20] NoMachine: Escritorio remoto gratuito para todo el mundo. Disponible en: https://www.nomachine.com/es. [Último acceso: 2 Mayo 2022].

[21] Wikipedia, la enciclopedia libre: Tecnología NX. Disponible en: https://es.wikipedia.org/wiki/Tecnología_NX. [Último acceso: 20 Mayo 2022].

[22] Apache Software Foundation: Apache Guacamole. Disponible en: https://guacamole.apache.org/. [Último acceso: 15 Mayo 2022].

[23] Universidad de Jaén: Protocolo del Servicio Web de la Universidad de Jaén. Disponible en: https://www.ujaen.es/servicios/sinformatica/catalogo-de-servicios-tic/web-institucional/protocolo-web. [Último acceso: 16 Abril 2022].

[24] PC Expansión: Servidores. Disponible en: https://www.pcexpansion.es/servidor_hp_proliant_dl360p_gen8_e5-2620_1p__4_gb-r_p420i_.php. [Último acceso: 30 Mayo 2022].

[25] Talent.com: Buscador de salarios. Disponible en: https://es.talent.com/salary. [Último acceso: 30 Mayo 2022].

[26] Canonical: Get Ubuntu Server. Disponible: https://ubuntu.com/download/server. [Último acceso: 30 Mayo 2022].

[27] Blog Desde Linux: SysMonTask, un útil y compacto monitor de sistemas para GNU/Linux. Disponible en: https://blog.desdelinux.net/sysmontask-compacto-monitor-sistemas-gnu-linux/. [Último acceso: 10 Junio 2022].

[28] VMware: ¿Qué es el escritorio como servicio (DaaS)?. Disponible en: https://www.vmware.com/latam/topics/glossary/content/desktop-as-a-service.html. [Último acceso: 10 Marzo 2022].

[29] Wikipedia, la enciclopedia libre: Escritorio Remoto. Disponible en: https://es.wikipedia.org/wiki/Escritorio_remoto. [Último acceso: 7 Marzo 2022].

[30] Servicio de Informática de la Universidad de Jaén: Guias prácticas. Disponible: https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Conexion_mediante_escritorio_remoto_Windows.pdf. [Último acceso: 4 Mayo 2022].