

# **TRABAJO FIN DE GRADO**

## **Servidor Web con Acceso Seguro a través de VPN**

---



---

Autor: Mohammed Maamla Razzak

Titulación: Técnico Superior en Administración de Sistemas Informáticos en Red

Fecha: 06/01/2026	Versión: 1_0
-------------------	--------------

## Índice de contenido

TRABAJO FIN DE GRADO .....	1
1. Resumen ejecutivo (ESP) .....	3
Resumen ejecutivo (EN) .....	4
2. Marco Teórico y Principios Tecnológicos .....	5
2.1. Descripción general, marco teórico y principios tecnológicos.....	5
2.1.1. Entorno de simulación: VirtualBox .....	5
2.1.2. Firewall Perimetral: PfSense .....	6
2.1.3. Servidor Central: Ubuntu Server (SRV1) .....	6
2.1.4. Servicio Web: Apache .....	6
2.1.5. Servicio VPN: WireGuard .....	6
2.1.6. Servidor de Almacenamiento Dedicado: TrueNAS .....	7
2.1.7. Dispositivos Cliente.....	7
2.1.8. Normas Técnicas y Estándares Aplicables .....	7
2.2. Análisis de la realidad.....	8
2.3. Justificación .....	9
2.4. Marco Legal .....	10
2.5. Destinatarios .....	11
3. Desarrollo del proyecto .....	11
3.1. Objetivos e indicadores para su medición .....	11
3.2. Fases, actividades y cronología .....	12
3.3. Metodología seguida.....	13
3.4. Recursos .....	14
3.5. Presupuesto .....	16
3.5.1. Fase de análisis .....	21
3.5.2. Fase de implementación.....	26
3.5.3. Fase de desarrollo.....	46
3.5.4. Fase de pruebas .....	54
3.5.5. Documentación del producto .....	68
3.5.6. Formación de usuarios.....	74
Resultados obtenidos y conclusiones.....	76
Bibliografía.....	77
Anexos .....	80
Anexo I - Control de Acceso y Gestión de Sesiones (validar_login.php).....	80
Anexo II - Gestión Segura de Solicitudes y Archivos (procesar_solicitud.php) .....	82
Anexo III - Monitorización de Servicios y Dashboard (admin/dashboard.php) .....	84
Anexo IV - Automatización de la Continuidad de Negocio (backup_web.sh).....	87
Anexo V – Repositorio de GitHub.....	88

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 3 de 89



## 1. Resumen ejecutivo (ESP)

Este proyecto aborda uno de los principales desafíos de las pequeñas y medianas empresas (PYMES) en el entorno digital actual: la necesidad de facilitar el teletrabajo y el acceso remoto a los recursos corporativos sin comprometer la seguridad ni incurrir en los altos costes de las soluciones comerciales tradicionales.

El objetivo central es el diseño, implementación y validación de una infraestructura tecnológica de bajo coste, robusta y escalable que garantice el acceso seguro y controlado a los servicios internos de la empresa.

Para lograr este propósito, la solución se fundamenta en la integración de dos componentes tecnológicos clave:

1. Un Servidor Web seguro, basado en Apache HTTP Server, que aloja los servicios corporativos internos (intranet, aplicaciones de gestión, etc.). La confidencialidad e integridad de las comunicaciones se aseguran mediante la implementación de certificados SSL/TLS (HTTPS).
2. Una Red Privada Virtual (VPN) de alto rendimiento, basada en el protocolo moderno WireGuard. Esta VPN actúa como un túnel cifrado que permite a los empleados (remotos o móviles) conectarse a la red interna desde cualquier ubicación de Internet, protegiendo todo el tráfico de accesos no autorizados.
3. Un Servidor de Almacenamiento Dedicado (NAS), basado en TrueNAS Core, que proporciona una solución de backups y recuperación ante desastres utilizando un volumen RAIDZ1 (RAID 5) cifrado. Esto garantiza la integridad y la persistencia de los datos críticos de la intranet.

La implementación de esta arquitectura se validará en un entorno de simulación controlado mediante el hipervisor VirtualBox. Esta simulación recreará una topología de red empresarial completa, incluyendo:

- Un router/firewall pfSense, que actuará como dispositivo perimetral, gestionando las reglas de acceso, el enrutamiento y la segmentación de la red.
- Un servidor Ubuntu Server (SRV1), que alojará de forma centralizada tanto el servicio web (Apache) como el servicio de VPN (WireGuard).
- Un servidor NAS virtualizado, dedicado exclusivamente a la gestión de copias de seguridad de la red.
- Una variedad de dispositivos cliente que simulan todos los casos de uso: un empleado interno (Ubuntu Desktop), un teletrabajador externo (Windows 10) y un empleado móvil (iPhone).

Este proyecto proporciona a las PYMES una solución integral que asegura la confidencialidad de los datos mediante cifrado extremo a extremo, garantiza la integridad de la información mediante redundancia con el RAID 5 y ofrece una alta disponibilidad. El resultado es un sistema flexible y robusto que permite a las empresas proteger sus activos digitales y habilitar la productividad de sus empleados de forma segura, desde cualquier lugar y con una inversión mínima.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 4 de 89



## Resumen ejecutivo (EN)

This project addresses one of the main challenges for Small and Medium-sized Enterprises (SMEs) in the current digital environment: the need to facilitate remote work and corporate resource access without compromising security or incurring the high costs of traditional commercial solutions.

The central objective is the design, implementation, and validation of a low-cost, robust, and scalable technological infrastructure that ensures secure and controlled access to the company's internal services.

To achieve this purpose, the solution is based on the integration of three key technological components:

1. A secure Web Server, based on Apache HTTP Server, hosting internal corporate services. Confidentiality and integrity of communications are ensured through SSL/TLS certificates (HTTPS).
2. A high-performance Virtual Private Network (VPN), based on the modern WireGuard protocol. This VPN acts as an encrypted tunnel allowing remote employees to connect to the internal network from any internet location, protecting all traffic from unauthorized access.
3. A Dedicated Storage Server (NAS), based on TrueNAS Core, which provides an encrypted backup and disaster recovery solution using a RAIDZ1 (RAID 5) volume. This guarantees the integrity and persistence of critical intranet data against hardware failure.

The implementation of this architecture will be validated in a controlled simulation environment using the VirtualBox hypervisor. This simulation will recreate a complete corporate network topology, including:

- A pfSense router/firewall, acting as the perimeter device, managing access rules, routing, and network segmentation.
- An Ubuntu Server (SRV1), centrally hosting both the web service (Apache) and the VPN service (WireGuard).
- A virtualized NAS server, dedicated exclusively to managing network and data backups.
- A variety of client devices simulating all use cases: an internal employee (Ubuntu Desktop), an external remote worker (Windows 10), and a mobile employee.

This project provides SMEs with an integral solution that ensures data confidentiality through end-to-end encryption, guarantees information integrity through redundancy (RAID), and offers high availability. The result is a flexible and robust system that allows companies to protect their digital assets and enable employee productivity securely, from anywhere, and with minimal investment.

## 2. Marco Teórico y Principios Tecnológicos

### 2.1. Descripción general, marco teórico y principios tecnológicos

El proyecto consiste en la implantación de un sistema corporativo seguro para una PYME, permitiendo que el empleado acceda a sus recursos internos por acceso remoto.

La solución se basa en una arquitectura cliente servidor protegida por un firewall perimetral implementado por un router y un túnel VPN cifrada, complementada con un servidor NAS para la protección de datos.

Para lograr este objetivo, se propone el diseño e instalación de los elementos que se muestran en el siguiente diagrama de arquitectura general:

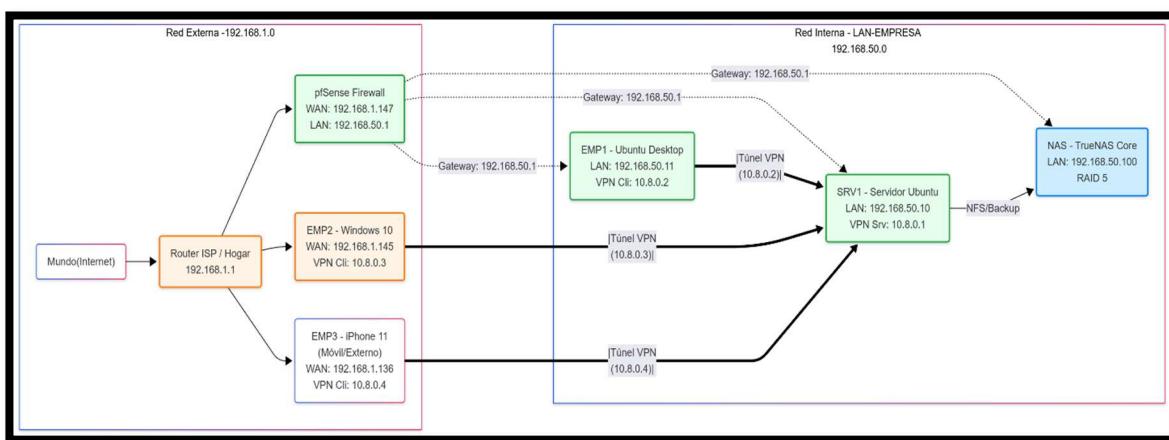


Imagen 1 - Diagrama creado con 'Mermaid Chart'

Como se observa en el diagrama, la infraestructura se divide en una "Red Externa" (simulando Internet, 192.168.1.0/24) y una "Red Interna" o LAN corporativa (simulando la oficina, 192.168.50.0/24). La solución constará de los siguientes componentes tecnológicos principales.

#### 2.1.1. Entorno de simulación: VirtualBox

Para simular el entorno sin hardware físico dedicado, se utiliza VirtualBox. Esta herramienta de virtualización permite simular un entorno empresarial completo con múltiples máquinas (servidores, clientes, firewall) en un mismo hardware físico. Permite la creación de redes virtuales aisladas (Red Interna) y redes puente (Adaptador Puente) para replicar de forma realista la topología de la empresa y su conexión a Internet.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 6 de 89



## 2.1.2. Firewall Perimetral: PfSense

El control de accesos y la seguridad perimetral se gestionan mediante pfSense. Esta es una solución de firewall de código abierto basada en FreeBSD que actúa como el router principal de la empresa.

Tendrá dos interfaces de red:

La interfaz WAN (Wide Area Network) conectada a la Red Externa (Internet) con la IP 192.168.1.147 y la interfaz LAN (Local Area Network) conectada a la Red Interna con la IP 192.168.50.1, que servirá como Gateway (puerta de enlace) para todos los dispositivos de la oficina.

Sus funciones clave en el proyecto son el NAT (Network Address Translation) y la redirección de puertos (Port Forwarding). Esta última es crítica, ya que se configurará para redirigir el tráfico VPN entrante desde Internet (WAN) al servidor WireGuard (SRV1) en la LAN.

## 2.1.3. Servidor Central: Ubuntu Server (SRV1)

El núcleo de los servicios se implementa sobre un servidor Ubuntu Server (SRV1), un sistema operativo Linux robusto, seguro y de amplio uso en entornos empresariales. Este servidor tendrá la IP estática 192.168.50.10 dentro de la Red Interna y alojará los dos servicios principales del proyecto.

## 2.1.4. Servicio Web: Apache

Para alojar la intranet de la empresa, se utiliza el servidor web Apache. Es un software ligero y seguro que permite alojar aplicaciones y servicios internos. En este proyecto, se configurará para servir un sitio web y se protegerá con certificados SSL/TLS (HTTPS) para cifrar la comunicación entre el empleado y el servidor, asegurando la confidencialidad de la información. El servicio será accesible en la LAN en <https://192.168.50.10>, y con la VPN habilitada en <https://10.8.0.1>.

## 2.1.5. Servicio VPN: WireGuard

El acceso remoto seguro se implementa con WireGuard. Es un protocolo de VPN moderno, muy rápido y que utiliza criptografía de última generación. Permite la conexión segura de clientes externos (teletrabajadores, móviles) hacia la red corporativa.

- El servidor WireGuard se ejecutará en SRV1 y tendrá la IP 10.8.0.1 dentro de su propia subred VPN (10.8.0.0/24).
- Cuando un cliente externo se conecta, WireGuard crea un túnel cifrado desde el cliente hasta el servidor y le asigna una IP virtual (ej. 10.8.0.2), permitiéndole acceder a los recursos de la Red Interna como si estuviera físicamente en la oficina.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 7 de 89



## 2.1.6. Servidor de Almacenamiento Dedicado: TrueNAS

La integridad y persistencia de los datos se gestiona mediante un servidor NAS virtualizado que utiliza TrueNAS Core. Este sistema es esencial para la estrategia de recuperación de desastres.

Función Principal: Almacenamiento de copias de seguridad cifradas y fuera de línea de la intranet, usando el protocolo NFS.

Redundancia: El volumen de almacenamiento está configurado con RAIDZ1 (equivalente a RAID 5), lo que asegura que los datos no se pierdan si uno de los discos duros virtuales falla.

Estrategia de Copias de Seguridad (Regla 3-2-1): La implementación del servidor NAS cumple con el estándar de oro de seguridad (Regla 3-2-1). El sistema mantiene una copia de los datos en el servidor de producción, una segunda copia en el volumen RAIDZ1 del NAS (dos soportes distintos) y una tercera copia en un dispositivo de almacenamiento de la empresa, y permite la exportación fácil de la imagen del servidor NAS a un almacenamiento externo (tercera copia fuera del sitio).

## 2.1.7. Dispositivos Cliente

Para validar la solución, se simulan tres perfiles de empleado:

- Empleado Interno (EMP1 - Ubuntu Desktop): Con IP 192.168.50.11, simula un trabajador en la oficina. Accederá al servidor web directamente por la LAN.
- Empleado Externo (EMP2 - Windows 10): Con IP 192.168.1.145, simula un teletrabajador. Se demostrará que no puede acceder a 192.168.50.10 directamente y que, tras conectarse a la VPN (obteniendo la IP 10.8.0.3), obtiene acceso completo.
- Empleado Móvil (EMP3 - iPhone 11): Con IP 192.168.1.136, valida la flexibilidad de la solución para dispositivos móviles, conectándose a la VPN de forma análoga al empleado externo.

## 2.1.8. Normas Técnicas y Estándares Aplicables

La implementación de este proyecto se fundamenta en estándares técnicos abiertos y ampliamente aceptados por la industria, garantizando la interoperabilidad y la seguridad:

- Protocolos de Red Base: La comunicación se basa en la familia de protocolos TCP/IP, definidos principalmente por los estándares RFC 791 (Protocolo Internet - IP) y RFC 793 (Protocolo de Control de Transmisión - TCP).
- Protocolos de Servidor Web: El servicio web seguro se rige por el RFC 9112 (HTTP/1.1) y, fundamentalmente, por el RFC 8446, que define el estándar TLS 1.3 (Transport Layer Security) para el cifrado HTTPS.
- Criptografía y VPN: El protocolo WireGuard se basa en primitivas criptográficas modernas, como las definidas en el RFC 8439 (ChaCha20 y Poly1305) para el cifrado autenticado.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 8 de 89



- Gestión de Seguridad (Marco): Aunque no se implementa una certificación, el diseño de la solución sigue los principios de buenas prácticas de gestión de la seguridad de la información descritos en la familia ISO/IEC 27000 (como la ISO 27001/27002), especialmente en lo relativo al control de acceso y la seguridad de las comunicaciones.
- Almacenamiento y Backups: Se aplica el protocolo NFS (Network File System) y los principios de redundancia de datos RAID (Redundant Array of Independent Disks) y cifrado AES-256.

## 2.2. Análisis de la realidad

En el panorama empresarial actual, la transformación digital ha dejado de ser una opción para convertirse en una necesidad imperativa de supervivencia, especialmente para las Pequeñas y Medianas Empresas (Pymes). Este escenario se ha dado por la aparición del teletrabajo como un modelo laboral estándar.

Hoy en día, las empresas necesitan que sus empleados puedan acceder a los recursos corporativos (servidores de archivos, aplicaciones de gestión, intranets) desde fuera de la oficina, ya sea desde sus hogares o mediante dispositivos móviles.

Sin embargo, esta necesidad genera un grave problema de seguridad. La realidad de muchas Pymes es que, por falta de presupuesto o de personal técnico especializado, recurren a métodos inseguros para habilitar este acceso. Prácticas como la simple redirección de puertos (Port Forwarding) para exponer servicios críticos como el Escritorio Remoto (RDP) o servidores de archivos (FTP/SMB) directamente a Internet son, lamentablemente, comunes.

Estas prácticas convierten a la empresa en un blanco fácil para ciberataques, como el ransomware o la filtración de datos, que pueden tener consecuencias muy graves.

Por otro lado, las soluciones de seguridad perimetral y VPN comerciales como las ofrecidas por Cisco, suponen un alto coste de licenciamiento y mantenimiento que queda fuera del alcance de una gran parte del tejido empresarial.

Actualmente, existe una brecha en el mercado: las Pymes necesitan una seguridad de nivel empresarial, pero con un coste asumible. Demandan soluciones que sean robustas, flexibles y económicas. Aquí es donde las soluciones basadas en software de código abierto, como las que se proponen en este proyecto, no solo son viables, sino estratégicas.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 9 de 89



## 2.3. Justificación

La justificación de este proyecto es su valor estratégico y económico para las PYMES. Resuelve el dilema de la necesidad de teletrabajo y el alto coste de las soluciones de seguridad o los graves riesgos de no tenerlas.

Este proyecto presenta una solución que es, simultáneamente, más segura, más rápida y más económica que las alternativas.

Los beneficios que justifican su implementación son los siguientes:

- Coste Cero en Licenciamiento: Se basa al 100% en software *open-source* (pfSense, WireGuard, Apache, TrueNAS). Esto "democratiza" la seguridad de nivel empresarial, haciéndola accesible para cualquier presupuesto.
- Seguridad Robusta: Cierra toda la superficie de ataque de Internet. Al forzar el acceso a través de un túnel cifrado, se mitiga el riesgo de accesos no autorizados, robo de datos y ransomware, además, garantiza la continuidad del negocio al proteger los datos críticos fuera del servidor principal.
- Rendimiento Superior: El uso del protocolo moderno WireGuard garantiza una conexión VPN mucho más rápida, estable y eficiente que las soluciones tradicionales. Esto se traduce directamente en una mayor productividad para el empleado que teletrabaja.
- Recuperación de Desastres: La inclusión del servidor NAS (TrueNAS) con volumen RAIDZ1 (RAID 5) asegura la integridad y redundancia de las copias de seguridad. Esto reduce a minutos el tiempo de inactividad del negocio ante un fallo de hardware en el servidor principal.

En resumen, este proyecto no es un gasto, es un habilitador de negocio. Permite a cualquier PYME implementar el teletrabajo de forma segura y eficiente, garantizando su continuidad y protegiendo sus activos digitales sin necesidad de una gran inversión.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 10 de 89



## 2.4. Marco Legal

Este proyecto, al gestionar el acceso a los datos de una organización, está directamente sujeto a varias normativas legales clave. El propio diseño de la solución es una medida técnica orientada a facilitar el cumplimiento de dichas leyes.

- Reglamento General de Protección de Datos (RGPD) (UE) 2016/679: Esta es la normativa principal. El RGPD exige que cualquier organización que trate datos personales (de clientes, empleados, etc.) implemente "medidas técnicas y organizativas apropiadas" para garantizar un nivel de seguridad adecuado al riesgo.
  - Artículo 32 (Seguridad del tratamiento): Este proyecto es una respuesta directa a este artículo. La implementación de un firewall (pfSense), el cifrado de las comunicaciones externas (WireGuard), el cifrado de la intranet (HTTPS) y el cifrado de los datos almacenados en el NAS son medidas técnicas explícitas para proteger los datos contra la destrucción, pérdida, alteración o acceso no autorizado son medidas técnicas explícitas para proteger los datos contra la destrucción, pérdida, alteración o acceso no autorizado.
  - Principios de Confidencialidad e Integridad: La VPN y el SSL garantizan que solo el personal autorizado acceda a la información y que esta no sea alterada en tránsito.
- Ley Orgánica 3/2018, de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD): Es la ley española que adapta el RGPD al ordenamiento jurídico nacional. Refuerza las obligaciones del RGPD y establece el régimen sancionador. No contar con medidas de seguridad como las propuestas puede derivar en sanciones económicas severas en caso de una brecha de seguridad.
- Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE): Aunque el proyecto se centra en una intranet (servicio interno) y no en un comercio electrónico público, esta ley es relevante. Si la intranet aloja aplicaciones que gestionan la relación con clientes o proveedores (un CRM, por ejemplo), la LSSI-CE aplica en cuanto a la validez de la información y la seguridad de las comunicaciones electrónicas.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 11 de 89



## 2.5. Destinatarios

Este proyecto está dirigido principalmente a Pequeñas y Medianas Empresas (PYMES) que necesitan habilitar el teletrabajo de forma segura, pero que operan con un presupuesto limitado que les impide acceder a soluciones comerciales costosas.

Dentro de la empresa, los beneficiarios directos son tanto la Gerencia, que protege la continuidad del negocio y reduce el riesgo financiero de un ciberataque, como el Departamento de TI, que obtiene una solución robusta, moderna y de bajo coste.

De forma indirecta, el proyecto beneficia a los empleados, que obtienen un acceso remoto rápido y fiable para teletrabajar con productividad y los clientes de la PYME, cuyos datos personales y comerciales están significativamente mejor protegidos.

## 3. Desarrollo del proyecto

### 3.1. Objetivos e indicadores para su medición

El objetivo central de este proyecto es que la empresa disponga de una infraestructura segura y centralizada que facilite el acceso y la gestión de la información corporativa (empleados, clientes, activos, etc.). La solución propuesta garantiza la integridad, confidencialidad y disponibilidad de los datos mediante una arquitectura robusta basada en Apache, WireGuard, un sistema de autenticación seguro y un sistema de almacenamiento redundante (NAS).

A continuación, se detallan los objetivos específicos y sus ventajas:

**Acceso Seguro y Autenticado:** Se implementa un sistema donde cada usuario se identifica mediante credenciales únicas. Una vez autenticado, el sistema gestiona los privilegios, asegurando que cada empleado acceda solo a la información autorizada, con ello se elimina el riesgo de accesos no autorizados y se mantiene la información sensible permaneciendo cifrada o inaccesible para externos.

**Centralización y Facilidad de Gestión:** El almacenamiento de la información en un servidor accesible vía intranet facilita enormemente la ejecución de tareas diarias. Los usuarios pueden consultar, modificar o añadir datos desde una única plataforma, evitando la dispersión de la información mejorando la eficiencia operativa al reducir el tiempo de búsqueda y gestión de documentos, permitiendo una actualización constante y fiable de los datos de la empresa.

**Integridad y Disponibilidad del Dato:** Se garantiza la exactitud y la persistencia de la información ante fallos de hardware o errores humanos. El sistema implementa la Regla 3-2-1 para protección de datos que minimiza los errores humanos y se asegura que la toma de decisiones se base en datos actualizados y sin fallos. La inclusión del NAS virtual con RAIDZ1 reduce el tiempo de inactividad ante un fallo de disco.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 12 de 89



## 3.2. Fases, actividades y cronología

Para garantizar el éxito del proyecto y cumplir con los objetivos establecidos, se ha dividido el trabajo en cinco fases principales: Análisis, Diseño, Implementación, Pruebas y Documentación.

A continuación, se detalla la estimación de tiempo dedicado a cada actividad dentro de estas fases en horas:

FASE	ACTIVIDAD	TIEMPO
Análisis	Análisis sobre la estructura y topología de red	8
	Análisis de requisitos de seguridad	3
	Selección de herramientas	3
	Planificación del entorno de virtualización	2
Diseño	Instalación y configuración de las máquinas virtuales	8
	Despliegue del servidor web seguro	8
	Implementación de la VPN con Wireguard	10
	Configuración de red y servicios en pfSense	15
Desarrollo	Programación de la intranet y gestión de sesiones	11
	Implementación de scripts PHP de monitorización y seguridad	7
Pruebas	Pruebas de conectividad y acceso remoto por VPN	10
Documentación	Redacción de memoria técnica	10
	Desarrollo de manuales de usuario y administración	5

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 13 de 89



Y ahora se muestra la planificación del proyecto de manera cronológica con un diagrama de Gantt, especificando los días en los que se desarrolla cada tarea:

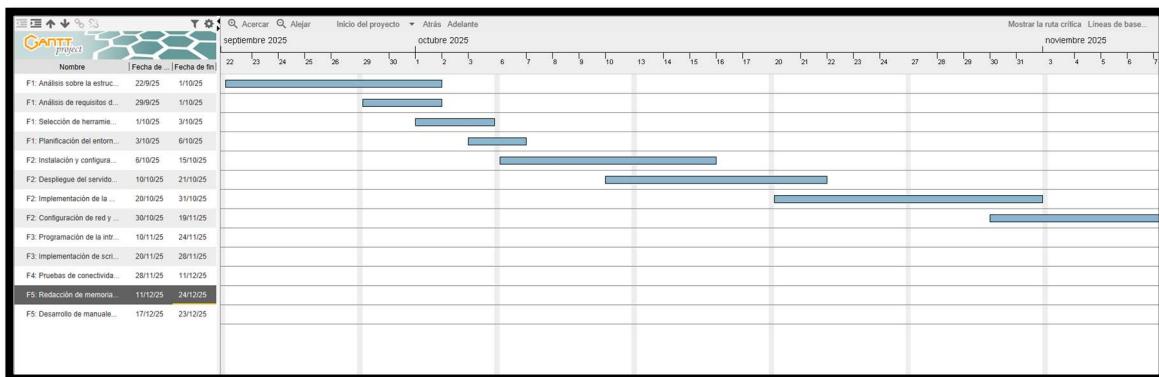


Imagen 2 - Tabla creada mediante el programa 'GanttProject'

### 3.3. Metodología seguida

La metodología elegida para el desarrollo y despliegue de esta infraestructura es el modelo de Cascada (Waterfall), ya que se ha seguido una metodología estructurada y secuencial que garantiza el éxito en la implementación de la infraestructura de red segura.

En primer lugar, la fase inicial consiste en el análisis de las necesidades y objetivos de la empresa. Se identifica la utilidad para los usuarios finales y los requisitos para el funcionamiento del acceso remoto y la que no se pierda la información. Después se procede al estudio de las herramientas tecnológicas disponibles, evaluando y seleccionando las soluciones *Open Source* más adecuadas (WireGuard, Apache, pfSense y TrueNAS) por su rendimiento y robustez.

Una vez definida la base teórica, pasamos a la fase de diseño de la arquitectura planificando la topología de red lógica, definiendo los segmentos de red (WAN, LAN, VPN) y el esquema de direccionamiento IP. Paralelamente, se diseñan las políticas de seguridad perimetral para el firewall y la estructura de la intranet corporativa incluyendo la arquitectura de almacenamiento RAID 5 para el servidor NAS.

Con el diseño completado, se inicia la fase de implementación técnica en un entorno de virtualización controlado. Se instalan y configuran los sistemas operativos de los servidores y el firewall, seguidos por el despliegue de los servicios críticos: el servidor web seguro (Apache con SSL) y el túnel VPN (WireGuard) así como la configuración del servidor NAS (TrueNAS) y el montaje del recurso compartido (NFS) en el servidor web, por otro lado se desarrolló la intranet en PHP, implementando los scripts y las medidas de seguridad en la aplicación web.

Finalmente, se ejecuta una fase de pruebas y validación para certificar el correcto funcionamiento del sistema. Se verifica la conectividad desde diferentes redes y se validó la funcionalidad de la intranet. Todo el proceso ha quedado registrado en la documentación técnica y los manuales de usuario, que servirán para la formación del personal y el mantenimiento futuro del sistema.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 14 de 89



## 3.4. Recursos

Para la realización de este proyecto, se han empleado los siguientes recursos.

Tipo	Descripción	Cantidad
Hardware	Lenovo ThinkCentre Neo 50t Gen 5	1
Hardware	Lenovo ThinkCentre Neo 50q Gen 4 'Mini'	4
Hardware	Netgate 2100	1
Hardware	UGREEN NASync DXP4800 Plus	1
Hardware	Samsung Galaxy A17	4
Hardware	Pack Monitor + Ratón/Teclado/Auriculares (PCVIP)	4
Software	Ubuntu Server 22.04 LTS	1
Software	Ubuntu Desktop 22.04LTS	4
Software	Wireguard	4
Software	Apache HTTP Server	4
Software	Visual Studio Core	4
Software	TrueNAS 25.10.0.1	1
Humanos	Administrador de Sistemas y Red	1
Humanos	Desarrollador Web	1
Humanos	Coordinador del Proyecto	1
Humanos	Formador	1
Humanos	Equipo Soporte técnico	2

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 15 de 89



Las especificaciones técnicas de los equipos a adquirir son las siguientes:

- Servidor (Lenovo ThinkCentre Neo 50t Gen 5): Formato torre para mejor refrigeración. Procesador Intel Core i5-14400, 16 GB de RAM y 512 GB SSD.
- Router (Netgate 2100): Hardware dedicado con procesador ARM Dual Core y 4 GB de RAM DDR4.
- Servidor de Almacenamiento (UGREEN NASync DXP4800 Plus): NAS con 4 bahías, lo que permite realizar el RAID 5 con 3 discos, con procesador Intel Plentium Gold 8505, 8 GB de RAM DDR5 y 128 GB SSD. Los discos duros irán a cargo de la empresa en función de sus necesidades.
- Equipos Cliente (Lenovo ThinkCentre Neo 50q Gen 4): Form "Mini" para optimizar espacio. Procesador Intel Core i5-13420H, 8 GB de RAM y 256 GB SSD. Se adquieren sin S.O. para reducir costes.
- Móviles corporativos (Samsung Galaxy A17 LTE): 8 GB de RAM y 256 GB de almacenamiento, con batería de 5000 mAh para jornada completa.
- Pack de Periféricos (Combo All-in-One PCVIP): Solución económica que incluye un monitor de 27" Curvo para mejorar la productividad y ergonomía, junto con teclado, ratón, alfombrilla y auriculares con micrófono, unificando toda la dotación del puesto de trabajo.

Tanto el servidor Lenovo ThinkCentre Neo 50t como los equipos cliente Lenovo ThinkCentre Neo 50q se adquieren en su versión 'Sin Sistema Operativo'. Esto permite un ahorro de costes y facilita la instalación personalizada de las imágenes corporativas: Ubuntu Server 22.04 LTS para el servidor y Ubuntu Desktop 22.04 LTS o Windows 11 Pro para los puestos de usuario estándar.

En este caso se utilizará para los empleados como Sistema Operativo Ubuntu Desktop 22.04 LTS y para el servidor Ubuntu Server 22.04 LTS, pero si el caso fuera real y en este momento se utilizaría la última versión compatible (Ubuntu Desktop 24.04 LTS y Ubuntu Server 24.04 LTS).

Las tareas de cada integrante del equipo son las siguientes:

- Administrador de Sistemas y Red: Responsable de la configuración y mantenimiento de toda la infraestructura de red.
- Desarrollador Web: Encargado de la programación de la intranet y gestión de datos.
- Coordinador del Proyecto: Responsable de la planificación, ejecución y control del proyecto.
- Formador: Responsable de formar a los usuarios para que tengan los conocimientos necesarios sobre el uso adecuado y seguro de la intranet y la conexión remota.
- Equipo Soporte técnico: Encargados de la asistencia a usuarios finales e incidencias de conectividad.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 16 de 89



## 3.5. Presupuesto

Estos son los gastos esperados del proyecto por su implementación:

Gastos mano de obra		
Gestión y Planificación del Proyecto	50 horas	608,50 €
Configuración de Infraestructura de Red	80 horas	1226,40 €
Desarrollo de la Intranet Corporativa	80 horas	1226,40 €
Formación a Usuarios Finales	25 horas	268,30 €
Soporte Técnico y Resolución de Incidencias	120 horas	1110,00 €
<b>TOTAL</b>		<b>4439,60 €</b>

Personal encargado de mano de obra	
Coordinador del Proyecto	Área 1 Grupo A Nivel 1
Administrador de Sistemas y Red	Área 3 Grupo C Nivel 1
Desarrollador Web	Área 3 Grupo C Nivel 1
Formador	Área 3 Grupo D Nivel 1
Equipo Soporte Técnico	Área 2 Grupo E Nivel 1

La jornada anual estipulada es de 1800 horas anuales según convenio.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 17 de 89



## Gastos fijos

Ubuntu Server 22.04 LTS	1 unidad	0,00 €
pfSense CE 2.7.2	1 unidad	0,00 €
Wireguard VPN	4 unidades	0,00 €
Apache HTTP	4 unidades	0,00 €
TrueNAS 25.10.0.1	1 unidades	0,00 €
Ubuntu Desktop 22.04 LTS	4 unidades	0,00 €
Visual Studio Core	4 unidades	0,00 €
<b>TOTAL</b>		<b>0,00 €</b>

En caso de querer Windows 11 Pro, la empresa se hará cargo de las licencias (259,00 € por licencia).

## Coste Hardware

Servidor	1 unidad	775,71 €
Router	1 unidad	369,00 €
PC para empleados	4 unidades	1701,24 €
Móviles Corporativos	4 unidades	796,00 €
Pack Monitor + Teclado + Ratón	4 unidades	796,00 €
Servidor de almacenamiento	1 unidad	559,99 €
<b>TOTAL</b>		<b>4997,94 €</b>

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 18 de 89



En función de los requisitos de la empresa, se elegirá el Pack Económico que contendrá solo el Servidor y el router con la instalación y el desarrollo de los servicios, o el Pack Completo, con todo lo nombrado anteriormente incluido.

**Gastos Pack Económico**

**5584,31 €**

**Gastos totales sin IVA**

**4411,60 €**

**Gastos Pack Completo**

**9437,54 €**

**Gastos totales sin IVA**

**7455,66 €**

Para facilitar la inversión y garantizar el mantenimiento, se ha diseñado un modelo de cobro mixto.

El coste del proyecto se abona en tres pagos: un pago inicial para la adquisición de hardware, un segundo pago tras la fase de instalación de la infraestructura, y un pago final al concluir la fase de desarrollo de la intranet.

Tras la entrega, se establece una cuota periódica por el servicio de Soporte Técnico, que cubre el mantenimiento, actualizaciones y asistencia a usuarios.

**Ingresos fijos por cliente (Pack Económico)**

Pago inicial

1600,00 €

Pago fase instalación

4200,00 €

Pago final tras desarrollo

4200,00 €

**TOTAL**

**10000,00 €**

Los dos primeros pagos cubren todos los costes y el tercer pago supone prácticamente el beneficio neto por servicio.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 19 de 89



## Ingresos fijos por cliente (Pack Completo)

Pago inicial	5600,00 €
Pago fase instalación	4200,00 €
Pago final tras desarrollo	4200,00 €
<b>TOTAL</b>	<b>14000,00 €</b>

## Ingreso mensual por cliente

Tasa mensual de mantenimiento y soporte	250,00 €
---	----------

Este pago mensual incluye monitorización del servidor, actualizaciones de seguridad y soporte remoto a usuarios.

El plan mensual consiste en una auditoría semanal que incluye revisión de logs de pfSense para identificar patrones de tráfico anómalo, comprobación de estado correcto del backup, verificación del estado del servidor, atención a incidencias y asistencia remota en caso de error crítico.

Hay que tener en cuenta que el Pack Completo está pensado para PYMES que vayan a trabajar con un máximo de 4 empleados, en caso de querer una mayor cantidad de usuarios las tarifas se modificarían en función de la cantidad de empleados requeridos.

Ahora lo siguiente es calcular los beneficios y la rentabilidad:

- Pack económico: Margen (Ingresos – Coste Fijo) = 10.000 – 5.584,31 = 4.415,69 €
- Pack completo: Margen = 14.000 – 9.437,54 = 4.562,46 €

Ese margen es lo que cada venta aporta para cubrir costes fijos y generar beneficio.

## Punto de equilibrio (Pack Económico)

Mínimo de clientes para rentabilizar el proyecto	0,55 clientes
--	---------------

El proyecto es rentable desde el primer cliente y sin incluir el plan mensual.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 20 de 89



## Punto de equilibrio (Pack Completo)

Mínimo de clientes para rentabilizar el proyecto

**0,67 clientes**

El proyecto es rentable desde el primer cliente y sin incluir el plan mensual.

## ROI a 1 año para 15 usuarios (Pack Económico)

(Ingresos – Inversión) / Inversión x 100

**79,07 %**

Se ha utilizado la formula del ROI suponiendo que en un año realizamos nuestro servicio a 15 clientes.

Se puede deducir del resultado que el proyecto tiene alta viabilidad económica ya que por cada 100 € invertidos la empresa recupera 79,07 € de beneficio puro.

La inversión neta anual sería:  $5584,31 \times 15 = 83764,65 \text{ €}$

Los ingresos netos anuales serían  $10000 \times 15 = 150000,00 \text{ €}$

El beneficio neto sería  $150000,00 - 83764,65 = 66235,35 \text{ €}$

## ROI a 1 año para 15 usuarios (Pack Completo)

(Ingresos – Inversión) / Inversión x 100

**48,34%**

Se puede deducir del resultado que el proyecto tiene alta viabilidad económica ya que por cada 100 € invertidos la empresa recupera 48,34 € de beneficio puro.

La inversión neta anual sería:  $9437,54 \times 15 = 141563,10 \text{ €}$

Los ingresos netos anuales serían  $14000 \times 15 = 210000,00 \text{ €}$

El beneficio neto sería  $210000,00 - 141563,10 = 68436,90 \text{ €}$

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 21 de 89



## 3.5.1. Fase de análisis

En esta fase inicial, se ha realizado un estudio exhaustivo de las distintas soluciones tecnológicas disponibles para cubrir las necesidades del proyecto. El objetivo ha sido seleccionar aquellas herramientas que ofrezcan el mejor equilibrio entre seguridad, rendimiento, facilidad de gestión y sobretodo en coste, ya que me he centrado en que las herramientas utilizadas sean Open Source porque el proyecto está enfocado en PYMES.

### SISTEMA OPERATIVO DEL SERVIDOR

Se ha seleccionado Ubuntu Server 22.04 LTS. Esta decisión se basa en la optimización de recursos y costes, siendo prioritario el cero coste de licencias (Open Source). Su arquitectura es robusta y segura, ideal para exposición 24/7, con el respaldo clave de un Soporte a Largo Plazo (LTS) que garantiza cinco años de mantenimiento y una amplia comunidad para soporte y rápida disponibilidad de software moderno. En caso de tener que implementarlo a día de hoy se utilizaría la versión más actual, en este caso 24.04 LTS, pero seguiría estando bien utilizar la versión 22.04 LTS, ya que sigue teniendo soporte.

Opción	Ventajas	Desventajas
Ubuntu Server (Linux)	Gratis y Open Source.	No tiene interfaz gráfica, gestión por terminal.
	Gran comunidad y soporte.	Requiere conocimientos de comandos Linux.
	Consumo mínimo de recursos.	

Opción	Ventajas	Desventajas
Windows Server (Microsoft)	Interfaz gráfica amigable que permite fácil administración.	Coste elevado de licencias.
	Soporte oficial de Microsoft.	Mayor superficie de ataque para malware común.
	Mayor compatibilidad con servicios Microsoft.	Mayor consumo de recursos de RAM y CPU.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 22 de 89



Para la infraestructura de este proyecto, se determina que la interfaz gráfica no es necesaria y su presencia solo penalizaría la eficiencia y el rendimiento operativo del servidor. Ubuntu Server 22.04 LTS garantiza la estabilidad, seguridad y fiabilidad requeridas para el servicio continuo, sin generar ningún incremento en el presupuesto por concepto de licencias. Por todas estas razones, es la opción técnica y económica más adecuada para el caso de estudio.

Recordemos que en caso de aplicar el proyecto, se utilizaría la última versión de Ubuntu Server LTS disponible (Ubuntu Server 24.04 LTS).

## SERVICIO DE VPN (Acceso Remoto)

La elección de WireGuard se fundamenta en su eficiencia y una buena experiencia de usuario. Al utilizar un protocolo VPN moderno, garantiza una conexión casi instantánea y un impacto mínimo en el consumo de recursos, lo cual es crucial para el teletrabajo.

La primera opción fue OpenVPN, pero las pruebas técnicas demostraron que este era más lento y significativamente más propenso a errores de configuración, justificando la adopción de WireGuard como la solución más rápida, estable y sencilla para el acceso remoto.

Opción	Ventajas	Desventajas
WireGuard	Código muy ligero, fácil de auditar.	Menos tiempo en el mercado.
	Velocidad de conexión superior y alto rendimiento.	Protocolo basado en UDP.
	Configuración sencilla y moderna.	

Opción	Ventajas	Desventajas
OpenVPN	Muy utilizado en la industria.	Código muy pesado.
	Máxima compatibilidad.	Rendimiento más lento.
	Flexibilidad para usar protocolos TCP o UDP.	Configuración compleja.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 23 de 89



Para este proyecto, WireGuard es la opción elegida por su superioridad técnica en velocidad, rendimiento y eficiencia. Su configuración sencilla minimiza los errores operativos, mientras que su diseño ligero garantiza una conexión casi instantánea con mínimo consumo de recursos, superando las desventajas de complejidad y lentitud observadas en OpenVPN.

A pesar de que WireGuard opera exclusivamente sobre UDP, lo que podría ser bloqueado por firewalls restrictivos (a diferencia de OpenVPN que soporta TCP para evadir bloqueos), su rendimiento superior y su impacto mínimo en la batería justifican su selección como la mejor alternativa para el acceso remoto.

## SEGURIDAD PERIMETRAL (Firewall)

En este proyecto pfSense permite implementar seguridad perimetral de nivel empresarial sin depender de licencias propietarias costosas. Al ser de licencia gratuita, el presupuesto puede invertirse íntegramente en hardware de calidad. Aunque requiere conocimientos técnicos específicos para su administración, su base en FreeBSD garantiza una plataforma robusta y estable.

Opción	Ventajas	Desventajas
pfSense	Licencia gratuita (Open Source).	Requiere conocimientos específicos de redes y sistemas FreeBSD.
	Basado en FreeBSD.	
	Interfaz web completa y profesional.	

Opción	Ventajas	Desventajas
Cisco	Hardware dedicado.	Coste de adquisición muy alto.
	Soporte técnico garantizado.	Licencias anuales obligatorias.
	Estándar en grandes entornos corporativos.	Flexibilidad limitada, hardware ligado al firmware.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 24 de 89



Este proyecto prioriza el control de costes y la inversión en hardware propio en lugar de depender de licencias y soportes anuales obligatorios.

Por ello se ha elegido pfSense, que ofrece las características de seguridad perimetral de nivel profesional sobre una base robusta y gratuita. Esto justifica su elección sobre alternativas con licencia.

## SERVIDOR WEB (Intranet)

Se ha seleccionado Apache HTTP Server por ser muy flexible y fácil de gestionar, características fundamentales para el entorno de una Intranet corporativa.

La decisión se basa en su capacidad para facilitar la seguridad y la gestión de accesos, Apache permite modificar las reglas y permisos de seguridad de forma sencilla dentro de cada carpeta sin necesidad de alterar la configuración principal del servidor. Además, Apache garantiza una excelente integración con lenguajes dinámicos como PHP, muy utilizados en este proyecto.

Opción	Ventajas	Desventajas
Apache HTTP Server	Estándar muy documentado y comunidad muy grande.	Lento bajo cargas muy altas.
	Integración fácil con PHP.	Alto consumo de RAM.
	Muy estable.	

Opción	Ventajas	Desventajas
Nginx	Rápido para contenido estático.	Configuración más compleja para aplicaciones dinámicas.
	Soporta muchas conexiones simultáneas.	No soporta .htaccess.
	Open Source.	

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 25 de 89



Opción	Ventajas	Desventajas
Microsoft IIS	Integración con el entorno Microsoft.	Coste de licenciamiento elevado.
	Interfaz gráfica de administración.	Dependencia de la plataforma Windows.
	Soporte garantizado de fabricante.	Baja compatibilidad con entornos Open Source.

Para este proyecto, donde la carga de tráfico no es masiva, se ha seleccionado Apache ya que es la más adecuada para la Intranet, debido a que prioriza la flexibilidad y la facilidad de gestión de permisos sobre la velocidad pura.

Además, las ventajas de sencillez y compatibilidad superan la eficiencia de Nginx (más complejo de configurar para contenido dinámico) y el alto coste de licenciamiento de Microsoft IIS.

## SISTEMA DE ALMACENAMIENTO (NAS y Backups)

Se ha seleccionado TrueNAS como el sistema operativo para el almacenamiento de red (NAS) debido a su uso del avanzado sistema de archivos ZFS.

Esta elección es crucial porque ZFS ofrece una protección robusta contra la corrupción de datos mediante la verificación constante de la integridad. Al proporcionar capacidades avanzadas de RAID por software, TrueNAS garantiza la seguridad, consistencia y fiabilidad de los backups sin depender de costosas soluciones de hardware. La plataforma también ofrece una interfaz web profesional que centraliza la gestión de almacenamiento, simplificando las tareas administrativas.

Opción	Ventajas	Desventajas
TrueNAS	Gratis y basado en FreeBSD.	Requiere reservar recursos de RAM para el host debido al caché.
	Soporte nativo para RAID 5.	
	Interfaz web profesional para gestión de almacenamiento.	

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 26 de 89



Opción	Ventajas	Desventajas
Sinology	Hardware dedicado.	Coste de adquisición elevado.
	Software muy fácil de usar.	Software propietario cerrado.
	Soporte técnico.	

Para este proyecto se ha elegido TrueNAS, ya que prioriza la integridad de los datos y la seguridad de los backups mediante el uso del sistema ZFS, sin generar costes de licencia. Aunque se necesite dedicar una cantidad adecuada de memoria RAM al host, esta inversión se justifica plenamente por la protección avanzada de datos que se obtiene, superando la comodidad de las soluciones propietarias de alto coste.

### 3.5.2. Fase de implementación

Se ha realizado la implementación completa del proyecto en un entorno virtualizado (VirtualBox) para replicar un entorno empresarial con control total sobre la topología de red y los recursos.

Las máquinas virtuales utilizadas son las siguientes:

Sistema	Especificaciones
Ubuntu Server 22.04 LTS (SRV1)	2 núcleos, 4096 MB de RAM, 25 GB de disco, adaptador Red Interna (LAN-EMPRESA).
Windows 10 (Empleado 1)	2 núcleos, 2048 MB de RAM, 50 GB de disco, adaptador Puente.
Ubuntu Desktop 22.04 LTS (Empleado 2)	2 núcleos, 4096 MB de RAM, 25 GB de disco, adaptador Red Interna (LAN-EMPRESA).
pfSense (Router Empresa)	2 núcleos, 2048 MB de RAM, 16 GB de disco, adaptador Puente y adaptador Red Interna (LAN-EMPRESA).
TrueNAS (NAS Empresa)	2 núcleos, 4096 MB de RAM, disco de 16 GB para SO y 3 discos de 50 GB cada uno para RAID 5, adaptador Red Interna (LAN-EMPRESA).

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 27 de 89



Además de estas máquinas virtuales, se utilizó un dispositivo físico (móvil personal, iPhone 11) para simular un móvil corporativo conectado a la Red Externa (WAN) y validar la funcionalidad del cliente VPN.



Imagen 3 - Panel de administración de VirtualBox con las máquinas virtuales que conforman la infraestructura del proyecto.

## Definición de la Topología de Red

La segmentación de la red en VirtualBox sigue el diagrama de arquitectura planteado:

Red Externa (WAN): Se utilizó un Adaptador Puente para conectar la máquina pfSense al host físico, y por extensión, a Internet. Esto simula que la Red Externa es 192.168.1.0/24 y permite que los clientes externos (EMP 2 y el móvil) se conecten desde fuera.

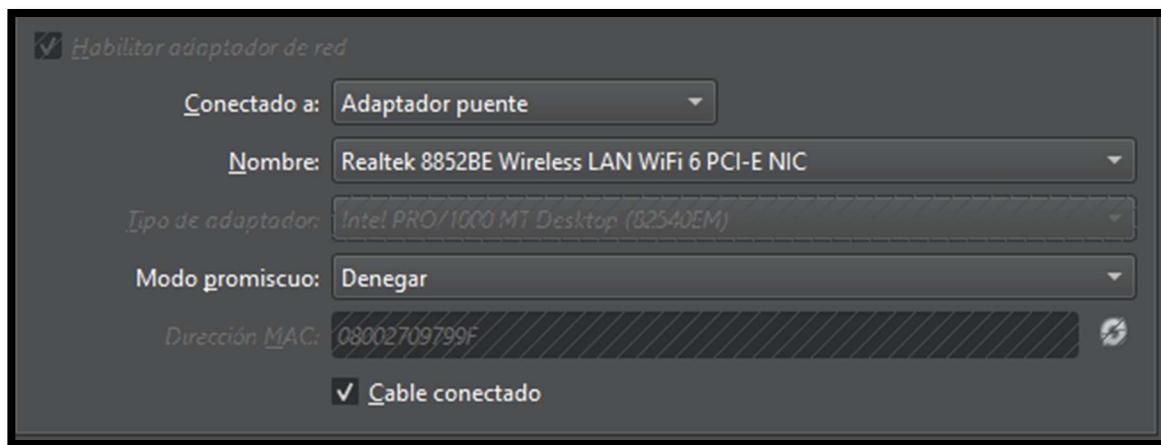


Imagen 4 – Configuración de adaptador puente

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 28 de 89



Red Interna (LAN): Se ha creado una Red Interna y privada en VirtualBox (LAN-EMPRESA) utilizando el segmento 192.168.50.0/24. Todos los servidores críticos (SRV1, NAS) y los empleados internos (EMP 1) se conectan a esta red aislada.

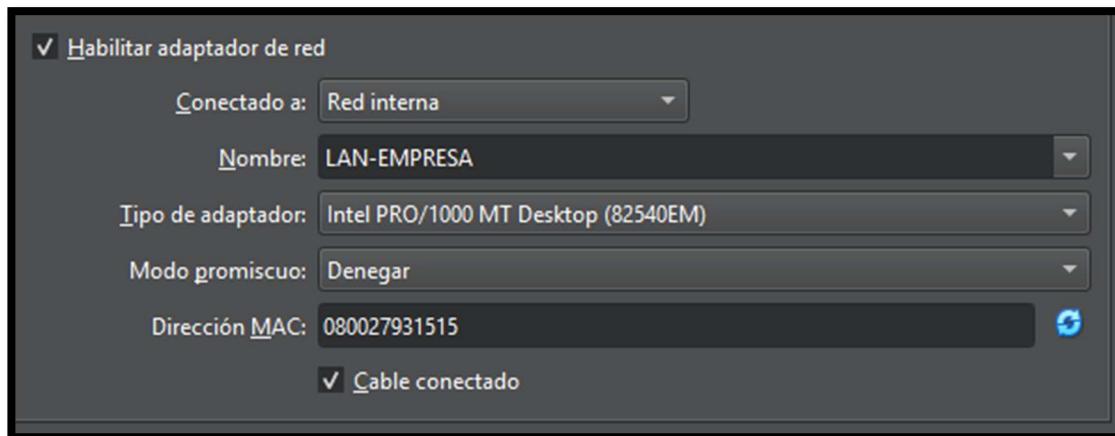


Imagen 5 – Configuración de la red interna (LAN-EMPRESA)

## Implementación del Firewall Perimetral: pfSense

La primera máquina en ser configurada fue el pfSense , que actúa como el punto de control de acceso principal y el *gateway* de la Red Interna (LAN). Se utilizó la ISO de la versión 2.7.2 para la instalación.

La finalidad de la instalación era que el *router* estuviese conectado a las dos redes y definir el direccionamiento IP:

WAN (em0): Conectada al Adaptador Puente. Se configuró como IP Estática (Static IPv4) para evitar que la dirección WAN cambie automáticamente y así asegurar la fiabilidad del *Port Forward* de Internet. Se asignó la IP 192.168.1.147.

LAN (em1): Conectada a la Red Interna (LAN-EMPRESA). Se asignó la IP estática 192.168.50.1, que actúa como *Gateway* para todos los dispositivos de la empresa.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 29 de 89



```
Router Empresa [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
8) Shell

Enter an option:

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 54d44563bff8c4c8390b
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.147/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24

8) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

Imagen 6 – Panel de administración de pfSense

Una vez configurado, se accedió a la interfaz gráfica de pfSense (utilizando la IP WAN 192.168.1.147) para definir las reglas de seguridad perimetral.

Las reglas configuradas en la interfaz WAN son las siguientes:

The changes have been applied successfully. The firewall rules are now reloading in the background.  
Monitor the filter reload progress.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/3.70 MB	IPv4 TCP	WAN subnets *	*	This Firewall (self)	443 (HTTPS)	*	none		PFSENSE HTTPS WAN	
✓ 0/0 B	IPv4 UDP	*	*	WAN address	51820	*	none		WIREGUARD UDP WAN	
✓ 0/0.24 MB	IPv4 UDP	*	*	192.168.50.10	51820	*	none		NAT	

Imagen 7 – Configuración de reglas del router pfSense

PFSENSE HTTPS WAN: Permite el acceso seguro (HTTPS) a la interfaz de administración de pfSense (192.168.1.147) solo desde equipos que se encuentren en la misma subred WAN. Esta regla es necesaria porque el firewall bloquea por defecto el acceso a su propia interfaz de gestión desde la red externa.

WIREGUARD UDP WAN: Es la regla que permite que los clientes externos envíen el tráfico cifrado de WireGuard al puerto 51820 del firewall. Es decir, permite que el tráfico UDP 51820 llegue a pfSense desde internet.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 30 de 89



NAT (Redirección): Esta regla indica que todo el tráfico UDP que entra por el puerto 51820 de la WAN (Regla 2) debe ser redirigido internamente al puerto 51820 de la IP privada del Servidor Ubuntu (192.168.50.10).

Gracias a las reglas 2 y 3 combinadas, se consigue que la única forma de acceder a los recursos internos de la LAN sea a través del túnel VPN, eliminando la superficie de ataque del resto de servicios.

A pesar de que todos los servidores críticos (SRV1, NAS) se han configurado con IPs estáticas manualmente en sus respectivos sistemas operativos, se mantuvo el Servidor DHCP habilitado en la LAN.

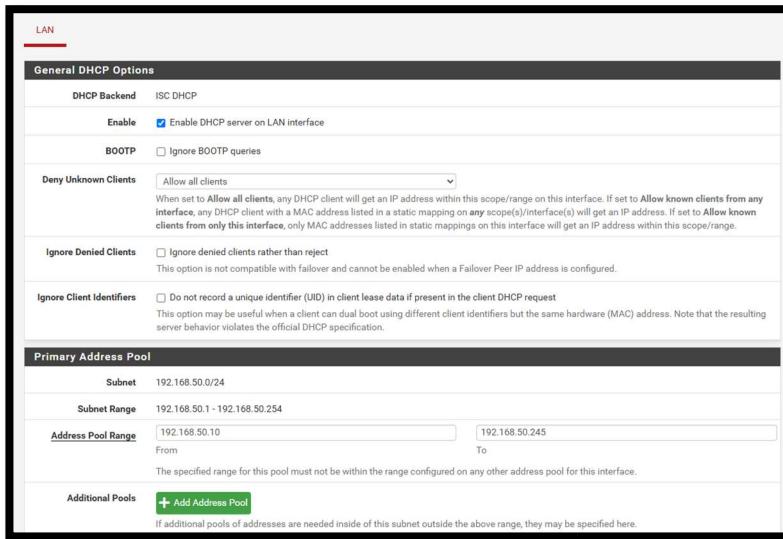


Imagen 8 – Configuración general DHCP

Rango de Asignación: Se configuró el Address Pool Range de 192.168.50.10 a 192.168.50.245 .

El DHCP permanece activo para asignar direcciones IP a clientes genéricos y a dispositivos que puedan añadirse en el futuro sin la necesidad de una configuración estática manual, manteniendo así la flexibilidad operativa.

Muy importante establecer la IP WAN como estática, ya que la regla de Redirección de Puertos (NAT) del router físico de casa debe apuntar siempre a la misma dirección IP (192.168.1.147). Si se usara DHCP, la IP podría cambiar, rompiendo el acceso VPN de los empleados remotos.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 31 de 89

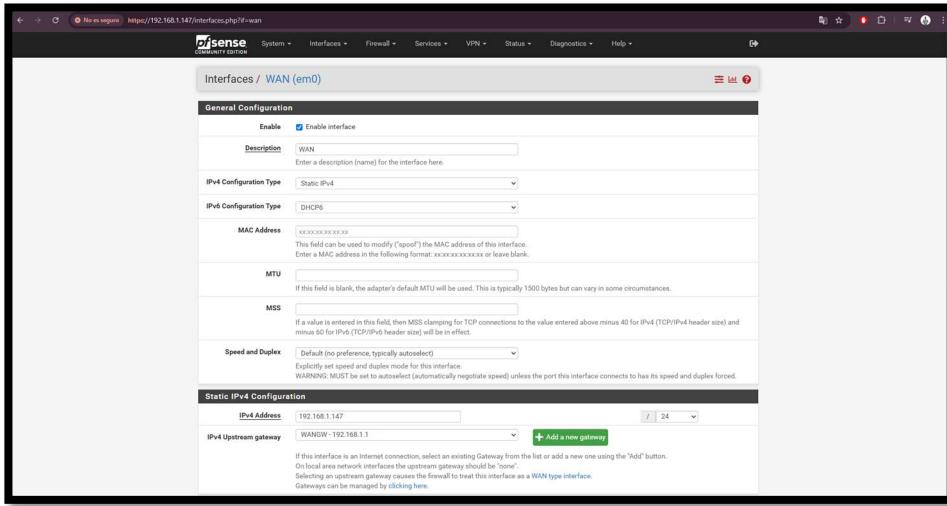


Imagen 9 – Configuración de la interfaz WAN

## Implementación del Servidor Central: Ubuntu Server (SRV1)

Después de configurar el router pfSense, el siguiente paso fue el Servidor Central (SRV1), que es el host principal para la Intranet y el Servidor VPN. Se instaló el Sistema Operativo Ubuntu Server 22.04 LTS.

Tras la instalación completa, la configuración de red del servidor es la siguiente:

```
srv1@srv1:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 0.0.0.0 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd 0.0.0.0 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:93:15:15 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.10/24 metric 100 brd 192.168.50.255 scope global dynamic enp0s3
        valid_lft 7198sec preferred_lft 7198sec
    inet6 fe80::a00:27ff:fe93:1515/64 scope link
        valid_lft forever preferred_lft forever
srv1@srv1:~$
```

Imagen 10 – Configuración de red del Servidor (SRV1)

Se procedió con la instalación del servidor web y los componentes necesarios para el desarrollo de la Intranet en PHP.

Además se instalaron libapache2-mod-php para el soporte de las páginas .php de la Intranet y apache2-utils (aunque el uso de .htaccess se modificó), son utilidades estándar de administración. Tras la instalación, se comprobó que el servicio Apache se estaba ejecutando correctamente

# Servidor Web con Acceso Seguro a través de VPN

*Mohammed Maamla Razzak*

maamla\_mohammed\_asir

Página 32 de 89



```
srv1@srv1:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Wed 2025-10-15 18:33:28 UTC; 47s ago
     Docs: https://httpd.apache.org/docs/2.4/
Main PID: 2191 (apache2)
  Tasks: 55 (limit: 4611)
    Memory: 5.5M (peak: 5.6M)
       CPU: 35ms
      CGroup: /system.slice/apache2.service
           └─2191 /usr/sbin/apache2 -k start
              ├─2193 /usr/sbin/apache2 -k start
              ├─2194 /usr/sbin/apache2 -k start
              └─2194 /usr/sbin/apache2 -k start

oct 15 18:33:28 srv1 systemd[1]: Starting apache2.service - The Apache HTTP Server...
oct 15 18:33:28 srv1 apache2[2190]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive
oct 15 18:33:28 srv1 systemd[1]: Started apache2.service - The Apache HTTP Server.
lines: 1-16/16 (END)
[2]+  Stopped                  sudo systemctl status apache2
srv1@srv1:~$
```

**Imagen 11 – El servicio Apache en funcionamiento en SRV1**

La Intranet corporativa se creó para ser funcional y de bajo consumo de recursos. Se estructuró en el directorio /var/www/html (Esta estructura no es la de la intranet final, ya que se ha ido mejorando a medida que avanzaba el proyecto).

```
srv1@srv1:/var/www/html$ ls
admin.css empleados.html index.html procesar_solicitud.php solicitudes.html
srv1@srv1:/var/www/html$ cd admin
srv1@srv1:/var/www/html/admin$ ls
dashboard.php solicitudes_guardadas.html
srv1@srv1:/var/www/html/admin$ cd ..
srv1@srv1:/var/www/html$ cd css
srv1@srv1:/var/www/html/css$ ls
estilo2.css estilo.css
srv1@srv1:/var/www/html/css$ _
```

## **Imagen 12 – Estructura inicial de la Intranet**

La Intranet se basa en dos scripts clave: `procesar_solicitud.php` (guarda las solicitudes) y `dashboard.php` (controla la interfaz del área administrativa y gestiona el acceso para **solo** permitir usuarios administradores, aplicando el principio de mínimo privilegio en la aplicación web).

Tecnycom - Formulario de Solicitud

No seguro http://192.168.50.10/solicitudes.html

Iniciar sesión

Inicio | Directorio de Empleados | Solicitudes | Área Administrativa

Nombre completo:

Correo electrónico:

Tipo de solicitud:

Descripción:

Enviar solicitud

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 33 de 89



The screenshot shows a web browser window with the URL 192.168.50.10/solicitudes.html. A modal dialog box is displayed, asking for a user name and password. The dialog box has a title bar with the IP address 192.168.50.10 and the message 'Este sitio le pide que inicie sesión.' It contains two input fields: 'Nombre de usuario' and 'Contraseña'. Below the fields are 'Cancelar' and 'Iniciar sesión' buttons. In the background, the main page has sections for 'Nombre completo', 'Correo electrónico', 'Tipo de solicitud' (with a dropdown menu), 'Descripción', and a button 'Enviar solicitud'. At the bottom of the page is a copyright notice: '© 2025 TEcnym - Todos los derechos reservados.'

Imagenes 13 y 14 – Intranet en funcionamiento (Solicitudes.html)

Dado que la Intranet maneja datos sensibles (credenciales de acceso y solicitudes), la comunicación debe estar cifrada para cumplir con el principio de Confidencialidad.

Se generó un certificado autofirmado (Self-Signed Certificate) y su clave privada para habilitar el protocolo HTTPS en Apache, utilizando el comando openssl:

```
srv1@srvi:/etc/apache2/sites-available$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/tecnym.com.key -out /etc/apache2/ssl/tecnym.com.crt
...
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
...
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
srv1@srvi:/etc/apache2/sites-available$
```

Imagen 15 – Creación de certificado autofirmado

Tras crear el certificado y configurar el Virtual Host de Apache, la Intranet pasa a ser accesible exclusivamente por HTTPS (puerto 443).

Antes de SSL el navegador mostraba un aviso de "No seguro" al acceder por HTTP.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 34 de 89

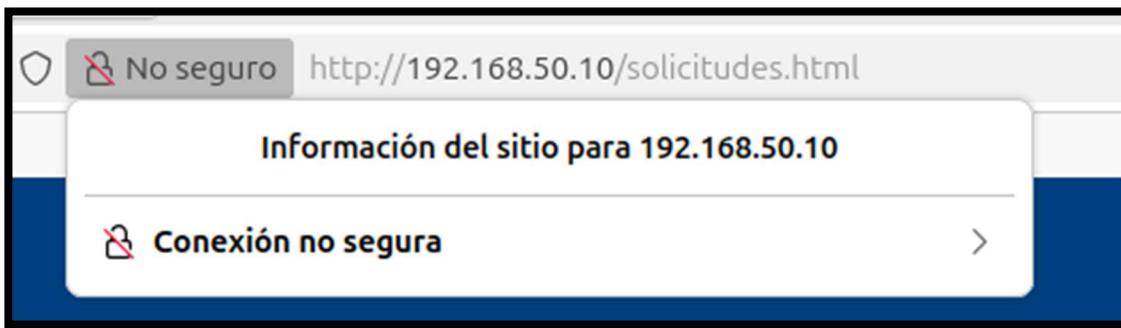


Imagen 16 – Intranet sin certificado autofirmado

Después de SSL (Acceso por HTTPS): Aunque es un certificado autofirmado (por lo que el navegador avisa del riesgo potencial), el tráfico ya viaja cifrado. El usuario puede aceptar el riesgo y continuar para establecer una conexión cifrada.

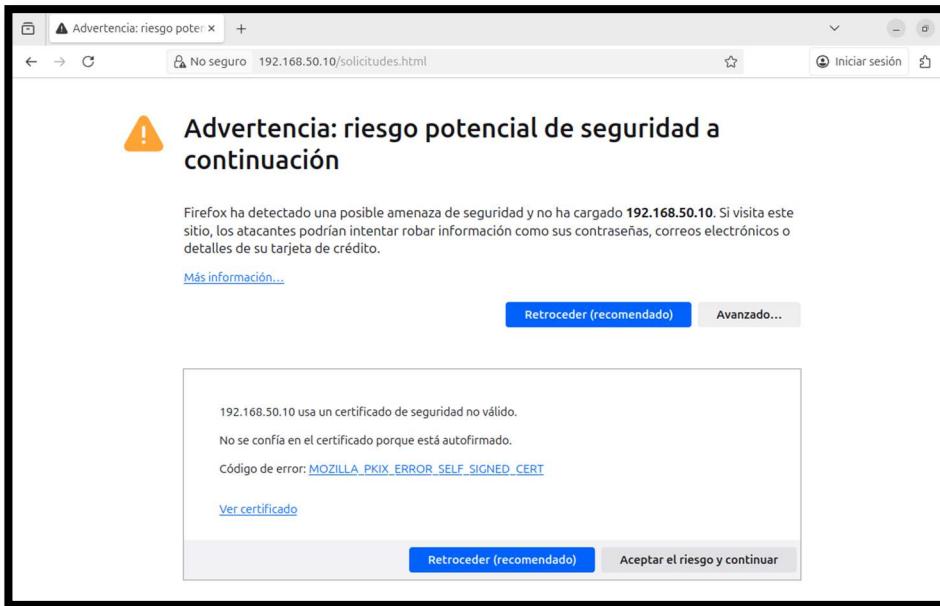


Imagen 17 – Intranet con certificado autofirmado (HTTPS)

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 35 de 89



## Implementación del Servicio VPN: WireGuard

El servicio de Red Privada Virtual (VPN) se implementa en el Servidor Central (SRV1 - 192.168.50.10) utilizando el protocolo WireGuard, seleccionado por su eficiencia, ligereza y robustez criptográfica.

La seguridad de WireGuard se basa en el intercambio de claves públicas entre el servidor y cada cliente. Lo primero fue generar los pares de claves (públicas y privadas) para el servidor y los tres clientes simulados (EMP1, EMP2, EMP3).

Se generaron las claves públicas y privadas para cada empleado, usando tuberías (|) y el comando tee para guardar los archivos.

```
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/server_private.key | wg pubkey | sudo tee /etc/wireguard/server_public.key
RbBEuk//5y6viogaheQNoKoDFhzVdynlQKCYtYq0Mgo=
srv1@srv1:~$ _
```

```
srv1@srv1:~$ sudo cat /etc/wireguard/server_private.key
gP4hgRgBXSthnWMGiFYTkDz+PAckWpezEvp+UnwOXW0Q=
srv1@srv1:~$ sudo cat /etc/wireguard/server_public.key
RbBEuk//5y6viogaheQNoKoDFhzVdynlQKCYtYq0Mgo=
srv1@srv1:~$
```

## Imagenes 18 y 19 – Creación de claves del Servidor

```
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp1_private.key | wg pubkey | sudo tee /etc/wireguard/emp1_public.key
p20HK7fNKRdiJNImxUHhUvnQQc3GtwuGcx7jBjf/f1k=
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp2_private.key | wg pubkey | sudo tee /etc/wireguard/emp2_public.key
NrjUJuY1HpMn9nJGoGR+D/dgTA9zsU3w/cK4qONWAlc=
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp3_private.key | wg pubkey | sudo tee /etc/wireguard/emp3_public.key
bBR4t3xyoazk0EcC/Nr92M1InVL0RIxphIxF0JNmXY=
srv1@srv1:~$ sudo cat /etc/wireguard/emp1_private.key
IJKi0CbJvaov155ogZD073/FH3KAxslKoSTL5e8aiw=
srv1@srv1:~$ sudo cat /etc/wireguard/emp2_private.key
oNvp3b/hk1UBXCYcjggUyimN2SeSSuEHE/MUq/04r0M=
srv1@srv1:~$ sudo cat /etc/wireguard/emp3_private.key
yMj8FsuC9DFcE0kS9yE2HcgdkUapwgnX3hU0mcrkM=
srv1@srv1:~$ sudo cat /etc/wireguard/emp1_public.key
p20HK7fNKRdiJNImxUHhUvnQQc3GtwuGcx7jBjf/f1k=
srv1@srv1:~$ sudo cat /etc/wireguard/emp2_public.key
NrjUJuY1HpMn9nJGoGR+D/dgTA9zsU3w/cK4qONWAlc=
srv1@srv1:~$ sudo cat /etc/wireguard/emp3_public.key
bBR4t3xyoazk0EcC/Nr92M1InVL0RIxphIxF0JNmXY=
srv1@srv1:~$
```

## Imagen 20 – Creación de claves del Cliente

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 36 de 89



```
GNU nano 7.2                                         /etc/wireguard/wg0.conf

[Interface]
Address = 10.8.0.1/24
ListenPort = 51820
PrivateKey = gP4hgRgBXSthnWMG1FYTkDz+PAcWpezEvp+UnwOXW0Q=

#Empleados
[Peer]
PublicKey = p20HX7fNKrdijNImxUHhUvnQQc3GtwuGcx7jBJf/f1k=
AllowedIPs = 10.8.0.2/32

[Peer]
PublicKey = NrjUJuY1HpMn9nJGoGR+D/dgTA9zsU3w/ck4qDNWAlc=
AllowedIPs = 10.8.0.3/32

[Peer]
PublicKey = bBR4t3xyoyazW0eCc/Nr92M1InVLoBIXphIxF0JNmXY=
AllowedIPs = 10.8.0.4/32
```

Imagen 21 - Archivo de configuración principal del servidor (/etc/wireguard/wg0.conf)

Para que el tráfico de la subred VPN (10.8.0.0/24) pueda saltar al segmento LAN (192.168.50.0/24) y acceder a la Intranet o al NAS, es imprescindible habilitar el reenvío de paquetes en el sistema operativo.

```
srv1@srv1:~$ echo 'net.ipv4.ip_forward=1' | sudo tee -a /etc/sysctl.conf
net.ipv4.ip_forward=1
srv1@srv1:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
srv1@srv1:~$
```

Imagen 22 – Reenvío de paquetes habilitado

Finalmente, se levanta la interfaz virtual wg0 y se comprueba su estado:

```
srv1@srv1:~$ sudo systemctl restart wg-quick@wg0
srv1@srv1:~$ sudo systemctl start wg-quick@wg0
srv1@srv1:~$ sudo systemctl status wg-quick@wg0
● wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0
   Loaded: loaded (/usr/lib/systemd/system/wg-quick@.service; enabled; preset: enabled)
   Active: active (exited) since Wed 2025-10-22 19:59:56 UTC; 9s ago
     Docs: man:wg-quick(8)
           man:wg(8)
           https://www.wireguard.com/
           https://www.wireguard.com/quickstart/
           https://git.zx2c4.com/wireguard-tools/about/src/man/wg-quick.8
           https://git.zx2c4.com/wireguard-tools/about/src/man/wg.8
   Process: 11269 ExecStart=/usr/bin/wg-quick up wg0 (code=exited, status=0/SUCCESS)
 Main PID: 11269 (code=exited, status=0/SUCCESS)
    CPU: 38ms

Oct 22 19:59:55 srv1 systemd[1]: Starting wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0...
Oct 22 19:59:56 srv1 wg-quick[11269]: [!] ip link add wg0 type wireguard
Oct 22 19:59:56 srv1 wg-quick[11269]: [!] wg setconf wg0 /dev/fd/63
Oct 22 19:59:56 srv1 wg-quick[11269]: [!] ip -4 address add 10.8.0.1/24 dev wg0
Oct 22 19:59:56 srv1 wg-quick[11269]: [!] ip link set mtu 1420 up dev wg0
Oct 22 19:59:56 srv1 systemd[1]: Finished wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0.
srv1@srv1:~$
```

Imagen 23 – El servicio Wireguard está funcionando correctamente en el Servidor (SRV1)

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 37 de 89



Pasamos a los clientes para comprobar que funcionan los servicios.

Primero el cliente Ubuntu que utilizará Ubuntu Desktop 22.04 LTS y luego el cliente Windows que utilizará Windows 10.

EMP 2 se encuentra en el segmento WAN (192.168.1.0/24).

```
emp2@emp2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2f:20:8a brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.11/24 brd 192.168.50.255 scope global dynamic noprefixroute
        valid_lft 7135sec preferred_lft 7135sec
    inet6 fe80::a00:27ff:fe2f:208a/64 scope link
        valid_lft forever preferred_lft forever
emp2@emp2:~$
```

Imagen 24 – Configuración de red del empleado Ubuntu (EMP2)

Se instaló WireGuard y se creó el archivo /etc/wireguard/emp2.conf con los datos del túnel para después levantar el servicio.

```
emp2@emp2:~$ sudo wg-quick up emp2
wg-quick: `emp2' already exists
emp2@emp2:~$ sudo wg
interface: emp2
  public key: NrjUJuY1HpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
  private key: (hidden)
  listening port: 34087

peer: RbBEuk//5y6viogaheQNoKoDFhzVdynlQKCYtYq0Mgo=
  endpoint: 192.168.1.147:51820
  allowed ips: 10.8.0.0/24
  transfer: 0 B received, 2.31 KiB sent
  persistent keepalive: every 25 seconds
emp2@emp2:~$
```

Imagen 25 – El servicio Wireguard ha sido habilitado y la conexión con el servidor ha sido exitosa

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 38 de 89

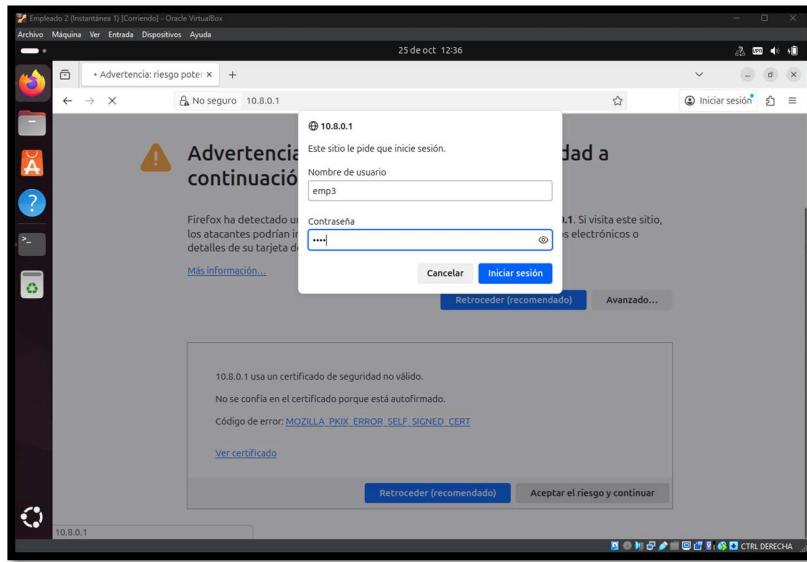


Imagen 26 – Interfaz de inicio de sesión en la intranet utilizando la VPN de Wireguard

Ahora pasamos al empleado Windows.

Se configuró el túnel emp1 con su clave privada, la IP virtual (10.8.0.2/24), y el Endpoint del firewall (192.168.1.147:51820).

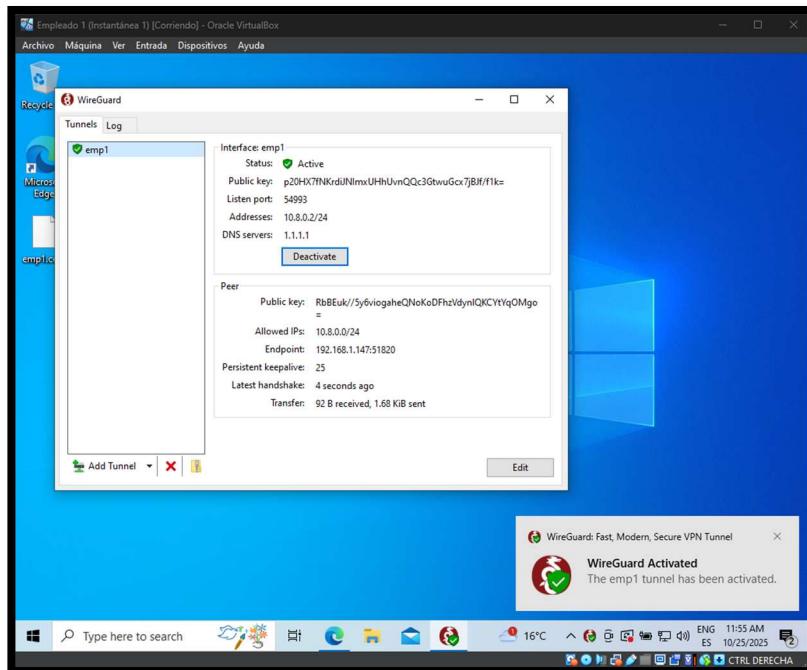


Imagen 27 – Configuración de Wireguard en el empleado Windows (EMP1)

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 39 de 89

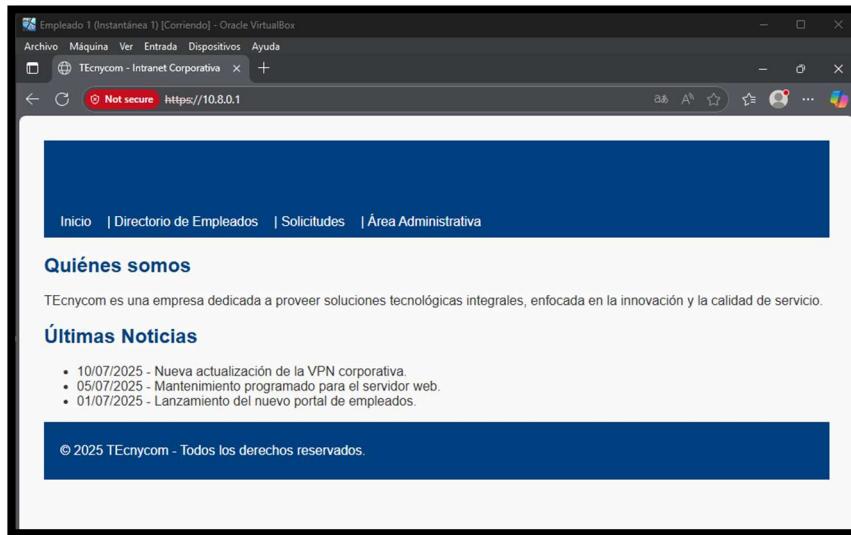
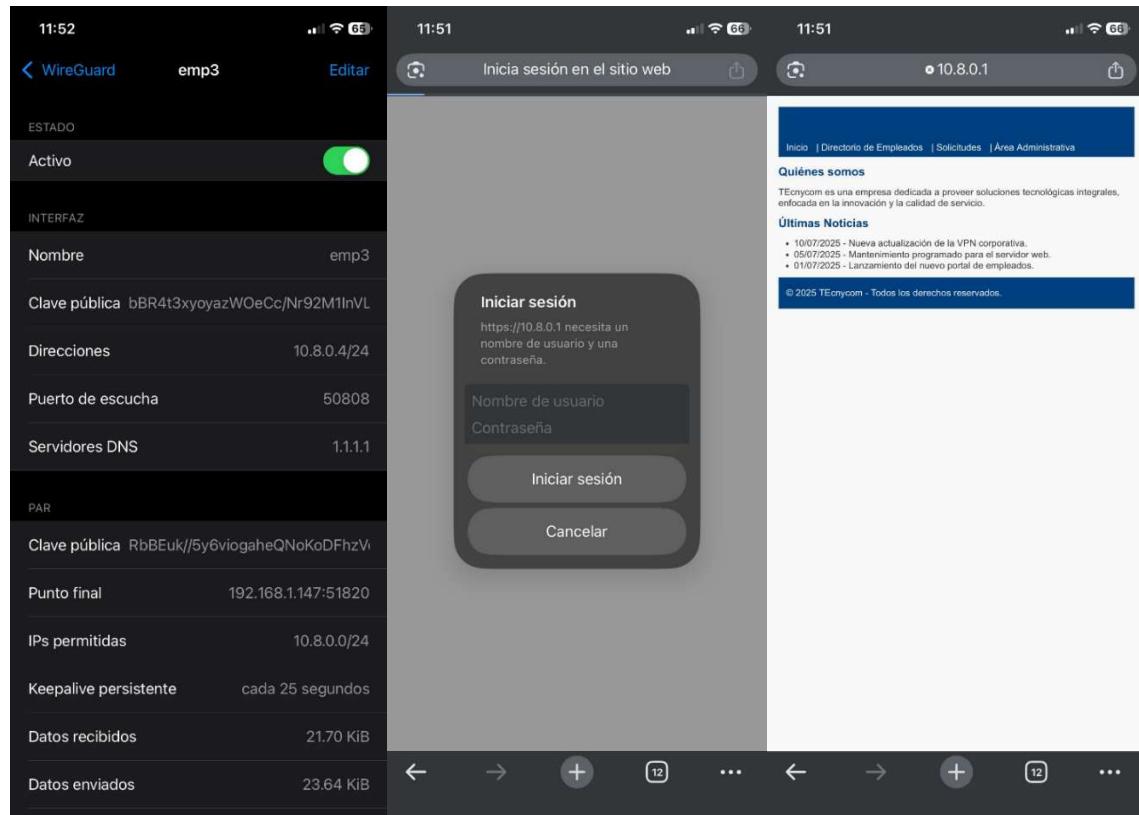


Imagen 28 – Acceso a la Intranet mediante VPN desde el empleado Windows

Finalmente se instaló la aplicación oficial de WireGuard en el dispositivo móvil y se configuró manualmente.



Imagenes 29, 30 y 31 – Configuración del servicio VPN Wireguard en el empleado móvil, interfaz de inicio de sesión e intranet desde el empleado móvil.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 40 de 89



Se utilizó el comando sudo wg en el Servidor Ubuntu (SRV1) para verificar que todos los clientes estaban conectados y enviando/recibiendo tráfico.

A screenshot of a terminal window titled "SRV 1 (Instantánea 1) [Corriendo] - Oracle VirtualBox". The window contains the output of the "sudo wg" command. It lists several wireguard interfaces (wg0) and their corresponding peers. Each peer entry includes details such as endpoint IP, allowed ips, latest handshake time, and transfer statistics. The output is color-coded for readability.

```
srv1@srv1:~$ sudo cat /etc/wireguard/emp3_public.key
bBR4t3xyoyazW0eCc/Nr92M1InVLoBIXphIxF0JNmXY=
srv1@srv1:~$ sudo cat /etc/wireguard/emp2_public.key
NrjUJuY1HpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
srv1@srv1:~$ sudo cat /etc/wireguard/emp2_private.key
oNvp3b/hk1UABXYCjqgUyi5N2SeS3uEWE/MUq/04r0M=
srv1@srv1:~$ sudo wg
interface: wg0
    public key: RbBEuk//5y6viogaheQNoKoDFhzVdynlQKCYtYq0Mgo=
    private key: (hidden)
    listening port: 51820

peer: p20HX7fNKrdiJNImxUHhUvnQQc3GtwuGcx7jBJf/f1k=
    endpoint: 192.168.1.143:54993
    allowed ips: 10.8.0.2/32
    latest handshake: 30 minutes, 50 seconds ago
    transfer: 61.92 KiB received, 96.23 KiB sent

peer: bBR4t3xyoyazW0eCc/Nr92M1InVLoBIXphIxF0JNmXY=
    endpoint: 192.168.1.136:50808
    allowed ips: 10.8.0.4/32
    latest handshake: 35 minutes, 52 seconds ago
    transfer: 23.58 KiB received, 21.73 KiB sent

peer: NrjUJuY1HpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
    allowed ips: 10.8.0.3/32
srv1@srv1:~$ sudo wg
interface: wg0
    public key: RbBEuk//5y6viogaheQNoKoDFhzVdynlQKCYtYq0Mgo=
    private key: (hidden)
    listening port: 51820

peer: NrjUJuY1HpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
    endpoint: 192.168.50.11:60316
    allowed ips: 10.8.0.3/32
    latest handshake: 1 minute, 23 seconds ago
    transfer: 276 B received, 92 B sent

peer: p20HX7fNKrdiJNImxUHhUvnQQc3GtwuGcx7jBJf/f1k=
    endpoint: 192.168.1.143:54993
    allowed ips: 10.8.0.2/32
    latest handshake: 39 minutes, 51 seconds ago
    transfer: 61.92 KiB received, 96.23 KiB sent

peer: bBR4t3xyoyazW0eCc/Nr92M1InVLoBIXphIxF0JNmXY=
    endpoint: 192.168.1.136:50808
    allowed ips: 10.8.0.4/32
    latest handshake: 44 minutes, 53 seconds ago
    transfer: 23.58 KiB received, 21.73 KiB sent
srv1@srv1:~$ _
```

Imagen 32 – Verificación de que la conexión entre Servidor y empleados es correcta

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 41 de 89



## Implementación del Servidor de Almacenamiento (NAS - TrueNAS)

La implementación del Servidor NAS, utilizando TrueNAS Core 25.10.0.1, es un paso crucial para el proyecto y el cumplimiento de la Regla 3-2-1 de backups, ya que proporciona una capa de almacenamiento redundante y cifrado.

TrueNAS se instaló en el disco de 16 GB reservado para el Sistema Operativo, asegurando que los discos de datos queden libres para el RAID de almacenamiento.

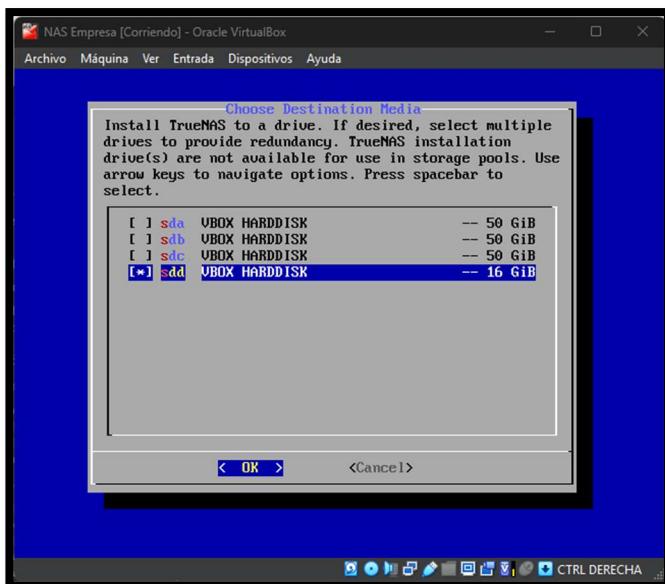


Imagen 33 – Discos instalados en el Servidor de almacenamiento (NAS)

Para garantizar que el SRV1 pueda acceder al NAS de manera constante, se configuró la IP estática 192.168.50.100 directamente en la consola de TrueNAS.



Imagen 34 – Interfaz inicial del servidor NAS

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 42 de 89



Se accedió a la interfaz web de TrueNAS para crear el RAID de almacenamiento con las características de seguridad diseñadas.

Se creó el RAID llamado Backups. Se seleccionó la opción Encryption (Cifrado) utilizando el estándar AES-256-GCM, que es el protocolo de cifrado más robusto y de alto rendimiento.

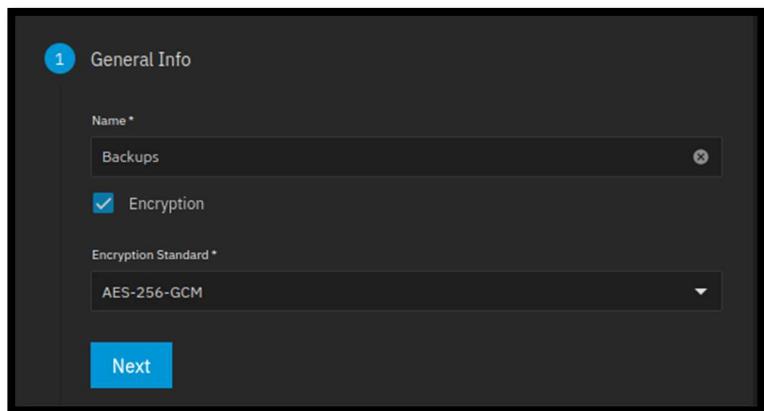


Imagen 35 – Configuración del RAID creado

Se seleccionó la topología RAIDZ1 (funcionalmente equivalente a RAID 5) sobre tres discos de 50 GB.

El RAIDZ1 permite que la infraestructura siga operando y manteniendo la integridad de los datos en caso de que uno de los tres discos falle.

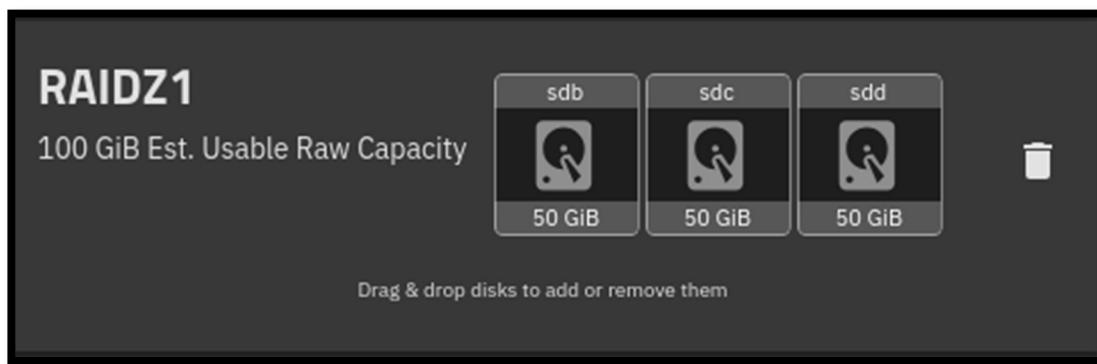


Imagen 36 – Discos seleccionados para la creación del RAID 5

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 43 de 89



## Configuración del Recurso Compartido (NFS)

Se configuró el servicio NFS para permitir que el Servidor Ubuntu (SRV1) escriba los backups en el NAS.

Se creó el Dataset TEcnycom dentro del RAID de Backups. Este Dataset permite la escritura únicamente a la IP del Servidor Central (192.168.50.10), siguiendo el principio de mínimo privilegio.

The screenshot shows the TrueNAS web interface with the URL [192.168.50.100/ui/sharing/nfs](http://192.168.50.100/ui/sharing/nfs). The left sidebar is visible with options like Dashboard, Storage, Datasets, Shares, Data Protection, Credentials, Containers, and Virtual Machines. The main content area is titled 'NFS' and displays a table of NFS shares. One entry is shown:

Path	Description	Networks	Hosts	Enabled
/mnt/Backups/ TEcnycom		192.168.50.0/24		<input checked="" type="checkbox"/>

At the bottom of the table, there are pagination controls: 'Items per page: 50', '1 of 1', and navigation arrows.

Imagen 37 – Creación del Dataset donde se ubicarán los backups

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 44 de 89



## Implementación del Script de Backup y Programación

Finalmente, se creó el vínculo entre el SRV1 y el NAS y se automatizó la tarea de seguridad.

```
SRV 1 (Instantánea OK) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
srvi@srvi:~$ sudo mount 192.168.50.100:/mnt/Backups/TEcnocom /mnt/backup_nas
srvi@srvi:~$ sudo touch /mnt/backup_nas/prueba.txt
srvi@srvi:~$
```

Imagen 38 – Montaje del Dataset para backups y creación de fichero para pruebas

Se creó el script que comprime la Intranet y la copia al punto de montaje.

```
SRV 1 (Instantánea OK) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 7.2
#!/bin/bash

FECHA=$(date +%F)
tar -czf /mnt/backup_nas/backup_.$FECHA.tar.gz /var/www/html
```

Imagen 39 – Script backup.sh

Aquí se encuentra el backup:

```
SRV 1 (Instantánea OK) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
srvi@srvi:~$ sudo ./backup.sh
tar: Removing leading `/' from member names
srvi@srvi:~$ ls -l /mnt/backup_nas
total 268
-rw-r--r-- 1 root root 261065 nov 29 2025 backup_2025-11-29.tar.gz
-rwxrwxrwx 1 root root 0 nov 29 2025 prueba.txt
srvi@srvi:~$
```

Imagen 40 – Backup de prueba creado correctamente

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 45 de 89



Para garantizar la ejecución sin fallos de permisos y la recurrencia diaria, el script fue programado para ejecutarse como root a las 03:00 AM con el comando crontab -e y esta línea de comando.

```
# m h dom mon dow command
0 3 * * * /home/srv1/backup.sh >> /var/log/backup_web.log 2>&1_
```

**Imagen 41 – Configuración de la línea de comando en crontab**

0 3 \* \* \*: Ejecuta el script cada noche a las 3:00 AM.

>> /var/log/backup\_web.log: Toma todo lo que el script dice y lo añade al final del archivo de log.

2>&1: Si el script da un error, también lo escriba en el log en lugar de perderlo.

## Estrategia de Backup: Cumplimiento de la Regla 3-2-1

Esta estrategia asegura que, incluso ante un desastre físico en la sede del cliente, la información crítica permanezca a salvo.

### 1. Tres copias de los datos

El sistema genera y mantiene tres ejemplares de la información:

Copia 1 (Datos Vivos): La instancia operativa en el Servidor Central (SRV1).

Copia 2 (Respaldo Local): Almacenada en el Pool RAIDZ1 del NAS TrueNAS en la oficina del cliente.

Copia 3 (Custodia Externa): Una copia de seguridad en las instalaciones de la empresa proveedora de servicios tecnológicos.

### 2. Dos soportes diferentes

Se utilizan medios tecnológicos distintos para evitar fallos por fatiga de materiales o errores de software de un solo fabricante:

Soporte A (Disco Local): Almacenamiento SSD/HDD del servidor del cliente.

Soporte B (NAS Dedicado): Sistema de archivos ZFS con RAIDZ1 que protege contra la degradación de datos y fallos de un disco físico.

### 3. Una copia fuera de la sede

Este es el punto crítico para la recuperación ante desastres. En este proyecto, el requisito de fuera de la sede se cumple mediante la custodia gestionada por el proveedor:

Implementación: Tras el servicio al cliente, se realiza un volcado de la intranet creada hacia un soporte distinto como podría ser un disco duro externo.

A diferencia de las soluciones en la nube pública, este método garantiza la soberanía absoluta de los datos y permite una recuperación inmediata (RTO - Recovery Time Objective) mediante el transporte físico del hardware en caso de caída total de las líneas de comunicación del cliente.

Esta implementación demuestra una gestión profesional de la seguridad, priorizando la privacidad y el control de los activos de información de la PYME.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 46 de 89



### 3.5.3. Fase de desarrollo

La Fase de Desarrollo se orientó a la creación de la lógica de la Intranet y los scripts de sistema en el Servidor Central (SRV1), aprovechando la estructura de servicios implementada.

La Intranet se basa en PHP para la lógica de autenticación y el procesamiento de solicitudes, y HTML/CSS para la interfaz de usuario. El objetivo es proporcionar un portal funcional y seguro.

La aplicación se alojó en el directorio /var/www/html y se estructuró para separar el acceso público de la gestión administrativa:

```
srv1@srv1:/var/www/html$ ls -l
total 292
drwxrwxrwx 2 www-data www-data 4096 nov 22 12:17 admin
drwxrwxrwx 2 www-data www-data 4096 nov 22 11:16 archivos
drwxr-xr-x 2 www-data www-data 4096 nov 17 20:25 css
-rw xr-xr-x 1 www-data www-data 3912 nov 22 11:21 empleados.php
-rw xr-xr-x 1 www-data www-data 8019 nov 22 11:12 index.php
-rw xr-xr-x 1 www-data www-data 3655 nov 22 11:24 login.php
-rw xr-xr-x 1 www-data www-data 231757 nov 17 20:25 logo.png
-rw xr-xr-x 1 www-data www-data 1467 nov 22 11:30 logout.php
-rw xr-xr-x 1 www-data www-data 7052 nov 22 11:33 procesar_solicitud.php
drwxrwxrwx 2 www-data www-data 4096 nov 22 12:18 solicitudes
-rw xr-xr-x 1 www-data www-data 5061 nov 22 11:36 solicitudes.php
-rw xr-xr-x 1 www-data www-data 4011 nov 22 11:47 subir_archivo.php
-rw xr-xr-x 1 www-data www-data 4138 nov 22 11:52 validar_login.php
srv1@srv1:/var/www/html$ _
```

```
srv1@srv1:/var/www/html/admin$ ls
dashboard.php  noticias_guardadas.html  procesar_noticia.php  solicitudes_guardadas.html
srv1@srv1:/var/www/html/admin$ _
```

Imagenes 42 y 43 – Estructura de la Intranet

#### Lógica de Autenticación (validar\_login.php y logout.php)

El acceso a la Intranet está protegido por un sistema de sesiones.

Validación de Credenciales (validar\_login.php): Este script verifica el usuario y la clave enviados por el formulario de login.php.

```
// --- 1. INICIAR EL SISTEMA DE SESIONES ---
session_start();

// --- 2. SIMULACIÓN DE BASE DE DATOS (Usuarios Válidos) ---
// Aquí se encuentran los usuarios de la empresa.
$usuarios_validos = [
    // 'nombre_de_usuario' => 'contraseña'
    'admin' => 'admin', // Este usuario tiene rol de Administrador
    'emp1' => 'emp1', // Este usuario tiene rol de Empleado
    'emp2' => 'emp2', // Este usuario tiene rol de Empleado
    'emp3' => 'emp3' // Este usuario tiene rol de Empleado
];
```

Imagen 44 – Creación de usuarios en validar\_login.php

Asignación de Roles: La lógica asigna un rol (admin o empleado) al usuario en la variable de sesión, lo cual es vital para el control de acceso al área administrativa.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 47 de 89



```
// --- 5. ¡ÉXITO! Usuario y contraseña correctos ---  
// "Recordamos" al usuario para las demás páginas.  
// Creamos una variable de sesión llamada 'usuario_logueado'  
// y le asignamos el nombre del usuario.  
// Esta variable $_SESSION estará disponible en TODAS las páginas  
// (siempre que hagamos session_start() al principio).  
$_SESSION['usuario_logueado'] = $usuario_form;  
  
// Asignamos un "rol" (permiso) a este usuario en la sesión.  
// Si el usuario es 'admin', dale el rol 'admin', si no, dale 'empleado'"  
$_SESSION['rol'] = ($usuario_form == 'admin') ? 'admin' : 'empleado';  
  
// Redirigimos al usuario al panel de administración  
// 'header('Location: ...')' envía una orden al navegador.  
header('Location: admin/dashboard.php');  
  
// 'exit' detiene la ejecución del script. Es una buena práctica  
// de seguridad para asegurar que la redirección ocurra inmediatamente.  
exit;
```

Imagen 45 – Asignación de roles en validar\_login.php

Cierre de Sesión (logout.php): Garantiza el cierre seguro mediante la destrucción de la sesión, aplicando el session\_unset() y session\_destroy().

```
<?php  
/*  
 * logout.php (Script de Cierre de Sesión)  
 *  
 * Este script NO es una página web que se ve. No tiene HTML.  
 * Su único trabajo es:  
 * 1. Iniciar la sesión actual del usuario.  
 * 2. Borrar todos los datos de esa sesión.  
 * 3. Destruir la sesión.  
 * 4. Redirigir al usuario de vuelta a la página de inicio.  
 */  
  
// --- 1. INICIAR LA SESIÓN ---  
session_start();  
  
// --- 2. VACIAR LAS VARIABLES DE SESIÓN ---  
// 'session_unset()' borra inmediatamente todas las variables  
// guardadas dentro de la sesión.  
session_unset();  
  
// --- 3. DESTRUIR LA SESIÓN ---  
// 'session_destroy()' elimina la sesión del servidor.  
// Esto invalida el ID de sesión (la cookie PHPSESSID)  
// que el navegador del usuario tenía.  
session_destroy();  
  
// --- 4. REDIRIGIR AL USUARIO ---  
// 'header('Location: ...')' envía una orden al navegador  
// para que cargue la página "index.php".  
// Como la sesión ya está destruida, cuando "index.php" cargue,  
// su '$_SESSION['usuario_logueado']' dará "falso"  
// y mostrará correctamente el botón de "Iniciar Sesión".  
header('Location: index.php');  
  
// 'exit' es una buena práctica de seguridad.  
// Detiene la ejecución del script inmediatamente.  
exit;  
?>
```

Imagen 46 – Script logout.php

Módulo de Solicitudes (procesar\_solicitud.php)

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 48 de 89



Este script es el backend del formulario de solicitudes y alberga dos de las medidas de seguridad más importantes contra ataques web:

Medida de Seguridad 1: Lista Blanca de Tipos de Archivo: Se implementa un filtro estricto para aceptar únicamente extensiones de archivo inofensivas (PDF, DOCX, JPG, etc.). Esto previene la subida de scripts maliciosos (.php, .exe).

```
// --- 3A. MEDIDA DE SEGURIDAD 1: VALIDAR TIPO DE ARCHIVO ---
// NO se confía en el tipo de archivo que dice el navegador, se confía en la extensión.

$nombre_original = $_FILES['adjunto']['name']; // ej. "mi_factura.pdf"

// 'pathinfo' saca la extensión, 'strtolower' la pasa a minúsculas (PDF -> pdf).
$extension = strtolower(pathinfo($nombre_original, PATHINFO_EXTENSION));

// Lista blanca de extensiones que SÍ permitimos.
// Esto es crucial para evitar que alguien suba un virus (ej. .exe) o
// un script malicioso (ej. .php).
$extensiones_permitidas = ['pdf', 'docx', 'jpg', 'jpeg', 'png', 'txt'];

// 'in_array()' comprueba si la $extension del archivo está en nuestra $extensiones_permitidas.
if (in_array($extension, $extensiones_permitidas)) {

    // --- 3B. MEDIDA DE SEGURIDAD 2: CREAR NOMBRE DE ARCHIVO ÚNICO ---
    // Si dos usuarios suben "factura.pdf", el segundo borraría al primero.
    // 'uniqid()' genera un ID único basado en la hora actual (ej. "6908e812c62f2").
    // Esto asegura que no haya colisiones.
    $nombre_seguro = uniqid() . '.' . $extension; // ej. "6908e812c62f2.pdf"
    $ruta_destino = $ruta_subidas . $nombre_seguro; // Ruta final donde se guardará
```

Imagen 47 – Configuración de archivos permitidos en las solicitudes en el script procesar\_solicitud.php

Medida de Seguridad 2: Prevención de XSS: Se utiliza la función htmlspecialchars() para sanear todos los datos introducidos por el usuario antes de ser guardados o mostrados, previniendo ataques de Cross-Site Scripting (XSS).

```
// --- 4. FORMATEAR LA SOLICITUD COMO HTML ---
// 'htmlspecialchars()' es la MEDIDA DE SEGURIDAD MÁS IMPORTANTE aquí.
// Evita que un usuario escriba código HTML o JavaScript malicioso (Ataque XSS)
$entrada = "<p><strong>". htmlspecialchars($nombre) . "</strong> (" . htmlspecialchars($email) . ") [". htmlspecialchars($tipo) . "]:<br>".
    "<br>". nl2br(htmlspecialchars($mensaje)) .
    // Añade el enlace <a> si la subida fue exitosa, o '' (vacío) si no.
    "<a href='". $enlace_archivo .
    "'></a>"; // '\n' es un salto de línea (para ordenar el archivo guardado)
```

Imagen 48 – Utilización de htmlspecialchars en el script procesar\_solicitud.php

## Panel de Administración (/admin/dashboard.php)

El dashboard.php es el área más sensible de la aplicación y requiere el doble control de acceso para garantizar el Principio de Mínimo Privilegio.

Doble Control de Acceso (Seguridad): El script comienza con dos comprobaciones:

Verificación de la existencia de sesión (isset(\$\_SESSION['usuario\_logueado'])).

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 49 de 89



Verificación del rol: Solo permite el acceso si el rol es 'admin'. Si el rol es 'empleado', el acceso es denegado.

```
// --- 2. MEDIDA DE SEGURIDAD 1: ¿ESTÁ LOGUEADO? ---
// 'isset' comprueba si la variable $_SESSION['usuario_logueado'] existe.
if (!isset($_SESSION['usuario_logueado'])) {
    // Si no ha iniciado sesión, lo "expulsamos" a la página de login.
    // 'header('Location: ...')' redirige al navegador.
    // Usamos '../login.php' porque tenemos que "subir un nivel"
    // desde la carpeta /admin/ para encontrar 'login.php' en la raíz.
    header('Location: ../login.php');

    // 'exit' detiene la ejecución del script. Es crucial después de una redirección.
    exit;
}

// --- 3. MEDIDA DE SEGURIDAD 2: ¿TIENE PERMISOS DE ADMIN?
// Comprobamos la variable 'rol' que creamos en 'validar_login.php'.
// Si el rol NO ES (!=) 'admin'...
if ($_SESSION['rol'] != 'admin') {
    // El usuario está logueado, pero es un "empleado" normal.
    // Le mostramos un mensaje de error y detenemos el script.
    echo "<h1>Acceso Denegado</h1><p>No tienes permisos de administrador.</p>";
    echo "<a href='../index.php>Volver al inicio</a>";
    exit;
}
```

Imagen 49 – Verificación de los roles de los usuarios en dashboard.php

Funcionalidad del Panel: El dashboard ofrece las siguientes funcionalidades clave:

Monitorización: Muestra el estado del Servidor Web (Apache) y el Servidor VPN (WireGuard) usando comandos shell\_exec

```
// 4A. Comprobar el estado de Apache
$apache_raw = shell_exec('sudo systemctl is-active apache2');
// 'trim()' limpia la respuesta (quita saltos de linea).
// Usamos un 'if' corto (ternario):
// (condición) ? (si es verdad) : (si es falso)
$estado_apache = (trim($apache_raw) == 'active') ? '◆ Activo' : '◆ Inactivo/Caído';

// 4B. Comprobar el estado de WireGuard
$vpn_raw = shell_exec('sudo systemctl is-active wg-quick@wg0');
$estado_vpn = (trim($vpn_raw) == 'active') ? '◆ En ejecución' : '◆ Detenido';
```

```
<!-- Sección de Estado (muestra las variables PHP de arriba) -->
<section>
    <h2>Estado del sistema</h2>
    <ul>
        <li>Servidor Web (Apache): <strong><?php echo $estado_apache; ?></strong></li>
        <li>Servidor VPN (WireGuard): <strong><?php echo $estado_vpn; ?></strong></li>
        <li>Base de datos: <strong>Desconectada</strong> (Simulado)</li>
    </ul>
</section>
```

Imágenes 50 y 51 – Líneas de comando que permiten la verificación del estado de los servicios en dashboard.php

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 50 de 89



Para que la monitorización funcione correctamente, hay que ejecutar sudo visudo en el servidor y agregar esta línea de comando:

```
www-data ALL=(ALL) NOPASSWD: /usr/bin/systemctl is-active apache2, /usr/bin/systemctl is-active wg-quick@wg0_
```

**Imagen 52 – Línea de comando ejecutada en el servidor con visudo que permite la verificación del estado de los servicios en la Intranet**

Lectura de Solicitudes: Muestra las solicitudes guardadas por los empleados.

```
<!-- Sección de Solicitudes (Lectura de archivo) -->
<section>
    <h2>Últimas solicitudes</h2>
    <?php
        // '__DIR__' es la carpeta actual (/admin/)
        $archivo = __DIR__ . '/solicitudes_guardadas.html';

        // Comprueba si el archivo existe Y no está vacío
        if (file_exists($archivo) && filesize($archivo) > 0) {
            // "Imprime" todo el contenido del archivo aquí
            echo file_get_contents($archivo);
        } else {
            echo "<p>No hay solicitudes nuevas.</p>";
        }
    ?>
</section>
```

**Imagen 53 – Sección de solicitudes en dashboard.php**

Publicación de Noticias: Permite al administrador publicar nuevos anuncios internos.

```
<!-- Sección de Noticias (Formulario de envío) -->
<section>
    <h2>Publicar Nueva Noticia</h2>
    <!--
        Este formulario envía los datos a 'procesar_noticia.php',
        que está en esta misma carpeta /admin/.
    -->
    <form action="procesar_noticia.php" method="post">
        <label for="noticia">Contenido de la noticia:</label><br>
        <textarea id="noticia" name="noticia" rows="5" style="width: 90%;" required></textarea><br><br>
        <input type="submit" value="Publicar Noticia">
    </form>
</section>
```

**Imagen 54 – Sección de creación de noticias en dashboard.php**

## Archivos de Configuración Críticos

En esta sección se documentan las modificaciones realizadas a nivel de sistema operativo y aplicación para garantizar la operatividad y la seguridad de la infraestructura.

### Script de Copia de Seguridad (backup.sh)

Se desarrolló un script en Bash para automatizar la copia de seguridad de la Intranet, que es el desarrollo clave de seguridad y cumplimiento normativo.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 51 de 89



El backup.sh es el desarrollo clave para la Integridad de los Datos. Este script comprime la Intranet y la copia al NAS a través del punto de montaje NFS (/mnt/backup\_nas).

```
GNU nano 7.2                                     backup.sh
#!/bin/bash

FECHA=$(date +%F)
tar -czf /mnt/backup_nas/backup_${FECHA}.tar.gz /var/www/html
```

Imagen 55 – Script de creación de backups (Backup.sh)

## Configuración de Apache con SSL (tecnycom-ssl.conf)

El archivo de configuración del Virtual Host de Apache para el puerto 443 es vital para forzar el uso de HTTPS y cifrar la conexión a la Intranet.

Activación de HTTPS: Se define el bloque VirtualHost \*:443 y se apuntan las directivas SSLCertificateFile y SSLCertificateKeyFile a los certificados creados.

Control de Acceso (Legacy): Se mantiene una configuración de autenticación simple (AuthType Basic) a nivel de Apache dentro del directorio raíz de la Intranet, como una segunda capa de seguridad si fallara la gestión de sesiones PHP.

En este caso el .htaccess no se utiliza ya que fue una implementación inicial, pero se conserva en el proyecto ya que en caso de fallar la autenticación por PHP se podría habilitar.

```
GNU nano 7.2                                         /etc/apache2/sites-available/tecnycom-ssl.conf
<VirtualHost *:443>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin admin@tecnycom.local
    ServerName 192.168.50.10

    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/tecnycom.crt
    SSLCertificateKeyFile /etc/apache2/ssl/tecnycom.key

    <Directory /var/www/html>
        AuthType Basic
        AuthName "Intranet TEcnocom"
        AuthUserFile /etc/apache2/.htpasswd
        AuthGroupFile /etc/apache2/.htgroup
        Require group empleados admins
    </Directory>

    <Directory /var/www/html/admin>
        AllowOverride All
    </Directory>

    CustomLog ${APACHE_LOG_DIR}/access.log combined
    ErrorLog ${APACHE_LOG_DIR}/error.log
</VirtualHost>
```

Imagen 56 – Archivo de configuración del servicio Apache

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 52 de 89



## Configuración del Servidor VPN (wg0.conf)

El archivo wg0.conf del Servidor Ubuntu (SRV1) define el túnel WireGuard y a todos los clientes que tienen permiso para conectarse.

[Interface]: Define la IP interna de la VPN del servidor (10.8.0.1/24) y su clave privada.

[Peer]: Cada bloque representa un cliente (EMP1, EMP2, EMP3) con su clave pública y su IP estática asignada dentro de la subred VPN.

```
GNU nano 7.2                                         /etc/wireguard/wg0.conf
[Interface]
Address = 10.8.0.1/24
ListenPort = 51820
PrivateKey = gP4hgRgBXSthnWMG1FYTkDz+PAckpezEvp+UnwOXW0Q=

#Empleados
[Peer]
PublicKey = p20HX7fNKrdiJNImxUHhUvnQQc3GtwwGcx7jBJf/f1k=
AllowedIPs = 10.8.0.2/32

[Peer]
PublicKey = NrjUJuY1HpMn9nJGoGR+D/dgTA9zsuzw/ck4qONWAlc=
AllowedIPs = 10.8.0.3/32

[Peer]
PublicKey = bBR4t3xyonyazwDeCc/Nr92M1InVL0BIXphIxF0JNmXY=
AllowedIPs = 10.8.0.4/32
```

Imagen 57 – Archivo de configuración de Wireguard en el Servidor

## Habilitación de IP Forwarding (sysctl.conf) y Automatización (crontab)

El reenvío de IP es esencial para que el tráfico que llega por el túnel VPN pueda ser enrutado a la LAN (192.168.50.0/24). Se asegura su persistencia editando el archivo de configuración.

Se agrega una única línea para habilitar el reenvío de paquetes:

```
net.ipv4.ip_forward=1
```

Imagen 58 – Línea de comando que habilita el reenvío de paquetes

El script de backup se programó en el crontab del usuario root para garantizar el acceso a todos los archivos y al NAS, así como para generar un registro de auditoría, en este caso, se ha programado un backup diario a las 3:00.

```
GNU nano 7.2                                         /tmp/crontab.h7AmN3/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 3 * * * /home/srv1/backup.sh >> /var/log/backup_web.log 2>&1
```

Imagen 59 – Archivo de configuración de crontab en el Servidor

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 53 de 89



## Cliente EMP 2 (Ubuntu Desktop)

El cliente se configura con su clave privada, la IP virtual asignada (10.8.0.3/32) para el correcto funcionamiento de la VPN.

The screenshot shows a terminal window titled "emp2@emp2: ~" with the command "nano /etc/wireguard/emp2.conf". The file contains the following configuration:

```
GNU nano 7.2          /etc/wireguard/emp2.conf *
[Interface]
PrivateKey = oNvp3b/hk1UABXYcjgUyi5N2SeS3uEWE/MUq/04r0M=
Address = 10.8.0.3/24
DNS = 1.1.1.1

[Peer]
PublicKey = RbBEuk//5y6viogaheQNoKoDFhzVdynlQKCYtYqOMgo=
Endpoint = 192.168.1.147:51820
AllowedIPs = 10.8.0.0/24
PersistentKeepalive = 25
```

At the bottom of the terminal window, there is a menu bar with options like Ayuda, Guardar, Buscar, Cortar, Ejecutar, Ubicación, Salir, Leer fich., Reemplazar, Pegar, Justificar, and Ir a línea.

Imagen 60 – Archivo de configuración de Wireguard en el empleado Ubuntu (EMP2)

## Cliente Móvil EMP 3 (iPhone 11)

El cliente móvil se configuró manualmente utilizando la aplicación oficial de WireGuard.



Imagen 61 – Configuración de la aplicación VPN Wireguard en el móvil

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 54 de 89



## 3.5.4. Fase de pruebas

El siguiente plan de pruebas se divide en tres áreas clave para validar que la infraestructura implementada cumple con los objetivos, además de verificar la funcionalidad de la Intranet.

### Pruebas de Seguridad Perimetral y Acceso Remoto

El objetivo de este bloque es validar que el firewall pfSense blinda correctamente la red interna y que el acceso remoto a través de la VPN es seguro y funcional desde distintas plataformas.

#### Escaneo de Puertos (Nmap)

Para verificar el funcionamiento del firewall, se han realizado pruebas de escaneo desde el Cliente EMP 2 situado en la zona WAN (fuera de la oficina) hacia la IP pública del firewall (192.168.1.147).

##### A. Escaneo General TCP (Políticas de Firewall)

Se ejecutó un escaneo sobre los 65535 puertos TCP para asegurar que ningún servicio crítico (HTTP, SSH, MySQL) está expuesto directamente a internet.

Comando: sudo nmap -p- -T4 192.168.1.147

El uso de -p- garantiza que no dejamos ningún puerto sin revisar. El parámetro -T4 optimiza la velocidad en entornos virtuales.

```
emp2@emp2:~$ sudo nmap -p- -T4 192.168.1.147
[sudo] contraseña para emp2:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-18 14:52 CET
Nmap scan report for 192.168.1.147
Host is up (0.00047s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 233.91 seconds
emp2@emp2:~$
```

Imagen 62 - Identificación de los servicios TCP del pfSense (DNS, HTTP y HTTPS)

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 55 de 89



## B. Escaneo Específico UDP (Validación de WireGuard)

Dado que WireGuard utiliza el protocolo UDP y opera en modo invisible, no responde a escaneos convencionales a menos que se especifique el protocolo.

Comando: sudo nmap -sU -p 51820 192.168.50.10

El modo invisible de WireGuard hace que el puerto aparezca como open|filtered. El servicio no responde a paquetes que no estén firmados criptográficamente, lo que mitiga ataques de reconocimiento.

```
emp2@emp2:~$ sudo nmap -sU -p 51820 192.168.50.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-18 15:03 CET
Nmap scan report for 192.168.50.10
Host is up (0.00032s latency).

PORT      STATE      SERVICE
51820/udp open|filtered unknown
MAC Address: 08:00:27:93:15:15 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
emp2@emp2:~$
```

Imagen 63 - El servidor está a la escucha de túneles VPN válidos

## C. Descubrimiento de Hosts Activos

Para verificar qué equipos están operativos en la LAN de la empresa (192.168.50.0/24).

Comando: sudo nmap -sn 192.168.50.0/24

```
emp2@emp2:~$ sudo nmap -sn 192.168.50.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-18 15:22 CET
Nmap scan report for _gateway (192.168.50.1)
Host is up (0.00039s latency).
MAC Address: 08:00:27:5D:7F:A8 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.10
Host is up (0.00024s latency).
MAC Address: 08:00:27:93:15:15 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.50.100
Host is up (0.00044s latency).
MAC Address: 08:00:27:3B:10:39 (Oracle VirtualBox virtual NIC)
Nmap scan report for emp2 (192.168.50.11)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.37 seconds
emp2@emp2:~$
```

Imagen 64 - Identificación exitosa del pfSense (.1), SRV1 (.10), EMP2 (.11) y el NAS (.100)

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 56 de 89



## D. Identificación del NAS (TrueNAS)

Se auditó el servidor de almacenamiento para confirmar que solo expone los servicios necesarios (como NFS en el puerto 2049).

Comando: sudo nmap -O -sV 192.168.50.100

```
emp2@emp2: ~$ sudo nmap -O -sV 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-18 15:23 CET
Nmap scan report for 192.168.50.100
Host is up (0.00040s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
111/tcp   open  rpcbind 2-4 (RPC #100000)
443/tcp   open  ssl/http nginx
2049/tcp  open  nfs_acl 3 (RPC #100227)
5357/tcp  open  http    BaseHTTPServer 0.6 (Python 3.11.9)
MAC Address: 08:00:27:3B:10:39 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.89 seconds
emp2@emp2: ~$
```

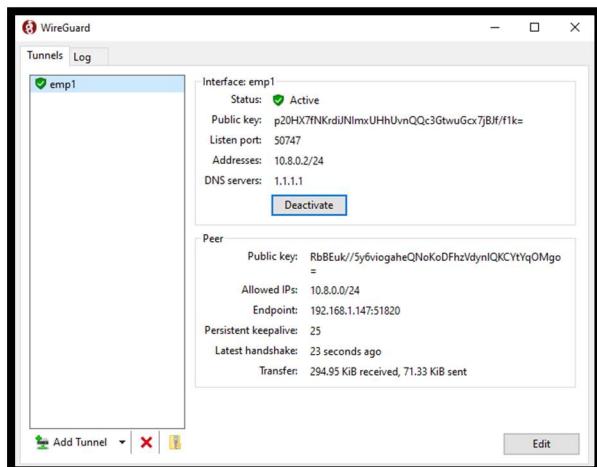
Imagen 65 - Nmap identifica la versión de los servicios activos

## Validación de Acceso Remoto VPN

Se realizaron pruebas de conexión de extremo a extremo para garantizar que el teletrabajo es viable desde cualquier dispositivo.

### A. Cliente Windows (EMP 1)

Se activó el túnel en el cliente Windows 10 para verificar la interoperabilidad.



# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 57 de 89

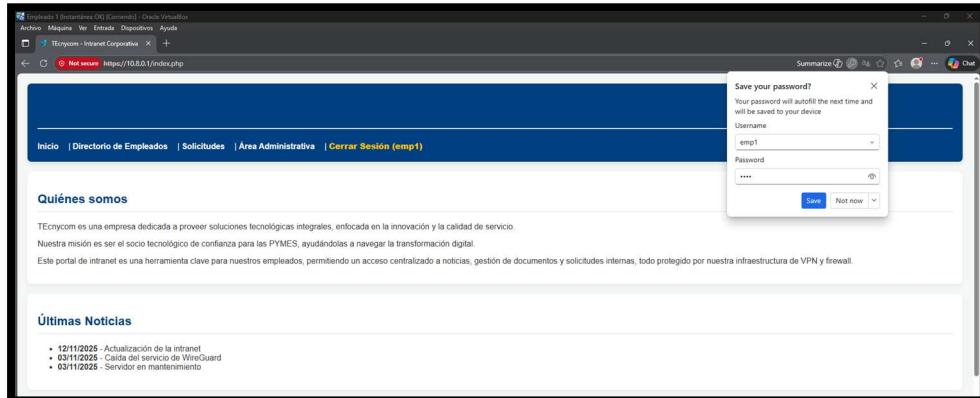


Imágenes 66 y 67 - Conexión exitosa con obtención de la IP virtual 10.8.0.2.

## B. Cliente Linux (EMP 2)

Validación de la conexión persistente desde el puesto de trabajo interno con Linux.

```
emp2@emp2: ~
emp2@emp2: $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:2f:20:8a brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.11/24 brd 192.168.50.255 scope global dynamic noprefixroute
        enp0s3
            valid_lft 7148sec preferred_lft 7148sec
3: emp2: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 10.8.0.3/24 scope global emp2
        valid_lft forever preferred_lft forever
emp2@emp2: ~
```



Imágenes 68 y 69 - Conexión exitosa con obtención de la IP virtual 10.8.0.3

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

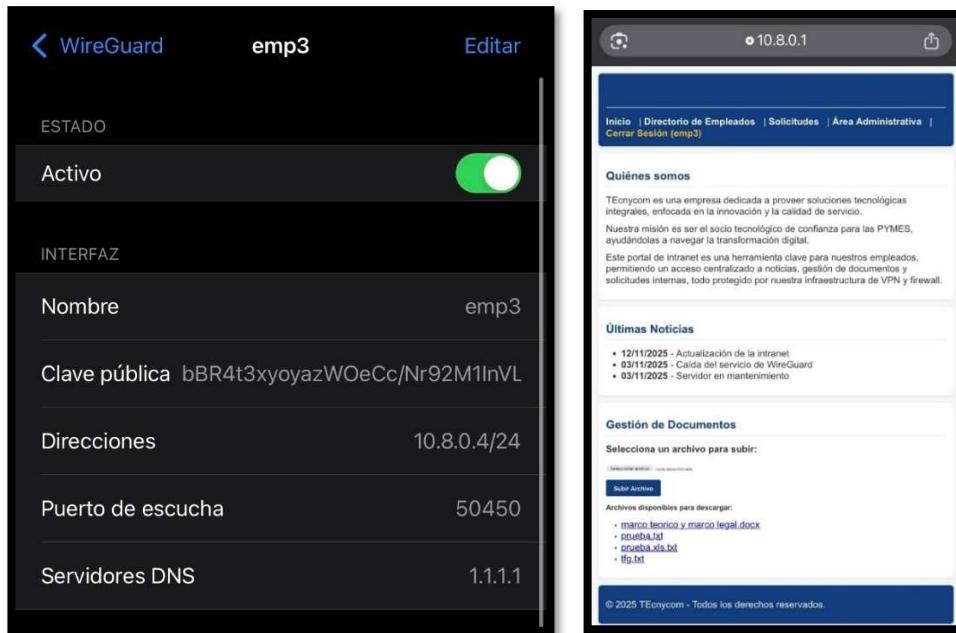
Página 58 de 89



## C. Acceso desde Dispositivo Móvil (EMP 3)

Prueba de movilidad utilizando mi iPhone 11 conectado a una red externa.

Metodología: Activación de la App WireGuard y navegación a <https://10.8.0.1>.



**Imagenes 70 y 71 - La Intranet carga correctamente sobre HTTPS, demostrando que el cifrado es total desde el dispositivo hasta el servidor central**

## Pruebas de Integridad y Resiliencia (Backups y NAS)

Estas pruebas confirman que el proyecto funciona correctamente, garantizando que los datos críticos de la empresa están protegidos incluso ante fallos críticos de hardware.

## Validación del Sistema de Copias de Seguridad

El objetivo es asegurar que el proceso de backup automatizado es capaz de empaquetar la intranet y transferirla exitosamente al almacenamiento centralizado (NAS).

```
srv1@srv1:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           392M   1M  391M   1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv    12G  5,7G  5,0G  54% /
tmpfs            2,0G     0  2,0G   0% /dev/shm
tmpfs            5,0M     0  5,0M   0% /run/lock
/dev/sda2         2,0G  194M  1,6G  11% /boot
tmpfs           392M   16K  392M   1% /run/user/1000
192.168.50.100:/mnt/Backups/TEcnycom  96G  1,0M  96G   1% /mnt/backup_nas
srv1@srv1:~$
```

**Imagen 72 – Comprobación de que el Dataset de backups está montado correctamente**

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 59 de 89



## A. Ejecución del Script de Backup

Se ejecutó manualmente el script backup.sh en el Servidor Central (SRV1).

```
SRV 1 (Instantánea OK) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
srv1@srv1:~$ sudo ./backup.sh
tar: Removing leading `/' from member names
srv1@srv1:~$ ls -l /mnt/backup_nas
total 268
-rw-r--r-- 1 root root 261065 nov 29 2025 backup_2025-11-29.tar.gz
-rwxrwxrwx 1 root root      0 nov 29 2025 prueba.txt
srv1@srv1:~$
```

Imagen 73 - El sistema generó un archivo comprimido .tar.gz y lo depositó en el punto de montaje NFS /mnt/backup\_nas/

## B. Auditoría y Verificación del Contenido (tar -tvf)

Antes de validar una restauración, es vital auditar el backup para asegurar que no está corrupto y contiene los permisos correctos.

Comando: tar -tvf /mnt/backup\_nas/backup\_intranet\_XXXX.tar.gz

Parámetros:

t (list): Lista el contenido.

v (verbose): Muestra detalles como permisos y dueño.

f (file): Especifica el archivo.

```
SRV 1 (Instantánea OK) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
srv1@srv1:~$ tar -tvf /mnt/backup_nas/backup_2025-11-29.tar.gz
drwxr-xr-x www-data/www-data 0 2025-11-22 11:52 var/www/html/
-rwxr-xr-x www-data/www-data 4011 2025-11-22 11:47 var/www/html/subir_archivo.php
-rwxr-xr-x www-data/www-data 3912 2025-11-22 11:21 var/www/html/empleados.php
-rwxr-xr-x www-data/www-data 4138 2025-11-22 11:52 var/www/html/validar_login.php
drwxrwxrwx www-data/www-data 0 2025-11-22 11:16 var/www/html/archivos/
-rwxr-xr-x www-data/www-data 14433 2025-11-17 20:25 var/www/html/archivos/marco teorico y marco legal.docx
-rw-r--r-- www-data/www-data 0 2025-11-22 11:16 var/www/html/archivos/prueba.txt
-rwxr-xr-x www-data/www-data 1189 2025-11-17 20:25 var/www/html/archivos/tfg.txt
-rw-r--r-- www-data/www-data 0 2025-11-17 20:48 var/www/html/archivos/prueba.xls.txt
drwxrwxrwx www-data/www-data 0 2025-11-22 12:17 var/www/html/admin/
-rwxr-xr-x www-data/www-data 2473 2025-11-17 20:25 var/www/html/admin/procesar_noticia.php
-rwxr-xr-x www-data/www-data 415 2025-11-17 20:49 var/www/html/admin/solicitudes_guardadas.html
-rwxr-xr-x www-data/www-data 206 2025-11-17 20:25 var/www/html/admin/noticias_guardadas.html
-rwxr-xr-x www-data/www-data 6302 2025-11-22 12:01 var/www/html/admin/dashboard.php
drwxr-xr-x www-data/www-data 0 2025-11-17 20:25 var/www/html/css/
-rwxr-xr-x www-data/www-data 5582 2025-11-17 20:25 var/www/html/css/estilo.css
-rwxr-xr-x www-data/www-data 635 2025-11-17 20:25 var/www/html/css/estilold.css
-rwxr-xr-x www-data/www-data 3655 2025-11-22 11:24 var/www/html/login.php
-rwxr-xr-x www-data/www-data 7052 2025-11-22 11:33 var/www/html/procesar_solicitud.php
-rwxr-xr-x www-data/www-data 5061 2025-11-22 11:36 var/www/html/solicitudes.php
-rwxr-xr-x www-data/www-data 8019 2025-11-22 11:12 var/www/html/index.php
-rwxr-xr-x www-data/www-data 1467 2025-11-22 11:30 var/www/html/logout.php
-rwxrwxrwx www-data/www-data 0 2025-11-22 12:18 var/www/html/logo.png
drwxrwxrwx www-data/www-data 0 2025-11-22 12:18 var/www/html/solicitudes/
-rw-r--r-- www-data/www-data 0 2025-11-17 20:49 var/www/html/solicitudes/691b8a62c48ac.txt
srv1@srv1:~$
```

Imagen 74 - Visualización de la estructura de la intranet con integridad total

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 60 de 89



## C. Prueba de Restauración (sudo tar -xzvf)

Se simuló la pérdida de un archivo en la intranet y se procedió a su recuperación.

Comando: sudo tar -xzvf /mnt/backup\_nas/backup.tar.gz

```
srv1@srv1:~$ mkdir /tmp/prueba1
srv1@srv1:~$ cd /tmp/prueba1
srv1@srv1:/tmp/prueba1$ sudo tar -xzvf /mnt/backup_nas/backup_2025-11-29.tar.gz
var/www/html/
var/www/html/subir_archivo.php
var/www/html/empleados.php
var/www/html/validar_login.php
var/www/html/archivos/
var/www/html/archivos/marco teorico y marco legal.docx
var/www/html/archivos/prueba.txt
var/www/html/archivos/tfg.txt
var/www/html/archivos/prueba.xls.txt
var/www/html/admin/
var/www/html/admin/procesar_noticia.php
var/www/html/admin/solicitudes_guardadas.html
var/www/html/admin/noticias_guardadas.html
var/www/html/admin/dashboard.php
var/www/html/css/
var/www/html/css/estilo.css
var/www/html/css/estilold.css
var/www/html/login.php
var/www/html/procesar_solicitud.php
var/www/html/solicitudes.php
var/www/html/index.php
var/www/html/logout.php
var/www/html/logo.png
var/www/html/solicitudes/
var/www/html/solicitudes/691b8a62c48ac.txt
srv1@srv1:/tmp/prueba1$
```

**Imagen 75 - Los archivos fueron extraídos y descomprimidos correctamente en el directorio creado para la prueba /tmp/prueba1**

Parámetros:

x (extract): Extrae los archivos.

z (gzip): Descomprime el formato .gz.

```
srv1@srv1:/tmp/prueba1$ ls -R
.:
var
./var:
www
./var/www:
html
./var/www/html:
admin.css index.php logo.png procesar_solicitud.php solicitudes.php validar_login.php
archivos empleados.php login.php logout.php solicitudes subir_archivo.php
./var/www/html/admin:
dashboard.php noticias_guardadas.html procesar_noticia.php solicitudes_guardadas.html
./var/www/html/archivos:
'marco teorico y marco legal.docx' prueba.txt prueba.xls.txt tfg.txt
./var/www/html/css:
estilo.css estilold.css
./var/www/html/solicitudes:
691b8a62c48ac.txt
srv1@srv1:/tmp/prueba1$
```

**Imagen 76 - Los archivos fueron restaurados satisfactoriamente**

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 61 de 89



## Resiliencia del Almacenamiento RAIDZ1

Esta prueba valida la tolerancia a fallos del servidor TrueNAS ante la pérdida física de un dispositivo de almacenamiento.

### A. Simulación de Fallo de Disco

Desde el hipervisor, se desconectó el tercer disco (50 GB) asignado al Pool de datos mientras el sistema estaba operativo.

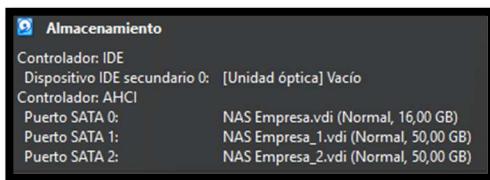


Imagen 77 – Discos del Servidor NAS tras desconectar el tercer disco de 50 GB

Observación en TrueNAS: El sistema detectó la anomalía inmediatamente. Al acceder al Shell de TrueNAS y ejecutar zpool status, el estado del pool cambió a DEGRADED.

Imagenes 78 y 79 – El estado del RAID se muestra como degradado

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 62 de 89



## C. Recuperación y Remontado

Se procedió a conectar el disco nuevamente para observar el proceso de recuperación automática.

```
Welcome to TrueNAS
Last login: Thu Dec 18 17:01:50 PST 2025 on pts/0
truenas_admin@truenas[~]$ lsblk -l
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 16G 0 disk
sda1 8:1 0 1M 0 part
sda2 8:2 0 512M 0 part
sda3 8:3 0 15.5G 0 part
sdb 8:16 0 50G 0 disk
sdb1 8:17 0 49.5G 0 part
sdc 8:32 0 50G 0 disk
sdc1 8:33 0 49.5G 0 part
sdd 8:48 0 50G 0 disk
sdd1 8:49 0 49.5G 0 part
sr0 11:0 1 1024M 0 rom
truenas_admin@truenas[~]$
```

Imágenes 80,81 y 82 - Reincorporación del hardware y ejecución del comando de reemplazo en la interfaz de TrueNAS.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 63 de 89



## Pruebas de Funcionalidad y Mínimo Privilegio (Intranet)

Este bloque de pruebas valida la lógica de programación en PHP y la implementación de las medidas de seguridad dentro de la aplicación web, asegurando que los roles de usuario se respetan estrictamente.

### Acceso Denegado (Mínimo Privilegio)

Se pone a prueba el control de sesiones y la jerarquía de roles para evitar que un usuario sin privilegios acceda a herramientas administrativas.

Metodología: Iniciar sesión con la cuenta de empleado (emp1) e intentar navegar manualmente a la sección de administrador.



Imagen 83 – El acceso al apartado administrador ha sido denegado al empleado corriente

La lógica del servidor debe detectar que el rol en la sesión no es admin, denegar el acceso inmediatamente y mostrar un mensaje de error.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 64 de 89



## Enviar Solicitud/Noticia

Verificación del correcto funcionamiento del flujo de información entre los usuarios y el administrador.

Prueba de Solicitud: Un empleado envía un formulario de incidencia. Se verifica que los datos se almacenan correctamente.

Nombre completo:  
Mohammed Maamla

Correo electrónico:  
mohammedmaamla@tecnyc.com.es

Tipo de solicitud:  
Permitido

Descripción:  
Necesito permisos de administrador

Adjuntar archivo (opcional):  
Examinar... No se ha seleccionado ningún archivo.

Enviar solicitud

Estado del sistema

- Servidor Web (Apache): Activo
- Servidor VPN (WireGuard): En ejecución
- Base de datos: Desconectada (Simulado)

Últimas solicitudes

Mohammed Maamla (mohammedmaamla@tecnyc.com.es) [permiso]: Necesito permisos de administrador

**Imágenes 84 y 85 – La solicitud creada se muestra correctamente en el apartado de últimas solicitudes**

Prueba de Noticia: El administrador publica un aviso desde el panel. Se verifica que la noticia aparece instantáneamente en el index.php para todos los usuarios.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 65 de 89



**Publicar Nueva Noticia**

Contenido de la noticia:

Actualización de última hora

**Publicar Noticia**

A screenshot of a web browser window titled "TEcnym - Intranet Corp". The address bar shows "http://192.168.50.10/index.php". The page has a blue header with navigation links: "Inicio", "Directorio de Empleados", "Solicitudes", "Área Administrativa", and "Cerrar Sesión (admin)". Below the header, there are two sections: "Quiénes somos" and "Últimas Noticias".

**Quiénes somos**

TEcnym es una empresa dedicada a proveer soluciones tecnológicas integrales, enfocada en la innovación y la calidad de servicio. Nuestra misión es ser el socio tecnológico de confianza para las PYMES, ayudándolas a navegar la transformación digital. Este portal de intranet es una herramienta clave para nuestros empleados, permitiendo un acceso centralizado a noticias, gestión de documentos y solicitudes internas, todo protegido por nuestra infraestructura de VPN y firewall.

**Últimas Noticias**

- 19/12/2025 - Actualización de última hora
- 12/11/2025 - Actualización de la intranet
- 03/11/2025 - Caída del servicio de WireGuard
- 03/11/2025 - Servidor en mantenimiento

**Imágenes 86 y 87 – Las noticias se actualizan dinámicamente, demostrando que el sistema de persistencia basado en archivos es funcional y eficiente para la escala de la PYME.**

## Prevención de Ataques XSS

Validación de la capa de seguridad en la presentación de datos para evitar la ejecución de código malicioso.

Metodología: Enviar una solicitud introduciendo el código `<script>alert('XSS')</script>` en el campo de descripción.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 66 de 89



The screenshot shows a web browser window titled "TEcnycom - Formulario de..." with the URL "http://192.168.50.10/solicitudes.php". The form fields are as follows:

- Nombre completo: Mohammed Maamla
- Correo electrónico: mohammedmaamla@tecnyc.com.es
- Tipo de solicitud: Otro
- Descripción:  
<script>alert('XSS Test TECNYCOM');</script>
- Adjuntar archivo (opcional): Examinar... No se ha seleccionado ningún archivo.

A blue "Enviar solicitud" button is at the bottom.

The screenshot shows the "Panel Admin" dashboard with the URL "http://192.168.50.10/admin/dashboard.php". It displays the following information:

- Estado del sistema:
  - Servidor Web (Apache): Activo
  - Servidor VPN (WireGuard): En ejecución
  - Base de datos: Desconectada (Simulado)
- Últimas solicitudes:

Mohammed Maamla (mohammedmaamla@tecnyc.com.es) [otro]:  
<script>alert('XSS Test TECNYCOM');</script>

**Imágenes 88 y 89 - Los caracteres < y > se convierten en entidades HTML, por lo que el navegador muestra el texto literalmente en lugar de ejecutar la ventana de alerta.**

Se confirma que la aplicación es resiliente ante ataques de inyección de código en el lado del cliente. Esta medida protege la sesión del administrador y evita el robo de cookies o la redirección maliciosa, cumpliendo con los requisitos de seguridad de la aplicación definidos en el análisis.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 67 de 89



## Subir Archivo Prohibido

Se comprueba la robustez del script procesar\_solicitud.php ante intentos de subida de archivos peligrosos.

Metodología: Intentar adjuntar un archivo con extensión .exe y seguidamente un .pdf

The top screenshot shows a "Gestión de Documentos" interface with a file input field containing "prueba.exe" and a "Subir Archivo" button. The bottom screenshot is a browser window showing an error message: "Error: Tipo de archivo no permitido. Solo se aceptan: pdf, docx, doc, xlsx, xls, jpg, jpeg, png, txt, zip, rar". It also includes a "Redirigiendo a la página principal en 3 segundos..." message.

Imágenes 90 y 91 – Prueba fallida, archivo .exe no permitido

The top screenshot shows the same "Gestión de Documentos" interface with a file input field containing "prueba.pdf" and a "Subir Archivo" button. The middle screenshot is a browser window showing a success message: "¡Éxito! Archivo subido correctamente: prueba.pdf". It also includes a "Redirigiendo a la página principal en 3 segundos..." message. The bottom screenshot shows a list titled "Archivos disponibles para descargar:" with links to "marco teorico y marco legal.docx", "prueba.pdf", "prueba.txt", "prueba.xls.txt", and "tfg.txt".

Imágenes 92, 93 y 94 – Prueba exitosa, archivo .pdf subido correctamente

El sistema rechaza el archivo y muestra un mensaje de error de "Extensión no permitida", permitiendo únicamente los formatos definidos en la lista blanca (PDF, JPG, DOCX).

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 68 de 89



## 3.5.5. Documentación del producto

Para la documentación del proyecto se presenta como un conjunto de manuales de uso concisos y bien organizados. Estos documentos sirven como herramienta de referencia y formación, garantizando que tanto los usuarios finales como el administrador puedan operar el sistema de manera segura y eficiente.

### Manual de Usuario (Empleado Final)

Dirigido a: Empleados, colaboradores y teletrabajadores.

#### 1. Instalación y Conexión al Túnel VPN (WireGuard)

El acceso a la red corporativa es obligatorio a través del túnel VPN.

Instalación: Instalar la aplicación WireGuard en el dispositivo (Windows, móvil, etc.).

Importación del Perfil: El administrador proporcionará un archivo de configuración único (.conf).

Activación: Haga clic en el botón "Activar" o "Connect" para establecer la conexión.

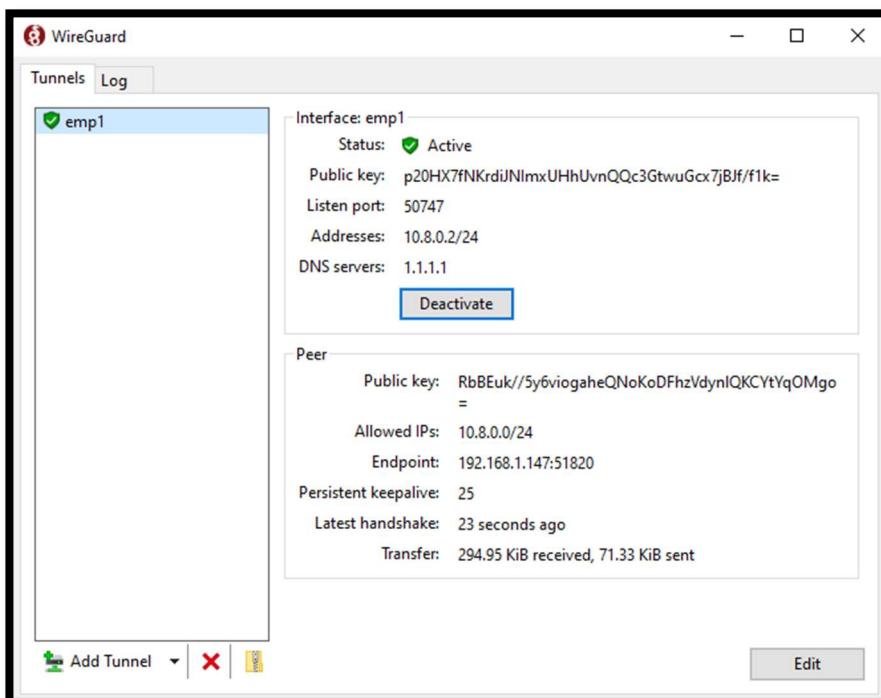


Imagen 95 - El túnel VPN activo en el cliente Windows (EMP 1), mostrando la conexión cifrada establecida

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 69 de 89

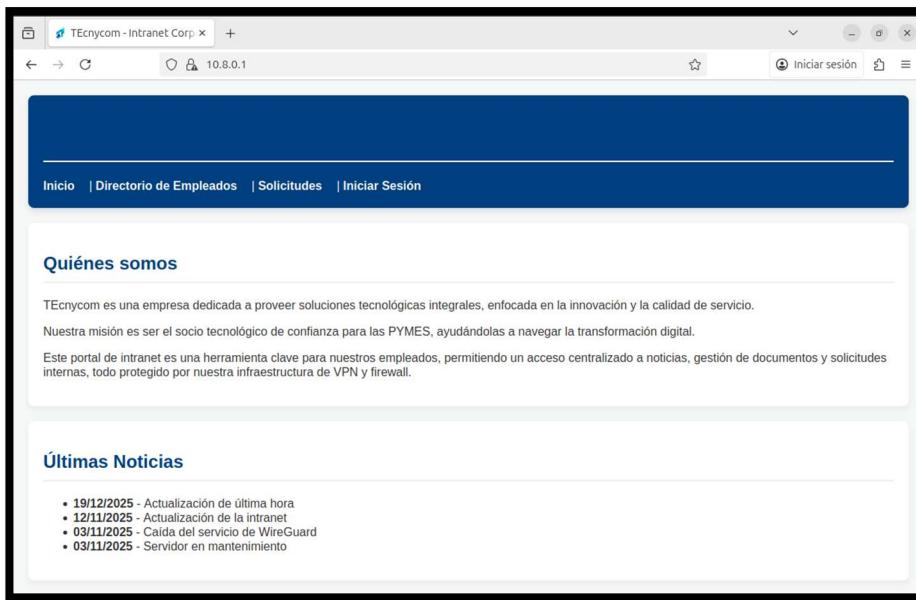


## 2. Acceso a la Intranet Corporativa

Solo con la VPN activa, podrá acceder a la Intranet.

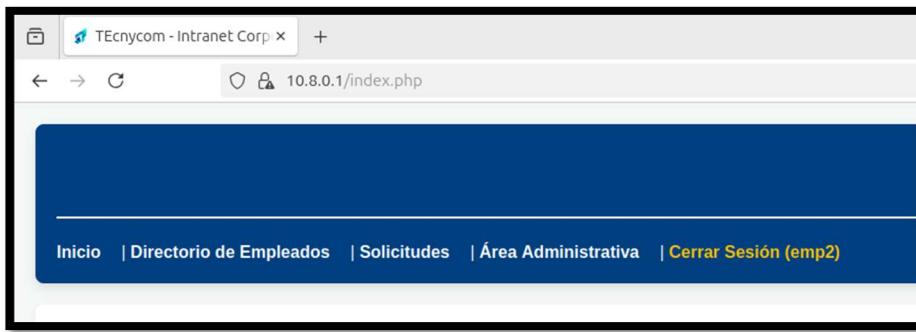
URL Segura: Abrir el navegador e introducir la dirección IP segura del servidor.

Dirección: <https://10.8.0.1>



**Imagen 96 - La URL de acceso a la Intranet. La conexión es segura (HTTPS) gracias al certificado instalado en el Servidor Central**

Inicio de Sesión: Introducir el usuario y la contraseña proporcionados.



**Imagen 97 – Se muestra la cabecera de la Intranet tras el inicio de sesión de EMP2**

Cierre de Sesión: Cuando finalice, use el enlace "Cerrar Sesión" y desactive el túnel VPN para liberar recursos.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 70 de 89



## Manual de Administrador (Infraestructura y Servicios)

Dirigido a: Personal técnico responsable de la infraestructura y el mantenimiento diario.

### 1. Gestión de Usuarios VPN (WireGuard)

#### A. Alta de Nuevos Empleados (Generación de Claves)

Acceder a la consola del Servidor Ubuntu (SRV1).

Generar un nuevo par de claves privada/pública para los nuevos empleados:

```
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp1_private.key | wg pubkey | sudo tee /etc/wireguard/emp1_public.key
p20HX7fNKrdiJNImxUHhUvnQc3GtwuGcx7jBJf/f1k=
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp2_private.key | wg pubkey | sudo tee /etc/wireguard/emp2_public.key
NrjUJuY1hpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
srv1@srv1:~$ wg genkey | sudo tee /etc/wireguard/emp3_private.key | wg pubkey | sudo tee /etc/wireguard/emp3_public.key
bBR4t3xyoyazW0eCc/Nr92M1InVLoBIXphIxF0JNmXY=
srv1@srv1:~$ sudo cat /etc/wireguard/emp1_private.key
IJKi0CxbJvaov155ogZDC73/FH3KAxxLkoSTL5e8aiw=
srv1@srv1:~$ sudo cat /etc/wireguard/emp2_private.key
oNvp3b/Hk1UABXYcjggUyi5N2SeS3uEWE/MUq/04r0M=
srv1@srv1:~$ sudo cat /etc/wireguard/emp3_private.key
yMj8FsuvCS9DfcE0WS9yE2HCggdUapwqnX3hU0mcrkM=
srv1@srv1:~$ sudo cat /etc/wireguard/emp1_public.key
p20HX7fNKrdiJNImxUHhUvnQc3GtwuGcx7jBJf/f1k=
srv1@srv1:~$ sudo cat /etc/wireguard/emp2_public.key
NrjUJuY1hpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
srv1@srv1:~$ sudo cat /etc/wireguard/emp3_public.key
bBR4t3xyoyazW0eCc/Nr92M1InVLoBIXphIxF0JNmXY=
srv1@srv1:~$
```

### Imagen 98 – Claves de los empleados creadas

Configuración en el Servidor: Editar el archivo /etc/wireguard/wg0.conf para añadir el nuevo [Peer].

```
GNU nano 7.2
/etc/wireguard/wg0.conf
[Interface]
Address = 10.8.0.1/24
ListenPort = 51820
PrivateKey = gP4hgRgBXSthnWMGiFYTkDz+PAcKpezEvp+UnwOXh0Q=


#Empleados
[Peer]
PublicKey = p20HX7fNKrdiJNImxUHhUvnQc3GtwuGcx7jBJf/f1k=
AllowedIPs = 10.8.0.2/32

[Peer]
PublicKey = NrjUJuY1hpMn9nJGoGR+D/dgTA9zsu3w/ck4qONWAlc=
AllowedIPs = 10.8.0.3/32

[Peer]
PublicKey = bBR4t3xyoyazW0eCc/Nr92M1InVLoBIXphIxF0JNmXY=
AllowedIPs = 10.8.0.4/32
```

### Imagen 99 - Extracto de wg0.conf mostrando la estructura de un nuevo [Peer] con su clave pública y su IP virtual asignada

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 71 de 89



## Baja de un Empleado

Para revocar el acceso a un usuario, simplemente se debe eliminar su bloque [Peer] completo del archivo /etc/wireguard/wg0.conf y recargar la configuración.

## 2. Gestión de Almacenamiento (TrueNAS)

Acceso: Acceder a la interfaz web del NAS (IP: 192.168.50.100).

Verificación del Pool (Redundancia): Revisar el Dashboard para confirmar el estado de salud del pool de backups (Backups).

Estado Ideal: ONLINE.

Estado de Advertencia: DEGRADADO (implica que un disco ha fallado y debe ser reemplazado urgentemente).

Imagen 100 - Interfaz del TrueNAS confirmando el estado de salud del Pool de Backups y la configuración RAIDZ1

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 72 de 89



### 3. Verificación de Seguridad Perimetral (pfSense)

El firewall protege la LAN, permitiendo únicamente el tráfico VPN.

Revisión de Reglas: En Firewall → Rules → WAN, confirmar que solo las reglas para el puerto 51820 (WireGuard) y la gestión están activas.

The screenshot shows the pfSense Firewall Rules interface. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a breadcrumb trail: Firewall / Rules / WAN. The WAN tab is selected. The main area displays a table titled "Rules (Drag to Change Order)". The table has columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are three entries:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
3/10.81 MiB	IPv4 TCP	WAN subnets	*	This Firewall (self)	443 (HTTPS)	*	none		PFSENSE HTTPS WAN	
0/0 B	IPv4 UDP	*	*	WAN address	51820	*	none		WIREGUARD UDP WAN	
0/2.69 MiB	IPv4 UDP	*	*	192.168.50.10	51820	*	none		NAT	

At the bottom of the table are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Imagen 101 - Vista de las reglas de Firewall en pfSense, confirmando la aplicación de la política de mínimo privilegio (solo 51820 abierto)

## Manual de Seguridad y Mantenimiento

Dirigido a: Personal técnico.

Objetivo: Establecer una rutina semanal de verificación y auditoría para prevenir fallos y ataques.

### 1. Rutina de Mantenimiento

Diaria

Auditoría de Backups

Revisar el archivo de log (/var/log/backup\_web.log) para confirmar la ejecución del script backup.sh.

Semanal

Estado del RAID

Acceder a TrueNAS y verificar el estado del Pool (ONLINE).

Mensual

Revisión de Logs

Revisar los logs de pfSense (WAN) para identificar patrones de ataque bloqueados.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 73 de 89



## 2. Procedimiento de Recuperación ante Desastres

Si el Servidor Central (SRV1) sufre un fallo total, se sigue este proceso:

Identificación de Fallo: Confirmar que SRV1 está inoperativo.

Recuperación del Backup:

Montar la carpeta NFS del NAS en un nuevo Servidor Ubuntu de reemplazo.

Copiar el último archivo backup\_AAAA-MM-DD.tar.gz al nuevo servidor.

Restauración: Descomprimir el archivo en el directorio /var/www/html para restaurar la Intranet a su estado más reciente.

Comando: sudo tar -xzf backup\_AAAA-MM-DD.tar.gz

## B. Procedimiento en Caso de Fallo del Túnel VPN

Diagnóstico del Firewall: Verificar si el pfSense (192.168.1.147) está accesible.

Diagnóstico del Servicio: En SRV1, verificar que el servicio WireGuard está activo

Comando: sudo systemctl status wg-quick@wg0.

Diagnóstico del Peer: Usar sudo wg para ver si hay algún Latest Handshake de los clientes. Si no hay, la clave pública del cliente podría estar mal configurada.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 74 de 89



## 3.5.6. Formación de usuarios

La implementación de una nueva infraestructura y una Intranet corporativa requiere un proceso de transferencia de conocimiento para garantizar que los empleados puedan utilizar el sistema de manera eficiente y segura.

El plan de formación se estructura en dos niveles, adaptados a las necesidades y privilegios de cada grupo de usuarios.

### Formación Nivel 1: Usuarios Finales (Empleados)

Público Objetivo: Todo el personal que requiere acceso a la Intranet y a la red corporativa.

#### A. Acceso Seguro (VPN)

Asegurar que el empleado puede instalar, configurar y conectar el túnel WireGuard desde cualquier dispositivo (PC, móvil).

Demostración práctica en vivo (compartir pantalla) de la instalación en un cliente Windows y en la aplicación móvil.

#### B. Uso de la Intranet

Demostrar el proceso de inicio de sesión seguro (HTTPS) y el uso correcto de los módulos de la Intranet (Consulta de Empleados, Formulario de Solicitudes).

Énfasis en la URL correcta (<https://...>) y el proceso de cierre de sesión.

#### C. Seguridad y Privilegios

Concienciar sobre qué contenido es sensible y la importancia de no compartir credenciales ni utilizar la VPN en redes públicas inseguras.

Explicación de por qué el acceso al área /admin/ está denegado para el rol 'empleado'.

### Formación Nivel 2: Administrador del Sistema

Público Objetivo: El técnico de la PYME o el jefe de departamento que se encargará del mantenimiento de la infraestructura.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 75 de 89



## A. Gestión de la Seguridad Perimetral

Saber cómo verificar el estado de pfSense, revisar los logs (WAN) para detectar ataques y confirmar que el Port Forward del puerto 51820 está activo.

Uso del Manual de Seguridad y Mantenimiento (En Documentación del Producto) como guía de referencia.

## B. Gestión de Usuarios VPN

Saber cómo generar un nuevo par de claves WireGuard, añadir un nuevo [Peer] a wg0.conf y proporcionar el archivo de configuración al nuevo empleado.

Uso del Manual de Administrador (En Documentación del Producto) como guía de referencia.

## C. Verificación de Backups y Resiliencia

Saber cómo comprobar el estado del pool RAIDZ1 en TrueNAS y cómo verificar que la tarea programada (cron) ha funcionado correctamente.

Revisión del archivo de log diario (/var/log/backup\_web.log) y acceso a la interfaz web del NAS (192.168.50.100).

La formación durará entorno a 50 horas repartida en 10 días.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 76 de 89



## Resultados obtenidos y conclusiones

Tras la ejecución del plan de pruebas, se concluye que el proyecto ha cumplido satisfactoriamente con todos los objetivos planteados inicialmente. Se ha logrado desplegar una infraestructura de red segura y resiliente que proporciona a la PYME las herramientas necesarias para el teletrabajo seguro (VPN), la comunicación interna (Intranet) y la protección de datos (Firewall y Backup).

La integración de tecnologías de código abierto ha permitido mantener un presupuesto ajustado sin comprometer la calidad ni la seguridad de nivel profesional.

La realización de este proyecto ha significado un crecimiento notable en mi capacidad de resolución de problemas técnicos de forma autónoma. He aprendido que lo estudiado ayuda a resolver errores reales, como los problemas de montaje NFS o la gestión de estados degradados en sistemas RAID, y a pesar de haber utilizado inteligencia artificial para archivos y scripts he sido capaz de entender cada punto y modificarlo de tal manera que todo sea compatible y funcione.

A nivel de organización, me ha ayudado a entender que un proyecto de sistemas no es una serie de tareas aisladas, sino un engranaje donde la red, el almacenamiento y el desarrollo deben estar perfectamente alineados.

A pesar de la robustez del sistema actual, existen áreas que podrían ampliarse para mejorar la funcionalidad y seguridad a largo plazo:

**Alta Disponibilidad (HA):** Implementar un segundo servidor para que la conexión a internet y la VPN nunca se pierdan si un hardware falla.

**Monitorización Avanzada:** Desplegar un sistema para recibir alertas en tiempo real sobre el consumo de recursos o intentos de intrusión bloqueados.

**Copia en la Nube:** Conseguir que el NAS cree copias de seguridad y las envíe a un almacenamiento externo cifrado.

**Base de datos:** Implementar una base de datos en la que guardar los empleados y sus datos en vez de usar 'empleados.php'.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 77 de 89



## Bibliografía

Canonical Ltd. (s.f.). *Ubuntu Server*. <https://ubuntu.com/server>

Clockwork Computer. (2024, 26 de diciembre). *PFSENSE 01. INSTALACIÓN en VIRTUALBOX* [Video]. YouTube. <https://www.youtube.com/watch?v=OahhshKMM9Y>

Clockwork Computer. (2025, 5 de febrero). *PFSENSE 09. WIREGUARD VPN IDS IPS SIEM* [Video]. YouTube. <https://www.youtube.com/watch?v=tKhKMBpnsZQ>

Cloudflare. (s.f.). ¿Qué es un certificado SSL? <https://www.cloudflare.com/es-es/learning/ssl/what-is-an-ssl-certificate/>

Cloudflare. (s.f.). ¿Qué es una red Zero Trust? <https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/>

Donenfeld, J. A. (2017). *WireGuard: Next generation kernel network tunnel* [White paper]. <https://www.wireguard.com/papers/wireguard.pdf>

ISOTOOLS Excellence. (s.f.). *Norma ISO 27001*. <https://www.normaiso27001.es/>

Jefatura del Estado. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado, 294, de 6 de diciembre de 2018. <https://www.boe.es/eli/es/lo/2018/12/05/3>

Netgate. (s.f.). *pfSense documentation*. <https://docs.netgate.com/pfsense/>

OpenAI. (s.f.). *ChatGPT* [Aplicación web]. <https://chat.openai.com>

Oracle Corporation. (s.f.). *Oracle VM VirtualBox. User Manual*. <https://www.virtualbox.org/manual/UserManual.html>

Organización Internacional de Normalización. (2022). *ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos*. (ISO/IEC 27001:2022). <https://www.iso.org/standard/82875.html>

Parlamento Europeo y Consejo de la Unión Europea. (2016, 27 de abril). *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)*. Diario Oficial de la Unión Europea, L 119/1. <http://data.europa.eu/eli/reg/2016/679/oj>

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 78 de 89



The Apache Software Foundation. (s.f.). *Apache HTTP Server Project*. <https://httpd.apache.org/>

The Apache Software Foundation. (s.f.). *SSL/TLS Strong Encryption: How-To*. Apache HTTP Server Project. [https://httpd.apache.org/docs/2.4/ssl/ssl\\_howto.html](https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html)

WireGuard. (s.f.). *WireGuard: fast, modern, secure VPN tunnel*. <https://www.wireguard.com/>

Mermaid Chart. (s.f.). *Mermaid Chart* [Aplicación web]. <https://www.mermaidchart.com/>

GanttProject. (s.f.). *GanttProject* (Versión 3.2) [Software de ordenador]. <https://www.ganttproject.biz/>

Google. (s.f.). *Gemini Pro* [Modelo de lenguaje grande multimodal]. <https://deepmind.google/technologies/gemini/#gemini-1.5>

IbericaVIP. (s.f.). *Combo All in One: Monitor + Teclado/Ratón/Auriculares - 100% PCVIP*. <https://ibericavip.com/teclados/combo-all-in-one-monitor-tecladoratonauriculares-100-pcvip>

Lenovo. (s.f.). *ThinkCentre Neo 50t Gen 5 (Intel) Torre*. <https://www.lenovo.com/es/es/p/desktops/thinkcentre/thinkcentre-neo-series/lenovo-thinkcentre-neo-50t-gen-5-intel-tower/12udcto1wwes2>

MediaMarkt. (s.f.). *Mini PC - LENOVO ThinkCentre neo 50q Gen 4, Intel® Core™ i5-13420H*. [https://www.mediamarkt.es/es/product/\\_mini-pc-lenovo-thinkcentre-neo-50q-gen-4-intelr-coretm-i5-i5-13420h-8-gb-ram-256-gb-ssd-uhd-graphics-sin-sistema-operativo-negro-159085824.html](https://www.mediamarkt.es/es/product/_mini-pc-lenovo-thinkcentre-neo-50q-gen-4-intelr-coretm-i5-i5-13420h-8-gb-ram-256-gb-ssd-uhd-graphics-sin-sistema-operativo-negro-159085824.html)

MediaMarkt. (s.f.). *Móvil - Samsung Galaxy A17 LTE, Azul, 256 GB, 8 GB RAM*. [https://www.mediamarkt.es/es/product/\\_movil-samsung-galaxy-a17-lte-azul-256-gb-8-gb-ram-67-fhd-super-amoled-mediatek-g99-octa-core-5000-mah-android-15-1604164.html](https://www.mediamarkt.es/es/product/_movil-samsung-galaxy-a17-lte-azul-256-gb-8-gb-ram-67-fhd-super-amoled-mediatek-g99-octa-core-5000-mah-android-15-1604164.html)

MicroPyme. (s.f.). *Netgate 2100 Base pfSense+ Security Gateway*. <https://shop.micropyme.com/es/gateways-pfsense/29-netgate-2100-base-pfsense-security-gateway.html>

Microsoft. (s.f.). *Comprar y descargar Windows 11 Pro*. <https://www.microsoft.com/es-es/d/windows-11-pro/dg7gmgf0d8h4/000P>

TrueNAS Community. (s.f.). *TrueNAS CORE Download*. Recuperado de <https://www.truenas.com/download-truenas-community-edition/>

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 79 de 89



UGREEN. (s.f.). *UGREEN NASync DXP4800 Plus, NAS 4 bahías, Intel Pentium Gold 8505 (DXP4800 Plus)*. Amazon.es. Recuperado de <https://www.amazon.es/dp/B0D2KKVZN2>

Resolución de 4 de abril de 2025, de la Dirección General de Trabajo, por la que se registra y publica el XIX Convenio colectivo estatal de empresas de consultoría, tecnologías de la información y estudios de mercado y de la opinión pública. (16 de abril de 2025). *Boletín Oficial del Estado*, núm. 92, Disposición 7766. Recuperado de <https://www.boe.es/boe/dias/2025/04/16/pdfs/BOE-A-2025-7766.pdf>

Repositorio de GitHub. (2025). TFG: Infraestructura de Red Segura para PYME – Tecnycom, GitHub. Recuperado de <https://github.com/mohamaamla77/TFG.git>

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 80 de 89



## Anexos

### Anexo I - Control de Acceso y Gestión de Sesiones (validar\_login.php)

Este archivo es el corazón de la seguridad de la aplicación. Su función es verificar la identidad de los usuarios y asignarles un rol que determinará qué partes de la infraestructura pueden ver.

```
GNU nano 7.2                               validar_login.php
<?php
/*
 * validar_login.php (Script de Lógica de Autenticación)
 *
 * Este script NO es una página web que se ve. Es un script.
 * Su único trabajo es:
 * 1. Iniciar el motor de sesiones de PHP.
 * 2. Simular una base de datos con usuarios y contraseñas válidos.
 * 3. Recoger los datos (usuario/clave) que el usuario escribió en 'login.php'.
 * 4. Comprobar si el usuario y la clave son correctos.
 */

// --- 1. INICIAR EL SISTEMA DE SESIONES ---
session_start();

// --- 2. SIMULACIÓN DE BASE DE DATOS (Usuarios Válidos) ---
// Aquí se encuentran los usuarios de la empresa.
$usuarios_validos = [
    // 'nombre_de_usuario' => 'contraseña'
    'admin' => 'admin', // Este usuario tiene rol de Administrador
    'emp1' => 'emp1', // Este usuario tiene rol de Empleado
    'emp2' => 'emp2', // Este usuario tiene rol de Empleado
    'emp3' => 'emp3' // Este usuario tiene rol de Empleado
];

// --- 3. RECOGIDA DE DATOS DEL FORMULARIO ---
// $_POST es un array especial de PHP que contiene los datos
// enviados por un formulario con 'method='post''.
// '$_POST['usuario']' -> coge el valor del campo con name="usuario".
// '$_POST['clave']' -> coge el valor del campo con name="clave".
//
// Usamos el "operador de fusión de null" (?? '') como atajo.
// Significa: "coge el valor de $_POST['usuario']", pero si no existe, usa '' (vacío)".
// Esto es una medida simple para evitar errores si alguien accede a este script directamente.
$usuario_form = $_POST['usuario'] ?? '';
$clave_form = $_POST['clave'] ?? '';

// --- 4. VALIDACIÓN DE CREDENCIALES ---
// Esta es la comprobación de seguridad principal.
//
// 'isset($usuarios_validos[$usuario_form])'
// Comprueba si el usuario que escribió el usuario (ej. 'admin')
// existe como "clave" en nuestro array de $usuarios_validos.
// (Evita errores si el usuario no existe)
//
```

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 81 de 89



```
// '$usuarios_validos[$usuario_form] == $clave_form'  
// Comprueba si la contraseña de ese usuario en nuestro array  
// (ej. $usuarios_validos['admin'] que es 'admin')  
// es EXACTAMENTE igual a la contraseña que escribió el usuario.  
  
if (isset($usuarios_validos[$usuario_form]) && $usuarios_validos[$usuario_form] == $clave_form) {  
    // --- 5. ¡ÉXITO! Usuario y contraseña correctos ---  
  
    // "Recordamos" al usuario para las demás páginas.  
    // Creamos una variable de sesión llamada 'usuario_logueado'  
    // y le asignamos el nombre del usuario.  
    // Esta variable $_SESSION estará disponible en TODAS las páginas  
    // (siempre que hagamos session_start() al principio).  
    $_SESSION['usuario_logueado'] = $usuario_form;  
  
    // Asignamos un "rol" (permiso) a este usuario en la sesión.  
    // Si el usuario es 'admin', dale el rol 'admin', si no, dale 'empleado'  
    $_SESSION['rol'] = ($usuario_form == 'admin') ? 'admin' : 'empleado';  
  
    // Redirigimos al usuario al panel de administración  
    // 'header('Location: ...')' envía una orden al navegador.  
    header('Location: admin/dashboard.php');  
  
    // 'exit' detiene la ejecución del script. Es una buena práctica  
    // de seguridad para asegurar que la redirección ocurra inmediatamente.  
    exit;  
}  
else {  
    // --- 6. ¡FALLO! Usuario o contraseña incorrectos ---  
  
    // El usuario no existía o la contraseña era incorrecta.  
    // Lo redirigimos de vuelta a la página de login para que lo intente de nuevo.  
    header('Location: login.php'); // (Tu archivo se llama 'login.html', pero lo renombramos a 'login.php')  
    exit;  
}
```

## Imágenes 102 y 103 – Script validar\_login.php

Lógica principal:

Inicio de Sesión: Se utiliza session\_start() para crear una cookie de sesión única en el navegador del usuario.

Verificación Criptográfica: Compara el usuario y la clave introducidos en el formulario contra el array de usuarios válidos (simulando una base de datos).

Asignación de Roles: Dependiendo de la identidad, se guarda en la variable global \$\_SESSION['rol'] el valor 'admin' o 'empleado'.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 82 de 89



## Anexo II - Gestión Segura de Solicitudes y Archivos (procesar\_solicitud.php)

Este script gestiona la entrada de datos externos, aplicando medidas contra las vulnerabilidades más comunes de la web (OWASP).

```
GNU nano 7.2                                         procesar_solicitud.php

<?php
/*
 * procesar_solicitud.php
 *
 * Este script NO es una página web que se ve.
 * Su trabajo es:
 * 1. Recoger los datos enviados por el formulario de 'solicitudes.php'.
 * 2. Validar los datos de texto.
 * 3. Procesar y guardar el archivo adjunto (si existe) de forma segura.
 * 4. Guardar la solicitud en un archivo de texto/HTML.
 * 5. Mostrar un mensaje de éxito y redirigir al usuario.
 */

// --- 1. RECOGIDA DE DATOS DEL FORMULARIO ---

// '$_POST' es un array especial de PHP que contiene todos los datos
// enviados por un formulario con 'method='post''.
// Usamos el "operador de fusión de null" (?? '') como atajo.
// Significa: "coge el valor de $_POST['nombre'], pero si no existe, usa '' (vacío)".
// Esto evita errores si alguien accede al script directamente.
$nombre = $_POST['nombre'] ?? '';
$email = $_POST['email'] ?? '';
$tipo = $_POST['tipo'] ?? '';
$mensaje = $_POST['mensaje'] ?? '';

// --- 2. VALIDACIÓN BÁSICA DE TEXTO ---

// Si falta algún campo obligatorio, muestra un error y detiene el script.
if (!$nombre || !$email || !$tipo || !$mensaje) {
    echo "Faltan datos en el formulario. <a href='solicitudes.php'>Volver</a>";
    exit; // 'exit' detiene la ejecución del script aquí.
}

// --- 3. PROCESAMIENTO DEL ARCHIVO ADJUNTO ---

// Esta variable guardará el enlace <a> si la subida es exitosa.
// Si no se sube archivo, se quedará vacía.
$enlace_archivo = '';

// '__DIR__' es una constante de PHP que significa "el directorio de este script"
$ruta_subidas = __DIR__ . '/solicitudes/'; // La carpeta de destino

// '$_FILES' es otro array especial de PHP para los archivos subidos.
// 'isset($_FILES['adjunto'])' -> Comprueba si se envió un archivo con name="adjunto".
// '$_FILES['adjunto']['error'] == 0' -> Comprueba que la subida fue exitosa (código 0).
if (isset($_FILES['adjunto']) && $_FILES['adjunto']['error'] == 0) {
```

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 83 de 89



```
// --- 1A. MEDIDA DE SEGURIDAD 1: VALIDAR TIPO DE ARCHIVO ---
// NO se confía en el tipo de archivo que dice el navegador, se confía en la extensión.
$nombre_original = $_FILES['adjunto']['name']; // ej. "mi_factura.pdf"
// 'pathInfo' saca la extensión, 'strtolower' la pasa a minúsculas (PDF > pdf).
$extension = strtolower(pathinfo($nombre_original, PATHINFO_EXTENSION));

// Lista blanca de extensiones que SÍ permitimos.
// Esto es crucial para evitar que alguien suba un virus (ej. .exe) o
// un script malicioso (ej. .php).
$extensiones_permitidas = ['pdf', 'docx', 'jpg', 'jpeg', 'png', 'txt'];

// 'in_array()' comprobamos si la extensión del archivo está en nuestra $extensiones_permitidas.
if (in_array($extension, $extensiones_permitidas)) {

    // --- 2B. MEDIDA DE SEGURIDAD 2: CREAR NOMBRE DE ARCHIVO ÚNICO ---
    // Si dos usuarios suben "factura.pdf", el segundo borraría al primero.
    // 'uniqid()' genera un ID único basado en la hora actual (ej. "6900e812c62f2").
    // Esto asegura que no haya colisiones.
    $nombre_seguro = uniqid() . '.' . $extension; // ej. "6900e812c62f2.pdf"
    $ruta_destino = $ruta_subidas . $nombre_seguro; // Ruta final donde se guardará

    // --- 3C. MOVER EL ARCHIVO ---
    // 'move_uploaded_file()' es la función segura de PHP para mover
    // el archivo desde la carpeta temporal de PHP (tmp_name) a nuestra carpeta de destino.
    if (move_uploaded_file($_FILES['adjunto']['tmp_name'], $ruta_destino)) {

        // El archivo está en /solicitudes/. Ahora creamos el HTML.
        // 'htmlspecialchars()' es OTRA MEDIDA DE SEGURIDAD (XSS)
        // para los nombres de archivo.
        $enlace_archivo = "<br><b>Archivo adjunto:</b> <a href='../../solicitudes/' . htmlspecialchars($nombre_seguro) . '" target='_blank'>" . htmlspecialchars($enlace_archivo) . "</a>";

    } else {
        // Error si 'move_uploaded_file()' falla.
        echo "Error: No se pudo mover el archivo. <a href='solicitudes.php'>Volver</a>";
        exit;
    }
} else {
    // Error si la extensión (ej. ".exe") no estaba en nuestra lista blanca.
    echo "Error: Tipo de archivo no permitido (solo PDF, DOCX, JPG, PNG, TXT). <a href='solicitudes.php'>Volver</a>";
    exit;
}
}

// --- 4. FORMATEAR LA SOLICITUD COMO HTML ---
// 'htmlspecialchars()' es la MEDIDA DE SEGURIDAD MÁS IMPORTANTE aquí.
// Evita que un usuario escriba código HTML o JavaScript malicioso (Ataque XSS)
$entrada = "<p><strong>" . htmlspecialchars($nombre) . "</strong> (" . htmlspecialchars($email) . ") [ " . htmlspecialchars($tipo) . "]<br>" .
    "<hr>" . htmlspecialchars($mensaje) . ";
    // 'nl2br()' convierte los saltos de línea (Enter) en etiquetas <br>
    nl2br(htmlspecialchars($mensaje));
    // Añade el enlace <a> si la subida fue exitosa, o '' (vacío) si no.
    $enlace_archivo =
        "</p>\n"; // '\n' es un salto de línea (para ordenar el archivo guardado)

// --- 5. GUARDAR LA SOLICITUD EN EL ARCHIVO ---
// Ruta al archivo donde guardamos todo (nuestra "base de datos" plana)
$archivo = __DIR__ . '/admin/solicitudes_guardadas.html';

// 'file_get_contents()' lee el contenido antiguo del archivo
// El '?' es un if corto:
// Si el archivo existe, leelo; si no, usa '' (vacío)
$contenido_actual = file_exists($archivo) ? file_get_contents($archivo) : '';

// 'file_put_contents()' escribe en el archivo.
// Escribimos la $entrada nueva primero, y luego el $contenido_actual.
// Esto hace que las solicitudes más nuevas aparezcan arriba.
file_put_contents($archivo, $entrada . $contenido_actual);

// --- 6. MOSTRAR MENSAJE DE ÉXITO Y REDIRIGIR ---
echo "<h2>Solicitud recibida correctamente</h2>";
echo "<p>Gracias, <strong>" . htmlspecialchars($nombre) . "</strong>. Su solicitud ha sido enviada.</p>";
echo "<p>Redirigiendo al panel administrativo...</p>";

// 'header("refresh:3;")' es una orden de PHP al navegador,
// Le dice: "Espera 3 segundos, y luego redirige a esta URL".
header("refresh:3;url=admin/dashboard.php");
exit; // Termina el script
?>
```

## Imágenes 104, 105 y 106 – Script procesar\_solicitud.php

### Capas de Seguridad:

Saneamiento XSS: Uso de htmlspecialchars() para neutralizar etiquetas de código malicioso.

Lista Blanca (Whitelist): El script solo permite subir archivos con extensiones seguras como PDF, JPG o DOCX, bloqueando cualquier intento de subir ejecutables (.exe) o scripts (.php).

Anonimización de Archivos: Se utiliza uniqid() para renombrar los archivos subidos, evitando que un usuario pueda sobreescribir el archivo de otro empleado.

# Servidor Web con Acceso Seguro a través de VPN

*Mohammed Maamla Razzak*

maamla\_mohammed\_asir

Página 84 de 89



### **Anexo III - Monitorización de Servicios y Dashboard (admin/dashboard.php)**

El panel del administrador no solo muestra datos, sino que actúa como una consola de monitorización básica del estado de los servicios del servidor Ubuntu.

```
GNU nano 7.2 dashboard.php
<?php
/*
 * admin/dashboard.php (Panel de Administración)
 *
 * Esta es la página principal y privada del administrador.
 * Es el archivo más complejo porque combina 4 tareas:
 * 1. Seguridad (Comprobar quién eres).
 * 2. Monitorización (Ver el estado del servidor).
 * 3. Lectura de datos (Ver solicitudes).
 * 4. Escritura de datos (Publicar noticias).
 */

// --- 1. INICIAR LA SESIÓN ---
session_start();

// --- 2. MEDIDA DE SEGURIDAD 1: ¿ESTÁ LOGUEADO? ---
// 'isset' comprueba si la variable $_SESSION['usuario_logueado'] existe.
if (!isset($_SESSION['usuario_logueado'])) {
    // Si no ha iniciado sesión, lo "expulsamos" a la página de login.
    // 'header('Location: ...')' redirige al navegador.
    // Usamos '../login.php' porque tenemos que "subir un nivel"
    // desde la carpeta /admin/ para encontrar 'login.php' en la raíz.
    header('Location: ../login.php');

    // 'exit' detiene la ejecución del script. Es crucial después de una redirección.
    exit;
}

// --- 3. MEDIDA DE SEGURIDAD 2: ¿TIENE PERMISOS DE ADMIN? ---
// Comprobamos la variable 'rol' que creamos en 'validar_login.php'.
// Si el rol NO ES (!=) 'admin'...
if ($_SESSION['rol'] != 'admin') {
    // El usuario está logueado, pero es un "empleado" normal.
    // Le mostramos un mensaje de error y detenemos el script.
    echo "<h1>Acceso Denegado</h1><p>No tienes permisos de administrador.</p>";
    echo "<a href='../../index.php'>Volver al inicio</a>";
    exit;
}

// --- SI EL SCRIPT LLEGA HASTA AQUÍ, SIGNIFICA QUE EL USUARIO ES EL ADMIN ---
// --- 4. LÓGICA DE MONITORIZACIÓN DEL SERVIDOR ---

/*
```

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 85 de 89



```
* 'shell_exec' es una función de PHP que ejecuta un comando
* directamente en la terminal del servidor Linux.
*
* ¿Por qué 'sudo'?
* Porque el usuario de Apache ('www-data') no tiene permisos
* para ver el estado de los servicios.
*
* ¿Cómo funciona?
* 1. En el servidor Linux, se ha ejecutado 'sudo visudo'.
* 2. Al final de ese archivo, se ha añadido esta línea:
* www-data ALL=(ALL) NOPASSWD: /usr/bin/systemctl is-active apache2, /usr/bin/systemctl is-active wg-quick@wg0
* 3. Esto le da permiso a Apache para ejecutar *solos* esos dos
* comandos de forma segura y sin pedir contraseña.
*/
// 4A. Comprobar el estado de Apache
$apache_raw = shell_exec('sudo systemctl is-active apache2');
// trim() limpia la respuesta (quita saltos de linea).
// Usamos un 'if' corto (ternario):
// (condición) ? (si es verdad) : (si es falso)
$estado_apache = (trim($apache_raw) == 'active') ? '↑ Activo' : '↑ Inactivo/Caído';

// 4B. Comprobar el estado de WireGuard
$vpn_raw = shell_exec('sudo systemctl is-active wg-quick@wg0');
$estado_vpn = (trim($vpn_raw) == 'active') ? '↑ En ejecución' : '↑ Detenido';

?>
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8" />
    <title>TEcnycam - Panel Administrativo</title>
    <!--
        RUTAS RELATIVAS (...)
        Como este archivo está en la carpeta /admin/,
        necesitamos "subir un nivel" (con '../') para
        encontrar las carpetas /css/ y el 'logo.png' que están en la raíz.
    -->
    <link rel="stylesheet" href="../css/estilo.css" />
    <link rel="icon" href="../logo.png" type="image/png">
</head>
<body>
    <header>
        <h1>Panel Administrativo</h1>
        <nav>
```

```
<!-- Los enlaces también suben un nivel (../) -->
<a href="../index.php">Inicio</a> |
<!--
<a href="../empleados.php">Directorio de Empleados</a> |
<a href="../solicitudes.php">Solicitudes</a>
<!--
    Como este dashboard SÓLO lo ve un admin logueado,
    no necesitamos el 'if (isset...)' aquí.
    Podemos poner el enlace de "Cerrar Sesión" directamente.
-->
<a href="../logout.php" style="color: #FFC107;"><b>Cerrar Sesión (<?php echo htmlspecialchars($_SESSION['usuario_logueado']); ?>)</b></a>
</nav>
</header>
<!-- Sección de Estado (muestra las variables PHP de arriba) -->
<section>
    <h2>Estado del sistema</h2>
    <ul>
        <li>Servidor Web (Apache): <strong><?php echo $estado_apache; ?></strong></li>
        <li>Servidor VPN (WireGuard): <strong><?php echo $estado_vpn; ?></strong></li>
        <li>Base de datos: <strong>Desconectada</strong> (Simulado)</li>
    </ul>
</section>
<!-- Sección de Solicitudes (Lectura de archivo) -->
<section>
    <h2>Últimas solicitudes</h2>
    <?php
        // __DIR__ es la carpeta actual (/admin/)
        $archivo = __DIR__ . '/solicitudes_guardadas.html';
        // Comprueba si el archivo existe y no está vacío
        if (file_exists($archivo) && filesize($archivo) > 0) {
            // Imprime todo el contenido del archivo aquí
            echo file_get_contents($archivo);
        } else {
            echo "<p>No hay solicitudes nuevas.</p>";
        }
    </?php
</section>
```

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 86 de 89



```
<!-- Sección de Noticias (Formulario de envío) -->
<section>
    <h2>Publicar Nueva Noticia</h2>
    <!--
        Este formulario envía los datos a 'procesar_noticia.php',
        que está en esta misma carpeta /admin/.
    -->
    <form action="procesar_noticia.php" method="post">
        <label for="noticia">Contenido de la noticia:</label><br>
        <textarea id="noticia" name="noticia" rows="5" style="width: 90%;" required></textarea><br><br>
        <input type="submit" value="Publicar Noticia">
    </form>
</section>
<footer>
    <p>© 2025 TEcnycam - Todos los derechos reservados.</p>
</footer>
</body>
</html>
```

## Imágenes 107, 108, 109 y 110 – Script dashboard.php

### Funcionalidades destacadas:

Comandos de Sistema: Mediante la función shell\_exec, el script ejecuta el comando systemctl is-active para comprobar si Apache y WireGuard están funcionando.

Permisos Sudoers: Para que esto funcione de forma segura, se configuró el archivo /etc/sudoers permitiendo que el usuario de la web ejecute únicamente esos comandos específicos sin contraseña.

Seguridad de Acceso: Incluye un bloque de código que expulsa a cualquier usuario que intente entrar sin el rol de administrador.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 87 de 89



## Anexo IV - Automatización de la Continuidad de Negocio (backup\_web.sh)

Para asegurar la disponibilidad de los datos ante fallos críticos, se ha implementado un script de automatización en Bash que se ejecuta de forma recurrente.

A screenshot of a terminal window titled "SRV 1 (Instantánea OK) [Corriendo] - Oracle VirtualBox". The window shows the contents of a file named "backup.sh" in the "nano" text editor. The code in the editor is:

```
GNU nano 7.2
#!/bin/bash

FECHA=$(date +%F)
tar -czf /mnt/backup_nas/backup_$FECHA.tar.gz /var/www/html
```

Imagen 111 – Script backup.sh

El archivo backup.sh se encarga de capturar la fecha actual, definir las rutas de origen y destino (el punto de montaje del NAS) y realizar la compresión de todo el directorio web.

Programación de la tarea (Crontab):

```
# m h dom mon dow   command
0 3 * * * /home/srv1/backup.sh >> /var/log/backup_web.log 2>&1_
```

Imagen 112 – Línea de comando en crontab

Para que este proceso sea totalmente desatendido, se ha programado su ejecución diaria a las 03:00 AM mediante el programador de tareas cron del sistema. La salida se redirige a un archivo de log para permitir auditorías posteriores del estado de las copias.

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 88 de 89



## Anexo V – Repositorio de GitHub

El código fuente completo, así como las actualizaciones del proyecto, se encuentran disponibles para su consulta en el repositorio de GitHub creado por mi:

<https://github.com/mohamaamla77/TFG.git>

A screenshot of a GitHub repository page. The top navigation bar shows the repository name "mohamaamla77/TFG" and the URL "https://github.com/mohamaamla77/TFG.git". The repository has 2 commits, updated 9 minutes ago, and 2 forks. The README file is open, showing the project's purpose: "Infraestructura de Red Segura para PYME - TEcnicom". It details the architecture, mentioning pfSense for perimeter security, WireGuard for remote access, PHP/Apache for corporate services, and TrueNAS for centralized storage. It also notes automated backups and a 3-2-1 backup strategy. The repository has no releases or packages published. A sidebar on the right shows the tech stack: PHP 88.5%, CSS 9.5%, HTML 1.8%, and Shell 0.2%. Suggested workflows for Symfony, Laravel, and PHP are listed at the bottom.

Imagen 113 – Repositorio de GitHub

# Servidor Web con Acceso Seguro a través de VPN

Mohammed Maamla Razzak

maamla\_mohammed\_asir

Página 89 de 89



Mohammed Maamla Razzak

Técnico Superior en Administración de Sistemas Informáticos en Red

2025-2026