

2025

IES San Vicente

José Martínez León – José Luis Sánchez Sánchez



[IMPLEMENTACIÓN INTEGRAL DE INFRAESTRUCTURA IT]

Este documento recoge el desarrollo completo de un proyecto de implementación de infraestructura IT para una empresa desde cero. Incluye el diseño de red, la configuración de servicios como DNS, DHCP, Active Directory y herramientas de seguridad como Greenbone y Wazuh, así como la implementación de una base de datos en Docker y una página web corporativa.

Tabla de contenido

| | |
|-----------------------------------------------------------------------------|----|
| 1. Introducción | 2 |
| 2. Antecedentes | 2 |
| 3. Análisis..... | 2 |
| 3.1. Crear una red escalable, organizada por departamentos..... | 3 |
| 3.2. Administrar usuarios mediante Active Directory | 3 |
| 3.3. Asegurar el sistema mediante herramientas como Wazuh y Greenbone | 3 |
| 3.4. Implementar servicios de red: DHCP, DNS, web y base de datos..... | 4 |
| 3.5. Permitir acceso web y gestión de recursos mediante login seguro..... | 4 |
| 3.6. Dividir entornos de red para mejorar la seguridad | 4 |
| 4. Diseño y resultados: | 5 |
| 4.1. Diseño de la red..... | 5 |
| 4.2. Implementación de Active Directory | 7 |
| 4.3. Base de datos en Docker | 12 |
| 4.4. Páginas web corporativas..... | 13 |
| 4.5. Seguridad: Wazuh y Greenbone..... | 15 |
| 5. Plan de Empresa..... | 20 |
| 6. Conclusión | 24 |

1. Introducción

Este proyecto lo hemos desarrollado conjuntamente **José Martínez León** y **José Luis Sánchez Sánchez**, con el objetivo de diseñar e implementar desde cero la infraestructura IT de una empresa simulada. La idea principal ha sido construir una red corporativa funcional, segura y preparada para la gestión de usuarios y recursos, incluyendo tanto la parte de red como los servicios de sistemas.

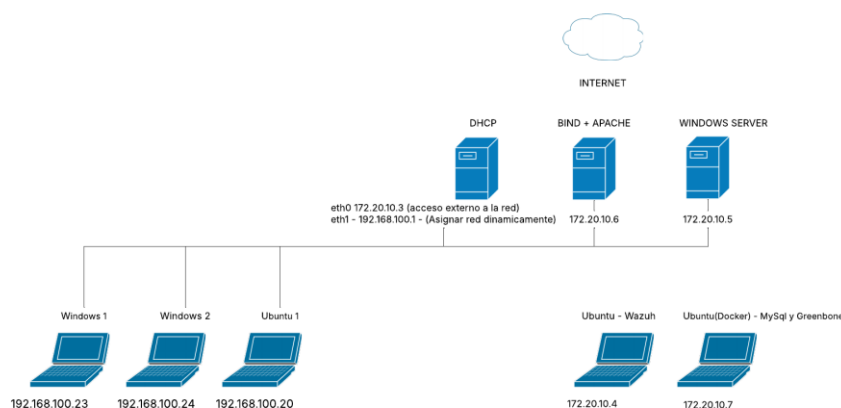
2. Antecedentes

En el contexto actual, una infraestructura IT bien definida y segura es esencial para cualquier empresa. A lo largo de nuestra formación hemos adquirido conocimientos sobre **redes, sistemas operativos, virtualización, servicios web y seguridad**. Este proyecto nos ha permitido integrar esos conocimientos en un entorno práctico, emulando una empresa real.

3. Análisis

Antes de comenzar con la implementación, fue fundamental realizar un análisis de las necesidades tecnológicas que debía cubrir la empresa simulada. El objetivo principal era **diseñar una infraestructura IT completa, segura, escalable y adecuada para el funcionamiento de una organización real**. A partir de esto, se definieron los siguientes puntos clave:

Diagrama de Red



3.1. Crear una red escalable organizada por departamentos

La empresa debía contar con una red que no solo funcionara de manera estable, sino que también pudiera crecer en el futuro sin generar conflictos. Para ello, se diseñó una topología jerárquica con servidores y clientes, en la que se separaron los distintos departamentos mediante subredes, favoreciendo tanto la organización como la seguridad.

3.2. Administrar usuarios mediante Active Directory

La gestión centralizada de usuarios era esencial. Por eso, se decidió implementar **Active Directory en un Windows Server**, permitiendo:

- Crear y administrar **cuentas de usuario**.
- Establecer **Unidades Organizativas** (OUs) por departamento.
- Aplicar **GPOs** (Políticas de Grupo) para configurar automáticamente aspectos del entorno de trabajo (como fondos de escritorio).
- Asignar **políticas de contraseñas** iniciales que luego cada usuario puede personalizar.

3.3. Asegurar el sistema mediante herramientas como Wazuh y Greenbone

Para proteger la red, se integraron herramientas de análisis y monitorización de seguridad:

- **Greenbone** permite detectar vulnerabilidades como puertos abiertos, servicios obsoletos o configuraciones inseguras. Es útil para hacer auditorías periódicas a las máquinas de la red.
- **Wazuh** monitorea comportamientos sospechosos como accesos fallidos, cambios en archivos o intentos de fuerza bruta vía RDP, permitiendo reaccionar ante amenazas en tiempo real.

3.4. Implementar servicios de red: DHCP, DNS, web y base de datos

Se analizaron los servicios fundamentales para el funcionamiento de la empresa:

- **DHCP**: configurado para asignar direcciones IP automáticamente a los clientes, organizando por rango y evitando conflictos.
- **DNS (BIND9)**: para traducir nombres de dominio como marlutech.com y portal.marlutech.com, facilitando la navegación interna sin depender de IPs.
- **Web interna y externa**: página corporativa visible desde la red interna y portal exclusivo para empleados.
- **Base de datos en Docker**: donde se almacenan credenciales y datos de los empleados. Modular y portátil.

3.5. Permitir acceso web y gestión de recursos mediante login seguro

Se desarrolló una página interna con sistema de **login** que autentica a los empleados. El acceso a servicios (como eventos o recursos) se gestiona de forma segura a través de una **base de datos protegida**, aislada en un contenedor **Docker**. Esto permite tener un sistema de validación robusto y centralizado.

3.6. Dividir entornos de red para mejorar la seguridad

Como medida adicional, se implementó una segmentación de red, **separando el entorno de servidores** (como AD y DNS) del de los clientes. Esto ayuda a:

- Limitar el acceso directo a recursos críticos.
- Aumentar la resistencia ante ataques internos.
- Aislar servicios sensibles (como bases de datos) de accesos no autorizados.

4. Diseño y resultados:

4.1. Diseño de la red

Comenzamos el proyecto diseñando la topología de red y planificando los elementos que íbamos a necesitar: servidores, routers, switches y equipos cliente. Para facilitar la administración y asegurar la escalabilidad, definimos un esquema de direccionamiento IP bien organizado.

Para la asignación de direcciones IP configuramos un **servidor DHCP**, el cual distribuye las IPs de forma dinámica a los dispositivos conectados a la red (en este caso a los clientes). Esto nos ha permitido automatizar la gestión de direcciones y garantizar que no haya conflictos. También mejora la seguridad ya que los servidores que hemos usado para asignar red, el servidor de Active Directory... están en otra red.

En cuanto a la resolución de nombres, instalamos y configuramos un **servidor BIND9** como servidor DNS. Con él, pudimos crear zonas directas e inversas, permitiendo a los usuarios acceder a recursos internos, como la página web corporativa (marlute.com - portal.marlute.com), mediante nombres de dominio personalizados en lugar de tener que recordar direcciones IP.

Configuración inicial de BIND9

```

GNU nano 4.8 /etc/bind/db.marlute.com
;
; STTL 604800
; IN SOA marlute.com. root.marlute.com. (
;      2      ; Serial
;      604800 ; Refresh
;      86400  ; Retry
;      2419200 ; Expire
;      604800 ) ; Negative Cache TTL
;
; @ IN NS localhost.
; @ IN A 127.0.0.1
; @ IN AAAA ::1
server IN A 10.30.0.1
portal IN A 10.30.0.1

```

```

Josemartinez@Josemartinez-VirtualBox: ~
Josemartinez@Josemartinez-VirtualBox: $ ping server.marlute.com
PING server.marlute.com (10.30.0.1) 56(84) bytes of data:
64 bytes from 10.30.0.1 (10.30.0.1): icmp_seq=1 ttl=64 time=0.701 ms
64 bytes from 10.30.0.1 (10.30.0.1): icmp_seq=2 ttl=64 time=1.10 ms

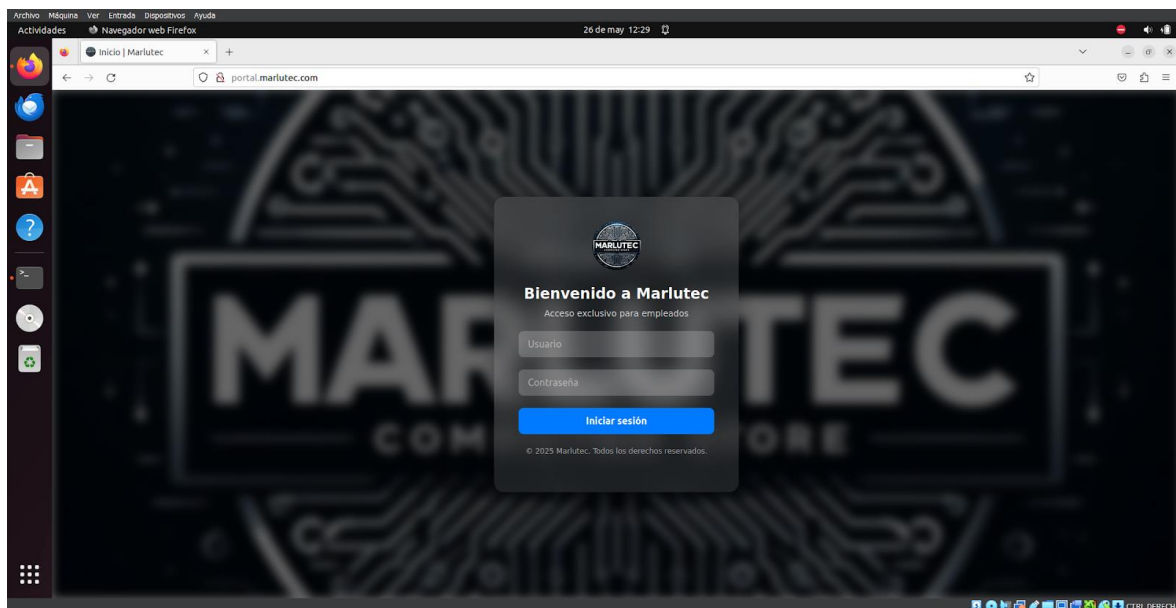
--- server.marlute.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.701/0.902/1.104/0.201 ms
Josemartinez@Josemartinez-VirtualBox: $

```

```

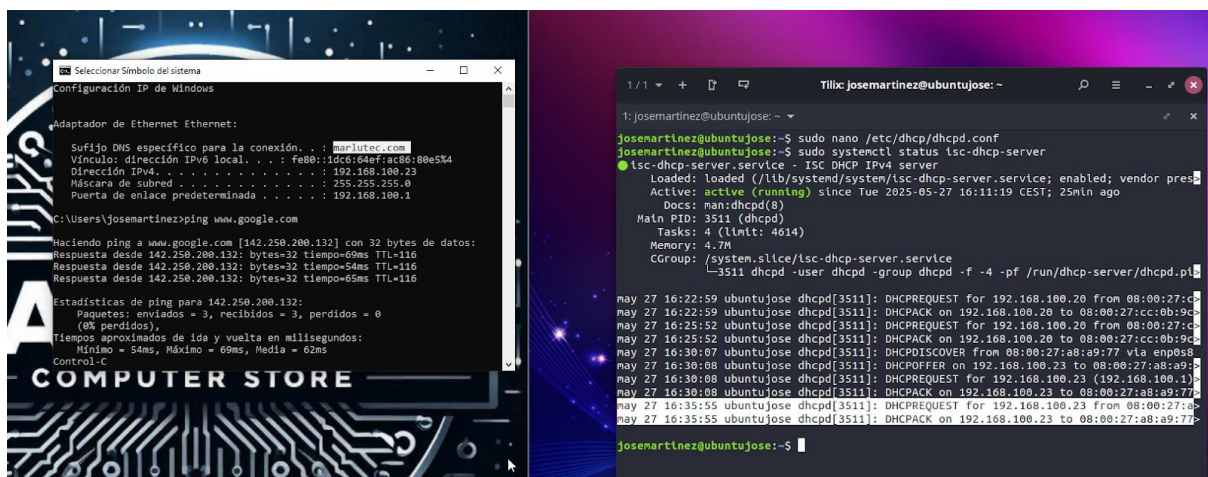
GNU nano 4.8 /etc/bind/named.conf.local
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
// Directa marlute.com
zone "marlute.com"{
    type master;
    file "/etc/bind/db.marlute.com";
    allow-transfer { 10.30.0.2; };
    also-notify { 10.30.0.2; };
};
// Inversa
zone "30.10.in-addr.arpa"{
    type master;
    file "/etc/bind/db.10.30.0.0.rev";
};

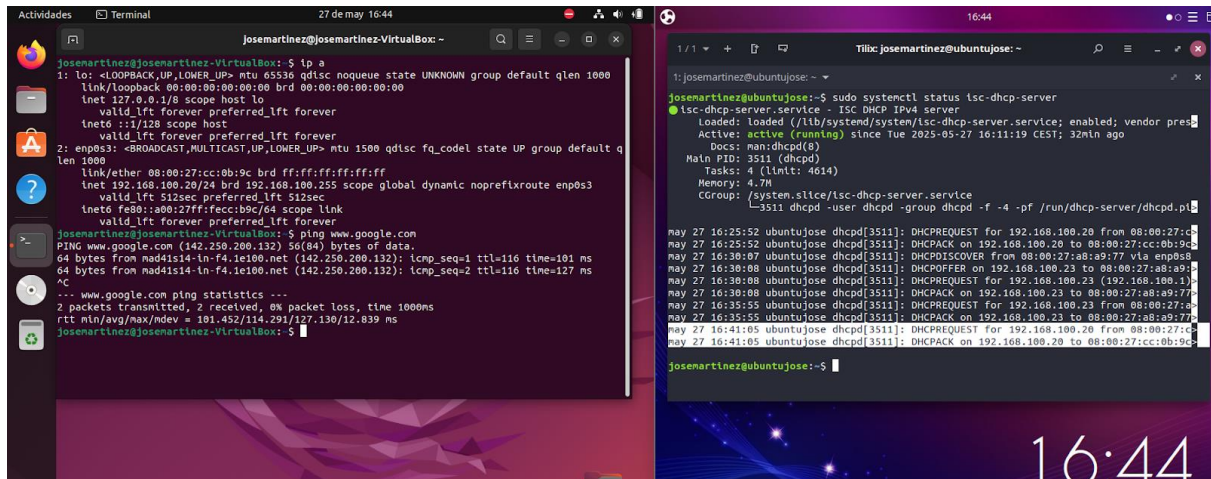
```


Resolución de nombres al buscar la web corporativa.**DHCP.**

Montamos esta red en una rama separada, para que los clientes estén aislados del resto (por ejemplo, del servidor de Active Directory). Así ganamos en seguridad, porque si un cliente se infecta o hay algún problema, no afecta directamente a los servidores principales. Además, nos permite tener todo más organizado y preparado por si en el futuro la empresa crece.

```
# Configuración de la subred
subnet 192.168.100.0 netmask 255.255.255.0 {
    range 192.168.100.20 192.168.100.100;
    option routers 192.168.100.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
}
```

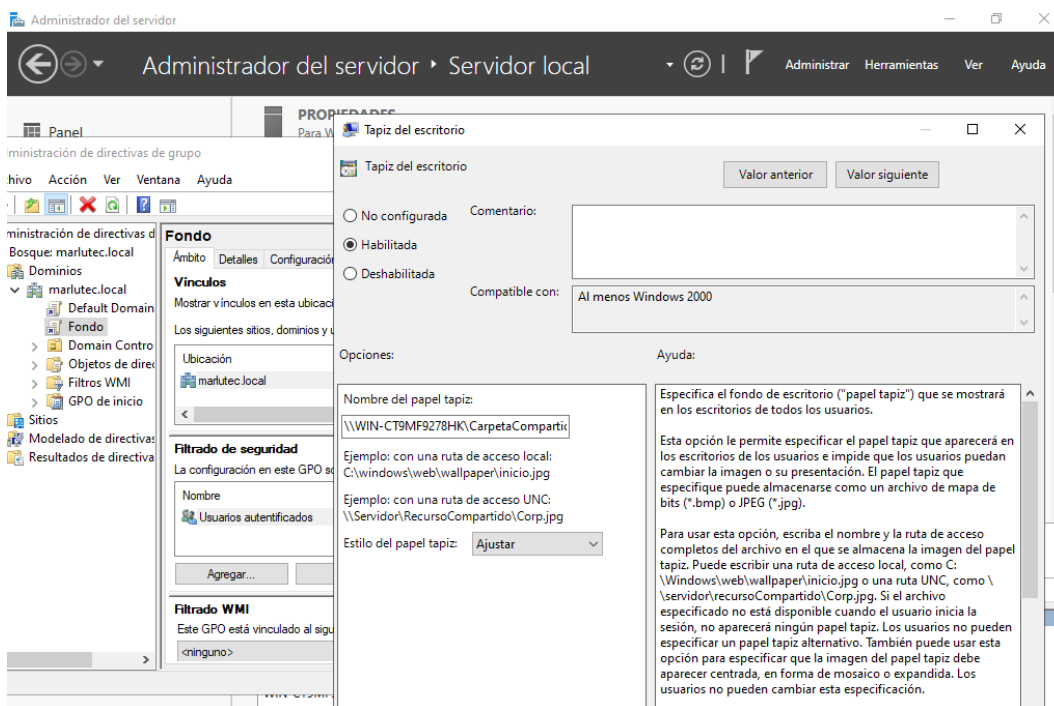
Clientes Windows y Ubuntu de los empleados funcionando.

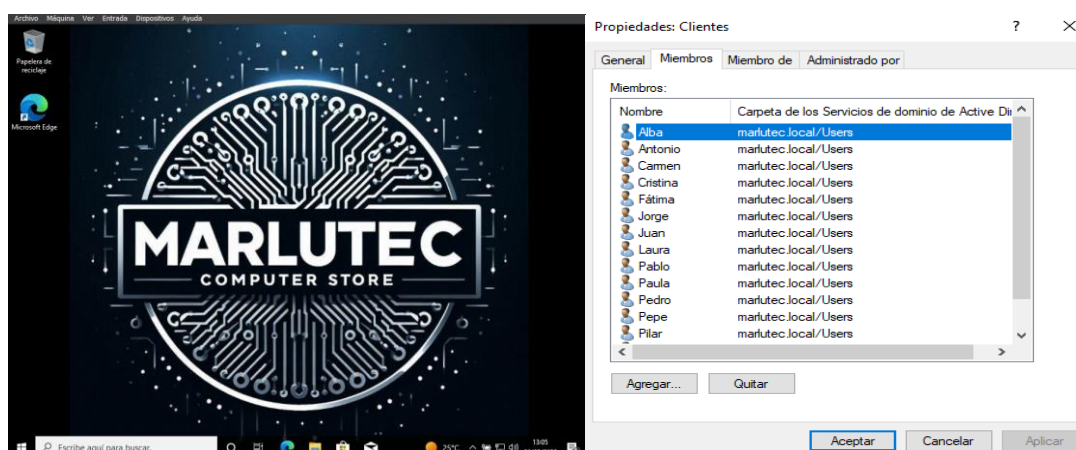
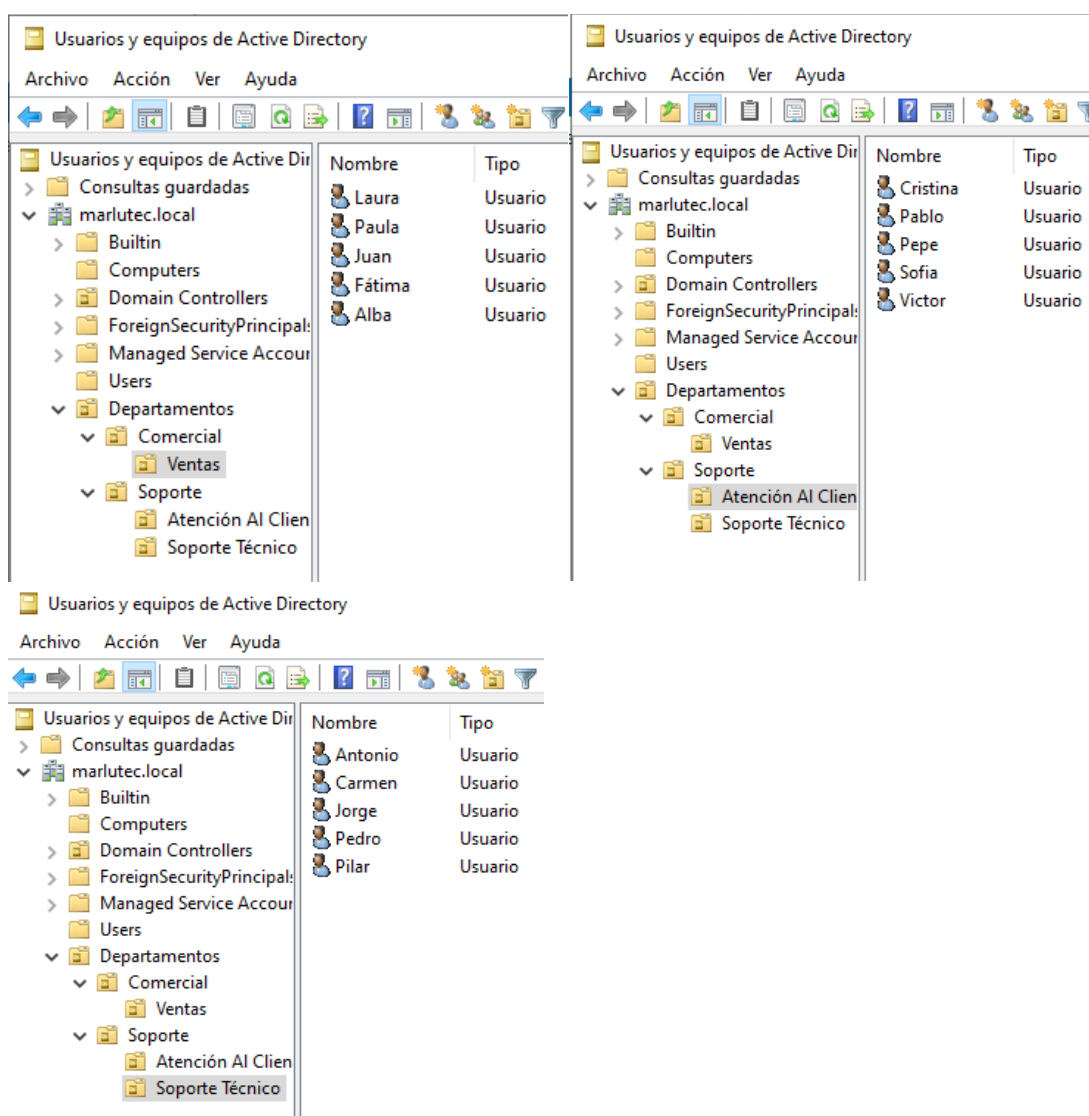


4.2. Implementación de Active Directory

Después, instalamos un servidor **Windows Server** y lo promovimos como Controlador de Dominio. Desde aquí, configuramos el Active Directory para gestionar a todos los usuarios de la empresa. Creamos diferentes unidades organizativas (OUs) para separar departamentos, definimos cuentas de usuario, y políticas de grupo (GPOs) para controlar el entorno de trabajo (fondos personalizados), etc.

GPO creada para el fondo personalizado



Fondo personalizado y clientes:**Unidades Organizativas con los Departamentos correspondientes.**

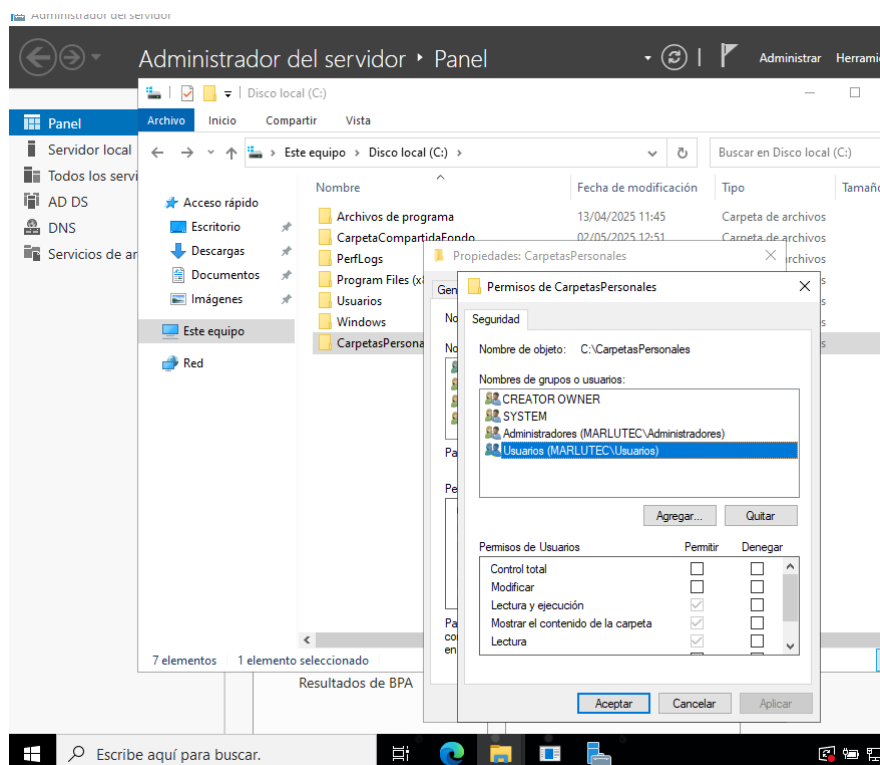
Política de contraseñas:

Hemos configurado para que la primera contraseña sea Admin123 y luego cada usuario por privacidad se ponga la contraseña que él quiera.

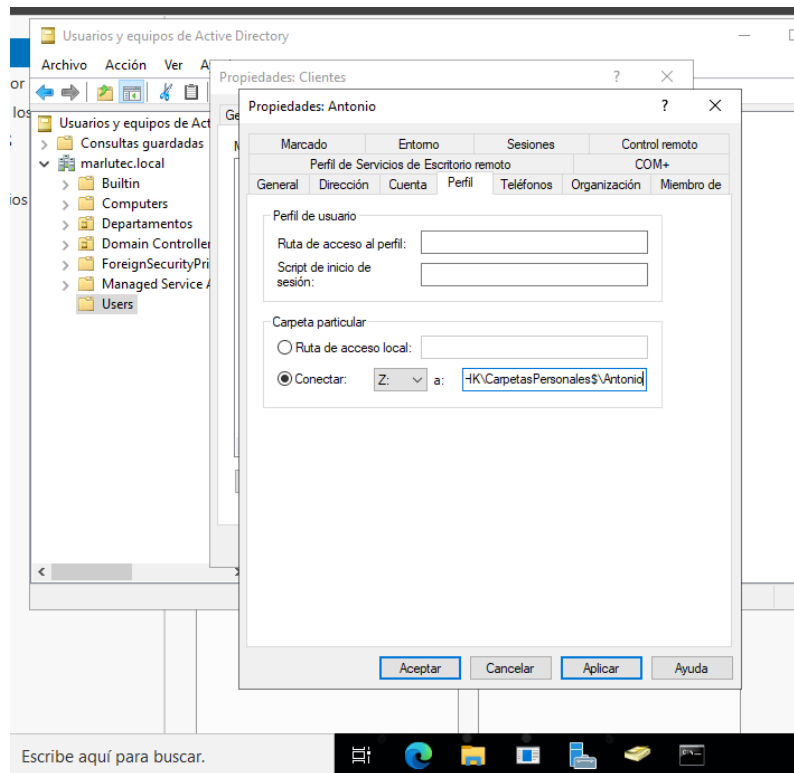


Carpetas personales

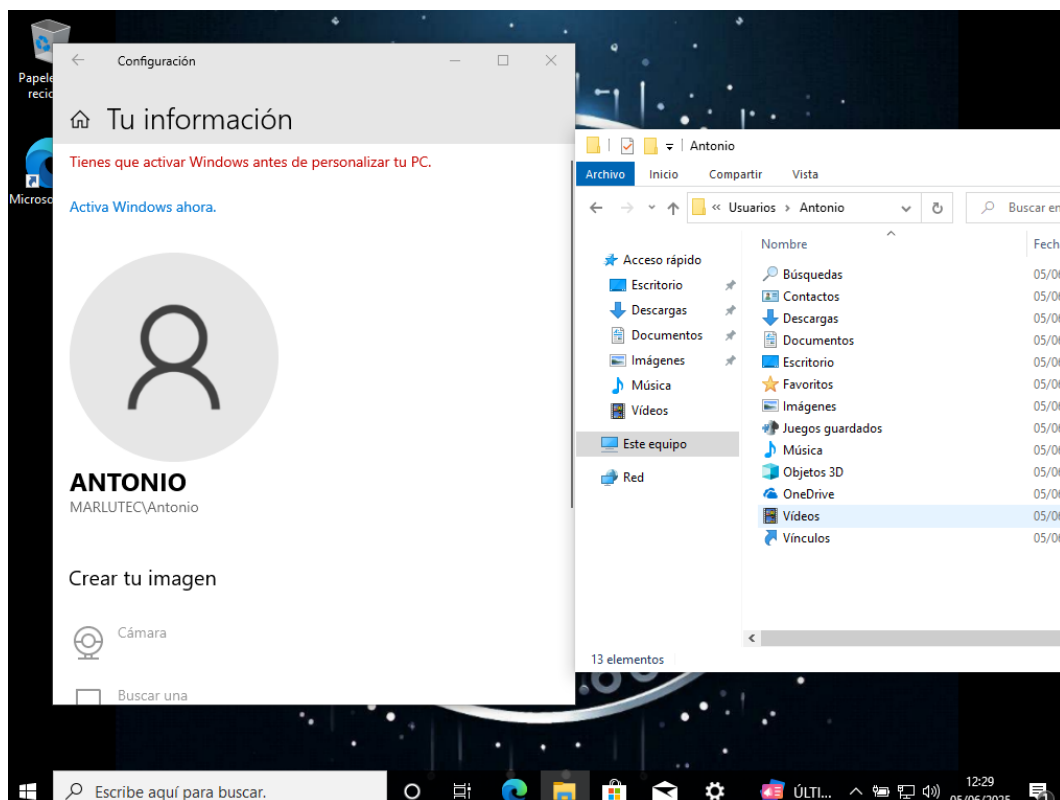
Creamos una carpeta en el disco local C y la compartimos con los siguientes permisos:



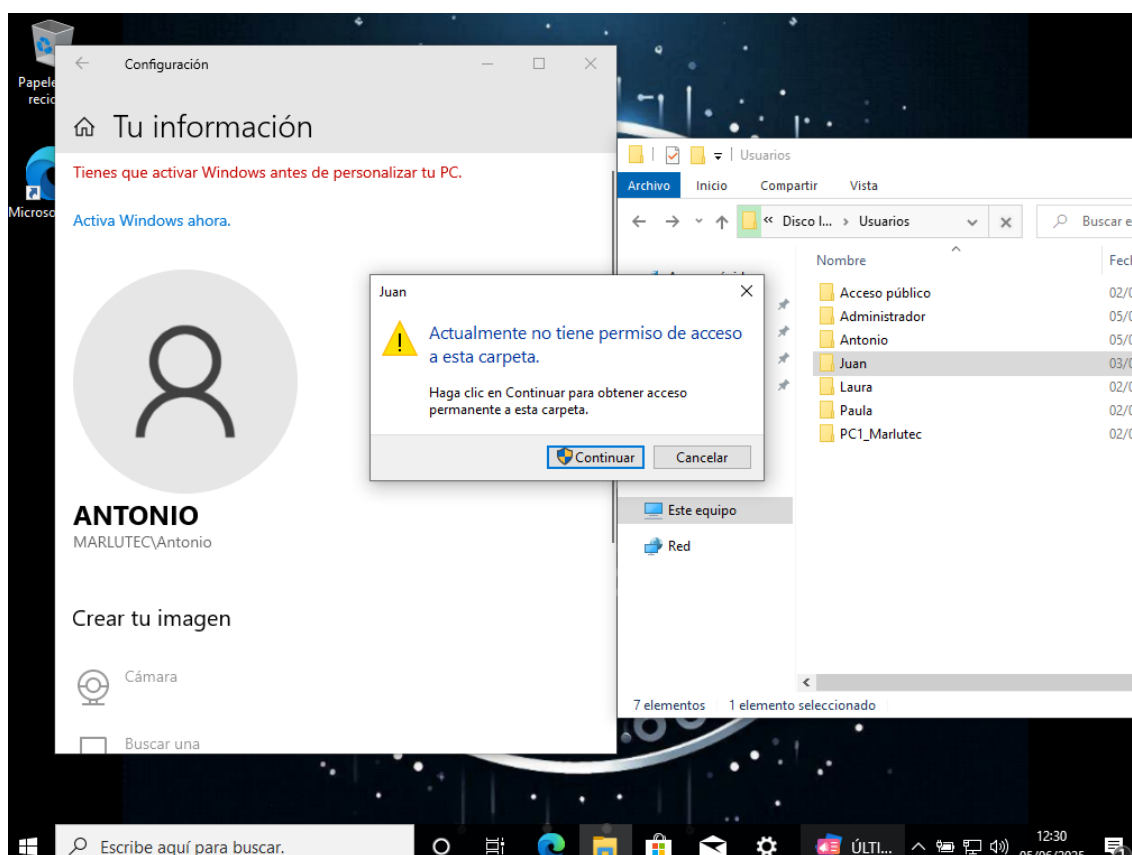
Nos vamos al perfil de cada uno y asignamos la ruta de la carpeta personal que hemos creado anteriormente con su nombre de usuario. (El \$ lo oculta en la red)



Accedemos en el cliente con Antonio y observamos como tiene acceso a su directorio con su nombre:



En cambio si nos intentamos meter a el directorio de otro usuario no nos dejará ya que por privacidad cada trabajador tendra acceso únicamente a su carpeta.



4.3. Base de datos en Docker

Como parte del soporte a procesos internos de la empresa (acceso a la página corporativa de usuarios clientes portal.marlutec.com), montamos una **base de datos MySQL** utilizando **Docker**. En ella registramos la información de los empleados y sus contraseñas para el login. Aprendimos a crear contenedores, gestionar volúmenes y conectar aplicaciones a la base de datos, todo de forma modular y portable.

```

pruebas@pruebas-VirtualBox: ~$ sudo docker ps -a
[sudo] contraseña para pruebas:
CONTAINER ID   IMAGE      COMMAND                  CREATED        STATUS      PORTS
3bba73410918   mysql:5.7   "docker-entrypoint.s..." 6 weeks ago   Exited (255) About a minute
ago           0.0.0.0:3306->3306/tcp, [::]:3306->3306/tcp, 33060/tcp   marlutec
ca03e2deb00b   mysql:5.7   "docker-entrypoint.s..." 6 weeks ago   Exited (1) 6 weeks ago
vigorous_robinson
15a8c46c8bb9   mysql:latest "docker-entrypoint.s..." 6 weeks ago   Exited (1) 6 weeks ago
jolly_allen
bec229f5ecde   mysql:latest "docker-entrypoint.s..." 6 weeks ago   Exited (0) 6 weeks ago
bec229f5ecde_mysql-container
9c4b96837f4b   hello-world "/hello"                 6 weeks ago   Exited (0) 6 weeks ago
happy_kalam

pruebas@pruebas-VirtualBox:~$ sudo docker start marlutec
marlutec
pruebas@pruebas-VirtualBox:~$
pruebas@pruebas-VirtualBox:~$ sudo docker ps
CONTAINER ID   IMAGE      COMMAND                  NAMES          CREATED        STATUS      PORTS
3bba73410918   mysql:5.7   "docker-entrypoint.s..." 6 weeks ago   Up 9 seconds   0.0.0.0:3306->3306/tcp, [::]:3306->3306/tcp, 33060/tcp   marlutec
pruebas@pruebas-VirtualBox:~$ sudo docker exec -it marlutec mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.44 MySQL Community Server (GPL)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql>
  
```

Base de datos en docker con usuarios almacenados.

```

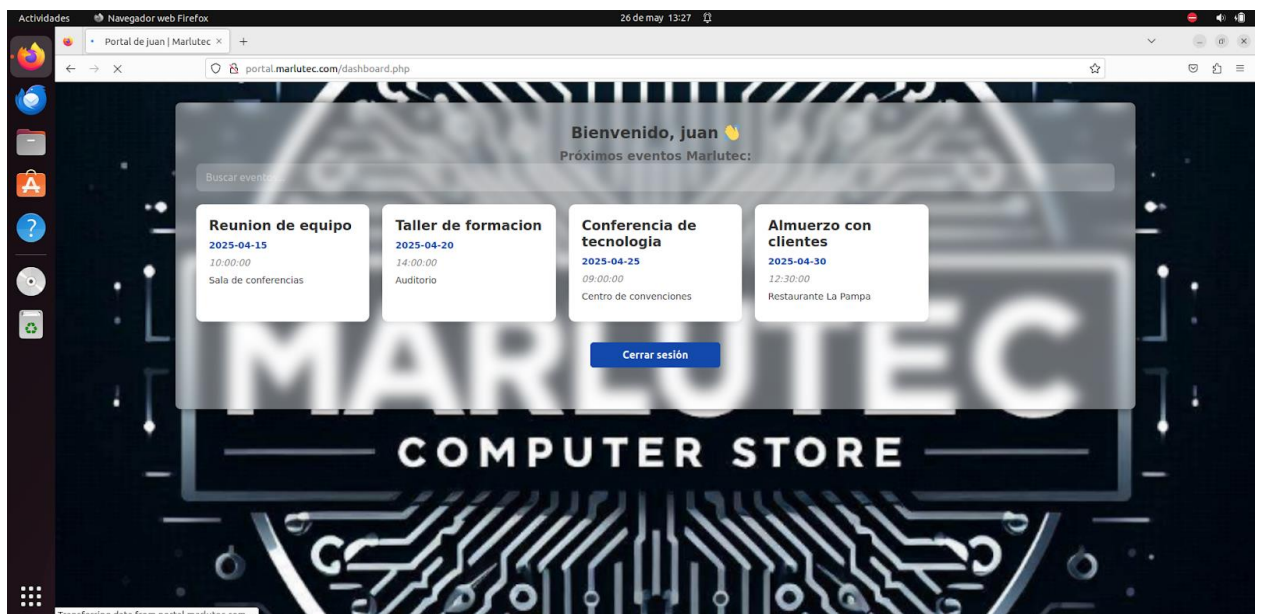
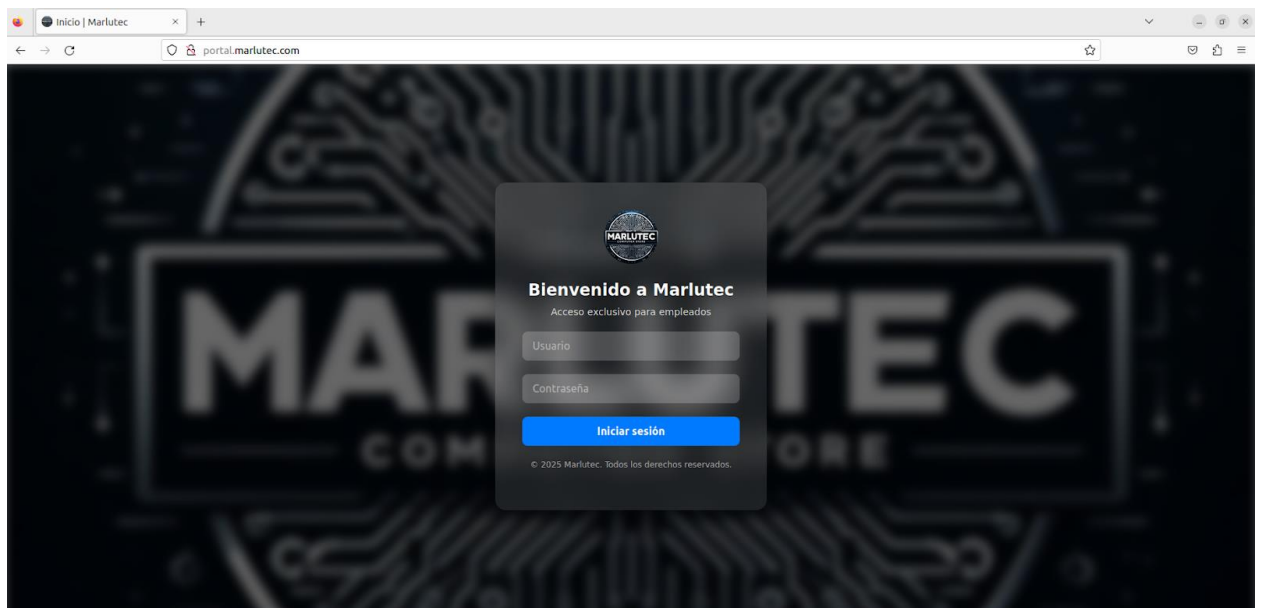
mysql> USE marlutec;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SELECT * FROM usuarios;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | juan     | 1234     |
+----+-----+-----+
1 row in set (0.00 sec)
  
```

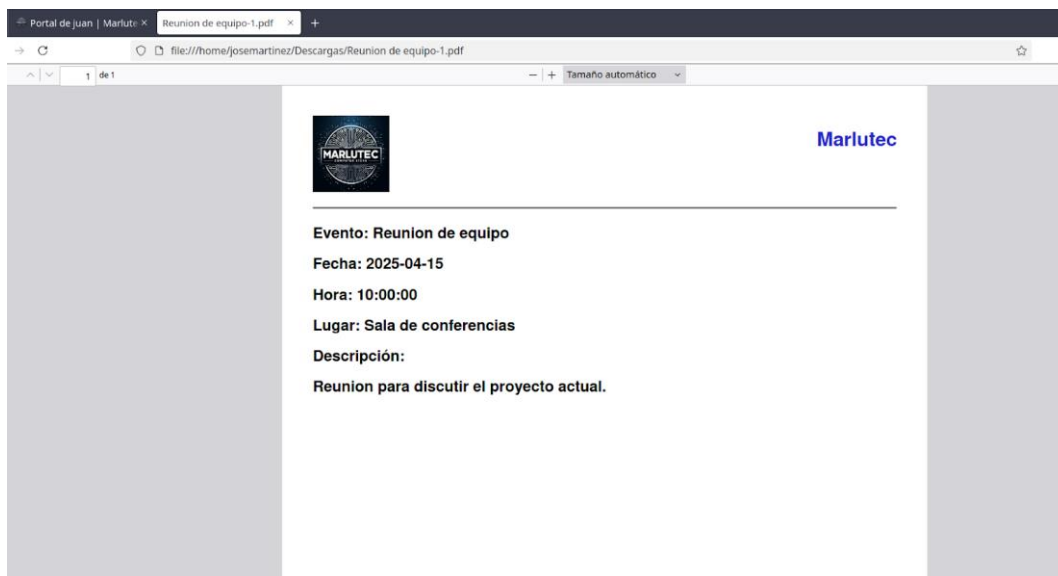
4.4. Páginas web corporativas

Finalmente, desarrollamos una **página web corporativa** para presentar la empresa. Esta página está alojada en un servidor web interno y es accesible a través del nombre de dominio que configuramos en el DNS (Domain Name System). La web incluye información básica sobre la empresa, servicios y contacto. También hemos hecho una página exclusiva para trabajadores llamada `portal.marlutec.com` vinculada también en el servidor BIND, en esta página accederán a través de un login con la base de datos almacenada vista en Docker anteriormente.

Página exclusiva usuarios (trabajadores):



Al pulsar un evento se descargará un recordatorio personalizado.



conexion.php

```

Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
12:35
conexion.php
/var/www/portal.marlutec.com

1 <?php
2
3 $host = '172.20.10.7'; // Direccion IP de la maquina Docker
4 $dbname = 'marlutec';
5 $username_db = 'root'
6 $password_db = 'admin123';
7
8
9 try {
10     $pdo = new PDO("mysql:host=$host;dbname=$dbname", $username_db, $password_db);
11     $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
12 } catch (PDOException $e) {
13     echo 'Error al conectar a la base de datos: ' . $e->getMessage();
14     exit();
15 }
16 }
17 ?>

```

Página web de acceso global

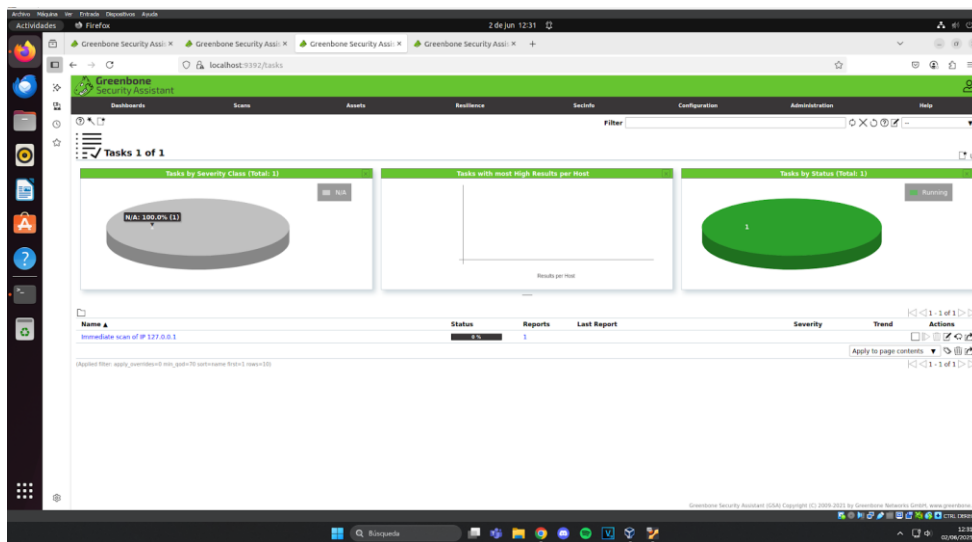


4.5. Seguridad: Wazuh y Greenbone

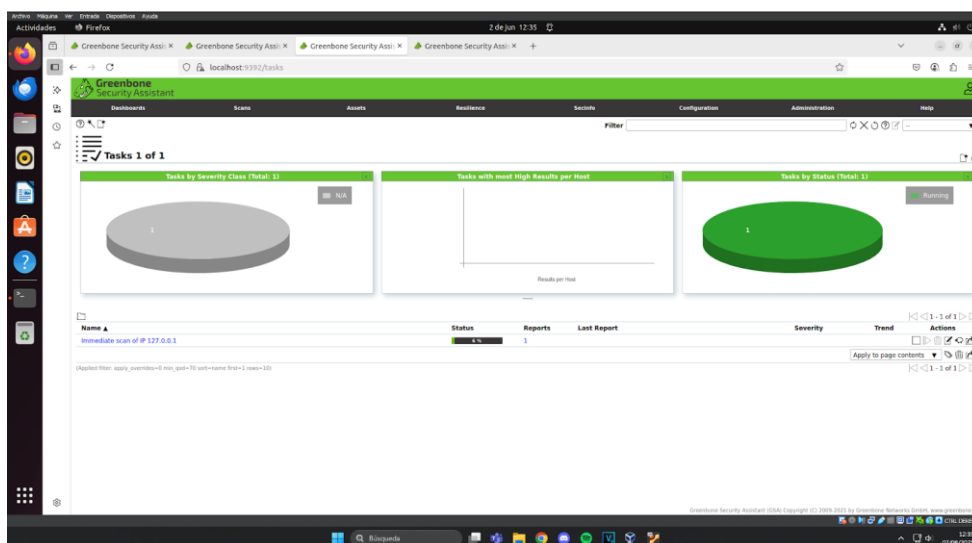
La parte de seguridad fue clave en el proyecto

En este proyecto usamos **Greenbone**, una herramienta que funciona desde el navegador y que sirve para buscar posibles fallos de seguridad en ordenadores que están dentro de una misma red. Lo que hace Greenbone es escanear esos equipos y comprobar si hay cosas mal configuradas o si se está usando software desactualizado. También puede detectar si hay puertos abiertos que no se deberían usar o si hay formas conocidas de atacar ese sistema que ya han sido publicadas. Para hacerlo más fácil y rápido, hemos montado Greenbone usando Docker, lo que nos permite tenerlo funcionando sin necesidad de instalarlo directamente en el sistema. De esta manera podemos ver qué tan seguro está un equipo y qué cosas habría que cambiar o mejorar para protegerlo mejor. El objetivo es realizar escaneos a los ordenadores de los trabajadores para chequear que no sean un punto de ataque.

- Comienzo de un escaneo a una máquina de prueba:



- Avance del escaneo:



Escaneo finalizado:

Tras realizar un escaneo a la máquina local con **Greenbone**, se han detectado varias vulnerabilidades de alta severidad. Una de las más críticas es el uso de credenciales por defecto en Greenbone, lo que supone un gran riesgo si alguien externo accede a la interfaz. También se ha encontrado que el servicio de PostgreSQL permite autenticación sin contraseña, lo cual facilita el acceso no autorizado a la base de datos.

Además, se ha detectado que algunos componentes del sistema están obsoletos (fin de vida útil), lo que significa que ya no reciben actualizaciones de seguridad. Esto aumenta las probabilidades de que existan fallos que puedan ser aprovechados por atacantes. También aparece un aviso relacionado con un certificado SSL no confiable, que podría hacer que las conexiones cifradas no sean completamente seguras.

Este tipo de hallazgos demuestra que el sistema analizado tiene varias puertas abiertas que podrían ser aprovechadas, y que usar Greenbone es útil para identificar estos puntos débiles antes de que sean explotados.

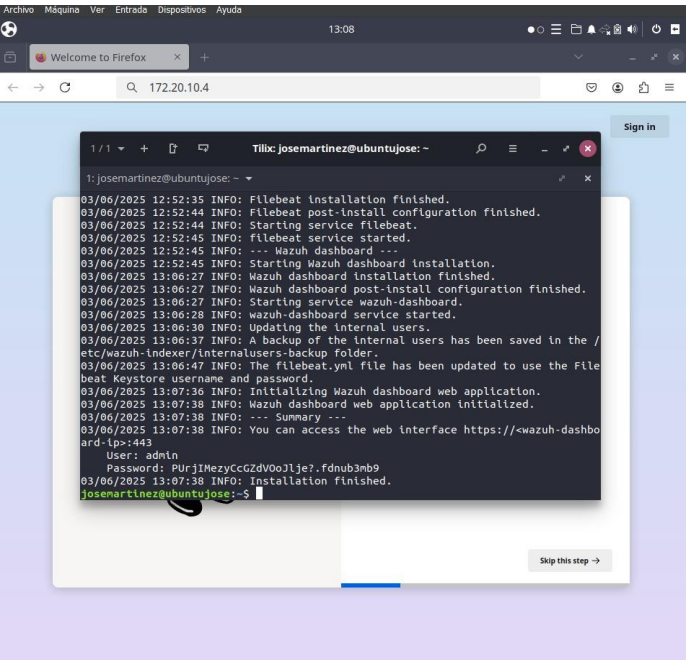
Report: Mon, Jun 2, 2025 8:26 AM UTC

| Information | Results (5 of 48) | Hosts (1 of 1) | Ports (2 of 4) | Applications (5 of 5) | Operating Systems (1 of 1) | CVEs (0 of 0) | Closed CVEs (0 of 0) | TLS Certificates (1 of 1) | Error Messages (0 of 0) | User Tags (0) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|----------------|----------------|-----------------------|----------------------------|-------------------------------|----------------------|---------------------------|-------------------------|---------------|---------------|----------|-----|---------|------|----------|---------|---------------------------------------------------------------|-------------|------|-----------|-----------|----------|-------------------------------|----------------------------------------------------------------------------------------|-------------|-------|-----------|-----------|----------|-------------------------------|----------------------------------------------------------------|-------------|------|-----------|-----------|----------|-------------------------------|-----------------------------------------------------------------|-------------|------|-----------|-----------|-------------|-------------------------------|---------------------------------------------------------------------------|--------------|------|-----------|-----------|----------|-------------------------------|
| <table border="1"> <thead> <tr> <th>Vulnerability</th> <th>Severity</th> <th>QoD</th> <th>Host IP</th> <th>Name</th> <th>Location</th> <th>Created</th> </tr> </thead> <tbody> <tr> <td>PostgreSQL Trust Authentication Enabled (PostgreSQL Protocol)</td> <td>10.0 (High)</td> <td>99 %</td> <td>127.0.0.1</td> <td>localhost</td> <td>5432/tcp</td> <td>Mon, Jun 2, 2025 10:48 AM UTC</td> </tr> <tr> <td>OpenVAS / Greenbone Vulnerability Manager (GVM) Default Credentials (OMF/GMP Protocol)</td> <td>10.0 (High)</td> <td>100 %</td> <td>127.0.0.1</td> <td>localhost</td> <td>9390/tcp</td> <td>Mon, Jun 2, 2025 10:49 AM UTC</td> </tr> <tr> <td>OpenVAS Framework / GVM Components End of Life (EOL) Detection</td> <td>10.0 (High)</td> <td>80 %</td> <td>127.0.0.1</td> <td>localhost</td> <td>9390/tcp</td> <td>Mon, Jun 2, 2025 10:44 AM UTC</td> </tr> <tr> <td>Report outdated / end-of-life Scan Engine / Environment (local)</td> <td>10.0 (High)</td> <td>97 %</td> <td>127.0.0.1</td> <td>localhost</td> <td>general/tcp</td> <td>Mon, Jun 2, 2025 10:31 AM UTC</td> </tr> <tr> <td>SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection</td> <td>5.0 (Medium)</td> <td>99 %</td> <td>127.0.0.1</td> <td>localhost</td> <td>9390/tcp</td> <td>Mon, Jun 2, 2025 10:45 AM UTC</td> </tr> </tbody> </table> | | | | | | | | | | | Vulnerability | Severity | QoD | Host IP | Name | Location | Created | PostgreSQL Trust Authentication Enabled (PostgreSQL Protocol) | 10.0 (High) | 99 % | 127.0.0.1 | localhost | 5432/tcp | Mon, Jun 2, 2025 10:48 AM UTC | OpenVAS / Greenbone Vulnerability Manager (GVM) Default Credentials (OMF/GMP Protocol) | 10.0 (High) | 100 % | 127.0.0.1 | localhost | 9390/tcp | Mon, Jun 2, 2025 10:49 AM UTC | OpenVAS Framework / GVM Components End of Life (EOL) Detection | 10.0 (High) | 80 % | 127.0.0.1 | localhost | 9390/tcp | Mon, Jun 2, 2025 10:44 AM UTC | Report outdated / end-of-life Scan Engine / Environment (local) | 10.0 (High) | 97 % | 127.0.0.1 | localhost | general/tcp | Mon, Jun 2, 2025 10:31 AM UTC | SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection | 5.0 (Medium) | 99 % | 127.0.0.1 | localhost | 9390/tcp | Mon, Jun 2, 2025 10:45 AM UTC |
| Vulnerability | Severity | QoD | Host IP | Name | Location | Created | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PostgreSQL Trust Authentication Enabled (PostgreSQL Protocol) | 10.0 (High) | 99 % | 127.0.0.1 | localhost | 5432/tcp | Mon, Jun 2, 2025 10:48 AM UTC | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OpenVAS / Greenbone Vulnerability Manager (GVM) Default Credentials (OMF/GMP Protocol) | 10.0 (High) | 100 % | 127.0.0.1 | localhost | 9390/tcp | Mon, Jun 2, 2025 10:49 AM UTC | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OpenVAS Framework / GVM Components End of Life (EOL) Detection | 10.0 (High) | 80 % | 127.0.0.1 | localhost | 9390/tcp | Mon, Jun 2, 2025 10:44 AM UTC | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Report outdated / end-of-life Scan Engine / Environment (local) | 10.0 (High) | 97 % | 127.0.0.1 | localhost | general/tcp | Mon, Jun 2, 2025 10:31 AM UTC | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection | 5.0 (Medium) | 99 % | 127.0.0.1 | localhost | 9390/tcp | Mon, Jun 2, 2025 10:45 AM UTC | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Applied filter: apply_overrides=0 level=html rows=100 min_age=70 first=1 sort=reverse=severity

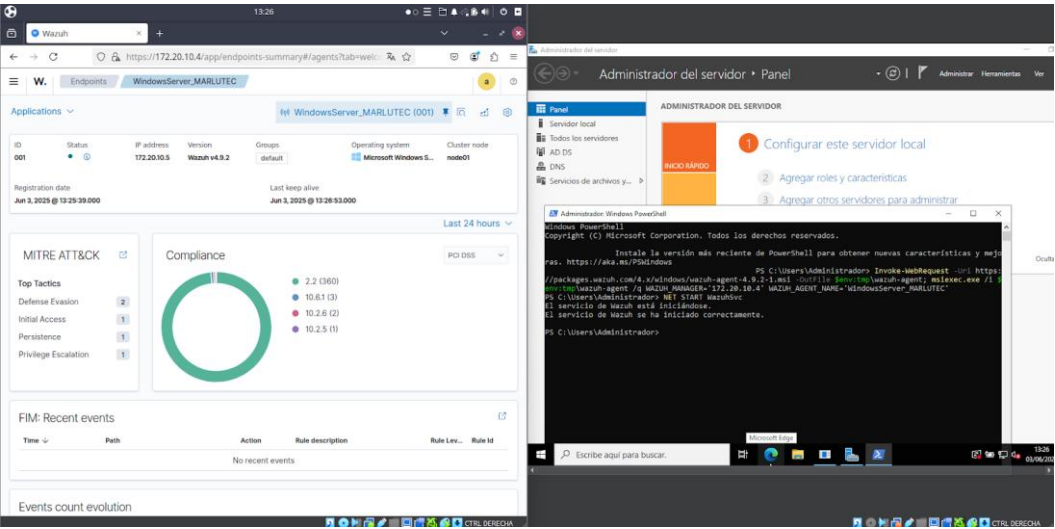
También usamos **Wazuh**, que es una herramienta que sirve para vigilar lo que pasa dentro de los ordenadores y detectar cosas raras o peligrosas. Básicamente, Wazuh se instala en una máquina y empieza a revisar todo lo que ocurre como los inicios de sesión, los cambios en archivos importantes o si alguien intenta hacer algo que no debería. Toda esa información se manda a un panel central donde se puede ver todo en tiempo real y saber si hay algo sospechoso. Gracias a esto se puede detectar si alguien está intentando atacar el sistema o si hay algo mal configurado que pueda ser un riesgo para la seguridad.

Lo instalamos directamente en terminal:



```
1/1 + + + Tilix: josemartinez@ubuntu: ~
1: josemartinez@ubuntu: ~
03/06/2025 12:52:35 INFO: Filebeat installation finished.
03/06/2025 12:52:44 INFO: Filebeat post-install configuration finished.
03/06/2025 12:52:44 INFO: Starting service filebeat.
03/06/2025 12:52:45 INFO: filebeat service started.
03/06/2025 12:52:45 INFO: --- Wazuh dashboard ---
03/06/2025 12:52:45 INFO: Starting Wazuh dashboard installation.
03/06/2025 13:06:27 INFO: Wazuh dashboard installation finished.
03/06/2025 13:06:27 INFO: Wazuh dashboard post-install configuration finished.
03/06/2025 13:06:27 INFO: Starting service wazuh-dashboard.
03/06/2025 13:06:28 INFO: wazuh-dashboard service started.
03/06/2025 13:06:30 INFO: Updating the internal users.
03/06/2025 13:06:37 INFO: A backup of the internal users has been saved in the /
etc/wazuh-indexer/internalusers-backup folder.
03/06/2025 13:06:47 INFO: The filebeat.yml file has been updated to use the File
beat Keystore username and password.
03/06/2025 13:07:36 INFO: Initializing Wazuh dashboard web application.
03/06/2025 13:07:38 INFO: Wazuh dashboard web application initialized.
03/06/2025 13:07:38 INFO: --- Summary ---
03/06/2025 13:07:38 INFO: You can access the web interface https://wazuh-dashbo
ard-tp-443
User: admin
Password: PURjIMezyCcGZdV0oJlJe7.fdnub3nb9
03/06/2025 13:07:38 INFO: Installation finished.
josemartinez@ubuntu:~$
```

Añadimos el agente que en este caso es el **Windows Server de MARLUTEC**.



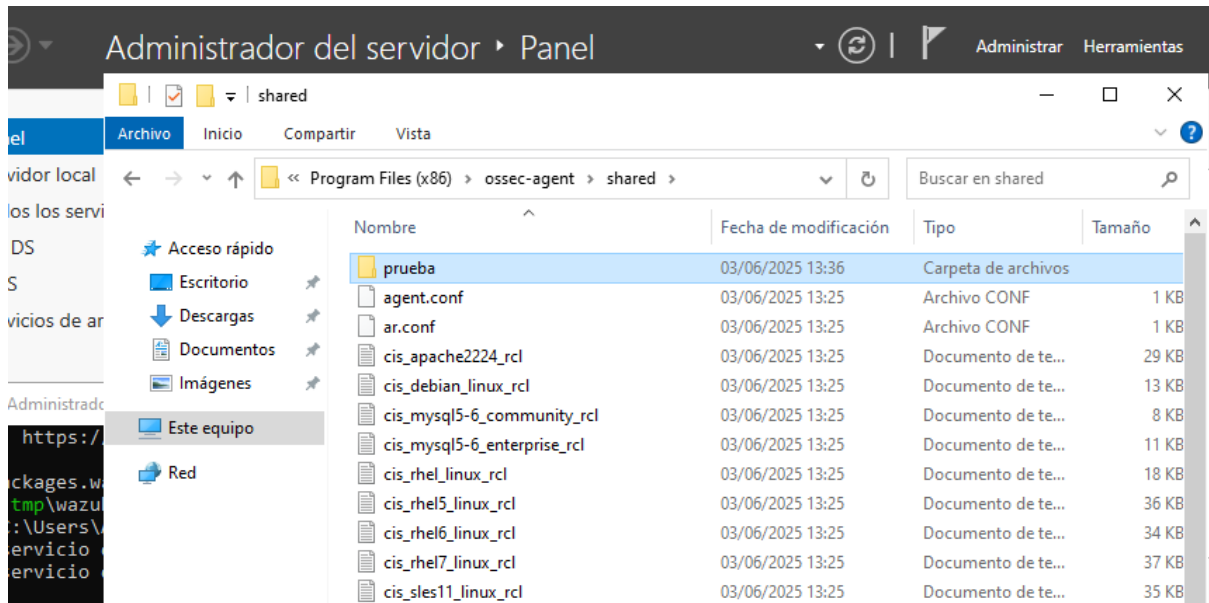
SCA: Lastest scans

CIS Microsoft Windows Server 2022 Benchmark v2.0.0 cis_win2022

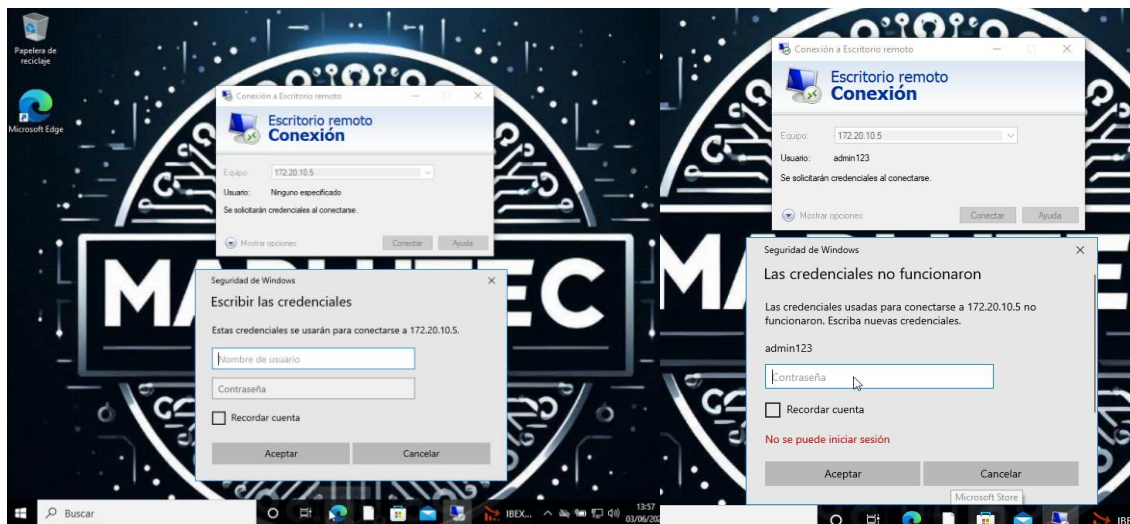
| Policy | End scan | Passed | Failed | Not applic... | Score |
|----------------------------------------------------|----------------------------|--------|--------|---------------|-------|
| CIS Microsoft Windows Server 2022 Benchmark v2.0.0 | Jun 3, 2025 @ 13:26:10.000 | 113 | 246 | 0 | 31% |

< 1 >

Probamos a crear un archivo y a borrarlo para que nos salga en Wazuh



Probamos a intentar acceder por RDP al servidor Windows Server por fuerza bruta para que nos muestre la alerta en Wazuh.



Esto de aquí es probable que sea una alerta de que estamos intentando acceder por RDP pero no podemos entrar ya que la contraseña que ponemos es incorrecta para simular un ataque.

The screenshot displays the Wazuh configuration assessment interface in a web browser. The URL is [https://172.20.10.4/app/configuration-assessment/#/overview?tab=sca&redirectPolicy=cis_win2022&agentId=001&g=\(filters:0\),refreshInterval\(pause:0,value:0\),time:\(from:now-24h\)](https://172.20.10.4/app/configuration-assessment/#/overview?tab=sca&redirectPolicy=cis_win2022&agentId=001&g=(filters:0),refreshInterval(pause:0,value:0),time:(from:now-24h)). The interface shows a list of configuration checks for a Windows Server. The selected check is 27322, titled 'Ensure 'Require use of specific security layer for remote (RDP) connections' is s...'. The check is marked as 'Failed'. The details for this check are as follows:

- Rationale:** The native Remote Desktop Protocol (RDP) encryption is now considered a weak protocol, so enforcing the use of stronger Transport Layer Security (TLS) encryption for all RDP communications between clients and RD Session Host servers is preferred.
- Remediation:** To establish the recommended configuration via GP, set the following UI path to Enabled: SSL: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require use of specific security layer for remote (RDP) connections Note: This Group Policy path is provided by the Group Policy template TerminalServer.admx/adml that is included with all versions of the Microsoft Windows Administrative Templates.
- Description:** This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections. The recommended state for this setting is: Enabled: SSL. Note: In spite of this setting being labeled SSL, it is actually enforcing Transport Layer Security (TLS) version 1.0, not the older (and less secure) SSL protocol.
- Checks (Condition: all):**
 - r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
 - r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services → SecurityLayer
 - r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services → SecurityLayer → 2
- Compliance:**
 - cis: 18.10.57.3.9.3
 - cis_csc_v8: 3.10
 - cmmc_v2.0: AC-L2-3.1.13, AC-L2-3.1.17, JAL2-3.5.10, SC-L2-3.13.11, SC-L2-3.13.15, SC-L2-3.13.8
 - hipaa: 164.312(a)(2)(iv), 164.312(e)(1), 164.312(e)(2)(ii), 164.312(e)(2)(ii)
 - nist_sp_800-53: AC-17(2), SC-8, SC-8(1)
 - pcl_dss_v3.2.1: 2.1.1, 4.1.1, 4.1.1, 8.2.1
 - pcl_dss_v4.0: 2.2.7, 4.1.1, 4.2.1, 4.2.1, 4.2.2, 8.3.2

The check is located in the Registry at HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services. The status is 'Failed'.

5. Plan de Empresa

Matriz DAFO.

La Matriz DAFO es una herramienta de análisis estratégico utilizado para evaluar las características internas y el entorno externo de una organización, proyecto o situación. Su nombre proviene de las iniciales de cuatro elementos clave: Debilidades, Amenazas, Fortalezas y Oportunidades.

Fortalezas (F)

Son los aspectos positivos y las ventajas competitivas que tiene la empresa. Incluyen habilidades, recursos y capacidades que le permiten destacarse frente a la competencia.

Experiencia técnica especializada: los fundadores de Marlutec saben de qué hablan. Tienen un montón de conocimientos en redes, desarrollo web y seguridad. Esto les permite ofrecer un servicio bueno y de calidad.

Ubicación estratégica: la tienda está en una calle súper transitada de San Vicente del Raspeig, lo cual hace que sea fácil atraer a gente del barrio.

Debilidades (D)

Son las áreas en las cuales la empresa tiene desventajas o limitaciones. Estas pueden ser faltas de experiencia, recursos insuficientes o habilidades que necesitan mejorar, lo cual podría afectar su desempeño.

Falta de experiencia en marketing: aunque son unos cracks en el técnico, los fundadores no son muy diestros en ventas y promoción. Esto podría ser un problema.

Dependencia del mercado local: al ser una tienda física, están un poco ligados en la zona de San Vicente del Raspeig. No pueden vender a gente otras ciudades sin complicarse la vida.

Oportunidades (O)

Son factores externos que la empresa puede aprovechar para crecer y mejorar. Incluyen tendencias del mercado, cambios en el comportamiento del consumidor o nuevas tecnologías que pueden beneficiar a la empresa.

Aumento de la demanda de apoyo técnico: con el rollo del teletrabajo, cada vez más personas necesitan ayuda con sus dispositivos.

Conciencia sobre sostenibilidad: la gente está más interesada a reparar sus gadgets que a comprarlos nuevos. Esto le viene bien a Marlutec, que se enfoca en la reparación.

Amenazas (A)

Son factores externos que pueden poner en riesgo a la empresa. Esto puede incluir la competencia, cambios en la regulación, crisis económicas o cualquier otra situación que pueda afectar negativamente su operación.

Competencia de grandes superficies: tiendas como MediaMarkt o Amazon pueden vender productos a precios súper bajos, lo cual podría atraer a los clientes que buscan chollos.

Plan de tesorería

El plan de tesorería es un documento clave que permite controlar y prever los flujos de efectivo de la empresa. En él se detallan todas las entradas (ingresos por ventas, aportaciones de socios, préstamos) y salidas (pagos de suministros, alquiler, salarios, impuestos) de dinero mes a mes. Su principal objetivo es garantizar que la empresa siempre dispongo de suficiente liquidez para hacer frente a sus obligaciones y evitar problemas financieros. Un control adecuado de la tesorería es fundamental para la estabilidad del negocio y su crecimiento a largo plazo.

| Entrades de diners | Gen. | Febr. | Març | Abr. | Mai | Juny | Jul. | Ag. | Set. | Oct. | Nov. | Des. | Total |
|-------------------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| Aportacions dels socis | 25.500 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 25.500 |
| Vendes | 900 | 1.000 | 1.500 | 2.000 | 3.000 | 3.500 | 3.500 | 3.000 | 5.000 | 4.600 | 4.000 | 4.000 | 36.000 |
| Prèstec | 20.000 | | | | | | | | | | | | 20.000 |
| Total entrades | 46.400 | 1.000 | 1.500 | 2.000 | 3.000 | 3.500 | 3.500 | 3.000 | 5.000 | 4.600 | 4.000 | 4.000 | 81.500 |
| Eixides de diners | Gen. | Febr. | Març | Abr. | Mai | Juny | Jul. | Ag. | Set. | Oct. | Nov. | Des. | Total |
| Compra de | 500 | 500 | 500 | 600 | 500 | 600 | 600 | 600 | 700 | 700 | 800 | 900 | 7.500 |
| Subministraments | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 150 | 1.800 |
| Lloguer | 800 | 800 | 800 | 800 | 800 | 800 | 800 | 800 | 800 | 800 | 800 | 800 | 9.600 |
| Fiança (lloguer) | 1.600 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1.600 |
| Cuota Autònomo | 240 | 240 | 240 | 240 | 240 | 240 | 240 | 240 | 240 | 240 | 240 | 240 | 2.880 |
| Costes legals | 800 | | | | | | | | | | | | 800 |
| Assessoria | 120 | 120 | 120 | 120 | 120 | 120 | 120 | 120 | 120 | 120 | 120 | 120 | 1.440 |
| Salario promotors | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Salario del treballador | 1188 | 1188 | 1188 | 1188 | 1188 | 1188 | 1188 | 1188 | 1188 | 1188 | 1188 | 1188 | 14.256 |
| Stock inicial | 13500 | | | | | | | | | | | | 13.500 |
| Publicidad inicial | 500 | | | | | | | | | | | | 500 |
| Compra de mobiliari | 1900 | | | | | | | | | | | | 1.900 |
| Equips informàtics | 3.200 | | | | | | | | | | | | 3.200 |
| Llicències | 600 | | | | | | | | | | | | 600 |
| Prèstec | 346,67 | 346,67 | 346,67 | 346,67 | 346,67 | 346,67 | 346,67 | 346,67 | 346,67 | 346,67 | 346,67 | 346,67 | 4160,04 |
| Total eixides | 25.445 | 3.345 | 3.345 | 3.445 | 3.345 | 3.445 | 3.445 | 3.445 | 3.545 | 3.545 | 3.645 | 3.745 | 63.736 |
| Resultats | Gen. | Febr. | Març | Abr. | Mai | Juny | Jul. | Ag. | Set. | Oct. | Nov. | Des. | Total |
| Entrades menys eixides | 20.955 | -2.345 | -1.845 | -1.445 | -345 | 55 | 55 | -445 | 1.455 | 1.055 | 355 | 255 | 17.764 |
| Saldo acumulat | 20.955 | 18.611 | 16.766 | 15.321 | 14.977 | 15.032 | 15.087 | 14.643 | 16.098 | 17.153 | 17.509 | 17.764 | |

Análisis del plan de tesorería

Las entradas de dinero son suficientes para cubrir las salidas a lo largo del año. A pesar de que en los primeros meses se producen déficits por los elevados gastos iniciales, a medida que avanzan los meses y aumentan las ventas, el saldo acumulado mejora progresivamente. Esto indica una evolución positiva en la gestión de la tesorería, aunque sería recomendable optimizar ciertos costes fijos para garantizar una mejor estabilidad financiera desde el comienzo.

Cuenta de resultados (pérdidas y ganancias)

La cuenta de resultados es un informe que muestra la rentabilidad de la empresa durante un periodo determinado, generalmente un año. En este documento se registran todos los ingresos y gastos operativos y financieros, permitiendo calcular si el negocio está generando beneficios o pérdidas. Es un elemento clave para evaluar la viabilidad y sostenibilidad del proyecto a medio y largo plazo.

| COMPTA DE RESULTATS | | | |
|----------------------------------------|---------------|----------------------------------------------|---------------|
| INGRESSOS D'EXPLOTACIÓ | | GASTOS D'EXPLOTACIÓ | |
| Vendes | 36.000 | Compra de mercaderies | 7.500 |
| | | Subministraments | 1800 |
| | | Lloguer | 9600 |
| | | Fiança (lloguer) | 1600 |
| | | Quota autonom | 2880 |
| | | Salari del treballador | 14256 |
| | | Costes legals | 990 |
| | | Assesoria | 1440 |
| | | Publicitat | 500 |
| | | Amortització (Mobiliari +equips informàtics) | 990 |
| | | Llicencia | 600 |
| Total Ingressos d'explotació | 36.000 | Total Gastos d'explotació | 42.156 |
| INGRESSOS FINANCIERS | | GASTOS FINANCERS | |
| | | Interessos del préstec | 160 |
| Total ingressos financers | 0 | Total gastos financers | 160 |
| RESULTAT D'EXPLOTACIÓ | | | -6.156 |
| RESULTAT FINANCER | | | -160 |
| RESULTAT FINAL ABANS D'IMPOSATS | | | -6.316 |

Análisis de la cuenta de resultados

Se obtienen unas pérdidas de -6.316 €, que, en comparación con el volumen de ingresos y gastos de la empresa, no son excesivamente grandes. Un estudio detallado de los datos indica que la actividad principal genera beneficios, pero los costes de explotación y los intereses del préstamo absorben estas ganancias, provocando un resultado negativo.

Sin embargo, este planteamiento no es desfavorable, puesto que los intereses del préstamo se reducirán progresivamente con el tiempo. Si la empresa puede asumir estas pérdidas iniciales, parece recomendable continuar con la actividad, puesto que la rentabilidad mejorará a medida que se consolidan las ventas y se reduzcan los gastos financieros.

Balance

El balance es una herramienta contable que muestra la situación económica y financiera de la empresa en un momento determinado. Se divide en activos (los bienes y derechos de la empresa) y pasivos (las deudas y obligaciones) y permite analizar la solidez financiera del negocio. Es esencial para entender la capacidad de la empresa para afrontar sus obligaciones y planificar su crecimiento

| BALANÇ | | | | | | | |
|----------------------------------------|--------|--|--------|--------------------------|--------|--|-------|
| ACTIU | | | | PASSIU | | | |
| Actiu no corrent | | | 6310 | | | | |
| Inmobilitzat immaterial | | | | Patrimonio Neto | | | 19184 |
| | | | | Capital | 25500 | | |
| | | | | Pérdidas y ganancias | -6.316 | | |
| Inmobilitzat material | | | | | | | |
| Mobiliari | 1900 | | | | | | |
| Amortització(mobiliari)10 anys | -190 | | | Passiu no Corrent | | | 12000 |
| Equips informàtics | 3200 | | | | | | |
| Amortització (equips informàtics) 25% | -800 | | | Préstec a llarg termini | 12000 | | |
| Llicències | 600 | | | | | | |
| Inmobilitzat financer | | | | | | | |
| Fiança del lloguer | 1600 | | | | | | |
| Actiu corrent | | | 28.874 | Passiu Corrent | | | 4000 |
| | | | | | | | |
| Existències | | | | Prestec a curt termini | 4000 | | |
| Stock (300 unitatdes) | 11110 | | | Proveïdor de mercaderies | 0 | | |
| Realitzable | | | | | | | |
| Disponible | | | | | | | |
| Banc c/c | 17.764 | | | | | | |
| TOTAL | | | 35184 | TOTAL | | | 35184 |

Análisis del balance

El pasivo indica que se han aportado 25.500 €, se han pedido 20.000 € en préstamo (12.000 € a largo plazo y 4.000 € a corto plazo, puesto que el primer año han abonado 4000€) y no hay ninguna deuda pendiente con los proveedores. Con todo esto, la empresa cuenta con un activo de 35.184 €, lo cual implica unas pérdidas de -6.316 €, que, teniendo en cuenta las cifras, no resultan excesivamente preocupantes.

$35.184 > 16.000 \rightarrow$ La empresa dispone de solvencia y se encuentra lejos de la quiebra.

$17.764 > 4.000 \rightarrow$ La empresa presenta un buen nivel de liquidez y minimiza el riesgo de suspensión de pagos.

Fondos propios / deudas = 55% / 45% \rightarrow El nivel de equilibrio financiero es aceptable.

Relación deudas a largo plazo / deudas a corto plazo = 75% / 25% \rightarrow La estructura financiera es razonable, con un predominio de la deuda a largo plazo.

Conclusión:

A pesar de las pérdidas registradas, la situación patrimonial de la empresa es adecuada, puesto que presenta buenos niveles de solvencia y liquidez. Si se pueden asumir estas pérdidas iniciales, resulta recomendable continuar con la actividad.

6. Conclusión final

Este proyecto nos ha permitido integrar muchos de los conocimientos teóricos que hemos ido adquiriendo, aplicándolos de manera práctica en un entorno completo y realista. Hemos trabajado con servidores Windows y Linux, servicios de red, seguridad informática, contenedores y administración de usuarios, lo que nos ha dado una visión muy completa de cómo funciona la infraestructura IT de una empresa moderna.

7. Bibliografía

- <https://www.welivesecurity.com/es/recursos-herramientas/evaluacion-vulnerabilidades-openvas/>
- <https://www.w3schools.com/>
- <https://somebooks.es/crear-carpetas-personales-para-los-usuarios-en-windows-server-2019/>
- [Apuntes proporcionados durante el curso](#)
- <https://josejuansanchez.org/bd/practica-05/index.html>