Davante

Proyecto técnico de configuración

Actividad 9

Título del índice

Proyecto Técnico de Configuración

El departamento técnico de TecnoOffice Solutions S.L. ha sido encomendado con la tarea de preparar y optimizar los ordenadores portátiles del equipo comercial de una empresa cliente. Los objetivos dados han sido asegurar su correcto funcionamiento en distintos entornos de redes, optimizar el consumo energético a lo largo de la jornada para ahorrar batería, y configurar los aspectos necesarios en cuanto a seguridad e imagen corporativa de los equipos.

Para esto, tendremos que profundizar en algunas configuraciones avanzadas de Windows. Esta documentación está dividida en las tres partes principales de la tarea: Redes, Energía, y Configuración básica.

Desarrollo técnico

Fase 1: Análisis DNS y fichero *hosts*

Se nos plantea una situación conflictiva en la que un empleado comercial de la compañía no puede conectarse a un recurso compartido desde fuera de la oficina. Una de las ideas planteadas es comprobar la configuración del DNS de su equipo. Esta configuración es la encargada de traducir nombres de dominio como los que podemos encontrar en páginas web (por ejemplo: google.com) a direcciones IP, que indican al sistema operativo la ubicación del recurso al que se quiere acceder ya sea en internet o en la red local.

1.1. Análisis de métodos de resolución de nombres en Windows 11

En Windows 11, los nombres de dominio se resuelven –es decir, se traducen a una dirección IP– en un orden de preferencia. Esto significa que, si buscas “google.com”, utilizará la primera dirección IP que encuentre asignada a ese dominio. Este orden de preferencia sería:

1. Comprueba si coincide con el nombre del mismo sistema.
2. El contenido del archivo “Hosts”.
3. Se consulta al servidor DNS configurado.
4. Se usa como respaldo la secuencia de resolución de nombres de NetBIOS.

Windows comprobará las distintas listas de direcciones hasta encontrar el dominio solicitado o quedarse sin opciones, en cuyo caso dará un error de conexión. Los más importantes para nosotros son el fichero *Hosts* y la configuración del DNS. [1]

1.1.1. Fichero Hosts

Este fichero, en Windows NT, se encuentra en `%Systemroot%\System32\Drivers\Etc`. Este fichero viene con texto comentado para explicar su funcionamiento. En resumen, el archivo debe contener un listado de direcciones con su respectivo nombre de dominio en la misma línea, y el sistema ignorará todo el texto a partir de una almohadilla (#) hasta el final de esa línea. Así se ve mi archivo de ejemplo, tras quitar el contenido inicial para que se vea más claro mi nueva configuración:

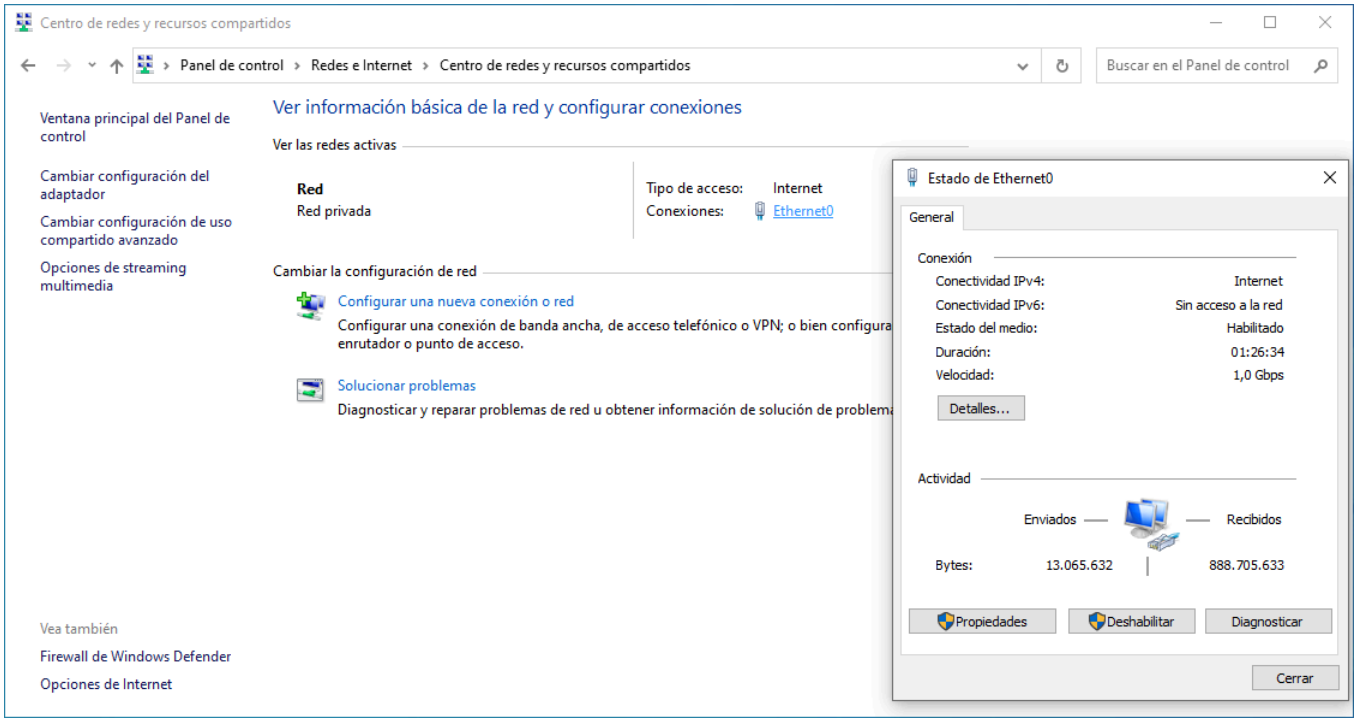
```
  0.0.0.0      google.com        # Esto bloqueará las conexiones a
google.com
127.0.7.80   corporation.local # Al entrar a corporation.local, Windows
encontrará una dirección a un servicio en esta máquina.
```

Más adelante comprobaremos cómo se comportan estas direcciones pidiendo al sistema que las resuelva.

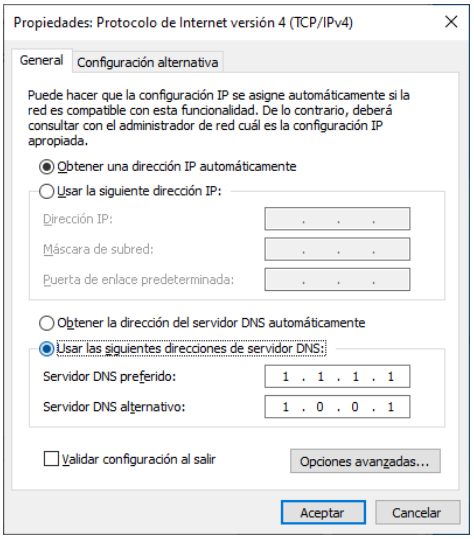
1.1.2. Configuración DNS

El término DNS viene del inglés: *Domain Name System*. Es un servidor que contiene una lista de dominios y direcciones similares a la del archivo *Hosts* visto anteriormente, pero muchísimo más amplia. Los servidores DNS son una de las partes más importantes de internet. Se usa en un equipo para completar las direcciones que no hayamos introducido manualmente.

Para configurar el DNS en Windows, hay que buscar el Panel de Control. Una vez abierto el programa, entramos en Redes e Internet > Centro de Redes y Recursos Compartidos; y entrar en el nombre de la red actual como se ve en la siguiente imagen:



Ahora, en la nueva ventana de estado, hay que entrar en Propiedades, lo que abrirá otra ventana. En esta hay que seleccionar “Protocolo de Internet versión 4 (TCP/IPv4)” y, de nuevo, entrar a “Propiedades” y se abrirá otra ventana más.



En esta última ventana, en la sección de abajo. Seleccionamos la segunda opción: “Usar las siguientes direcciones de servidor DNS”. Luego, escribimos la dirección del servidor DNS deseado; en este caso he elegido el servidor de Cloudflare (1.1.1.1) y su servidor de respaldo (1.0.0.1).

1.1.3. Buenas prácticas

Ahora que conocemos los dos métodos principales de configurar la resolución de nombres de dominio en nuestros equipos; queda decidir cuál de ellos usar. Por lo general, el método a utilizar depende del entorno en el que te encuentres. Para un único equipo al que sólo vas a modificar la configuración esporádicamente puedes usar el archivo *hosts* sin problemas, pero para una red con mayor densidad como una oficina, lo mejor es utilizar un servidor DNS. De ser posible, lo idóneo sería ejecutar un servidor en la propia red de la compañía, por motivos de

seguridad, rendimiento, y personalización; pero también se puede usar un servidor público como el de Cloudflare (1.1.1.1) o el de Google (8.8.8.8) si no hay necesidad de configurar dominios personalizados.

1.2. Demostración de funcionamiento práctico

1.2.1. Comando ping

Para comprobar que un nombre de dominio se resuelve de forma correcta basta con hacer un *ping* al dominio configurado y verificar que intenta conectar a la dirección correcta, sin importar si llega a realizar la conexión con éxito o no. Este comando sirve para muchas tareas de diagnóstico, como puede ser comprobar la configuración del DNS o el tiempo de respuesta de una conexión. Para este caso, sólo necesitaremos el funcionamiento básico, que es `ping nombre-de.dominio` Así es como se vería el comando, ejecutado en una terminal de Windows (el programa cmd):

```
  C:\Users\Usuario>ping google.com
La solicitud de ping no pudo encontrar el host google.com. Compruebe el
nombre y
vuelva a intentarlo.
```

```
  C:\Users\Usuario>ping corporation.local

Haciendo ping a corporation.local [127.0.7.80] con 32 bytes de datos:
Respuesta desde 127.0.7.80: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.7.80: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.7.80: bytes=32 tiempo<1m TTL=128
Respuesta desde 127.0.7.80: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 127.0.7.80:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Usando la configuración del punto 1.1.1, el intento de conexión a google.com ha sido bloqueado, como esperábamos, y Windows ha sido capaz de resolver de forma exitosa el dominio corporation.local y dar con la dirección IP que le dimos (127.0.7.80). El comando también muestra cómo la conexión ha fallado al no haber ningún servidor en la dirección que le hemos dado.

1.2.2. Comando nslookup

El comando *nslookup* es una herramienta de diagnóstico de DNS. Su uso básico es muy sencillo, al ser un programa interactivo. Ingresamos el comando `nslookup` en el cmd de Windows y la línea de la consola cambiará a sólo un `>`, entonces, podremos escribir el dominio a comprobar y pulsar "Enter" para ver la información del dominio. La terminal debería devolver una lista de direcciones IP relacionadas con el dominio o un error si no logra resolverlo. Nótese que, de forma predeterminada, este comando se salta el fichero *Hosts* y consulta al servidor DNS de Cloudflare. Esto es porque esta herramienta no está diseñada para comprobar el fichero *hosts* sino un servidor DNS. [2]

Este es el resultado de comprobar el dominio www.microsoft.com utilizando el comando *nslookup*:

```
  C:\Users\Usuario>nslookup
Servidor predeterminado:  one.one.one.one
Address:  1.1.1.1

> www.microsoft.com
Servidor:  one.one.one.one
Address:  1.1.1.1

Respuesta no autoritativa:
Nombre:  e13678.dscb.akamaiedge.net
Addresses:  2a02:26f0:980:6a9::356e
          2a02:26f0:980:6a6::356e
          2a02:26f0:980:6a2::356e
          2a02:26f0:980:6aa::356e
          2a02:26f0:980:6a5::356e
          2.22.209.211
Aliases:  www.microsoft.com
          www.microsoft.com-c-3.edgekey.net
```

```
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net
```

Como vimos antes; este comando es bastante sencillo. Al iniciar, nos muestra la configuración por defecto. Después de introducir el dominio, nos devuelve:

- Servidor: El nombre del servidor DNS.
- Address: La dirección del servidor DNS al que estamos realizando consultas.
- Nombre: El nombre del servidor del proveedor de dominios.
- Addresses: Las direcciones IPv4 e IPv6 relacionadas con el dominio consultado.
- Aliases: Nombres de dominio que están conectados a las mismas direcciones que el consultado.

1.2.3. Registro DNS

Las resoluciones del DNS se guardan en un archivo que podemos comprobar con el comando `ipconfig /displaydns`,[3] que nos devuelve una lista de todos los dominios que se han guardado e información sobre el dominio y las consultas. Voy a mostrar sólo un par de entradas de ejemplo:

```
  C:\Users\Usuario>ipconfig /displaydns

Configuración IP de Windows

    t-ring-fallback-s2.msedge.net
    ----------------------------------------
    Nombre de registro  . : t-ring-fallback-s2.msedge.net
    Tipo de registro  . . : 5
    Período de vida . . . : 48
    Longitud de datos . . : 8
    Sección . . . . . . . : respuesta
    Registro CNAME. . . . : t-ring.s-part2-t-9999.fb-t-msedge.net


    Nombre de registro  . : t-ring.s-part2-t-9999.fb-t-msedge.net
    Tipo de registro  . . : 5
    Período de vida . . . : 48
    Longitud de datos . . : 8
```

```
Sección . . . . . : respuesta
Registro CNAME. . . . : s-part2-t-9999.fb-t-msedge.net


Nombre de registro  . : s-part2-t-9999.fb-t-msedge.net
Tipo de registro  . . : 1
Período de vida . . . : 48
Longitud de datos . . : 4
Sección . . . . . : respuesta
Un registro (host). . : 13.107.226.254


p-ring.msedge.net
----------------------------------------
Nombre de registro  . : p-ring.msedge.net
Tipo de registro  . . : 5
Período de vida . . . : 34
Longitud de datos . . : 8
Sección . . . . . : respuesta
Registro CNAME. . . . : p-ring.p-9999.p-msedge.net


Nombre de registro  . : p-ring.p-9999.p-msedge.net
Tipo de registro  . . : 5
Período de vida . . . : 34
Longitud de datos . . : 8
Sección . . . . . : respuesta
Registro CNAME. . . . : p-9999.p-msedge.net


Nombre de registro  . : p-9999.p-msedge.net
Tipo de registro  . . : 1
Período de vida . . . : 34
Longitud de datos . . : 4
Sección . . . . . : respuesta
Un registro (host). . : 150.171.84.254
```

```
   Nombre de registro  . : p-9999.p-msedge.net
   Tipo de registro  . . : 1
   Período de vida . . . : 34
   Longitud de datos . . : 4
   Sección . . . . . . . : respuesta
   Un registro (host). . : 150.171.85.254
```

Para eliminar la caché del DNS, se puede utilizar el comando ipconfig /flushdns, que simplemente elimina la caché y te devuelve esto:

```
  Configuración IP de Windows

Se vació correctamente la caché de resolución de DNS.
```

Fase 2: Optimización de portátiles y comparación

2.1. Análisis de las necesidades de un portátil profesional

Los clientes de TecnoOffice Solutions S.L. han solicitado equipos para su equipo comercial, haciendo especial énfasis en la necesidad de que estos se adapten a muchos viajes. Dadas estas necesidades, buscaremos equipos con las siguientes especificaciones:

- Buena batería
- Poco peso
- Buena conectividad inalámbrica
- Procesador promedio
- Sin procesador gráfico dedicado

Algunos extras que podrían ser prácticos pero no esenciales serían tener lector de huellas, conectividad 5G, y carga por usb-c para mayor compatibilidad. Hemos terminado escogiendo el Asus Vivobook M1502YA-BQ881, que tiene:

- Bajo consumo
- Peso de sólo 1,7Kg
- WiFi 6E

- Un procesador más que suficiente

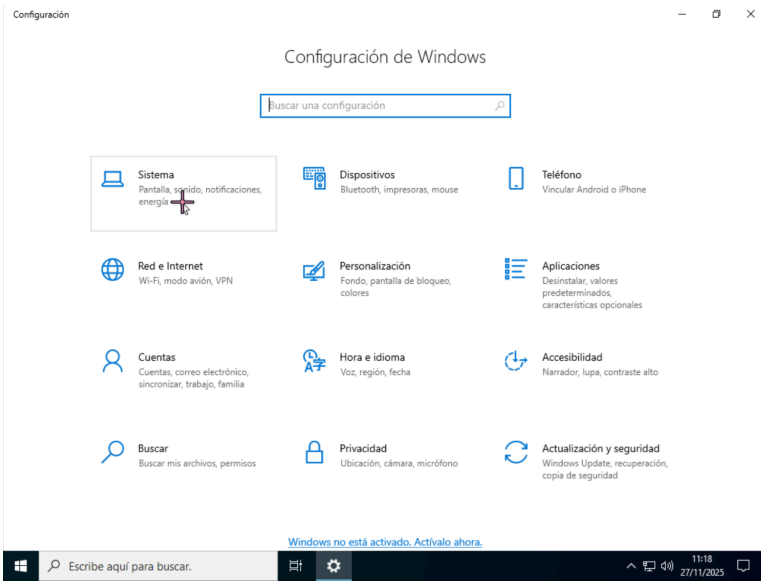
2.2. Optimización del sistema

Ahora que hemos seleccionado un equipo según las características deseadas para este puesto de trabajo, queda configurar las opciones de energía del sistema operativo. Estas opciones tienen como fin ahorrar energía, lo que será vital para equipos pensados para el continuo movimiento.

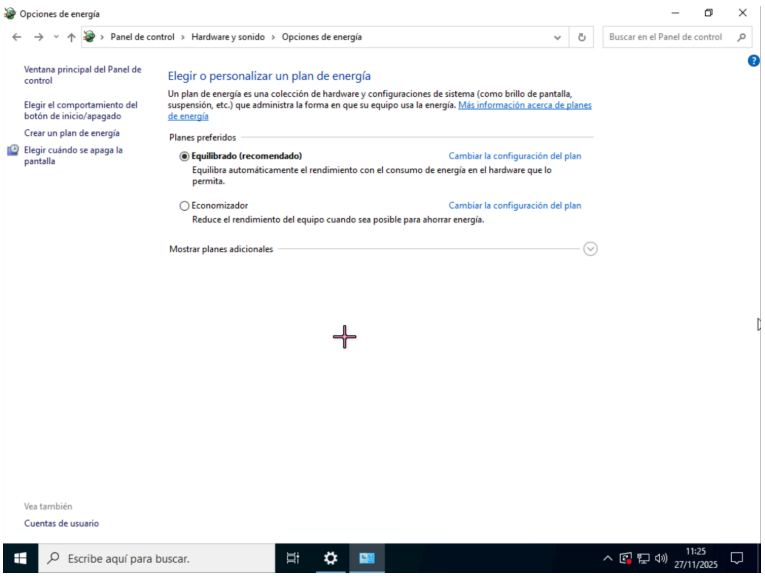
2.2.1. Configuración de energía en Windows 10 de escritorio

Actualmente sólo tenemos disponibles equipos de sobremesa con Windows, que tiene una configuración de energía reducida, por lo que configuraremos esta versión.

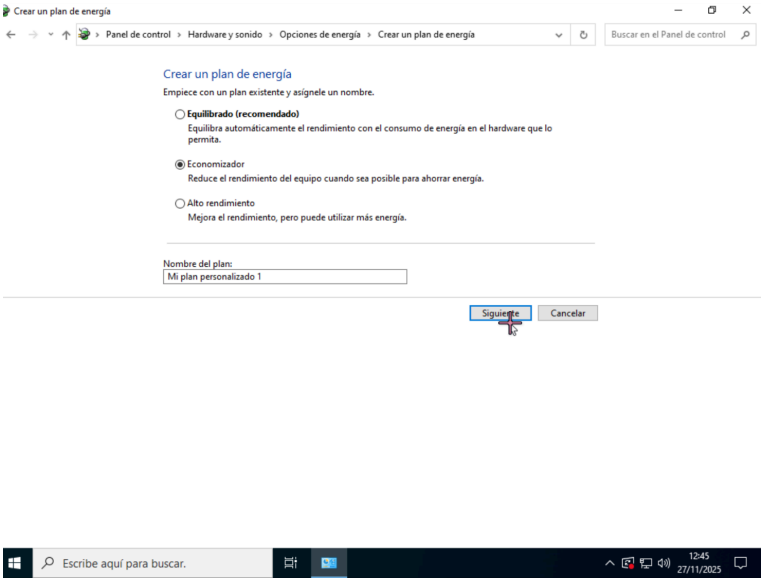
a. Abrimos la configuración de Windows 10 y entramos en el menú de “Sistema”



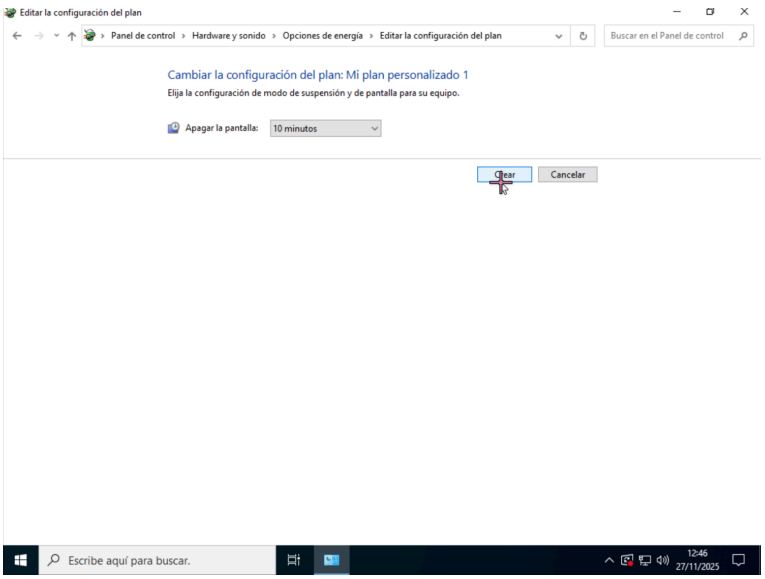
b. Entramos en “Energía y suspensión”
c. En este menú podemos seleccionar entre los tres perfiles de consumo predeterminados: Ahorro de energía, Equilibrado, y Máximo rendimiento. Estos modos están ordenados de menos potencia y consumo a mayor potencia y consumo. Si queremos ahorrar batería y no necesitamos mucha potencia, lo óptimo es usar el modo de ahorro de energía.
d. Si queremos modificar estos perfiles en mayor detalle, tenemos que entrar en “Configuración adicional de energía”. Aquí, lo mejor sería crear un nuevo plan haciendo clic en “Crear un nuevo plan de energía” en el menú de la izquierda.



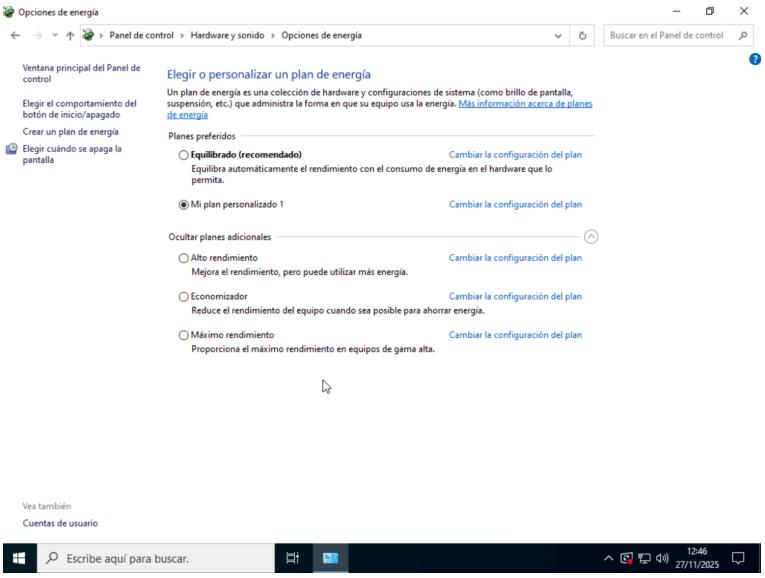
e. Elegimos un plan predeterminado en el que basarnos y le asignamos un nombre.



f. Le damos un tiempo de apagado de pantalla.



g. Ahora tenemos una nueva opción entre los planes de energía con el que hemos creado.

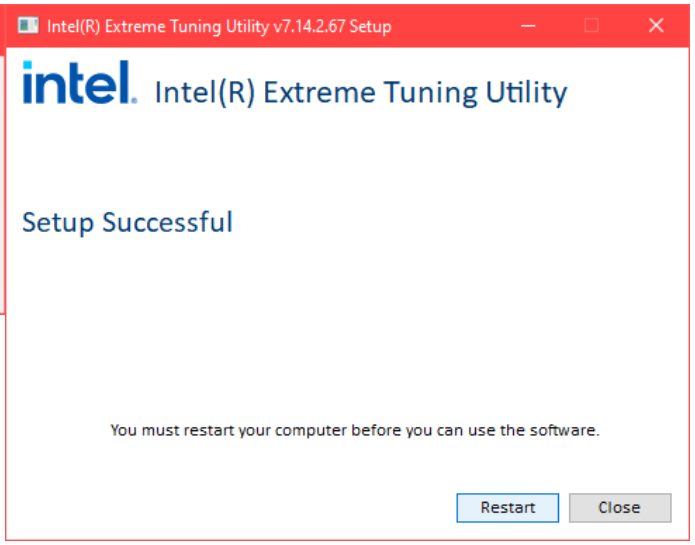


2.3. Análisis de herramientas de optimización profesional

Además de las opciones que nos ofrece Windows para el control de la energía del equipo, podemos utilizar herramientas especializadas de terceros diseñadas específicamente para nuestro hardware. Como vamos a configurar un equipo con un procesador de Intel (i5-10400), utilizaremos el software oficial de Intel para optimizar la configuración.

2.3.1. Instalación de Intel Extreme Tuning Utility

a. Empezamos, como con cualquier otro programa, buscando la página oficial de los desarrolladores y descargando el instalador. Lo ejecutamos, seleccionamos el idioma, y aceptamos los términos de uso.

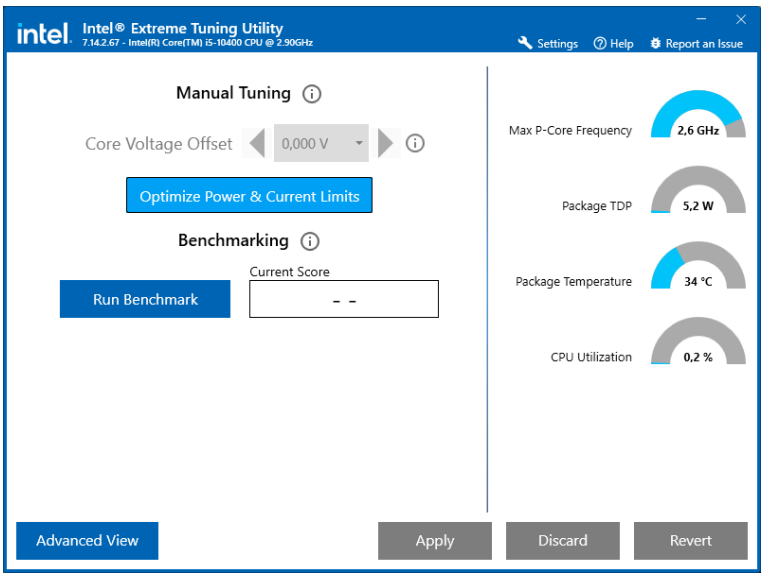


b. Tras la instalación, es necesario reiniciar el equipo antes de utilizar la aplicación.

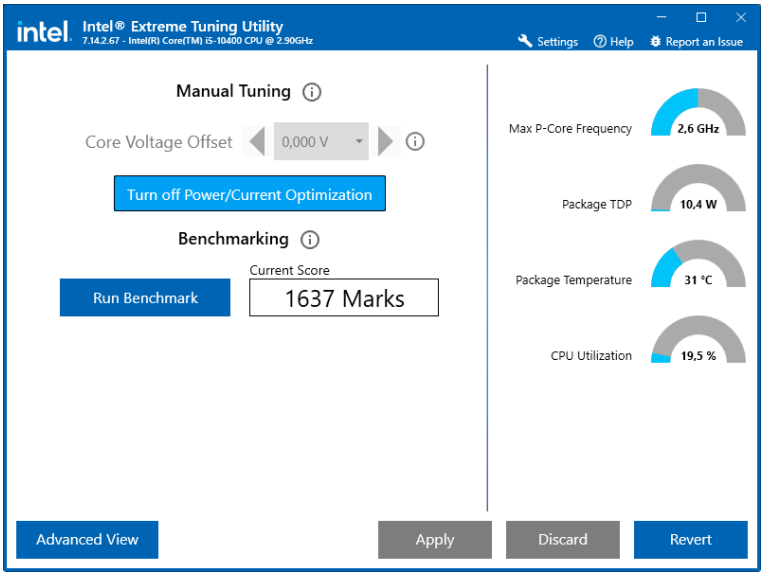
2.3.2. Configuración de alto rendimiento

Lo primero que probaremos será activar las optimizaciones automáticas de rendimiento. Este es un modo que maximiza la capacidad de la CPU sin riesgo a dañar el hardware. Para ello,

simplemente pulsamos el botón azul claro que dice “Optimize Power & Current Limits”.



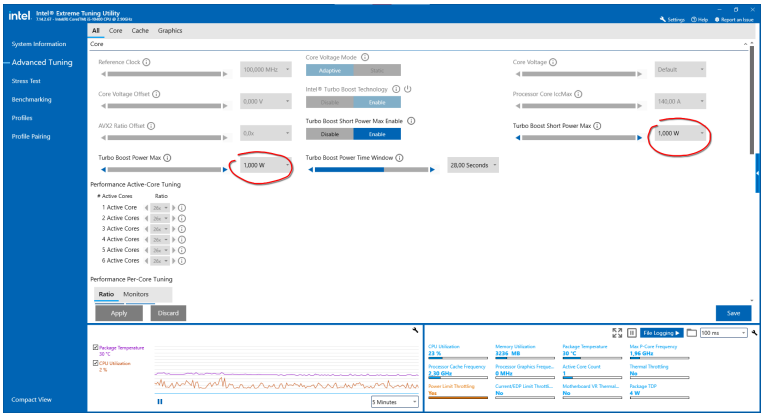
Ahora, con el fin de comparar con los resultados de la siguiente parte, realizaremos una prueba de rendimiento pulsando en el botón azul oscuro que dice “Run Benchmark”. Tras un par de minutos de espera, aparecerá una puntuación en el centro del menú. Cuanto más alto, mejor rendimiento ha tenido la CPU durante la prueba. Esto se traducirá en más consumo de



batería.

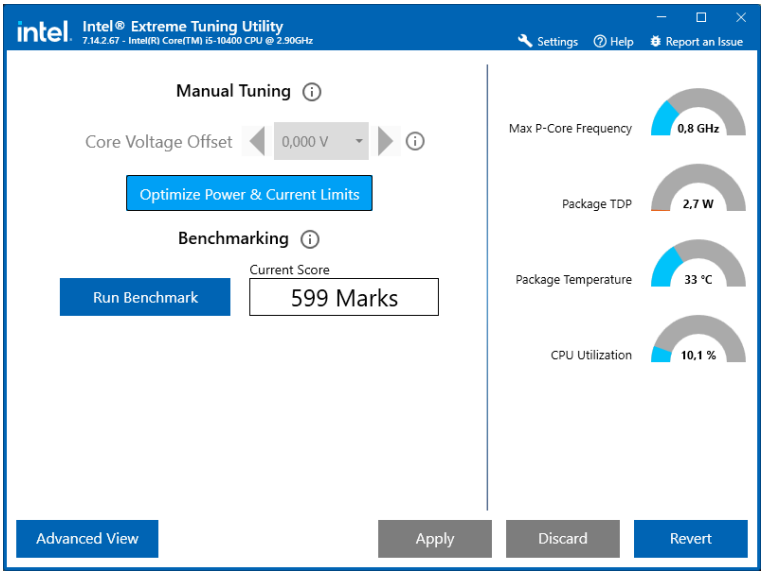
2.3.3. Configuración de bajo consumo

Con el fin de evitar el consumo excesivo de la batería, ahora haremos lo contrario de antes. Para ello, entramos en “Advanced View”, que abrirá una ventana llena de información. Entramos, en el menú izquierdo, en “Advanced Tuning” y veremos la configuración avanzada de energía. Las dos opciones señaladas son las que vamos a modificar.



En este caso, para ver clara la diferencia, he establecido los valores al mínimo, pero lo suyo es probar distintos valores hasta quedarnos en el valor más bajo en el que las aplicaciones que necesitemos utilizar funcionen de forma fluida. Este será el punto óptimo de equilibrio entre eficiencia y consumo.

Repetimos el *benchmark*, que naturalmente tardará un poco más que antes. Como podemos apreciar, el puntaje ha sido mucho más bajo que antes, por debajo de la mitad:



2.3.4. ¿Merece la pena?

En resumen: sí. Estamos utilizando un software oficial del fabricante de la CPU de forma apropiada y dentro de márgenes más que seguros. Este proceso hará una gran diferencia en la duración final de la batería de los equipos comerciales y, si se realiza con algo de esmero, no debería de impactar negativamente al rendimiento en situaciones de uso reales.

2.4. Investigación y comparación de imágenes optimizadas

A la hora de optimizar un sistema operativo, una de las ideas que pueden surgir es, sencillamente, instalar un sistema operativo mejor optimizado. Suena obvio y es una opción, pero no siempre es buena idea hacer esto. Si estamos trabajando con sistemas operativos de código libre, tomar esta decisión es más trivial, ya que tenemos cientos de distribuciones para elegir, pero en el caso de Windows la situación se complica.

2.4.1. ¿Qué quiere decir que el sistema esté optimizado?

Generalmente, cuando hablamos de un sistema más optimizado, se trata de sistemas operativos más eficientes y con menos procesos de fondo que permitan dedicar más recursos del ordenador a la tarea principal. También se tienen en cuenta la cantidad de programas preinstalados innecesarios (*bloatware* en inglés) y la capacidad de eliminarlos si los hay.

2.4.2. Versiones oficiales de Windows

Al contrario que sus alternativas, Microsoft ofrece muy pocas versiones distintas de Windows, y ninguna está optimizada para maximizar el rendimiento del sistema para batería ni para tareas de alto rendimiento. Nada de “Windows Lite”.

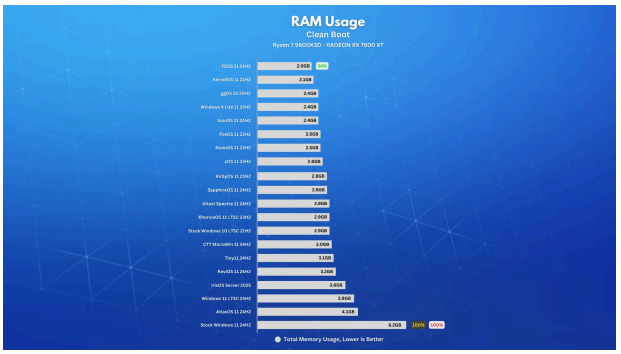
2.4.3. Versiones no oficiales de Windows

Con el fin de suplir esta necesidad entre los usuarios de Windows que desean mejor rendimiento, siempre han habido intentos de la comunidad de modificar sus instalaciones de Windows para alcanzar los objetivos deseados de rendimiento. Estas versiones modificadas tienden a distribuir Windows con menos programas instalados por defecto y muchos procesos considerados innecesarios deshabilitados o eliminados. Estas versiones, sin embargo, traen una serie de problemas y riesgos:

- En ocasiones, eliminan o deshabilitan software importante para el correcto funcionamiento del sistema.

- Algunas versiones rompen la compatibilidad con las actualizaciones de seguridad oficiales de Microsoft
- Pueden incluir *malware*, software malicioso que puede dañar el sistema o comprometer la seguridad y privacidad del usuario.

Dicho eso, las ventajas en cuanto a rendimiento y eficiencia energética de estas versiones modificadas son tan claras como sus riesgos. Las siguientes benchmarks realizadas en distintas versiones de Windows muestran algunas de las muchas diferencias que afectan a este



rendimiento final: [4]

2.4.4. Recomendaciones en un entorno corporativo

Pese a lo tentadora que es la alternativa de instalar una versión modificada de Windows en estos equipos, los riesgos de seguridad en este entorno son inadmisibles. Sacrificar potencialmente funcionalidad, actualizaciones, además del riesgo de incluir malware no es una opción realista por mucha eficiencia que ganáramos. Si realmente nos viéramos obligados a abandonar Windows por estos motivos, sería más recomendable investigar sobre distribuciones de Linux ligeras y adaptar el software que necesite el equipo para ser compatible con el nuevo sistema.

Fase 3: Configuración del software base

En esta fase del proyecto nos encargamos de configurar el software de base de Windows 11; específicamente las opciones de seguridad y la apariencia e idioma. Para ello, vamos a empezar configurando el *Firewall*.

3.1. Firewall de Windows

El *Firewall* es el módulo del sistema operativo encargado de la seguridad en red del equipo. Su función principal es permitir o denegar conexiones externas según lo que diga la configuración que, por defecto, bloquea casi todas las conexiones entrantes y permite todas las conexiones salientes. El *firewall* distingue dos tipos de redes con sus respectivos sets de reglas:

- Red privada:

Este tipo de redes tiende a tener reglas más laxas, ya que se asume que es una red de un hogar o una oficina en la que todos los dispositivos deberían ser de confianza.

- Red pública:

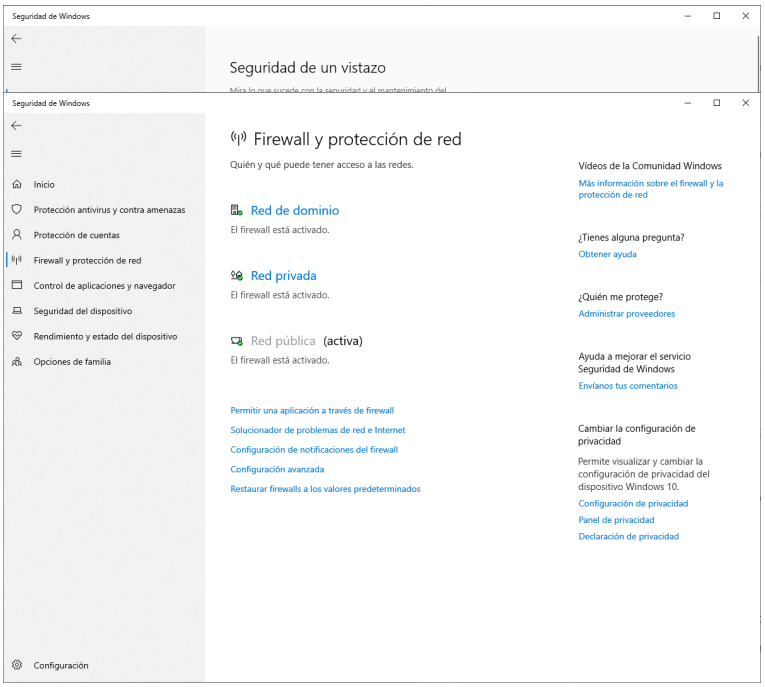
Las redes públicas, al contrario que las privadas, asumen que pueden haber dispositivos maliciosos conectados, por lo que se suelen configurar reglas más estrictas para este tipo de conexiones. Un ejemplo de conexión pública sería el WiFi de una cafetería o un aeropuerto.

3.1.1. Tipos de reglas

Una regla puede especificar aplicaciones o puertos concretos. Los puertos son puntos de entrada al sistema; si un puerto está abierto, todas las conexiones que traten de pasar por este serán permitidas, no importa la aplicación que lo solicite. Si la regla está establecida para una aplicación, todos los puertos serán accesibles por ella incluso si están cerrados. Esto podría ser una brecha de seguridad enorme si estuviera mal gestionado, por lo que hay que tener cuidado a la hora de configurar reglas del *firewall* en la red de una compañía.

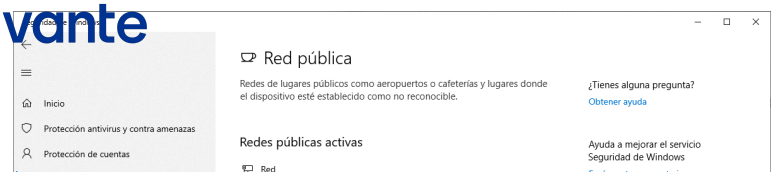
3.1.2. Configuración básica del Firewall en Windows

1. Abrimos la aplicación “Seguridad de Windows” y seleccionamos “Firewall y protección de red”.



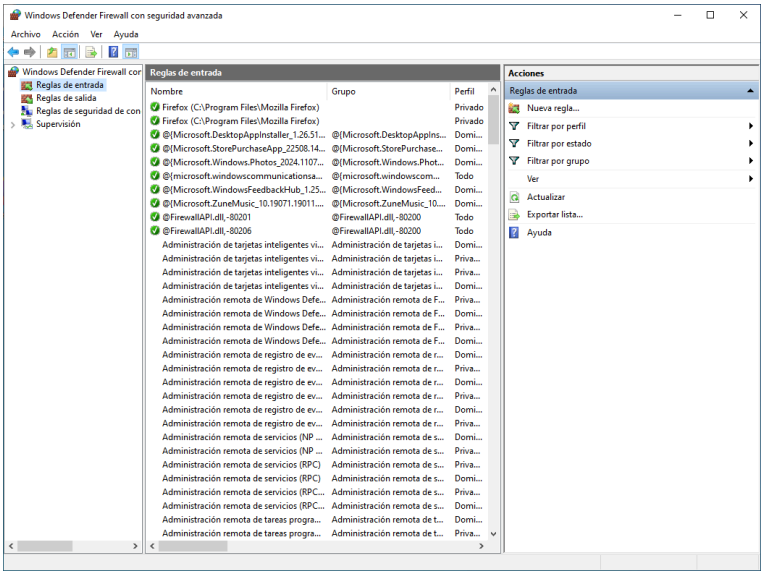
2. En esta pantalla seleccionamos el perfil que queramos modificar; en este caso, “Red pública”

3. En esta pantalla tenemos toda la configuración básica de las redes públicas. Primero se puede ver un interruptor azul para activar o desactivar el *firewall* completo. La siguiente opción permite activar o desactivar todas las conexiones entrantes. [5]



3.1.3. Configuración avanzada del Firewall de Windows

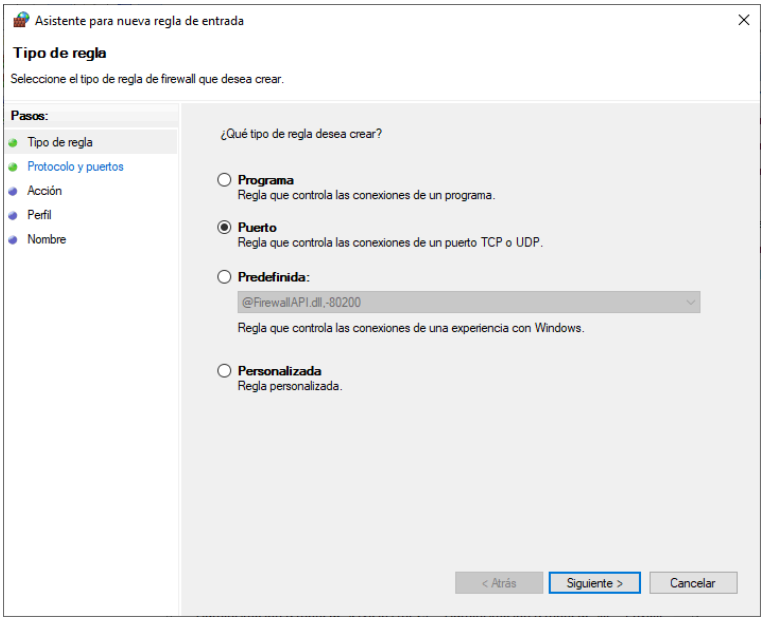
1. En el paso 2 de la configuración básica, en lugar de seleccionar un perfil de red, seleccionamos la opción “Configuración avanzada”, abajo en el centro de la pantalla.
2. En este menú podemos ver una cantidad de opciones algo abrumadora. En este ejemplo, voy a crear una regla que bloquee explícitamente las peticiones de entrada al puerto 80 del sistema. Para ello, comenzamos con entrar en el menú “Reglas de entrada”, en el menú



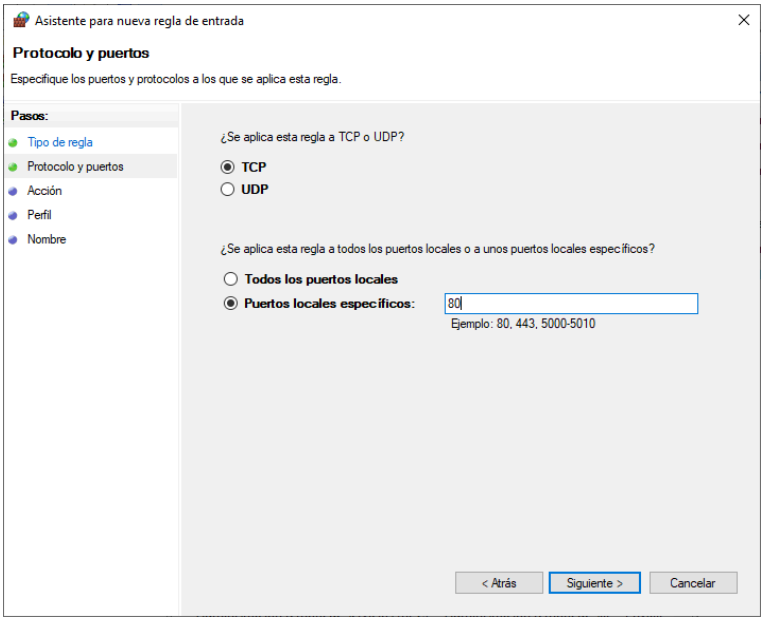
lateral izquierdo:

3. Ahora aparecerá la opción “Nueva regla…” en el menú derecho. Entramos ahí.

4. En la nueva ventana, seleccionamos la opción “Puerto”:

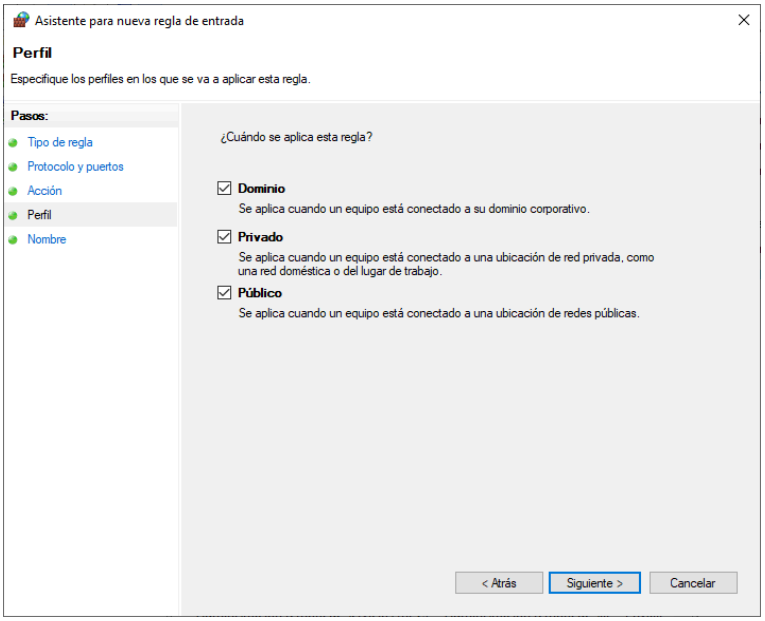


5. En la siguiente pantalla, dejamos la opción “TCP” e ingresamos el número 80 en el campo de texto



6. En la siguiente pantalla, seleccionamos “Bloquear la conexión” y seguimos.

7. En esta pantalla mantenemos todas las opciones seleccionadas. Si quisiéramos, por ejemplo, permitir esta conexión en casa y bloquearla fuera, podríamos deseleccionar “Privado” para que la regla no se aplique en redes privadas.



8. En la última pantalla le asignamos un nombre y descripción a la regla.
9. Para completar esta configuración; deberíamos duplicar esta regla seleccionando “UDP” en el paso 5 y asignando un nombre distinto a la regla.

3.1.4. Comando “netsh advfirewall”

Windows también incluye una utilidad de consola para gestionar el *firewall*, lo que podría permitirnos gestionarlo a través de un script para automatizar tareas, por ejemplo. Al igual que la configuración avanzada, este comando tiene demasiadas opciones para explicarlas todas en este proyecto, por lo que me limitaré a replicar la configuración que apliqué en la sección anterior. Para más detalles, recomiendo leer de primera mano la documentación oficial sobre este comando de Microsoft. [6]

1. Abrimos la terminal de Windows (cmd). Es importante que, en lugar de hacer clic sobre la aplicación, hacemos clic derecho y seleccionemos la opción “Ejecutar como administrador”, ya que este comando necesita privilegios para funcionar.

2. Escribimos el comando `netsh advfirewall firewall add rule name= "Bloquear puerto 80" dir=in action=block protocol=TCP localport=80`. Desglosamos el comando completo para explicarlo de forma más clara:

a. **netsh advfirewall**: Comando de configuración del *firewall*.
b. **firewall**: Indica que vamos a modificar reglas del *firewall*.
c. **add**: Indica que vamos a añadir una configuración.
d. **rule**: Lo que vamos a añadir es una regla.
e. **name= "Nombre"**: El nombre de la regla; puede ser cualquier texto.
f. **dir=in**: Especifica si es una regla de entrada (*in*) o de salida (*out*).
g. **action=block**: Indica si es una regla de permitir (*allow*) o denegar (*block*) conexiones.
h. **protocol=TCP**: Indica el protocolo, que puede ser TCP o UDP.
i. **localport=80**: Elige el puerto al que afecta esta regla. Puede ser cualquier número entre el 1 y el 65535.

3. El resultado esperado sería una simple confirmación de que la regla ha sido aceptada:

```
C:\Windows\system32>netsh advfirewall firewall add rule name= "Bloquear
puerto 80" dir=in action=block protocol=TCP localport=80
Aceptar
```

3.2. Antivirus y seguridad

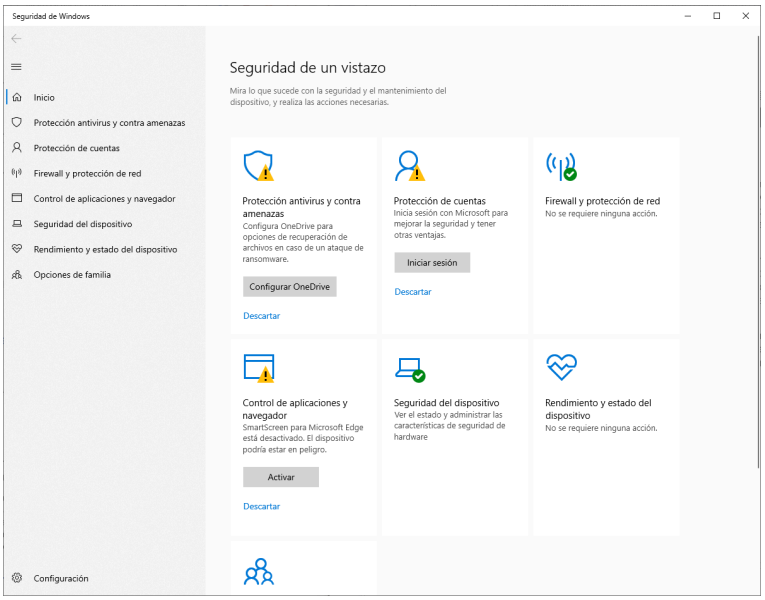
El antivirus es una pieza esencial para la seguridad de cualquier sistema operativo. Sin este, el equipo estaría desnudo ante cualquier amenaza proveniente de un software malicioso. En un entorno corporativo, el antivirus es incluso aún más importante que en dispositivos personales, ya que los atacantes suelen tener preferencia por las empresas a la hora de elegir a sus víctimas debido a la cantidad de datos sensibles que pueden poseer y a su mayor posibilidad de terminar pagando un restate en casos de *ransomware*, por ejemplo.

Desde Windows 10, el sistema operativo trae preinstalado un antivirus llamado Windows Defender. Es un antivirus básico y gratuito, suficientemente efectivo para entornos de pocos requisitos de seguridad, como el ordenador de un hogar. Para entornos corporativos es más común contratar un antivirus profesional en paquetes de licencias. Algunos ejemplos serían Avast, Malwarebytes, o Kaspersky.

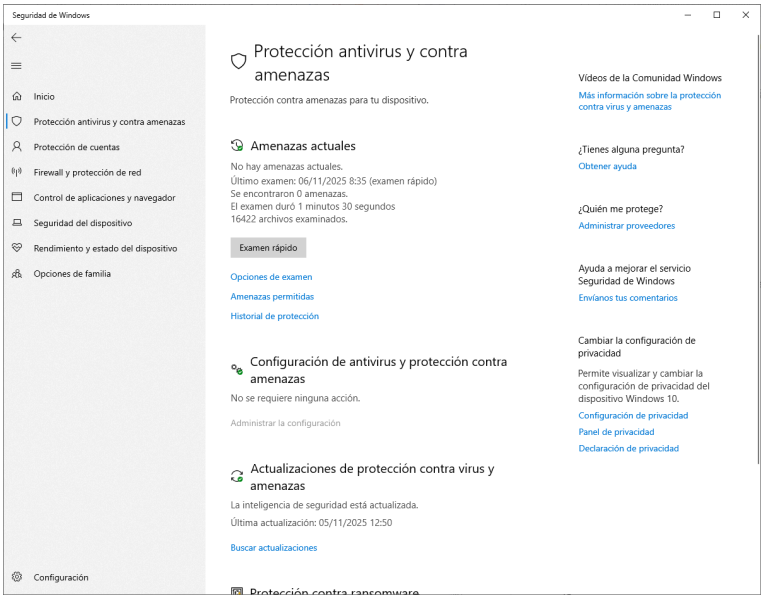
En algunos casos, al instalar un programa, Windows Defender elimina archivos o bloquea directorios necesarios para el proceso de instalación porque considera que el software está actuando de forma sospechosa. En esta situación, a veces, la única solución es desactivar Windows Defender temporalmente. Los pasos a seguir para esto serían:

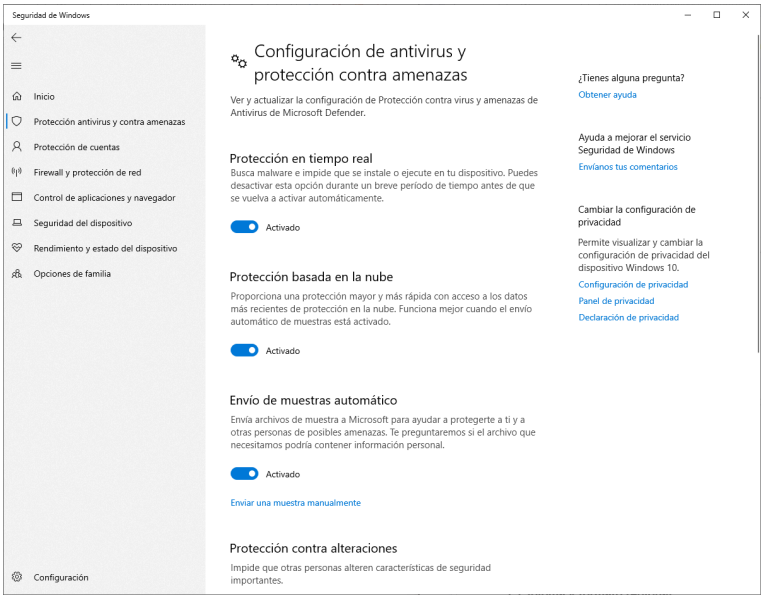
1. Abrir la aplicación "Seguridad de Windows"

2. Entrar en “Protección antivirus y amenazas”



3. Entrar en “Administrar la configuración”, bajo “Configuración de antivirus y protección de amenazas”



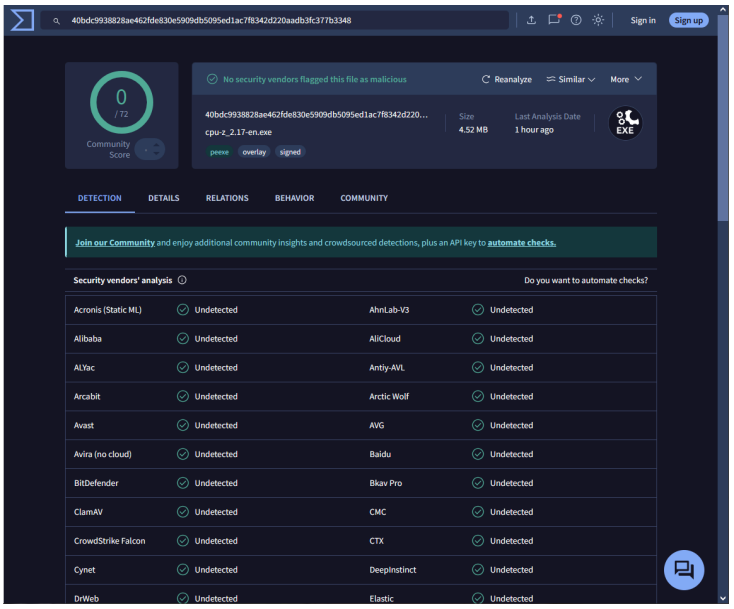


4. Desmarcar la casilla donde dice “Protección en tiempo real”

Dicho todo eso: Está extremadamente poco recomendado desactivar la seguridad del sistema por completo bajo ningún concepto, ya que estarías abriendo todas las ventanas que quieran a posibles atacantes. En su lugar, hay una serie de pautas que puedes seguir para continuar de forma segura:

- Verificar que el software proviene de una fuente oficial y de confianza.
- Escanear el instalador de forma activa para confirmar que no contiene ningún *malware* real, es decir, confirmar que efectivamente nos encontramos ante un falso positivo. Una opción efectiva y de confianza sería utilizar la herramienta VirusTotal (made in spain), que contrasta el archivo con una gran variedad de antivirus distintos para darte una probabilidad más realista de que se trate de una amenaza real. El proceso sería algo así:

a. Visitar la web, seleccionar la opción “Choose file”, y seleccionar el instalador que queremos escanear.



b. Rápidamente, el sitio nos devolverá resultados claros sobre el archivo:

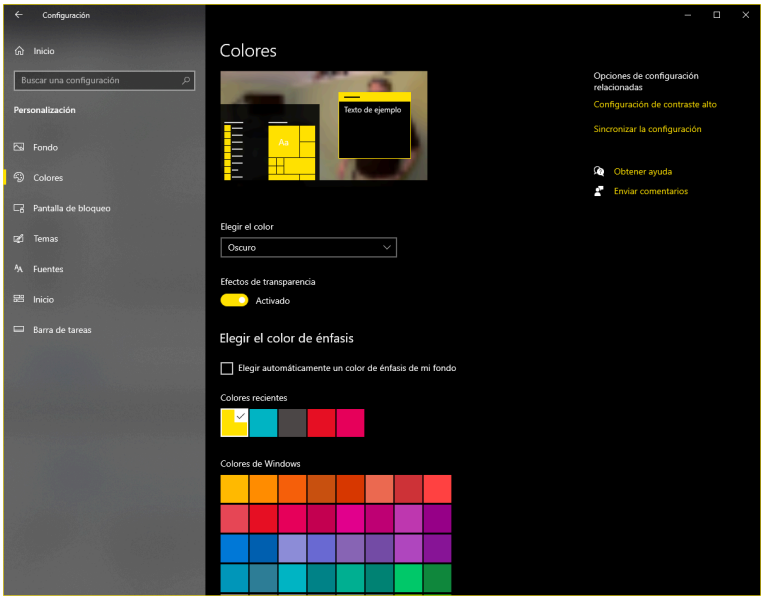
- Si resulta ser un falso positivo, entonces podemos añadir el archivo a las excepciones de Windows Defender para que el sistema nos permita ejecutarlo sin más contratiempos. Puedes ver más detalles sobre este proceso en la documentación oficial de Windows. [7]

3.3. Apariencia del sistema

En Windows podemos cambiar la apariencia para adaptarse a los gustos o necesidades del usuario. Es una configuración sencilla que puede ayudar en algunos casos, sobre todo como herramienta de accesibilidad. Para personalizar la apariencia del sistema, abrimos la configuración de Windows y entramos a “Personalización”. El primer menú no lo vamos a tocar por ahora, ya que lo estableceremos en el punto 3.4 como directiva del grupo local.

3.3.1. Colores

El segundo menú, “Colores”, nos permite elegir entre temas claro u oscuro y los colores de acento del sistema. Algunas aplicaciones de terceros, como Firefox, tratarán de usar el mismo tema para integrarse mejor con las aplicaciones del sistema, pero no todas hacen esto. Las opciones de esta pantalla son autoexplicativas, por lo que no vamos a profundizar mucho en



ellas.

3.3.2. Pantalla de bloqueo

Este menú permite modificar el fondo y contenido de la pantalla de bloqueo. La primera opción cambia el tipo de fondo de pantalla, que puede ser una imagen normal, una serie de imágenes en rotación, o “Contenido destacado de Windows”; que es una galería de fondos curada por Microsoft que suele incluir paisajes e información sobre regiones interesantes. Vamos a seleccionar una imagen estática, lo que habilitará otra opción debajo en la que podemos elegir qué imagen será el fondo de pantalla.

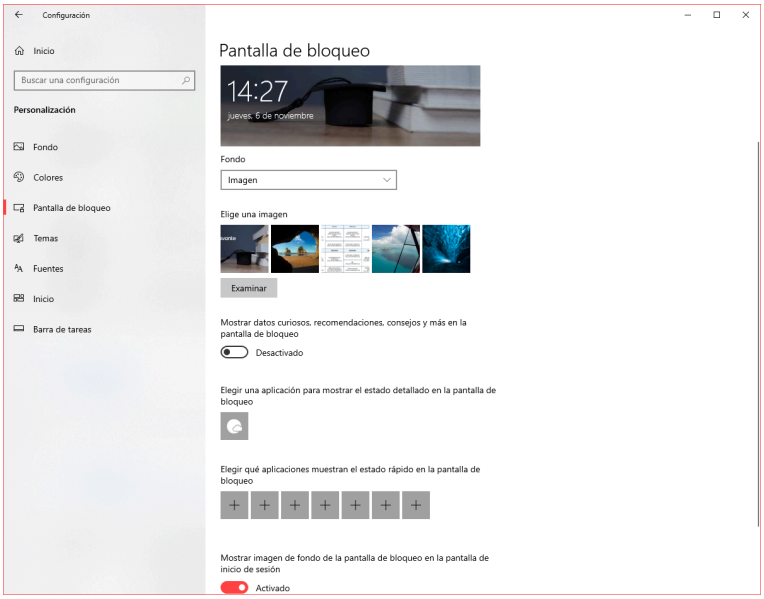
La siguiente opción nos ofrece información interesante, curada también por Microsoft, en la pantalla de bloqueo. La vamos a mantener desactivada.

Después de esto, vienen accesos directos a algunas aplicaciones. Estos accesos directos muestran información detallada y sencilla respectivamente y permiten acceder a algunas

aplicaciones sin desbloquear la pantalla. Vamos a dejar solamente el acceso directo al tiempo, y desactivar opciones como correo o calendario por motivos de seguridad y privacidad.

La última opción simplemente permite seguir esta configuración en la pantalla de inicio de sesión, es decir, la que aparece al iniciar el equipo y no al bloquear manualmente la pantalla; o mantener la configuración por defecto en caso de desactivarla. Vamos a dejarla activada.

Con estas opciones, la configuración se vería así:



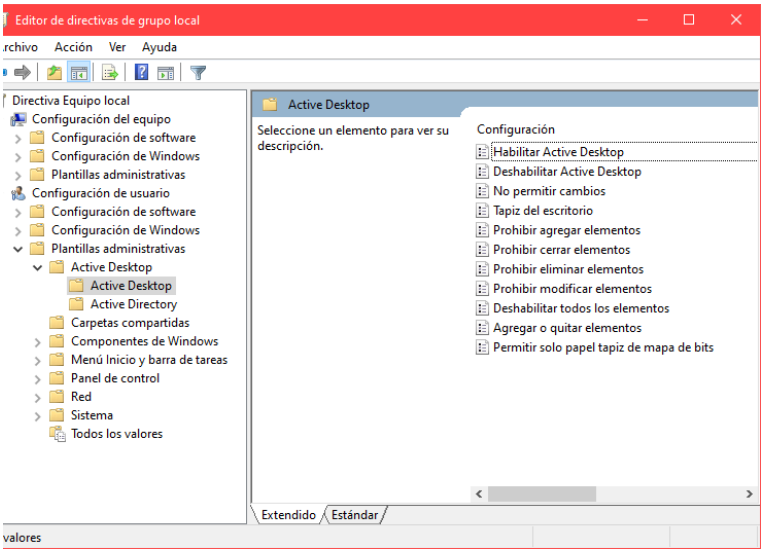
3.4. Fondo de pantalla corporativo

En algunos casos, la empresa podría necesitar establecer un fondo de pantalla a todos los trabajadores y retirarles la capacidad de modificarlo. Esto es útil si se desea tener una imagen corporativa consistente en la oficina, por lo que Microsoft ha desarrollado un método para lograr este fin a través de las directivas del grupo local. [8]

Para establecer un fondo de pantalla obligatorio, debemos seguir los siguientes pasos:

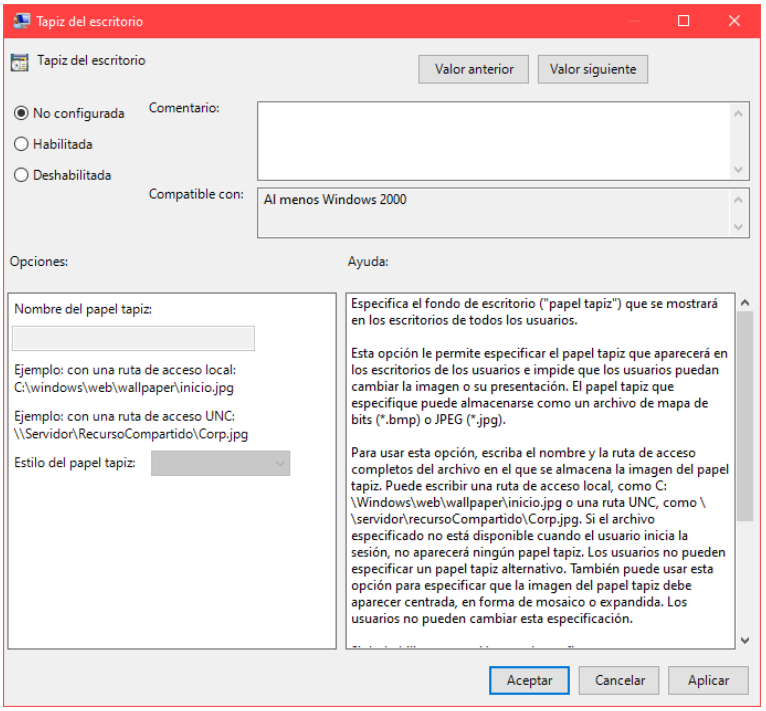
1. Entrar al programa “Editor de directivas del grupo local”.

2. Dentro de este, en el menú izquierdo, entrar en: Configuración de usuario > Directivas > Plantillas administrativas > Active Desktop > Active Desktop. Verás la siguiente ventana, que



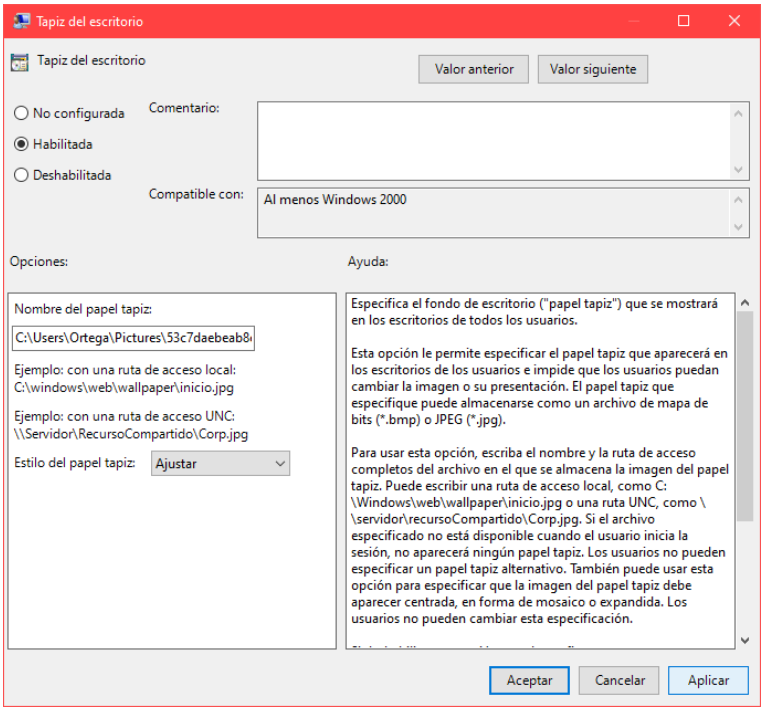
contiene todas las opciones que vamos a utilizar:

3. Seleccionamos “Tapiz del escritorio” y aparecerá texto en el centro de la ventana. Entramos en el siguiente menú haciendo clic sobre el texto azul.



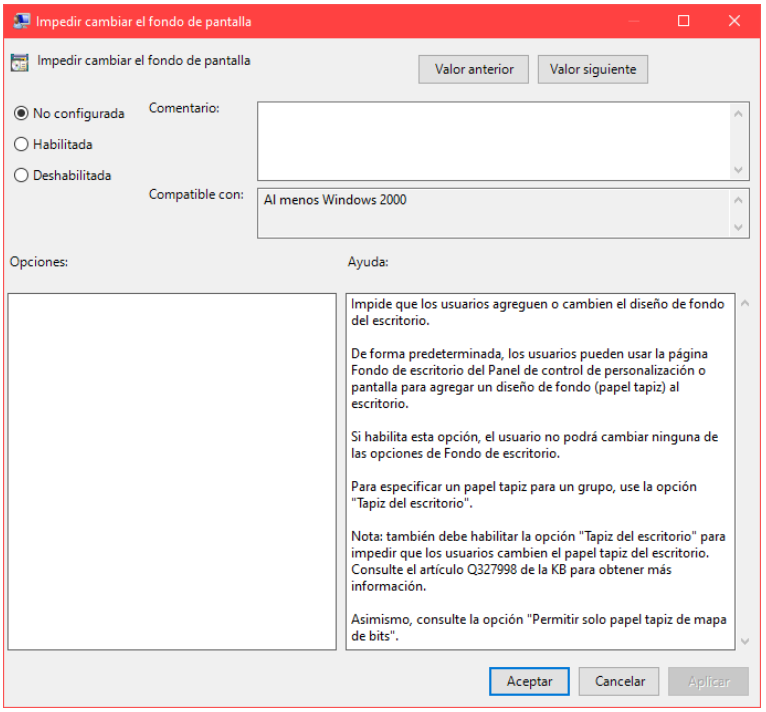
4. En esta ventana lo primero que debemos hacer es habilitar el tapiz del escritorio.

5. Lo siguiente sería seleccionar el archivo que queremos establecer como fondo de pantalla. Como no hay ningún selector de imágenes, tendremos que copiar la ruta completa de



esta.[9] Tras eso, aplicar y aceptar.

6. Para bloquear el cambio de fondo de pantalla, accedemos a Configuración de usuario > Directivas > Plantillas administrativas > Panel de control > Personalización. Entramos en la opción “Impedir cambiar el fondo de pantalla” y, tras hacer clic en el texto azul, veremos esta ventana:



7. Habilitamos la directiva, aplicamos, y aceptamos.

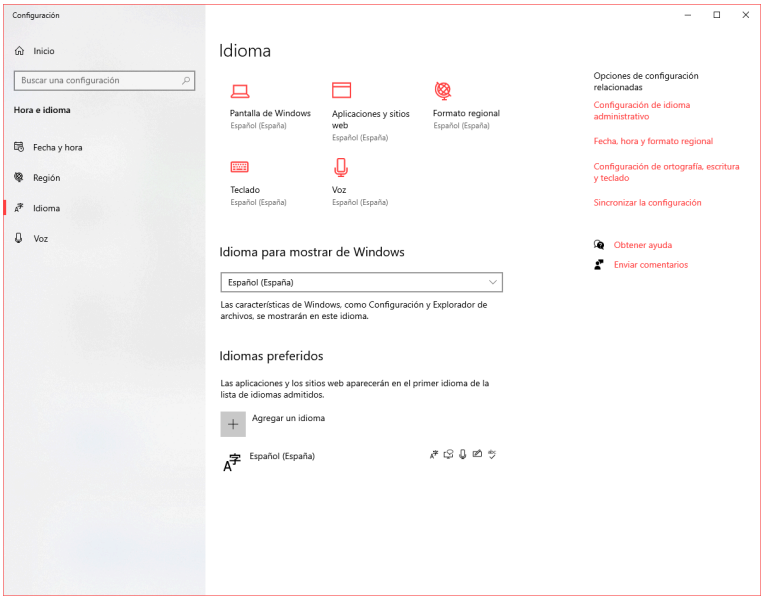
Con esto tendríamos terminado de configurar el estilo e imagen corporativa del equipo.

3.5. Idioma y formato regional

Poder cambiar el idioma es una característica que no necesita mucha introducción. Es una función básica y necesaria para cualquier tipo de software. Para cambiar el idioma en Windows, debemos seguir los siguientes pasos:

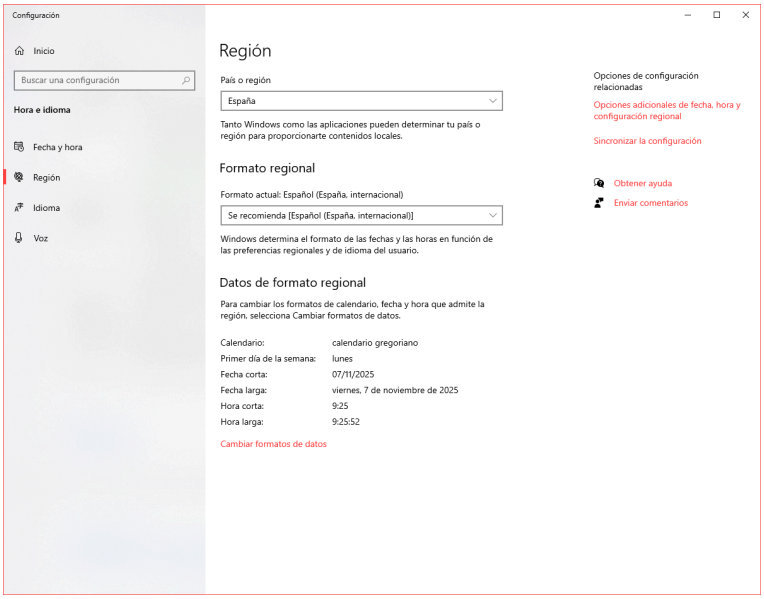
1. Buscar en el menú de inicio “Idiomas”.

2. En esta ventana, pulsamos sobre “Agregar un idioma” y seleccionamos el deseado. En este ejemplo, añadiremos el inglés de Estados Unidos.



3. Ahora aparecerá el Inglés en la lista de idiomas disponibles. Podemos seleccionar un idioma de esta lista como idioma principal en el menú desplegable de arriba.

Para cambiar otras opciones regionales, como formato de fechas, hora, calendario, unidades, etc; tendremos que acceder al menú “Región”, a la izquierda de la configuración de idiomas. Una vez dentro, podremos seleccionar la región deseada en los dos desplegables en pantalla:



Conclusiones

En este proyecto hemos terminado configurando con éxito los ordenadores portátiles solicitados para el equipo comercial de la empresa cliente. En cada fase del proyecto nos hemos asegurado de comprobar cada aspecto de los nuevos equipos, poniendo especial foco en la seguridad de los sistemas, la optimización, y el correcto funcionamiento en entornos de trabajo cambiantes.

Anexos

Webgrafía

[1] Resolución de nombres en Windows:
https://support.microsoft.com/en-us/topic/microsoft-tcp-ip-host-name-resolution-order-dae00cc9-7e9c-c0cc-8360-477b99cb978a

[2] Nslookup:
https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup

[3] Registro DNS:
https://www.xataka.com/basics/como-ver-ultimas-webs-que-visitaste-modo-incognito-tu-navegador-como-evitarlo

[4] "I Tested ALL Custom Windows OS - Which One's Best For Gaming? (+ Benchmarks)":
https://www.youtube.com/watch?v=uHjGV1NrO_Y

[5] Firewall de Windows:
https://support.microsoft.com/es-es/windows/firewall-y-protecci%C3%B3n-de-red-en-la-aplicaci%C3%B3n-seguridad-de-windows-ec0844f7-aebd-0583-67fe-601ecf5d774f

[6] Netsh advfirewall:
https://learn.microsoft.com/es-es/windows-server/administration/windows-commands/netsh-advfirewall?tabs=consecadd%2Cfirewalladd%2Cmainmodeadd%2Cmonitordelete

[7] Excepciones de Windows Defender:
https://learn.microsoft.com/es-es/defender-endpoint/configure-exclusions-microsoft-defender-antivirus

[8] Fondo de pantalla corporativo (directivas locales):
https://www.sysadmit.com/2016/05/gpo-establecer-fondo-escritorio.html

[9] Copiar la ruta de un fichero:
https://www.supportyourtech.com/articles/how-to-copy-path-of-a-file-in-windows-10-a-step-by-step-guide/