2025

PRACTICA 2.1: BASTIONADO DE UN DISPOSITIVO

IZAN NAVARRO LUJAN

13/11/2025

INDICE

1-Introducción:

En el mundo interconectado actual, la seguridad de los sistemas y dispositivos juega un papel fundamental para proteger la información y garantizar la continuidad de las operaciones en cualquier entorno profesional. El bastionado, o la implementación de medidas de seguridad para fortalecer un dispositivo, es una práctica esencial que permite reducir al mínimo los riesgos asociados a vulnerabilidades o configuraciones inseguras.

Esta práctica tiene como objetivo proporcionar a los alumnos una experiencia práctica completa en la implementación de estrategias de bastionado. A través de un enfoque progresivo y orientado a casos reales.

A lo largo de esta práctica, los alumnos adquirirán habilidades técnicas esenciales y comprenderán la importancia de adoptar un enfoque proactivo en la gestión de la seguridad informática. Esta actividad no solo fomenta la capacidad de análisis y resolución de problemas, sino que también prepara a los futuros profesionales para enfrentar los desafíos reales que encontrarán en el ámbito laboral.

Con esta práctica, se busca no solo aprender las técnicas necesarias para proteger un dispositivo, sino también desarrollar una mentalidad orientada a la seguridad y la mejora continua, principios fundamentales en el sector tecnológico. Requisitos Para esta práctica se necesitará:

- Un dispositivo Windows, a bastionar
- Un dispositivo Linux, para auditar la máquina a bastionar

Ejercicio 1: Análisis y evaluación de riesgo de nuestro equipo.

Analiza los riesgos que puede tener el dispositivo que vas a analizar dependiendo en el entorno en el que se vaya a utilizar, puedes utilizar el entorno de clase, tu trabajo, tu despacho o cualquier sitio que se te ocurra

2 riesgos que pueden afectar a nuestro dispositivo en un ambiente lectivo dentro de un aula podrían ser:

1.Acceso no autorizado: En un entorno de clase, es común que los equipos estén físicamente accesibles a varias personas, como compañeros de clase, personal de soporte o visitantes ocasionales.

Esto representa un riesgo significativo porque cualquier persona con acceso físico puede:

1. **Encender o reiniciar la máquina virtual** sin autorización.
2. **Acceder a archivos personales**, trabajos académicos o credenciales guardadas en el sistema.
3. **Manipular configuraciones de seguridad**, como contraseñas o servicios, que podrían debilitar la protección del equipo.

Para mitigar este riesgo podríamos:

- Configurar contraseñas fuertes para usuarios y BIOS.
- Limitar privilegios de usuarios locales (solo administrador para quien corresponda).
- Evitar dejar la máquina desatendida en horarios no vigilados.

2.Red Compartida: En la mayoría de los entornos de clase, los equipos están conectados a la misma red local (LAN). Esto facilita la comunicación entre dispositivos, pero también aumenta los riesgos de seguridad:

- **Exposición a malware o virus:** si un dispositivo de la red está infectado, puede propagarse fácilmente a otros equipos.
- **Ataques de red internos:** usuarios malintencionados podrían intentar explotar vulnerabilidades de Windows o de aplicaciones para acceder a otros equipos.
- **Intercepción de datos:** información transmitida por la red (archivos compartidos, credenciales, tráfico web) podría ser capturada por otros usuarios si no se protege adecuadamente.

Medidas de mitigación:

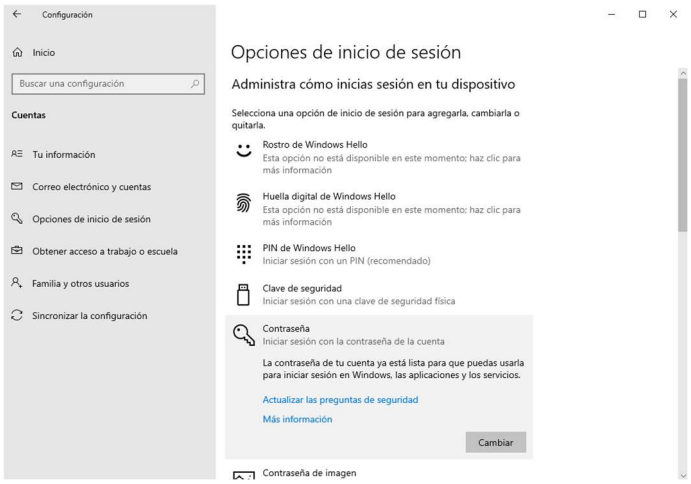
- Configurar un firewall que limite conexiones entrantes no autorizadas.
- Deshabilitar servicios innecesarios que escuchen en la red.
- Evitar compartir carpetas sin control de acceso.

Ejercicio 2: Uso de contraseña, protección de arranque y si es posible 2FA.

Quiero que me demuestres que el usuario para iniciar necesita una contraseña, averigua si es posible aplicar unos criterios mínimos de seguridad a esa contraseña. Además, quiero que investigues si es posible configurar el inicio de sesión con doble factor de autenticación y de ser así que opciones tenemos.

Comenta con tus palabras como configurarías una contraseña para la BIOS y como fortificarías el gestor de arranque del sistema operativo

Por defecto la Ova de Windows10 que he instalado te pone por defecto una contraseña “afi” junto a su usuario AFI. Pese a ello adjunto foto del sistema donde se confirma que hay una contraseña añadida y donde se podría cambiar:



Los criterios mínimos de seguridad de una contraseña son:

· 12 caracteres mínimo.

· Mezcla de mayúsculas, minúsculas, números y símbolos.

· No usar palabras comunes ni fechas de nacimiento.

Respecto al Inicio de sesión con doble factor (2FA), Windows 10/11 ofrece al usuario 3 métodos de inicio de sesión:

- Reconocimiento facial
- Huella Dactilar
- PIN

Primero, al encender el PC entró en la BIOS **presionando F2, DEL o ESC**, dependiendo del fabricante. Dentro configuraré una contraseña de administrador de BIOS, lo que significa que nadie podrá cambiar las opciones del sistema ni modificar el orden de arranque sin introducirla. Esto protege mi equipo de que alguien pueda entrar en la BIOS y modificarla

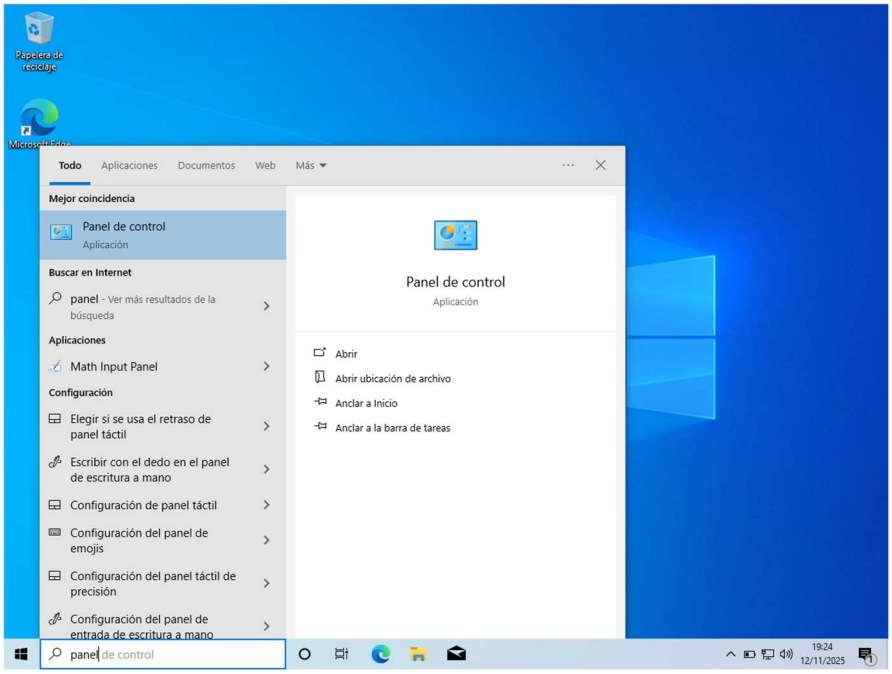
Luego, para fortalecer el gestor de arranque, activo la opción de arranque seguro **(Secure Boot).** Esta función se asegura de que solo se puedan cargar sistemas operativos y controladores que estén firmados y verificados, evitando que se ejecute software malicioso antes de que Windows inicie.

Además, **bloqueo el arranque desde USB o CD no autorizados**, de modo que nadie pueda iniciar el equipo con un dispositivo externo para copiar archivos, instalar malware o alterar la configuración.

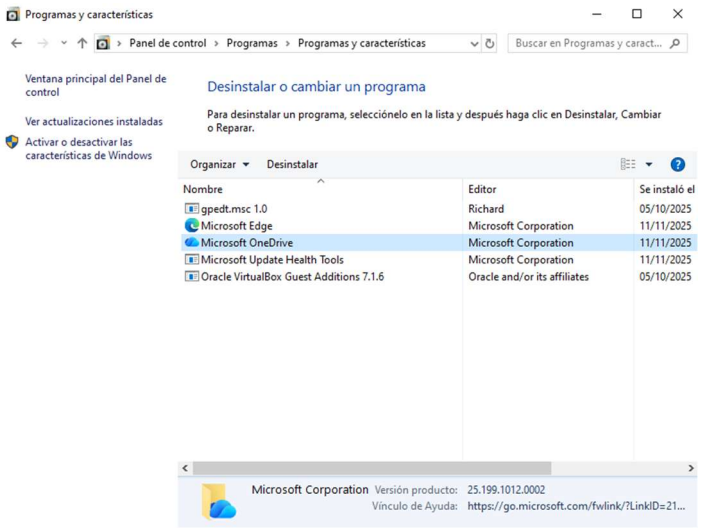
Ejercicio 3: Análisis y evaluación de riesgo de nuestro equipo.

Explica con tus palabras y adjuntado evidencias, como comprobarías las aplicaciones instaladas en tu dispositivo y como borrarías aquellas que no son necesarias.

1) Primero entraríamos dentro del Panel de control



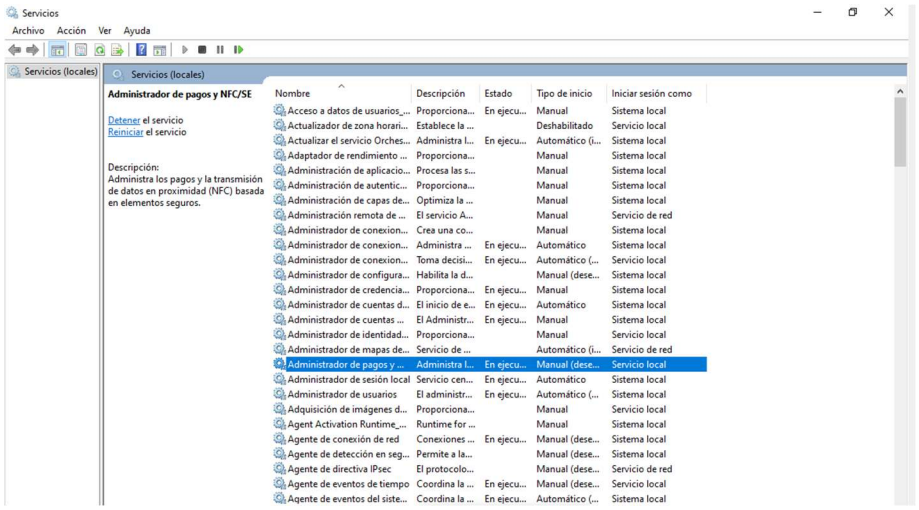
2) Entramos en Programas y Características y ahí tendremos todas las acciones con respecto a las apps:



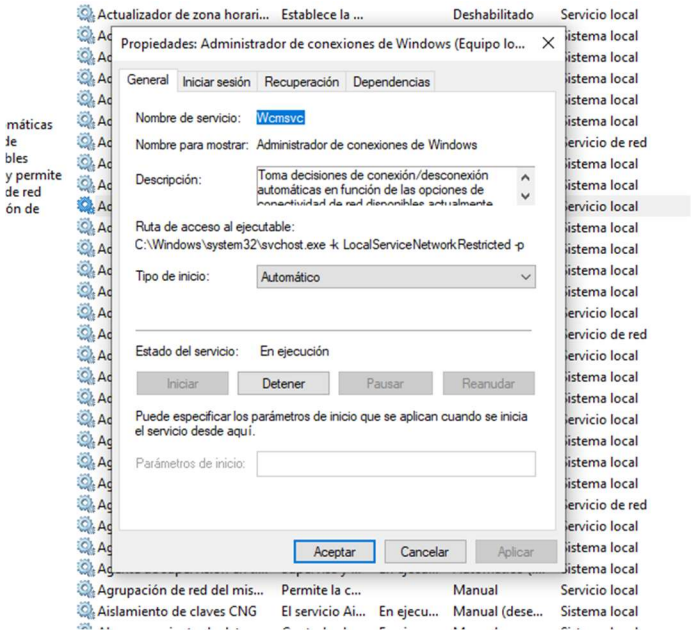
Ejercicio 4: Que servicios tenemos instalados y cuales no son necesarios.

Comprueba los servicios que están activos en tu sistema y explica como deshabilitarías aquellos que no son necesarios.

1. Primero entraremos dentro de “Win + R” y pondremos “services.msc”



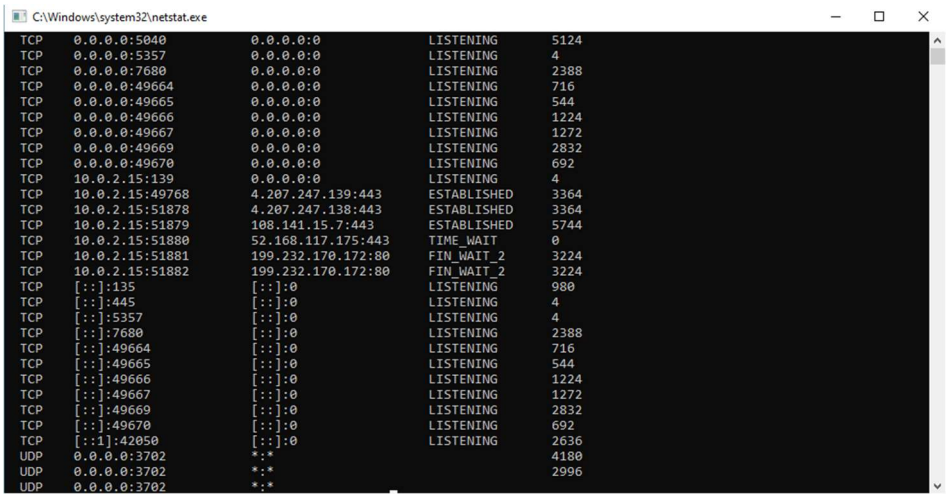
2. Después seleccionamos el servicio que queremos inspeccionar y pulsamos en “Propiedades”:



Ejercicio 5: Comprueba los puertos abiertos.

Realiza un escaneo de puertos a la máquina y comprueba los servicios que tiene abiertos

Para poder mostrar los procesos que están abiertos utilizamos “Win + R” y ponemos “netstat -ano” y nos mostrará en un terminal los puertos y sus identificadores:



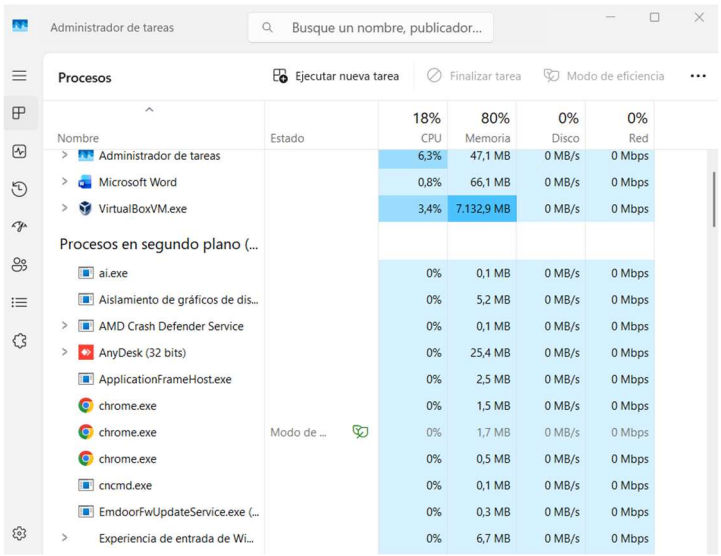
Ejercicio 6: Comprueba los puertos abiertos.

Una vez se han revisado los servicios y las aplicaciones, se supone que nuestro sistema es óptimo y está ejecutando sus tareas habituales, es buen momento para tomar una muestra del estado en el que se encuentras los recursos del sistema y tomarlo de referencia como el estado de referencia.

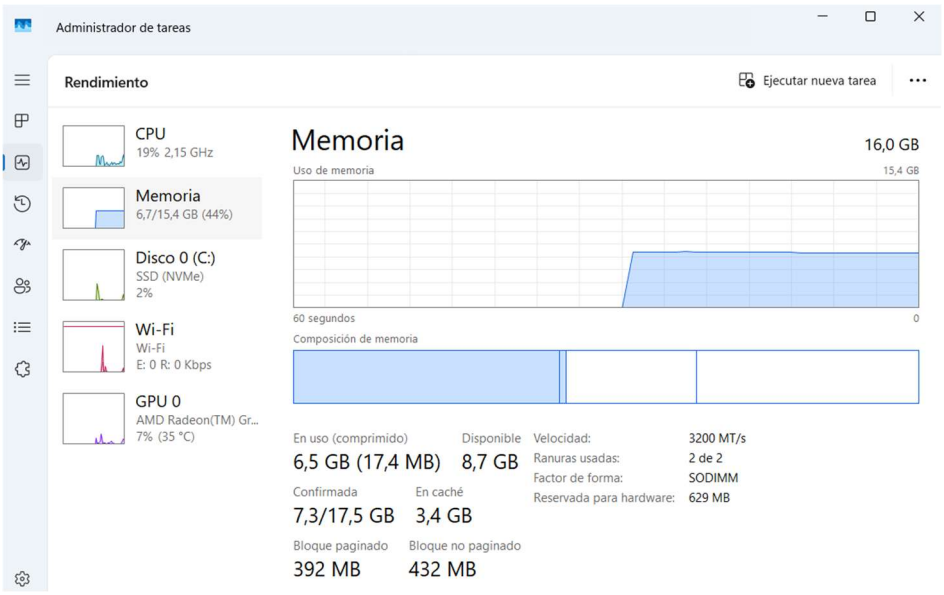
Explica con todo detalle el estado de los recursos del sistema, almacenamiento, CPU, RAM… Y explícame con tus palabras que limites le pondrías a los recursos para que generara una alerta y se considera umbrales peligrosos.

1) Para poder acceder a ver los recursos del sistema ejecutaremos “Ctrl + Alt + Del” para mostrarnos la opción de “Administrador de Tareas” y pulsarlo.

Se nos abrirá esta pestaña:



2) Para ver en más detalle todas estas características del PC le daríamos a la pestaña “Rendimiento” y se nos mostrarían los componentes del PC y su rendimiento actual:



3) Alertas dependiendo de cada componente del equipo y su rendimiento:

Para poder generar estas alertas podríamos utilizar una herramienta externa “Prometheus” la cual nos creará alertas (Windows: windows_exporter / wmi_exporter).

CPU

- **Advertencia (warning)**: uso sostenido > 75% durante 5 minutos.
- **Crítico (action)**: uso sostenido > 90% durante 2–5 minutos o cola de procesos (run queue) alta → investigar.

Memoria (RAM)

- **Warning**: uso > 75% o tasa de paginación creciente sostenida.
- **Crítico**: uso > 90% o page-faults/s elevada → riesgo de OOM o degradación.

Disco (espacio)

- **Warning**: uso >= 80% del volumen.
- **Crítico**: uso >= 95% del volumen → detener escritos no esenciales y limpiar; causa fallos y actualizaciones fallidas.
- Para discos del sistema, mantener al menos 10–20% libre o 10–20 GB (lo que sea mayor) para Windows Updates y VSS.

Temperatura / SMART

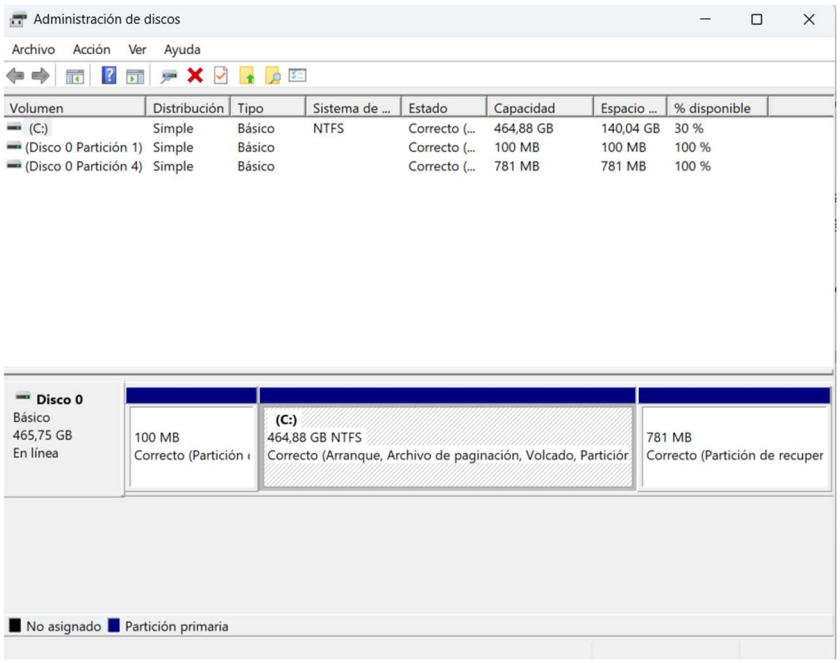
- **Warning**: CPU/GPU > 75°C.
- **Crítico**: > 90°C o SMART con atributos críticos.

Ejercicio 7: Particionamiento de discos.

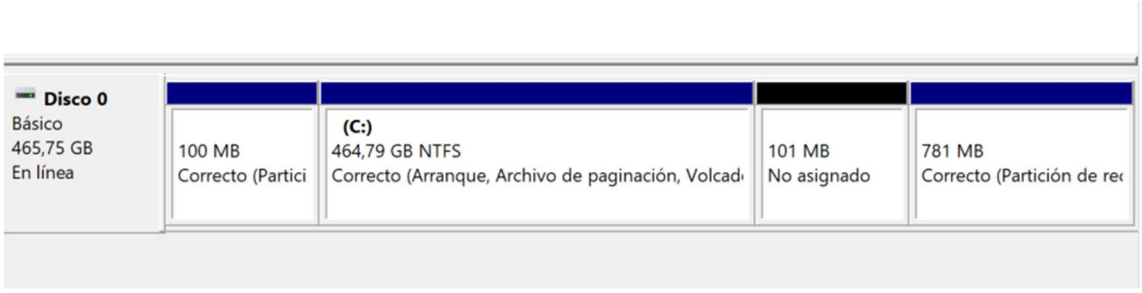
Muestra la configuración del disco y genera particiones, una para el sistema operativo, otra para albergar datos y otra partición destinada a una copia de seguridad. Si consideras alguna partición más que sea necesaria explícalo.

He tenido que hacer las particiones en mi Windows anfitrión ya que en el W11 de la VM no hay espacio de almacenamiento suficiente para poder crear 2 o más particiones.

1) Le damos a la tecla Windows y buscamos “Crear y Formatear particiones de discos” y se nos abrirá esta pestaña:



2) Para generar una partición elegimos el Disco Duro (C:) y le clickamos a “reducir volumen” y elegimos la cantidad de la nueva partición, en este caso “101MB”.



1 partición de 100MB para albergar datos, 1 partición de 101MB para copias de seguridad y 1 partición de 781MB para el S.O.

Ejercicio 8: Plan de copias de seguridad.

Explica como programarías un plan de copias de seguridad del sistema y que medidas tomarías para custodiar dichas copias de seguridad.

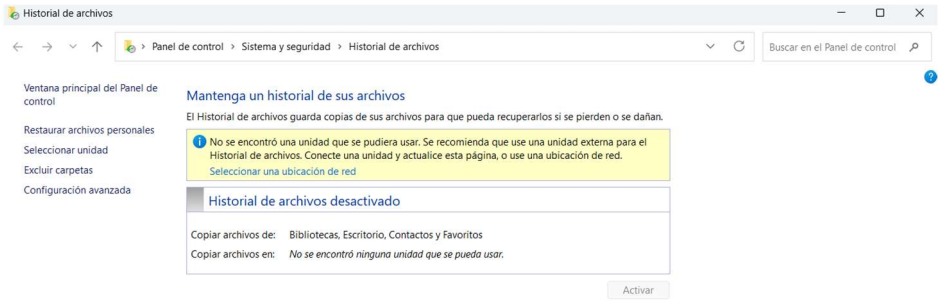
Para realizar un plan de copias de seguridad automáticas debe incluir:

· Copia completa del sistema (imagen)

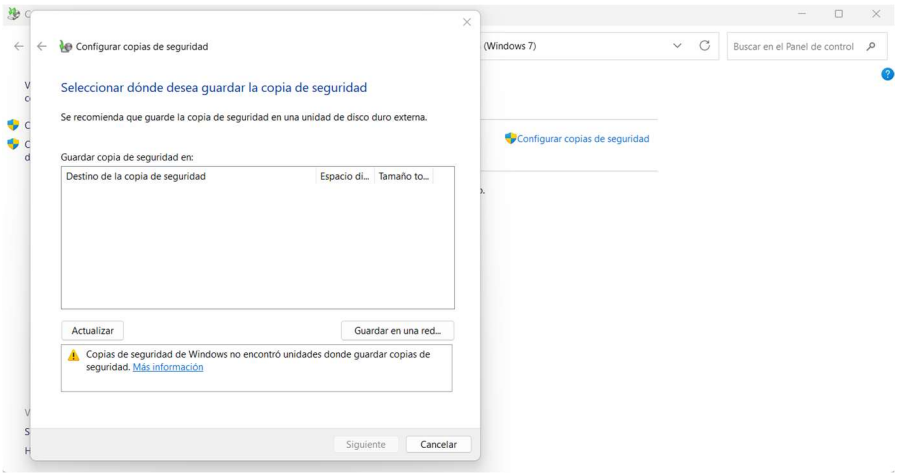
· Copias incrementales de ficheros

· Seguridad y custodia de las copias

1) Para poder hacer una copia de seguridad de manera gráfica por interfaz debemos pulsar la letra “Windows” y poner en el buscador “Historial de archivos”, una vez dentro nos saldrá esta pantalla y seleccionaremos el texto de abajo a la izquierda (copia de seguridad).



2) Una vez clickamos en “copia de seguridad de imagen del sistema” nos aparecerá una pestaña para seleccionar donde guardar este proceso:



3) Una vez puesto, le damos a siguiente y realizaríamos la copia de seguridad.

4) Si quisiéramos crear la imagen completa del sistema por comandos, usaríamos este comando en el servidor:

```
wbadmin start backup -backupTarget:E: -include:C: -allCritical -quiet
```

Para custodiar estas copias de seguridad usaría una serie de pautas o acciones:

1-Cifrado

2-Copias en Disco Externo

3-Control de acceso

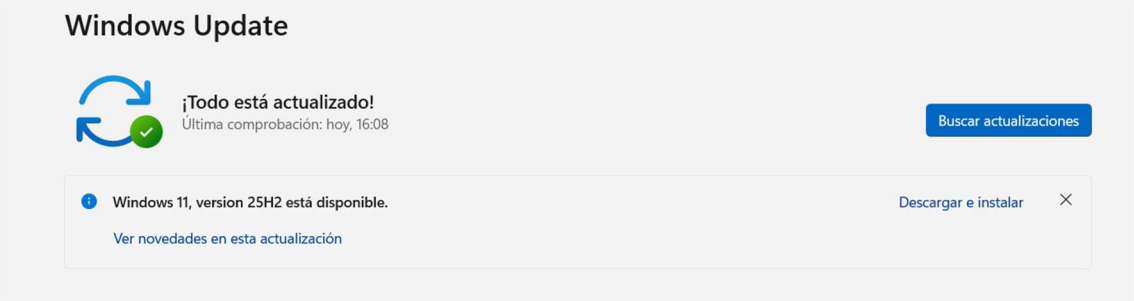
4-Registro de Backup en un log

5-Restauración

Ejercicio 9: Actualización del sistema.

Realiza una comprobación del sistema, averigua cuando Windows saca las actualizaciones y planifica la comprobación de actualizaciones periódicamente, para mantener el sistema actualizado. Explica la importancia de mantener el sistema actualizado

1) Para poder comprobar las actualizaciones del sistema tendremos que poner en el buscador de Windows “Buscar Actualizaciones” y clickamos:



2) Dándole a “Buscar Actualizaciones” se nos mostrarán todas las actualizaciones pendientes o opcionales por instalar.

3) Después tenemos las “Más opciones”: Pausar, Historial, Opciones Avanzadas, Windows Insider…

4) Mantener el sistema actualizado nos garantiza:

- Mayor Seguridad

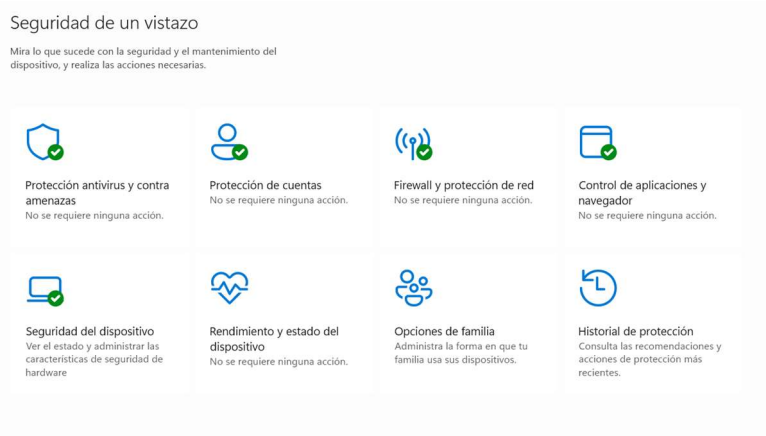
- Mayor Estabilidad y Compatibilidad

- Mejor Cumplimiento

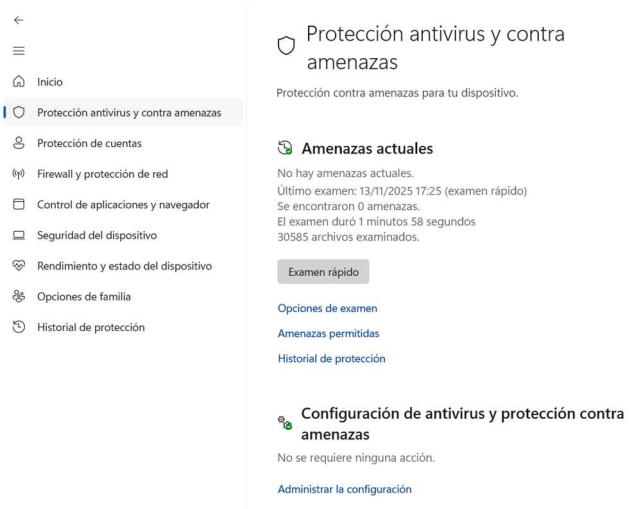
Ejercicio 10: Analiza el dispositivo con tu antivirus.

Una vez tenemos listo el dispositivo analiza las opciones que trae tu antivirus a la hora de lanzar un análisis. Lanza aquel que consideres oportuno y muestra los resultados

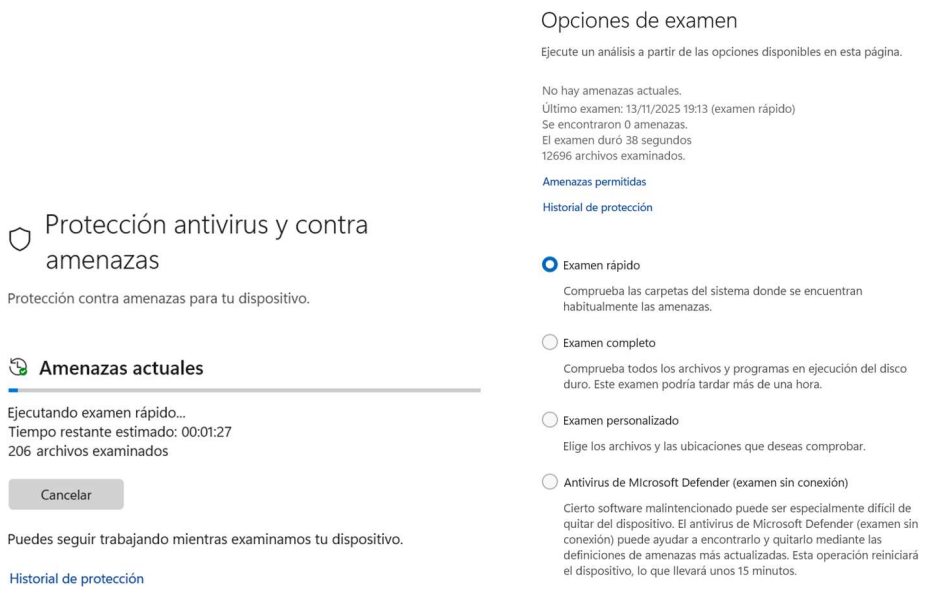
1) Para poder observar todo lo relacionado con la seguridad de nuestro dispositivo Windows debemos escribir en el buscador de W11 “Seguridad de Windows” y se nos abrirá esta pantalla:



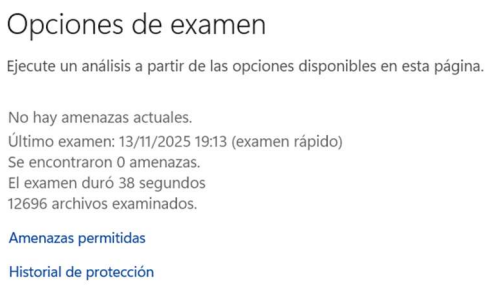
2) Entraremos dentro de “Protección antivirus y contra amenazas” y nos mostrará una pantalla así:



3) Aquí se nos detallarán todas las amenazas y configuraciones de nuestro antivirus junto con mucha más información relevante (Duración, último examen...) y también los tipos de examen de antivirus que podemos elegir. Igualmente volveremos a lanzar el examen dándole en este caso a “Examen rápido”:



4) Nos saldrán los resultados al acabar este análisis del equipo. Todo Correcto.



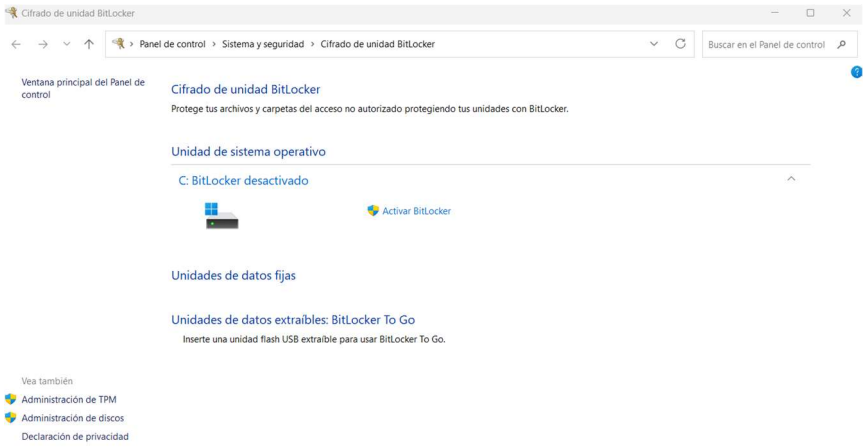
Ejercicio 11: Cualquier medida que consideres oportuna e interesante.

Explica cualquier medida adicional que consideres interesante para bastionar un dispositivo y por qué

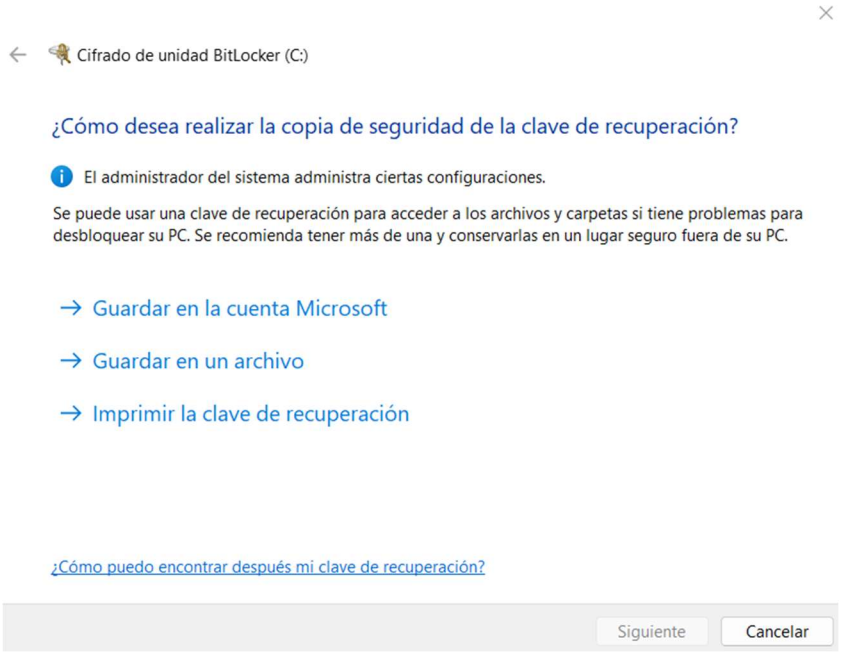
· BitLocker:

Para este punto voy a hablar de una herramienta de Windows llamada **“Bitlocker”,** la cual se encarga de cifrar el disco completo y cifrar sus datos en caso de robo, pérdida o acceso no autorizado al equipo.

1) Para poder acceder de forma gráfica a las opciones de Bitlocker debemos poner en el buscador de Windows “Administrar Bitlocker” y seleccionarlo:



2) Una vez dentro tendremos la opción de activar BitLocker y nos preguntará donde desearemos guardar la clave de recuperación de estos datos encriptados con la codificación EAS:



3) Por otro lado también podemos ejecutar todo esto por comandos:

"Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -UsedSpaceOnly"

Seleccionando "C:" para partir de nuestro disco duro para crear la imagen de cifrado con el método Aes256.

4) Conclusión de Bitlocker:

BitLocker ayuda a cumplir con políticas de seguridad corporativa y normativa legal (como GDPR o LOPDGDD), al evitar fugas de datos personales o sensibles. También se integra de forma nativa con Windows, lo que facilita su administración y uso sin necesidad de software adicional.

BitLocker refuerza la seguridad del sistema operativo y protege la información crítica del usuario o la empresa, siendo una de las medidas más efectivas para bastionar un dispositivo frente a

accesos no autorizados o ciberataques que busquen extraer datos desde el almacenamiento físico.