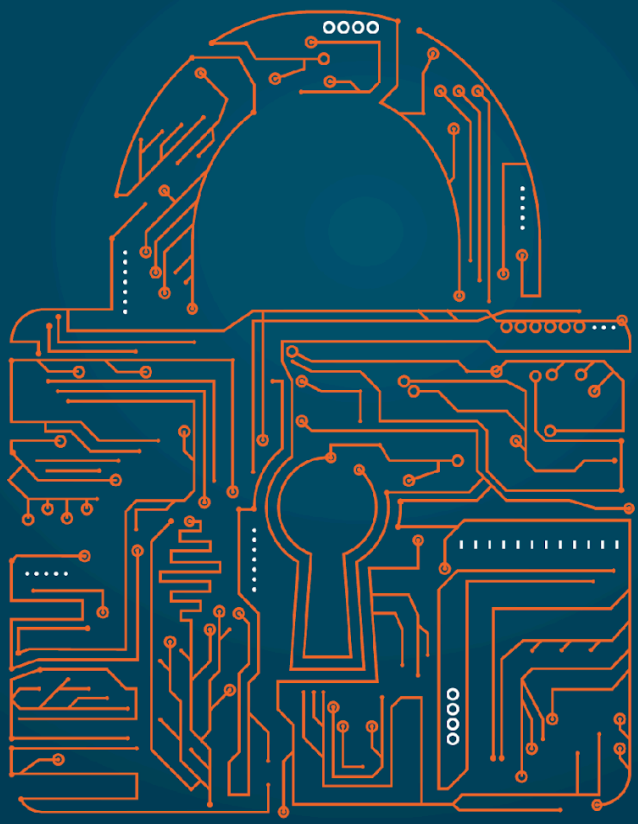
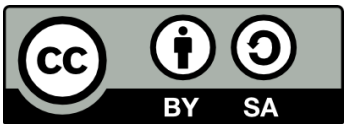
CONEXO



# GUÍA: CONFIGURACIÓN SEGURA DE WINDOWS DEFENDER Y MALWAREBYTES

**Edición:** Noviembre 2024




Esta obra está bajo una Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional.

# ÍNDICE


- ¿CUÁL ES EL CONTEXTO? 4
- CONCEPTOS BÁSICOS 4
- CARACTERÍSTICAS WINDOWS DEFENDER 5
- CARACTERÍSTICAS MALWAREBYTES 5
- CONFIGURACIÓN DE WINDOWS DEFENDER ANTIVIRUS 7
- CONFIGURACIÓN DE MALWAREBYTES ANTI-MALWARE 10
- REFERENCIAS 15

## ¿CUÁL ES EL CONTEXTO?

En organizaciones y personas que realizan su trabajo en contextos de alto riesgo, las amenazas digitales juegan un papel central, por lo que la protección de la información se convierte en una prioridad, ya que los ataques cibernéticos y las infecciones de malware pueden poner en peligro la seguridad de los datos y de los dispositivos utilizados en sus actividades.

Con el objetivo de brindar un apoyo eficaz en este contexto, es esencial no solo comprender los conceptos relacionados con la seguridad digital, sino también proporcionar herramientas prácticas para la protección de los dispositivos. En este sentido, el foco de esta guía será desarrollar un material que facilite la configuración de soluciones de seguridad, específicamente el **antivirus Microsoft Defender y el antimalware Malwarebytes.** Estas herramientas serán muy útiles para proteger la información en los dispositivos, evitando infecciones de malware que puedan comprometer la seguridad y la integridad de los datos.

## CONCEPTOS BÁSICOS

**ANTIVIRUS:** Un antivirus es un software diseñado para detectar, prevenir y eliminar programas maliciosos (malware), tales como virus, troyanos, gusanos y otras amenazas informáticas. Su principal función es proteger los dispositivos contra la infección por estos tipos de malware, detectando su presencia antes de que puedan causar daño al sistema o a la información almacenada. Los antivirus suelen realizar análisis periódicos en busca de amenazas conocidas y también incluyen mecanismos de protección en tiempo real, que monitorean el comportamiento de los archivos y programas para identificar posibles infecciones antes de que se propaguen.

**ANTIMALWARE:** el antimalware es una categoría más amplia de software de seguridad diseñado para identificar, prevenir y eliminar diversos tipos de malware, incluyendo no sólo virus, sino también spyware, ransomware, adware, rootkits y otros programas maliciosos. A diferencia del antivirus tradicional, el antimalware suele estar más enfocado en la protección contra malware más moderno o especializado, como los programas que pueden espiar, robar información sensible o cifrar archivos. Aunque los antivirus ofrecen protección básica contra muchas amenazas, el antimalware se enfoca en ofrecer una defensa más robusta y completa frente a una mayor variedad de amenazas.

Tanto el antivirus como el antimalware contribuyen a mantener la seguridad de los dispositivos, y el antimalware tiende a ser más específico en la detección y eliminación de amenazas más avanzadas y diversas.

## CARACTERÍSTICAS DE WINDOWS DEFENDER

**Microsoft Defender Antivirus** es una solución de seguridad integrada en el sistema operativo Windows, diseñada para proteger a los usuarios contra virus, malware, spyware y otras amenazas cibernéticas. Ofrece una capa de protección constante en tiempo real, sin necesidad de instalar software adicional. Al ser parte del sistema operativo, su integración y funcionamiento son eficientes y transparentes para el usuario.

**Características principales:**

- **Protección en tiempo real:** Microsoft Defender Antivirus ofrece protección continua contra virus, spyware, malware y otras amenazas. Monitorea el sistema en busca de actividades sospechosas y bloquea amenazas antes de que puedan infectar el dispositivo.

- **Análisis programado y manual:** Permite realizar análisis completos, rápidos o personalizados, que pueden configurarse para ejecutarse automáticamente en horarios específicos.

- **Integración con Windows:** Al estar integrado de manera nativa en Windows, Defender funciona de manera eficiente con otras funciones de seguridad del sistema operativo, como el firewall y la protección contra ransomware.

- **Actualizaciones automáticas:** El antivirus se actualiza automáticamente para detectar amenazas nuevas y mejorar continuamente la protección.

- **Protección contra ransomware:** Incluye funciones avanzadas para prevenir ataques de ransomware, como la "Protección de carpetas controladas", que bloquea el acceso no autorizado a archivos importantes.

- **Análisis en la nube:** Utiliza inteligencia artificial y análisis en la nube para detectar amenazas emergentes más rápidamente.

## CARACTERÍSTICAS DE MALWAREBYTES

**Malwarebytes** es un programa de seguridad avanzado diseñado para detectar y eliminar una amplia gama de malware, incluidos virus, ransomware, spyware, adware, troyanos y rootkits. A diferencia de los antivirus tradicionales, Malwarebytes se especializa en ofrecer protección contra amenazas más sofisticadas y complejas que podrían eludir otros sistemas de seguridad.

**Características principales:**

- **Protección contra una amplia gama de amenazas:** Malwarebytes detecta y elimina virus, ransomware, spyware, adware, rootkits y otros tipos de malware, proporcionando una defensa más completa que los antivirus tradicionales.

- **Escaneo y eliminación de malware avanzado:** Su tecnología de escaneo profundo es eficaz para detectar malware que puede ser pasado por alto por otros programas antivirus.

- **Protección en tiempo real:** Malwarebytes ofrece protección en tiempo real que bloquea amenazas automáticamente antes de que puedan infectar el sistema. Esto incluye la protección contra sitios web maliciosos y la vigilancia continua de procesos sospechosos.

- **Modo de recuperación:** En casos graves, Malwarebytes permite entrar en un "modo seguro" para realizar un análisis completo sin que el malware interfiera en el proceso.

- **Anti-ransomware:** Malwarebytes ofrece protección avanzada contra ransomware, identificando y bloqueando comportamientos típicos de estos ataques, como el cifrado de archivos.

- **Interfaz amigable:** La interfaz de Malwarebytes es fácil de usar, lo que facilita la ejecución de análisis y la gestión de la protección.

- **Compatibilidad con otros antivirus:** Malwarebytes puede instalarse junto con otros antivirus, proporcionando una capa adicional de seguridad sin interferir con el software existente.

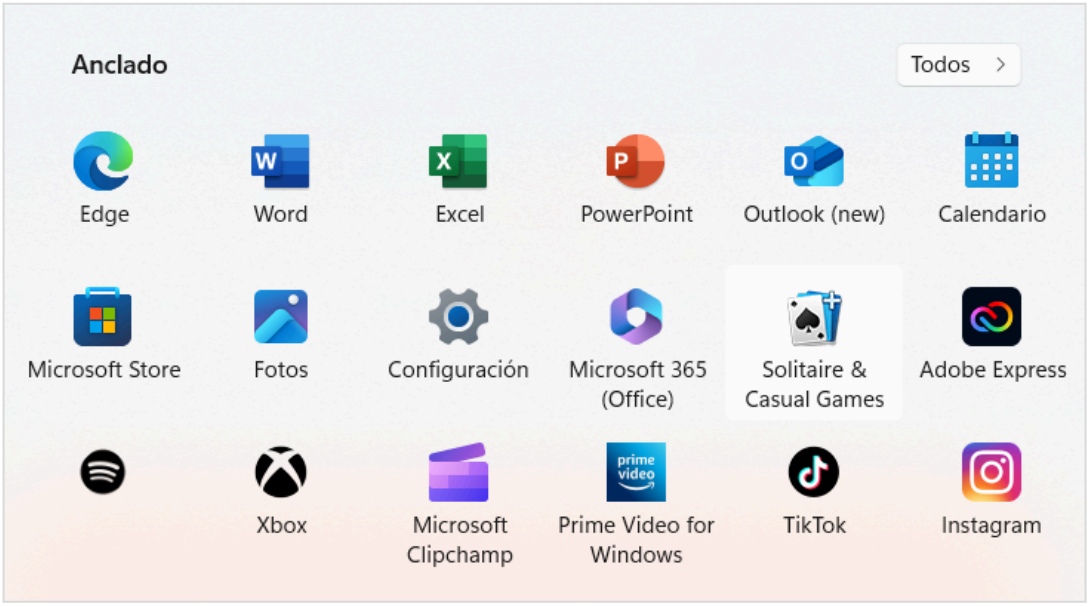
**Windows Defender** es una solución integrada en Windows, ideal para quienes necesitan protección básica, pero robusta, contra amenazas comunes. Su facilidad de uso y actualizaciones automáticas lo hacen una opción confiable para la mayoría de los usuarios. **Malwarebytes**, ofrece una protección más especializada, especialmente contra amenazas avanzadas como ransomware y spyware. Es una opción recomendada para usuarios que buscan una defensa más exhaustiva y centrada en amenazas más complejas.

Combinando **Windows Defender** y **Malwarebytes**, se obtiene una solución de seguridad más robusta y completa, que cubre una mayor variedad de amenazas. **Windows Defender** ofrece una base sólida de protección, mientras que **Malwarebytes** agrega una capa extra contra amenazas avanzadas que otros antivirus podrían no detectar. Juntas, estas herramientas proporcionan una defensa integral, especialmente importante en entornos con alto riesgo de infección, como los utilizados por organizaciones que manejan información sensible.

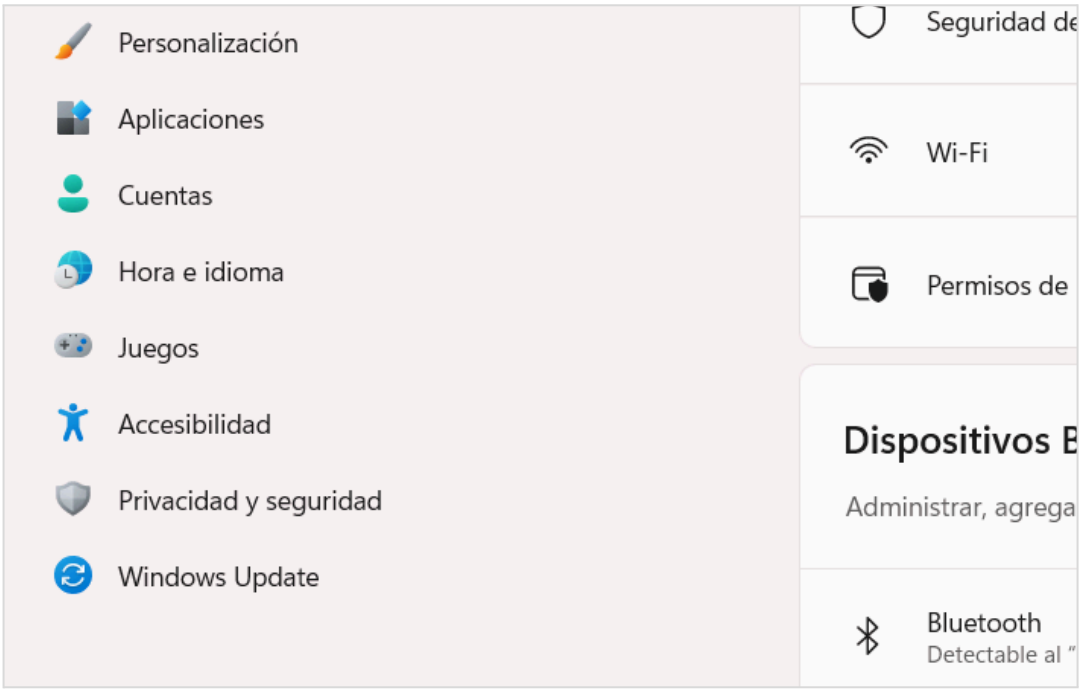
# CONFIGURACIÓN WINDOWS DEFENDER

1. En tu computadora con sistema operativo Windows, haz clic en el ícono de inicio

2. Haz clic en "**Configuración**"



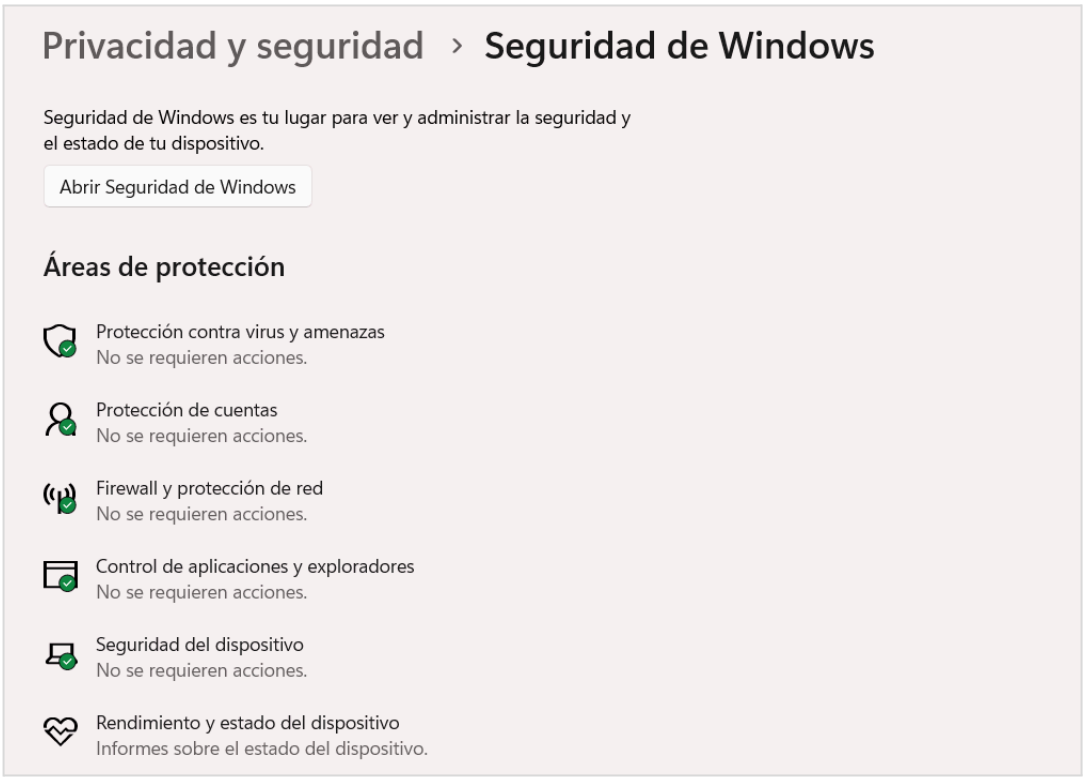

3. En el menú lateral izquierdo haz clic en "**Privacidad y seguridad**"



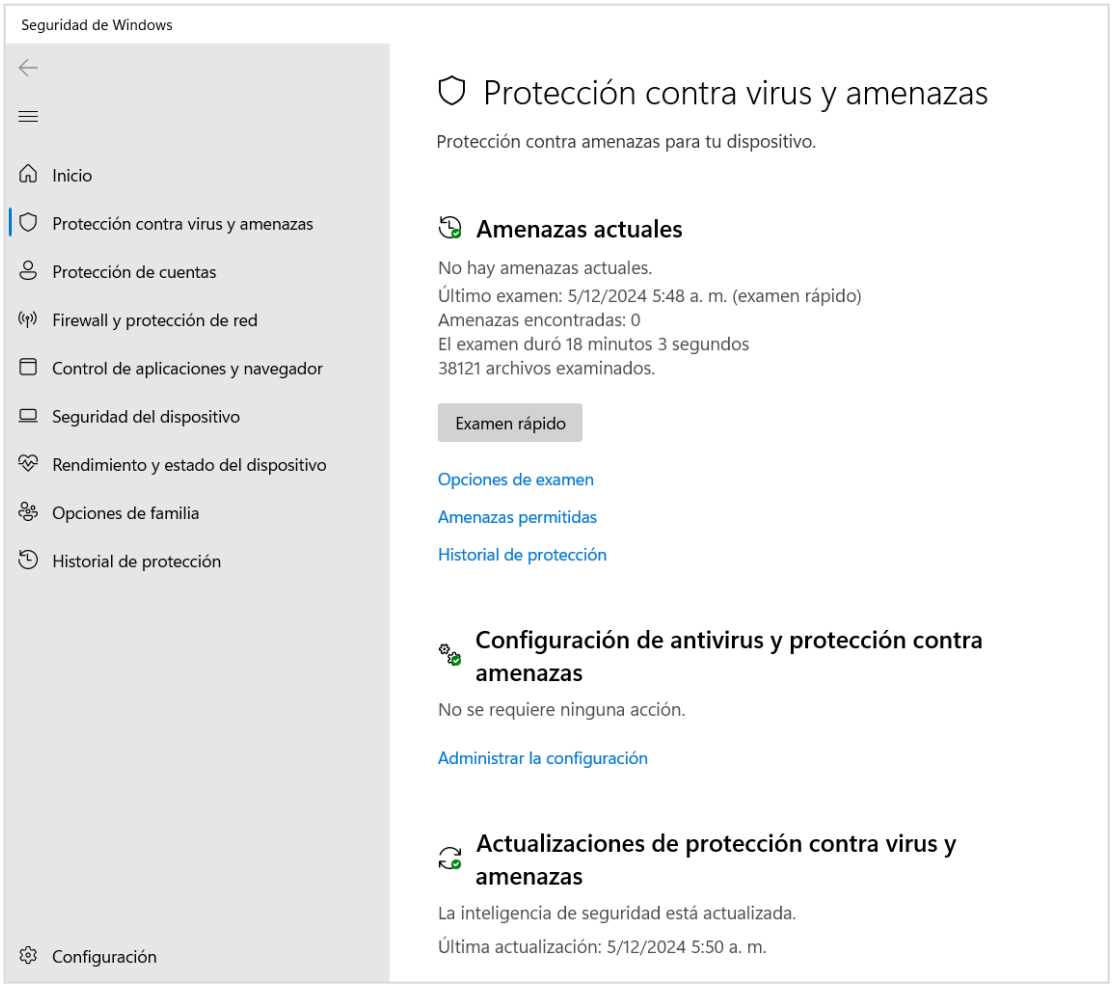
4. Haz clic en “**Seguridad de Windows**”




5. Selecciona “**Protección contra virus y amenazas**”



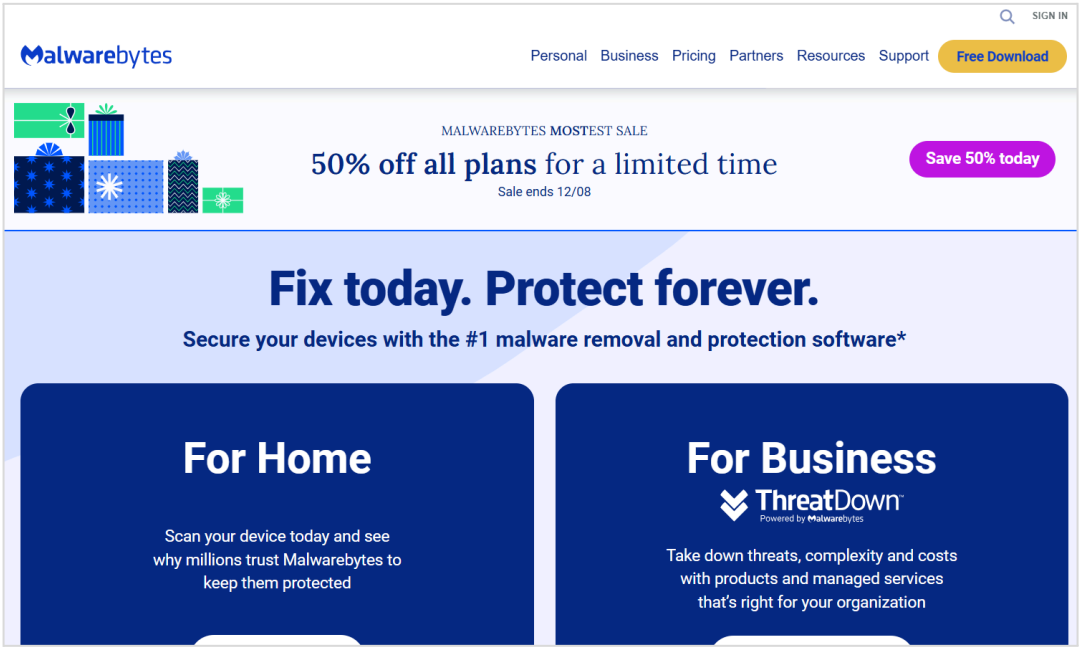
6. Verifica que esté **activo** el **Windows Defender** y que **no existan amenazas presentes**



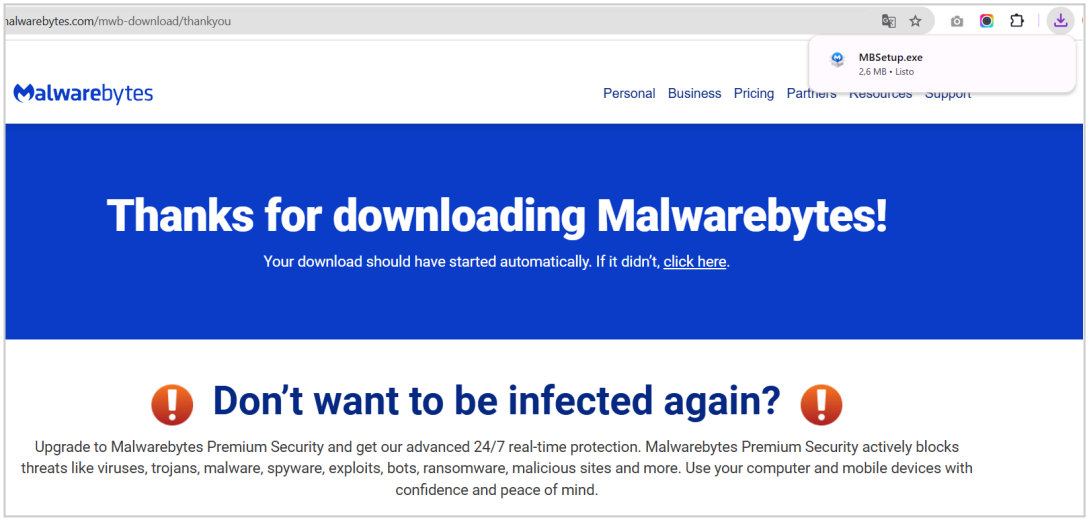
# CONFIGURACIÓN MALWAREBYTES

1. Navega al **sitio web oficial** de MalwareBytes: https://www.malwarebytes.com/

2. Haz clic en "**Free Download**"

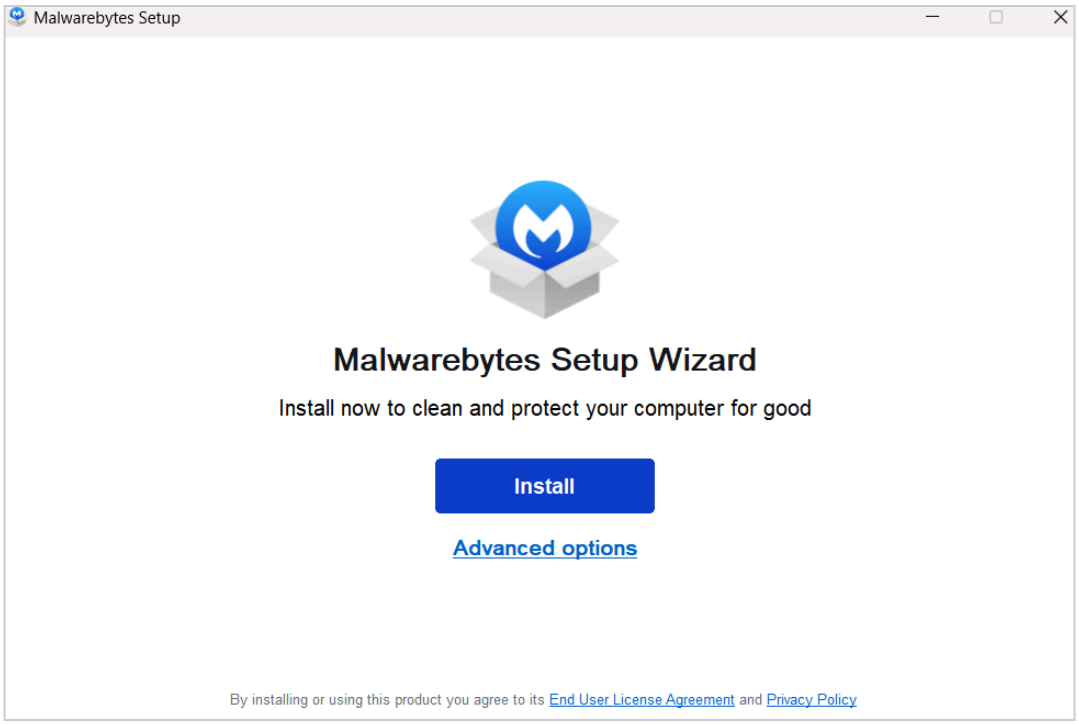



3. Automáticamente se descarga el archivo ejecutable para la instalación

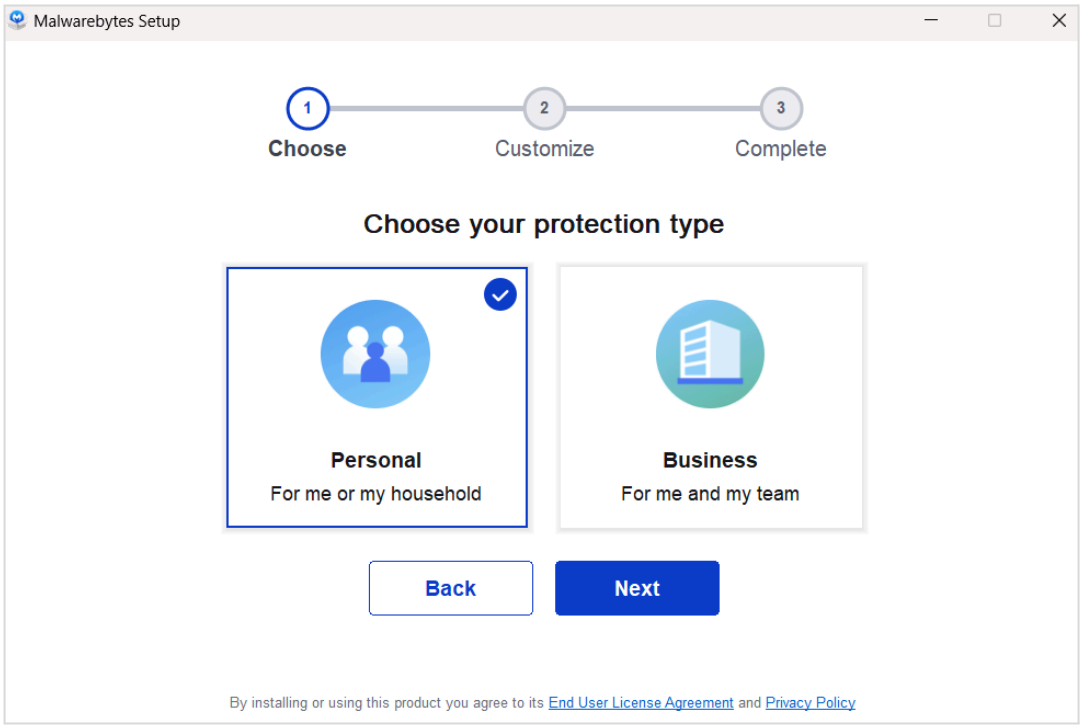



4. Abre el instalador y acepta los permisos de instalación, se abrirá la ventana del instalador de MalwareBytes.

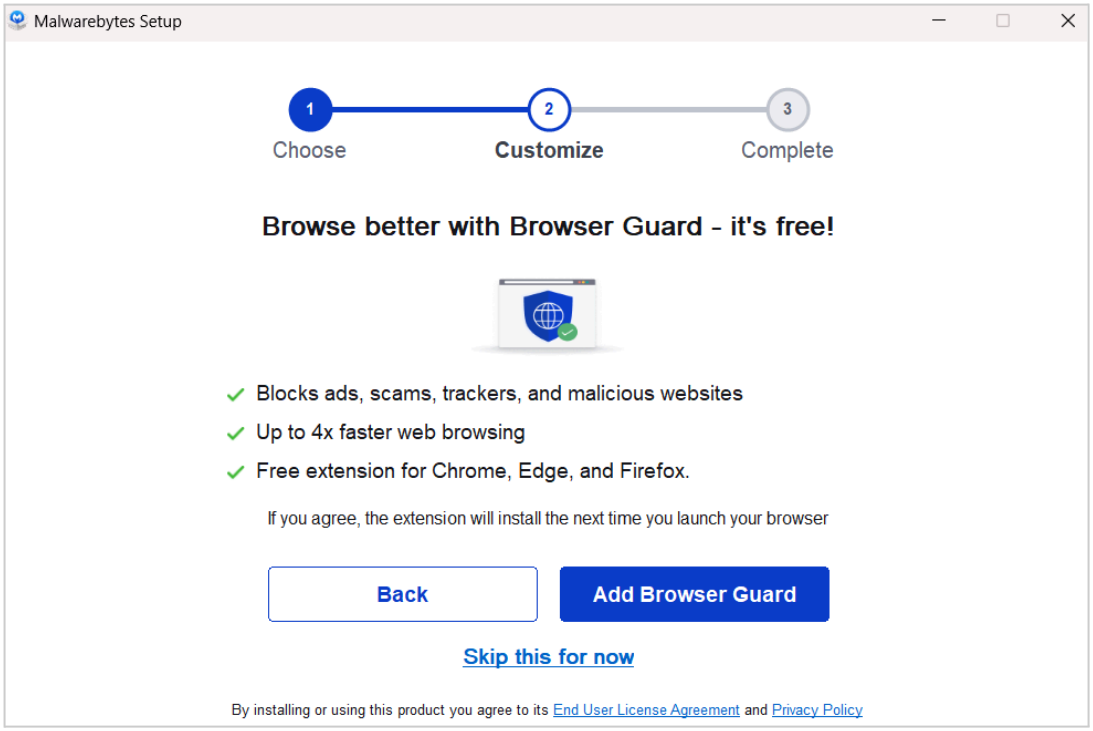
5. Haz clic en “**Install**”



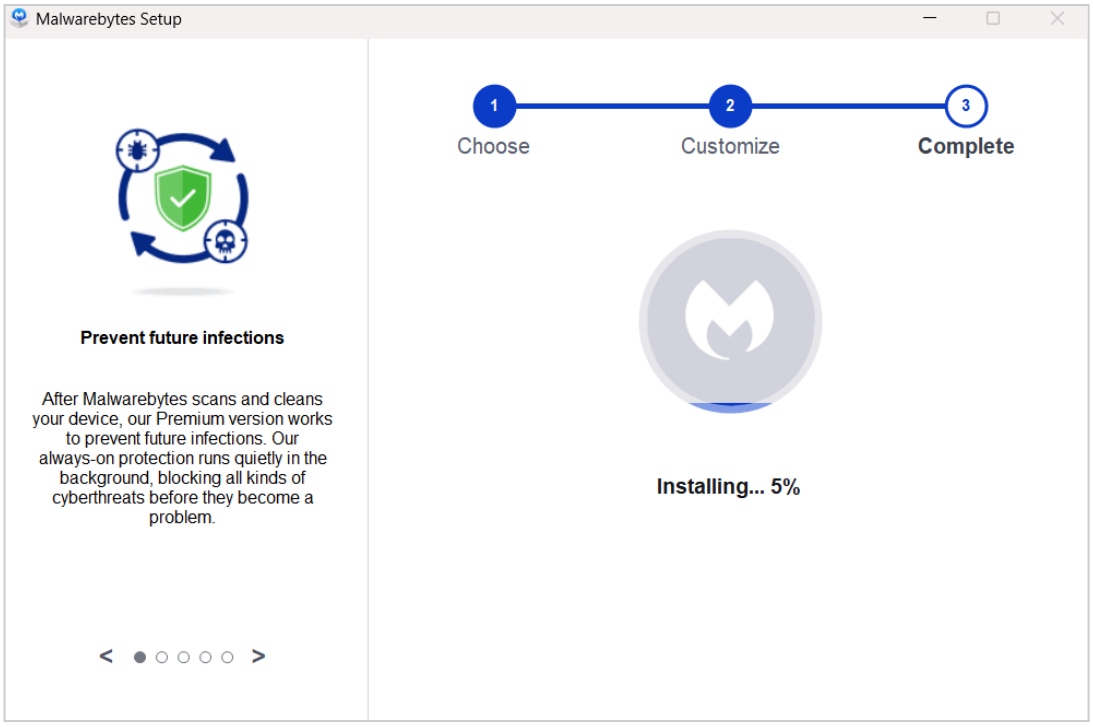

6. Selecciona el tipo de protección “**Personal**” y haz clic en “**Next**”



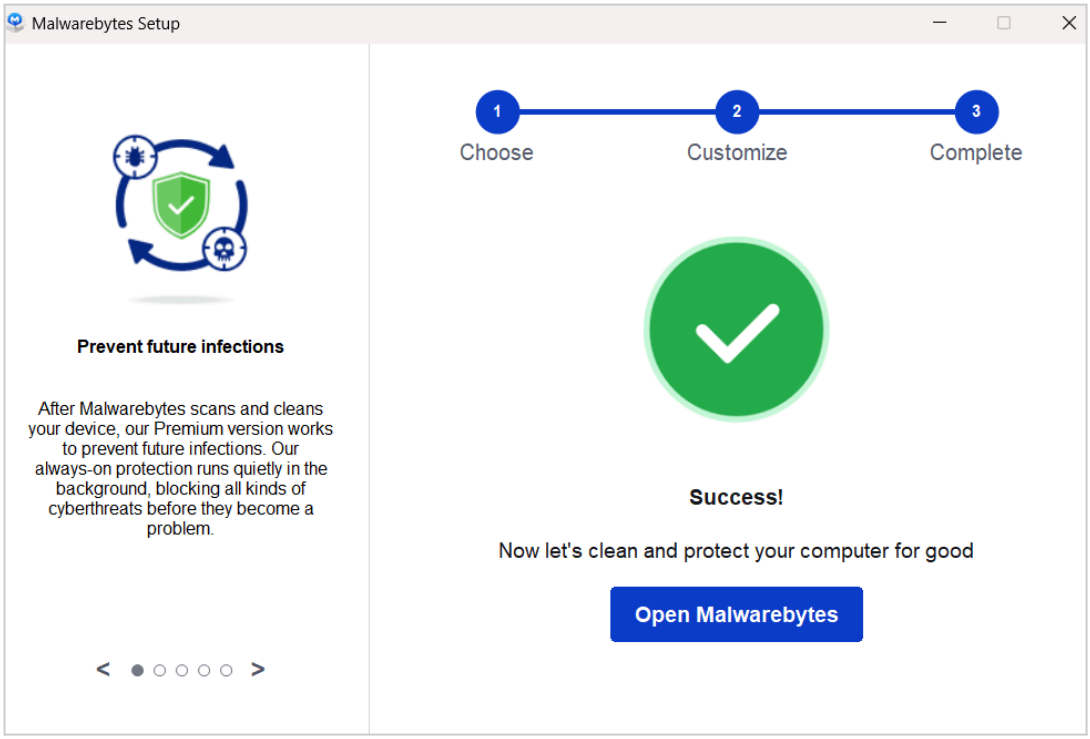

7. Haz clic en “**Skip for now**”



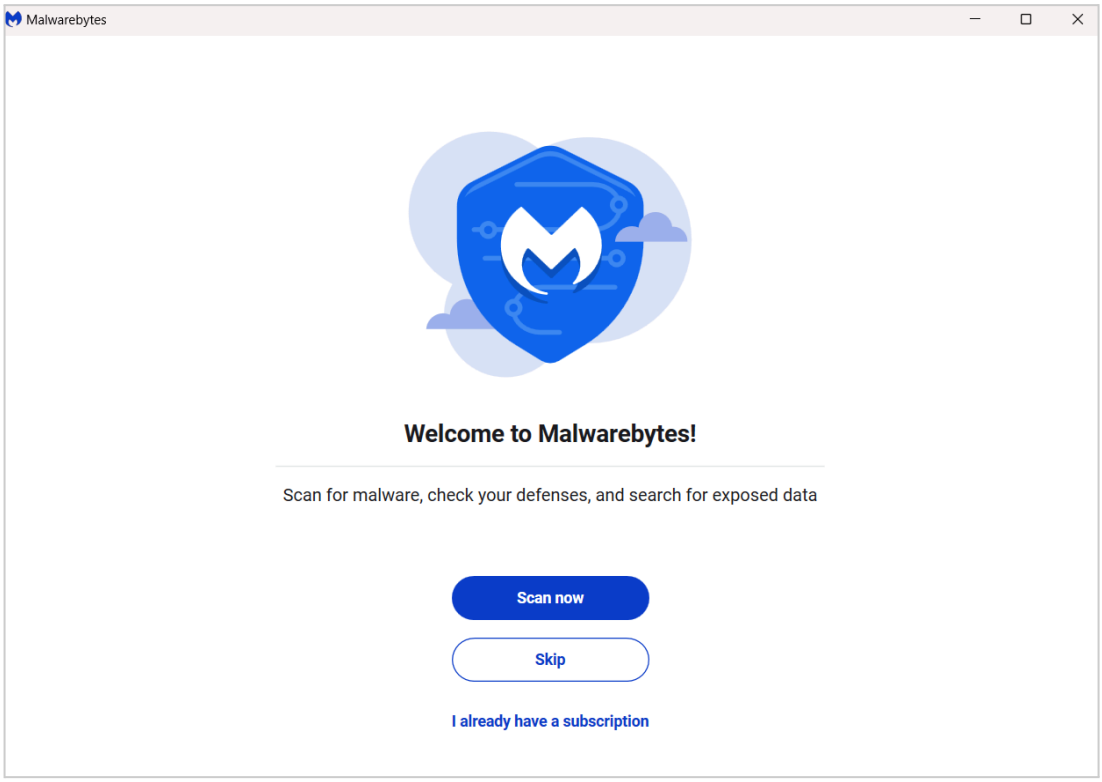

8. Espera a que culmine la instalación.



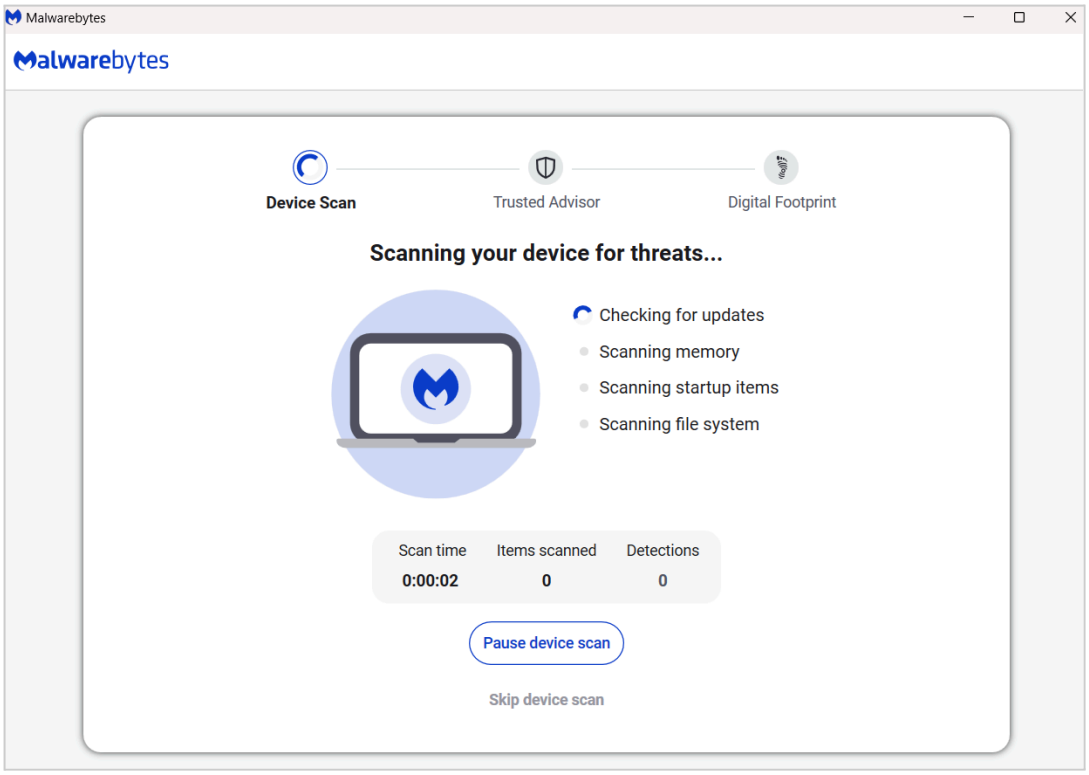

9. Al finalizar, haz clic en "**Open MalwareBytes**"




10. Haz clic en "**Scan now**"




11. Espera a que culmine el escaneo del MalwareBytes:




12. Una vez obtengas el resultado, revisa que no existan amenazas. Es recomendable repetir este proceso de escaneo cada cierto tiempo.

# REFERENCIAS


- Introducción a Microsoft Defender Antivirus en Windows. (n.d.). Microsoft.com. Retrieved December 5, 2024, from https://learn.microsoft.com/es-es/defender-endpoint/microsoft-defender-antivirus-windows

- (N.d.). Malwarebytes.com. Retrieved December 5, 2024, from https://support.malwarebytes.com/hc/en-us/articles/360038984693-Malwarebytes-for-Windows-v4-guide