





Antivirus

En caso que tu antivirus no te permitiera instalar KLARWAY, puedes darle el permiso de manera manual. Esta acción se conoce como "establecer excepciones". Para ello, debes agregar a la lista de excepciones la URL o Carpeta que desees.

A continuación, te brindamos el paso a paso para realizar esta acción de permiso, en los antivirus más comunes: AVAST, McAfee, Norton, Windows Defender y Kaspersky.

En caso que tu antivirus no se encuentre en esta lista, podrás buscar cómo hacerlo en tu explorador de la siguiente manera: "establecer excepciones en antivirus XXX (colocar el nombre del antivirus)" o "excluir un archivo del análisis en XXX (colocar el nombre del antivirus)"

ÍNDICE:

AVAST	4
McAfee	9
Norton	12
Windows Defenser	16
Kaspersky	20





 Asegurate de que esté seleccionada la pestaña General y hacé clic en Excepciones.





• Hacé clic en el botón Añadir una excepción.



Las excepciones se pueden agregar de varias formas:



a) Escribí la ruta del archivo, de la carpeta o la URL en el cuadro de texto y luego hacé clic en Añadir una excepción.

b) Hacé clic en Examinar, marcá la casilla que hay junto al archivo o la carpeta que deseas agregar a la lista de excepciones y, a continuación, hacé clic en Aceptar.



	×				
on					
able file, or MIME	type				
or browse local	tion				
	Select the areas				×
	Desktop Documents	ualBox Guest Additions			~
	Selected paths:				
			OK	Canor	•



HADRANGE MARKET MARKET MARKET AND MARKET AN



1. Abrí el software de seguridad de McAfee. 2. Hacé clic en PC Security (en Windows) o Mac Security (en macOS). 3. Hacé clic en Real-Time Scanning (Análisis en tiempo real). 4. Hacé clic en Excluded Files (Archivos excluidos). 5. Hacé clic en Add file (Agregar archivo). 6. Localizá y seleccioná el archivo que deseas excluir de los análisis. 7. Repetí el proceso para excluir de los análisis otros archivos.

El Análisis en tiempo real no analizará los archivos seleccionados después de llevar a cabo estos pasos.



Extraído de:



D MCAfee Together is power.



- Iniciá Norton.
- Si ves la ventana de Mi Norton junto a Seguridad del dispositivo, hacé clic en Abrir.
- En la ventana principal de Norton, hacé clic en Configuración.
- En la ventana Configuración, hacé clic en Antivirus.
- En la ventana de configuración Antivirus, hacé clic en la ficha Análisis y riesgos.
- En Exclusiones/Riesgos de seguridad bajos, realizá una de las siguientes acciones:
 - En la fila Elementos que se deben excluir del análisis, hacé clic en Configurar.
 - En la fila Elementos que se deben excluir de la detección de Auto-Protect, Control de scripts, SONAR e Inteligencia sobre descargas, hacé clic en Configurar.

- En la ventana que aparece, hacé clic en Agregar carpetas o Agregar archivos.
- Podés asignar exclusiones a unidades locales, carpetas, grupos de archivos, archivos individuales o unidades de red.
- En el cuadro de diálogo Agregar elemento, hacé clic en el icono de navegación.
- En el cuadro de diálogo que aparece, seleccioná el elemento que desea excluir del análisis.
- Cuando agregues carpetas, podés especificar si deseas incluir o excluir subcarpetas.
- Hacé clic en Aceptar.
- En el cuadro de diálogo Agregar elemento, hacé clic en Aceptar.
- En la ventana que aparece, hacé clic en Aplicar y, luego, en Aceptar.





Extraído de:

NortonLifeLock⁻

PERMITIR INSTALACIÓN:

Windows Defender



• Ir a INICIO y seleccioná CONFIGURACIÓN



• En el cuadro de búsqueda seleccioná FIREWALL Y PROTECCIÓN DE RED.



H: 🗐 🗷 🕽 🔯 🜈 🌍 😰 🥃 🛷 👘 🥰 🌣 Q



- 0 \times

Internet y red Wi-Fi, modo avión, VPN



Barra de juegos, DVR, difusión.



colores

Narrador, lupa, contraste alto



- Seleccioná CONTROL DE APLICACIONES Y EXPLORADOR
- En la sección COMPROBAR APLICACIONES Y ARCHIVOS seleccioná la opción DESACTIVADO.
 - Centro de seguridad de Windows Defender ← \equiv Protección contra virus y amenazas Protección de cuentas Q (p) Firewall y protección de red Control de aplicaciones y explorador Seguridad del dispositivo Rendimiento y estado del dispositivo S A Opciones de familia

Control de aplicaciones y explorador

Configura SmartScreen de Windows Defender para aplicaciones y exploradores.

Comprobar aplicaciones y archivos

SmartScreen de Windows Defender ayuda a proteger el dispositivo mediante la comprobación de de aplicaciones y archivos no reconocidos en Internet.

O Bloquear O Advertir

Desactivado

Declaración de privacidad

SmartScreen para Microsoft Edge

ORADOR CHIVOS seleccioná la

- 0 >

• Regresa a instalar Klarway nuevamente.

IMPORTANTE:

Cuando termines de instalar y ejecutar Klarway, debes volver a activar el firewall. Realizá los mismos pasos y en COMPROBAR APLICACIONES Y ARCHIVOS seleccioná la opción ADVERTIR

kaspersky



- Abrí la ventana de configuración de la aplicación.
- En la parte izquierda de la ventana, en la sección Configuración general, seleccioná Exclusiones. La configuración de las exclusiones se mostrará en la parte derecha de la ventana.
- En la sección Exclusiones de análisis y aplicaciones de confianza, hacé clic en el botón Configuración. Se abrirá la ventana Zona de confianza en la pestaña Exclusiones del análisis.
- Hacé clic en el botón Agregar. Se abrirá la ventana Exclusión del análisis. En esta ventana, podrás crear una exclusión de análisis con el o los criterios de la sección Propiedades.

- Para excluir un archivo o una carpeta del análisis:
 - En la sección Propiedades, selecciona la casilla de verificación Archivo o carpeta.
 - Hacé clic en el enlace Seleccionar archivo o carpeta de la sección Descripción de la exclusión del análisis para abrir la ventana Nombre de archivo o carpeta.
 - Introduce el archivo o el nombre de la carpeta, o bien la máscara del archivo o del nombre de carpeta. También podés seleccionar el archivo o carpeta en el árbol de carpetas haciendo clic en Examinar.

- Especificá los componentes de Kaspersky Endpoint Security que van a emplearse en la exclusión del análisis:
 - Hacé clic en el enlace Todos de la sección Descripción de la exclusión del análisis para abrir el enlace Seleccionar componentes.
 - Hacé clic en el enlace Seleccionar componentes para abrir la ventana Componentes de protección.
 - Seleccioná las casillas de verificación situadas junto a los componentes a los cuales se debe aplicar la exclusión del análisis.
 - En la ventana Componentes de protección, hacé clic en Aceptar.

*Si se especifican los componentes en la configuración de la exclusión del análisis, dicha exclusión se aplica solo durante el análisis realizado por estos componentes de Kaspersky Endpoint Security. *Si no se especifican los componentes en la configuración de la exclusión del análisis, dicha exclusión se aplica durante el análisis realizado por todos los componentes de Kaspersky Endpoint Security.

- En la ventana Exclusión del análisis, hacé clic en Aceptar.
- La exclusión del análisis que agregaste aparecerá en la tabla en la pestaña Exclusiones del análisis de la ventana Zona de confianza. Los parámetros configurados de esta exclusión del análisis aparecen en la sección Descripción de la exclusión del análisis.
- En la ventana Zona de confianza, hacé clic en Aceptar.
- Para guardar los cambios realizados, hacé clic en el botón Guardar.



Extraído de:

