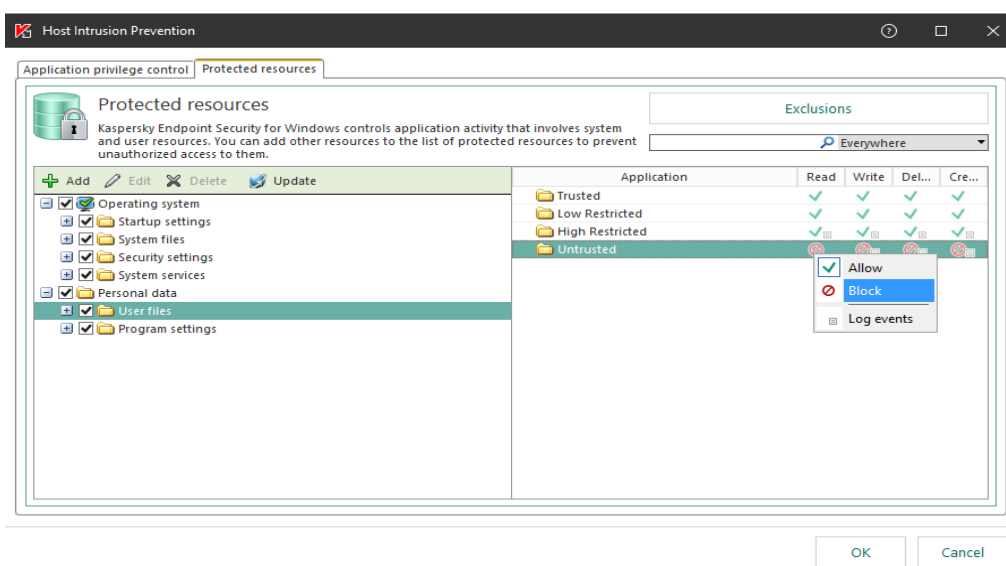


EXCLUIR APLICACIONES EN EL MODULO DE PREVENCION DE INTRUSIONES EN EL HOST

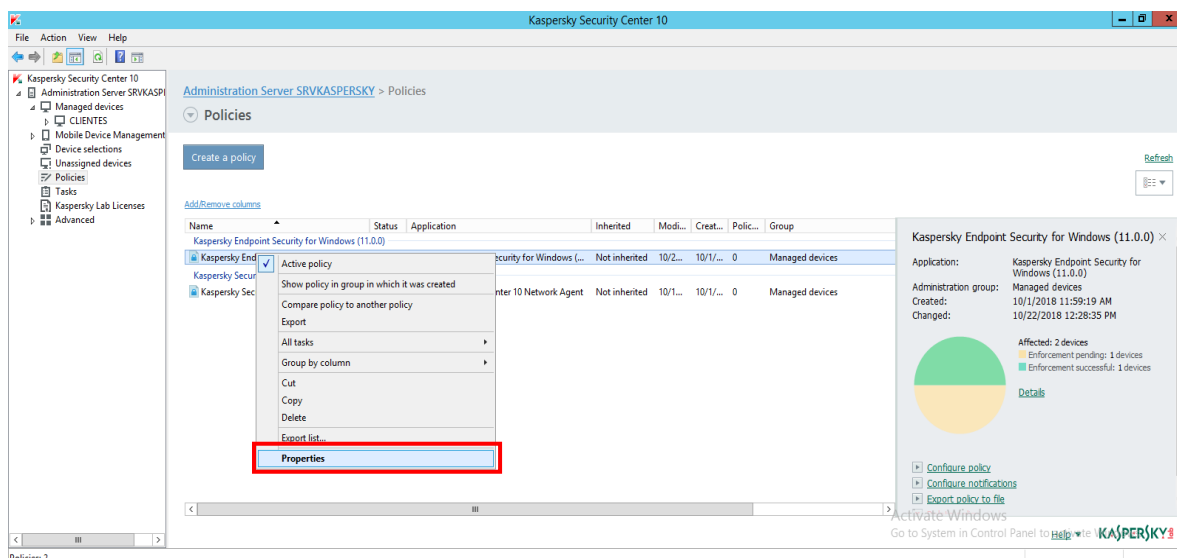
Para proteger archivos (por ejemplo, “Documentos” para archivos con extensión *.doc , *.docx, *.jpg, *.dbs, *.xls, *.xlsx *.ppt, *.pptx, etc).

Esta configuración protege los archivos con estas extensiones para que no puedan ser modificadas por aplicaciones catalogadas según Kaspersky como aplicaciones que no son de confianza.



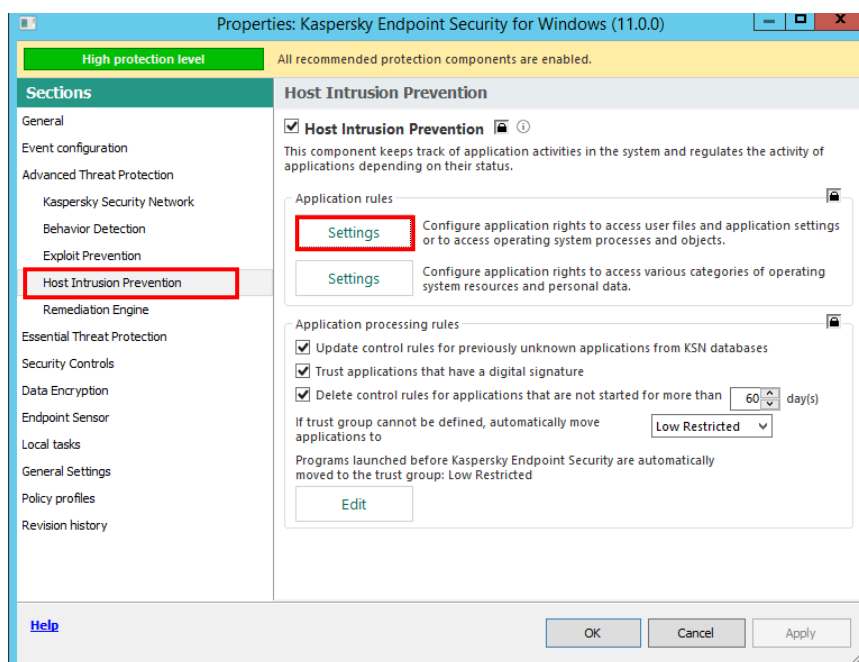
El procedimiento adjunto es para agregar una aplicación confiable del cliente que Kaspersky no ha catalogado como tal.

- Diríjase a las propiedades de la directiva donde desea realizar los cambios que estén trabajando los equipos de la versión que corresponda.

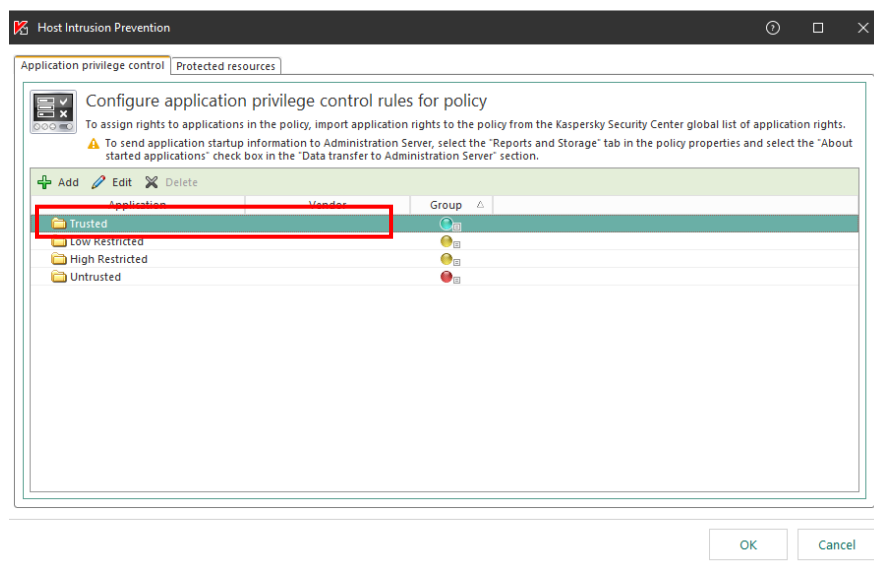


Luego ir a la Sección “Protección de Amenazas Avanzadas” y seleccionar el módulo “Prevención de Intrusiones en el Host”, verificar que se encuentra activada

Seleccionar la opción de “Configurar Reglas de Control (primera opción).”

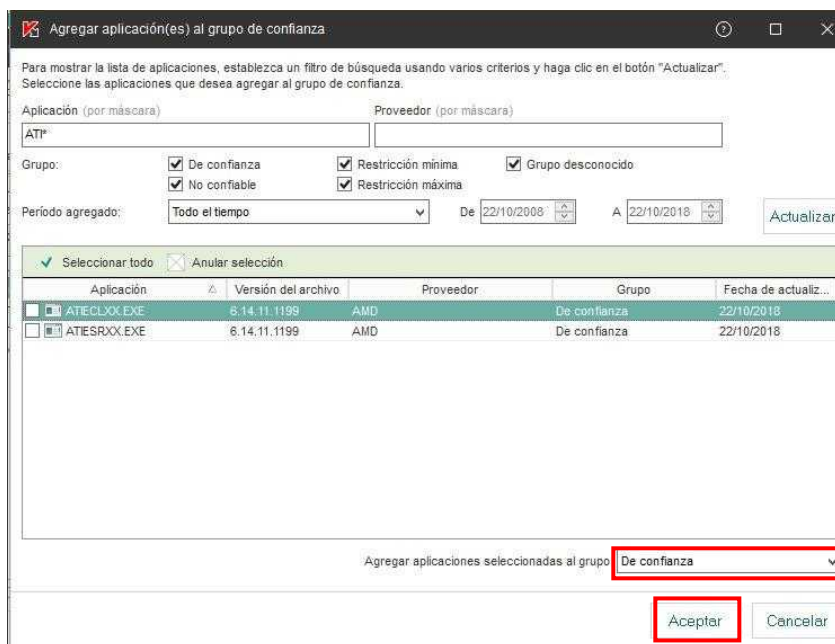


- Ir a “Control de Actividad de Aplicaciones” : Luego seleccionar la carpeta “De Confianza” seguido dar en “Agregar”



- Ingresar el nombre de la aplicación a excluir (como mascara)

Luego una vez hecho el filtro seleccionar todas las aplicaciones que muestren en el resultado y verificar que se agreguen al grupo de Confianza.



Para mostrar la lista de aplicaciones, establezca un filtro de búsqueda usando varios criterios y haga clic en el botón "Actualizar".
Seleccione las aplicaciones que desea agregar al grupo de confianza.

Aplicación (por máscara) Proveedor (por máscara)

Grupo: ☒ De confianza ☒ Restricción mínima ☒ Grupo desconocido
☒ No confiable ☒ Restricción máxima

Periodo agregado: De A

☒ Seleccionar todo ☐ Anular selección

Aplicación	Versión del archivo	Proveedor	Grupo	Fecha de actualiz...
<input checked="" type="checkbox"/> ATECLXX.EXE	6.14.11.1199	AMD	De confianza	22/10/2018
<input type="checkbox"/> ATESRXX.EXE	6.14.11.1199	AMD	De confianza	22/10/2018

Agregar aplicaciones seleccionadas al grupo

Finalmente aplicar los cambios y realizar las pruebas para validar que esté trabajando de manera correcta la política configurada.