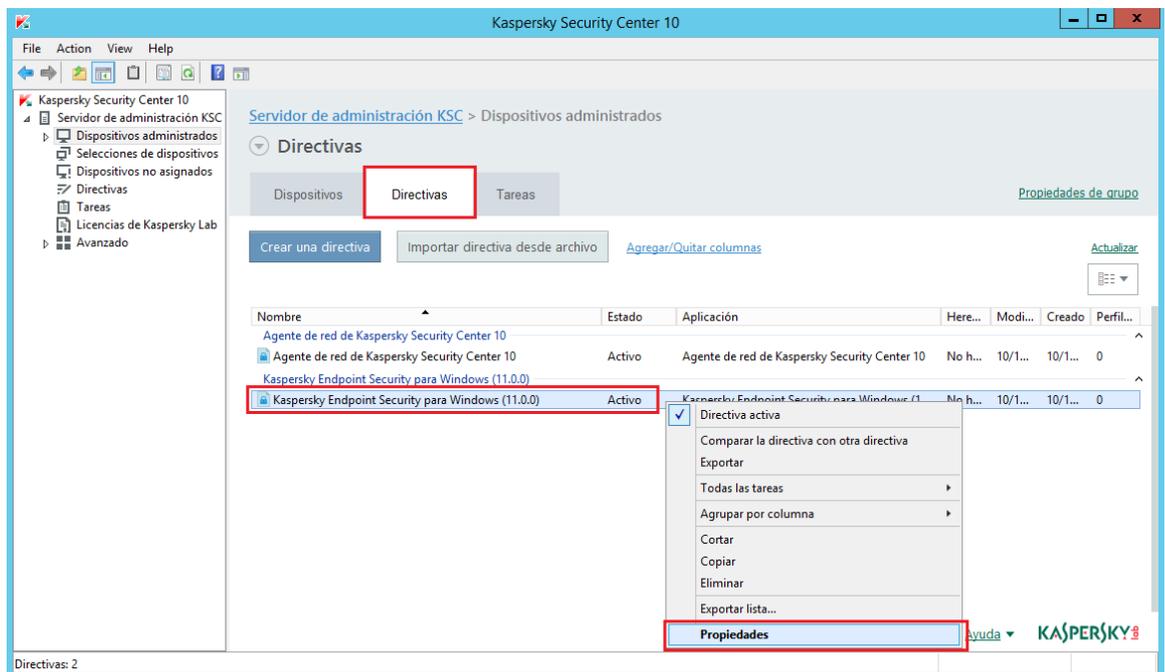


RECOMENDACIONES GENERALES CONTRA CRYPTOVIRUSES

Para reducir el riesgo de ser afectados por **cryptoviruses** (malware que cifra sus archivos y exige un rescate), se recomienda realizar la siguiente información.

Nivel de protección de Endpoint

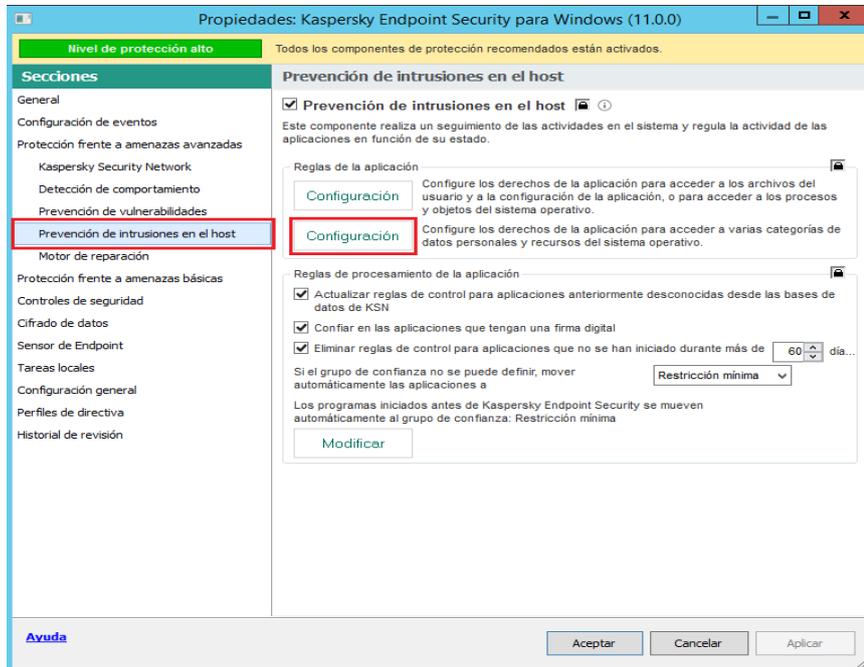
1. Ir al nodo “Equipos administrados”, en la pestaña “Directivas”, y abra las propiedades de la directiva “Kaspersky Endpoint Security para Windows (11.0.0)” .



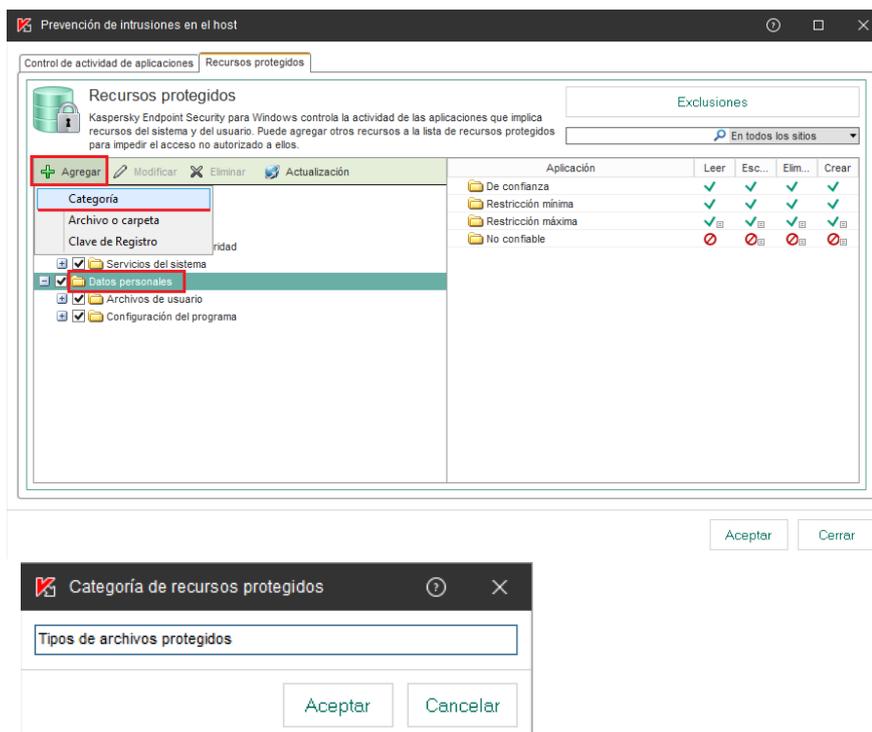
The screenshot shows the Kaspersky Security Center 10 interface. The 'Directivas' tab is selected, and the 'Kaspersky Endpoint Security para Windows (11.0.0)' policy is highlighted. A context menu is open over the policy, with the 'Propiedades' option highlighted.

Nombre	Estado	Aplicación	Here...	Modi...	Creado	Perfil...
Agente de red de Kaspersky Security Center 10						
Agente de red de Kaspersky Security Center 10	Activo	Agente de red de Kaspersky Security Center 10	No h...	10/1...	10/1...	0
Kaspersky Endpoint Security para Windows (11.0.0)	Activo	Kaspersky Endpoint Security para Windows (11.0.0)	No h...	10/1...	10/1...	0

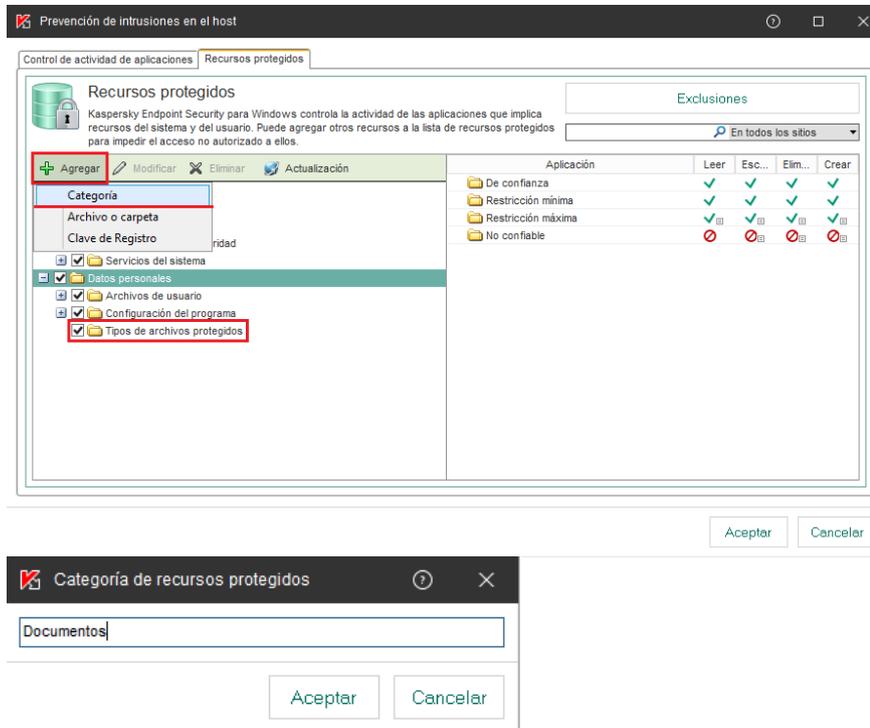
2. Ir al nodo “Prevención de intrusiones en el host”, después clic en el segundo botón de configuración.



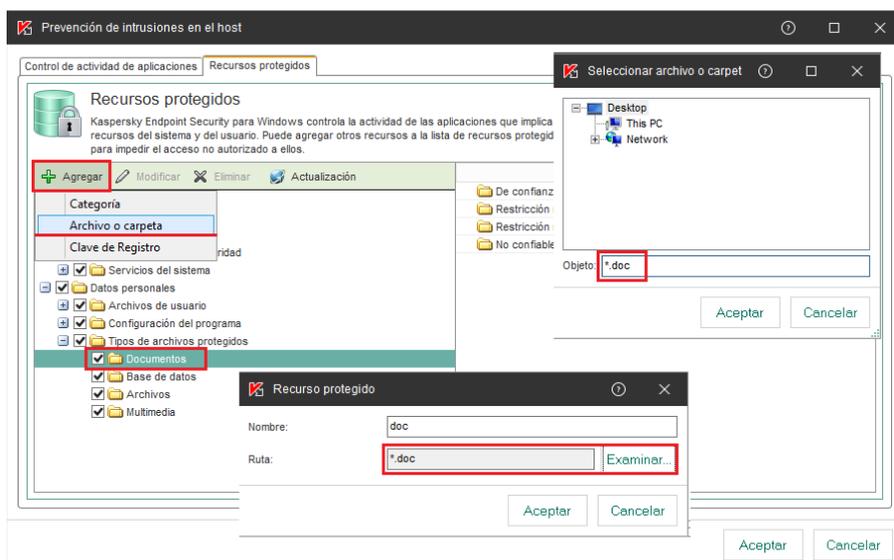
3. Desplegar el nodo “Datos Personales”, después, clic en “Agregar”, después, clic en “Categoría”, después, en la ventana emergente digitar el nombre “Tipos de archivos protegidos”, luego clic en Aceptar.



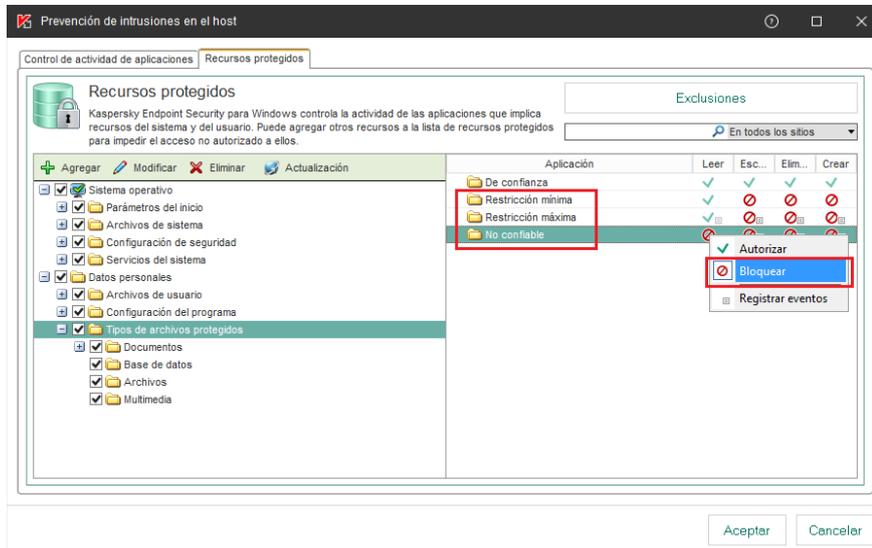
4. Seleccionar categoría creada, después, clic en el botón “Agregar”, clic en “Categoría”, después, en la ventana emergente digitar el nombre “Documentos”.



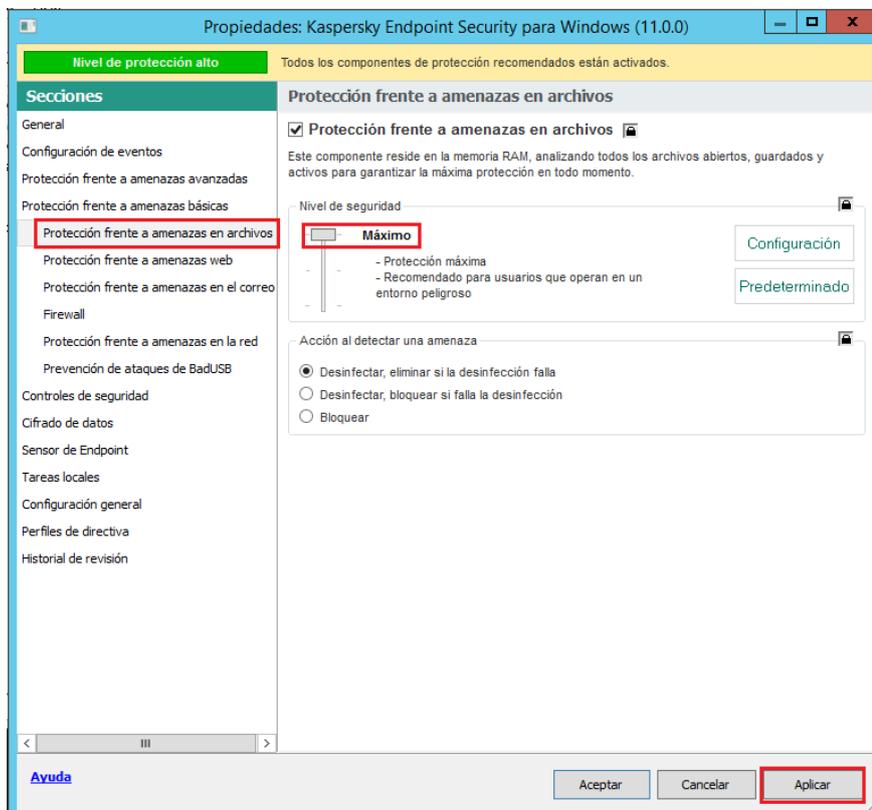
5. Repetir el paso 4 para crear otras “Categorías”, con los nombres “Imágenes”, “Base de datos”, “Archivos”, “Multimedia”.
6. Seleccionar la categoría que corresponda con los archivos que desea proteger (por ejemplo, “Documentos” para archivos .doc y .docx), clic en el botón “Agregar”, después, clic en “Archivo o carpeta”, puede especificar, en la ruta, un comodín (*. extensión). Ejemplo “*.doc” (sin comillas). ****Repetir este paso para las diferentes extensiones a proteger (*.jpg, *.dbs, *.exe, *.xls, *.ppt, etc)**



- Configurar los permisos de acceso al grupo “Tipo de archivos protegidos”, para las aplicaciones que hacen referencia a “Restricción mínima y alta restringida”, después clic en “Aceptar”.



- Ir al nodo “Protección frente a amenazas en archivos”, después, elevar el “Nivel de seguridad” al estado “Máximo”, después, clic en el botón “Aplicar”, después, clic en el botón “Configuración”.

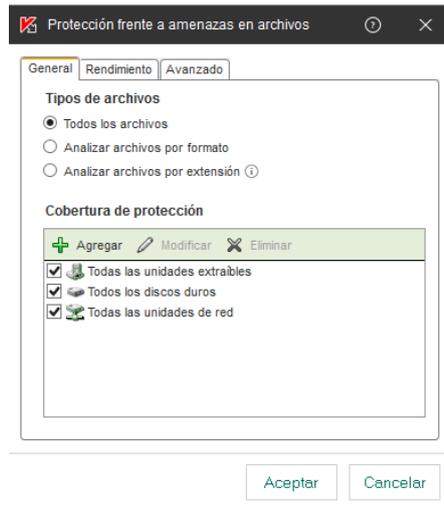


9. En la ventana emergente “Protección frente a amenazas en archivos”, seleccionar los siguientes parámetros:

a. Pestaña “General”

Tipos de archivos: seleccionar “todos los archivos”.

Cobertura de protección: Seleccionar todas las opciones listadas por defecto.



b. Pestaña “Rendimiento”

Métodos de análisis: verificar la selección “Aprendizaje automático y análisis de firmas” y “Análisis heurístico” (elevar el nivel hasta “análisis avanzado”).

Optimización del análisis: verificar que no esté seleccionada la opción “Analizar solamente archivos nuevos y modificados”.

Análisis de archivos compuestos: seleccionar todas las opciones listadas por defecto.

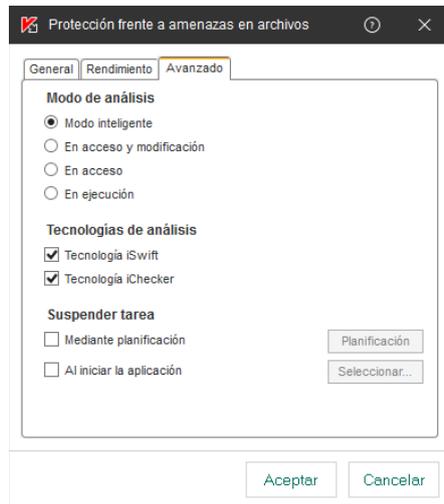


c. Pestaña “Avanzado”

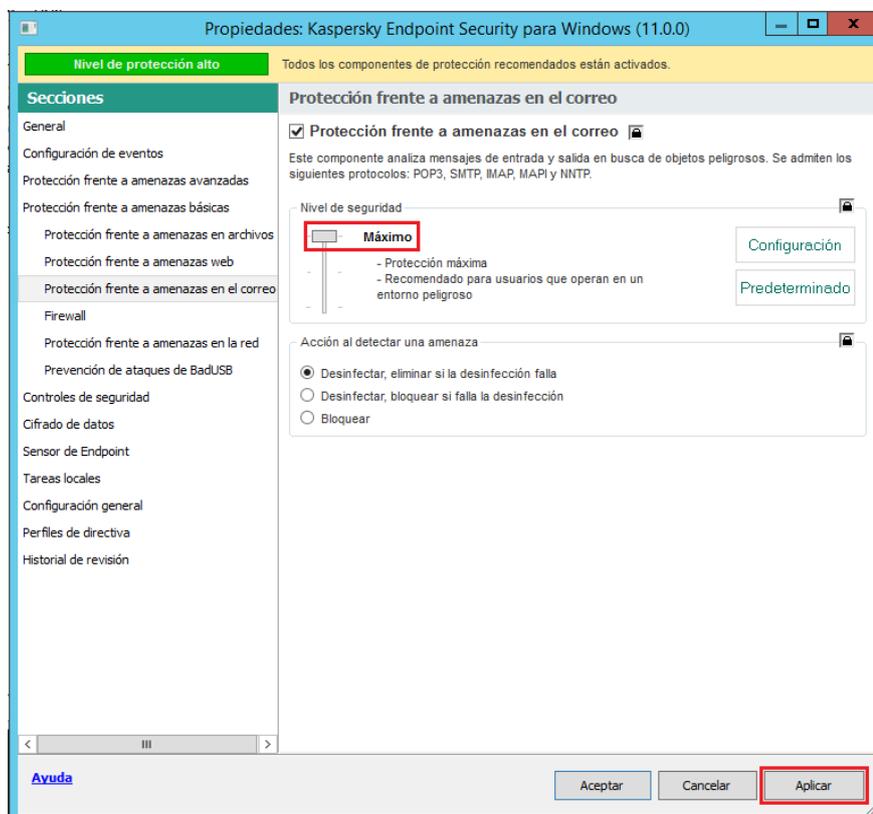
Modo de análisis: seleccionar “Modo inteligente”.

Tecnología de análisis: seleccionar todas las opciones listadas por defecto.

Suspender tarea: verificar que no estén seleccionadas las opciones listadas por defecto.

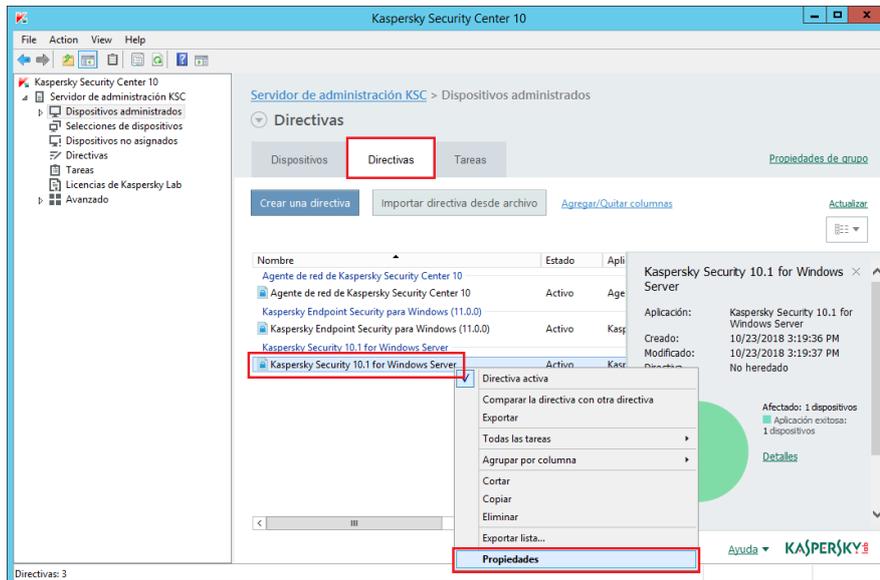


10. Ir al nodo “Protección frente a amenazas en el correo”, después elevar el “Nivel de seguridad” al estado “Máximo”, después, clic en el botón “Aplicar”.

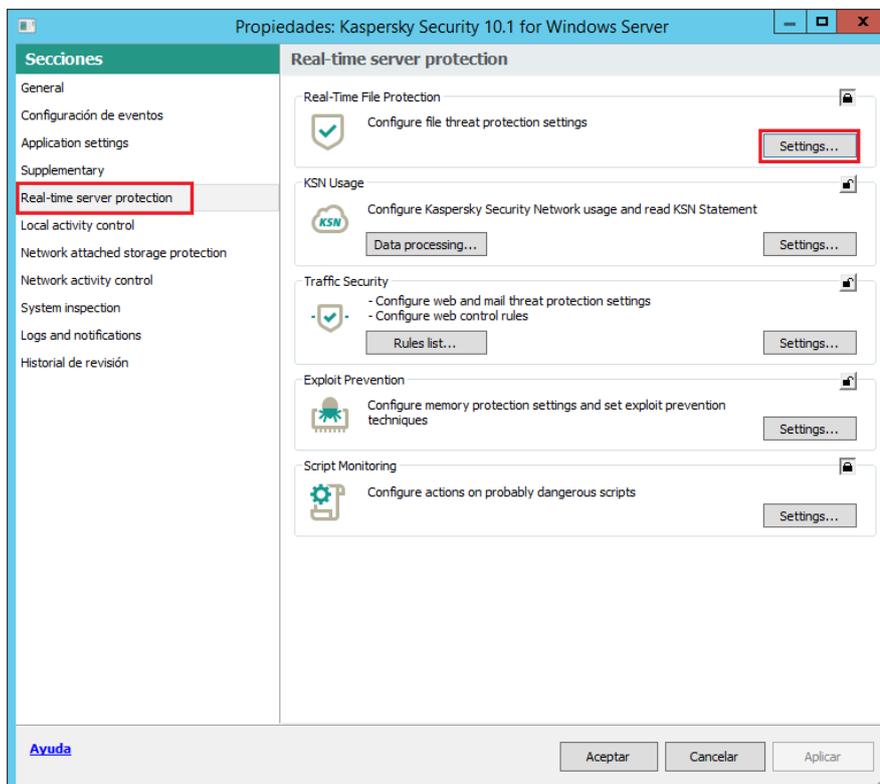


Nivel de protección de servidores

1. Ir al nodo “Equipos administrados”, en la pestaña “Directivas”, y abra las propiedades de la directiva “Kaspersky Security 10 for Windows Server”.



2. Ir al nodo “Real-time server protection”, después en la parte “Real-Time File Protection”, clic en el botón “Settings”.

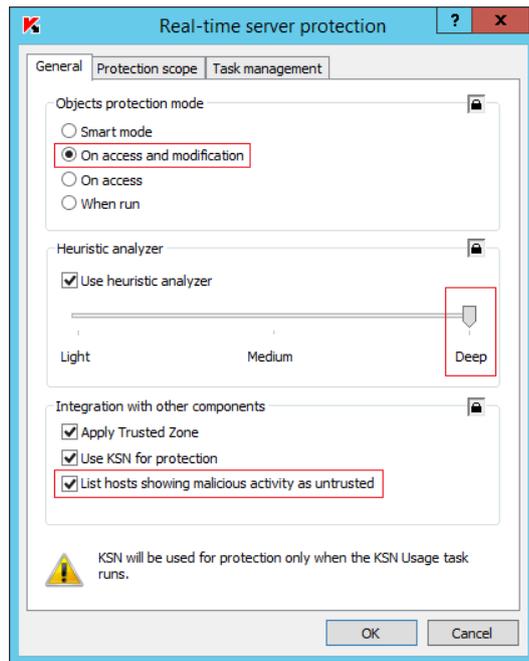


a. Pestaña “General”

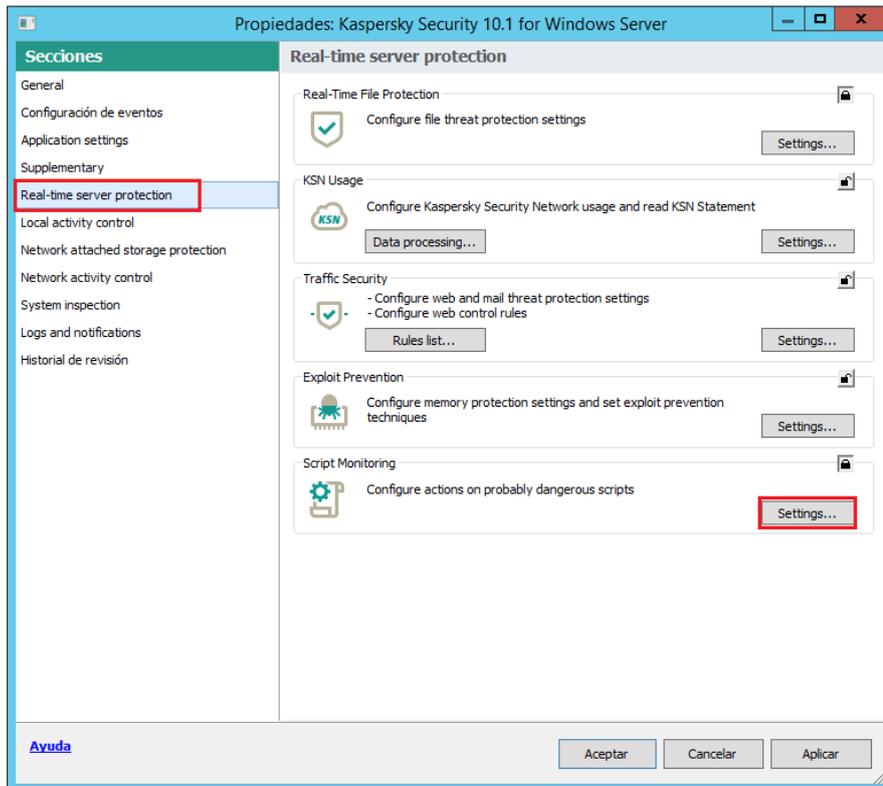
Objects protection mode: seleccionar la opción “On access and modification”.

Heuristic analyzer: verificar la opción “Use heuristic analyzer” y aumentar el nivel del análisis hasta “Deep”.

Integration with other components: verificar, adicionalmente a las verificadas por defecto, la casilla “List hosts showing malicious activity as untrusted”.



3. Ir al nodo “Real-Time Protection”, después, en la parte “Script Monitoring” clic en el botón settings.

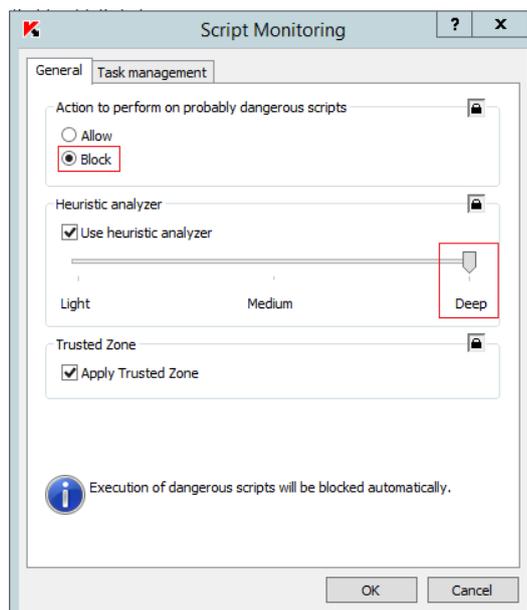


- a. Pestaña “General”

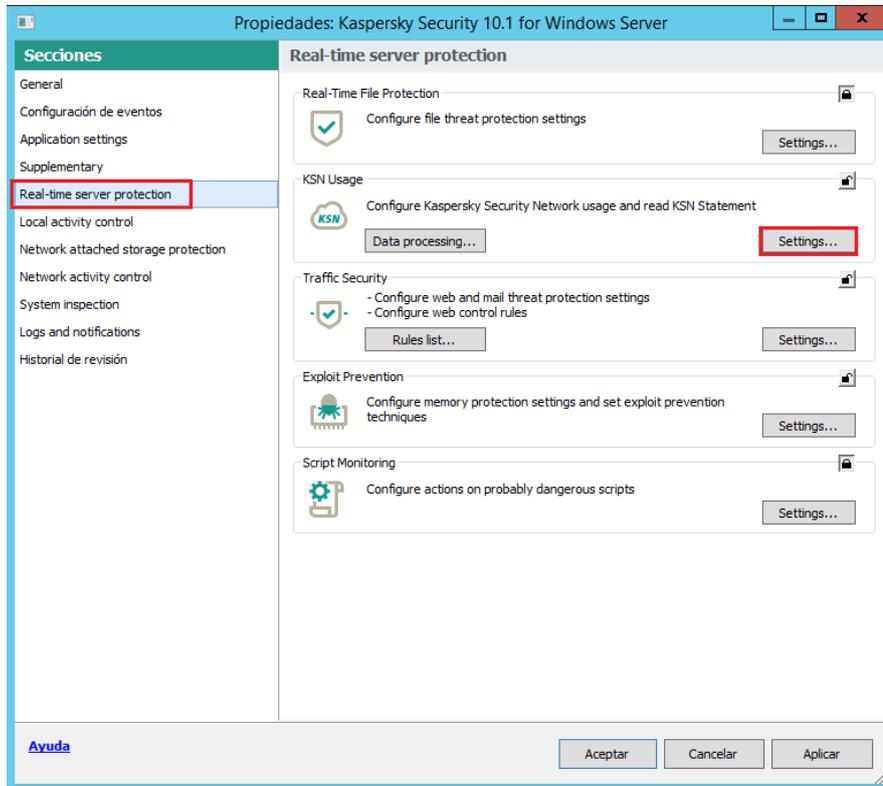
Action to perform on probably dangerous scripts: seleccionar la opción “Block”.

Heuristic analyzer: verificar la opción “Use heuristic analyzer”

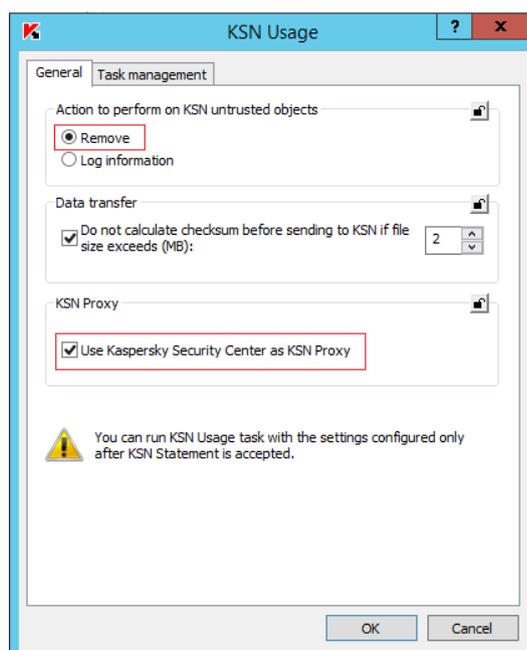
Elevar el nivel de heuristic: hasta el nivel “Deep”



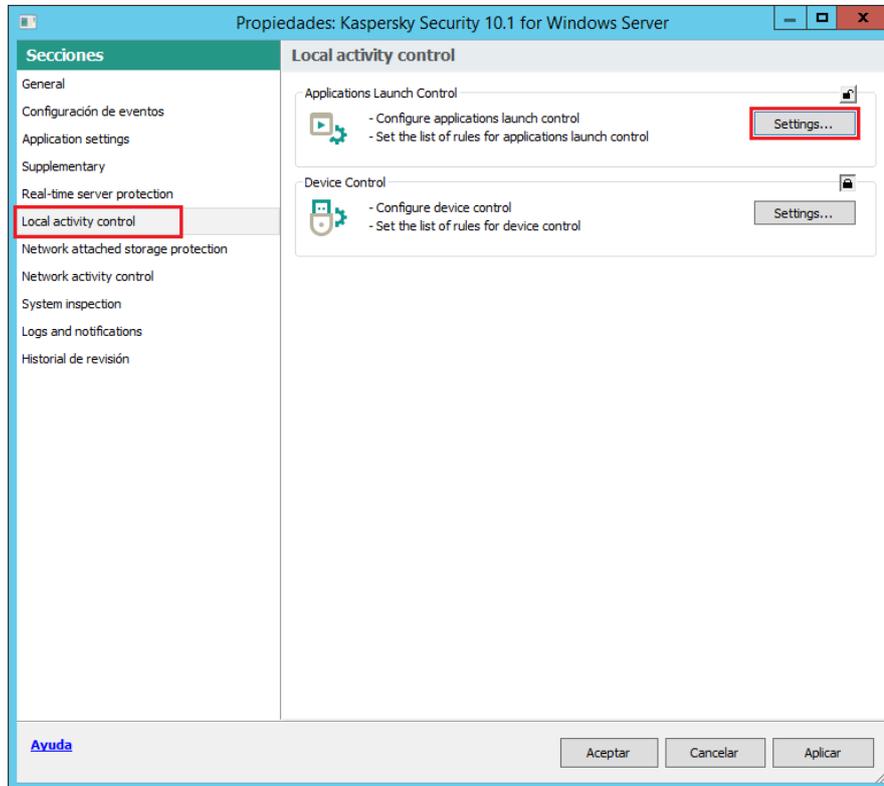
4. Ir al nodo “Real-Time Protection”, después, en la parte “KSN Usage” clic en el botón settings.



- a. Pestaña “General”
Action to perform on KSN untrusted objects: seleccionar “Remove”.
KSN Proxy: seleccionar “Use Kaspersky Security Center as KSN Proxy”

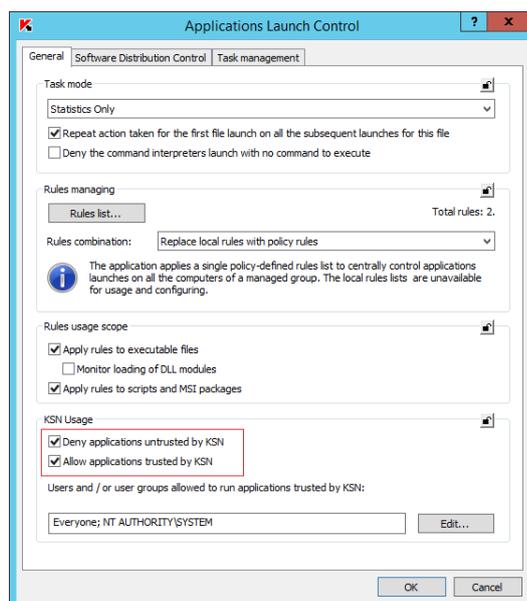


5. Ir al nodo “Local activity control”, después, en la parte “Applications Launch Control”, clic en el boton “Settings”.

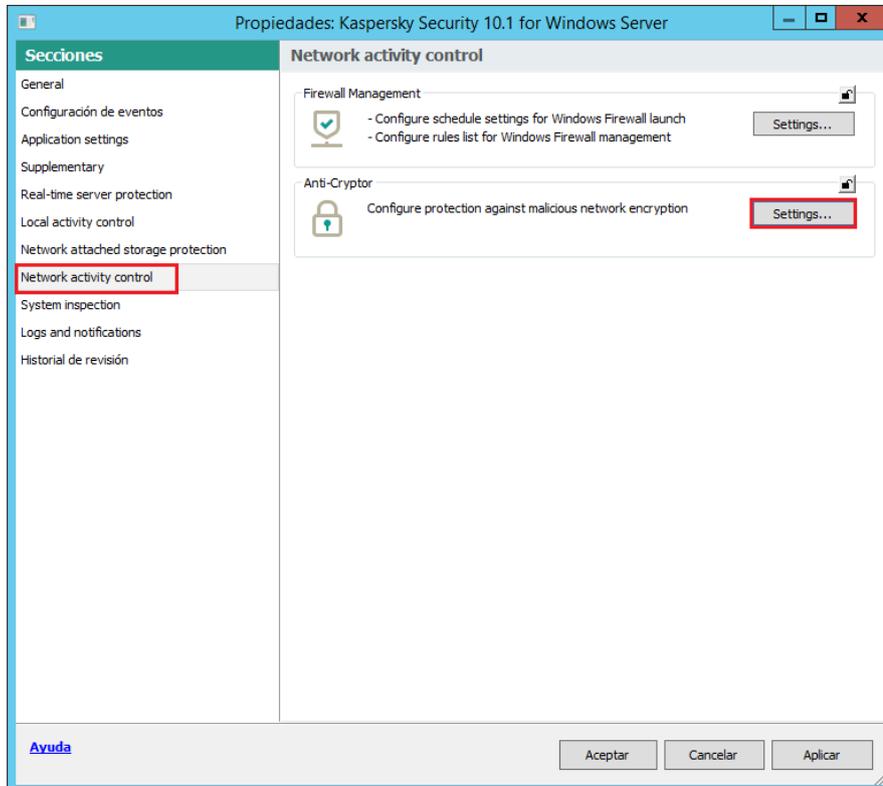


- a. Pestaña “General”

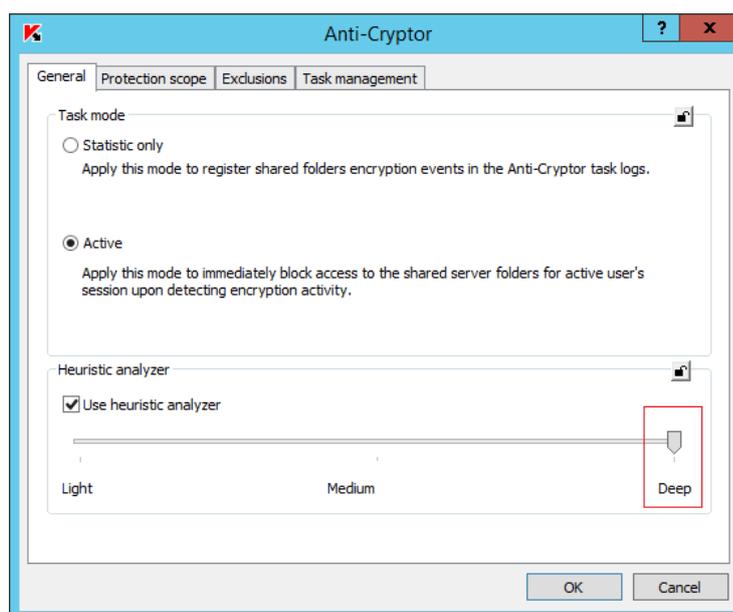
KSN Usage: verificar las casillas “Deny applications untrusted by KSN” y “Allow applications trusted by KSN”.



6. Ir al nodo “Network activity control”, después en la parte “Anti-Cryptor”, clic en el botón “Settings”.



- a. Pestaña “General”
Heuristic analyzer: elevar el nivel hasta “Deep”.



b. Pestaña “Protection scope”

Protection scope: seleccionar la opción “All shared network folders on server”

