

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.

🔀 Host Intrusion Prevention				0) [⊐ ×
Application privilege control Protected resources						
Protected resources Kaspersky Endpoint Security for Windows controls application activity that involves system and user resources. You can add other resources to the list of protected resources to prevent unauthorized access to them.		Ex	lusions			
		Everywhere				
🕂 Add 🖉 Edit 💥 Delete 💕 Update	Appli	cation	Read	Write	Del	Cre
Operating system	🚞 Trusted		\checkmark	\checkmark	\checkmark	\checkmark
🗉 🔽 🧰 Startup settings	Low Restricted		\checkmark	\checkmark	\checkmark	\checkmark
🔳 🗹 🧰 System files	High Restricted					
🗉 🗹 🧰 Security settings	🛄 Untrusted					
🗉 🗹 🧰 System services				Allow	_	
🖃 🗹 🧰 Personal data			0	Block		
🛨 🗹 🛅 User files			Ξ	Log eve	ents	
🖿 🗹 🧰 Program settings						
				OK		Cancel

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.

K				Kaspersky Se	curity Cente	10					_ 0 ×
File Action View Help					,						
🗢 🔿 🙍 📰 🙆 🖉 📼											
Kaspersky Security Center 10 Administration Server SRVKASPI A Managed devices b CLIENTES b Mobile Device Management	Administration Ser	rver SRVKASPERSKY > Po	olicies								
교 Device selections 도 Unassigned devices ☞ Policies 면 Tasks 답 Kaspersky Lab Licenses	Create a policy										Refresh
Advanced	Name	 Status 	Application		Inherited	Modi	Creat	Polic	Group	Kasasala, Endasia	Committee fore Windows (11.0.0) V
	Kaspersky Endpoint S	Security for Windows (11.0.0)								Kaspersky Endpoin	t Security for Windows (11.0.0) ×
	Kaspersky End	Active policy		ecurity for Windows (Not inherited	10/2	10/1/	0	Managed devices	Application:	Kaspersky Endpoint Security for
	Kaspersky Secur	Show policy in group in which	it was created	10 10 10 10 10 10 10 10 10 10 10 10 10 1	Market Charles	10/1	10/17	0	Managed de lass	Administration group:	Managed devices
	 Naspersky Sec 	Compare policy to another po	olicy	hter to Network Agent	Not inherited	10/1	10/1/	0	ivianaged devices	Created:	10/1/2018 11:59:19 AM
		Export								Changed:	10/22/2018 12:28:35 PM
		All tasks	,								Affected: 2 devices
		Group by column	,								Enforcement pending: 1 devices
		Cut									Envicement auccession. Toevices
		Сору									Details
		Delete									
		Export list									
		Properties									
										Configure policy Configure policy	
										Export policy to file	
	<		ш							Activate Window	s · · · · · · · · · · · · · · · · · · ·
/ III >										Go to System in Contro	- I Panel to <u>Help</u> vete \ KASPERSKY1
Policiec 2											



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"

🔀 Host Intrusion Prevention	0		×
Application privilege control Protected resources			
Configure application privilege control rules for policy To assign rights to applications in the policy, import application rights to the policy from the Kaspersky Security Center glo ▲ To send applications startup information to Administration Server, select the "Reports and Storage" tab in the policy pro- started applications" check box in the "Data transfer to Administration Server" section.	bal list of applicat	tion rights t the "Abo	i. ut
🐥 Add 🖉 Edit 💥 Delete			
Application Vender Group A			
Low Restricted			
🗎 High Restricted 🔴 🛛			
	ОК	Can	cel



• 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.

De confianza	Restric	sción mínima 🔽 G	2 W - W2	
Le no comanie	Restric	cción máxima	rupo desconocido	
Todo el tiempo		✓ De 22/10/200	8 🗘 A 22/10/2018	8 😥 Actualiz
Anular selec	ción			
A Versi	ión del archivo	Proveedor	Grupo	Fecha de actualiz.
6.14.1	1.1199 AMD		De confianza	22/10/2018
	1.1100		De comanza.	LEFTOLETO
	Todo el tiempo Anular selec: 3.14.1 6.14.1	Todo el tiempo Anutar selección S. Versión del archivo S.14.11.1199 AMD 6.14.11.1199	Todo el tiempo V De 22/10/200 Anular selección Anular selección Autor Proveedor 6:14:11:1199 AMD 6:14:11:1199 AMD	Todo el tiempo Pe De 22/10/2008 A 22/10/2011 Anular selección Anular selección Contractor Grupo 6.14.11.1199 AMD De conflanza 6.14.11.1199 AMD De conflanza

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