centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1209

Procedimiento de Empleo Seguro
Kaspersky Endpoint Security 12 for Windows

Mayo 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-250-7.
Fecha de Edición: Mayo de 2024

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.08.14 13:11:16 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN

1. Kaspersky Endpoint Security es una solución de seguridad informática diseñada para proteger dispositivos finales, como computadoras, servidores y dispositivos móviles, dentro de una red empresarial. Ofrece diversas funcionalidades, como protección antivirus y antimalware, firewall, control de aplicaciones y dispositivos, cifrado de datos, administración de parches, detección de comportamiento, control de anomalías adaptativa, protección contra Ransomware y prevención de exploits. Su objetivo principal es salvaguardar los endpoints contra amenazas cibernéticas y asegurar la integridad y confidencialidad de los datos.

2 OBJETO Y ALCANCE

2. En la presente guía se recoge el procedimiento de empleo seguro del software Kaspersky Endpoint Security for Windows 12.1.0.506 AES256.

3. El producto Kaspersky Endpoint Security for Windows 12.1.0.506 AES256 ha sido cualificados en el catálogo CPSTIC para las familias “EDR (Endpoint Detection and Response)” y “Anti-virus / EPP (Endpoint Protection Platform)”.

3 ORGANIZACIÓN DEL DOCUMENTO

4. Este documento está organizado en diferentes capítulos, de acuerdo a diferentes fases del ciclo de vida del producto:

   a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

   b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

   c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

5. Durante el proceso de entrega deberán llevarse a cabo una serie tareas de comprobación, de cara a garantizar que el producto recibido no se ha manipulado indebidamente.

6. Se deberá obtener el software del producto desde la página web de Kaspersky Lab. A continuación se muestran dos tablas para obtener el producto en español e inglés.

ESPAÑOL	
ENLACE DE DESCARGA	
https://aes.s.kaspersky-labs.com/endpoints/keswin11/12.1.0.506/spanish-21.13.5.506.0.312.0/3734323731307c44454c7c31/keswin_12.1.0.506_es_aes256.exe	
FICHERO	keswin_12.1.0.506_es_aes256.exe
SHA256	E16DE516FD45C7073572571ADEDB6AD68F360AE110C980EA3E77CF6228F65AB9

Tabla 1: Entrega segura en español

INGLÉS	
ENLACE DE DESCARGA	
https://aes.s.kaspersky-labs.com/endpoints/keswin11/12.1.0.506/english-21.13.5.506.0.311.0/3734323432357c44454c7c31/keswin_12.1.0.506_en_aes256.exe	
FICHERO	keswin_12.1.0.506_en_aes256.exe
SHA256	E93A047A0EF7F8A11C5F30A7542102E7FFADD2925A6E4AED95AB32B17EE3D462

Tabla 2: Entrega segura en inglés

7. Comprobar que el resumen SHA256 del paquete descargado coincide con el listado en la misma página web de Kaspersky Lab.

8. El SHA256 se puede obtener mediante cualquier aplicación de cálculo de hashes (HashCheck, CertUtil, etc) sobre el ejecutable previamente descargado.

9. Una vez verificado que se dispone del paquete correcto de instalación del producto, se puede proceder a realizar los pasos de la sección **5**.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. El entorno de instalación tiene que estar controlado por administradores competentes. El producto puede ser instalado sobre una plataforma hardware o virtual que cumpla con los siguientes requisitos:

CATEGORÍA	REQUISITO
Hardware	Procesador con una velocidad igual o superior a 1 GHz (que soporte el conjunto de instrucciones SSE2) Espacio en disco: al menos 2 GB Memoria RAM: • al menos 1 GB para sistemas 32-bit • al menos 2 GB para sistemas 64-bit
Sistema Operativo	Windows 7 Home / Professional / Enterprise Service Pack 1 o superior Windows 8 Professional / Enterprise Windows 8.1 Professional / Enterprise Windows 10 Home / Pro / Education / Enterprise Windows Small Business Server 2011 Essentials / Standard (64-bit); Windows MultiPoint Server 2011 (64-bit); Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later; Windows Server 2012 Foundation / Essentials / Standard / Datacenter; Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; Windows Server 2016 Essentials / Standard / Datacenter; Windows Server 2019 Essentials / Standard / Datacenter.
Sistemas de Virtualización	VMWare Workstation 16 Pro VMware ESXi 7.0 Update 1a Microsoft Hyper-V Server 2019 Citrix Virtual Apps and Desktops 7 Citrix Provisioning 2009 Citrix Hypervisor 8.2 LTSR

Tabla 3: Plataformas hardware y virtuales

4.3 REGISTRO Y LICENCIAS

11. **Para registrar el producto primero debemos seguir los pasos de instalación definidos en la sección 5 de este documento.**

12. Una vez instalado, para activar el producto debemos añadir una licencia válida para la solución que acabamos de instalar desde el menú de la aplicación como se ve en la siguiente imagen.

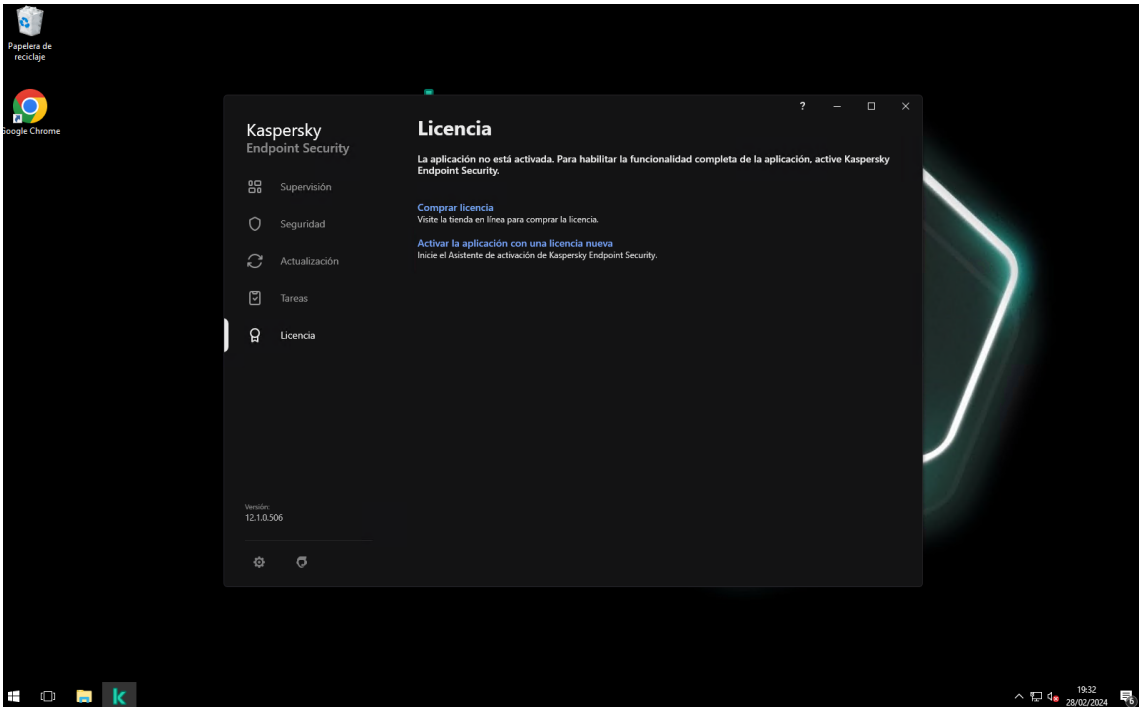

Ilustración 1: Menu licencia

13. Al hacer click sobre el icono de la barra de tareas, se nos mostrará el menú de configuración de la solución. En ese menú, hacemos click sobre “licencia”.

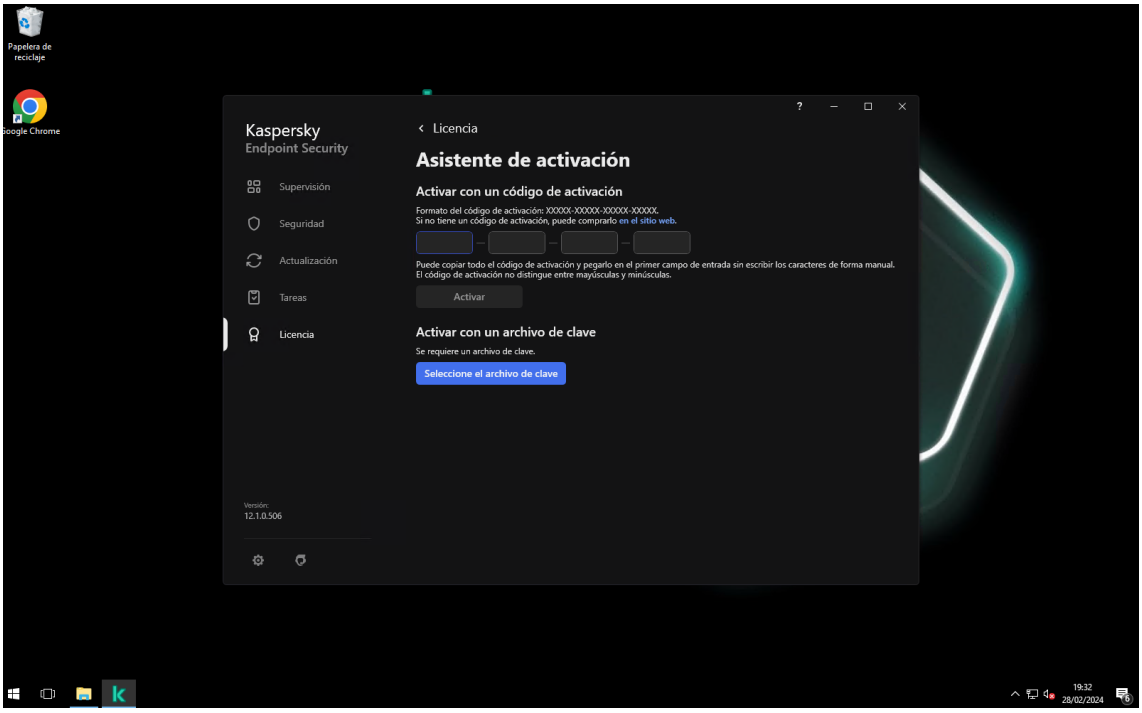

Ilustración 2: Asistente de activación

14. Añadimos el código de activación de la licencia en las casillas y hacemos click sobre “activar”.

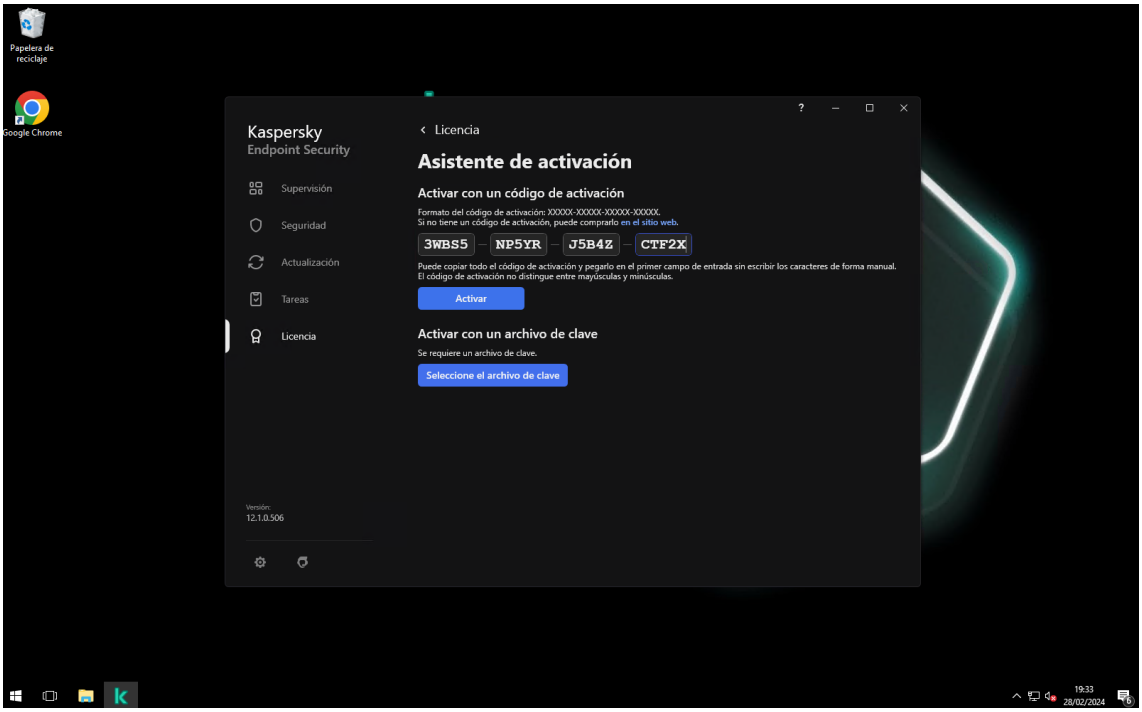

Ilustración 3: Ejemplo de código de licencia

15. Si todo ha sido correcto, se nos mostrará un mensaje en pantalla de que la activación ha terminado de forma correcta.

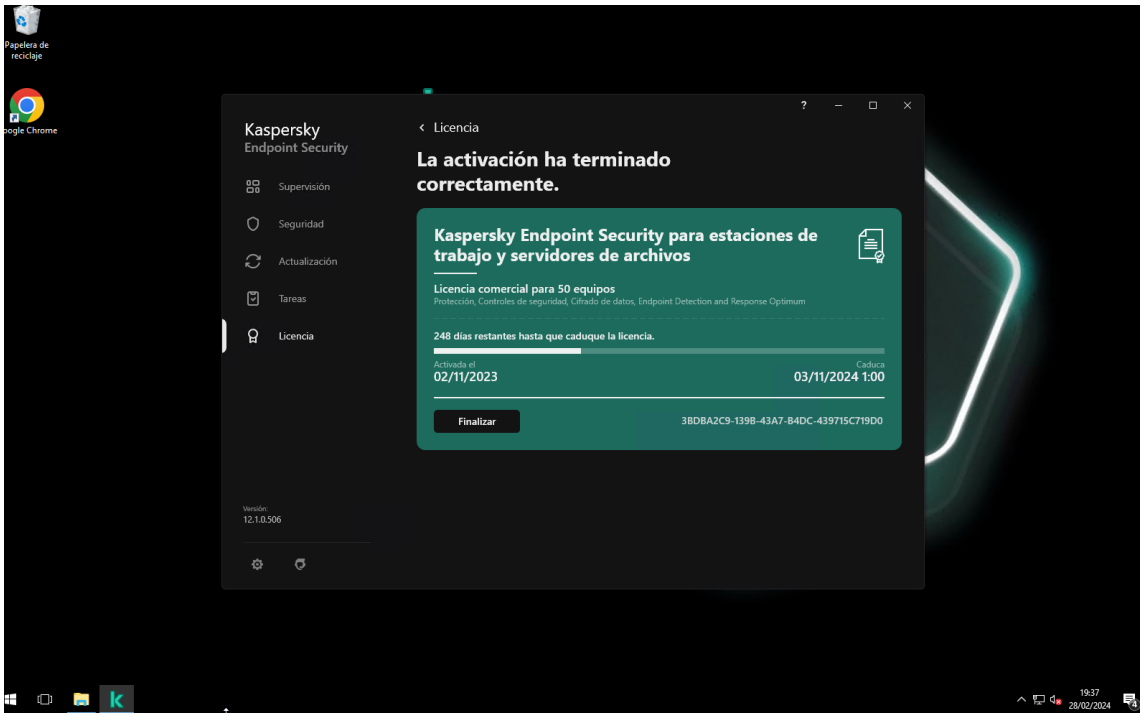

Ilustración 4: Mensaje de activación

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

16. Kaspersky Endpoint Security 12 es un producto de Kaspersky diseñado para proporcionar seguridad en los endpoints (puntos finales) de una red empresarial.
17. Esta solución puede ser gestionada remotamente mediante Kaspersky Security Center (KSC) para tener centralizados todos los productos Kaspersky desde un único punto.
18. A parte de la utilización de KSC para realiza la gestión del producto, este no requiere de más elementos en su entorno de operación.

5 FASE DE INSTALACIÓN

20. El paquete previamente descargado debe instalarse sobre la máquina que se quiere proteger. Para realizar este proceso será necesario configurar el entorno previamente.

21. La instalación del producto Kaspersky Endpoint Security for Windows podrá llevarse a cabo siguiendo dos métodos; instalación manual o instalación remota a través de Kaspersky Security Center. Los dos métodos de instalación se detallan en los enlaces a continuación:

    a) **Instalación centralizada** a través de Kaspersky Security Center: https://support.kaspersky.com/help/KESWin/12.1/es-ES/176372.htm

    b) **Instalación local** mediante el asistente de instalación: https://support.kaspersky.com/help/KESWin/12.1/es-ES/141289.htm

22. De forma adicional, la referencia publica de la documentación para realizar los pasos de instalación de forma local está definido en el siguiente enlace: https://support.kaspersky.com/help/KESWin/12.1/es-ES/141289.htm

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

23. Una vez finalizada la instalación y la activación de la licencia (ver secciones **4.3** y **5**), todos los componentes de seguridad de la solución estarán activos, para comprobarlo, abriremos la consola local de la solución de EndPoint y haremos click sobre “seguridad”.

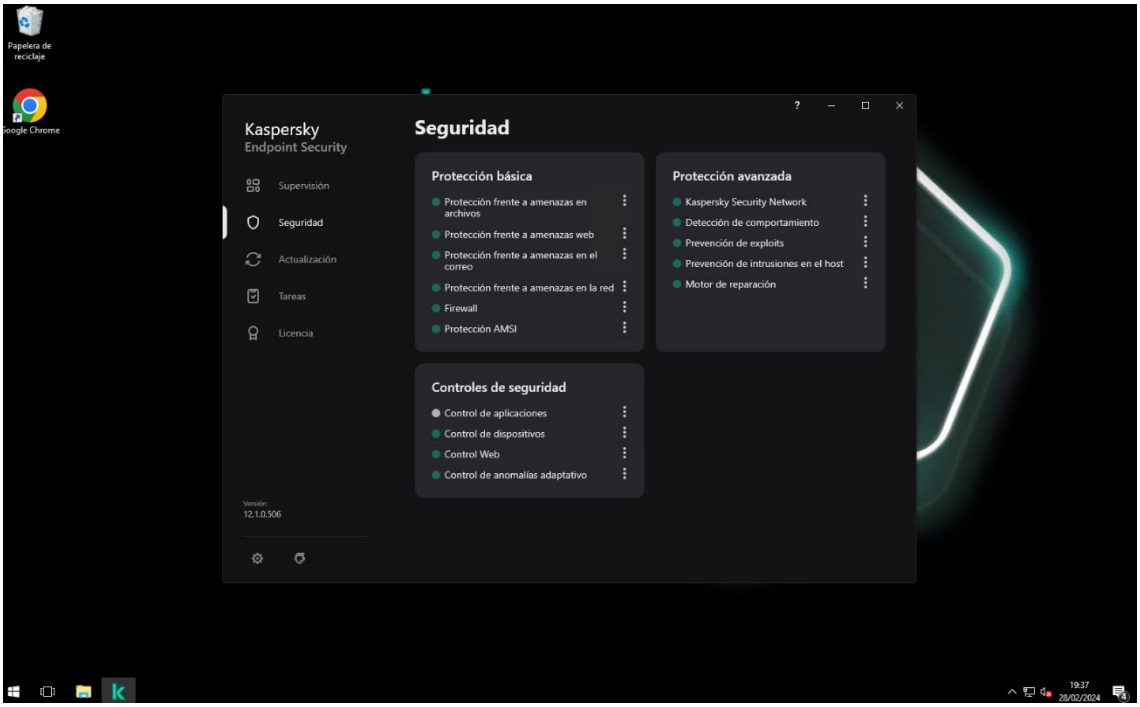

Ilustración 5: Menú Seguridad

24. Si la instalación ha sido correcta y la licencia esta activa, por defecto se activarán los complementos necesarios para la protección del Sistema Operativo.

6.2 AUTENTICACIÓN

25. De manera local, en el propio dispositivo, el usuario se validará con su cuenta de acceso de su propia organización.

26. En el caso, de que la gestión sea centralizada a través del Security Center, el administrador podrá administrar la plataforma mediante consola web o consola MMC. En los dos casos, el administrador dependiendo de los permisos que se le hayan asignado, tendrá más o menos capacidad de gestionar los dispositivos.

27. Autenticación mediante consola MMC:

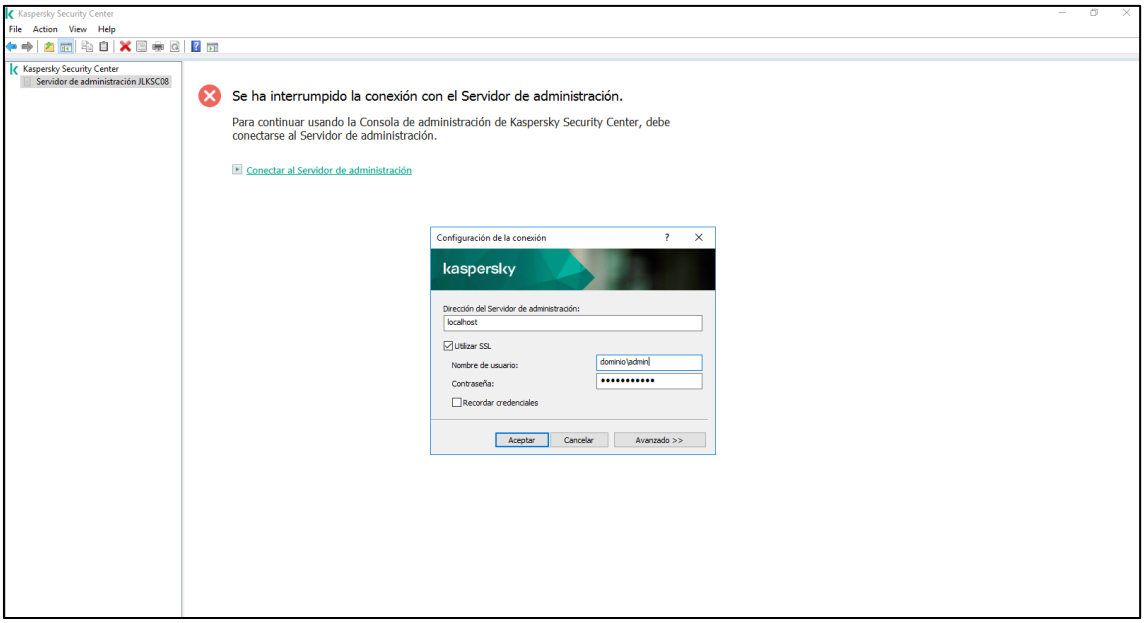

Ilustración 6: Autenticación mediante consola MMC

28. Autenticación mediante consola Web:

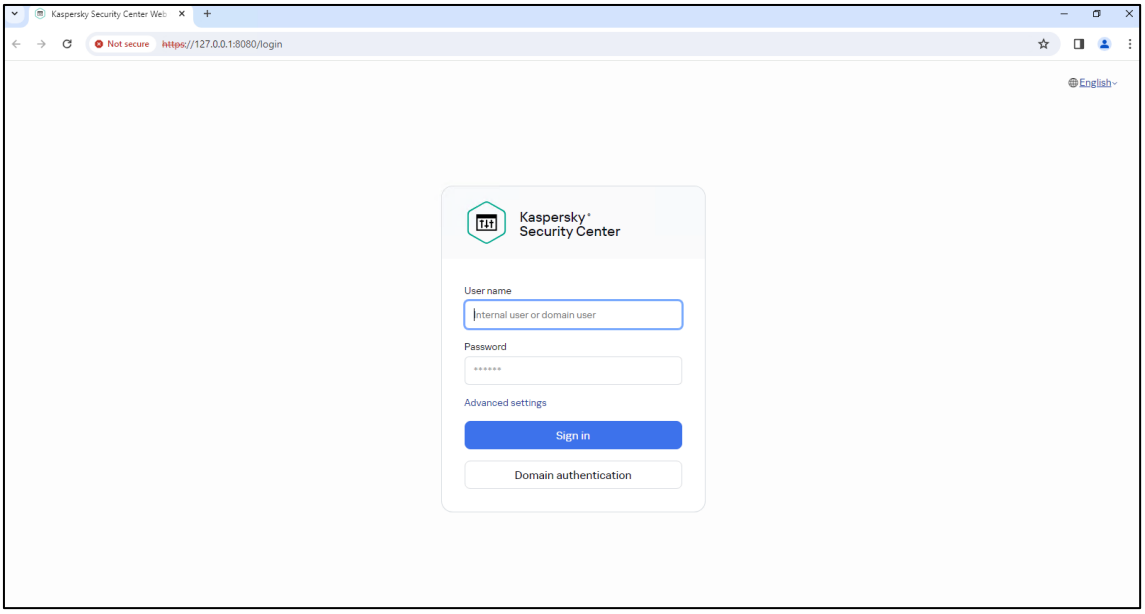

Ilustración 7: Autenticación mediante consola Web

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

29. La gestión de la solución de Kaspersky EndPoint se puede realizar de una manera local o remota.

30. Para realizar la gestión centralizada de forma remota, podemos instalar la herramienta Security Center (ver párrafo 20.a)). La información para realizar la gestión se encuentra en el siguiente enlace.

https://support.kaspersky.com/KSC/14.2/es-ES/166361.htm

La gestión de Kaspersky EndPoint se puede realizar de manera local via GUI, podemos acceder a la consola de gestión haciendo click sobre el icono de Kaspersky Endpoint Security en la barra de tareas.

Ilustración 8: Icono de KES en la barra de tareas

31. Al hacer click sobre el icono, se mostrará en pantalla la consola de gestión de Kaspersky Endpoint Security.

Ilustración 9: Consola de gestión

32. Mediante esta consola podremos realizar una gestión completa de la protección, definiendo que complementos queremos activar o gestionando las tareas de actualización.

33. La configuración de los complementos que viene aplicada por defecto, es la recomendada por Kaspersky, en caso de necesitar realizar algún cambio por ejemplo en los

complementos, hacer click sobre “seguridad”, para acceder al menú donde poder realizar los cambios necesarios.

Ilustración 10: Menú seguridad

34. El proceso de instalación local de Kaspersky Endpoint la podemos encontrar en el párrafo 20 de este documento y toda la información sobre la gestión local en el siguiente enlace.

    https://support.kaspersky.com/help/KESWin/12.1/es-ES/222859.htm

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

35. Si los usuarios cuentan con acceso ilimitado a Kaspersky Endpoint Security y su configuración, el nivel general de protección del equipo puede verse reducido. La protección con contraseña permite restringir el acceso de los usuarios a Kaspersky Endpoint. Para generar diferentes perfiles y definir esos accesos, podemos configurar perfiles nuevos o bien utilizar los ya existentes. Para acceder a la configuración de los perfiles, haremos click sobre la ruleta de gestión, una vez que aparezca el menú, haremos click sobre “interfaz”.

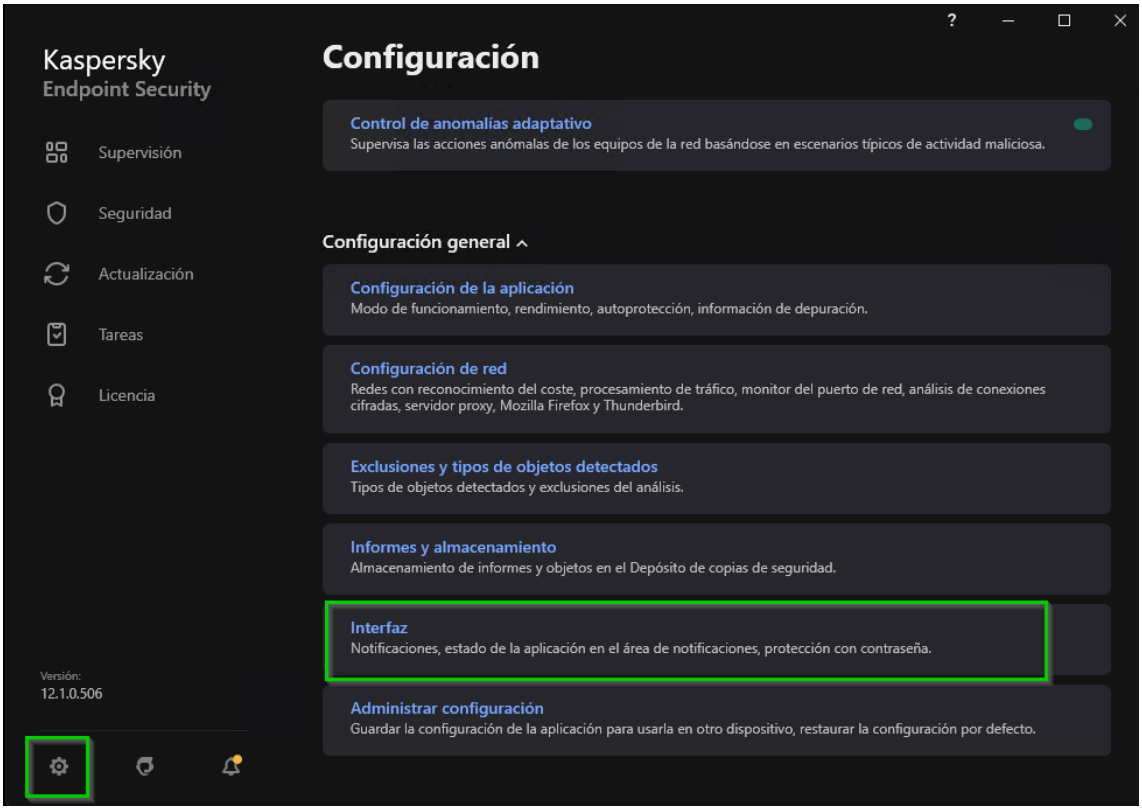

Ilustración 11: Acceso a menú interfaz

36. En el menú de interfaz, activar la "protección con contraseña y modificar en caso necesario los perfiles o si es necesario añadir nuevos.

Ilustración 12: Usuarios y contraseñas

37. Podemos modificar los permisos para que el perfil modificado, tenga más o menos capacidad de gestión en la solución de Kaspersky EndPoint.

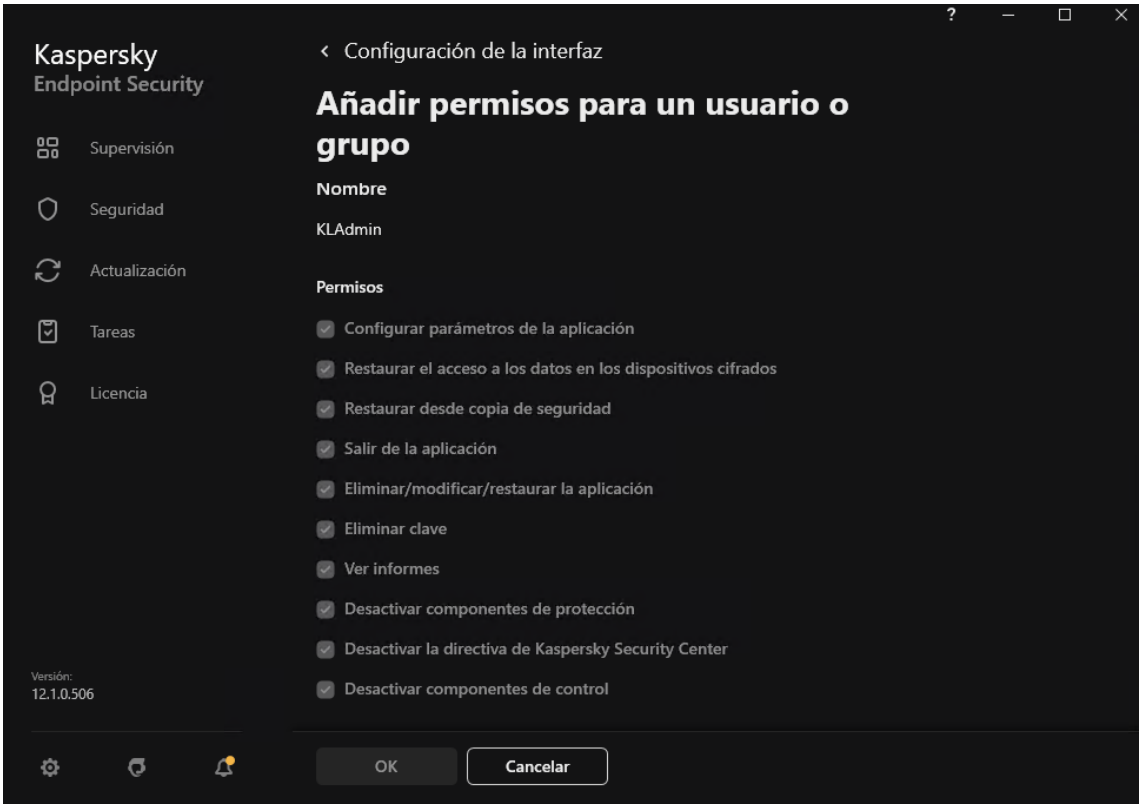

Ilustración 13: Permisos y grupos

38. En la siguiente URL podemos obtener más información de la gestión de perfiles.

    https://support.kaspersky.com/help/KESWin/12.1/es-ES/41045.htm

39. Al hacer click con el botón derecho sobre el icono de Kaspersky Endpoint de la barra de tarea, accederemos a un menú, donde podremos realizar diferentes acciones, dependiendo de nuestros permisos.

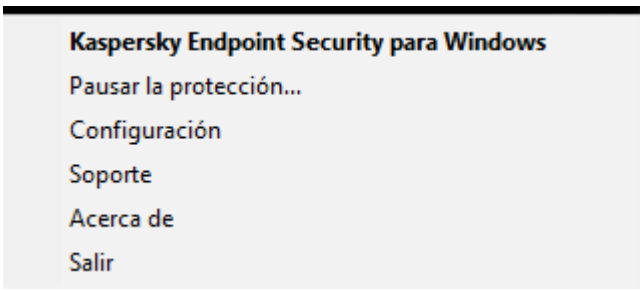

Ilustración 14: Menú de la barra de tareas

40. Si hacemos click sobre Pausar la protección, por ejemplo, por algún tipo de prueba de bloqueo de alguna solución, aparecerá un menú, en el que nos indicará cuanto tiempo necesitamos detener la protección.

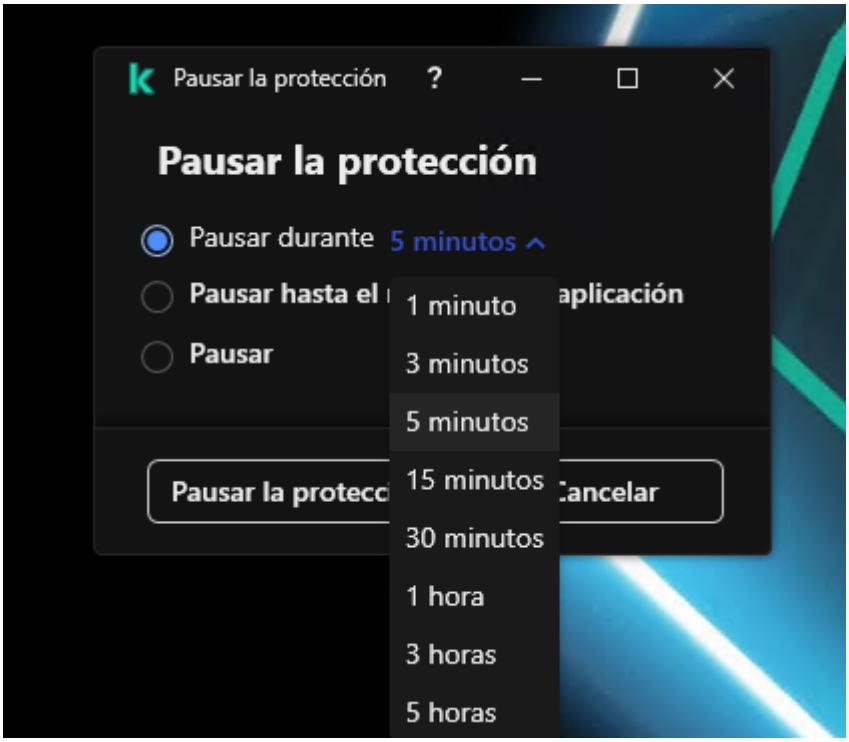

Ilustración 15: Menú de pausa de protección

41. Una vez que decidimos el tiempo que necesitamos parar la protección, haremos click sobre “Pausar la protección”, se nos pedirá el Usuario y la Password para comprobar que tenemos permisos suficientes para realizar dicha acción.

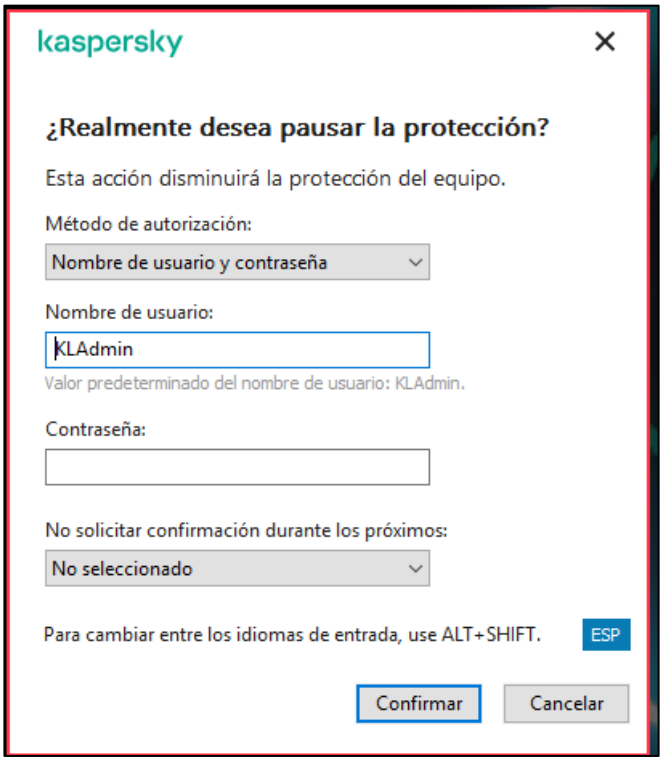

Ilustración 16: Confirmación de pausa de protección

42. En el caso de que necesitemos aplicar permisos de forma centralizada a través del Security Center, debemos gestionar estos permisos a través de la política que aplica a la versión 12.1 de Kaspersky Endpoint.

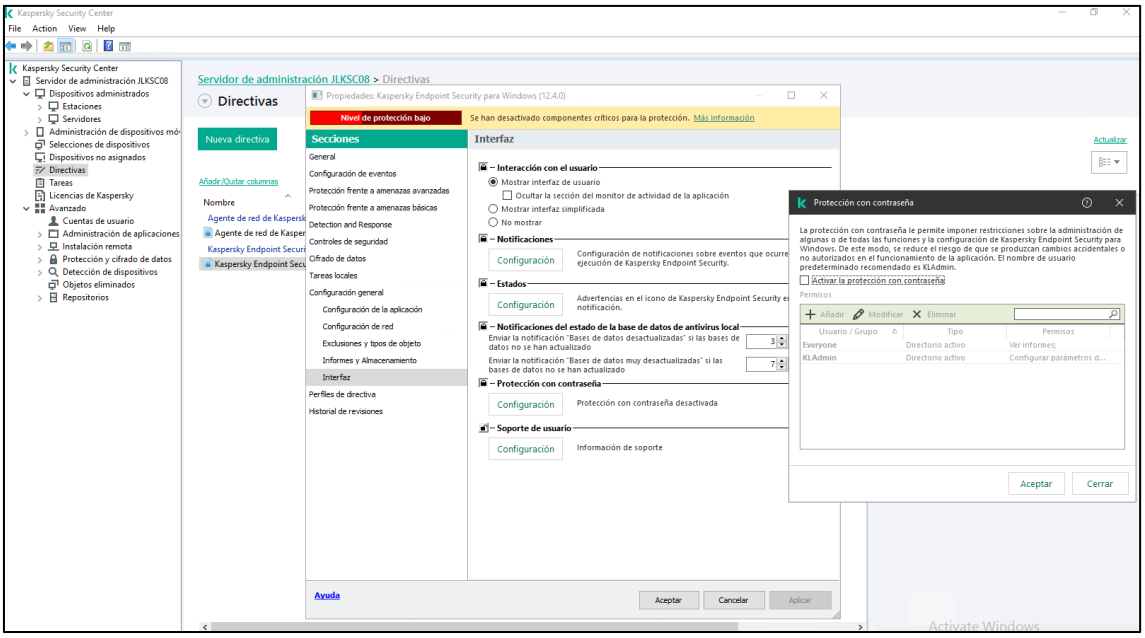

Ilustración 17: Gestión de permisos

43. En el siguiente enlace encontramos más información sobre la gestión de directivas.

    https://support.kaspersky.com/KSC/14.2/es-ES/165762_1.htm

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

44. Si la gestión se realiza centralizadamente a través del Security Center, hay una serie de puertos que deben estar abiertos para establecer una comunicación correcta entre la consola centralizada y los dispositivos gestionados. En este enlace se encuentra información sobre los puertos necesarios.

    https://support.kaspersky.com/help/KSC/14.2/es-ES/158830.htm

45. En la configuración local de Kaspersky Endpoint, no sería necesario realizar ninguna modificación a nivel de puertos.

6.5 SINCRONIZACIÓN

46. La sincronización en caso de que la gestión sea centralizada, será entre los dispositivos gestionados y el Security Center. Ese intervalo de tiempo es configurable a través de la política del agente de comunicaciones.

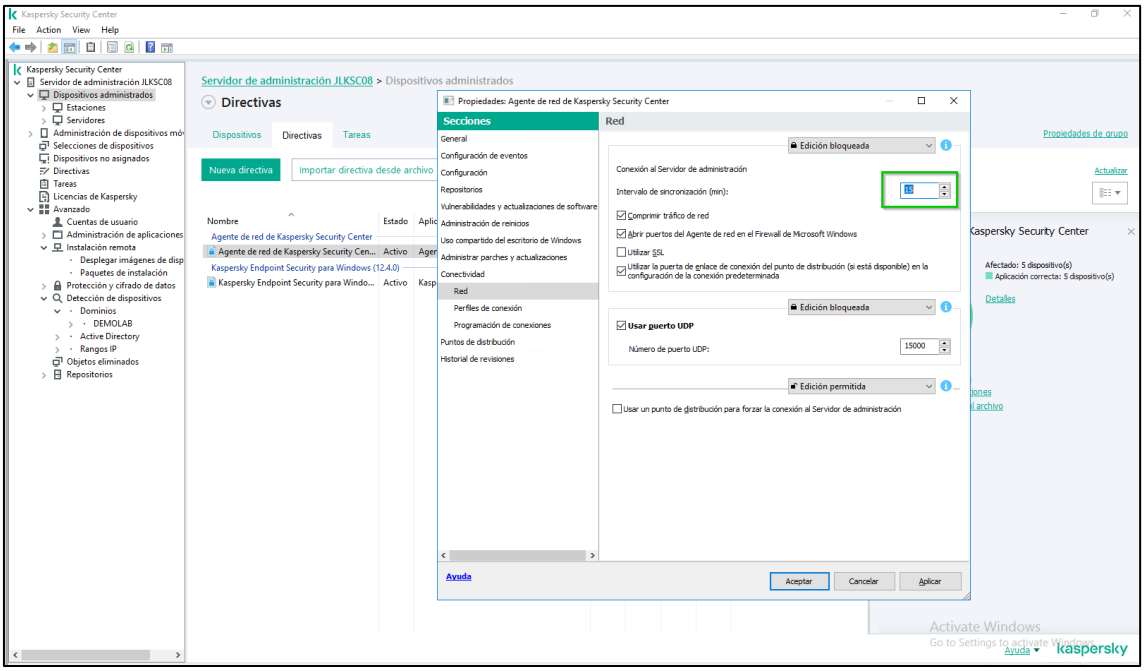

Ilustración 18: Configuración del intervalo de sincronización

6.6 ACTUALIZACIONES

47. Puede haber dos procesos de actualización en la solución de Kaspersky Endpoint 12.1. El producto avisará, cuando existan versiones nuevas de producto mediante un warning en el icono existente en la barra de tareas.

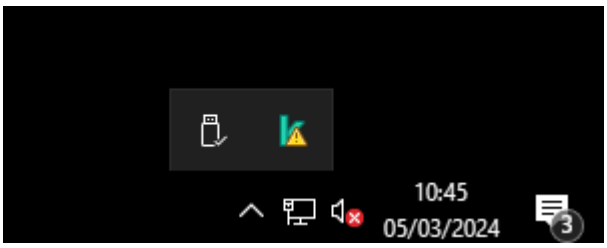

Ilustración 19: Aviso de actualización

48. Si hacemos click sobre el icono y una vez aparezca el menú contextual, hacemos click sobre la campana de notificaciones.

Ilustración 20: Icono de actualizaciones

49. Aparecerá una pantalla en la cual, podemos definir si queremos hacer upgrade a una versión mas reciente en caso de que exista.

50. La otra actualización es a nivel de firmas y módulos de aplicación. Para ello, existe por defecto una tarea de actualización configurable, podemos modificar esta actualización en el menú de la aplicación.

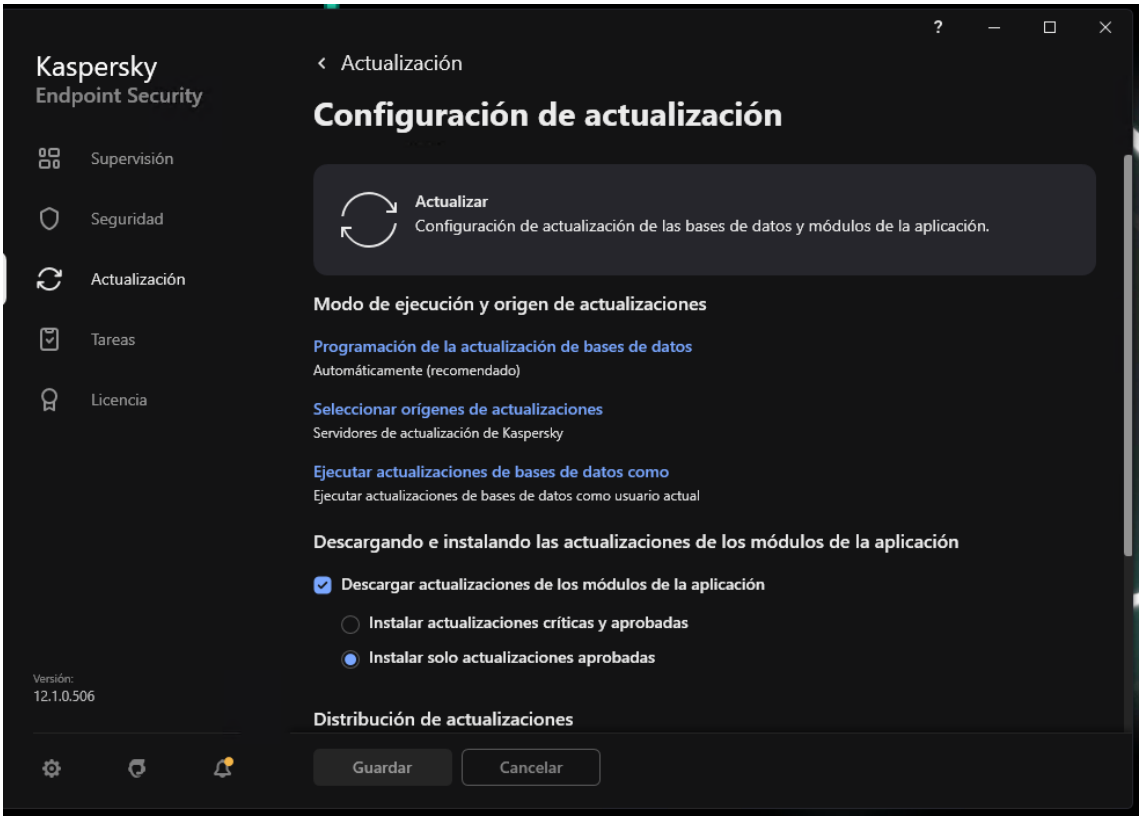

Ilustración 21: Actualización de firmas y módulos

6.7 AUTO-CHEQUEOS

51. Kaspersky Endpoint Security realiza una comprobación de los módulos de la aplicación en busca de datos corruptos o modificaciones. Si detecta, por ejemplo, que una de las bibliotecas no tiene la firma digital correcta, considera que la biblioteca está dañada. Los archivos de la aplicación se comprueban a través de la tarea Comprobación de integridad. Recomendamos que ejecute la tarea Comprobación de integridad si observa que Kaspersky Endpoint Security detecta, pero no neutraliza, un objeto malicioso.

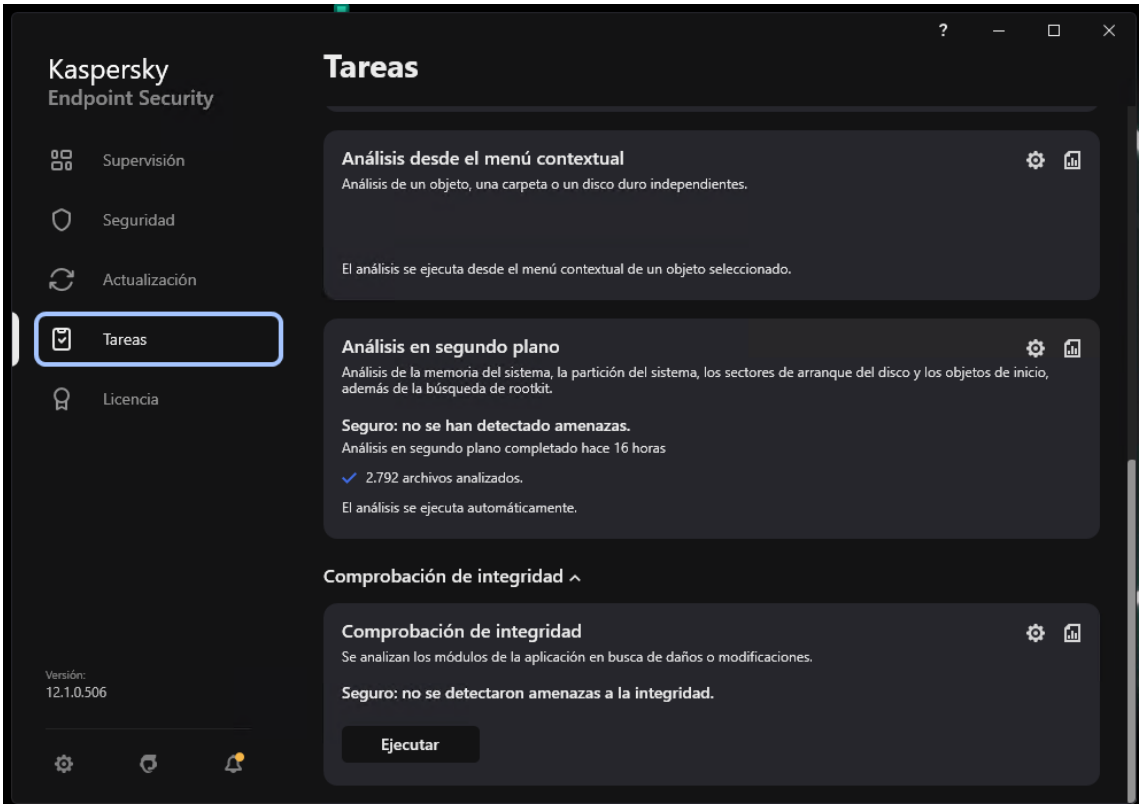

Ilustración 22: Comprobación de integridad

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

52. Para la gestión de eventos y notificaciones podemos consultar la ayuda on-line de la solución de Kaspersky Endpoint.

    https://support.kaspersky.com/help/KESWin/12.1/es-ES/214871.htm

53. En caso de que la gestión sea centralizada a través del Security Center, podemos consultar la ayuda en línea de Kaspersky Security Center.

    https://support.kaspersky.com/help/KSC/14.2/es-ES/30023.htm

6.8.2 ALMACENAMIENTO LOCAL

54. Para la gestión del almacenamiento local podemos consultar la ayuda on-linea de la solución de Kaspersky Endpoint.

    https://support.kaspersky.com/help/KESWin/12.1/es-ES/128118.htm

55. En caso de que la gestión sea centralizada a través del Security Center, podemos consultar la ayuda en línea de Kaspersky Security Center.

    https://support.kaspersky.com/help/KSC/14.2/es-ES/30023.htm

6.9 BACKUP

56. Es recomendable realizar backups de manera periodica, para poder recuperar configuraciones en caso necesario. Para realizar un backup en Kaspersky Endpoint podemos consultar la ayuda on-line de la solución.

    https://support.kaspersky.com/help/KESWin/12.1/es-ES/201016.htm

57. En caso de que la gestión sea centralizada a través del Security Center, podemos consultar la ayuda de cómo realizar el backup de la consola centralizada en la ayuda en línea de Kaspersky Security Center.

    https://support.kaspersky.com/help/KSC/14.2/es-ES/3670.htm

7 FASE DE OPERACIÓN Y MANTENIMIENTO

58. Durante la fase de operación de los dispositivos, los administradores de seguridad deberán llevar a cabo las siguientes tareas de mantenimiento:

a) Comprobaciones periódicas del software para asegurar que no se ha introducido software no autorizado. En caso de que haya una versión mas reciente de Kaspersky EndPoint de la que tenemos instalada, el icono de la barra de tareas mostrara un “warning” para advertir de esa nueva versión.

b) Mantenimiento de registros de auditoria incluyendo los eventos del sistema. En este enlace encontraremos información referente a la gestión de eventos de Kaspersky Endpoint.

https://support.kaspersky.com/help/KESWin/12.1/es-ES/237451.htm

c) Comprobación de que los ficheros de auditoria están protegidos del borrado y modificación no autorizada, incluso accidentales. En caso de que Kaspersky Endpoint estegestionado de manera centralizada, podremos aplicar políticas para que no exista ningún tipo de modificación localmente si la gestión es local, se puede aplicar roles locales para delimitar permisos mediante contraseña (ver sección 6.3.2 de este documento).

d) Almacenamiento de la información de auditoria en las condiciones establecidas en la normativa de seguridad y por el período establecido. A través del Security Center y bajo la directiva se puede definir un periodo de almacenamiento de los eventos generados.

e) Comprobación periódica del estado de los dispositivos con KES que han sido añadidos a KSC desde la interfaz de KSC.

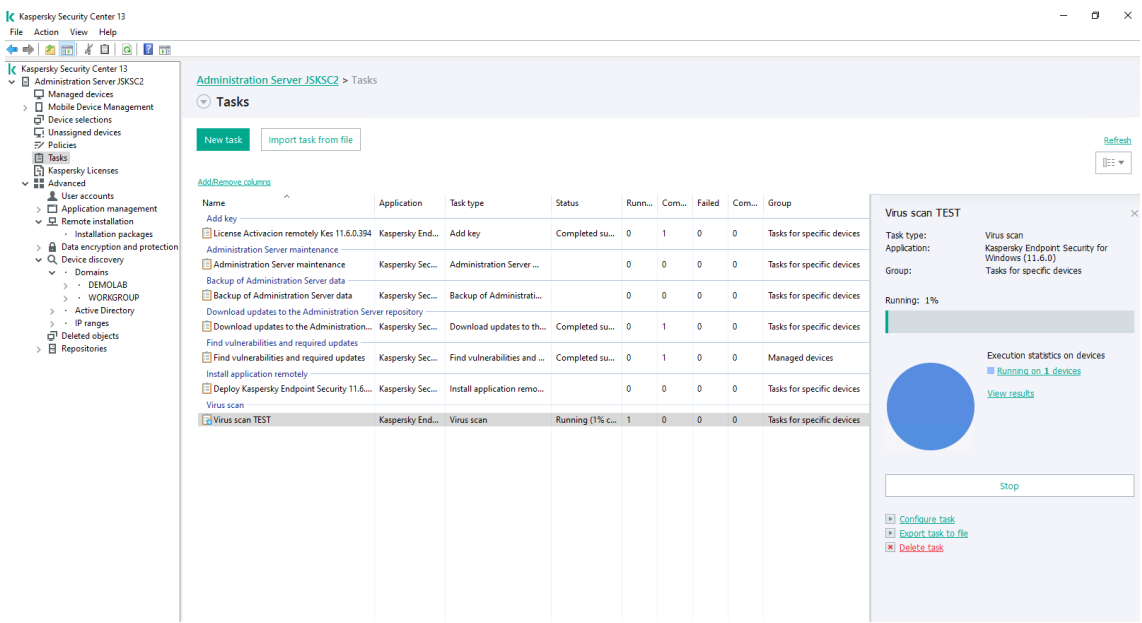

Ilustración 23: Listado de dispositivos

8 REFERENCIAS

59. Los siguientes documentos se han referenciado a lo largo de la guía.

[HLP] Ayuda Online
https://support.kaspersky.com/help/KSC/14.2/es-ES/5022.htm

[MAN] Manual del usuario
https://support.kaspersky.com/help/KESWin/12.1/es-ES/KESWin-12.1-es-ES.pdf

9 ABREVIATURAS

AES256	Advanced Encryption Standard 256-bit
CCN	Centro Criptolócido Nacional
CPSTIC	Catálogo de Productos de Seguridad TIC
GUI	Graphical User Interface
KES	Kaspersky Endpoint Security
KSC	Kaspersky Security Center
KSN	Kaspersky Security network
MMC	Microsoft Management Console
SHA256	Secure Hash Algorithm 256-bit
SSE2	Streaming SIMD Extensions 2
SSL	Secure Sockets Layer Protocol

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL