VERSIÓN 2.0.5

WinCVE

Explorer & Control Center



Manual de usuario

Consulta el catálogo de vulnerabilidades, revisa tu equipo y documenta las medidas de corrección.

Interfaz gráfica de Windows y consola

Ediciones x64, x86 y ARM64

Oscar de la Cuesta Campillo

Proyecto WinCVE · palentino.es

27 de noviembre de 2026

GUÍA DE LECTURA

Índice

Pulsa un capítulo para abrirlo. Puedes volver a esta página desde el encabezado o usar los marcadores del lector PDF.

Descargar, instalar y arrancar 03
Arquitectura, formatos y SHA-256

Inicio y navegación 04
Panel, accesos rápidos y atajos

Catálogo local y fuentes 05
Sincronización y trabajo sin conexión

Actualizar y comprobar fuentes 06
NVD, KEV, EPSS y verificación

Explorar y filtrar CVE 07
Filtros, ficha y CSV de la página

Consultas por fechas UTC 08
Ejemplos de publicación e importación

Leer indicadores y priorizar 09
CVSS, KEV, EPSS y prioridades P1–P5

Inventario y correlación 10
Evidencias, cobertura y diccionario CPE

Del hallazgo a la decisión 11
Versión, rango y aviso del fabricante

Windows, parches y auditoría 12
Compilación, KB y publicaciones MSRC

Red y firmware 13
Lectura local y perfiles de dispositivos

Informes e historial 14
Report Studio PRO y exportaciones

Leer un análisis integral 15
Cobertura, estados y plan de actuación

Configurar un proveedor de IA 16
OpenAI, OpenRouter, modelos y claves

Consultar una CVE con IA 17
Ejercicio completo con CVE-2024-11477

IA local con Ollama y LM Studio 18
Instalar el modelo y probar la conexión

IA desde PowerShell 19
Modelo, variables de entorno y temas

Resolver incidencias de IA 20
HTTP, modelos y recuperación de perfiles

Personalización e integraciones 21
Idiomas, temas y herramientas Palentino

Primeros pasos en consola 22
Ayuda, diagnóstico y consulta por ID

Consultas y tareas repetibles 23
PowerShell, JSON y códigos de salida

Referencia rápida de la CLI 24
Comandos por tarea y ayuda en línea

Copias, restauración y migración 25
Datos locales y catálogo transportable

Dos recorridos de principio a fin 26
Aplicar un aviso y trasladar un catálogo

Resolver incidencias 27
Síntomas, comprobaciones y recuperación

Fuentes y créditos 28
Descargas, soporte y documentación

Primera sesión

Importa el catálogo incluido y busca una CVE conocida. El ejercicio de IA parte de ese mismo Explorador y termina con la comprobación del aviso.

Configurar un proveedor de IA ›

Consultar una CVE paso a paso ›

01 / INSTALACIÓN

Descargar, instalar y arrancar

Palentino publica seis paquetes autocontenidos de WinCVE 2.0.5 con catálogo, uno por cada combinación de arquitectura y formato. El runtime .NET va incluido.

Tu equipo	Edición	Formatos publicados
Windows de 64 bits en Intel o AMD	**x64**	Instalador EXE y portable ZIP
Windows de 32 bits compatible	**x86**	Instalador EXE y portable ZIP
Windows en procesador ARM de 64 bits	**ARM64**	Instalador EXE y portable ZIP

1. **Identifica el tipo de sistema.** Abre **Configuración › Sistema › Acerca de** en Windows. En **Tipo de sistema** comprueba la arquitectura y elige la misma en la sección Descargas de Palentino.

2. **Verifica la descarga.** En PowerShell, ejecuta este ejemplo desde la carpeta de descargas. Cambia el nombre por el de tu paquete y compara los 64 caracteres con el SHA-256 publicado para ese archivo.

```powershell
$archivo = ".\WinCVE-2.0.5-win-x64-con-catalogo-setup.exe"
Get-FileHash -Algorithm SHA256 -Path $archivo
```

3. **Instala o extrae.** Para el EXE, sigue el asistente y abre WinCVE desde su acceso directo. Para el ZIP, extrae todo en una carpeta escribible y ejecuta **WinCVE.exe** desde allí.

4. **Carga el catálogo incluido.** Si la base está vacía, WinCVE ofrece importar **WinCVE-Catalogo.zip** sin Internet. Espera a que termine y verifica el recuento en **Actualizaciones**. Puedes hacerlo también con **IMPORTAR_CATALOGO_INCLUIDO.bat**, con WinCVE cerrado.

> **Prepara espacio para la importación**
>
> Deja espacio libre para los archivos extraídos y para la base SQLite que se crea al importar. Los paquetes públicos ya compilados se descargan desde la web del proyecto.

Ver descargas y huellas publicadas ›

02 / PANEL DE CONTROL

Inicio y navegación

El panel reúne los resultados del equipo, el estado de las fuentes y el historial. Los recuentos dependen de la sesión y del catálogo que tengas cargado.

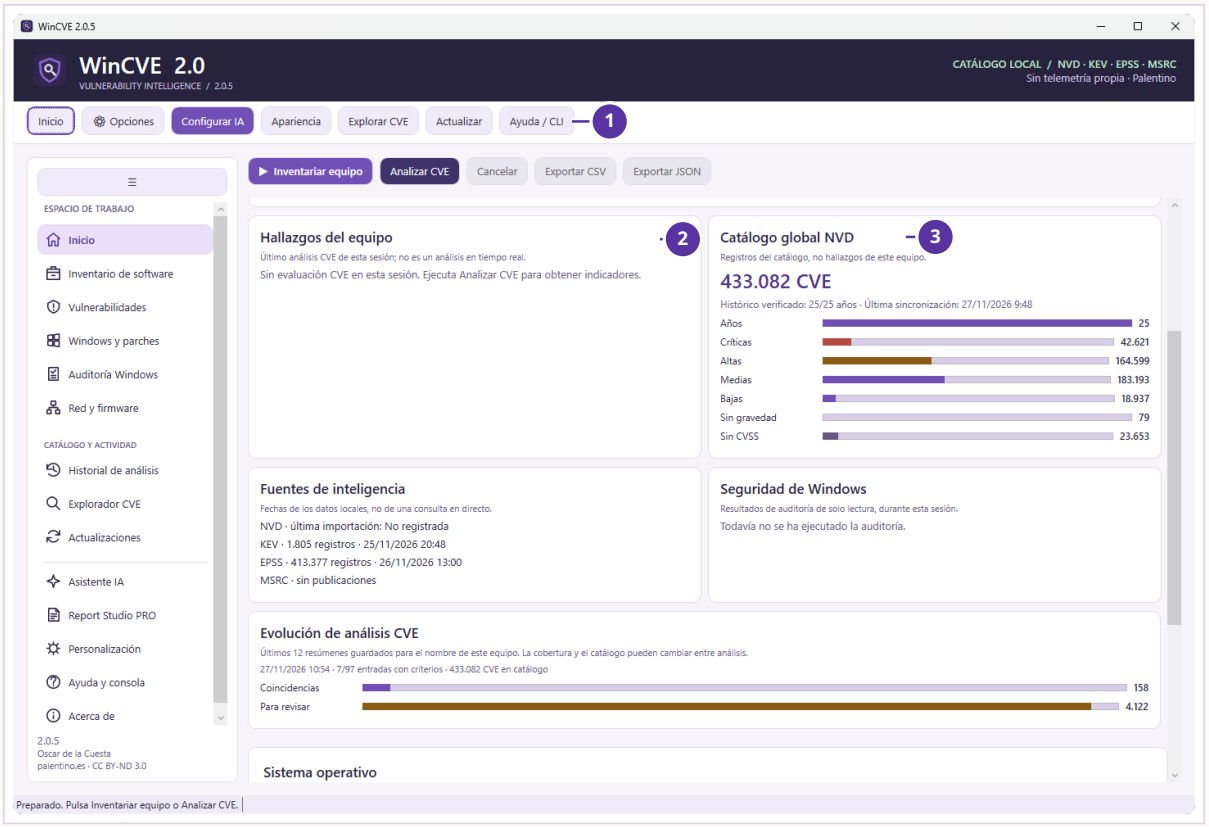

Figura 1. Inicio de WinCVE 2.0.5. La captura publicada corresponde al 27 de noviembre de 2026.

1 **Barra superior.** Acceso directo a **Opciones**, **Configurar IA**, **Explorar CVE**, **Actualizar** y **Ayuda / CLI**.

2 **Hallazgos del equipo.** Se completan tras pulsar **Analizar CVE**. La evolución muestra hasta 12 resúmenes guardados para ese equipo.

3 **Catálogo global NVD.** Muestra el volumen y la cobertura de la copia local. Lee en el panel inferior las fechas de KEV, EPSS y MSRC.

Atajos del escritorio

Ir a	Atajo	Ir a	Atajo
Explorador CVE	Ctrl+F	Actualizaciones	Ctrl+U
Configurar IA	Ctrl+I	Historial	Ctrl+H
Opciones	Ctrl+,	Ayuda y consola	F1 o Ctrl+T

03 / DATOS LOCALES

Catálogo local y fuentes

WinCVE guarda los registros en SQLite. Puedes consultar la copia local sin Internet y conectarte cuando necesites actualizarla.

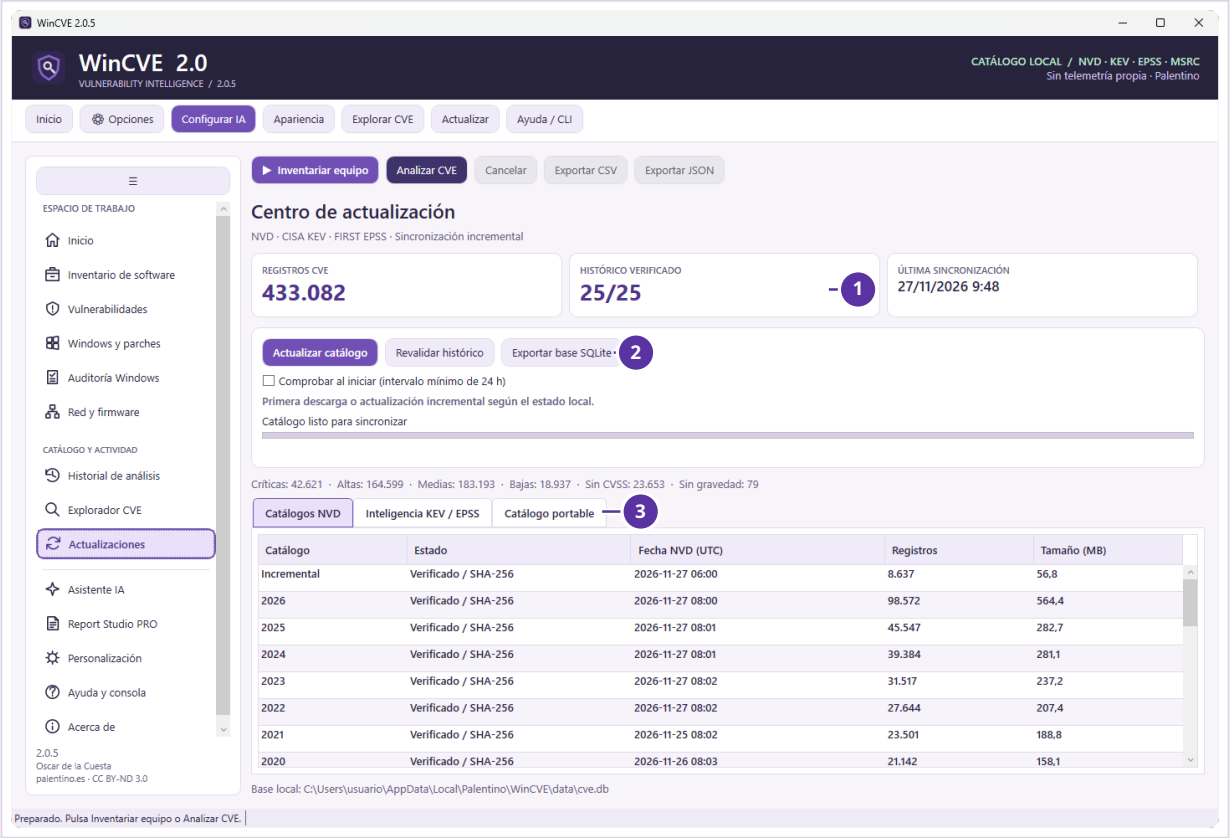

Figura 2. Centro de actualización. Comprueba la cobertura y la fecha de sincronización de tu propia copia.

1 **Comprueba la cobertura.** En **Actualizaciones**, revisa registros, histórico verificado y última sincronización. Contrasta el estado y la fecha UTC de los catálogos en la tabla.

2 **Actualiza NVD.** Pulsa **Actualizar catálogo** para el flujo normal. **Revalidar histórico** revisa los catálogos anuales cuando necesitas comprobar la cobertura.

3 **Actualiza los indicadores.** Abre **Inteligencia KEV / EPSS** y pulsa **Actualizar KEV y EPSS**. La pestaña **Catálogo portable** permite comprobar, exportar o recuperar un catálogo.

MSRC y Diccionario CPE

Windows y parches sincroniza sus propias publicaciones MSRC. El Diccionario CPE admite una importación local desde los formatos oficiales de NIST.

La opción **Comprobar al iniciar** revisa el catálogo al abrir WinCVE, con un intervalo mínimo de 24 horas.

04 / ACTUALIZACIONES

Actualizar y comprobar fuentes

Los indicadores del panel proceden de copias locales con sus propias fechas. Antes de analizar un equipo, comprueba la cobertura histórica y la fecha de la fuente que vas a utilizar.

Cómo elige WinCVE el modo de actualización NVD

Situación	Qué hace la versión 2.0.5
Catálogo completo y reciente	Consulta el fichero de modificaciones de NVD. Verifica la fecha, el tamaño y el SHA-256 cuando descarga contenido nuevo.
Faltan años o la copia ha quedado fuera del intervalo	Revisa el histórico desde 2002. El motor usa un margen de siete días para decidir cuándo necesita recuperarlo.
Revalidar histórico	Comprueba los metadatos de los catálogos anuales y del incremental. Cuando la huella coincide, puede actualizar su marca sin descargar otra vez el contenido.

Actualizar cada fuente desde su pantalla

1. **NVD.** En **Actualizaciones › Actualizar catálogo** inicia la actualización normal. Para un fichero local, usa **Explorador CVE › Importar NVD JSON / GZ** y comprueba el resultado de la importación.
2. **CISA KEV y FIRST EPSS.** En **Actualizaciones › Inteligencia KEV / EPSS**, pulsa **Actualizar KEV y EPSS**. La opción **Importar KEV / EPSS offline** admite JSON de CISA y CSV de FIRST comprimido como GZIP.
3. **Windows y parches.** Usa **Sincronizar MSRC** y comprueba los meses disponibles en **Publicaciones locales**.

> **Comprueba el resultado de una sincronización interrumpida**
>
> WinCVE conserva los catálogos cuya importación ya se confirmó. Revisa el estado de cada fichero y la última sincronización completada. Si indica metadatos futuros, comprueba la fecha y hora de Windows antes de reintentar.

NIST · Catálogos y metadatos de NVD ›

05 / CONSULTA DEL CATÁLOGO

Explorar y filtrar CVE

En **Explorador CVE**, busca por el identificador exacto o por palabras de la descripción. Usa gravedad y año para acotar una consulta amplia.

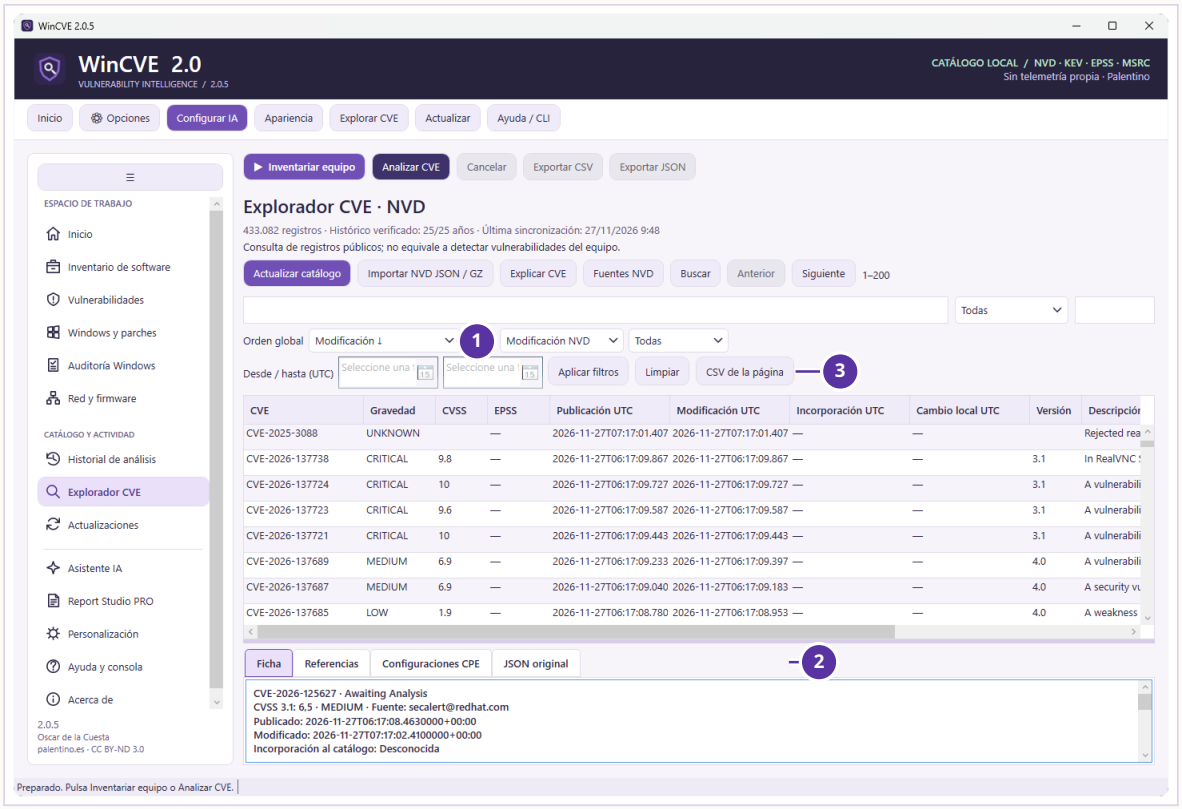

Figura 3. Explorador con orden global, filtros por fechas UTC y cuatro pestañas de detalle.

1 **Orden y filtros.** Elige **Orden global**, el campo **Fecha** y un periodo. Pulsa **Aplicar filtros**. Puedes ordenar todo el conjunto por fecha, CVSS, EPSS o gravedad.

2 **Detalle.** Selecciona una fila. Abre **Ficha**, **Referencias**, **Configuraciones CPE** o **JSON original** según la evidencia que necesites.

3 **Exportación. CSV de la página** guarda las filas de la página visible con sus fechas y descripción. Usa **Anterior** o **Siguiente** para consultar el resto.

Campo UTC	Qué fecha representa
Publicación NVD	Primera publicación del registro en la fuente.
Modificación NVD	Última modificación que informa la fuente.
Primera importación	Primera incorporación de esa CVE registrada por tu copia local.
Último cambio local	Último cambio real importado. «Desde última sinc.» usa este campo.

06 / FILTROS Y ORDEN

Consultas por fechas UTC

En el Explorador, **Fecha** decide qué dato se filtra y **Orden global** decide cómo se ordenan los resultados. Puedes elegir ambos de forma independiente.

Pregunta	Ajustes del Explorador	Qué vas a obtener
¿Qué se publicó esta semana?	Fecha **Publicación NVD** y periodo **Últimos 7 días**. Orden **Publicación** descendente.	Primera publicación de los registros que entran en ese periodo.
¿Qué registros se revisaron este mes?	Fecha **Modificación NVD**, periodo **Personalizado** y fechas UTC. Orden **Modificación** descendente.	Registros con una modificación informada por NVD en el intervalo.
¿Qué datos se incorporaron a mi copia?	Fecha **Primera importación**, periodo deseado y orden **Incorporación** descendente.	Registros cuya primera incorporación está fechada en tu copia local.

Un mismo registro puede tener cuatro fechas

Ejemplo ficticio. NVD publica una CVE el día 18 y revisa su ficha el 26. WinCVE la incorpora el 24 y descarga la revisión el 27.

Campo	Fecha de ejemplo	De dónde sale
Publicación NVD	18 de noviembre	Primera publicación del registro.
Modificación NVD	26 de noviembre	Última modificación publicada por NVD.
Primera importación	24 de noviembre	Primera incorporación anotada en esta copia.
Último cambio local	27 de noviembre	Importación de la versión revisada de la ficha.

Dos detalles al revisar tus resultados

Año filtra por los cuatro dígitos del identificador CVE. **Desde última sinc.** usa el último cambio local y toma como inicio la marca de la última sincronización completada. Las marcas locales desconocidas quedan fuera de los filtros de fecha local.

07 / INTELIGENCIA

Leer indicadores y priorizar

Empieza por producto y versión. Una vez contrastada la aplicabilidad, usa las señales del catálogo para ordenar el trabajo de corrección.

Indicador	Cómo usarlo
CVE y CPE	CVE identifica la vulnerabilidad. CPE identifica el producto o la plataforma. Revisa fabricante, versión y condiciones de aplicación.
CVSS	Gravedad técnica en una escala de 0 a 10. Consulta la versión del estándar y la fuente del valor cuando estén disponibles.
KEV	Una entrada de CISA indica evidencia de explotación observada. Contrasta las medidas publicadas y la fecha de tu copia.
EPSS	Estimación de la probabilidad de observar explotación del CVE en los próximos 30 días. Lee el porcentaje y la fecha del modelo.

Prioridades en WinCVE 2.0.5

El motor de correlación de software y firmware aplica el primer criterio que encaja en este orden. Una marca ausente indica que falta esa señal en la ficha o en la fuente local.

Prioridad	Criterio de la aplicación
P1 · KEV	La CVE figura en el catálogo KEV disponible.
P2 · EPSS	EPSS igual o superior al 10 %.
P3 · CVSS crítico	CVSS igual o superior a 9,0.
P4 · CVSS alto	CVSS igual o superior a 7,0.
P5 · Evaluar	Demás casos, incluidos los que tienen señales incompletas.

> **Decide con datos del equipo**
>
> Si un hallazgo aparece como P1, valida la versión exacta y el aviso del fabricante. Ajusta el plazo a la exposición, al impacto operativo y a las mitigaciones ya activas.

Si la evidencia incluye un percentil EPSS, léelo como una posición relativa. El porcentaje EPSS es la probabilidad que usa WinCVE al calcular P2.

Ver las fuentes de CVSS, KEV y EPSS ›

08 / SOFTWARE LOCAL

Inventario y correlación

El inventario lee las entradas de desinstalación registradas para el equipo y el usuario actual. La correlación cruza los productos identificados con el catálogo local.

1. **Pulsa Inventariar equipo.** Abre **Inventario de software**. Filtra por nombre, fabricante, versión o ámbito. Selecciona una fila para consultar la evidencia de registro.
2. **Pulsa Analizar CVE.** Abre **Vulnerabilidades › Hallazgos**. Comprueba qué producto y versión se han asociado, qué CVE aparece y con qué evidencia.
3. **Comprueba la cobertura.** En **Cobertura y productos sin mapa**, revisa las entradas sin versión, sin asociación, con asociación ambigua o sin criterios disponibles. Evalúa el software portable, los paquetes MSIX y las dependencias con su inventario específico.

Estado frecuente	Qué revisar
Coincidencia CPE	Verifica proveedor, versión, edición y rango del aviso. Comprueba si hay parches o variantes del producto que alteren la aplicabilidad.
Revisión necesaria	Abre la evidencia y resuelve la condición pendiente. Puede depender de una comparación de versiones, de otros componentes o de una configuración CPE compleja.
Sin asociación o sin versión	Contrasta la aplicación con el inventario del fabricante. Si procede, documenta una asociación CPE y vuelve a analizar.

Crear una asociación CPE verificada

En **Vulnerabilidades › Diccionario CPE**, importa el diccionario oficial en JSON o XML. Selecciona el producto en Cobertura, pulsa **Usar aplicación de Cobertura** y comprueba el fabricante y el producto de la fila antes de **Guardar asociación verificada**. Repite el análisis para usar el mapa guardado.

> **Al cerrar una revisión**
>
> Anota el CVE, la versión instalada, el enlace al aviso y la decisión. Si la evidencia es insuficiente, registra qué dato falta y quién lo puede validar.

09 / VALIDACIÓN DE HALLAZGOS

Del hallazgo a la decisión

Parte de **Vulnerabilidades › Hallazgos** y usa la ficha del Explorador para contrastar la asociación. El resultado final debe indicar qué comprobaste en el equipo y qué criterio lo respalda.

1. **Identifica qué observó WinCVE.** Apunta la aplicación, el editor y la versión que figuran en el inventario. En el detalle del hallazgo, lee el criterio CPE, el rango y el motivo de la coincidencia o de la revisión.
2. **Abre la ficha del mismo CVE.** Busca el identificador en **Explorador CVE**. Revisa **Configuraciones CPE** y **Referencias**. Comprueba en el aviso original el producto, la edición y la versión corregida.
3. **Resuelve el alcance real.** Comprueba si existen componentes opcionales, versiones de un proveedor distinto o correcciones integradas por tu distribuidor. Si el formato de versión no coincide, valida con la herramienta de inventario o con el proveedor.
4. **Anota una decisión.** Registra qué versión está instalada, en qué fecha la verificaste y por qué consideras el caso aplicable, descartado o pendiente de evidencia. Conserva el enlace que respalda el criterio.

Cómo leer un límite de versión

Dato observado	Lectura de ejemplo
versionEndExcluding = 24.07	El criterio de ejemplo termina antes de 24.07. La versión 24.06 entra en ese límite superior.
versionEndIncluding = 24.07	El criterio de ejemplo incluye 24.07. Comprueba también el límite inferior y el resto de condiciones.
Revisión necesaria	Busca qué condición queda por verificar, por ejemplo, una versión sin formato comparable o una combinación de productos.

> **Para priorizar la corrección**
>
> Consulta la prioridad P1–P5 del hallazgo y valora el uso real del software, la exposición y el impacto en el servicio. Vuelve a inventariar después del cambio y registra la versión final.

10 / SISTEMA OPERATIVO

Windows, parches y auditoría

WinCVE permite revisar por un lado la compilación y las KB observadas y por otro el estado de controles de seguridad del equipo.

Evaluar Windows con MSRC

1. **Selecciona Windows y parches › Inventariar Windows / KB.** Anota edición, arquitectura y compilación. Revisa los indicadores de reinicio pendiente.
2. **Carga las publicaciones.** Usa **Sincronizar MSRC** con Internet o **Importar CVRF JSON** con un archivo local de confianza. Verifica los meses disponibles en **Publicaciones locales**.
3. **Elige el producto MSRC exacto.** Contrasta edición, versión y arquitectura del equipo. Después pulsa **Evaluar build** y abre **Evaluación MSRC** para revisar la evidencia y el enlace de cada resultado.

> **Si una KB no aparece**
>
> Comprueba la compilación actual, la compilación corregida indicada por Microsoft y las actualizaciones acumulativas que puedan sustituir a esa KB. Registra como pendiente de validación cualquier caso con evidencia incompleta.

Comprobar controles con Auditoría Windows

Pulsa **Auditar Windows** para leer la configuración actual. El módulo revisa, entre otros, Firewall, Defender, BitLocker, Secure Boot, TPM, UAC, SMB y Escritorio remoto. Cada fila aporta estado, evidencia y origen del dato.

Observación	Acción de revisión
Lectura completada	Contrasta el valor con la política aplicable al equipo.
Lectura incompleta	Revisa el motivo en la evidencia y comprueba el control desde la herramienta de administración que corresponda.

Exporta CSV o JSON cuando necesites incorporar el resultado a un parte. La auditoría se ejecuta en modo de solo lectura.

11 / DISPOSITIVOS

Red y firmware

El inventario de red muestra lo que conoce el equipo Windows. La evaluación de firmware usa perfiles registrados con datos que puedas verificar.

Consultar la red local en modo pasivo

1. **Ve a Red y firmware › Inventario de red.** Pulsa **Leer red local** para ver interfaces, puertas de enlace y vecinos presentes en la caché de Windows.
2. **Contrasta la observación.** Usa el inventario de activos o la consola de gestión del equipo para confirmar qué dispositivo corresponde a cada entrada. La caché recoge vecinos observados desde ese Windows y puede estar incompleta.

Evaluar un firmware conocido

1. **Obtén la identificación exacta.** Consulta la etiqueta o la consola de administración de un equipo bajo tu gestión. Registra fabricante, modelo, revisión de hardware y versión de firmware.
2. **Rellena Dispositivos y firmware.** Selecciona el tipo de CPE adecuado (sistema o hardware) y usa los identificadores de fabricante y producto verificados, además de los datos del perfil. Pulsa **Guardar perfil**.
3. **Revisa el resultado de Evaluar CVE.** Selecciona el perfil, ejecuta la consulta y contrasta las coincidencias con el aviso del fabricante para esa revisión y esa versión. Puedes exportar la evaluación en CSV o JSON.

Dato	Dónde validarlo
Modelo y revisión	Etiqueta, consola de administración o inventario de activos.
Versión de firmware	Pantalla de estado del dispositivo y documentación de la versión.
Corrección disponible	Aviso de seguridad y notas de publicación del fabricante.

> **Evidencia mínima para un parte de firmware**
>
> Conserva el modelo y la revisión, la versión observada, la fecha, el aviso de seguridad y la decisión de actualización o revisión.

12 / DOCUMENTACIÓN

Informes e historial

Elige el informe según el trabajo realizado. Conserva la fecha, el alcance, la evidencia y la versión del catálogo junto al resultado.

Informe de software en Report Studio PRO

1. **Ejecuta Analizar CVE.** Entra en **Report Studio PRO** y confirma que el resumen corresponde al análisis de software que quieres documentar.
2. **Configura el informe.** Indica título y organización. Elige el anexo técnico y revisa la opción **Ocultar nombre del equipo, rutas del registro y detalles de avisos**.
3. **Pulsa Generar informe HTML.** Guarda y abre el resultado. Para compartir una copia en PDF, usa la opción de impresión del navegador y el destino **Guardar como PDF**.

Análisis integral

En **Inicio › Análisis integral** o desde **Report Studio PRO**, puedes coordinar software, Windows, perfiles de firmware, auditoría y red pasiva. Para evaluar MSRC indica el producto exacto. Usa **Omitir MSRC** si todavía debes verificarlo.

Pulsa **Iniciar análisis integral**, revisa el estado de cada etapa y exporta en HTML o JSON antes de cerrar la aplicación. El informe recoge la cobertura y las acciones propuestas por módulo.

Salida	Para qué usarla
HTML	Parte legible o informe de auditoría. Abre el archivo localmente y revisa el anexo.
CSV	Revisión tabular de inventario, hallazgos u otros módulos que ofrecen ese formato.
JSON	Conservar campos de evidencia o consumir resultados en otro proceso.

Historial y alcance al compartir

Historial de análisis permite reabrir inventarios guardados. Exporta los informes que quieras conservar y comprueba qué versiones, evidencias y datos del equipo quedan visibles antes de compartirlos.

13 / REPORT STUDIO PRO

Leer un análisis integral

Desde **Inicio › Análisis integral**, revisa el estado de cada módulo antes de interpretar la lista de actuaciones. El informe incorpora la cobertura de la ejecución.

Estado	Cómo leerlo
Completado	El módulo terminó dentro de su alcance. Lee sus recuentos y conserva las fechas de las fuentes.
Parcial	Hay criterios útiles y faltan comprobaciones. El detalle indica qué faltó. MSRC y firmware se informan como parciales cuando se evalúan por su alcance orientativo.
No comprobado	Falta un requisito, por ejemplo, un producto MSRC declarado, catálogo NVD o perfiles de firmware.
Error	Abre el módulo específico para revisar el mensaje. Corrige el problema y vuelve a ejecutar el análisis que necesites.

1. **Antes de ejecutar.** Actualiza las fuentes pertinentes, comprueba los perfiles de firmware y usa **Cargar productos MSRC** si puedes indicar el producto exacto de tu Windows.
2. **En la lista de actuaciones.** Usa las prioridades de software y firmware. Para cada criterio MSRC, contrasta la compilación y la actualización acumulativa. Para Auditoría Windows, comprueba el estado frente a la política del equipo.
3. **En el archivo exportado.** El HTML presenta el alcance, las primeras 50 acciones y un anexo con el conjunto de resultados. Usa JSON cuando quieras tratar todas las filas con otro programa.

> **Ejemplo de lectura por módulo**
>
> Si ves 2 coincidencias de software, 1 criterio MSRC y 3 controles para revisar, registra esas cantidades por módulo. Comprueba el criterio y la evidencia antes de dar por confirmado cada caso.

La salida integral puede mostrar productos, versiones y evidencias sensibles. Revisa el anexo antes de circular el informe.

14 / ASISTENTE IA

Configurar un proveedor de IA

Abre **Configurar IA** en la barra superior o pulsa **Ctrl+I**. En el Centro de configuración puedes preparar y probar un proveedor antes de consultar una CVE.

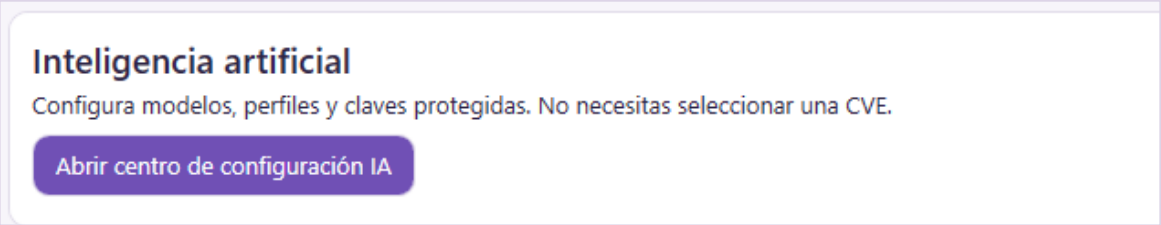

Figura 4. Acceso al Centro de configuración IA desde Personalización. También está en la barra superior.

Ejemplo completo con OpenAI

1. **Obtén la clave API del proveedor.** En la plataforma de OpenAI, crea una clave para un proyecto con acceso a la API. La facturación de la API se gestiona de forma independiente de la suscripción de ChatGPT.
2. **Introduce la clave en WinCVE.** En **Proveedor** elige **OpenAI**. Pega la clave en **Clave API** dentro del centro de configuración. Mantén la clave fuera de capturas, informes y repositorios.
3. **Elige un modelo.** Pulsa **Cargar modelos** y autoriza la conexión. Selecciona uno compatible con chat o escribe su identificador completo en **Modelo (ID exacto)**.
4. **Haz una prueba.** Pulsa **Probar IA** y autoriza el envío del mensaje sintético. Comprueba que aparece una respuesta y su tiempo en milisegundos. El proveedor puede contabilizar la prueba como uso de la API.
5. **Guarda la selección. Guardar perfil** conserva la configuración de ese proveedor. **Guardar y usar por defecto** lo selecciona para el asistente. Marca **Recordar clave cifrada en este equipo** si quieres conservarla para tu cuenta de Windows.

Si has elegido guardar el perfil sin recordar la clave, introdúcela de nuevo en el asistente cuando la necesites en otra sesión.

> **Con OpenRouter**
>
> Sigue los mismos pasos con su propia clave API y un ID de modelo del catálogo de OpenRouter. La consulta puede llegar al proveedor que ejecuta el modelo.

OpenAI · Dónde obtener una clave API ›

OpenRouter · Guía oficial de inicio ›

Continuar con la consulta de una CVE ›

15 / EJERCICIO GUIADO

Consultar una CVE con IA

Busca **CVE-2024-11477**, un aviso de 7-Zip, y usa el asistente para preparar una revisión de alcance, versiones y mitigación.

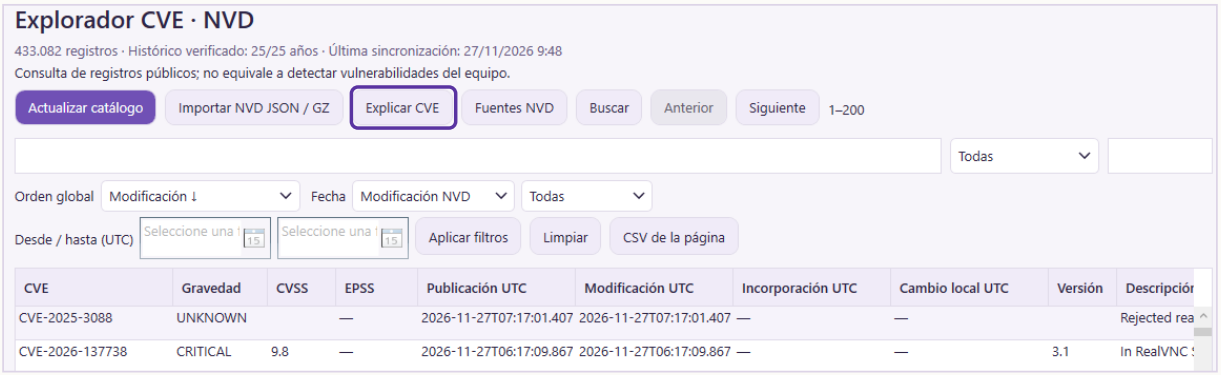

Figura 5. Explicar CVE usa la fila que selecciones. En el ejercicio, busca y selecciona CVE-2024-11477.

1. **Busca el identificador.** Abre **Explorador CVE**, escribe **CVE-2024-11477** y pulsa **Buscar**. Si tienes filtros activos, límpialos antes de repetir la consulta.
2. **Selecciona el registro y pulsa Explicar CVE.** WinCVE abre **Asistente IA**, copia el identificador y prepara una primera evidencia. También puedes escribir el ID directamente en el asistente.
3. **Ajusta la consulta.** Selecciona **Mitigación y verificación** y el proveedor que configuraste. Pulsa **Preparar evidencia** después de cambiar el tema. Para empezar con la ficha local, selecciona **Ficha offline (sin IA)**.
4. **Lee la evidencia y consulta.** Comprueba el contenido de **Evidencia que utiliza la IA**. Pulsa **Consultar** y, si usas un servicio remoto, autoriza ese envío. El resultado aparece en **Respuesta**.
5. **Verifica y registra el resultado.** Abre el aviso de CERT-EU y comprueba la versión instalada en el equipo. El aviso documenta la corrección en 7-Zip 24.07. Registra versión observada, decisión y evidencia antes de cerrar el caso.

> **Qué utiliza el asistente**
>
> La evidencia se forma con texto del catálogo local, métricas, criterios CPE y referencias, según disponibilidad. La respuesta te ayuda a interpretar esa información. Abre las referencias y contrasta el aviso antes de aplicar una decisión.

Ejemplo de nota de revisión

«CERT-EU sitúa la corrección en 7-Zip 24.07. La aplicabilidad queda pendiente hasta comprobar la versión instalada en este equipo. Si procede actualizar, registrar la versión corregida que se haya instalado y repetir el inventario».

CERT-EU · Aviso de 7-Zip usado en el ejercicio ›

16 / INFERENCIA EN TU EQUIPO

IA local con Ollama y LM Studio

WinCVE 2.0.5 puede usar un modelo que se ejecuta en el mismo equipo Windows. Prepara primero el servidor local y usa el identificador del modelo que reconoce ese servidor.

Ollama

1. **Instala y abre Ollama en Windows.** Mantén el servicio abierto. Para este ejercicio descarga **llama3.2**. La descarga inicial del modelo requiere acceso a su catálogo.

```powershell
ollama pull llama3.2
ollama list
```

2. **Conecta desde WinCVE.** En **Configurar IA › Proveedor**, elige **Ollama · local**. WinCVE busca el servicio en **127.0.0.1:11434**. Pulsa **Cargar modelos** y selecciona el que aparezca en la lista.
3. **Prueba y úsalo en el asistente.** Pulsa **Probar IA**. Al recibir respuesta, puedes guardar el perfil como predeterminado y seguir la consulta guiada de la página anterior.

LM Studio

1. **Carga un modelo de chat en LM Studio.** En su pestaña **Developer**, inicia el servidor local con **Start server** en **127.0.0.1:1234**.
2. **Selecciona LM Studio · local en WinCVE.** Carga los modelos, selecciona su ID y pulsa **Probar IA**. WinCVE 2.0.5 usa la conexión local sin token. Si tu instancia exige autenticación, elige un proveedor que encaje con la configuración de tu entorno.

> **Consulta con el modelo ya instalado**
>
> Comprueba que el modelo y el servidor procesan la consulta localmente. Para obtener solo el material de referencia del catálogo, también puedes abrir **Ficha offline (sin IA)**.

Ollama · Documentación para Windows ›

LM Studio · Servidor local ›

17 / MODO TEXTO

IA desde PowerShell

Los comandos de IA de **WINCVE_CLI.bat** usan el catálogo local para preparar la consulta. Para un proveedor remoto, la CLI lee su variable de entorno y solicita que indiques **--allow-remote**.

Abrir la ficha o consultar un modelo local

POWERSHELL

```
$cve = 'CVE-2024-11477'
.\WINCVE_CLI.bat explain $cve --provider offline --topic 3
.\WINCVE_CLI.bat ai-models --provider ollama
.\WINCVE_CLI.bat explain $cve --provider ollama --model llama3.2 --topic 3
```

El primer **explain** muestra la ficha local. El segundo usa Ollama y requiere que el modelo esté instalado y que el servicio responda en ese Windows.

Ejemplo con OpenAI en una sesión de PowerShell

POWERSHELL

```
$clave = Read-Host 'Clave API de OpenAI' -AsSecureString
$env:OPENAI_API_KEY = [System.Net.NetworkCredential]::new('', $clave).Password
.\WINCVE_CLI.bat ai-models --provider openai --allow-remote
$modelo = Read-Host 'ID exacto del modelo'
.\WINCVE_CLI.bat ai-test --provider openai --model $modelo --allow-remote
$consulta = @('explain', $cve, '--provider', 'openai', '--model', $modelo,
              '--topic', '3', '--allow-remote', '--json')
.\WINCVE_CLI.bat @consulta
Remove-Item Env:OPENAI_API_KEY
Remove-Variable clave
```

Ejecuta este ejemplo con **$cve** definido en el bloque anterior. **ai-test** envía un mensaje sintético. En **explain**, **--allow-remote** autoriza que la evidencia CVE se envíe al proveedor seleccionado.

--topic	Tema	--topic	Tema
1	Resumen y alcance	3	Mitigación y verificación
2	Prioridad y exposición	4	Explicación didáctica

Consulta **ai-providers** para conocer la variable de entorno de cada servicio, como **OPENROUTER_API_KEY** para OpenRouter.

18 / ASISTENTE IA

Resolver incidencias de IA

Prueba en este orden. Primero localiza la CVE en el catálogo, después conecta el proveedor y finalmente usa el modelo elegido para generar la respuesta.

Mensaje o síntoma	Qué revisar en WinCVE 2.0.5
«CVE no encontrada»	Comprueba el identificador en el Explorador y la fecha del catálogo. Actualiza o importa NVD si el registro falta.
Consultar está deshabilitado	Pulsa **Preparar evidencia** después de cambiar de CVE o de tema. Si hay una operación en curso, deja que finalice o cancélala.
HTTP 401	Comprueba que la clave pertenece al proveedor y al proyecto seleccionado.
HTTP 403 o 404	Revisa los permisos de la clave, el acceso al modelo o que su ID coincida con el que devolvió el proveedor.
HTTP 402 o 429	Revisa el saldo, la facturación, los límites de peticiones y la cuota en el panel del proveedor.
Hay modelos en la lista y la prueba falla	Prueba un modelo compatible con chat. El listado y la inferencia son operaciones distintas.
Ollama o LM Studio no responde	Comprueba que el servicio está abierto en el mismo Windows y que utiliza su puerto local previsto.

Perfiles y recuperación de claves

Los perfiles de la interfaz se guardan en **data/ai-profiles.dpapi**, vinculados a la cuenta de Windows. **Olvidar clave** retira la credencial del perfil. Si cambiaste de usuario o de equipo y el archivo ya no se abre, cierra WinCVE, conserva ese archivo bajo otro nombre en una ubicación privada y vuelve a configurar el proveedor.

> **Proveedores incluidos en 2.0.5**
>
> Además de Ollama y LM Studio, puedes elegir OpenAI, OpenRouter, Anthropic Claude, Google Gemini, DeepSeek, Mistral AI, Groq y xAI Grok. Cada servicio tiene su clave, su catálogo y sus condiciones de uso.

OpenAI · Gestión de facturación de ChatGPT y de la API ›

19 / ESPACIO DE TRABAJO

Personalización e integraciones

Abre **Apariencia** en la barra superior o **Personalización** en el menú lateral para adaptar la aplicación a tu pantalla y a tu forma de trabajar.

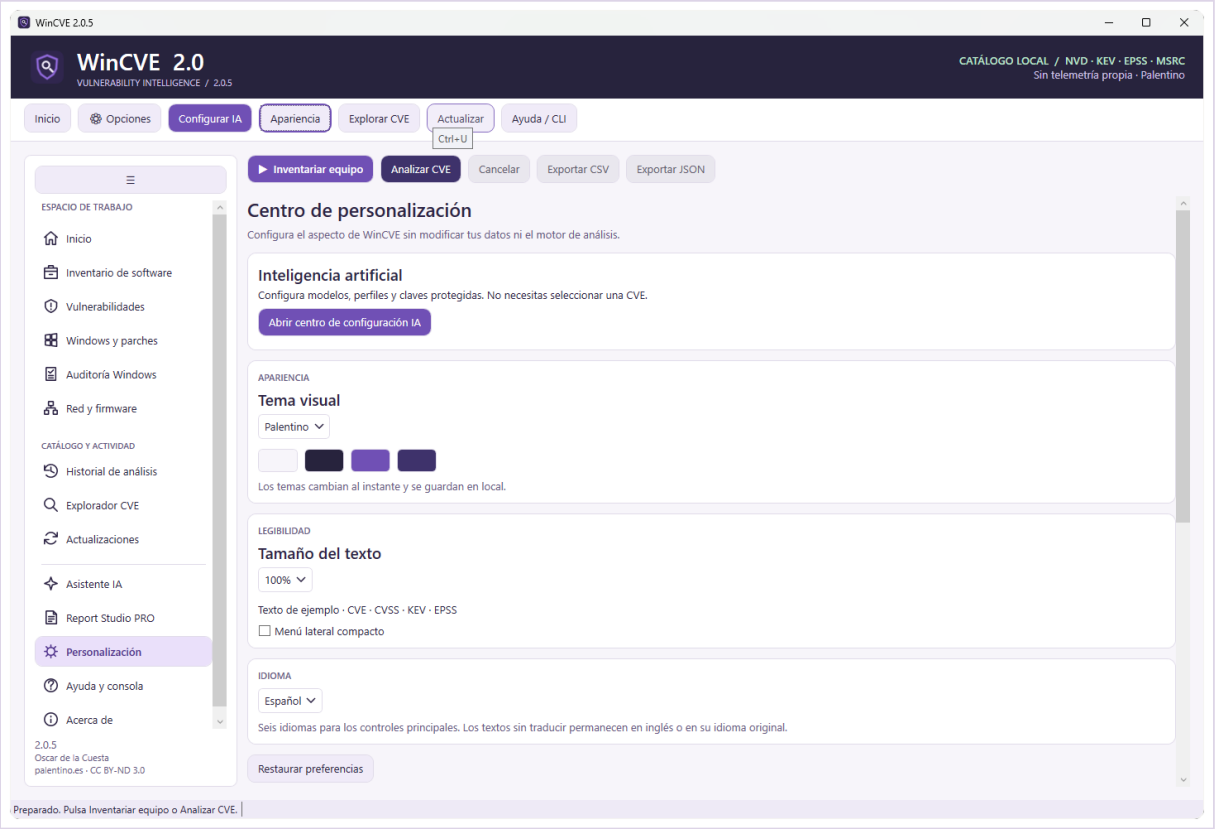

Figura 6. Centro de personalización con el acceso al centro de configuración de IA.

Preferencia	Opciones
Tema visual	Palentino, Dark PRO, Light PRO, Cream, Cyber y Graphite.
Tamaño y navegación	Escala de texto del 90, 100, 110 o 120 %. Activa el menú lateral compacto si necesitas más espacio.
Idioma de la aplicación	Español, inglés, francés, alemán, italiano y portugués. Selecciona Auto / System para usar el idioma de Windows si está disponible.

Las preferencias se guardan para el siguiente inicio. Los registros de la fuente y algunas pantallas conservan su idioma original.

PalClam y Modern Terminal AI. En Opciones encontrarás accesos a las webs y a las aplicaciones complementarias de Palentino. Puedes comprobar si están instaladas o seleccionar su ejecutable para abrirlas.

20 / MODO TEXTO

Primeros pasos en consola

Abre PowerShell en la carpeta de WinCVE que contiene **WINCVE_CLI.bat**. Puedes consultar el catálogo local sin abrir la interfaz gráfica.

```powershell
.\WINCVE_CLI.bat version
.\WINCVE_CLI.bat doctor
.\WINCVE_CLI.bat status --json
.\WINCVE_CLI.bat intel-status --json
.\WINCVE_CLI.bat cve CVE-2024-11477
.\WINCVE_CLI.bat help search
```

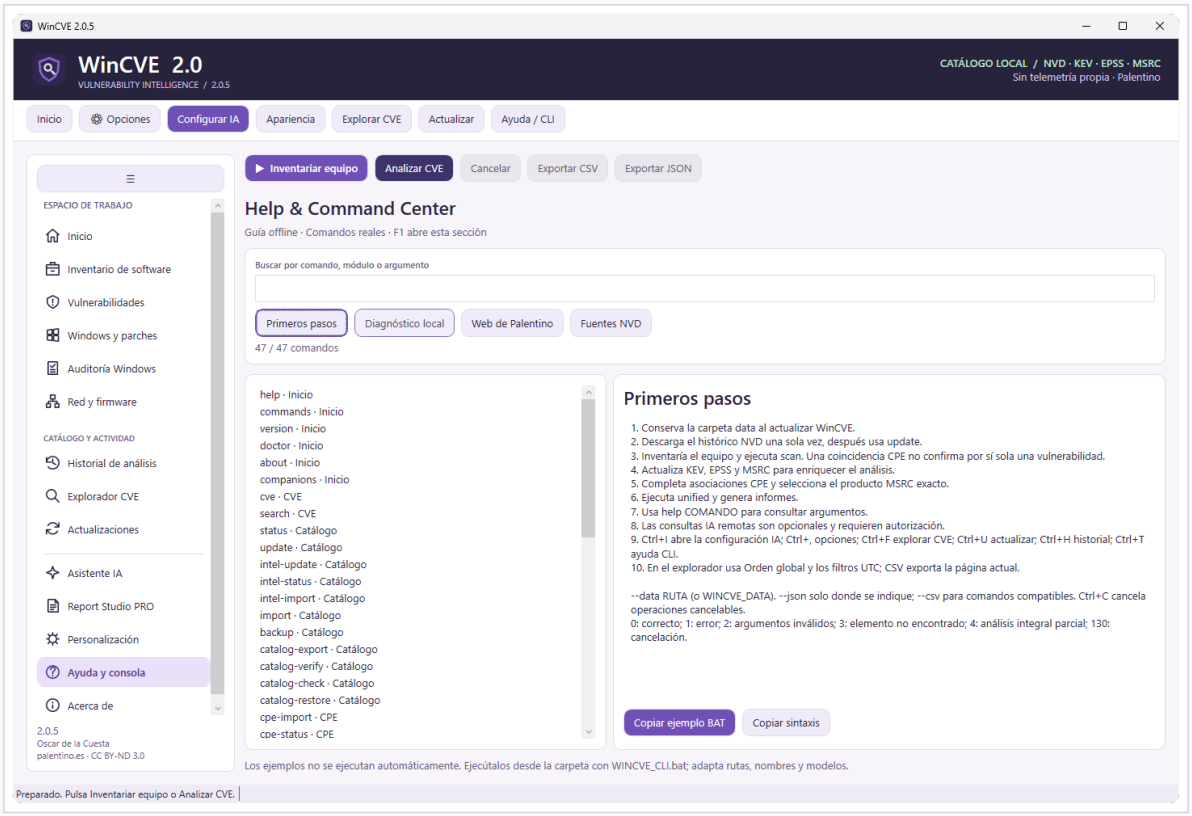

Figura 7. Ayuda y consola ofrece búsqueda de comandos, sintaxis y ejemplos que puedes copiar.

doctor revisa rutas y archivos locales. **status** sí consulta la cobertura de NVD. **intel-status** permite comprobar las fechas de KEV y EPSS.

Pulsa **F1** en la aplicación o ejecuta **commands** en consola para consultar los 47 comandos documentados en la versión 2.0.5.

21 / POWERSHELL

Consultas y tareas repetibles

Usa argumentos explícitos para reproducir una consulta y guarda el resultado con un nombre que identifique el periodo o la ejecución.

Buscar por publicación o por cambios

```powershell
.\WINCVE_CLI.bat search "7-Zip" --sort published-desc --limit 20
.\WINCVE_CLI.bat search --date-field modified `
  --since 2026-11-01 --until 2026-12-01 --dates --limit 50
```

El segundo ejemplo consulta modificaciones de noviembre en UTC. El límite **--until** es exclusivo. **--dates** añade las columnas temporales a la salida de texto. Usa **--json** para obtener fechas estructuradas.

Guardar inventario, correlación e informe

```powershell
.\WINCVE_CLI.bat inventory --json > inventario.json
.\WINCVE_CLI.bat scan --save --json > hallazgos.json
.\WINCVE_CLI.bat unified --output informe-integral.html
$LASTEXITCODE
```

scan --save guarda el historial del análisis. Comprueba **$LASTEXITCODE** justo después de cada uso en un script. Para exportar solo el informe de software en HTML, consulta **help report**.

Código	Significado	Código	Significado
0	Operación correcta	**3**	Elemento sin localizar
1	Error de ejecución	**4**	Análisis integral parcial
2	Argumentos inválidos	**130**	Operación cancelada

> **Confirma la ubicación de datos**
>
> Puedes indicar **--data RUTA** o usar **WINCVE_DATA**. El argumento explícito tiene prioridad. Verifica con **doctor** la carpeta que va a utilizar la consola.

22 / COMANDOS DE USO HABITUAL

Referencia rápida de la CLI

Ejecuta los comandos con **WINCVE_CLI.bat** y consulta **help COMANDO** para obtener la sintaxis completa en tu copia de WinCVE.

Tarea	Comandos	Cuándo usarlos
Encontrar comandos	help, commands, version, doctor	Sintaxis, versión instalada y ubicación local de datos.
Consultar el catálogo	cve, search, status, intel-status	Consultar un ID y comprobar cobertura y fechas.
Conservar el catálogo	backup, catalog-check, catalog-export, catalog-verify	Copia, comprobación local y verificación de un ZIP transportable.
Poner al día las fuentes	update, intel-update, windows-update	Actualizar NVD, inteligencia KEV/EPSS o publicaciones MSRC, respectivamente.
Investigar el equipo	inventory, scan, audit, windows-inventory, windows-products	Software, correlación, configuración, compilación y productos MSRC disponibles.
Consultar CPE o firmware	cpe-status, cpe-search, device-list, firmware-scan	Buscar correspondencias y evaluar un perfil ya registrado.
Documentar	report, unified, dashboard-history	Generar un informe o consultar el historial de análisis guardados.
Utilizar IA	ai-providers, ai-models, ai-test, explain	Consultar proveedores y modelos, probar y explicar una CVE.

Tres ejemplos que puedes copiar

POWERSHELL

```
.\WINCVE_CLI.bat commands --filter windows
.\WINCVE_CLI.bat search "7-Zip" --limit 50 --offset 50 --json
.\WINCVE_CLI.bat help catalog-restore
```

En **search**, un desplazamiento de 50 empieza después de los primeros 50 resultados. Conserva el mismo filtro, orden y versión del catálogo si vas a recopilar varias páginas.

23 / MANTENIMIENTO

Copias, restauración y migración

Usa una copia de la carpeta de datos para recuperar tu instalación. Para mover solo el catálogo de vulnerabilidades, crea el ZIP desde WinCVE.

Modalidad	Directorio de datos habitual
Instalador EXE	%LOCALAPPDATA%\Palentino\WinCVE\data
Portable ZIP	Carpeta data junto a WinCVE.exe
Ruta personalizada	WINCVE_DATA para la aplicación. La CLI también admite --data.

Respaldar o migrar una instalación

1. **Cierra la interfaz y la consola.** Comprueba la ruta en pantalla o con **doctor**. Copia la carpeta **data** completa a una ubicación privada si quieres conservar bases, inventarios y preferencias.
2. **Migra con copia previa.** La versión 2.0.5 añade campos e índices temporales a **cve.db**. Conserva la copia anterior para poder volver a la versión previa. Al abrir 2.0.5, revisa el catálogo y el directorio de datos.

Transportar el catálogo SQLite

1. **Exporta y verifica.** En **Actualizaciones › Catálogo portable**, pulsa **Crear catálogo ZIP** y después **Verificar paquete**. La aplicación exporta NVD, KEV y EPSS junto con el manifiesto.
2. **Restaura en el destino.** En el mismo panel, usa **Restaurar catálogo / copia**. Si ya existe un catálogo, verifica el origen y confirma la sustitución solo cuando corresponda. WinCVE crea una copia del catálogo previo en **data/backups**.

```powershell
.\WINCVE_CLI.bat catalog-export catalogo.zip
.\WINCVE_CLI.bat catalog-verify catalogo.zip
```

> **Datos de cada instalación**
>
> Las fechas locales desconocidas permanecen vacías tras migrar. El ZIP de catálogo público se genera sin las marcas locales de importación. Para conservar MSRC, el Diccionario CPE y el inventario, usa la copia privada de **data**. Mantén las claves cifradas en su cuenta original.

24 / CASOS PRÁCTICOS

Dos recorridos de principio a fin

El primero parte de un aviso público de software. El segundo lleva un catálogo actualizado a un Windows que trabaja sin Internet.

1. Comprobar un aviso de 7-Zip

1. **Localiza CVE-2024-11477.** Pega el identificador en el Explorador. Abre **Ficha** y **Referencias**. El aviso de CERT-EU documenta que se corrigió en 7-Zip 24.07.
2. **Identifica la instalación real.** Abre **Inventario de software**, busca 7-Zip y confirma la versión. Si se trata de una edición portable, consulta la versión en la propia aplicación.
3. **Documenta y comprueba.** Si la versión instalada está afectada, adopta una versión compatible y actual desde su canal oficial. Registra la versión anterior, la nueva y el aviso. Vuelve a inventariar para confirmar el cambio.

2. Preparar una estación sin conexión

1. **Actualiza en un equipo conectado.** Comprueba cobertura y fechas de NVD, KEV y EPSS. Crea un ZIP de catálogo y verifícalo antes de trasladarlo por el medio aprobado por tu organización.
2. **Carga el catálogo en el destino.** Cierra otras instancias y restaura el paquete de confianza desde **Catálogo portable**. Verifica la cobertura y repite una consulta conocida del Explorador.
3. **Fecha el análisis.** Anota cuándo se sincronizó cada fuente. Haz la correlación local y deja constancia de qué módulos y publicaciones estaban disponibles al emitir el informe.

Ejemplo de registro de actuación sobre 7-Zip

Campo	Ejemplo
Producto y versión inicial	7-Zip 24.06 en un equipo de ejemplo.
Referencia y criterio	CVE-2024-11477. CERT-EU 2024-118 documenta la corrección en 24.07.
Decisión	Actualizar a la versión aprobada para el entorno que incluye la corrección.
Cierre	Registrar versión final observada, fecha de comprobación y responsable.

Abrir la relación de avisos y fuentes ›

25 / DIAGNÓSTICO

Resolver incidencias

Empieza comprobando la versión de WinCVE, la ruta de datos y el estado del catálogo. Estos pasos cubren los problemas habituales al abrir, consultar o actualizar.

Síntoma	Comprobación y acción
La edición portable no arranca	Confirma arquitectura y SHA-256. Extrae todo el ZIP en una carpeta escribible y ejecuta WinCVE.exe desde esa carpeta.
Catálogo vacío o no disponible	Consulta **doctor** y **status**. Comprueba la ruta y el espacio libre. Importa el catálogo incluido o restaura un paquete de confianza.
Una búsqueda queda vacía	Pulsa **Limpiar**, consulta el ID exacto y revisa año, gravedad, rango UTC y fecha de sincronización.
Fechas de importación en blanco	Pueden proceder de un catálogo publicado o de registros anteriores a la versión 2.0.5. Consulta publicación y modificación NVD cuando necesites esas fechas.
Actualización incompleta	Revisa el mensaje de estado, la conectividad y el espacio libre. Confirma las fechas de las copias locales y evita que dos procesos escriban en los mismos datos.
MSRC sin resultados	Comprueba meses importados, producto exacto, edición, compilación y arquitectura. Abre el aviso de Microsoft para validar la aplicabilidad.
La prueba de IA falla	Comprueba proveedor, disponibilidad del modelo y clave. Para IA local inicia el servidor correspondiente. Para IA remota revisa la autorización y la conectividad.

Si compilas y preparas una distribución

El mensaje **Missing KEV** aparece si los datos de la entrega carecen de registros KEV. Desde el proyecto, ejecuta **ACTUALIZAR_TODO.bat** y revisa su resumen de NVD, Intel y MSRC. Si el problema solo afecta a inteligencia, **ACTUALIZAR_INTEL.bat** actualiza KEV y EPSS.

Comprueba con **WINCVE_CLI.bat intel-status --json** que ambas fuentes tienen recuentos positivos en la ruta que usa **PREPARAR_DISTRIBUCION.bat**. Si falla la descarga, revisa el error de Intel o importa los archivos oficiales desde el centro de actualización. Las carpetas con sufijo **.incompleto** conservan resultados parciales para diagnóstico.

Ver dónde comunicar una incidencia ›

26 / REFERENCIAS

Fuentes y créditos

WinCVE Explorer & Control Center es un proyecto de Oscar de la Cuesta Campillo en Palentino. Esta guía cubre la edición 2.0.5 publicada para Windows.

Proyecto y soporte

Palentino · Página de WinCVE
Descargas por arquitectura, verificaciones SHA-256, galería y centro de confianza.

GitHub · Publicación v2.0.5
Paquetes públicos del instalador y del portable.

GitHub · Incidencias de WinCVE
Para reportar un problema, incluye versión, arquitectura, modalidad, pasos y el mensaje exacto. Revisa los datos que adjuntes.

Fuentes de inteligencia y ejemplo

NIST NVD · Vulnerabilidades y referencias
Consulta de registros, fechas, gravedad y enlaces técnicos.

NIST NVD · Diccionario CPE
Identificación normalizada de productos, sistemas y paquetes.

FIRST · Estándar CVSS
Especificaciones de la puntuación de gravedad técnica.

CISA · Known Exploited Vulnerabilities
Catálogo de vulnerabilidades explotadas de forma conocida.

FIRST · Exploit Prediction Scoring System
Metodología y significado de la probabilidad EPSS.

Microsoft · Security Update Guide
Avisos, productos y actualizaciones de seguridad de Microsoft.

CERT-EU · Aviso 2024-118 sobre 7-Zip
Referencia del caso CVE-2024-11477 utilizado en el manual.

Las capturas son de la galería de Palentino. Los procedimientos se contrastaron con el código, el archivo README, la guía CLI y el changelog del proyecto 2.0.5.

Licencia declarada por el proyecto · CC BY-ND 3.0 Unported
Las dependencias y los datos de terceros se rigen por sus propias condiciones.