centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1508

Procedimiento de Empleo Seguro
OLVIDO WINDOWS

Octubre 2022

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

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
2022.10.24 17:25:26 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-222-3

Fecha de Edición: octubre de 2022

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. **OLVIDO Windows es una solución *software* que realiza tareas de sobreescritura y borrado sobre los sistemas de archivos y discos** reconocidos por el sistema operativo Windows (32 y 64 bits) independientemente de su tecnología subyacente (Discos magnéticos, SSD, Flash USB, …) e interfaz (SATA, ATA, SCSI, …). El software solicita a la controladora del disco, a través de las APIs disponibles en el sistema operativo, las operaciones necesarias a nivel clúster para llevar a cabo las tareas de sobreescritura y borrado necesarias.
2. La aplicación OLVIDO ofrece al usuario la posibilidad de borrar de forma segura distintos elementos guardados en dispositivos de almacenamiento:
   - Ficheros y carpetas
   - Espacio Libre
   - Fragmentos de clúster no utilizados
   - Discos y volúmenes
3. Dispone de un módulo de planificación con el que podrá programar la ejecución de las tareas de borrado.
4. OLVIDO Windows provee la posibilidad de seleccionar el algoritmo de borrado a aplicar en cada tarea. Dispone de distintos algoritmos estándar ya implementados. Así mismo, permite al administrador la definición de algoritmos de borrado personalizados, especificando el número de pases y el patrón de sobreescritura a aplicar a cada uno de ellos.
5. Permite también la configuración de un destino Syslog para el envío de registros de actividad y estado de las tareas de borrado realizadas.

2. OBJETO Y ALCANCE

7. El objetivo del presente documento es detallar la **configuración de seguridad del producto OLVIDO Windows**, para que su funcionamiento se realice de acuerdo con unas garantías mínimas de seguridad. La configuración por defecto de la herramienta es la configuración considerada segura para sistemas bajo el alcance del ENS.
8. OLVIDO Windows es un producto *software* que se instala sobre el Sistema Operativo Windows.
9. La solución ha sido cualificada y aprobada y, por tanto, está **incluida en el Catálogo de Productos y Servicios STIC (CPSTIC) en la familia *'Herramientas de borrado seguro'*.**
10. La funcionalidad principal de Olvido es la de borrado seguro de ficheros y carpetas en sistemas Windows, no obstante, también permite el borrado de discos magnéticos y SSD, así como de memorias flash USB.
11. **El alcance de la aprobación permite la reclasificación y desclasificación de:**
    - **Discos magnéticos hasta RESERVADO o equivalente.**
    - **Discos SSD hasta DIFUSIÓN LIMITADA o equivalente.**

3. ORGANIZACIÓN DEL DOCUMENTO

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

    a) FASE DE DESPLIEGUE E INSTALACIÓN. En este apartado se recogen recomendaciones para tener en cuenta durante la fase de despliegue e instalación del producto.

    b) FASE DE CONFIGURACIÓN. En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

    c) FASE DE OPERACIÓN. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de operación del producto.

    d) *CHECKLIST*. En este apartado se incluye un *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.

    e) ABREVIATURAS. Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 OBTENCIÓN DE LICENCIAS

13. La obtención de licencias de OLVIDO WINDOWS se realiza mediante el envío de formulario de solicitud a la dirección de correo olvido@ccn.cni.es.
14. El solicitante recibirá un correo electrónico desde olvido@ccn.cni.es con la siguiente información:
    - Enlace de descarga del paquete de instalación.
    - Identificador de la organización, necesario en la fase de activación del software.
    - Credenciales de acceso a https://olvido.ccn.cni.es/ para la consulta y gestión de licencias.
15. Este paso de registro solamente es necesario una vez por organización. Con el identificador de organización y el link de descarga es posible activar tantas instalaciones y activaciones como licencias haya solicitado el solicitante.

4.2 ENTREGA SEGURA DEL PRODUCTO

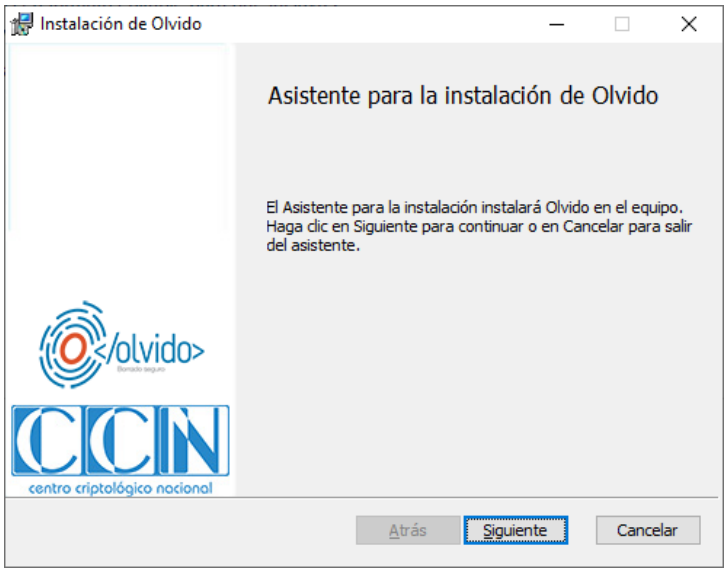
16. El instalador de la herramienta, que se podrá descargar a través de la dirección web proporcionada mediante correo electrónico, está firmado digitalmente basado en un certificado emitido a authUsb S.L. por parte de Sectigo.
17. En la dirección web *https://www.ccn.cni.es/index.php/es/soluciones-ccn/olvido* se encuentra publicado el *hash* (SHA256) del paquete de instalación que **el usuario deberá utilizar para la verificación de su integridad previa a su instalación.**

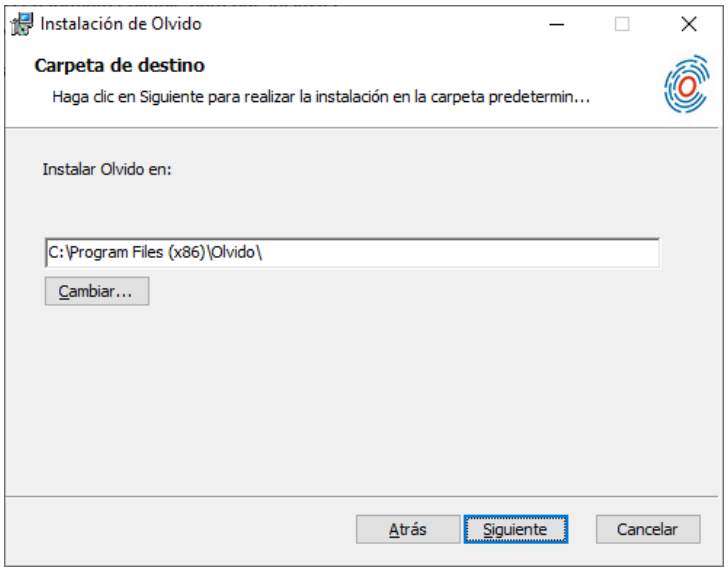
4.3 REQUISITOS PREVIOS

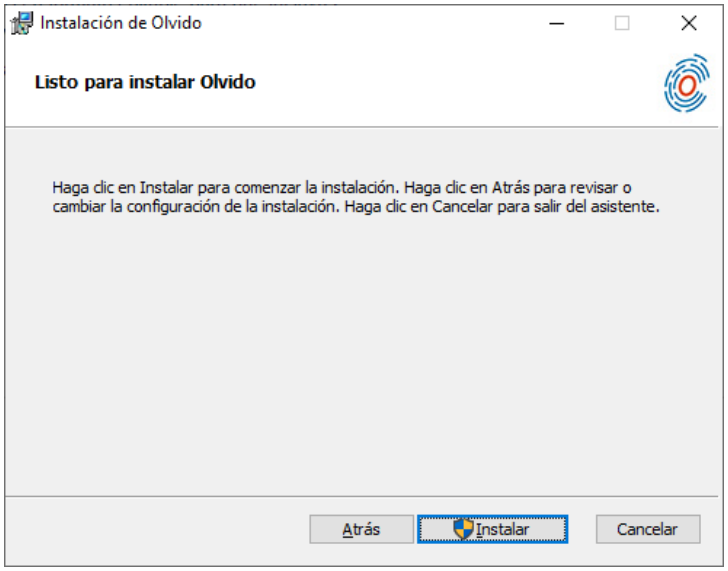
18. A continuación, se recogen los requisitos previos que es necesario tener en cuenta para la correcta instalación y ejecución de la herramienta:
    - El producto deberá ejecutarse en un ordenador con sistema operativo Windows (Windows 10 de 32 o 64 bits, Windows Server 2012 R2, Windows Server 2016 o Windows server 2021) con soporte activo por Microsoft.
    - El sistema operativo estará libre de malware y actualizado con las últimas actualizaciones de seguridad.
    - *Microsoft .Net Framework 4.7.2.*
19. Es necesario que el usuario que ejecute el paquete de instalación tenga permisos de administrador en el equipo local.

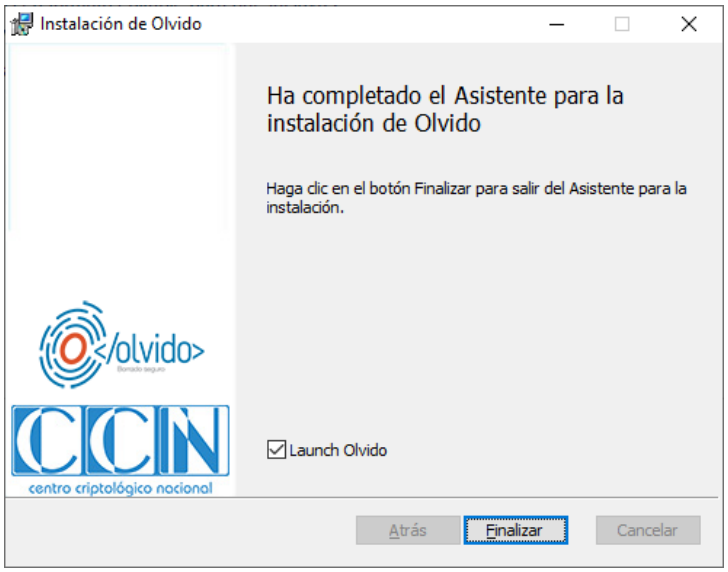
4.4 INSTALACIÓN

20. Para instalar el producto, se debe ejecutar el instalador (*Olvido.msi*) y seguir los pasos indicados por el asistente.




Instalación de Olvido
Carpeta de destino
Haga clic en Siguiente para realizar la instalación en la carpeta predetermin...
Instalar Olvido en:
C:\Program Files (x86)\Olvido\
Cambiar...
Atrás
Siguiente
Cancelar


Instalación de Olvido
Listo para instalar Olvido
Haga clic en Instalar para comenzar la instalación. Haga clic en Atrás para revisar o cambiar la configuración de la instalación. Haga clic en Cancelar para salir del asistente.
Atrás
Instalar
Cancelar

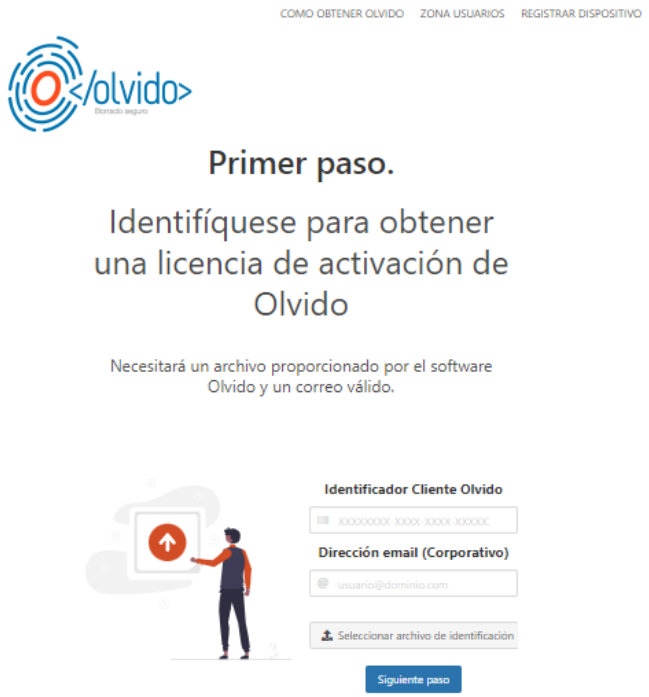

Instalación de Olvido
Ha completado el Asistente para la instalación de Olvido
Haga clic en el botón Finalizar para salir del Asistente para la instalación.
Launch Olvido
Atrás
Finalizar
Cancelar

4.5 ACTIVACIÓN DEL SOFTWARE

21. Tras finalizar la instalación e iniciar OLVIDO se mostrará la pantalla de activación:

22. El usuario dispone de dos (2) opciones de registro:

- **Registro offline**, para equipos sin acceso a internet. Mediante el botón "*Exportar*" se generará un fichero de activación (extensión .act). Se trasladará este archivo a un equipo con acceso a internet, desde el que se accederá a *https://olvido.ccn.cni.es/descargarLicencia*. En esta página se proporcionará el identificador de la organización (incluido en el email de alta recibido por el administrador), una dirección de email válida de la organización y el fichero de activación.

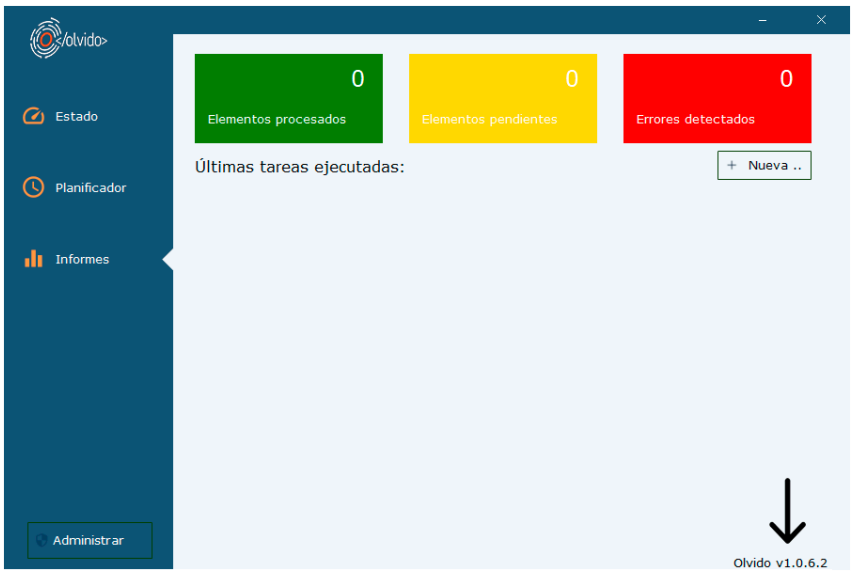


La página mostrará un botón de descarga donde se obtendrá el archivo de licencia (extensión .lic). Este archivo deberá ser copiado en el equipo en el que se quiere instalar OLVIDO y se pulsará la opción "*Activar*", donde seleccionará el archivo de licencia y el *software* quedará activado.

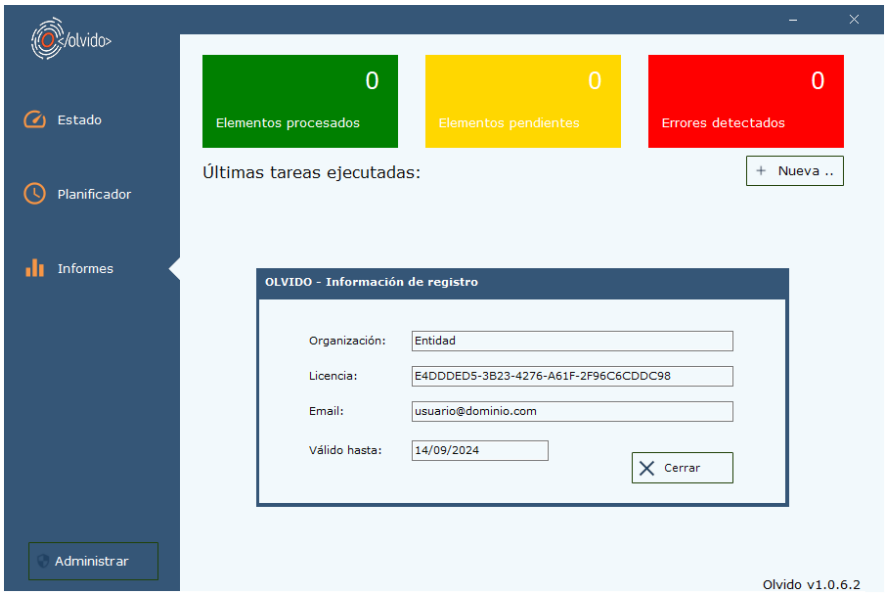
– **Registro online**, para equipos con acceso a internet. El usuario proporcionará el identificador de la organización (incluido en el email de alta recibido por el administrador) y una dirección de email válida de la organización. Tras pulsar "*Registrar*" el *software* realizará la activación automáticamente.

4.6 VERIFICACIÓN DE LA VERSIÓN DEL *SOFTWARE*

23. Tanto en la pantalla de activación como en la pantalla principal de OLVIDO, indicada en la esquina inferior derecha, se mostrará la versión del *software*. **El usuario deberá verificar que se corresponde con la 1.0.6 (la versión cualificada)**:



24. Pulsando con el ratón sobe el número de versión se mostrará la información de registro:



5. FASE DE CONFIGURACIÓN

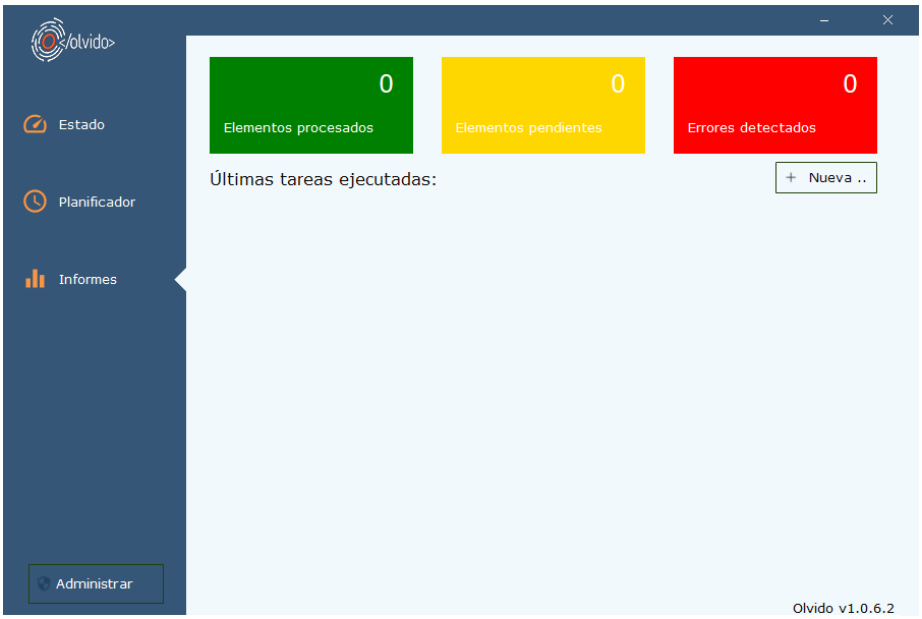
5.1 PERFILES DE USUARIO

25. La aplicación OLVIDO contempla dos (2) perfiles de usuarios:
    - Usuarios con perfil de administrador en el sistema operativo Windows, ejecutando OLVIDO con permisos elevados. En adelante, **usuarios administradores**.
    - Usuarios no administradores o administradores ejecutando OLVIDO sin permisos elevados. En adelante, **usuarios estándar**.

26. En función del perfil de usuario, la aplicación OLVIDO restringirá el acceso a secciones (sólo los usuarios administradores tendrán acceso a la configuración de la aplicación) y filtrará el acceso a los informes de estado y tareas programadas. El usuario administrador tendrá acceso a todos los informes y tareas creadas por cualquier usuario, mientras que el usuario estándar sólo tendrá acceso a las tareas ejecutadas o planificadas por él, así como a los informes generadas por éstas.

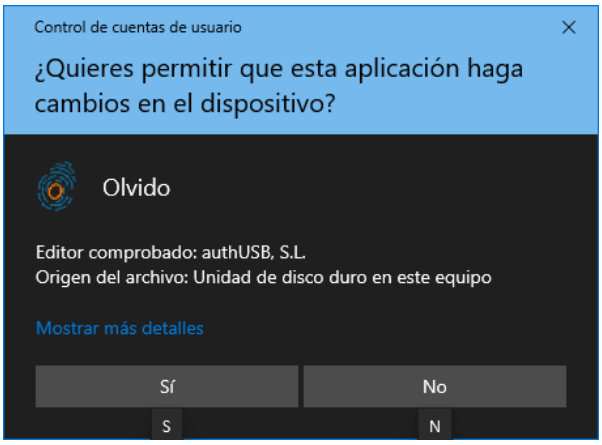
27. El borrado de volcados de memoria o discos no extraíbles son operaciones que solamente son accesibles para los usuarios administradores.

28. Tras la instalación de OLVIDO, el usuario podrá iniciar la aplicación desde el acceso directo creado en el menú inicio. Por defecto se iniciará sin permisos elevados:

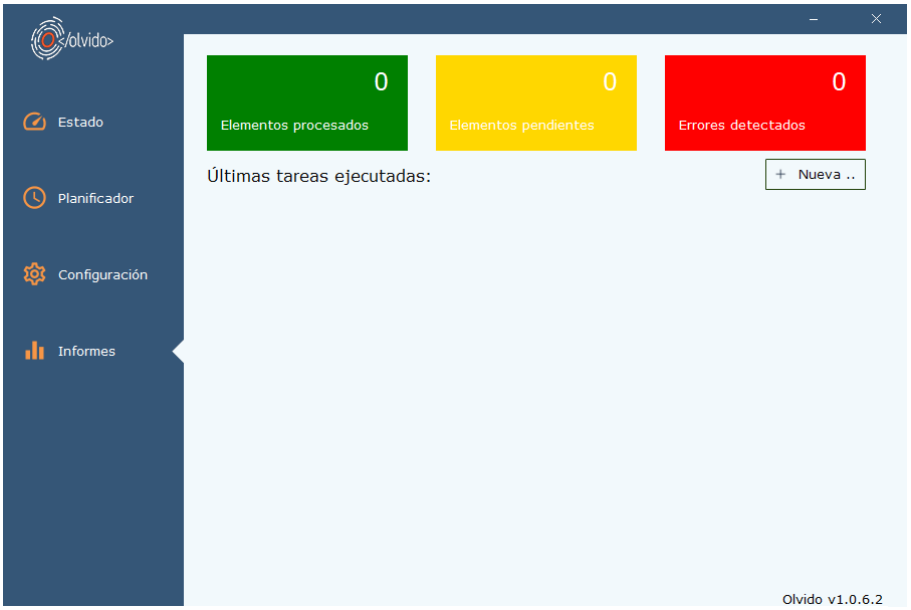


5.2 ADMINISTRACIÓN LOCAL DEL PRODUCTO

29. Si el usuario pertenece al grupo de administradores de Windows, podrá elevar sus privilegios pulsando el botón "*Administrar*" en el menú principal de la aplicación. Tras confirmar la acción el usuario adquirirá privilegios de usuario administrador de OLVIDO:



30. La aplicación se iniciará en modo administrador:



31. En este caso se mostrará la opción "*Configuración*" en el menú principal.

5.2.1 USO SEGURO

32. **La configuración por defecto de OLVIDO establece los valores necesarios para un uso seguro de la herramienta para sistemas bajo el alcance del ENS**. Estos valores son:

Campo	Valor
Algoritmo de borrado (Archivos)	CCN_ENS (1 pase)
Algoritmo de borrado (Carpetas)	CCN_ENS (1 pase)
Algoritmo de borrado (Espacio libre)	CCN_ENS (1 pase)
Algoritmo Hash	SHA256

Campo	Valor
Máximo tiempo de apagado	12 Horas
Protocolo Syslog	TCP/TLS 1.2 (Seguro)
Verificar certificado de servidor	Activo
Regenerar archivos de paginación al reiniciar	Activo

5.2.2 SISTEMAS CLASIFICADOS

33. Para niveles superiores a Difusión Limitada deberá modificarse la configuración por defecto de OLVIDO para establecer un algoritmo de borrado de 3 pases (0xFF, 0x00, aleatorio) con verificación en la última pasada, como el Algoritmo de borrado "CCN-CLASIFICADO" o el "***British HMG IS5***". A continuación, se muestra una tabla resumen con la configuración recomendada para sistemas clasificados:

Campo	Valor
Algoritmo de borrado (Archivos)	CCN-CLASIFICADO (3 pases)
Algoritmo de borrado (Carpetas)	CCN-CLASIFICADO (3 pases)
Algoritmo de borrado (Espacio libre)	CCN-CLASIFICADO (3 pases)
Algoritmo Hash	SHA256
Máximo tiempo de apagado	12 Horas
Protocolo Syslog	TCP/TLS 1.2 (Seguro)
Verificar certificado de servidor	Activo
Regenerar archivos de paginación al reiniciar	Activo

5.3 ALGORITMOS DE BORRADO

34. La operativa principal de OLVIDO se basa en la ejecución de operaciones de sobreescritura sobre los elementos objetivo (archivos, discos, etc.) previamente a su borrado del sistema de archivos. Estas operaciones están predefinidas en diferentes algoritmos. **OLVIDO proporciona 11 algoritmos estándar** ya

preconfigurados, y ofrece la posibilidad al Administrador de definir nuevos algoritmos personalizados, **aunque no se recomienda esta última opción salvo que sea requerida por alguna causa justificada**.

35. Los algoritmos predefinidos en OLVIDO son:

Algoritmo	Pases	Pase	Patrón
British HMG IS5	**3**	1	0x00
		2	0xFF
		3	Random (comprobación)
CCN-Clasificado	**3**	1	0xFF
		2	0x00
		3	Random (comprobación)
CCN-ENS	**1**	1	Random
GOST P50739-95	**2**	1	0x00
		2	Random
German VSITR	**7**	1	0x00
		2	0xFF
		3	0x00
		4	0xFF
		5	0x00
		6	0xFF
		7	Random
Gutmann	**35**	1	Random
		2	Random
		3	Random
		4	Random
		5	0x55
		6	0xAA
		7	0x92,0x49,0x24
		8	0x49,0x24,0x92
		9	0x24,0x92,0x49
		10	0x00
		11	0x11
		12	0x22
		13	0x33
		14	0x44

Algoritmo	Pases			
			15	0x55
			16	0x66
			17	0x77
			18	0x88
			19	0x99
			20	0xAA
			21	0xBB
			22	0xCC
			23	0xDD
			24	0xEE
			25	0xFF
			26	0x92,0x49,0x24
			27	0x49,0x24,0x92
			28	0x24,0x92,0x49
			29	0x6D,0xB6,0xDB
			30	0xB6,0xDB,0x6D
			31	0xDB,0x6D,0xB&
			32	Random
			33	Random
			34	Random
			35	Random
Pseudorandom	**1**		**Pase**	**Patrón**
			1	Random
RCMP TSSIT OPS-II	**7**		**Pase**	**Patrón**
			1	0x00
			2	0xFF
			3	0x00
			4	0xFF
			5	0x00
			6	0xFF
			7	Random & 0xFF (Comprobación)
Schneier	**7**		**Pase**	**Patrón**
			1	0xFF
			2	0x00
			3	Random
			4	Random
			5	Random
			6	Random
			7	Random
US Army AR380-19	**3**		**Pase**	**Patrón**
			1	Random

Algoritmo	Pases			
			2	0xFF
			3	0x00
US DoD 5220.22-M (E)	**3**		**Pase**	**Patrón**
			1	0xFF
			2	0x00
			3	Random
US DoD 5220.22-M (ECE)	**7**		**Pase**	**Patrón**
			1	Random & 0xFF (Comprobación)
			2	0x00 (Comprobación)
			3	Random
			4	Random & 0xFF
			5	Random & 0xFF
			6	0x00
			7	Random
USAF 5020	**3**		**Pase**	**Patrón**
			1	0x00
			2	0xFF
			3	Random
Zero	**1**		**Pase**	**Patrón**
			1	0x00 (Comprobación)

36. El método ***Gutmann*** (35 pasadas) fue desarrollado en 1996 para borrado de discos magnéticos que utilizasen cualquier tipo de codificación MFM/RLL. Los discos magnéticos actuales ya no utilizan dicha codificación y cuentan con una mayor densidad de datos, por lo que la utilización de este método es innecesaria. Es más**, se desaconseja su utilización salvo que se disponga de un disco antiguo cuyo tipo de codificación se desconozca**, dado que puede suponer una sobrecarga computacional innecesaria, disparar el tiempo de borrado y reducir la vida útil de un disco en el caso de que esta dependa de ciclos de lectura/escritura.

37. El usuario Administrador **podrá seleccionar el algoritmo de borrado por defecto** (**ver algoritmo de borrado recomendado en el apartado 5.2.1**) según el tipo de operación:

    - Borrado de archivos. Será de aplicación también en los borrados de archivos temporales, papelera de reciclaje y volcados de memoria Windows.
    - Borrado de discos.
    - Borrado del espacio libre de un volumen.

38. Algoritmo Hash: Los algoritmos de borrado está compuestos de 1 o más pases, cada uno de los cuales define una operación de sobreescritura concreta (constante, aleatoria, …). Cada uno de estos pases puede ser configurado para realizar una comprobación que verifique su correcta aplicación, utilizando un algoritmo Hash

para comparar los datos utilizados para la sobreescritura con los obtenidos en una lectura completa posterior. El usuario puede seleccionar, en orden ascendente en seguridad y también en tiempo de proceso, entre MD5, SHA1 y SHA256. **Se debe utilizar SHA256.**

39. Máximo tiempo de apagado: Los usuarios de OLVIDO pueden planificar tareas de borrado que se activarán al cierre del sistema. Con esta opción el usuario Administrador puede limitar el tiempo máximo que OLVIDO puede retrasar el reinicio o cierre del sistema mientras espera por la finalización de las tareas planificadas. La herramienta establece un valor máximo de 12 horas por defecto.

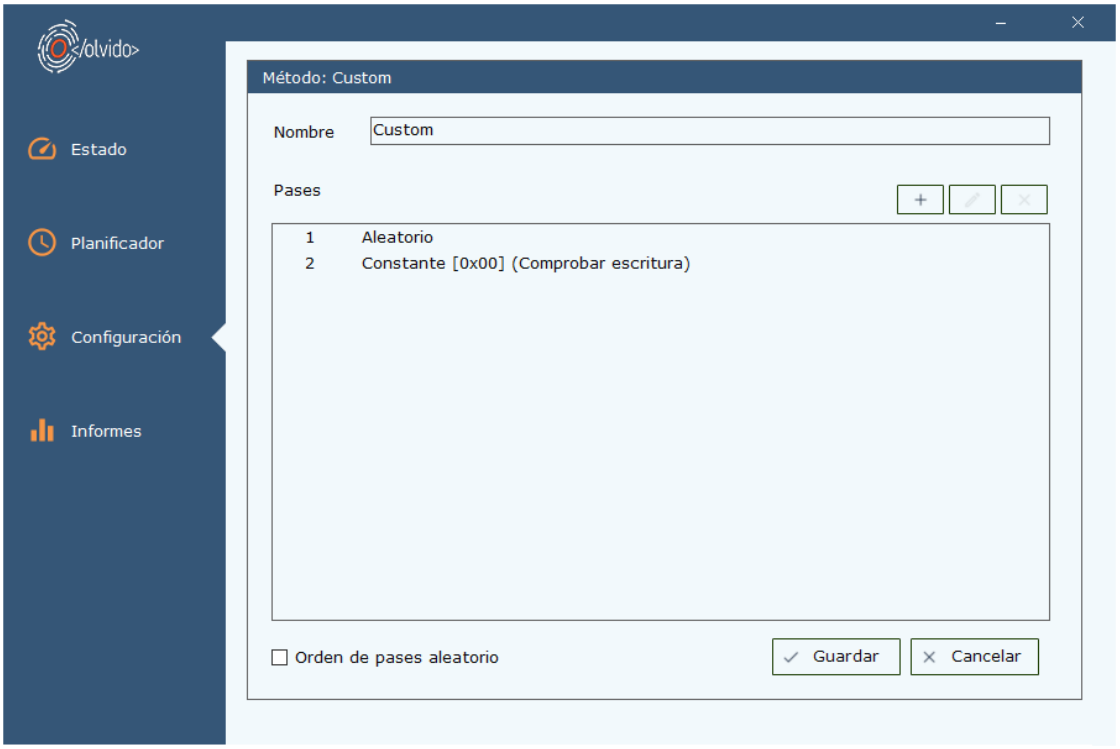
5.4 EDICIÓN DE ALGORITMOS DE BORRADO

40. Mediante el botón "*Editar*" el usuario Administrador accederá a la pantalla de edición de métodos de borrado. Se mostrarán los algoritmos existentes en el sistema, tanto los predefinidos como los creados por el usuario.

41. Los métodos predefinidos incluidos en OLVIDO no son modificables y no se permite su eliminación, aunque sí se permite la visualización de los distintos pases que componen cada uno pulsando el botón Editar de la barra de botones superior.

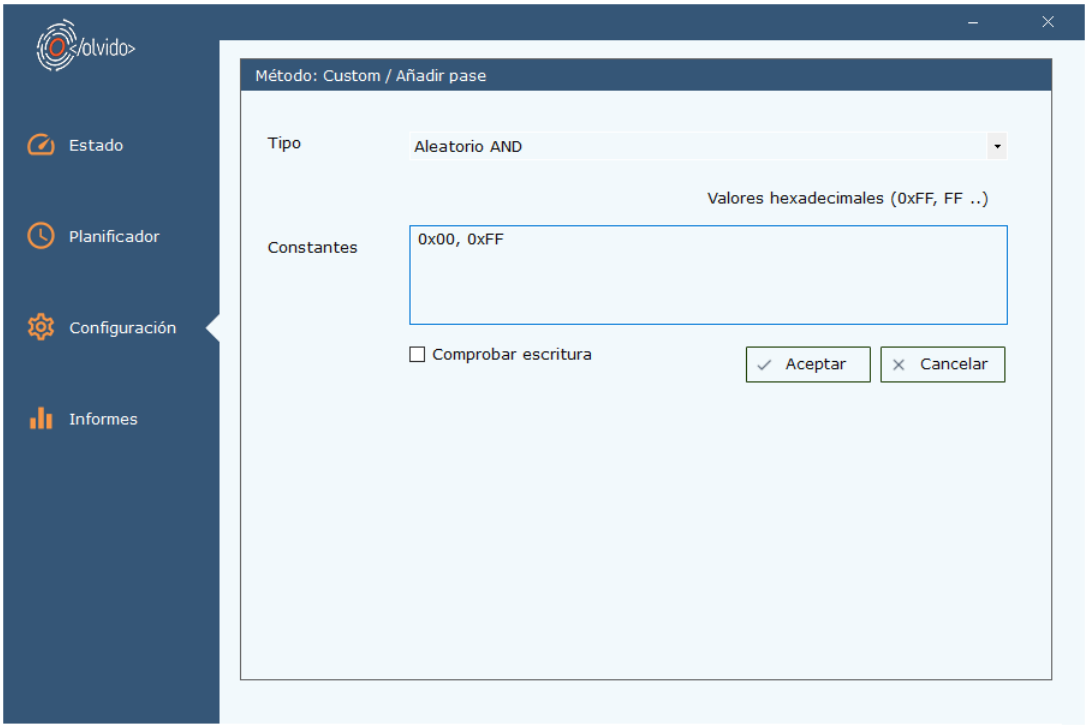
Nombre	Pases	Pases aleatorios	Sistema
British HMG IS5	3	No	Si
CCN-CLASIFICADO	3	No	Si
CCN-ENS	1	No	Si
GOST P50739-95	2	No	Si
German VSITR	7	No	Si
Gutmann	35	Si	Si
Pseudorandom	1	No	Si
RCMP TSSIT OPS-II	7	No	Si
Schneier	7	No	Si
US Army AR380-19	3	No	Si
US DoD 5220.22-M (E)	3	No	Si
US DoD 5220.22-M (ECE)	7	No	Si
USAF 5020	3	No	Si
Zero	1	No	Si

42. El usuario Administrador puede definir un nuevo método de borrado mediante el botón "+", lo que muestra la siguiente pantalla de edición:



43. Será necesario proporcionar un nombre al método, y añadir uno o más pases mediante el botón "+". También es posible definir si el orden de los pases es el definido o se reordenan aleatoriamente en cada ejecución.

44. Al añadir un nuevo pase, el usuario deberá seccionar la fuente de datos de sobreescritura y opcionalmente activar la opción de comprobación. Si esta opción está activa, tras la ejecución del pase OLVIDO comprobará que el objetivo ha sido sobrescrito correctamente. Implica un mayor tiempo de proceso ya que es necesario leer completamente el objetivo y utilizar un algoritmo *hash* para comparar los datos escritos con los leídos posteriormente.



45. Fuentes de datos:
    - Constante: El usuario debe proporcionar 1 o más bytes que serán los utilizados para sobrescribir el objetivo. Separados por comas, en formato decimal o hexadecimal.
    - Aleatorio: OLVIDO generará bytes aleatorios para el proceso de sobreescritura.
    - Aleatorio AND: OLVIDO generará bytes aleatorios y les aplicará un AND lógico con los valores constantes proporcionados por el usuario.

5.5 REGENERAR ARCHIVOS DE PAGINACIÓN

46. Esta opción configura el sistema operativo para que regenere el archivo de paginación en cada reinicio incrementando la seguridad del sistema. Debido a que esta tarea depende del tiempo que el sistema operativo tarde en cerrar los procesos en ejecución, no es posible asegurar el borrado seguro mediante sobreescritura de todo el archivo.

5.6 ACTUALIZACIONES

47. Las actualizaciones de producto se proporcionarán como paquete de instalación de Windows firmado digitalmente, válido tanto para la instalación inicial como para la actualización de instalaciones existentes de versiones anteriores.

5.7 AUDITORÍA

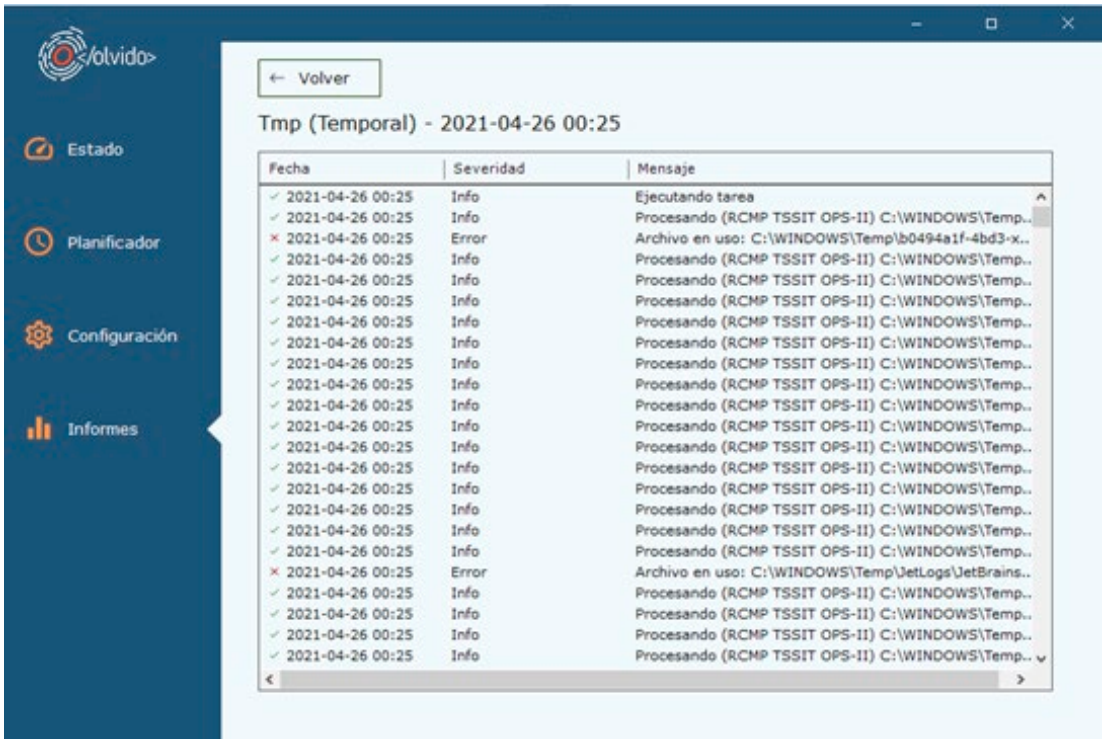
48. Todas las tareas de borrado ejecutadas por OLVIDO generarán un informe que contiene el detalle de las operaciones realizadas y los posibles errores o advertencias generadas. Estos informes serán enviadas en tiempo real por Syslog si el administrador así lo configura.

49. Cada tarea ejecutada generará una entrada resumen en esta pantalla, que muestra el usuario propietario de la tarea, fecha de inicio y fin, y el resultado de la ejecución, junto con el icono asociado a dicho resultado.

50. Las tareas mostradas están filtradas por usuario, de forma que los usuarios estándar sólo podrán visualizar los informes generados por las tareas generadas por ellos, mientras que el administrador tendrá acceso a todos los informes.

51. A través de la barra de botones el usuario administrador podrá vaciar el registro de informes, aunque se generará automáticamente una entrada que reflejará este hecho. El usuario administrador también tiene la opción de exportar los informes a un fichero CSV.

52. Si se hace doble *click* sobre cualquiera de las entradas, se mostrará el detalle de su ejecución



Tmp (Temporal) - 2021-04-26 00:25

Fecha	Severidad	Mensaje
✓ 2021-04-26 00:25	Info	Ejecutando tarea
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✕ 2021-04-26 00:25	Error	Archivo en uso: C:\WINDOWS\Temp\b0494a1f-4bd3-x..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✕ 2021-04-26 00:25	Error	Archivo en uso: C:\WINDOWS\Temp\JetLogs\JetBrains..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..
✓ 2021-04-26 00:25	Info	Procesando (RCMP TSSIT OPS-II) C:\WINDOWS\Temp..

5.7.1 REGISTRO DE EVENTOS

53. Cada tarea de borrado generará un registro en la pantalla de informes indicando el resumen de la tarea con los siguientes campos:

Campo	Descripción
Usuario	Nombre del usuario Windows que ha iniciado o planificado la tarea
Tarea	Nombre de la tarea. En el caso de las tareas almacenadas incluirá la descripción proporcionada en su creación. Para tareas de ejecución inmediata se especifica el tipo de destino de la tarea.
Inicio	Fecha de inicio de ejecución
Fin	Fecha de fin de ejecución en su caso
Resultado	Incompleta (tarea en ejecución), correcta o con errores

54. Si se hace doble *click* sobre el registro, se mostrará el detalle de las operaciones realizadas en la ejecución de la tarea, con los siguientes campos:

Campo	Descripción
Fecha	Fecha y hora del evento

Campo	Descripción
Severidad	Info, Alerta, Crítico o error
Inicio	Fecha de inicio de ejecución
Mensaje	Descripción del evento

5.8 CONFIGURACIÓN *SYSLOG*

55. OLVIDO genera informes de cada operación realizada que se almacena localmente para su posterior consulta. Activando el envío Syslog, estas trazas serán enviadas en tiempo real al destino Syslog configurado.

56. Los campos necesarios para la configuración son:

    - Servidor: Nombre de red o dirección IP del servidor Syslog destino
    - Puerto: Número de puerto UDP o TCP en el cual el servidor Syslog espera recibir las tramas.
    - Formato: Define el formato de codificación de cada trama Syslog que soporta el servidor.
    - Terminador: Define el método soportado por el servidor para identificar el fin de trama.
    - Protocolo: OLVIDO soporta el envío clásico (UDP sin cifrado) o TLS 1.2 (TCP cifrado).
    - Certificado cliente: Si el servidor espera una conexión TLS y necesita autenticar el origen de tramas con un certificado cliente, el usuario puede seleccionar entre los instalados en el almacén de equipo de Windows.
    - Verificar certificado del servidor: Activa la comprobación de la cadena de certificados utilizada por el servidor.

57. OLVIDO utiliza la configuración del sistema operativo a la hora de negociar con el destino TLS la suite de cifrado a utilizar en la conexión. Las suites disponibles pueden ser consultadas y/o deshabilitadas a través de comandos *Powershell* ejecutados por un administrador del equipo:

    - Comando *Get-TlsCipherSuite*:

      Obtiene la lista de suites habilitadas en el equipo. Los detalles de su uso pueden ser consultados en la dirección:

      https://docs.microsoft.com/en-us/powershell/module/tls/get-tlsciphersuite?view=windowsserver2019-ps

    - Comando *Disable-TlsCipherSuite:*

Permite deshabilitar suites específicas que no se deseen utilizar en la conexión. La documentación del comando está disponible en:

https://docs.microsoft.com/en-us/powershell/module/tls/disable-tlsciphersuite?view=windowsserver2019-ps

Nota importante: Estos comandos actúan a nivel sistema operativo, no solamente al software OLVIDO.

58. Tanto para sistemas bajo el alcance del ENS como para sistemas que manejan información clasificada se debe hacer uso únicamente de las *ciphersuites* marcadas como Recomendadas (R) en la guía *CCN-STIC-807 Criptología de empleo en el ENS*.

6. FASE DE OPERACIÓN

6.1 USO DE UNA POLÍTICA DE BORRADO SEGURO DE LA INFORMACIÓN

59. Las tareas de borrado que se realicen o planifiquen deberán estar de acuerdo con la política de borrado seguro establecida por la organización.

6.2 VERSIÓN *SOFTWARE*

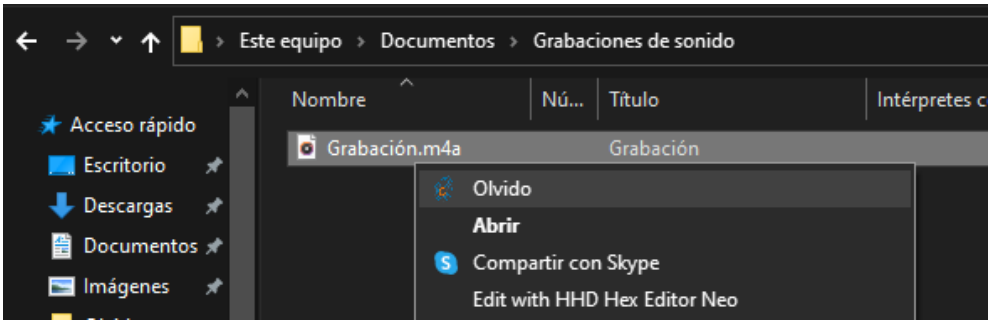
60. Desde la ventana principal de OLVIDO se puede consultar la versión software actual de la herramienta.

6.3 CREACIÓN DE TAREAS DE BORRADO

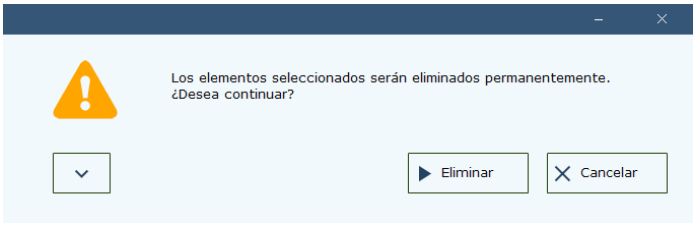
61. El usuario dispone de dos (2) métodos para crear tareas de borrado:
    - Tarea inmediata: Invocada desde el explorador de archivos, al abrir el menú contextual de ficheros o carpetas.
    - Editor de Tareas: Invocada desde la aplicación principal de OLVIDO, desde la pantalla de estado o planificación.

6.3.1 TAREA INMEDIATA

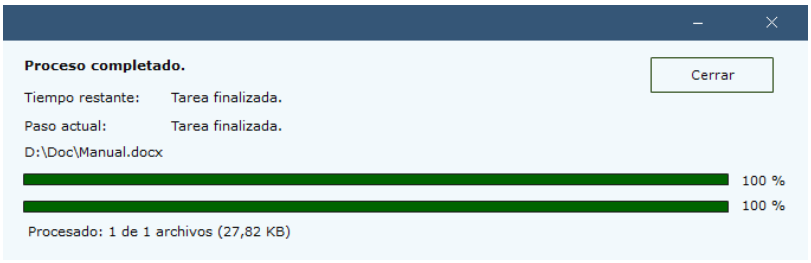
62. OLVIDO se integra en el menú contextual del explorador de archivos de Windows. Al hacer *click* con el botón derecho sobre carpetas o archivos aparecerá la opción "Olvido" que permitirá de forma rápida eliminar de forma segura los elementos seleccionados.



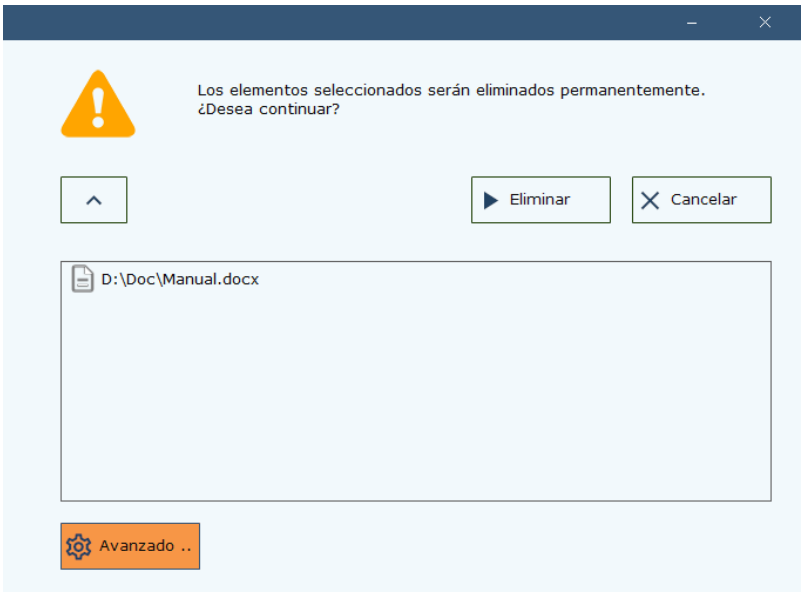
63. Al invocar a OLVIDO, se mostrará una ventana de confirmación:



64. Al pulsar "*Eliminar*", se llevará a cabo el borrado seguro de los elementos seleccionados, utilizando en este caso el algoritmo por defecto configurado por el administrador y mostrando el progreso de la tarea.



65. También es posible personalizar el borrado o planificarlo de forma periódica, desplegando el botón detalle y "*Avanzado*".



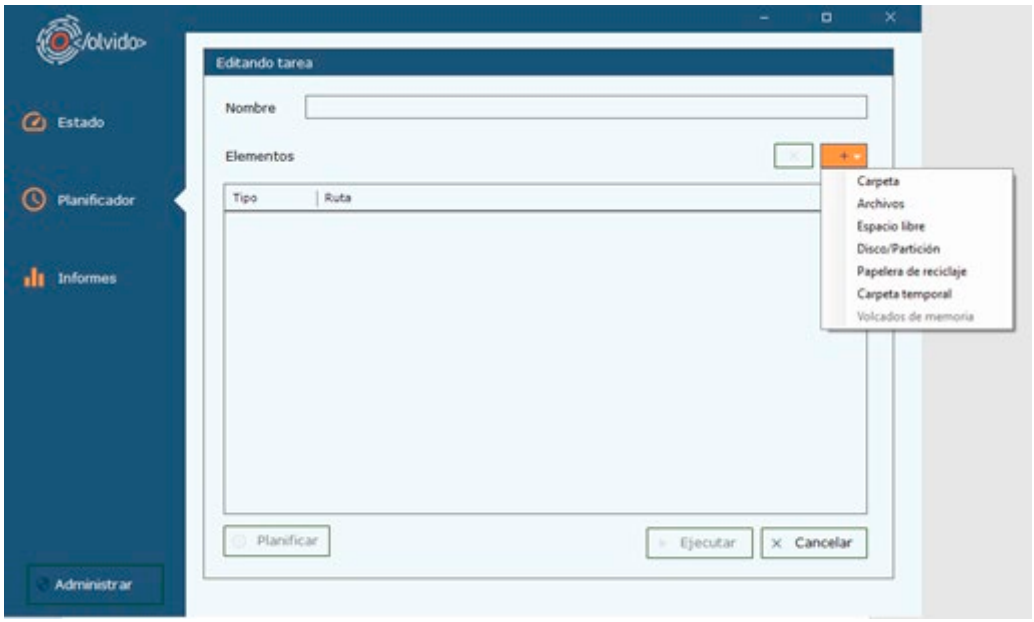
6.3.2 EDITOR DE TAREAS

66. Permite la creación de tareas de borrado en uno o más destinos y la selección de los métodos de borrado por defecto. También permite la planificación de la ejecución de forma puntual, en la fecha y hora seleccionada, o de forma periódica.

67. Además del acceso desde la pantalla de Tarea Inmediata, el usuario podrá acceder al editor de tareas de dos (2) maneras:

    - Desde la pantalla de estado, pulsando "*Nueva*"
    - Desde la sección Planificador, botón "+"

68. Se mostrará al usuario el editor, que permitirá añadir distintos elementos a eliminar desde el menú desplegable. También podrá asignar un nombre a la tarea para futura referencia e invocar su ejecución inmediata o planificarla.



69. A continuación, se describen los diferentes tipos de objetivos de borrado disponibles.

6.3.2.1 CARPETAS

70. Tras seleccionar la carpeta deseada, el usuario podrá seleccionar el algoritmo de borrado y decidir si desea eliminar la carpeta o los elementos que contenga, pudiendo incluir máscaras de inclusión o exclusión.

71. El campo '*Incluir*' es utilizado para indicar el nombre de los ficheros que se desean borrar, mientras que el campo '*Excluir*' se utiliza para indicar aquellos ficheros que se desean mantener. En caso de rellenar este campo, se borrarán todos los ficheros de la jerarquía de carpetas, salvo aquellos cuyo nombre coincida con el indicado en el campo.

72. Es posible utilizar expresiones regulares para seleccionar conjuntos de ficheros o carpetas cuyo nombre o extensión contenga un determinado patrón alfanumérico. Para ello, e se utiliza el carácter '*', que indica "cualquier valor". Es decir, los siguientes filtros actúan de la siguiente manera:

- **a**: Selecciona todos los ficheros que contengan a.
- *a**: Selecciona todos los ficheros que comiencen por a.
- **a*: Selecciona todos los ficheros que acaben en a.
- *a*: Solo selecciona los archivos que se llamen exactamente así.

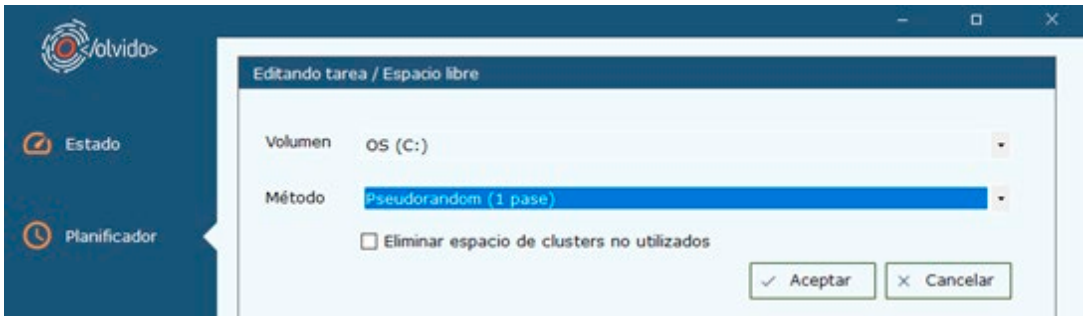
73. Las siguientes combinaciones, a modo de ejemplo, también podrían ser utilizadas: *a*.txt*, **.txt*, *a*a.txt*, etc.

6.3.2.2 ARCHIVOS

74. Tras seleccionar los archivos deseados, el usuario podrá seleccionar el algoritmo de borrado.

6.3.2.3 ESPACIO LIBRE

75. Tras seleccionar la unidad deseada, el usuario podrá seleccionar el algoritmo de borrado a utilizar y activar el borrado del espacio no utilizado de los clústers en uso.

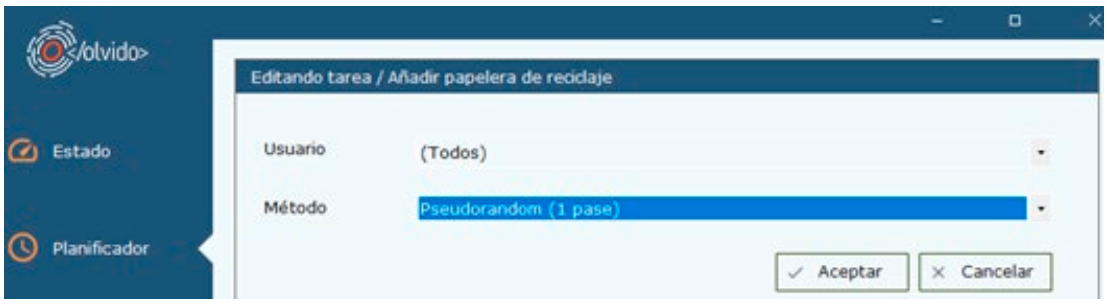


6.3.2.4 DISCO / PARTICIÓN

76. Esta opción, además de la sobreescritura definida por el método de borrado, implica la destrucción del sistema de archivos (si se selecciona una partición) o de la tabla de particiones (si se selecciona un disco).

6.3.2.5 PAPELERA DE RECICLAJE

77. El usuario estándar únicamente podrá seleccionar la papelera asociada a su usuario. El usuario administrador podrá además seleccionar las de todos los usuarios del sistema.



6.3.2.6 CARPETA TEMPORAL

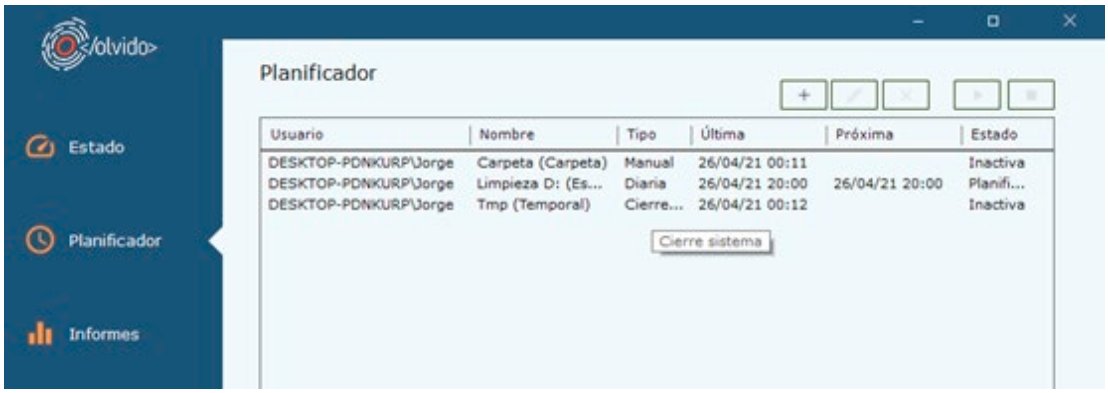
78. El usuario estándar únicamente podrá seleccionar la carpeta temporal asociada a su usuario. El usuario administrador podrá seleccionar, además, las de todos los usuarios del sistema.

6.3.2.7 VOLCADOS DE MEMORIA

79. El borrado del volcado de memoria de Windows es solo accesible por un usuario administrador.

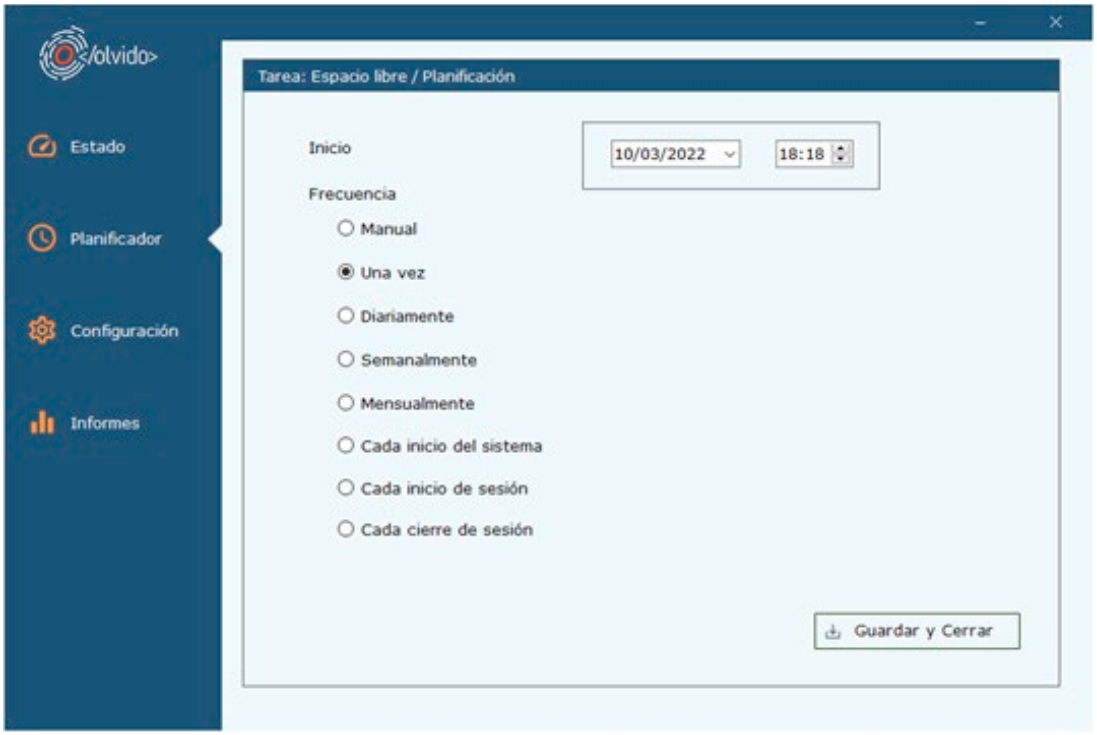
6.4 PLANIFICADOR

80. Una vez creada una tarea, esta puede ser almacenada para su activación futura, ya sea de forma automática o manual. En la ventana de planificación, el usuario podrá gestionar estas opciones:



81. Mediante la barra de botones, se puede:
    - Crear nuevas tareas
    - Editar la tarea seleccionada y su planificación
    - Eliminar la tarea seleccionada
    - Activar la ejecución de la tarea seleccionada
    - Detener la ejecución de una tarea si ésta se encuentra activa

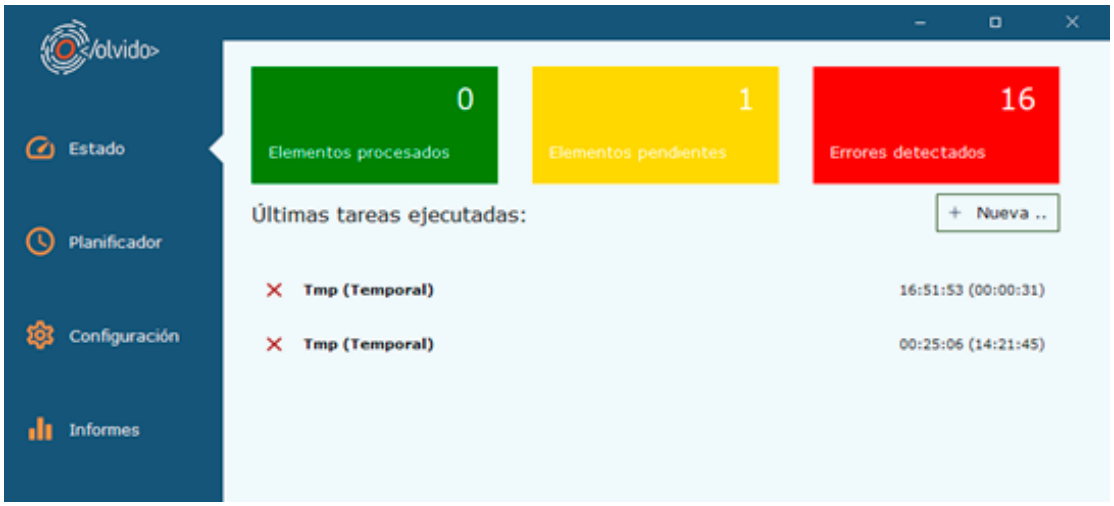
82. Al editar una tarea y pulsar el botón "*Planificar*" se mostrará la ventana de planificación:



83. En esta ventana, el usuario podrá seleccionar el momento de ejecución, puntual o periódico, o seleccionar "*Manual*" para simplemente almacenar la tarea para su futura activación manual por parte del usuario.

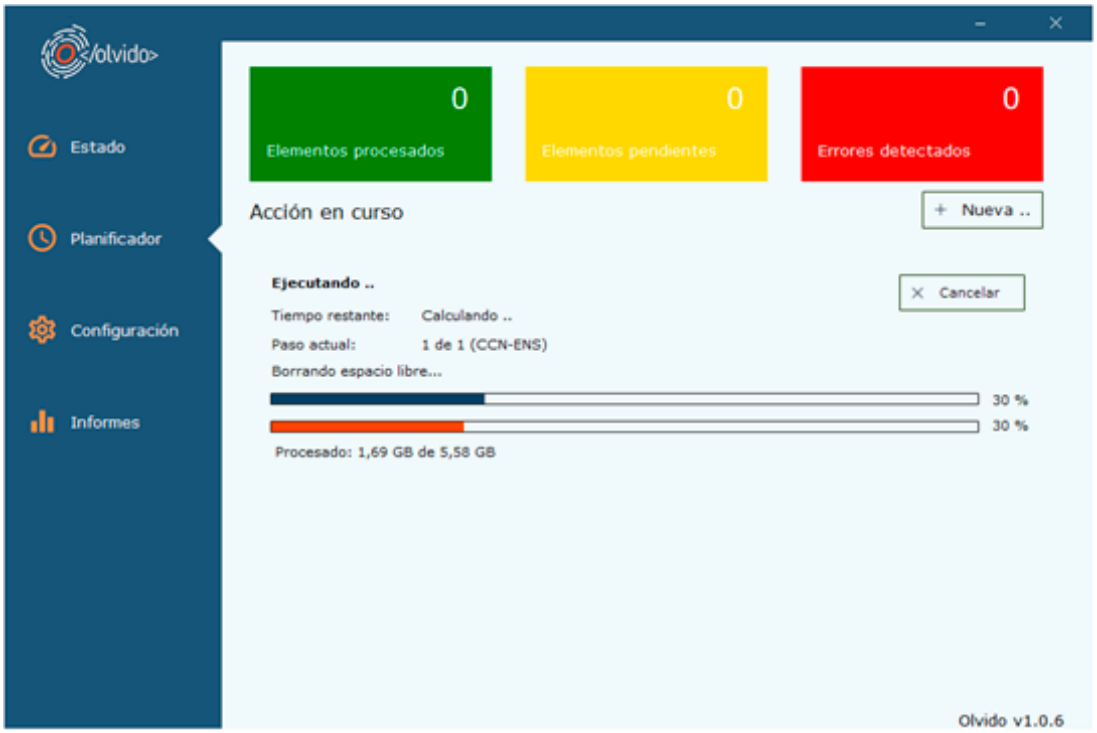
6.5 PANTALLA DE ESTADO

84. La pantalla de estado mostrará un resumen de las tareas ejecutadas en el día.



85. En los cuadros superiores se indica el número de tareas ejecutadas en el día (Elementos procesados), las tareas planificadas para su ejecución durante el día, y un contador global de los errores detectados en la ejecución de las mismas.

86. Adicionalmente, se muestra un resumen y acceso rápido al detalle de las tareas ejecutadas en el día. En caso de existir alguna tarea activa, su estado y progreso se mostrará en esta pantalla, permitiendo la posibilidad de cancelar su ejecución.



7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad del paquete	☐	☐	
Verificación versión cualificada OLVIDO	☐	☐	
CONFIGURACIÓN Y OPERACIÓN			
Verificación del método de borrado recomendado	☐	☐	
Utilización de TLS v1.2 para la protección de las comunicaciones	☐	☐	
Configuración SHA-256	☐	☐	
Planificación de tareas de borrado	☐	☐	
Configuración almacenamiento remoto	☐	☐	
Análisis de logs	☐	☐	
Desarrollo de una política de borrado seguro de la información	☐	☐	

8. ABREVIATURAS

CPSTIC	Catálogo de Productos y Servicios STIC
DMP	Archivos de Volcado de memoria de Windows
ENS	Esquema Nacional de Seguridad
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*

PUBLICACIONES DE DEFENSA

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