



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



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2024

NIPO: 083-24-026-8.

Fecha de Edición: enero de 2024

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN	3
2 OBJETO Y ALCANCE	4
3 ORGANIZACIÓN DEL DOCUMENTO	5
4 FASE DE DESPLIEGUE E INSTALACIÓN	6
4.1 ENTREGA SEGURA DEL PRODUCTO	6
4.2 REGISTRO Y LICENCIAS	6
4.3 CONSIDERACIONES PREVIAS	6
4.4 INSTALACIÓN.....	7
5 FASE DE CONFIGURACIÓN	8
5.1 AUTENTICACIÓN.....	8
5.2 ADMINISTRACIÓN DEL PRODUCTO	8
5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA	8
5.2.2 CONFIGURACIÓN DE ADMINISTRADORES	8
5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.....	8
5.4 GESTIÓN DE CERTIFICADOS.....	8
5.5 SINCRONIZACIÓN HORARIA	8
5.6 ACTUALIZACIONES	8
5.7 SNMP.....	9
5.8 ALTA DISPONIBILIDAD.....	9
5.9 AUDITORÍA	9
5.9.1 REGISTRO DE EVENTOS	9
5.9.2 ALMACENAMIENTO LOCAL	9
5.9.3 ALMACENAMIENTO REMOTO	10
5.10 BACKUP	10
6 REFERENCIAS	11
7 ABREVIATURAS.....	12

1 INTRODUCCIÓN

1. Las soluciones metaOLVIDO (EndPoint y Server) procesan automáticamente los metadatos de los ficheros cuando estos son creados o modificados en los directorios o unidades de disco monitorizadas.
2. metaOLVIDO es compatible con documentos Microsoft Office (.doc, .dot, .docx, .docm, .dotx, .dotm, .xls, .xlt, .xlsx, .xlsm, .xltx, .xltm, .xlsb, .ppt, .pot, .pptx, .pptm, .potx, .potm, .ppsx, .ppsm, .vsd), Open/Libre Office (.odt, .ods y .odp), PDF, RTF y ficheros de imagen, audio y vídeo (ver listado completo en la url: <https://www.adarsus.com/formatos-de-ficheros-compatibles-con-metaclean/>).
3. metaOLVIDO permite tanto borrar metadatos, como aplicar plantillas de metadatos personalizadas a documentos del tipo: Microsoft Office, Open/Libre Office y PDF, para los ficheros de imagen, audio y vídeo solo está permitido el borrado de metadatos.
4. metaOLVIDO se puede integrar con metaOLVIDO Dashboard para Administrar, centralizar y controlar la aplicación de políticas preventivas de seguridad de metadatos a nivel corporativo.

2 OBJETO Y ALCANCE

5. El presente documento tiene como objetivo detallar las configuraciones de seguridad del producto metaOLVIDO, de forma que la protección y funcionamiento del producto se realice de acuerdo con unas garantías mínimas de seguridad.
6. Los componentes de metaOLVIDO se distribuyen mediante paquetes .MSI o .EXE. En el caso de los paquetes .MSI, estos pueden ir preconfigurados según las especificaciones del cliente y aptos para instalaciones masivas y desatendidas mediante políticas GPO de Active Directory.
7. Estos componentes de metaOLVIDO se ejecutan sobre sistemas Operativos Windows Server 2008 o superior (metaOLVIDO Server) o Windows 10 o superior (metaOLVIDO EndPoint). Se recomiendan los siguientes recursos para cada uno de los entornos:

	Requisitos básicos		
	vCPU	RAM	HD
metaOLVIDO EndPoint	1	4	130 MB
metaOLVIDO Server	4	8	130 MB

8. Los productos mencionados en esta guía han sido cualificados e incluidos en el **Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC)** en la familia de **“Gestión de metadatos”**. Se recomienda consultar el Catálogo para conocer la versión cualificada en cada momento.

3 ORGANIZACIÓN DEL DOCUMENTO

9. El presente documento se estructura en las secciones indicadas a continuación:
 - a) Apartado 4. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
 - b) Apartado 5. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
 - c) Apartado 6. Referencias.
 - d) Apartado 7. Abreviaturas.

4 FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Existe la posibilidad de crear paquetes de instalación .MSI preconfigurados de acuerdo con las necesidades del cliente. Esta opción es recomendable en el caso de que el cliente requiera customizaciones muy específicas o cuando la herramienta metaOLVIDO (EndPoint y/o Server) se vaya a integrar con metaOLVIDO Dashboard y siempre y cuando el número de instalaciones sea superior a 10 PC's o Servidores.
11. En caso de requerirse un paquete de instalación .MSI customizado, se solicitará a la organización la información específica de configuración de forma que no haya que hacer ningún ajuste posterior a la instalación.
12. Los paquetes de instalación de metaOLVIDO se ponen a disposición del cliente a través de la solución LORETO del Centro Criptológico Nacional.
13. Una vez publicados, se comunica al cliente vía email la siguiente información relacionada con la descarga de los paquetes de instalación:
 - URL de acceso a la aplicación LORETO.
 - Contraseña de acceso.

Desde la propia aplicación LORETO se mostrarán los enlaces para la descarga de los paquetes de instalación metaOLVIDO EndPoint y/o Server.

14. El manual de instalación y operación de metaOLVIDO está disponible en la web pública de la herramienta del Centro Criptológico Nacional
15. Antes de realizar el despliegue la solución metaOLVIDO **se debe validar que el hash del paquete descargado es correcto**. En la citada página web de la solución, también se publican los valores *hash* de los paquetes de instalación.

4.2 REGISTRO Y LICENCIAS

16. Los paquetes de instalación se encuentran preconfigurados de forma que, al iniciarse la aplicación por primera vez, esta se conecta al servidor de licencias del fabricante (vía HTTPS sobre TLSv1.2) y la licencia se registra y activa automáticamente.

4.3 CONSIDERACIONES PREVIAS

17. Si el número de instalaciones es superior a 10 equipos, se recomienda facilitar al fabricante (Adarsus Technologies) la información de configuración relativa a monitorización de cada uno de los directorios. De esta forma, dicha información se parametrizará en el paquete de instalación .MSI evitando así tener que hacer configuraciones posteriores al despliegue de la solución.

4.4 INSTALACIÓN

18. La organización se encargará del despliegue de la solución a partir de los paquetes de instalación descargados de la aplicación LORETO.
19. La instalación puede realizarse manualmente, equipo por equipo, o bien de manera desatendida utilizando alguna de las herramientas existentes en el mercado para la distribución masiva de software.
20. En caso de realizarse una instalación manual la interfaz gráfica del paquete de instalación no muestra opciones de configuración, solo hay que hacer clic en el botón siguiente > siguiente > ...
21. Si el proceso de instalación no finaliza correctamente, se debe verificar si el antivirus ha borrado el fichero: "MetaClean Sync Service.exe" del directorio de instalación del producto: "C:\Program Files (x86)\Adarsus\MetaClean Sync Server", en cuyo caso habrá que añadir una excepción para que el antivirus *confie* en todos los ficheros *.exe del directorio de instalación.

5 FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

22. El acceso a la interfaz gráfica de metaOLVIDO se realiza mediante un usuario con credenciales de Administrador de la máquina para evitar que usuarios no autorizados realicen cambios en las políticas de metadatos de la organización.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

23. La administración de metaOLVIDO EndPoint y Server se realiza mediante una Interfaz Gráfica de Usuario local.
24. Tan solo se puede acceder al producto remotamente mediante Terminal Server (si está habilitado). No existe otro tipo de acceso no seguro como HTTP, Telnet, etc.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

25. Los únicos usuarios con acceso a la interfaz gráfica de metaOLVIDO son aquellos con credenciales de Administrador, las políticas de contraseñas serán las marcadas por la organización.

5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

26. metaOLVIDO no expone servicios o puertos al exterior.

5.4 GESTIÓN DE CERTIFICADOS

27. Toda la información referida a la gestión de certificados, algoritmos de cifrado y configuración se encuentra detallada en el manual de instalación y operación de metaOLVIDO, sección "URL de Conexión al Servidor Dashboard" páginas 8 a 12.

5.5 SINCRONIZACIÓN HORARIA

28. Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y logging.

5.6 ACTUALIZACIONES

29. El proceso de actualización se encuentra detallado en el manual de instalación y operación de metaOLVIDO, sección "Política de Actualizaciones y Registro de Actividad" página 7.
30. Para comprobar la versión del producto iniciaremos la interfaz gráfica de metaOLVIDO donde se mostrará la nueva versión.

5.7 SNMP

31. No se habilita el servicio SNMP en los componentes de metaOLVIDO.

5.8 ALTA DISPONIBILIDAD

32. Se delega en el motor de virtualización del cliente la capacidad de alta disponibilidad ante errores de apagado o sufrimiento de alguna otra avería.

5.9 AUDITORÍA

5.9.1 REGISTRO DE EVENTOS

33. El registro de eventos se encuentra detallado en el manual de instalación y operación de metaOLVIDO, sección “Política de Actualizaciones y Registro de Actividad” página 8.
34. Todos los accesos y acciones realizadas desde la interfaz gráfica de metaOLVIDO quedarán registradas en el siguiente fichero de Log: "C:\Program Files (x86)\Adarsus\MetaClean Sync Server\log\MetaClean_Sync_Console.log".
35. metaOLVIDO genera registros de auditoría para todos los eventos relevantes relacionados con la seguridad. Estos incluyen el tipo de evento, la fecha y la hora del evento, el sujeto que genera el registro de autoría y si el resultado del evento es algún fallo se añadirá el siguiente texto al final de la cadena: ":::: Result :::: Fail". El formato de los registros de logs es el siguiente:

```
INFO 2023/12/30 12:56:51 :::: [user:DESKTOP-JIIHCEV\JuanLopez] Stops the directory monitor: C:\Users\Downloads
```

36. Todas las acciones realizadas por el Servicio Windows: “MetaClean Sync Service” quedarán registradas en el fichero: "C:\Program Files (x86)\Adarsus\MetaClean Sync Server\log\MetaClean_Sync_Service.log". El formato de los registros de logs es el siguiente:

```
INFO 2024/01/03 14:12:22 :::: Procesado correctamente :::: C:\Users\Downloads\Adarsus-ENS.docx
```

5.9.2 ALMACENAMIENTO LOCAL

37. Todos los registros de logs se almacenan en el directorio: "C:\Program Files (x86)\Adarsus\MetaClean Sync Server\log". Estos logs rotan periódicamente para garantizar que la máquina no se quede sin espacio.
38. Por defecto, los logs de auditoría tienen un tamaño de 1 Mb y se mantienen un total de 5 logs (5Mb de log en total). Esta configuración solo puede ser modificada por un usuario Administrador de la máquina.
39. Para editar o borrar cualquiera de los ficheros almacenados dentro del directorio: "C:\Program Files (x86)\Adarsus\MetaClean Sync Server" y subdirectorios se requieren credenciales de administrador.

5.9.3 ALMACENAMIENTO REMOTO

40. metaOLVIDO permite guardar en un fichero de log el registro de los metadatos originales de los ficheros procesados. La configuración de este proceso se detalla en la sección "Registro de Metadatos Procesados" del manual de instalación y operación de metaOLVIDO, página 8.
41. Cuando metaOLVIDO EndPoint o Server se integra con metaOLVIDO Dashboard, el registro de log de metadatos procesados se envía al Dashboard mediante protocolo HTTPS con TLSv1.2.
42. metaOLVIDO Dashboard debe verificar que el cliente (metaOLVIDO EndPoint o Server) que envía el fichero de log de metadatos procesados es legítimo, para ello se utiliza una **API-KEY que es única por cada organización**. El proceso para cambiar la configuración de esta API-KEY se describe en el manual de instalación y operación de metaOLVIDO, sección "Configuración de la API-KEY", páginas 12 y 13.

5.10 BACKUP

43. Se recomienda realizar una copia del fichero de configuración de metaOLVIDO de forma periódica y almacenarlo en una ubicación segura.
"C:\Program Files (x86)\Adarsus\MetaClean Sync Server\sync.properties"

6 REFERENCIAS

- REF1 Manual de instalación y operación de metaOLVIDO.
<https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/504-metaolvido-EndPoint-y-server/file>

7 ABREVIATURAS

CCN	Centro Criptológico Nacional.
CPD	Centro de Procesamiento de Datos.
GUI	Interfaz Gráfica de Usuario.
HTTPS	Hypertext Transfer Protocol Secure.
SSH	Secure Shell.
TLS	Transport Layer Security.
URL	Uniform Resource Locator.

