

ESET File Security

Manual de instalación y guía del usuario

Versión 3.0 - Abril de 2009



Protegemos su mundo digital



www.eset.es

ESET File Security

Copyright © 2009 por ESET, spol. s r.o.

ESET File Security ha sido desarrollado por ESET, spol. s r.o.
Para más información, visite www.eset.es.

Todos los derechos reservados.

Este documento no puede ser reproducido, guardado en un sistema automatizado de obtención de documentos, ni transmitido, total o parcialmente, bajo ningún formato ni medio electrónico o mecánico, para ningún propósito sin el consentimiento escrito del autor.

La información de este documento está sujeta a cambios sin previa advertencia.

Esta guía se actualiza frecuentemente para reflejar modificaciones en el producto.

Este producto ha sido desarrollado con PHP. Esta aplicación gratuita está disponible en <http://php.net/software/>.

Última revisión en inglés: febrero de 2009.

Traducción y adaptación al español: Ontinet.com, S.L., abril de 2009.

Contenidos

1. Introducción	4
1.1 Requisitos del sistema	5
2. Instalación de <i>ESET File Security</i>	6
3. Arquitectura de <i>ESET File Security</i>	8
4. Integración con los servicios del sistema	11
4.1 Análisis a petición del usuario	11
4.2 Análisis en el acceso basado sobre Dazuko	12
4.2.1 Principios de funcionamiento	13
4.2.2 Instalación y configuración	14
4.2.3 Recomendaciones	15
4.3 Análisis en el acceso utilizando la librería LIBC	16
4.3.1 Principios de funcionamiento	17
4.3.2 Instalación y configuración	18
4.3.3 Recomendaciones	19
5. Mecanismos principales de <i>ESET File Security</i>	20
5.1 Directivas de manejo de objetos	20
5.2 Configuración específica del usuario	21
5.3 Sistema de envío de muestras	22
5.4 Interfaz web	23
5.5 Administración remota	24
6. Sistema de actualización de <i>ESET File Security</i>	25
6.1 Herramienta de actualización de <i>ESET File Security</i>	25
6.2 Descripción del proceso de actualización	26
6.3 Proceso demonio del servidor local de actualizaciones HTTP	27
7. Glosario	28
8. Contacto	30
9. Apéndice A: Licencia PHP	31

1. Introducción

Apreciado usuario, gracias por adquirir **ESET File Security**, la mejor solución de seguridad para los sistemas operativos Linux, BSD y Solaris.

Pronto comprobará que la tecnología avanzada del motor de análisis **ESET**, proporciona una velocidad de exploración y tasas de detección insuperables, con un consumo de recursos mínimo. Esto convierte a **ESET File Security** en la elección ideal para los servidores en entornos de trabajo Linux, BSD o Solaris.

Características principales de **ESET File Security**:

- Elevada tasa de detección y máxima velocidad de análisis, gracias a los algoritmos del motor antivirus **ESET**.
- Diseño especialmente desarrollado para ejecutarse en ordenadores con uno o varios procesadores.
- Heurística avanzada única para detectar gusanos y puertas traseras de sistemas Windows de 32 bits.
- Sistema de descompresión de archivos integrado, que permite examinar objetos empaquetados sin la necesidad de recurrir a una aplicación externa.
- Arquitectura basada sobre un proceso demonio que permanece siempre activo (programa residente), y que recibe todas las solicitudes de análisis.
- Ejecución de procesos demonio limitada exclusivamente a cuentas de usuario con privilegios (excepto **esets_dac**), con el fin de mejorar aún más la seguridad.
- Personalización de configuraciones para cada usuario, equipo cliente o servidor.
- Opción para configurar varios niveles de registro, para obtener información detallada sobre la actividad del sistema y las infiltraciones.
- Interfaz web, intuitiva y simple, que permite configurar y administrar fácilmente el programa y sus licencias.
- Compatibilidad con **ESET Remote Administrator**. Esto permite administrar fácilmente su implementación en redes extensas.
- No es necesario recurrir a librerías o programas externos, excepto **libc**.
- Sistema de configuración de alertas, para enviar avisos a ciertos usuarios específicos, comunicando la detección de una infiltración u otro suceso importante.

1.1. Requisitos de sistema

- **Procesador**
 - Arquitectura i386 (Intel® 80386) o AMD64 (x86-64).
- **Sistemas operativos**
 - **Linux**
Con Kernel 2.2.x, 2.4.x o 2.6.x, glibc 2.2.5 o superior.
Módulo Dazuko kernel 2.0.0 o superior (opcional).
 - **FreeBSD**
Versión 5.x, 6.x o 7.x.
Módulo Dazuko kernel 2.0.0 o superior (opcional).
 - **NetBSD**
Versión 4.x.
 - **Sun Solaris**
Versión 10 o superior.
- **Memoria operativa**
 - 32 MB
- **Espacio en disco duro**
 - 32 MB para la instalación.
Espacio adicional para los archivos temporales

ESET File Security tiene el desempeño y la versatilidad que usted espera de una solución basada sobre UNIX.

Cuenta también con la seguridad incomparable de los productos **ESET**, tanto para servidores de oficina pequeños, como para grandes servidores corporativos con miles de usuarios, como los que utilizan los proveedores de Internet (ISP, *Internet Service Provider*).

2. Instalación de ESET File Security

Al adquirir la licencia de uso de **ESET File Security**, el usuario recibirá un mensaje de correo electrónico que contiene sus datos de autenticación —nombre de usuario y contraseña— y un archivo adjunto con la clave de licencia.

Esta información le permitirá identificarse como cliente, y también acceder a los servidores de **ESET** para descargar el paquete inicial del programa y sus actualizaciones.

ESET File Security se distribuye como archivo binario:

esets.i386.ext.bin

Donde **ext** es un sufijo que dependerá de la distribución del sistema operativo: **deb** corresponderá a la distribución Debian; **rpm** a las distribuciones Red Hat y SuSE; **tgz** a otras distribuciones de Linux; **fbs5.tgz** corresponderá a FreeBSD 5.xx; **fbs6.tgz** a FreeBSD 6.xx; **nbs4.tgz** a NetBSD 4.xx y **sol10.pkg.gz** corresponderá a Solaris 10.


El formato del nombre del archivo binario para Linux **RSR** es:

esets-rsr.i386.rpm.bin

Para instalar o actualizar el producto, siga las instrucciones detalladas a continuación:

1. En la interfaz de comandos, introduzca la instrucción:

```
sh ./esets.i386.ext.bin
```

 En la versión de **ESET File Security** para Linux **RSR**, el comando a utilizar es el siguiente:

```
sh ./esets-rsr.i386.rpm.bin
```

2. Después de ejecutar el comando correspondiente a la versión de Linux instalada, aparecerá en pantalla el **Contrato de licencia** solicitando la conformidad del usuario para continuar el proceso.
3. Una vez leído y aceptado el **Contrato de licencia**, se visualizará información relevante sobre el proceso de instalación, desinstalación o actualización, y el paquete de instalación se ubicará en el directorio en el que se esté trabajando en ese momento.
4. Cuando finaliza la instalación del producto, podrá verificar que el servicio principal de **ESET File Security** está activo, mediante el comando correspondiente al sistema operativo del equipo:
 - o En sistemas operativos Linux:
ps -C esets_daemon
 - o En sistemas operativos BSD:
ps -ax | grep esets_daemon
 - o En sistemas operativos Solaris:
ps -A | grep esets_daemon

Al presionar la tecla **Intro** (*Enter*), se visualizarán los procesos **esets** activos. Si el servicio se está ejecutando correctamente, el mensaje debería mostrar al menos dos procesos demonio (*daemon*), con el siguiente formato:

```
PID TTY TIME CMD
```

```
2226 ? 00:00:00 esets_daemon
```

```
2229 ? 00:00:00 esets_daemon
```

El primero de ellos representa al gestor de procesos e hilos de ejecución del sistema.
El segundo representa el proceso de análisis de **esets**.

3. Arquitectura de ESET File Security

Una vez instalado **ESET File Security**, es conveniente conocer su estructura para comprender mejor su funcionamiento.

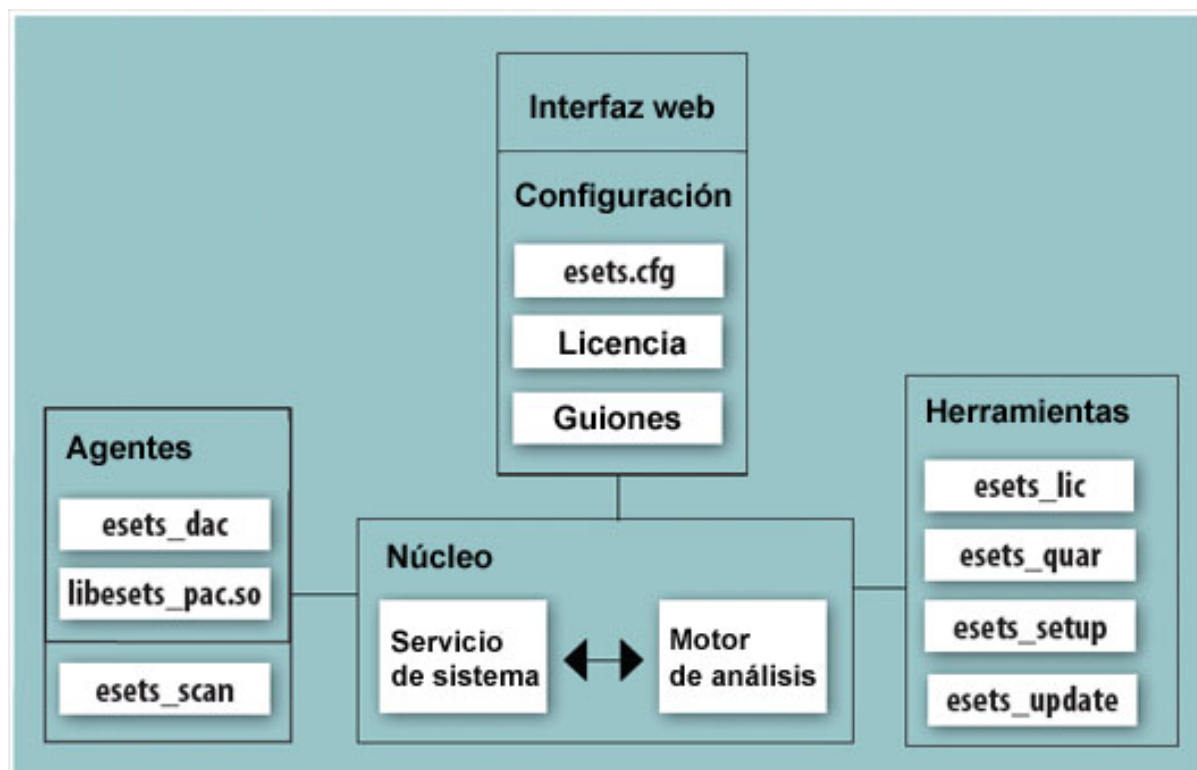


Figura 3.1 - Estructura de *ESET File Security*

El sistema está formado por los siguientes componentes:

- **Núcleo**

El corazón de **ESET File Security** reside en el proceso demonio **esets_daemon**.

Este, utiliza la librería **libesets.so** y los módulos **em00X_xx.dat** para efectuar tareas básicas del sistema, tales como análisis, mantenimiento del agente de procesos demonio y del sistema de envío de muestras, registros, avisos, etcétera.

Para obtener mayor información, consulte la página de manual **esets_daemon(8)**.

- **Agentes**

El propósito de los módulos agente, es integrar **ESET File Security** a los entornos Linux, BSD y Solaris.

- **Herramientas**

Los módulos de herramientas, permiten una administración simple y efectiva del sistema.

Son los responsables de realizar las tareas principales, tales como la administración de licencias, la gestión de la carpeta de cuarentena, y la configuración y actualización del sistema.

- **Configuración**

Para obtener un funcionamiento óptimo del sistema, es fundamental determinar la configuración apropiada.

El resto de este capítulo, está dedicado a explicar todos los componentes relacionados con este punto.

Asimismo, se recomienda estudiar los parámetros del archivo **esets.cfg**, el cual contiene información esencial para la configuración correcta de **ESET File Security**.

Una vez que el producto se ha instalado exitosamente, todos sus componentes de configuración se guardarán en el directorio **@ETCDIR@**, que contiene los siguientes archivos:

- **@ETCDIR@/esets.cfg**

El archivo de configuración **esets.cfg** es el más importante, ya que controla los aspectos principales del funcionamiento del producto. Está constituido por varias secciones y cada una de ellas presenta diversos parámetros configurables.

Hay una sección global y varias secciones **agente**, cuyos nombres aparecen entre corchetes. Los parámetros de la sección global se utilizan para definir las opciones de configuración del proceso demonio, así como también los valores predeterminados para la configuración del motor de análisis de **ESET File Security**.

En las secciones **agente**, los parámetros definen la configuración de los módulos dedicados a interceptar y preparar los flujos de datos para el análisis.

Es necesario destacar que, más allá de los distintos parámetros utilizados para la configuración del sistema, existen también reglas que rigen la organización del archivo. Para obtener información detallada sobre la manera más efectiva de organizar este archivo, consulte las páginas de manual **esets.cfg(5)** y **esets_daemon(8)**, así como las páginas de manual de los agentes pertinentes.

- **@ETCDIR@/certs**

En este directorio se guardan los certificados de autenticación utilizados por la interfaz web de **ESET File Security**.

Consulte la página de manual **esets_wwwi(8)** para más detalles.

- **@ETCDIR@/license**

En este directorio se guardan las claves de licencia de los productos adquiridos por el cliente. Al buscar una clave de licencia válida, el proceso demonio de **ESET File Security** registrará solamente este directorio, a menos que se redefina el parámetro **license_dir** en el archivo de configuración **esets.cfg**.

- **@ETCDIR@/scripts/license_warning_script**

Si en el archivo de configuración **esets.cfg**, se habilita el guión **license_warning_script** con el parámetro **license_warn_enabled**, este se ejecutará diariamente durante los 30 días anteriores a la expiración de la licencia del producto, enviando un mensaje de correo electrónico al administrador del sistema, advirtiéndole la situación.

- o **@ETCDIR@/scripts/daemon_notification_script**

Si en el archivo de configuración **esets.cfg**, se habilita el guión **daemon_notification_script** con el parámetro **exec_script**, este se ejecutará cuando el sistema antivirus detecte una infiltración, enviando un mensaje de correo electrónico al administrador del sistema para darle aviso del acontecimiento.

4. Integración con los servicios del sistema de archivos

Este capítulo describe la configuración del análisis a petición y del análisis en el acceso, que proporcionará la protección más efectiva contra infecciones de virus y gusanos.

El poder de análisis de **ESET File Security** proviene de sus dos módulos: el comando **esets_scan** del análisis a petición y el comando **esets_dac** del análisis en el acceso.

La versión para Linux de **ESET File Security** ofrece, además, un método adicional de análisis en el acceso que utiliza la librería **libesets_pac.so**.

En las siguientes secciones se describen estos comandos.

4.1 Análisis a petición

Este análisis puede ser activado por un usuario con privilegios de administrador a través de la interfaz de línea de comando, o mediante el calendario de tareas programadas del sistema operativo (por ejemplo: **cron**).

Esto explica la expresión **a petición**, ya que los objetos del sistema de archivos son analizados a partir de una orden del usuario, o del sistema.

No es necesario realizar ninguna configuración adicional para ejecutar el análisis a petición. Una vez que **ESET File Security** ha sido instalado correctamente y se ha guardado una licencia válida en el directorio de claves de licencia **@ETCDIR@/license**, podrá realizar un análisis de forma inmediata, tanto a través de la interfaz de línea de comando, como por medio de la herramienta de calendario.

Para ejecutar el análisis a petición desde la línea de comando, utilice la siguiente sintaxis:

```
@SBINDIR@/esets_scan [option(s)] archivos
```

Donde **archivos** es una lista de directorios o archivos para ser analizados.

Existen varias opciones disponibles para el comando de ejecución del análisis a petición de **ESET File Security**.

Si desea ver la lista completa, consulte la página de manual **esets_scan(8)**.

4.2. Análisis en el acceso basado sobre Dazuko


Este análisis se activa cuando un usuario o un proceso del sistema operativo acceden a un objeto del sistema de archivos. Esto explica la expresión **en el acceso**, ya que el análisis se ejecuta automáticamente con cada intento de acceso a un objeto del sistema de archivos.

El método utilizado por el análisis en el acceso de **ESET File Security** funciona con el módulo central (*kernel module*) Dazuko. Este método se basa sobre la interceptación de las llamadas del núcleo.

El proyecto Dazuko es de código abierto y distribución libre. Esto permite a los usuarios compilar el módulo central para sus propios núcleos.

Es necesario destacar que el módulo central (*kernel module*) Dazuko, no forma parte de ningún producto **ESET** y, por lo tanto, debe ser compilado e instalado en el núcleo (*kernel*) antes de utilizar el comando **esets_dac** de análisis en el acceso.

Por otra parte, el método Dazuko hace que el análisis en el acceso, sea independiente del tipo de sistema de archivos utilizado. Esto permite controlar los objetos en sistemas NFS (*Network File System*, Sistema de archivos de red), Nettalk y Samba.

 **Advertencia:** Antes de proporcionar información más detallada acerca de la configuración y el uso del análisis en el acceso, es necesario aclarar que esta función ha sido desarrollada y probada, principalmente, para proteger sistemas de archivos montados de manera externa. Si existieran varios sistemas de archivos que no hubieran sido montados de esta forma, habrá que excluirlos del control de acceso a archivos para evitar una caída del sistema. Entre los directorios que deben ser típicamente excluidos, se encuentran **/dev** y cualquier otro utilizado por **ESET File Security**.

4.2.1. Principio operativo

El análisis en el acceso es realizado por **esets_dac**, el controlador **ESET** de acceso a archivos basado sobre Dazuko. Se trata de un programa residente que monitoriza y controla continuamente el sistema de archivos.

La versión actual de este controlador reconoce los siguientes tipos de sucesos:

- **Sucesos de apertura**


El control de este tipo de acceso a archivos está activado si en la sección **[dac]** del archivo **esets.cfg**, el parámetro **event_mask** contiene la palabra **open**.

Esta configuración, activará la opción **on_open** del filtro de acceso a archivos de Dazuko.

- **Sucesos de cierre**

El control de este tipo de acceso a archivos está activado si en la sección **[dac]** del archivo **esets.cfg**, el parámetro **event_mask** contiene la palabra **close**.

Esta configuración, activará las opciones **on_close** y **on_close_modified** del filtro de acceso a archivos de Dazuko.

 Algunas versiones del núcleo (*kernel*) de sistema operativo, no soportan la intercepción de los sucesos de cierre, **on_close**. En esos casos, **esets_dac** no monitorizará este tipo de acciones.

- **Sucesos de ejecución**

El control de este tipo de acceso a archivos está activado si en la sección **[dac]** del archivo **esets.cfg**, el parámetro **event_mask** contiene la palabra **exec**.

Esta configuración, activará la opción **on_exec** del filtro de acceso a archivos de Dazuko.

En síntesis, el análisis en el acceso asegura que todo archivo que sea abierto, cerrado o ejecutado sea verificado por **esets_daemon** en busca de virus. Según el resultado de este análisis, se denegará o permitirá el acceso al archivo en cuestión.

4.2.2. Instalación y configuración

Como se mencionó previamente, para que **esets_dac** pueda funcionar, el módulo central (*kernel module*) de Dazuko debe ser compilado e instalado en el núcleo del sistema.

Para obtener más información acerca de la compilación e instalación de Dazuko, consulte:

<http://www.dazuko.org/howto-install.shtml> (sitio en idioma inglés)

Una vez que Dazuko ha sido instalado, en el archivo de configuración **esets.cfg** revise y modifique las secciones **[global]** y **[dac]**.

Tenga en cuenta que el funcionamiento apropiado del análisis en el acceso, depende de la configuración de la opción **agent_enabled**, que se encuentra en la mencionada sección **[dac]**.

También debe determinar los objetos del sistema de archivos que serán monitorizados por el análisis en el acceso. Para ello, en la sección **[dac]**, defina los parámetros de las opciones **ctl_incl** y **ctl_excl**.

Después de realizar los cambios en el archivo **esets.cfg**, podrá forzar la lectura de la nueva configuración creada, cargando nuevamente el proceso demonio de **ESET File Security**.

4.2.3. Recomendaciones

Para asegurar que el módulo Dazuko se cargue antes del inicio del proceso demonio **esets_dac**, siga los pasos detallados a continuación:

- 1) Guarde una copia del módulo Dazuko en alguno de los siguientes directorios, reservados para los módulos del núcleo:

- **/lib/modules**

o


- **modules**


2. Utilice las herramientas para núcleo **depmod** y **modprobe** para manejar las dependencias, así como el inicio correcto, del módulo Dazuko recientemente agregado.

 En sistemas operativos BSD, tendrá que usar **kldconfig** y **kldload**.

3. En el guión de inicio del proceso demonio **/etc/init.d/esets_daemon**, inserte la siguiente línea antes de la instrucción que ejecuta el proceso:

```
/sbin/modprobe dazuko
```

 Para sistemas operativos BSD, deberá modificar el guión **/usr/local/etc/rc.d/esets_daemon.sh**, insertando la línea **/sbin/kldconfig dazuko**.

 **Advertencia:** Es de extrema importancia que estos pasos se ejecuten exactamente en el orden especificado.

Si el módulo del núcleo no está ubicado dentro del directorio correcto, no se cargará apropiadamente, y el sistema se detendrá.

4.3. Análisis en el acceso utilizando la librería LIBC

En secciones anteriores hemos descrito la integración del análisis en el acceso, implementada a través de Dazuko, con los servicios del sistema de archivos de Linux y BSD.

Sin embargo, es conveniente destacar que la técnica de análisis en acceso mediante Dazuko no se recomienda para los administradores de sistemas críticos, especialmente en los siguientes casos:

- El código fuente o los archivos de configuración relacionados con el núcleo (*kernel*) actual, no están disponibles.
- El núcleo (*kernel*), es más monolítico que modular.
- El sistema operativo no es compatible con el módulo Dazuko.

En estas situaciones, debe utilizarse el método de análisis en el acceso basado sobre la librería LIBC.

La siguiente sección, contiene información exclusiva para los usuarios de sistemas operativos Linux, e incluye detalles acerca del funcionamiento, instalación y configuración del análisis en el acceso utilizando la librería **libesets_pac.so**.

4.3.1. Principio de funcionamiento

La librería de objetos compartidos **libesets_pac.so** controla el acceso a los archivos, y se activa automáticamente cuando se inicia el sistema.

Cada vez que un servidor de archivos de sistema (por ejemplo un servidor FTP, Samba, etcétera) realiza una llamada a LIBC, se utiliza esta librería.

La versión actual de **ESET File Security** permite personalizar la configuración de distintos tipos de sucesos, que activarán automáticamente el análisis del objeto afectado.

Los tipos de sucesos disponibles son:

- **Sucesos de apertura**

Este tipo de acceso se activa si en la sección **[pac]** del archivo **esets.cfg**, el valor del parámetro **event_mask** contiene la palabra **open** (abrir).

- **Sucesos de cierre**

Este tipo de acceso se activa si en la sección **[pac]** del archivo **esets.cfg**, el valor del parámetro **event_mask**, contiene la palabra **close** (cerrar).

En este caso, se interceptarán todas las funciones de cierre de archivos o de procesos invocadas por la librería LIBC.

- **Sucesos de ejecución**

Este tipo de acceso se activa si en la sección **[pac]** del archivo **esets.cfg**, el valor del parámetro **event_mask**, contiene la palabra **exec** (ejecutar).

En este caso, se interceptarán todas las funciones **exec** (ejecutar) invocadas por la librería LIBC.

El proceso demonio de *ESET File Security*, analiza todos los archivos abiertos, cerrados o ejecutados, en busca de virus.

El resultado de dichas verificaciones, determinará si se permitirá o denegará el acceso al archivo en cuestión.

4.3.2. Instalación y configuración

El módulo **libesets_pac.so** se instala mediante un mecanismo estándar de este tipo de librerías.

El usuario solamente debe definir la variable de entorno **LD_PRELOAD** junto con la ruta absoluta de la librería **libesets_pac.so**. Para más información, consulte la página de manual **ld.so(8)**.

Nota: es importante que la variable de entorno **LD_PRELOAD** esté definida únicamente para los procesos demonio del servidor de red (ftp, Samba, etcétera) que serán controlados por el análisis en el acceso. Por lo general, no se recomienda la carga previa de las llamadas a librerías LIBC para todos los procesos del sistema operativo, ya que podría disminuir el rendimiento del sistema notoriamente, o incluso interrumpir su funcionamiento.

Por lo tanto, no debe utilizarse el archivo **/etc/ld.so.preload** ni tampoco exportar globalmente la variable de entorno **LD_PRELOAD**. Estas acciones podrían superponerse a todas las llamadas de LIBC relevantes, ocasionando que el sistema se detenga durante el proceso de inicio.

Para interceptar solamente las llamadas relevantes de acceso a archivos, se pueden anular los comandos ejecutables, por medio de la siguiente instrucción:

```
LD_PRELOAD =/path/to/libesets_pac.so comando argumentos_del_comando
```

Donde **comando argumentos_del_comando** es el comando ejecutable original.

En el archivo de configuración **esets.cfg**, se recomienda revisar y modificar las secciones **[global]** y **[pac]**.

Para que el análisis en el acceso funcione correctamente, es necesario definir los objetos del sistema de archivos, es decir directorios y archivos, que debe controlar la librería de carga previa.

Para ello, en la sección **[pac]** del archivo de configuración **esets.cfg**, hay que definir los parámetros de las opciones **ctl_incl** y **ctl_excl**.

Después de hacer los cambios en el archivo **esets.cfg**, es necesario cargar nuevamente el proceso demonio de **ESET File Security** para que la configuración recientemente creada tenga vigencia.

4.3.3. Recomendaciones

La variable de entorno **LD_PRELOAD** debe estar definida dentro del guión de inicio del servidor de archivos de red apropiado, con el fin de ejecutar el análisis en el acceso inmediatamente después del inicio del sistema de archivos.

Ejemplo:

Para que el análisis en el acceso verifique todos los sucesos de acceso al sistema de archivos inmediatamente después del inicio del servidor Samba, realice la siguiente modificación:

En el guión de inicio del proceso demonio de Samba **/etc/init.d/smb**, reemplace el comando

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

por la siguiente línea:

```
LD_PRELOAD = /path/to/libesets_pac.so daemon /usr/sbin/  
smbd $SMBDOPTIONS
```

De esta forma, los objetos del sistema de archivos seleccionados que son controlados por Samba se analizarán apenas se inicie el sistema.

5. Principales mecanismos de seguridad de ESET File Security

5.1. Directivas para el manejo de objetos (*Handle Object Policy*)

El mecanismo de directivas para el manejo de objetos (*Handle Object Policy*), detallado en la figura 6.1, permite filtrar los objetos analizados según su estado.

Esta función se basa sobre las siguientes opciones de configuración: **action_av**, **action_av_infected**, **action_av_notscanned**, y **action_av_deleted**.

Para obtener mayor información sobre estas opciones y sus características, consulte la página de manual [esets.cfg\(5\)](#).

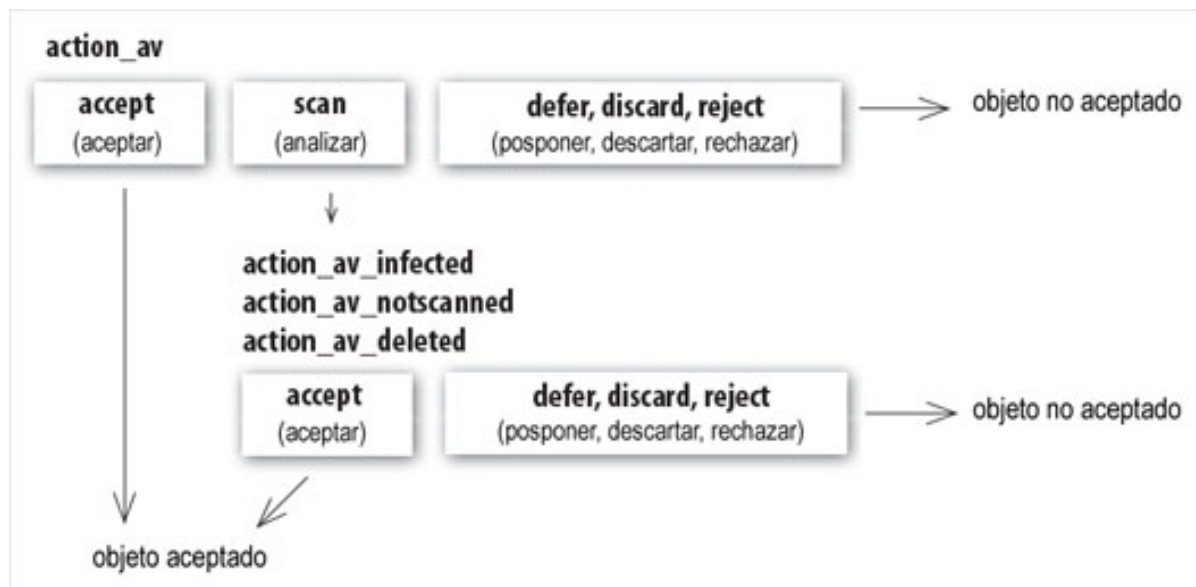


Figura 5-1. Esquema del mecanismo de directivas para el manejo de objetos (*Handle Object Policy*)

Inicialmente, cada objeto procesado se gestiona según la configuración de la opción **action_av**.

De acuerdo con el valor determinado para dicha opción, el objeto se aceptará (**accept**), pospondrá (**defer**), descartará (**discard**), o rechazará (**reject**), según corresponda.

Si se le ha asignado el valor **scan** (analizar), el objeto será examinado en busca de infiltraciones de virus. Si la opción **av_clean_mode** tiene el valor **yes** (sí), al encontrar una amenaza, el objeto será desinfectado automáticamente.

Las opciones **action_av_infected**, **action_av_notscanned** y **action_av_deleted** sirven para determinar la acción que se aplicará sobre el objeto.

Si cada una de ellas tuvo como resultado el valor **accept** (aceptar), el objeto será admitido. En caso contrario, será bloqueado.

5.2. Configuración específica del usuario (*User Specific Configuration*)

El propósito de la configuración específica del usuario (*User Specific Configuration*), es proporcionar un mayor nivel de personalización y funcionalidad al sistema.

Este mecanismo, le permite al administrador definir los parámetros del análisis antivirus de **ESET File Security**, basándose sobre las necesidades de cada usuario que accede al sistema.

En esta sección, daremos un breve ejemplo de una configuración específica del usuario.

Para obtener una descripción más detallada sobre esta función, consulte la página del manual **esets.cfg(5)**.

En nuestro ejemplo, el objetivo es utilizar el módulo **esets_dac** para controlar las acciones de acceso **on_openy on_exec** para un disco externo, montado bajo el directorio **/home**.

En la sección **[dac]** del archivo de configuración **esets.cfg**, se puede modificar este módulo, como se muestra a continuación:

```
[dac]
agent_enable = yes
event_mask = open
ctl_incl = /home
action_av = scan
```

ESET File Security permite asignar una configuración de análisis especial para un usuario en particular. Para ello, hay que seguir los pasos descritos a continuación:

1. En la sección **[dac]** del archivo de configuración de **ESETS**, hay que definir el parámetro **user_config**, especificando el nombre del archivo donde se guardarán las reglas especiales.
En el siguiente ejemplo, el archivo se llama **esets_dac_spec.cfg** y está ubicado dentro del directorio de configuración de **ESET File Security**.
La ruta de este directorio varía según el sistema operativo utilizado (Ver capítulo 2, Directorio de configuración).

```
[dac]
agent_enabled = yes
event_mask = open
ctl_incl = /home
action_av = scan
user_config = esets_dac_spec.cfg
```

2. Después de definir el archivo en el parámetro **user_config**, en el directorio de configuración de **ESET File Security** hay que crear el archivo **esets_dac_spec.cfg**.
3. Por último, hay que agregar las reglas deseadas.
Al comienzo de la sección especial, se debe introducir el nombre del usuario al cual se aplicará la configuración individual, y debajo especificar la lista de reglas.

La configuración determinada a continuación permitirá que se procesen normalmente los intentos de acceso al sistema de archivos realizados por los usuarios, excepto aquellos que provengan del usuario **antonio**:


```
[antonio]
action_av = reject
```

Es decir que, por ejemplo, todos los objetos del sistema de archivos a los cuales accedan los usuarios, serán analizados en busca de virus, excepto cuando el usuario activo sea el que se ha especificado en la configuración, en cuyo caso se denegará el acceso.

5.3. Sistema de envío de muestras

El sistema de envío de muestras, basado sobre la tecnología **ThreatSense.Net**, recolecta los objetos infectados que han sido detectados por la heurística avanzada, y los envía a un servidor especialmente dedicado.

Todas las muestras recibidas a través de este sistema, serán procesadas en el laboratorio de investigación de virus de **ESET**. Si es necesario, se agregarán a la base de datos de firmas de virus.

 Nuestro acuerdo de licencia especifica que, al habilitar el sistema de envío de muestras, el usuario acepta que la computadora o plataforma donde está instalado `esets_daemon` recopile ciertos datos, que pueden incluir información personal y muestras de los virus u otras amenazas detectadas recientemente, para enviarlos posteriormente a nuestro laboratorio.

De forma predeterminada, esta característica está desactivada.

Toda la información recolectada se utilizará únicamente para analizar nuevas amenazas, y no se usará con ningún otro fin.

Para activar el sistema de envío de muestras, en la sección **[global]** del archivo de configuración de **ESET File Security**, hay que habilitar la opción `samples_enabled`.

Para permitir el envío de las muestras a los servidores del laboratorio de análisis de virus de **ESET**, en la misma sección también se debe activar el parámetro `samples_send_enabled`.

Asimismo, el usuario tiene la posibilidad de proporcionar información complementaria al equipo del laboratorio de virus de **ESET**, si así lo desea.

Para esto puede utilizar las opciones de configuración `samples_provider_mail` y `samples_provider_country`.

La información recolectada mediante el uso de estas opciones, ayudará al equipo de **ESET** a tener una visión de conjunto sobre una infiltración específica, que podría estar diseminándose a través Internet.

Para obtener más información acerca del sistema de envío de muestras, consulte la página de manual `esets_daemon(8)`.

5.4. Interfaz web

La interfaz web simplifica las tareas de configuración, administración y gestión de licencias de los sistemas de seguridad **ESET**.

Este módulo, es un agente independiente y debe ser activado de forma explícita.

Para configurar rápidamente la interfaz web:

1. Modifique las siguientes entradas en el archivo de configuración **esets.cfg**:

```
[wwwi]
agent_enabled = yes
listen_addr = dirección de escucha
listen_port = puerto de escucha
username = nombre de usuario
password = contraseña
```

2. Reemplace los valores destacados por los datos correspondientes a su sistema, y abra su navegador en la página <https://address:port>.

Para acceder al contenido, deberá introducir su nombre de usuario y contraseña.

3. A continuación, reinicie el proceso demonio de **ESET File Security**.

En la página de ayuda encontrará instrucciones para el uso básico de esta característica. Si desea obtener más detalles técnicos, consulte la página de manual **esets_wwwi(1)**.

5.5. Administración remota

ESET File Security es compatible con **ESET Remote Administrator**. Esto permite gestionar de forma remota la seguridad en redes extensas.

Para más información, consulte el [manual de ESET Remote Administrator](#).

El cliente de administración remota es parte del proceso demonio principal de **ESET File Security**.

Para una configuración básica, en la sección **[global]** del archivo **esets_cfg**, utilice el parámetro **racl_server_addr**.

Si se ha establecido una contraseña para el uso de la consola de **ESET Remote Administrator**, también deberá definir el parámetro **racl_password**.

En la página de manual **esets_daemon(8)**, encontrará una lista con todas las variables disponibles para configurar el cliente **ESET Remote Administrator**.

El cliente **ESET Remote Administrator** integrado en las soluciones de seguridad **ESET** para sistemas Unix, realiza las siguientes operaciones:

- Se comunica con el servidor de administración remota **ERAS** y proporciona información del sistema, configuración, estado de la protección y sus características.
- Permite ver y modificar las configuraciones cliente utilizando **ESET Configuration Editor** y aplicarlas mediante una tarea específica.
- Realiza análisis y actualizaciones a petición del usuario y envía los registros de análisis al servidor de administración remota **ERAS**.
- Envía al registro de amenazas los análisis más importantes realizados por el proceso demonio de **ESET File Security**.
- Envía al registro de sucesos todos los mensajes que no contengan avisos de depuración de errores.

Funciones no compatibles:

- Registro de cortafuegos.
- Instalación remota.

6. Sistema de actualización de *ESET File Security*

6.1. Herramienta de actualización de *ESET File Security*

Para asegurar la eficacia de **ESET File Security**, la base de firmas de virus debe mantenerse actualizada. La herramienta **esets_update** ha sido desarrollada con este propósito.

Para obtener más información sobre su funcionamiento, consulte la página de manual **esets_update(8)**.

Antes de ejecutar una actualización, en la sección **[global]** del archivo de configuración de **ESET File Security** deben estar definidas las opciones **av_update_username** y **av_update_password**.

Si el acceso a Internet se realiza a través de un servidor *Proxy* HTTP, también hay que determinar las opciones **proxy_addr** y **proxy_port**.

Asimismo, si el servidor *Proxy* solicita un nombre de usuario y una contraseña, será necesario definir las opciones **proxy_username** y **proxy_password** en dicha sección.

Para iniciar una actualización, introduzca el siguiente comando:

```
@SBINDIR@/esets_update
```

Con el objetivo de ofrecer la mayor seguridad posible al usuario final, el equipo de investigadores de **ESET** recolecta permanentemente definiciones de virus provenientes de todo el mundo.

Los patrones nuevos, se agregan a la base de firmas en intervalos breves. Por tal motivo, se recomienda realizar actualizaciones con frecuencia.

En la sección **[global]** del archivo de configuración de **ESET File Security**, la opción **av_update_period** permite determinar la periodicidad de las actualizaciones.

Para que la actualización de la base de firmas de virus sea exitosa, el proceso demonio de **ESET File Security** debe estar activo y en funcionamiento.

6.2. Descripción del proceso de actualización de *ESET File Security*

El proceso de actualización consta de dos pasos:

1. En primer lugar, se descargan los módulos de actualización desde el servidor de **ESET**. Si en la sección **[global]** del archivo de configuración **esets.cfg** se encuentra presente la opción **av_mirror_enabled**, se crearán copias de dichos módulos. Estas, se guardarán de forma predefinida en el siguiente directorio:

@BASEDIR@/mirror

La ruta del directorio del servidor local de actualizaciones (*Mirror*) se puede redefinir en el archivo de configuración de **ESET File Security**, en la sección **[update]** (actualización), utilizando la opción **av_mirror_dir**.

El servidor recientemente creado es completamente funcional y también puede ser copiado para crear otras imágenes de actualización, de menor jerarquía en la estructura de árbol de la red. Sin embargo, es necesario cumplir con las siguientes condiciones:

1. El ordenador donde se descargarán los módulos debe tener instalado un servidor HTTP.
2. Los módulos que serán descargados por otros ordenadores, deben ubicarse en el siguiente directorio:

/http-serv-base-path/eset_upd

En el ejemplo anterior, **/http-serv-base-path/eset_upd** es la ruta básica de un servidor HTTP. Este será el primer directorio donde la herramienta de actualización buscará los archivos con los datos nuevos.

2. En el segundo paso del proceso, se compilan los módulos guardados en el servidor local de actualizaciones (*Mirror*), que utilizará posteriormente el motor de análisis de **ESET Mail Security**. Normalmente, se crearán los siguientes módulos de carga (entre otros):
 - Módulo cargador (*loader module*): em000.dat
 - Módulo de análisis (*scanner module*): em001.dat
 - Módulo de base de datos de firmas de virus (*virus signature database module*): em002.dat
 - Módulos de compatibilidad para diferentes archivos (*archive support module*): em003.dat
 - Módulos de heurística avanzada (*advanced heuristics module*): em004.dat

Todos ellos se crearán en el siguiente directorio:

@BASEDIR@

El proceso demonio de **ESET File Security**, carga sus módulos desde dicho directorio. En la sección **[global]** del archivo de configuración **esets.cfg**, la opción **base_dir** permite redefinir este valor, si fuera necesario hacerlo.

6.3. Proceso demonio del servidor local de actualizaciones HTTP de *ESET File Security*

El proceso del servidor local de actualizaciones HTTP se instala automáticamente con **ESET File Security**. Este servicio se inicia si el servidor **Mirror** está habilitado y en la sección **[global]** del archivo **esets.cfg**, la opción **av_mirror_httpd_enabled** tiene el valor **yes** (sí).

Las opciones **av_mirror_httpd_port** y **av_mirror_httpd_addr** definen el puerto (el valor predeterminado es 2221) y la dirección de escucha del servidor HTTP (las predeterminadas son todas las direcciones locales TCP).

La opción **av_mirror_httpd_auth_mode** permite cambiar al modo básico de autenticación de acceso. El valor predeterminado para esta opción es **none** (ninguno).

Las opciones **av_mirror_httpd_username** y **av_mirror_httpd_password** posibilitan que el administrador defina los parámetros de acceso al servidor local de actualizaciones.

7. Glosario

En esta sección, se detallarán algunos de los términos y abreviaciones que se utilizan a lo largo de este manual.

- **RSR**

Es la abreviatura de Red Hat / Novell (SuSE) Ready.

ESET File Security es compatible con las variantes Red Hat Ready y Novell (SuSE) Ready. La diferencia del paquete **RSR** con la versión estándar de **ESET File Security** para Linux, es que el primero cumple los requerimientos definidos por la norma FHS (*File-system Hierarchy Standar*, Estándar de jerarquía del sistema de archivos definido como parte de la base de Linux), exigidos por la certificación Red Hat Ready y Novell (SuSE) Ready.

El paquete **RSR** es un complemento de **ESET File Security**, y su directorio principal de instalación es `/opt/eset/esets`.

- **Proceso demonio esets_daemon**

El proceso `esets_daemon`, es el demonio principal de análisis y control del sistema.

- **Directorio base**

Es el directorio donde se guardan los módulos de **ESET File Security** que contienen la base de firmas de virus.

Utilizaremos la variable `@BASEDIR@` para referirnos a dicho directorio. A continuación se presenta el valor de `@BASEDIR@` para los siguientes sistemas operativos:

- Linux: `/var/lib/esets`
- Linux RSR: `/var/opt/eset/esets/lib`
- FreeBSD: `/var/lib/esets`
- NetBSD: `/var/lib/esets`
- Solaris: `/var/opt/esets/lib`

- **Directorio de configuración de *ESET File Security***

Es el directorio donde se guardan todos los archivos relacionados con la configuración de **ESET File Security**.

Utilizaremos la variable `@ETCDIR@` para referirnos a dicho directorio. A continuación se presenta el valor de `@ETCDIR@` para los para los siguientes sistemas operativos:

- Linux: `/etc/esets`
- Linux RSR: `/etc/opt/eset/esets`
- FreeBSD: `/usr/local/etc/esets`
- NetBSD: `/usr/pkg/etc/esets`
- Solaris: `/etc/opt/esets`

- **Archivo de configuración de *ESET File Security***

Es el archivo de configuración principal de **ESET File Security**. La ruta absoluta de su ubicación es:

@ETCDIR@/esets.cfg

- **Directorio de archivos binarios de *ESET File Security***

Es el directorio donde se guardan los archivos binarios de **ESET File Security**.

Utilizaremos la variable **@BINDIR@** para referirnos a dicho directorio.

A continuación se presenta el valor de **@BINDIR@** para los siguientes sistemas operativos:

- Linux: /usr/bin
- Linux RSR: /opt/eset/esets/bin
- FreeBSD: /usr/local/bin
- NetBSD: /usr/pkg/bin
- Solaris: /opt/esets/bin

- **Directorio de archivos binarios del sistema *ESET File Security***

Es el directorio donde se guardan los archivos de sistema binarios de **ESET File Security**.

Utilizaremos la variable **@SBINDIR@** para referirnos a dicho directorio.

A continuación se presenta el valor de **@SBINDIR@** para los siguientes sistemas operativos:

- Linux: /usr/sbin
- Linux RSR: /opt/eset/esets/sbin
- FreeBSD: /usr/local/sbin
- NetBSD: /usr/pkg/sbin
- Solaris: /opt/esets/sbin

- **Directorio de archivos objeto de *ESET File Security***

Es el directorio donde se guardan los archivos objeto y bibliotecas de **ESET File Security**.

Utilizaremos la variable **@LIBDIR@** para referirnos a dicho directorio.

A continuación se presenta el valor de **@LIBDIR@** para los siguientes sistemas operativos:

- Linux: /usr/lib/esets
- Linux RSR: /opt/eset/esets/lib
- FreeBSD: /usr/local/lib/esets
- NetBSD: /usr/pkg/lib/esets
- Solaris: /opt/esets/lib

8. Contacto

Apreciado usuario, esperamos que esta guía le haya permitido comprender cabalmente los requisitos para la instalación, configuración y mantenimiento de **ESET File Security**.

Sin embargo, nuestro objetivo es mejorar continuamente la calidad de nuestra documentación. Si considera que alguna sección de esta guía no es clara o se encuentra incompleta, por favor comuníquese con nosotros.

Nos dedicamos a proporcionar un servicio de asistencia técnica de excelencia, y estamos disponibles para ayudarlo ante cualquier duda, problema o comentario acerca de este producto

Soporte técnico:

ayuda@eset.es

Ventas:

ventas@eset.es

Información general:

info@eset.es

Direcciones:

ESET NOD32 en España

Ontinet.com, S.L.,
c/Martinez Valls 56 bajos
46870 Ontinyent (Valencia)
España

Teléfono: +34 902.33.48.33
Fax: +34 96.191.03.21

ESET, Central

ESET, LLC.
610 West Ash Street,
Suite 1900
San Diego, CA 92101
USA

Teléfono: +1 (619) 876-5400
Fax: +1 (619) 437-7045

9. Apéndice A: Licencia PHP

Licencia PHP, versión 3.01 (*The PHP License, version 3.01*).

Copyright (c) 1999 - 2006, por The PHP Group.

Todos los derechos reservados. Se permite la redistribución y uso del código fuente o binario, con o sin modificación, siempre y cuando se cumplan las siguientes condiciones:

1. Las redistribuciones del código fuente deben mantener el aviso de *copyright* arriba detallado, la presente lista de condiciones y la exención de responsabilidad enunciada al final del documento.
2. Las redistribuciones del código binario deben reproducir el aviso de *copyright* arriba detallado, la presente lista de condiciones, la exención de responsabilidad enunciada al final de documento, y cualquier otro material incluido en esta distribución.
3. El nombre **PHP** no debe utilizarse para auspiciar o promover productos derivados de esta aplicación sin previo permiso escrito. Para obtener un permiso escrito, envíe un mensaje a group@php.net.
4. Los productos derivados de esta aplicación no pueden denominarse **PHP**, como tampoco puede aparecer la sigla **PHP** en su nombre, sin haber obtenido el permiso escrito de group@php.net. Está permitido destacar que su programa trabaja en conjunto con **PHP** indicando, por ejemplo, **Nombre_del_programa para PHP** en lugar de **PHP Nombre_del_programa** o **phpnombre_del_programa**.
5. The PHP Group puede publicar, regularmente, versiones corregidas o renovadas de esta licencia. Estas tendrán asignado un número de versión distintivo. Una vez que el código ha sido publicado con un número de versión determinado, el usuario puede seguir utilizándolo bajo la reglamentación que posea esa versión, o bien puede registrarse bajo los términos de cualquier versión de licencia publicada posteriormente. Solamente The PHP Group tiene el derecho de modificar los términos aplicables al código creado bajo esta licencia.
6. Las redistribuciones de código fuente o binario deben conservar y enunciar la siguiente certificación:
"Este producto ha sido desarrollado con PHP. Esta aplicación gratuita está disponible en <http://php.net/software/>".

ESTE SOFTWARE ES DISTRIBUIDO POR EL EQUIPO DE DESARROLLO DE PHP EN UNA CONDICIÓN "TAL COMO ESTÁ". NO SE RECONOCE NINGUNA GARANTÍA EXPLÍCITA O IMPLÍCITA, INCLUYENDO GARANTÍA DE VENTA O IDONEIDAD PARA UNA FINALIDAD ESPECÍFICA. EL EQUIPO DE DESARROLLO DE PHP O SUS COLABORADORES NO SERÁN RESPONSABLES EN NINGÚN CASO POR DAÑOS DIRECTOS, INDIRECTOS, ACCIDENTALES, ESPECIALES O PUNITIVOS DE NINGÚN TIPO (INCLUYENDO LA ADQUISICIÓN DE BIENES O SERVICIOS SUSTITUTOS, PÉRDIDA DE INFORMACIÓN O DE BENEFICIOS O INTERRUPCIÓN DEL NEGOCIO), CUALQUIERA SEA SU CAUSA; Y BAJO NINGUNA SUPOSICIÓN DE RESPONSABILIDAD, YA SEA CONTRACTUAL, ABSOLUTA O FRAUDULENTO (POR NEGLIGENCIA O DE FORMA VOLUNTARIA) OCASIONADOS POR LA UTILIZACIÓN DE ESTE SOFTWARE, INCLUSO SI SE HA ADVERTIDO DE LA POSIBILIDAD DE DICHO DAÑO.