

SIN CLASIFICAR



# MARTA: Manual de Usuario

---

## Motor de Análisis Remoto de Troyanos Avanzados

Febrero 2016

SIN CLASIFICAR

**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

|                                                       |    |
|-------------------------------------------------------|----|
| ÍNDICE.....                                           | 3  |
| 1    SOBRE CCN-CERT .....                             | 6  |
| 2    FUNCIONALIDAD GENERAL .....                      | 7  |
| 2.1   RECEPCIÓN DE FICHEROS Y ANÁLISIS ESTÁTICO ..... | 7  |
| 2.2   ANÁLISIS DINÁMICO .....                         | 7  |
| 2.3   MOTOR DE REGLAS.....                            | 8  |
| 2.4   ETIQUETAS.....                                  | 9  |
| 2.5   BÚSQUEDA AVANZADA .....                         | 9  |
| 2.6   ESTADÍSTICAS .....                              | 9  |
| 2.7   TRIANA.....                                     | 9  |
| 2.8   INFORMES.....                                   | 10 |
| 3    VISTA DE ACCESO .....                            | 11 |
| 4    VISTA PRINCIPAL.....                             | 14 |
| 5    PESTAÑA DE BINARIOS .....                        | 16 |
| 5.1   LISTADO .....                                   | 16 |
| 5.2   ACCIONES SOBRE LOS FICHEROS .....               | 18 |
| 5.3   ACCIONES GENERALES.....                         | 20 |
| 5.4   ETIQUETAS.....                                  | 22 |
| 6    PESTAÑA DE ANÁLISIS .....                        | 31 |
| 6.1   LISTADO .....                                   | 31 |
| 6.2   ESTADOS DE UN ANÁLISIS .....                    | 32 |
| 6.3   ACCIONES SOBRE LOS ANÁLISIS .....               | 32 |
| 6.4   ACCIONES GENERALES.....                         | 36 |
| 6.5   ETIQUETAS.....                                  | 36 |
| 7    VISTA DE SUBIDA DE UN BINARIO .....              | 38 |
| 7.1   CAMPOS DEL FORMULARIO.....                      | 39 |
| 7.2   SUBIDA DEL FICHERO.....                         | 45 |
| 8    VISTA DE REANÁLISIS DE UN BINARIO .....          | 49 |
| 8.1   CAMPOS DEL FORMULARIO.....                      | 50 |
| 8.2   CREACIÓN DE LOS REANÁLISIS.....                 | 51 |
| 9    VISTA DE DETALLE DE UN BINARIO.....              | 54 |

|       |                                      |     |
|-------|--------------------------------------|-----|
| 9.1   | GENERAL .....                        | 55  |
| 9.2   | ANÁLISIS.....                        | 56  |
| 9.3   | ETIQUETAS.....                       | 57  |
| 9.4   | REANÁLISIS.....                      | 59  |
| 9.5   | DETALLES EJECUTABLE .....            | 60  |
| 9.6   | DETALLES PDF .....                   | 68  |
| 9.7   | DETALLES OFFICE .....                | 70  |
| 9.8   | DETALLES OPENOFFICE.....             | 71  |
| 10    | VISTA DE DETALLE DE UN ANÁLISIS..... | 72  |
| 10.1  | GENERAL .....                        | 74  |
| 10.2  | REGLAS .....                         | 78  |
| 10.3  | ETIQUETAS.....                       | 87  |
| 10.4  | EVIDENCIAS .....                     | 90  |
| 10.5  | STRINGS .....                        | 93  |
| 10.6  | RED.....                             | 99  |
| 10.7  | CLAVES DE REGISTRO .....             | 103 |
| 10.8  | FICHEROS .....                       | 104 |
| 10.9  | PROCESOS.....                        | 105 |
| 10.10 | SERVICIOS .....                      | 106 |
| 10.11 | HOOKS.....                           | 106 |
| 10.12 | INFORME PERSONALIZADO.....           | 108 |
| 11    | PESTAÑA DE BÚSQUEDA AVANZADA.....    | 110 |
| 12    | PESTAÑA DE CONFIGURACIÓN.....        | 119 |
| 13    | PESTAÑA DE REGLAS IOC.....           | 120 |
| 13.1  | LISTADO .....                        | 120 |
| 13.2  | ACCIONES SOBRE LAS REGLAS .....      | 121 |
| 13.3  | ACCIONES GENERALES.....              | 123 |
| 13.4  | ETIQUETAS.....                       | 126 |
| 14    | VISTA DE DETALLE DE UNA REGLA .....  | 128 |
| 14.1  | DATOS.....                           | 129 |
| 14.2  | ETIQUETAS.....                       | 148 |
| 15    | REGLAS YARA.....                     | 150 |

|             |                                       |            |
|-------------|---------------------------------------|------------|
| <b>15.1</b> | <b>LISTADO .....</b>                  | <b>150</b> |
| <b>15.2</b> | <b>ACCIONES REGLAS YARA .....</b>     | <b>150</b> |
| 15.2.1      | DETALLE REGLA YARA .....              | 151        |
| 15.2.2      | ELIMINAR REGLA YARA .....             | 152        |
| 15.2.3      | CREAR REGLA YARA .....                | 152        |
| 15.2.4      | ACTIVAR REGLAS SELECCIONADAS .....    | 152        |
| 15.2.5      | DESACTIVAR REGLAS SELECCIONADAS ..... | 153        |
| 15.2.6      | CARGAR REGLAS DESDE UN FICHERO .....  | 153        |
| 15.2.7      | ETIQUETAS.....                        | 154        |
| <b>16</b>   | <b>PESTAÑA DE ESTADÍSTICAS .....</b>  | <b>155</b> |

## 1 SOBRE CCN-CERT

El CCN-CERT ([www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN ([www.ccn.cni.es](http://www.ccn.cni.es)). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, del **Sector Público y de empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

## 2 FUNCIONALIDAD GENERAL

MARTA es una aplicación dedicada al **análisis automatizado** de múltiples tipos de ficheros, que podrían tener un comportamiento malicioso (**malware**). Esto incluye, por supuesto, ejecutables, pero también otros tipos de ficheros, como documentos de office o pdfs.

Para facilitar el uso de la aplicación, MARTA consta de una **interfaz web**, que se puede ejecutar a través de un navegador. Preferentemente, recomendamos el uso de Mozilla Firefox y Google Chrome, en su versión más actualizada.

A través de la interfaz web se pueden utilizar todas las funcionalidades de la aplicación, las cuales se describen a lo largo de este documento. A modo de resumen, el funcionamiento general es el siguiente:

### 2.1 RECEPCIÓN DE FICHEROS Y ANÁLISIS ESTÁTICO

En primer lugar, la aplicación recibe un fichero sospechoso de ser malware. Este fichero puede provenir de una subida manual a través de la interfaz web, o de un colector. Los colectores recogen periódicamente códigos dañinos de páginas web dedicadas al listado de malwares, tales como VirusTotal, Malc0de, etc.

Lo primero que hace la aplicación cuando recibe un fichero, es pasarle una serie de **scripts "estáticos"**. Los llamamos estáticos porque el código dañino no se ejecuta en ningún momento mientras se le analiza con estos scripts. Con ellos, MARTA obtiene cierta **información específica del fichero**, como su tipo (exe, dll, docx, pdf, etc), o sus hashes (MD5, SHA1, Ssdeep, etc).

En función del tipo de fichero, se obtiene más información. Por ejemplo, para ejecutables, se obtiene toda la información en la cabecera del fichero, la tabla de directorios, las secciones del binario, los recursos y librerías que utiliza, etc. En cambio, para pdfs, se obtienen sus metadatos, javascripts embebidos, objetos internos, etc.

Una vez se han pasado los scripts estáticos, el fichero queda registrado en la base de datos de MARTA, junto con todos los datos obtenidos. A través de la interfaz web, se pueden consultar todos los ficheros registrados, y, por supuesto, sus datos.

### 2.2 ANÁLISIS DINÁMICO

En cualquier momento, se puede pedir un **análisis dinámico** de uno de los ficheros registrados. Esta es la funcionalidad más relevante de MARTA. Un análisis dinámico consiste en **infectar una máquina virtual** que tenga instalado un sistema operativo concreto con el fichero sospechoso de ser malware. Es decir, cuando se pide un análisis dinámico de un fichero, se clona una máquina virtual, se copia el fichero en ella y se ejecuta.

En el momento de pedir el análisis, se puede elegir qué máquina virtual se desea infectar (en función del sistema operativo), junto con otras opciones, como la conexión a internet de la máquina (salida por TOR, Internet Simulado, sin Internet), la duración máxima

del análisis, aplicaciones que se deben instalar en la máquina virtual antes de ejecutar el fichero, si se desea hacer una simulación humana durante la ejecución (clics, tecleo, etc), entre otras.

Cada análisis dinámico se realiza clonando una máquina virtual “limpia”. Es decir, cuando se termina un análisis, la máquina virtual que se ha utilizado se destruye. Y en el siguiente análisis, se clona nuevamente una máquina virtual del sistema operativo elegido.

Lo que hace que el análisis dinámico sea la parte más relevante de MARTA es que durante la ejecución del fichero en la máquina virtual, hay un **software monitorizando** un conjunto factores clave para determinar el **comportamiento del fichero**: conexiones de red, claves de registro, ficheros, procesos, análisis sobre la memoria, etc.

A este software lo llamamos “**sandbox**”. Actualmente, MARTA integra dos sandbox diferentes: **Cuckoo** y **Joe**. En el momento de pedir un análisis dinámico de un fichero, se puede elegir qué sandbox se desea utilizar para el análisis. Cada sandbox monitoriza la ejecución del fichero de una forma diferente. Gracias a la integración de ambas, se puede determinar el comportamiento de códigos dañinos que de forma individual, una de las sandbox no podría determinar.

Cada vez que se realiza un análisis dinámico de un fichero, se registra en la base de datos de MARTA, junto con todos los factores claves para determinar el comportamiento del fichero extraídos por la sandbox. A través de la interfaz web, se pueden consultar todos los análisis realizados, y todos estos factores.

## 2.3 MOTOR DE REGLAS

MARTA cuenta con un **motor de reglas**, que permite **definir comportamientos reconocidos**, para que **MARTA los compruebe** de forma automática.

Por ejemplo, si sabemos que un código dañino reconocido modifica la clave de registro de internet explorer zone map, se conecta a la IP 84.22.100.108, y crea y ejecuta un fichero llamado info.exe, podemos definir una regla con todas estas características, y pedirle a MARTA que la compruebe contra todos los análisis dinámicos que se realicen.

A través de la interfaz web, podemos consultar qué reglas cumple cada análisis dinámico. De esta forma, podemos reconocer inmediatamente si un fichero se comporta como un código dañino conocido. Esto también puede utilizarse para definir y detectar comportamientos sospechosos o interesantes. La propia interfaz web proporciona una vista para gestionar las reglas de una manera sencilla e intuitiva. Las reglas siguen una estructura de árbol lógico (con operadores and y or), idéntica a la de los **IOC**.

## 2.4 ETIQUETAS

MARTA dispone de un sistema de etiquetado, que permite una organización sencilla, visual y ágil de ficheros, análisis y reglas. Desde la interfaz web, se pueden crear etiquetas, que constan de un nombre, un alias de hasta 4 letras y un color (para cada etiqueta, se crea un icono con forma de óvalo del color elegido y con el alias escrito dentro). Estas **etiquetas** se pueden **asignar a reglas**.

Siempre que un **análisis dinámico cumpla una regla**, se le asignarán todas las **etiquetas asociadas** a ella. De esta forma, echando un vistazo rápido a las etiquetas de un análisis, podemos conocer qué reglas cumple.

Además, a los **ficheros** se les asignan todas las **etiquetas asociadas a sus análisis**. Por lo que, de forma automática, todos los ficheros reciben etiquetas en función de sus comportamientos detectados entre todos sus análisis. Así, de un solo vistazo a las etiquetas de un fichero, podemos hacernos a la idea de si es un malware, y, en caso de que lo sea, cuál es su funcionamiento.

También se pueden asociar manualmente etiquetas a un análisis (además de las recibidas por las reglas que cumple), y su fichero recibiría automáticamente estas etiquetas. Similarmente, se pueden asociar de forma manual etiquetas a un fichero (además de las recibidas por sus análisis). Esta funcionalidad sólo tiene fines organizativos.

Tanto ficheros, como análisis y reglas pueden ser filtrados por etiquetas. De esta forma podemos buscar rápidamente todos los códigos dañinos que estén registrados en la base de datos de MARTA que tengan un comportamiento específico.

## 2.5 BÚSQUEDA AVANZADA

MARTA cuenta con una herramienta de **búsqueda avanzada**, que permite buscar ficheros **filtrando por cualquier dato** que pudiera obtenerse tanto de los resultados de los scripts estáticos como de los análisis dinámicos. Por ejemplo, es posible buscar todos los ficheros que crean un fichero .exe y sobrescriben la clave de registro Software\Microsoft\Windows\CurrentVersion\Run.

## 2.6 ESTADÍSTICAS

MARTA dispone de una sección de **estadísticas**, en la que se pueden consultar las etiquetas más comunes, el total de ficheros por tipo, o el número de ficheros subidos en los últimos 30 días.

## 2.7 TRIANA

MARTA está integrada con **Triana**, Threat Intelligent Analysis. Es una herramienta de **búsqueda de información por Internet sobre malwares**.

En el momento de pedir un análisis dinámico de un fichero, es posible seleccionar la opción Triana. De hacerlo, se realizará una búsqueda del MD5 del fichero en una serie de páginas de Internet dedicadas a la recopilación de información de malwares, tales como

Virus Total o Malwr (algunas de éstas páginas también son colectores). Cada una de estas páginas aporta información diversa acerca del código dañino correspondiente al MD5 buscado. Toda la información obtenida se almacena y se asocia al análisis dinámico.

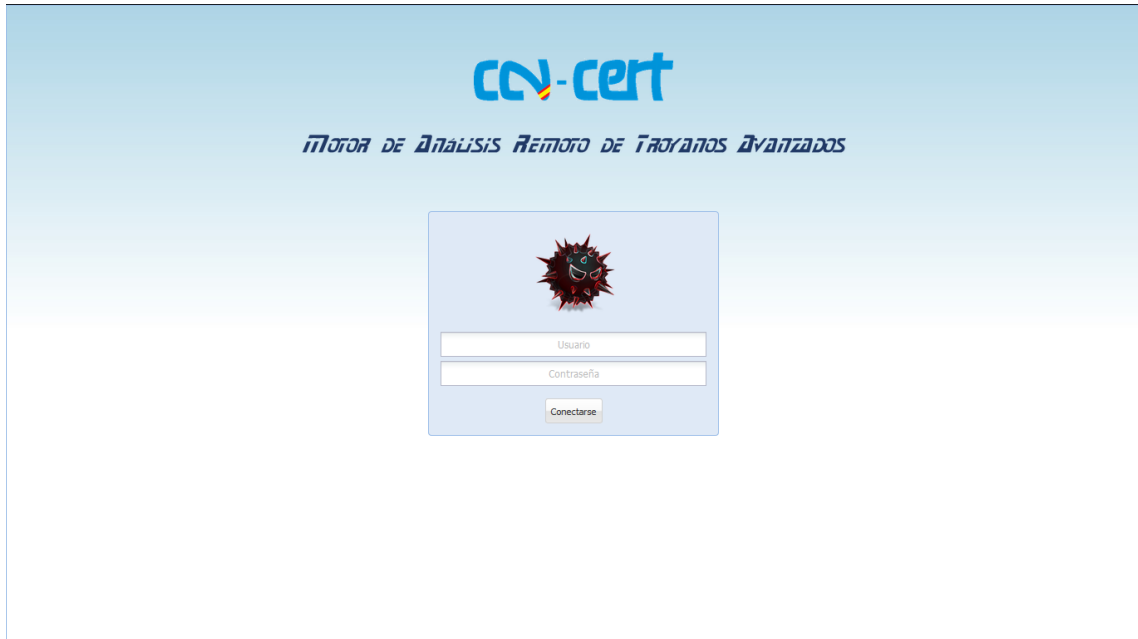
## 2.8 INFORMES

MARTA permite la generación de **informes** a partir de un análisis dinámico. Estos informes incluyen por defecto toda la información extraída del análisis, y también toda la información de los scripts estáticos. Sin embargo, es posible generar informes personalizados con sólo algunas partes de esta información.

Si el análisis dinámico tiene información de Triana asociada, el informe incluirá un anexo con toda esta información.

### 3 VISTA DE ACCESO

Lo primero que vemos al acceder a la aplicación es una vista de acceso, en la que podemos introducir nuestros **credenciales**:



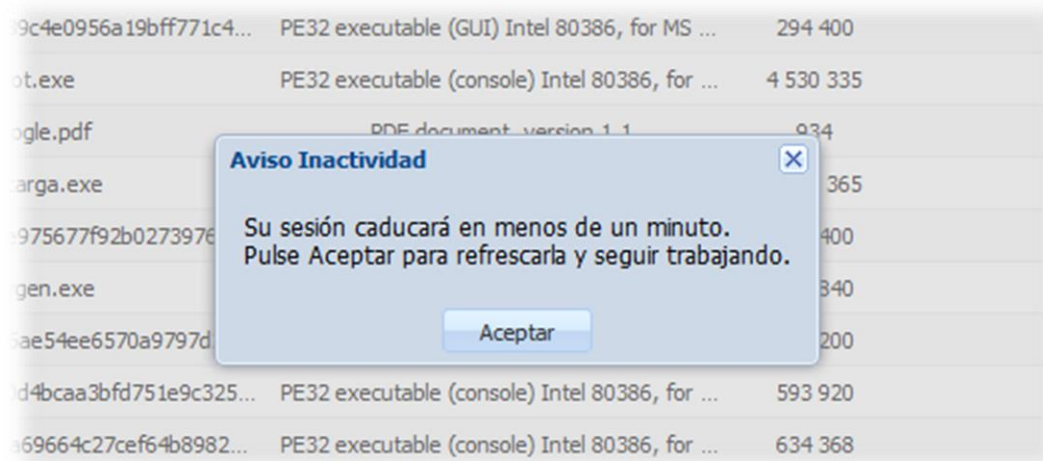
Una vez introducidos, si son correctos, accederemos a la vista principal de la aplicación:

| Binarios         | Análisis                         | Búsqueda Avanzada                       | Configuración                                 | Monitorización | Estadísticas | CCN-CERT | MARTA © Innotec System S.L. | Usuario: admin |
|------------------|----------------------------------|-----------------------------------------|-----------------------------------------------|----------------|--------------|----------|-----------------------------|----------------|
| Fecha            | MD5                              | Nombre Fichero                          | Tipo Fichero                                  | Tamaño         | Etiquetas    |          |                             |                |
| 10-08-2015 07:38 | 80cf5091de837e9df7c7129671f52cc  | pwbeyhjkfe.com_cxsonmpcwm.com_80...     | PE32 executable (GUI) Intel 80386, for MS...  | 215 866        |              |          |                             |                |
| 07-08-2015 11:55 | 88af21a3c01004d32c751674bb8eb4e6 | Scattered_Reply.bin                     | PE32 executable (GUI) Intel 80386, for MS...  | 8 016 749      |              |          |                             |                |
| 06-08-2015 07:25 | cba537975d7c42f0939ac34b15c930e  | Tinba malware                           | PE32 executable (GUI) Intel 80386 Mono/.N...  | 193 536        |              |          |                             |                |
| 03-08-2015 08:48 | cc0c51ce339e29344015591c87b7ffe5 | dumpeada.zzz                            | MS-DOS executable, MZ for MS-DOS              | 122 947        |              |          |                             |                |
| 30-07-2015 09:10 | e751a941b7cb8e85b4949cc3e7e39027 | 4ea9d1d436ff23df58bb9116295cae96d8b...  | PE32 executable (GUI) Intel 80386 Mono/.N...  | 240 152        |              |          |                             |                |
| 29-07-2015 11:11 | 89e93a926de9c212a2b148722c938ba3 | 9e4ef2f6b2d1c3d4cc4e25e77c423de406e0... | PE32 executable (GUI) Intel 80386, for MS...  | 273 587        |              |          |                             |                |
| 29-07-2015 08:46 | 9a8b519dd47761731e1a2c086172954  | freematter-output                       | data                                          | 10 597         |              |          |                             |                |
| 29-07-2015 08:15 | cd2d9c7bd5de6d12718785f495ce1bb4 | 1f03d447dee98eb639c4e0956a196ff771c4... | PE32 executable (GUI) Intel 80386, for MS...  | 294 400        |              |          |                             |                |
| 28-07-2015 00:39 | caf7d59508f6ab164c26bc3371c3a1c4 | bot.exe                                 | PE32 executable (console) Intel 80386, for... | 4 530 335      |              |          |                             |                |
| 25-07-2015 21:12 | bc8b42c2689ba8cc08cd6f5abd80cc19 | Google.pdf                              | PDF document, version 1.1                     | 934            |              |          |                             |                |
| 22-07-2015 09:00 | 190fa525529da5d7b0b13408664a9b79 | descarga.exe                            | PE32 executable (console) Intel 80386, for... | 4 564 365      |              |          |                             |                |
| 22-07-2015 08:35 | 6b9253446a9097763d5bfc8afcf3214  | aa0f38344a920bb9e975677f92b0273976f4... | PE32 executable (GUI) Intel 80386 (stripp...  | 102 400        |              |          |                             |                |
| 21-07-2015 13:18 | e2a76b5cfaa321d4c6d20ab0c4560403 | keygen.exe                              | PE32 executable (GUI) Intel 80386, for MS...  | 227 840        |              |          |                             |                |
| 20-07-2015 12:07 | 9be50fe744523a0fee21e0fc16069b1  | 68e8a0868b455dcfae54ee6570a9797d20...   | PE32 executable (console) Intel 80386, for... | 243 200        |              |          |                             |                |
| 20-07-2015 11:13 | edc4c569b2127e5cca7a02572a38fced | f127dbb67867294d044bcaa3bdf751e9c325... | PE32 executable (console) Intel 80386, for... | 593 920        |              |          |                             |                |
| 20-07-2015 11:12 | c1dd1cf756c4d5c66cf0570b1f8c1a5d | def1fae2727c80a2ca69664c27cef64b8982... | PE32 executable (console) Intel 80386, for... | 634 368        |              |          |                             |                |
| 20-07-2015 08:45 | d0455ff313b51ce60e3a7577cf474e1  | f5c716890a2a76785d53e8f9a5db2268501a... | PE32 executable (GUI) Intel 80386, for MS...  | 574 976        |              |          |                             |                |
| 17-07-2015 10:31 | ba6081413faa04fc75d06b95381b74b  | 25f49c7251272edc5c702719897ad1c07727... | PE32 executable (GUI) Intel 80386, for MS...  | 322 592        |              |          |                             |                |
| 17-07-2015 10:31 | f1c4d75a35271897be7795878d75125c | VBoxHook.dll                            | PE32+ executable (DLL) (GUI) x86-64, for...   | 62 240         |              |          |                             |                |
| 16-07-2015 09:00 | 87203a992023612c50f90f5db73d2356 | w0rm.exe                                | PE32 executable (GUI) Intel 80386, for MS...  | 929 792        |              |          |                             |                |

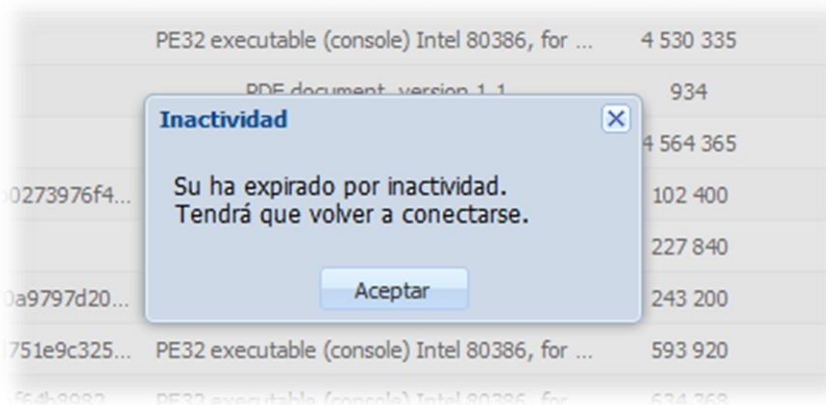
Además, se generará una **sesión**, de forma que no será necesario volver a introducir nuestros credenciales si volvemos a acceder a la aplicación, mientras esta dure, sino que accederemos directamente a la vista principal.

Mientras trabajemos con la aplicación, la sesión no caducará nunca, ya que se irá refrescando de forma automática. En caso de que no interactuemos con la aplicación de ninguna forma, la sesión caducará a los 15 minutos.

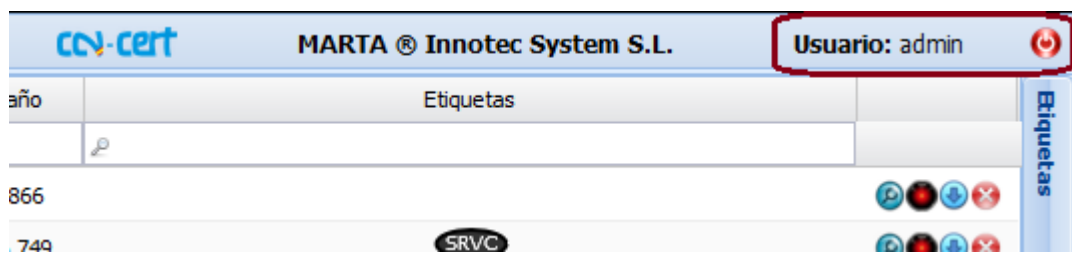
Un minuto antes de que caduque la sesión, se nos mostrará un aviso indicando que la sesión está a punto de caducar por inactividad, y podremos refrescarla:



En caso de no hacerlo, al cabo de un minuto caducará la sesión:



En la esquina superior derecha de la vista principal, podemos ver con qué usuario estamos conectados. Además, disponemos de un **botón para desconectarnos**, que anulará nuestra sesión inmediatamente:



Por seguridad, se recomienda utilizar este botón una vez hayamos terminado de utilizar la aplicación en lugar de cerrar la pestaña del navegador, aunque en caso de no hacerlo, la sesión caducará por si misma al cabo de 15 minutos.

## 4 VISTA PRINCIPAL

Esta es la vista que se muestra una vez introducidos los credenciales de acceso:

| <div> <div> <div></div> <div></div> <div></div> <div></div> <div></div> <div></div> </div> <div> <div>ccn-cert</div> <div>MARTA © Innotec System S.L.</div> <div>Usuario: admin</div> </div> </div> |                                  |                                          |                                                |           |               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------------------|------------------------------------------------|-----------|---------------|
| Fecha                                                                                                                                                                                               | MD5                              | Nombre Fichero                           | Tipo Fichero                                   | Tamaño    | Etiquetas     |
| 10-08-2015 07:38                                                                                                                                                                                    | 80cfd5091de837e9df7c7129671f52cc | privbeyhjkfe.com_cxoponmpcwnm.com_80...  | PE32 executable (GUI) Intel 80386, for MS ...  | 215 866   |               |
| 07-08-2015 11:55                                                                                                                                                                                    | 88af21a3c01004d32c751674bb8eb4e6 | Scattered_Reply.bin                      | PE32 executable (GUI) Intel 80386, for MS ...  | 8 016 749 | SRVC          |
| 06-08-2015 07:25                                                                                                                                                                                    | c8a53797f5d7c42f939ac34b15c930e  | Tirba malware                            | PE32 executable (GUI) Intel 80386 Mono/N...    | 193 536   |               |
| 03-08-2015 08:48                                                                                                                                                                                    | cc0c51ce339a29344015591c87b7dfe5 | dumpeada.zzz                             | MS-DOS executable, MZ for MS-DOS               | 122 947   |               |
| 30-07-2015 09:10                                                                                                                                                                                    | e751a941b7cb8e85b4949cc3e7e39027 | 4eaf9d1d436ff23df58bb9116295cae96d8b...  | PE32 executable (GUI) Intel 80386 Mono/N...    | 240 152   |               |
| 29-07-2015 11:11                                                                                                                                                                                    | 89e93a926de9c212a2b148722c938ba3 | 9e4ef2f6b2d1c3d4cc4e25e77c423de406e0...  | PE32 executable (GUI) Intel 80386, for MS ...  | 273 587   | SRVC IEZM     |
| 29-07-2015 08:46                                                                                                                                                                                    | 9a8b519dd47f671731e1a2c086172954 | freeformatter-output                     | data                                           | 10 997    |               |
| 29-07-2015 08:15                                                                                                                                                                                    | cd2d9c7bd5de6d12718785f495ce1bb4 | 1f03d447dee98eb639c4e095ea19bfff771c4... | PE32 executable (GUI) Intel 80386, for MS ...  | 294 400   | BOOT IEZM WPE |
| 28-07-2015 00:39                                                                                                                                                                                    | caf7d59508fab164c28bc3371c3a1c4  | bot.exe                                  | PE32 executable (console) Intel 80386, for ... | 4 530 335 |               |
| 25-07-2015 11:12                                                                                                                                                                                    | bcb842c2689ba8cc08cd6f5ab80cc19  | Google.pdf                               | PDF document, version 1.1                      | 934       | SRVC IEZM WPE |
| 22-07-2015 09:00                                                                                                                                                                                    | 190fa525529da5d7b0b13408664a9b79 | descarga.exe                             | PE32 executable (console) Intel 80386, for ... | 4 564 365 | SRVC WPE      |
| 22-07-2015 08:35                                                                                                                                                                                    | 6b92534460a907763d5bfcd8afc3214  | aa0f38344a920bb9e97567792b0273976f4...   | PE32 executable (GUI) Intel 80386 (stripte...  | 102 400   | SRVC WPE      |
| 21-07-2015 13:18                                                                                                                                                                                    | e2a7b5cf3a321d46d2d0ab0c4560403  | keygen.exe                               | PE32 executable (GUI) Intel 80386, for MS ...  | 227 840   |               |
| 20-07-2015 12:07                                                                                                                                                                                    | 9be50fe744523a0fee21e0f6c16069b1 | 68e8a0868b455dce6ae54ee6570a9797d20...   | PE32 executable (console) Intel 80386, for ... | 243 200   | SRVC WPE      |
| 20-07-2015 11:13                                                                                                                                                                                    | edb4c569b212765cca7a0257a38fced  | f127dbb6786729d40d4bcaa3bf751e9c325...   | PE32 executable (console) Intel 80386, for ... | 593 920   | SRVC          |
| 20-07-2015 11:12                                                                                                                                                                                    | c1dd1cf756c4d5c66cf0570b1f8c1a5d | def1fae2727c80a2ca69664c27cefb4b8982...  | PE32 executable (console) Intel 80386, for ... | 634 368   | SRVC          |
| 20-07-2015 08:45                                                                                                                                                                                    | d04f55f313b51ce60e3a7577cf474e1  | f5c716890a2a76785d53e8f9a5db2268501a...  | PE32 executable (GUI) Intel 80386, for MS ...  | 574 976   | SRVC WPE      |
| 17-07-2015 10:31                                                                                                                                                                                    | ba6081413faa04fc75d06b95381b74b  | 25f49c7251272edc5c702719897ad1c07727...  | PE32 executable (GUI) Intel 80386, for MS ...  | 322 592   | SRVC IEZM     |
| 17-07-2015 10:31                                                                                                                                                                                    | f1c4d75a35271897be7795878d75125c | VBoxHook.dll                             | PE32+ executable (DLL) (GUI) x86-64, for ...   | 62 240    |               |
| 16-07-2015 09:00                                                                                                                                                                                    | 87203e992023612c50f90fdb73d2356  | worm.exe                                 | PE32 executable (GUI) Intel 80386, for MS ...  | 929 792   |               |

Consta de 6 pestañas:

-  **Binarios:** Muestra una lista con todos los ficheros subidos a MARTA. Permite hacer filtros rápidos sobre los ficheros, ver sus detalles (incluyendo los datos extraídos por los scripts estáticos), crear análisis dinámicos y subir ficheros nuevos.
-  **Análisis:** Muestra una lista con todos los análisis de ficheros realizados. Permite hacer filtros rápidos sobre los análisis, ver sus detalles (incluyendo todos los datos extraídos por la sandbox), y también crear reanálisis y subir ficheros nuevos.
-  **Búsqueda Avanzada:** Permite hacer búsquedas de binarios que cumplan una serie de directrices, entre una gran cantidad de posibilidades, como tamaño del malware, técnicas anti detección, ficheros afectados por el malware, conexiones de red, procesos creados, etc.
-  **Configuración:** Permite la gestión de Reglas, Fuentes, Organismos y Usuarios de la aplicación.
-  **Monitorización:** Proporciona información sobre el estado de las sandbox y los subprocesos utilizados por la aplicación, de forma que, de producirse un fallo en alguno de los componentes, podría detectarse rápidamente.

-  **Estadísticas:** Proporciona información visual a través de gráficas sobre estadísticas interesantes del uso de la aplicación, como los tipos de binarios más comunes, las etiquetas más utilizadas, o la cantidad de binarios subidos en los últimos 30 días.

## 5 PESTAÑA DE BINARIOS

Esta pestaña está diseñada para facilitar todas las gestiones relativas a los ficheros subidos a MARTA.

| MARTA © Innotec System S.L. Usuario: admin |                                   |                                         |                                                |                |               |  |
|--------------------------------------------|-----------------------------------|-----------------------------------------|------------------------------------------------|----------------|---------------|--|
| Binarios                                   | Análisis                          | Búsqueda Avanzada                       | Configuración                                  | Monitorización | Estadísticas  |  |
| Fecha                                      | MD5                               | Nombre Fichero                          | Tipo Fichero                                   | Tamaño         | Etiquetas     |  |
| 10-08-2015 07:38                           | 80cfd5091de837e9df7c7129671f52cc  | pwbbehyjfe.com_cxoponmpcwmn.com_80...   | PE32 executable (GUI) Intel 80386, for MS ...  | 215 866        |               |  |
| 07-08-2015 11:55                           | 88af21a3c01004d32c751674bb8eb4e6  | Scattered_Reply.bin                     | PE32 executable (GUI) Intel 80386, for MS ...  | 8 016 749      | SRVC          |  |
| 06-08-2015 07:25                           | c8a53797f5d7c42fd939ac34b15c930e  | Trinba malware                          | PE32 executable (GUI) Intel 80386 Mono/N...    | 193 536        |               |  |
| 03-08-2015 08:48                           | cc0c51ce339a29344015591c87b7dfe5  | dumpeada.zzz                            | MS-DOS executable, MZ for MS-DOS               | 122 947        |               |  |
| 30-07-2015 09:10                           | e751a941b7c8e85b4949cc3e7e39027   | 4eaf9d1d436f723df58bb9116295cae96d8b... | PE32 executable (GUI) Intel 80386 Mono/N...    | 240 152        |               |  |
| 29-07-2015 11:11                           | 89e93a926de9c212a2b148722c938ba3  | 9e4ef2f6b2d1c3d4cc4e25e77c423de406e0... | PE32 executable (GUI) Intel 80386, for MS ...  | 273 587        | SRVC IEZM     |  |
| 29-07-2015 08:46                           | 9a8b519d447f671731e1a2c086172554  | freematter-output                       | data                                           | 10 597         |               |  |
| 29-07-2015 08:15                           | cd2d9c7bd5de6d12718785f495ce1bb4  | 1f03d447dee98eb639c4e0956a19bf7771c4... | PE32 executable (GUI) Intel 80386, for MS ...  | 294 400        | BOOT IEZM WPE |  |
| 28-07-2015 00:39                           | ca7d59508f6ab164c26bc3371c3a1c4   | bot.exe                                 | PE32 executable (console) Intel 80386, for ... | 4 530 335      |               |  |
| 25-07-2015 21:12                           | bc8b42c2689b8acc08cdf5abd80cc19   | Google.pdf                              | PDF document, version 1.1                      | 934            | SRVC IEZM WPE |  |
| 22-07-2015 09:00                           | 190fa525529da5d7b0b13408664e9b79  | descarga.exe                            | PE32 executable (console) Intel 80386, for ... | 4 564 365      | SRVC WPE      |  |
| 22-07-2015 08:35                           | 6b92534460a9097763d5bdc8afcc3214  | aa0f38344a920bb9e975677920273976f4...   | PE32 executable (GUI) Intel 80386 (stripte...  | 102 400        | SRVC WPE      |  |
| 21-07-2015 13:18                           | e2a76b5cfaa321d4c6d20ab0c4560403  | keygen.exe                              | PE32 executable (GUI) Intel 80386, for MS ...  | 227 840        |               |  |
| 20-07-2015 12:07                           | 9be507fe744523a0fee21e0f6c16069b1 | 68e8a0868b455dce6ae54ee5570a9797d20...  | PE32 executable (console) Intel 80386, for ... | 243 200        | SRVC WPE      |  |
| 20-07-2015 11:13                           | edb4c569b2127e5cca7a02572a38fced  | f127dbb6786729d40d4bcaa3bf751e9c325...  | PE32 executable (console) Intel 80386, for ... | 593 920        | SRVC          |  |
| 20-07-2015 11:12                           | c1dd1c7f56c4d5c66cf050b1f8c1a5d   | def1fae2727c80a2ca96664c27cef54b8982... | PE32 executable (console) Intel 80386, for ... | 634 368        | SRVC          |  |
| 20-07-2015 08:45                           | d04f5ff313b51ce60e3a757cf474e1    | f5c716890a2a76785d53e8f9a5db2268501a... | PE32 executable (GUI) Intel 80386, for MS ...  | 574 976        | SRVC WPE      |  |
| 17-07-2015 10:31                           | ba6081413faa04f4c75d06b95381b74b  | 25f49c7251272edc5c702719897ad1c07727... | PE32 executable (GUI) Intel 80386, for MS ...  | 322 592        | SRVC IEZM     |  |
| 17-07-2015 10:31                           | f1c4d75a35271897be779587d75125c   | VBoxHook.dll                            | PE32+ executable (DLL) (GUI) x86-64, for ...   | 62 240         |               |  |
| 16-07-2015 09:00                           | 87203a992023612c50f0fdd73d2356    | w0rm.exe                                | PE32 executable (GUI) Intel 80386, for MS ...  | 929 792        |               |  |

### 5.1 LISTADO

La pestaña muestra una **lista** a modo de resumen con **todos los ficheros** subidos a MARTA. Dado que el caso más común es que se suba una gran cantidad de binarios a la aplicación, la lista está paginada, por defecto a 20 binarios por página, y ordenada por fecha de subida del fichero, de más reciente a menos reciente. La barra de herramientas de la parte inferior de la pestaña permite cambiar entre las páginas y elegir el número de binarios que se desea mostrar por página.

En la tabla se muestran los **atributos** más significativos de cada fichero: la fecha en la que se subió, su MD5, su nombre, su tipo de fichero, su tamaño y sus etiquetas asociadas. Es posible **filtrar** por cualquiera de estos campos con los cuadros de filtro de cada una de las columnas:

| MARTA © Innotec System S.L. Usuario: admin |                                  |                                         |                                               |                |               |  |
|--------------------------------------------|----------------------------------|-----------------------------------------|-----------------------------------------------|----------------|---------------|--|
| Binarios                                   | Análisis                         | Búsqueda Avanzada                       | Configuración                                 | Monitorización | Estadísticas  |  |
| Fecha                                      | MD5                              | Nombre Fichero                          | Tipo Fichero                                  | Tamaño         | Etiquetas     |  |
| 29-07-2015                                 |                                  |                                         | exe                                           |                |               |  |
| 29-07-2015 11:11                           | 89e93a926de9c212a2b148722c938ba3 | 9e4ef2f6b2d1c3d4cc4e25e77c423de406e0... | PE32 executable (GUI) Intel 80386, for MS ... | 273 587        | SRVC IEZM     |  |
| 29-07-2015 08:15                           | cd2d9c7bd5de6d12718785f495ce1bb4 | 1f03d447dee98eb639c4e0956a19bf7771c4... | PE32 executable (GUI) Intel 80386, for MS ... | 294 400        | BOOT IEZM WPE |  |

En esta lista, y en todas las listas de la aplicación, es posible hacer doble clic en uno de los campos para acceder a su información y poder copiarla (esto no permite modificar la información, sólo copiarla):

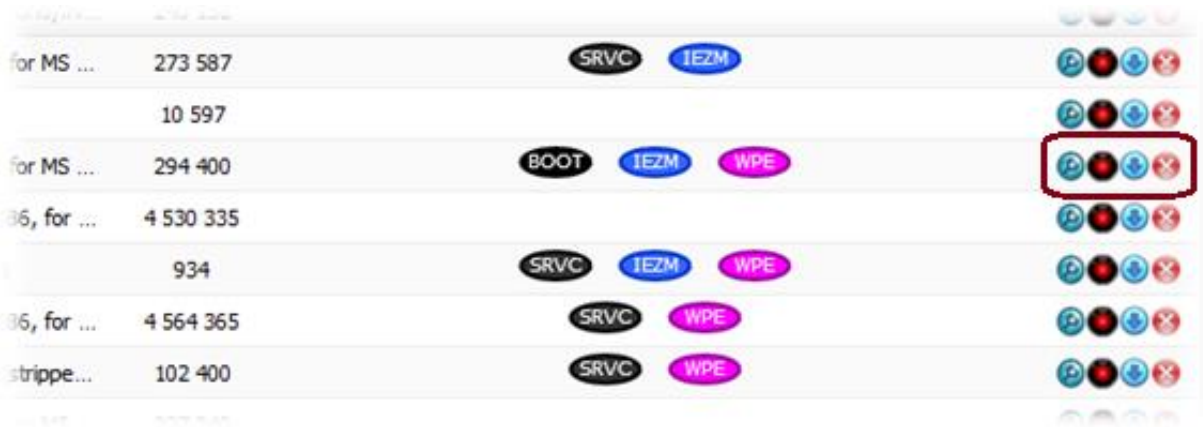
| Fecha            | MD5                              | Nombre Fichero                          | Tipo Fichero                                   | Tamaño    | Etiquetas     |  |
|------------------|----------------------------------|-----------------------------------------|------------------------------------------------|-----------|---------------|--|
| 10-08-2015 07:38 | 80cfd5091de837e9df7c7129671f52cc | pxibbeyhjkfe.com_cxoponmpovnm.com_80... | PE32 executable (GUI) Intel 80386, for MS...   | 215 866   |               |  |
| 07-08-2015 11:55 | 88af21a3c01004d32c751674bb8eb4e6 | Scattered_Reply.bin                     | PE32 executable (GUI) Intel 80386, for MS...   | 8 016 749 | SRVC          |  |
| 06-08-2015 07:25 | c8a537975d7c42fd939ac34b15c930e  | Tinba malware                           | PE32 executable (GUI) Intel 80386 Mono/N...    | 193 536   |               |  |
| 03-08-2015 08:48 | cc0c51ce339a29344015591c87b7df5e | dumpeada.zzz                            | MS-DOS executable, MZ for MS-DOS               | 122 947   |               |  |
| 30-07-2015 09:10 | e751e941b7cb8e85b4949cc3e7e39027 | 4eaf9d1d436ff23df58bb9116295cae96d8b... | PE32 executable (GUI) Intel 80386 Mono/N...    | 240 152   |               |  |
| 29-07-2015 11:11 | 89e93a926de9c212a2b148722c938ba3 | 9e4ef2f6b2d1c3d4cc4e25e77c423de406e0... | PE32 executable (GUI) Intel 80386, for MS...   | 273 587   | SRVC IEZM     |  |
| 29-07-2015 08:46 | 9a8b519dd47671731e1a2c086172954  | freematter-output                       | data                                           | 10 597    |               |  |
| 29-07-2015 08:15 | cd2d9c7bd5de6d12718785f495ce1bb4 | 1f03d447dee98eb639c4e0956a19eff771c4    | PE32 executable (GUI) Intel 80386, for MS...   | 294 400   | BOOT IEZM WPE |  |
| 28-07-2015 00:39 | caf7d59908fab164c26bc3371c3a1c4  | bot.exe                                 | PE32 executable (console) Intel 80386, for ... | 4 530 335 |               |  |
| 25-07-2015 21:12 | bc8b42c2689ba8cc08c6f5abdb80cc19 | Google.pdf                              | PDF document, version 1.1                      | 934       | SRVC IEZM WPE |  |
| 22-07-2015 09:00 | 190fa525529da5d70b13408664e9b79  | descarga.exe                            | PE32 executable (console) Intel 80386, for ... | 4 564 365 | SRVC WPE      |  |
| 22-07-2015 08:35 | 6b92534460a9097763d5bdc8af3214   | aa0f38344a920bb9e975677f92b0273976f4    | PE32 executable (GUI) Intel 80386 (stripp...   | 102 400   | SRVC WPE      |  |
| 21-07-2015 13:18 | e2a7b65cfaa321d4c6d20ab0c4560403 | keygen.exe                              | PE32 executable (GUI) Intel 80386, for MS...   | 227 840   |               |  |
| 20-07-2015 12:07 | 9be50fe744523a0fee21e0f6c16069b1 | 68e8a0868b455dce6ae54ee6570a9797d20...  | PE32 executable (console) Intel 80386, for ... | 243 200   | SRVC WPE      |  |
| 20-07-2015 11:13 | edb4c569b2127e5cca7a02572a38fed  | f127dbb6786729d40d4bca3bdf751e9c325     | PE32 executable (console) Intel 80386, for ... | 593 920   | SRVC          |  |
| 20-07-2015 11:12 | c1dd1cf756c4dc6c6f0570b1f8c1a5d  | def1fae2727c80a2ca69664c27cef64b8982... | PE32 executable (console) Intel 80386, for ... | 634 368   | SRVC          |  |
| 20-07-2015 08:45 | d04f55f313b51ce60e3a7577c474e1   | f5c716890a2a76785d53e8f9a5db2268501a    | PE32 executable (GUI) Intel 80386, for MS...   | 574 976   | SRVC WPE      |  |
| 17-07-2015 10:31 | ba6081413faa04fc75d06b95381b74b  | 25f49c7251272edc5c702719897ad1c07727... | PE32 executable (GUI) Intel 80386, for MS...   | 322 592   | SRVC IEZM     |  |
| 17-07-2015 10:31 | f1c4d75a35271897be7795878d75125c | VBoxHook.dll                            | PE32+ executable (DLL) (GUI) x86-64, for ...   | 62 240    |               |  |
| 16-07-2015 09:00 | 87203a992023612c50f90fdd673d2356 | w0rm.exe                                | PE32 executable (GUI) Intel 80386, for MS...   | 929 792   |               |  |

Además, si se mantiene el cursor del ratón sobre un campo, aparece un panel de ayuda con la información del campo:

| Fecha            | MD5                              | Nombre Fichero                          | Tipo Fichero                                   | Tamaño    | Etiquetas                                                                                       |  |
|------------------|----------------------------------|-----------------------------------------|------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------|--|
| 10-08-2015 07:38 | 80cfd5091de837e9df7c7129671f52cc | pxibbeyhjkfe.com_cxoponmpovnm.com_80... | PE32 executable (GUI) Intel 80386, for MS...   | 215 866   |                                                                                                 |  |
| 07-08-2015 11:55 | 88af21a3c01004d32c751674bb8eb4e6 | Scattered_Reply.bin                     | PE32 executable (GUI) Intel 80386, for MS...   | 8 016 749 | SRVC                                                                                            |  |
| 06-08-2015 07:25 | c8a537975d7c42fd939ac34b15c930e  | Tinba malware                           | PE32 executable (GUI) Intel 80386 Mono/N...    | 193 536   |                                                                                                 |  |
| 03-08-2015 08:48 | cc0c51ce339a29344015591c87b7df5e | dumpeada.zzz                            | MS-DOS executable, MZ for MS-DOS               | 122 947   |                                                                                                 |  |
| 30-07-2015 09:10 | e751e941b7cb8e85b4949cc3e7e39027 | 4eaf9d1d436ff23df58bb9116295cae96d8b... | PE32 executable (GUI) Intel 80386 Mono/N...    | 240 152   |                                                                                                 |  |
| 29-07-2015 11:11 | 89e93a926de9c212a2b148722c938ba3 | 9e4ef2f6b2d1c3d4cc4e25e77c423de406e0... | PE32 executable (GUI) Intel 80386, for MS...   | 273 587   | SRVC IEZM                                                                                       |  |
| 29-07-2015 08:46 | 9a8b519dd47671731e1a2c086172954  | freematter-output                       | data                                           | 10 597    |                                                                                                 |  |
| 29-07-2015 08:15 | cd2d9c7bd5de6d12718785f495ce1bb4 | 1f03d447dee98eb639c4e0956a19eff771c4    | PE32 executable (GUI) Intel 80386, for MS...   | 294 400   | BOOT IEZM WPE                                                                                   |  |
| 28-07-2015 00:39 | caf7d59908fab164c26bc3371c3a1c4  | bot.exe                                 | PE32 executable (console) Intel 80386, for ... | 4 530 335 |                                                                                                 |  |
| 25-07-2015 21:12 | bc8b42c2689ba8cc08c6f5abdb80cc19 | Google.pdf                              | PDF document, version 1.1                      | 934       | Etiquetas:<br>BOOT Boot Survival<br>IEZM Internet Explorer Zone Map<br>WPE Creación Ejecutables |  |
| 22-07-2015 09:00 | 190fa525529da5d70b13408664e9b79  | descarga.exe                            | PE32 executable (console) Intel 80386, for ... | 4 564 365 |                                                                                                 |  |
| 22-07-2015 08:35 | 6b92534460a9097763d5bdc8af3214   | aa0f38344a920bb9e975677f92b0273976f4    | PE32 executable (GUI) Intel 80386 (stripp...   | 102 400   |                                                                                                 |  |
| 21-07-2015 13:18 | e2a7b65cfaa321d4c6d20ab0c4560403 | keygen.exe                              | PE32 executable (GUI) Intel 80386, for MS...   | 227 840   |                                                                                                 |  |
| 20-07-2015 12:07 | 9be50fe744523a0fee21e0f6c16069b1 | 68e8a0868b455dce6ae54ee6570a9797d20...  | PE32 executable (console) Intel 80386, for ... | 243 200   | SRVC WPE                                                                                        |  |
| 20-07-2015 11:13 | edb4c569b2127e5cca7a02572a38fed  | f127dbb6786729d40d4bca3bdf751e9c325     | PE32 executable (console) Intel 80386, for ... | 593 920   | SRVC                                                                                            |  |
| 20-07-2015 11:12 | c1dd1cf756c4dc6c6f0570b1f8c1a5d  | def1fae2727c80a2ca69664c27cef64b8982... | PE32 executable (console) Intel 80386, for ... | 634 368   | SRVC                                                                                            |  |
| 20-07-2015 08:45 | d04f55f313b51ce60e3a7577c474e1   | f5c716890a2a76785d53e8f9a5db2268501a    | PE32 executable (GUI) Intel 80386, for MS...   | 574 976   | SRVC WPE                                                                                        |  |
| 17-07-2015 10:31 | ba6081413faa04fc75d06b95381b74b  | 25f49c7251272edc5c702719897ad1c07727... | PE32 executable (GUI) Intel 80386, for MS...   | 322 592   | SRVC IEZM                                                                                       |  |
| 17-07-2015 10:31 | f1c4d75a35271897be7795878d75125c | VBoxHook.dll                            | PE32+ executable (DLL) (GUI) x86-64, for ...   | 62 240    |                                                                                                 |  |
| 16-07-2015 09:00 | 87203a992023612c50f90fdd673d2356 | w0rm.exe                                | PE32 executable (GUI) Intel 80386, for MS...   | 929 792   |                                                                                                 |  |

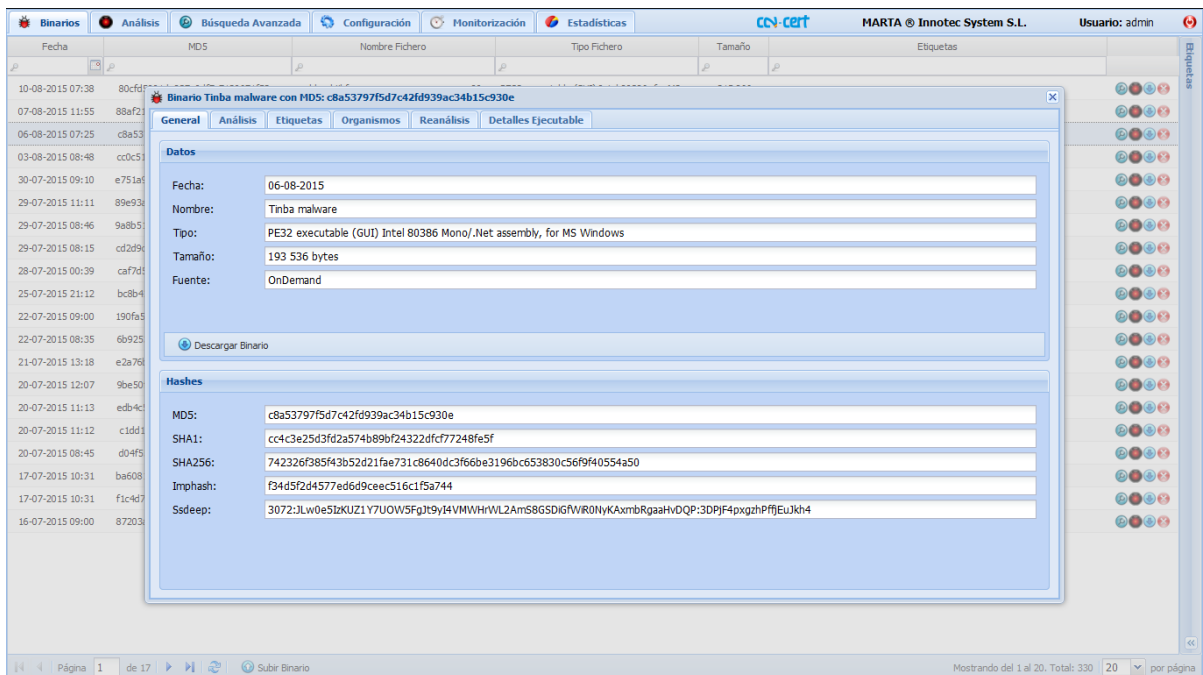
## 5.2 ACCIONES SOBRE LOS FICHEROS

La última columna de la lista de ficheros es de **acciones**:

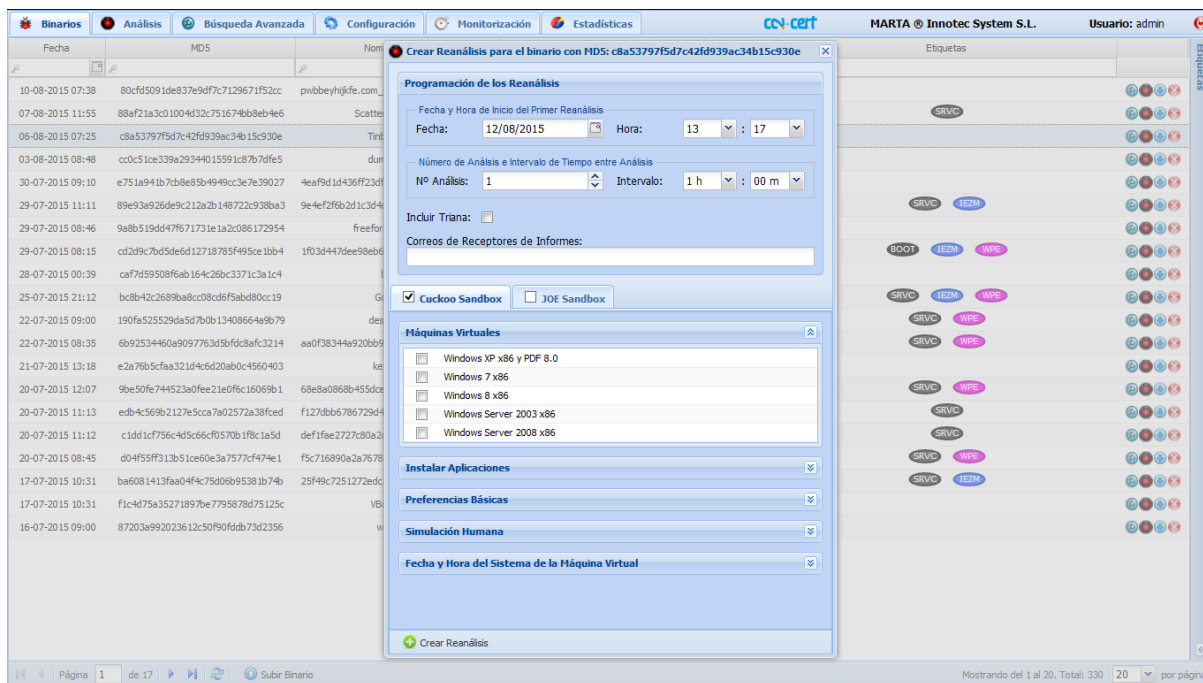


Permite realizar las siguientes gestiones sobre un fichero:

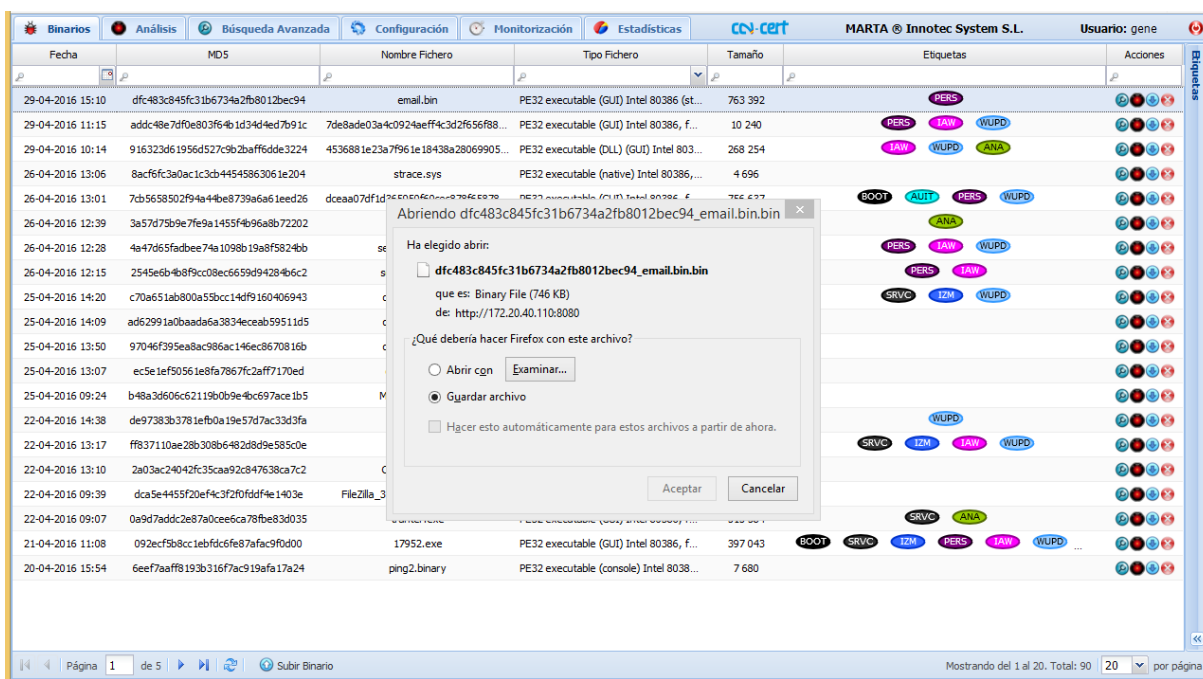
-  **Ver Detalle:** Abre la vista de detalles del fichero seleccionado. Esta vista contiene toda la información relativa a un fichero. Se describe en la sección [Vista de Detalle de un Binario](#) de este documento.



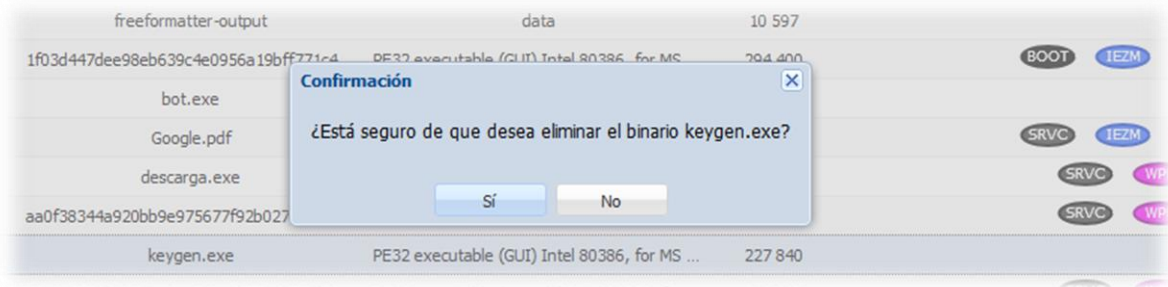
-  **Reanalizar Binario:** Abre la vista de reanálisis del fichero seleccionado. Esta vista permite lanzar o programar uno o varios análisis dinámicos de un fichero. Se describe en la sección [Vista de Reanálisis de un Binario](#) de este documento.



-  **Descargar Binario:** Descarga el fichero seleccionado. Esta acción debe realizarse con precaución ya que el fichero descargado podría ser un malware. El fichero se descarga con un nombre que está compuesto por el MD5 del fichero más el nombre de la muestra con su extensión y se le da extensión bin para evitar que lo ejecutemos por error al descargarlo.



-  **Eliminar:** Elimina el fichero seleccionado, y todos sus análisis. Pide confirmación antes de eliminar.



Todas estas acciones también pueden realizarse utilizando el botón derecho del ratón sobre un fichero de la lista. Esta opción está disponible en todas las listas con columna de acciones de la aplicación.



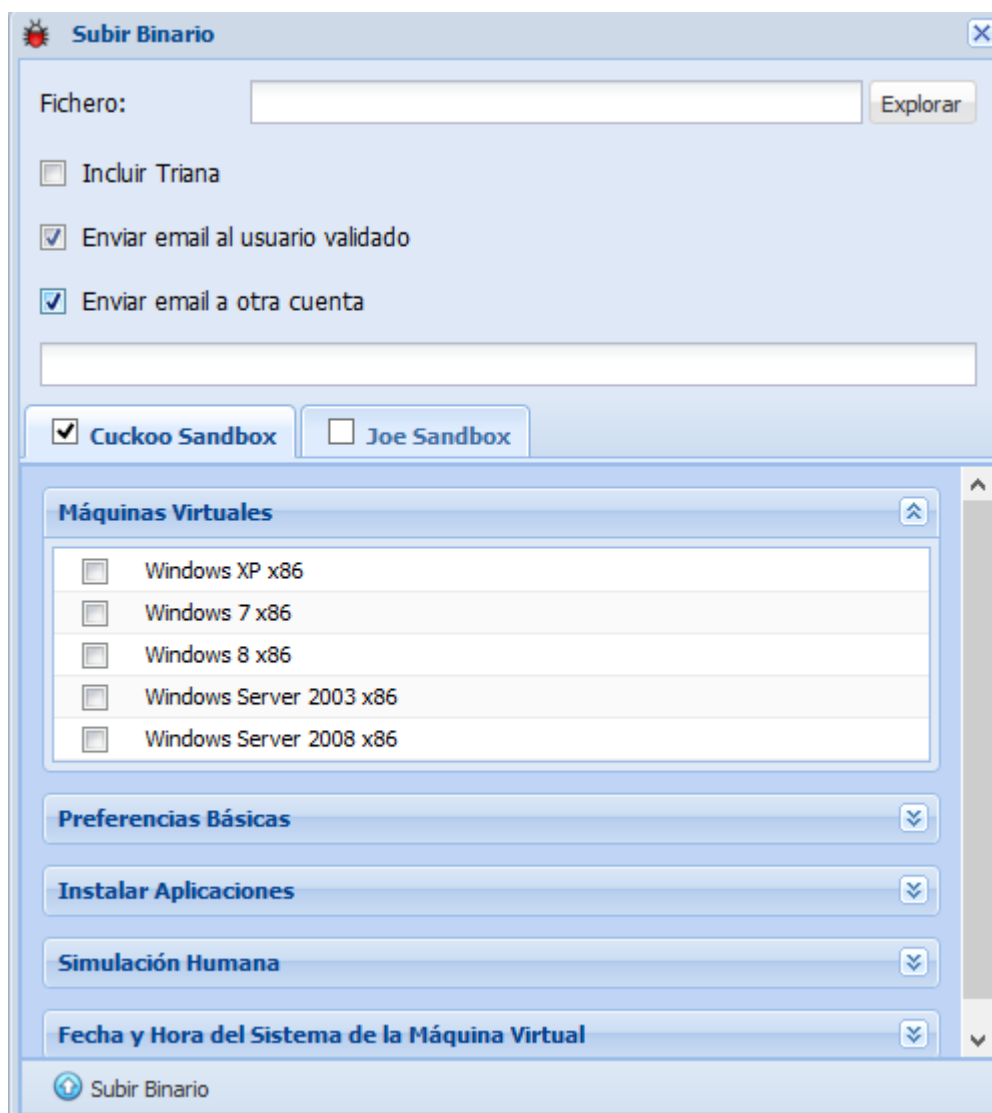
### 5.3 ACCIONES GENERALES

En la barra de herramientas de la parte inferior de la pestaña, hay botones que permiten realizar **gestiones** que no están directamente ligadas a un fichero:



En esta pestaña sólo hay una:

-  **Subir Binario:** Abre la vista de subida de un fichero. Esta vista permite subir un fichero nuevo a MARTA y hacerle uno o varios análisis dinámicos directamente. Se describe en la sección [Vista de Subida de un Binario](#) de este documento.



Fichero: elegimos el fichero que queremos analizar.

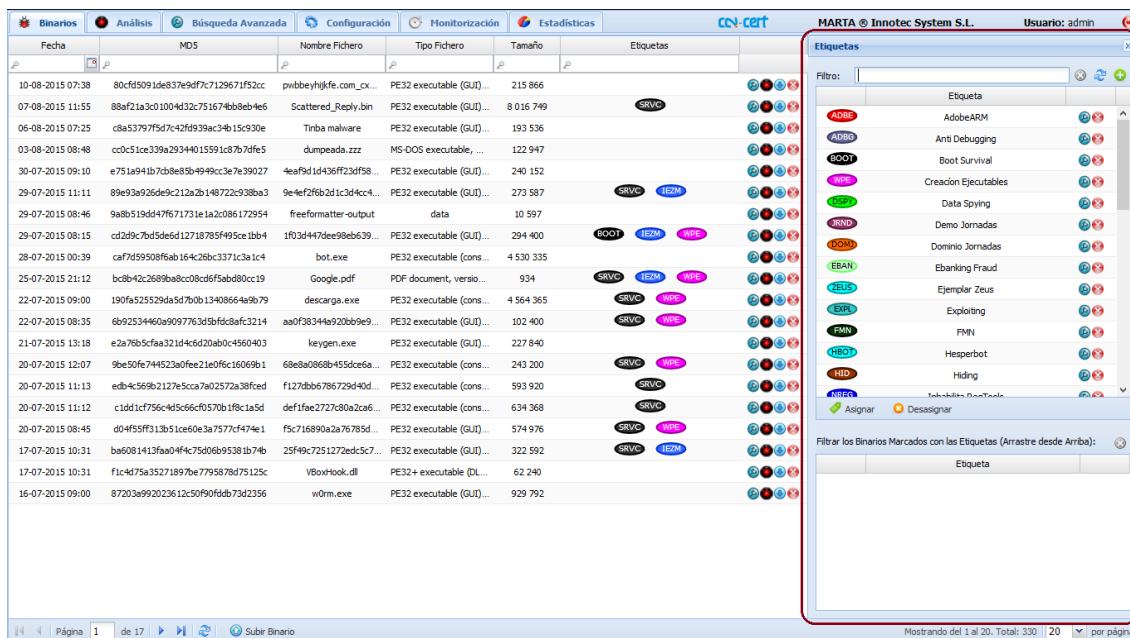
Incluir Triana: Si incluimos Triana analiza el fichero y cuando descarguemos el informe nos aparecerá una opción que será Triana.

Enviar email al usuario validado: Enviara un mail cuando solicitamos el análisis y otro mail cuando termine el análisis.

Enviar mail a otra cuenta: Rellenamos el mail a la cuenta que queremos enviarle nuestra subida de binario.

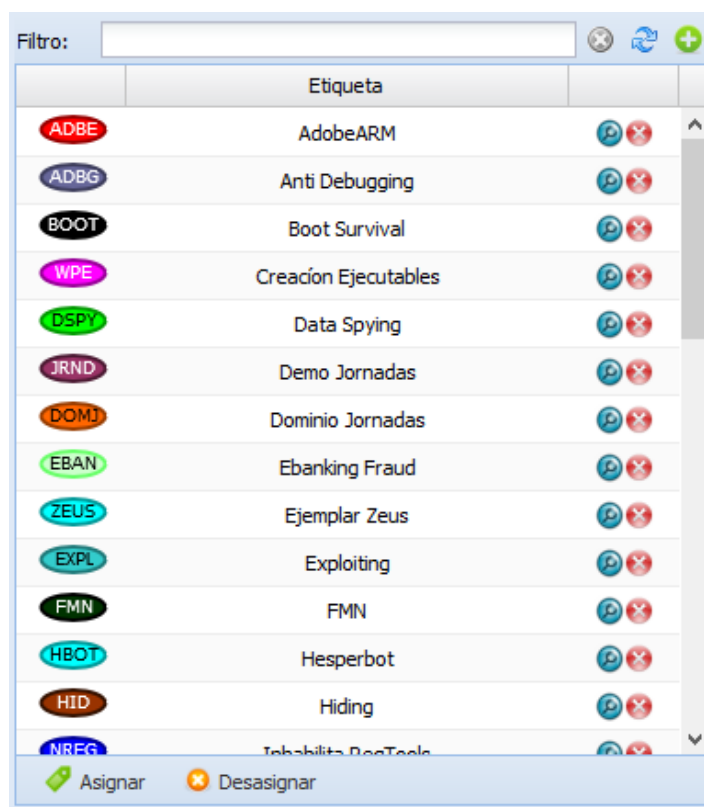
## 5.4 ETIQUETAS

En la parte derecha de la pestaña, hay un panel desplegable (puede abrirse o colapsarse clicando en el título del panel o en el botón de despliegue) que permite hacer **gestiones con las etiquetas** asociadas a los ficheros:



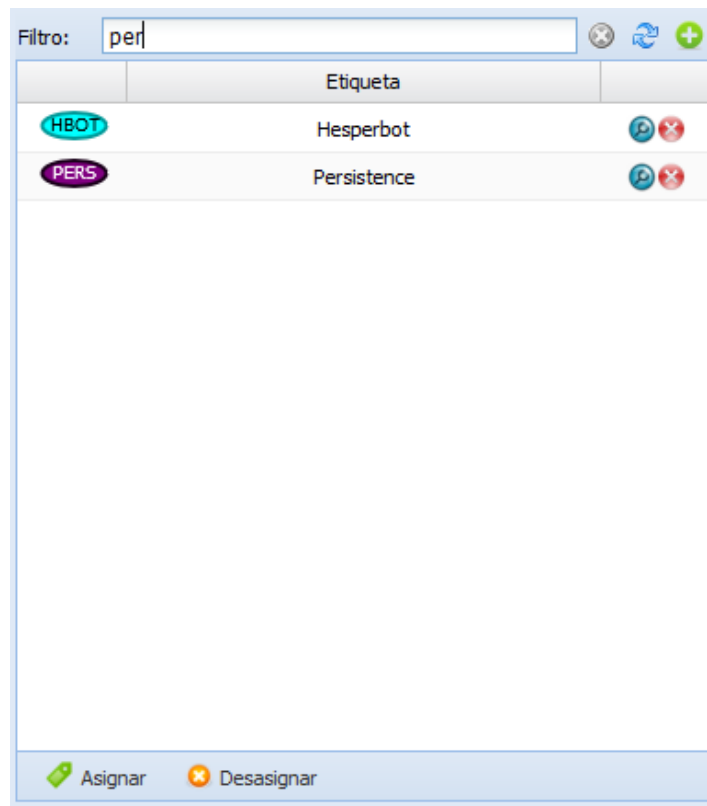
The screenshot shows the MARTA application interface. The main window displays a table of files with columns for Fecha, MD5, Nombre Fichero, Tipo Fichero, Tamaño, and Etiquetas. The right sidebar is open, showing the 'Etiquetas' panel. This panel contains a list of tags with their corresponding icons and a search filter. The tags listed are: ADBE (AdobeARM), ADBG (Anti Debugging), BOOT (Boot Survival), WPE (Creación Ejecutables), DSPY (Data Spying), JRND (Demo Jornadas), DOMI (Dominio Jornadas), EBAN (Ebanking Fraud), ZEUS (Ejemplar Zeus), EXPL (Exploiting), FMN (FMN), HBOT (Hesperbot), HID (Hiding), and NREG (Inhabilita RootTools). At the bottom of the sidebar, there are buttons for 'Asignar' (Assign) and 'Desasignar' (Unassign).

El panel está compuesto por dos listas. En la **lista superior**, podemos ver todas las **etiquetas existentes** en MARTA:



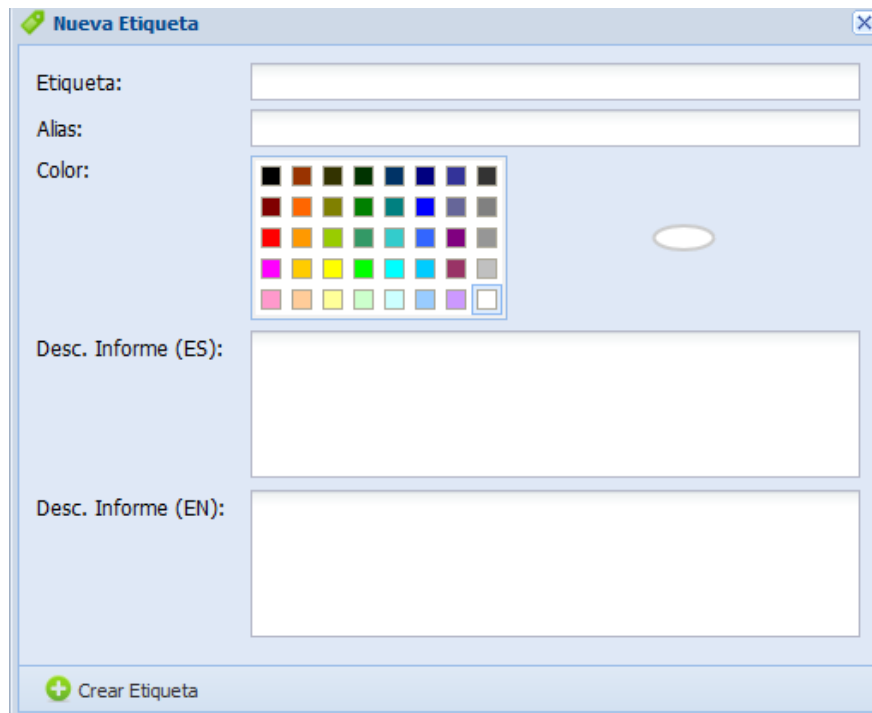
This image is a close-up of the 'Etiquetas' panel. It features a search filter at the top and a list of tags below. Each tag consists of a colored icon, the tag name, and a small circular button with a plus or minus sign. The tags are: ADBE (AdobeARM), ADBG (Anti Debugging), BOOT (Boot Survival), WPE (Creación Ejecutables), DSPY (Data Spying), JRND (Demo Jornadas), DOMI (Dominio Jornadas), EBAN (Ebanking Fraud), ZEUS (Ejemplar Zeus), EXPL (Exploiting), FMN (FMN), HBOT (Hesperbot), HID (Hiding), and NREG (Inhabilita RootTools). At the bottom, there are buttons for 'Asignar' (Assign) and 'Desasignar' (Unassign).

Podemos filtrarlas con el cuadro de texto de filtro:



Hay tres botones a la derecha de este cuadro de texto:

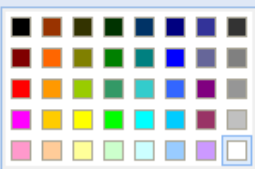
-  **Borrar Filtro:** Limpia el cuadro de texto de filtro, y muestra la lista de etiquetas sin filtrar.
-  **Recargar:** Recarga la lista de etiquetas.
-  **Agregar Etiqueta:** Abre la ventana de creación de etiquetas. Esta ventana permite crear una etiqueta nueva.



**Nueva Etiqueta**

Etiqueta:

Alias:

Color: 

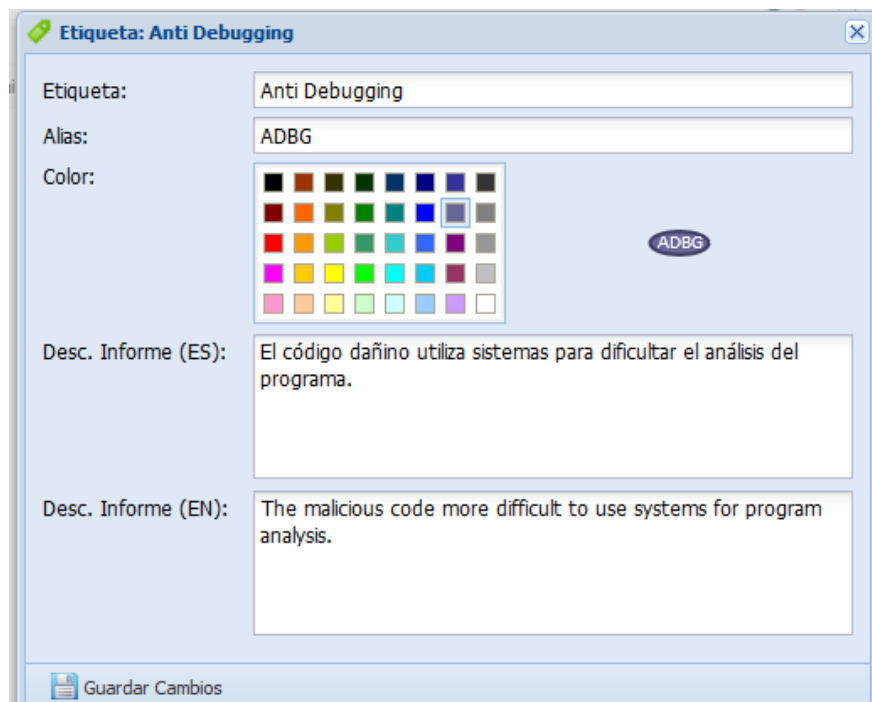
Desc. Informe (ES):

Desc. Informe (EN):



 Crear Etiqueta

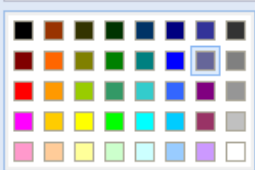
Basta con elegir un nombre para la etiqueta, un alias de hasta 4 letras, un color y el texto (tanto en español como en inglés) que va a aparecer en el informe cuando el análisis tenga la etiqueta asociada. Se generará automáticamente un icono con forma de óvalo del color elegido y con el alias escrito dentro:



**Etiqueta: Anti Debugging**

Etiqueta:

Alias:

Color: 

Desc. Informe (ES):

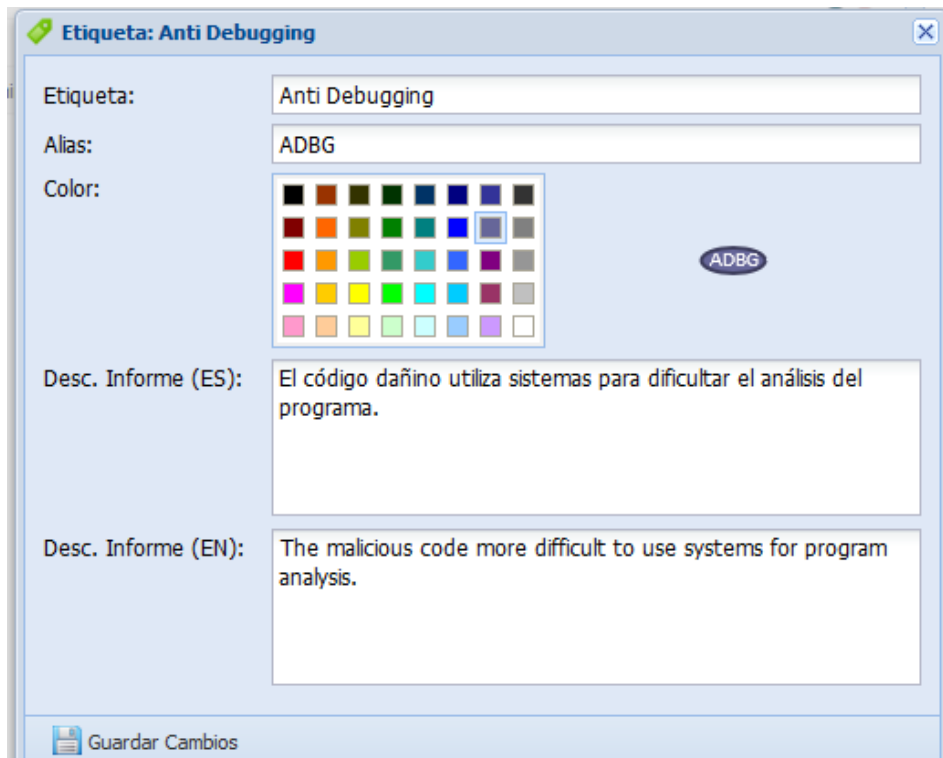
Desc. Informe (EN):



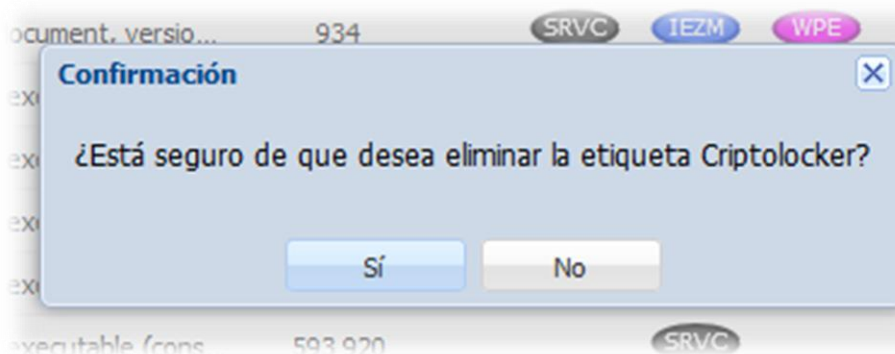
 Guardar Cambios

Para cada etiqueta, hay dos **acciones**:

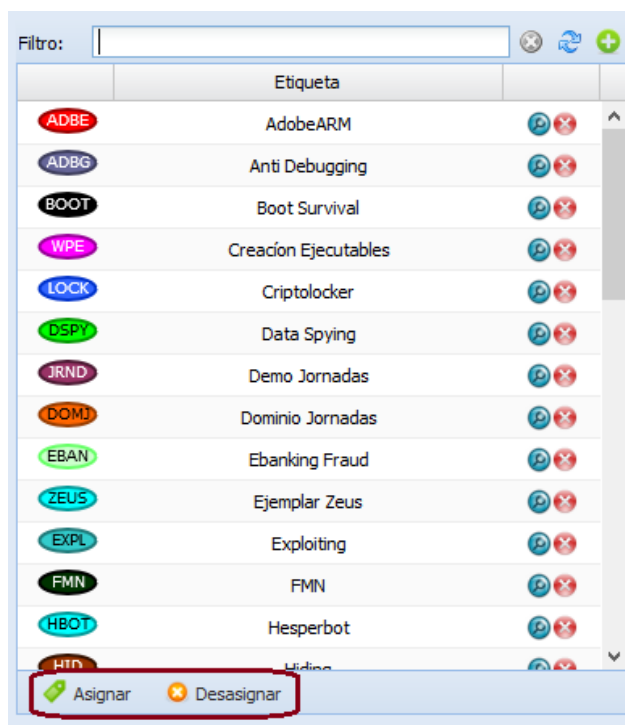
-  **Detalle:** Muestra la ventana de detalle de una etiqueta. Esta ventana permite modificar una etiqueta:



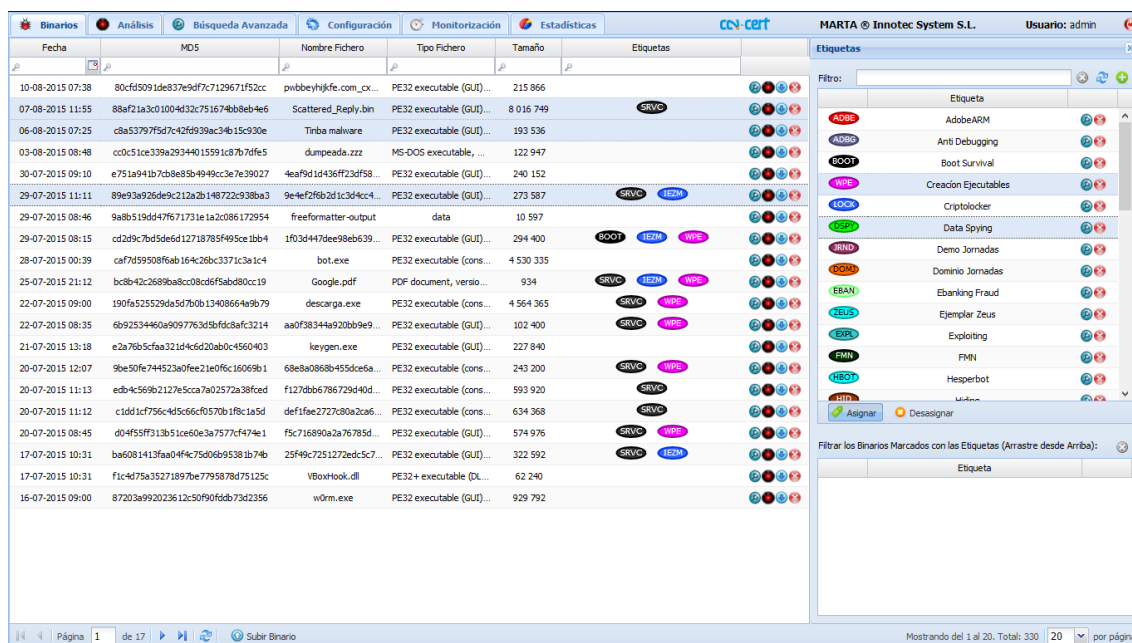
-  **Eliminar:** Elimina una etiqueta. Pide confirmación antes de eliminar:



En la barra de herramientas de esta lista, hay otras dos **acciones**:



- **Asignar:** Permite asignar todas las etiquetas seleccionadas a todos los ficheros seleccionados. Solo se podrán asignar etiquetas creadas por nuestra organización A modo de recordatorio: un fichero tiene asignadas todas las etiquetas que se le asignen manualmente, más todas las etiquetas que tengan asignadas todos sus análisis dinámicos.



**Binarios** **Análisis** **Búsqueda Avanzada** **Configuración** **Monitorización** **Estadísticas** **CCN-CERT** **MARTA © Innotec System S.L.** **Usuario: admin**

| Fecha            | MD5                              | Nombre Fichero        | Tipo Fichero                 | Tamaño    | Etiquetas               |
|------------------|----------------------------------|-----------------------|------------------------------|-----------|-------------------------|
| 10-08-2015 07:38 | 80cfd5091de837e9d7c7129671f52cc  | prbbeyhijfe.com_cx... | PE32 executable (GUI)...     | 215 866   |                         |
| 07-08-2015 11:55 | 88af21a3c01004d32c751674b8b8e4e5 | Scattered_Reply_bin   | PE32 executable (GUI)...     | 8 016 749 | SRVC, CRYPTO, WPE       |
| 06-08-2015 07:25 | c8a53797f5d7c42f9939ac34b15c930e | Tinba malware         | PE32 executable (GUI)...     | 193 536   | CRYPTO, WPE             |
| 03-08-2015 08:48 | c0c51ce339a29344015591c87b7dfe5  | dumpeada.zzz          | MS-DOS executable, ...       | 122 947   |                         |
| 30-07-2015 09:10 | e751a941b7cb8e8b4949cc3e7e39027  | 4ea9d1d436ff23df58    | PE32 executable (GUI)...     | 240 152   |                         |
| 29-07-2015 11:11 | 89e93a926de9c212a2b148722c938ba3 | 9e4ef2f6b2d1c3d4cc4   | PE32 executable (GUI)...     | 273 587   | SRVC, CRYPTO, REGM, WPE |
| 29-07-2015 08:46 | 9a8b519dd47671731e1a2c086172954  | freeformatter-output  | data                         | 10 597    |                         |
| 29-07-2015 08:15 | cd2d9c7bd5de6d12718785f495ce1bb4 | 1f03d447dee98eb639... | PE32 executable (GUI)...     | 294 400   | BOOT, IE2M, WPE         |
| 28-07-2015 00:39 | ca7d59508f6ab164c26bc3371c3a1c4  | bot.exe               | PE32 executable (cons...)... | 4 530 335 |                         |
| 25-07-2015 21:12 | bc8b42c2689ba8cc08cd6f5ab080cc19 | Google.pdf            | PDF document, versio...      | 934       | SRVC, IE2M, WPE         |
| 22-07-2015 09:00 | 190fa525529da5d7b0b13408664a9b79 | descarga.exe          | PE32 executable (cons...)... | 4 564 365 | SRVC, WPE               |
| 22-07-2015 08:35 | 6b92534660a9097763d5bfc3a3c3214  | aa0f38344a920bb9e9... | PE32 executable (GUI)...     | 102 400   | SRVC, WPE               |
| 21-07-2015 13:18 | e2a78b5cfaa321d4c6d20ab0c4560403 | keygen.exe            | PE32 executable (GUI)...     | 227 840   |                         |
| 20-07-2015 12:07 | 9be50fe744523a0fee21e0f6c16069b1 | 68e8a0868b455dce6a... | PE32 executable (cons...)... | 243 200   | SRVC, WPE               |
| 20-07-2015 11:13 | edb4c569b2127e5cca7a02572a38fced | f127dbb6786729d40d... | PE32 executable (cons...)... | 593 920   | SRVC                    |
| 20-07-2015 11:12 | c1dd1cf756c4d5c66c0570b1f8c1a5d  | def1fae2727c80a2ca6   | PE32 executable (cons...)... | 634 368   | SRVC                    |
| 20-07-2015 08:45 | d04f5ff313b51ce60e3a7577c474e1   | f5c716890a2a76785d    | PE32 executable (GUI)...     | 574 976   | SRVC, WPE               |
| 17-07-2015 10:31 | ba6081413faa04fc75006b95381b74b  | 25f49c7251272edc5c7   | PE32 executable (GUI)...     | 322 592   | SRVC, IE2M              |
| 17-07-2015 10:31 | f1c4d75a35271897be7795878d75125c | VBoxHook.dll          | PE32+ executable (DL...)...  | 62 240    |                         |
| 16-07-2015 09:00 | 87203a992023612c50f0f0db73d2356  | w0rm.exe              | PE32 executable (GUI)...     | 929 792   |                         |

**Etiquetas**

Filtro:

| Etiqueta |
|----------|
| ADBE     |
| ADBB     |
| ADBG     |
| BOOT     |
| CRYPTO   |
| LOCK     |
| REGM     |
| SRVC     |
| WPE      |
| IE2M     |
| IE3M     |
| IE4M     |
| IE5M     |
| IE6M     |
| IE7M     |
| IE8M     |
| IE9M     |
| IE10M    |
| IE11M    |
| IE12M    |
| IE13M    |
| IE14M    |
| IE15M    |
| IE16M    |
| IE17M    |
| IE18M    |
| IE19M    |
| IE20M    |
| IE21M    |
| IE22M    |
| IE23M    |
| IE24M    |
| IE25M    |
| IE26M    |
| IE27M    |
| IE28M    |
| IE29M    |
| IE30M    |
| IE31M    |
| IE32M    |
| IE33M    |
| IE34M    |
| IE35M    |
| IE36M    |
| IE37M    |
| IE38M    |
| IE39M    |
| IE40M    |
| IE41M    |
| IE42M    |
| IE43M    |
| IE44M    |
| IE45M    |
| IE46M    |
| IE47M    |
| IE48M    |
| IE49M    |
| IE50M    |
| IE51M    |
| IE52M    |
| IE53M    |
| IE54M    |
| IE55M    |
| IE56M    |
| IE57M    |
| IE58M    |
| IE59M    |
| IE60M    |
| IE61M    |
| IE62M    |
| IE63M    |
| IE64M    |
| IE65M    |
| IE66M    |
| IE67M    |
| IE68M    |
| IE69M    |
| IE70M    |
| IE71M    |
| IE72M    |
| IE73M    |
| IE74M    |
| IE75M    |
| IE76M    |
| IE77M    |
| IE78M    |
| IE79M    |
| IE80M    |
| IE81M    |
| IE82M    |
| IE83M    |
| IE84M    |
| IE85M    |
| IE86M    |
| IE87M    |
| IE88M    |
| IE89M    |
| IE90M    |
| IE91M    |
| IE92M    |
| IE93M    |
| IE94M    |
| IE95M    |
| IE96M    |
| IE97M    |
| IE98M    |
| IE99M    |
| IE100M   |

Asignar Desasignar

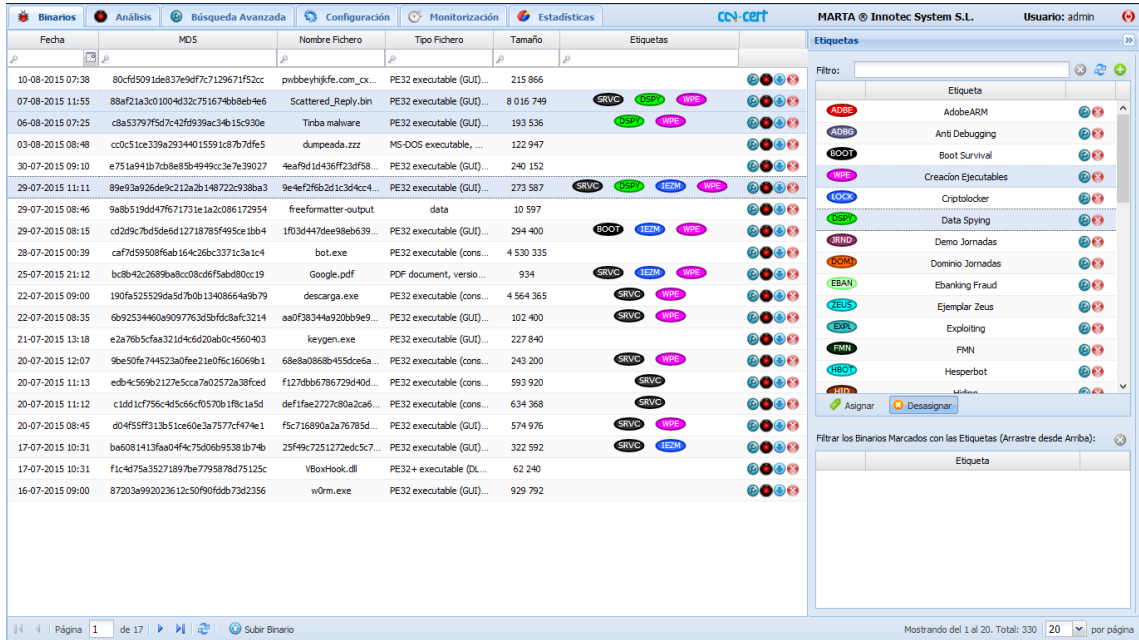
Filtrar los Binarios Marcados con las Etiquetas (Arrastre desde Arriba):

| Etiqueta |
|----------|
|----------|

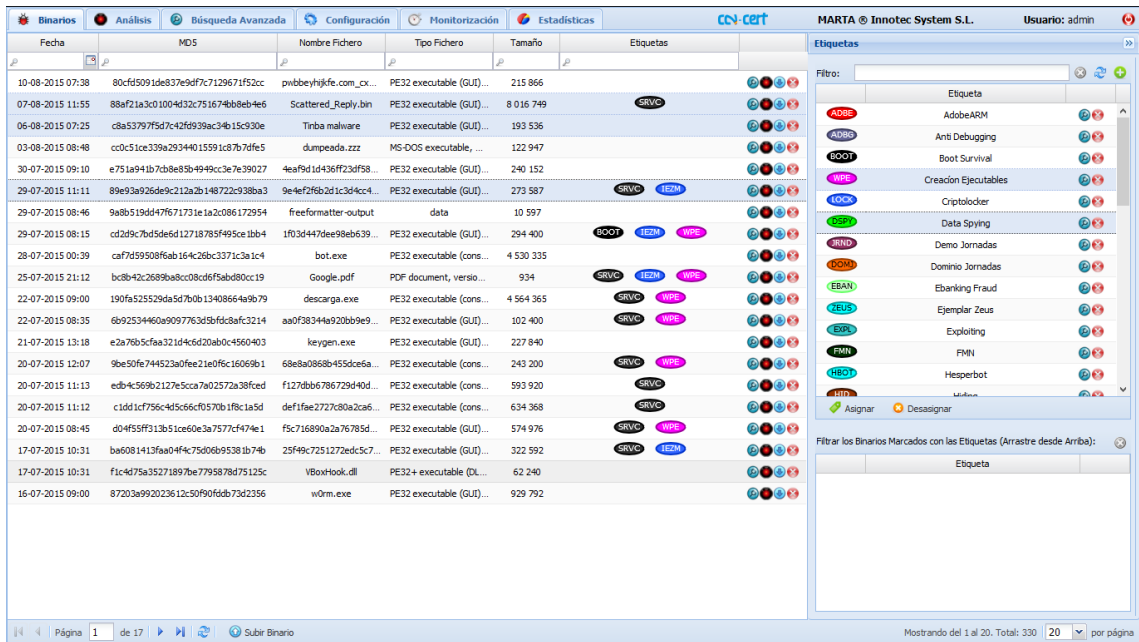
Página 1 de 17

Mostrando del 1 al 20. Total: 330 20 por página

-  **Desasignar:** Permite desasignar todas las etiquetas seleccionadas de todos los ficheros seleccionados.

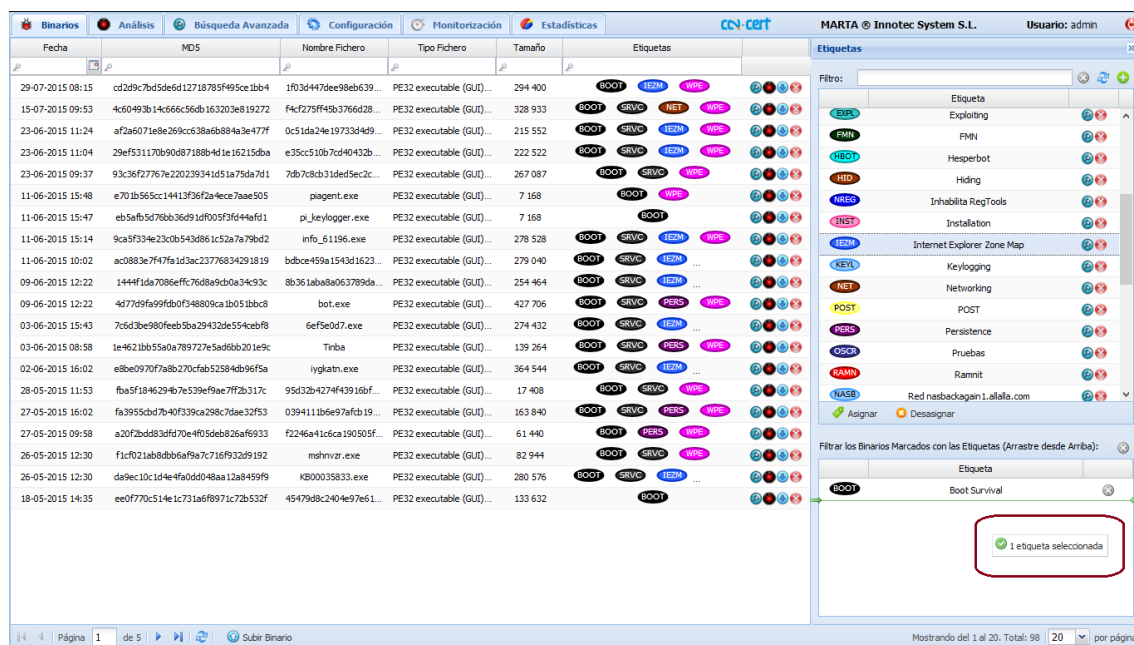


The screenshot shows the MARTA application interface. The top navigation bar includes tabs for Binarios, Análisis, Búsqueda Avanzada, Configuración, Monitorización, and Estadísticas. The 'Binarios' tab is active, displaying a table of files. The table has columns for Fecha, MD5, Nombre Fichero, Tipo Fichero, and Tamaño. The 'Etiquetas' column shows various colored icons representing different security labels. On the right, the 'Etiquetas' panel lists these labels: ADRB, ADBB, BOOT, CREACIÓN EJECUTABLES, CRIPTOLLOCKER, DATA SPYING, DEMO JORNADAS, DOMINIO JORNADAS, EBANKING FRAUD, EJEMPLAR ZEUS, EXPLOITING, FMN, HESPERBOT, and others. Each label has a checkbox and a small icon. Below the list, there are buttons for 'Asignar' and 'Desasignar'.

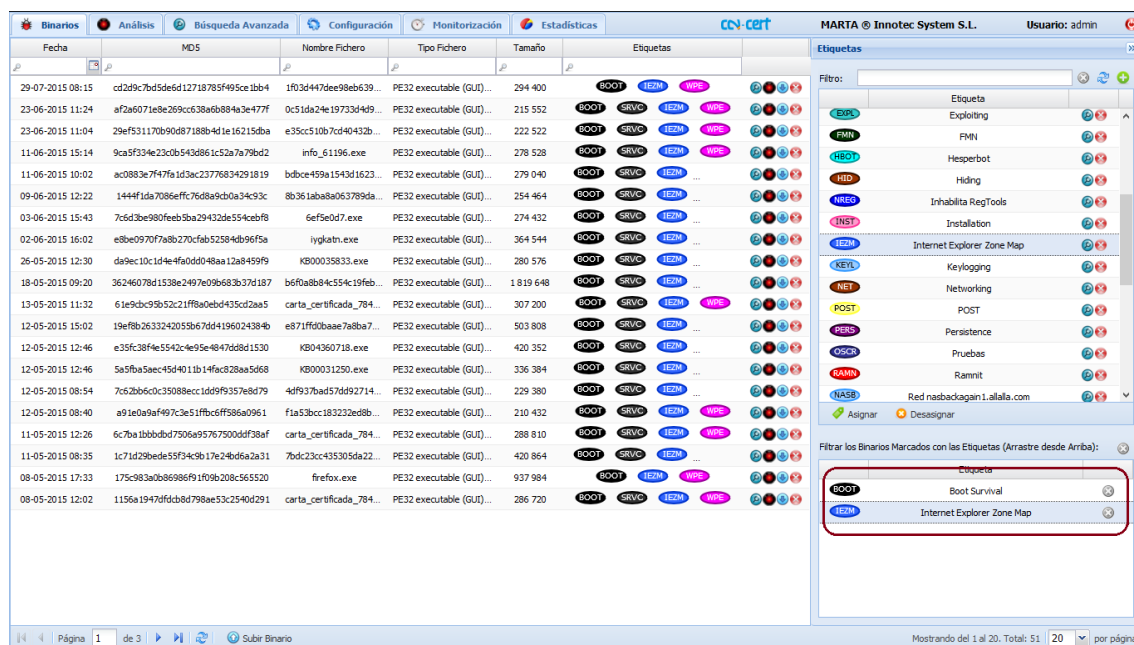


This screenshot is identical to the one above, showing the MARTA application interface with the 'Binarios' tab selected. It displays a table of files and a panel on the right for managing security labels (Etiquetas) such as ADRB, ADBB, BOOT, etc.

La **lista inferior** es una lista de **filtro**. Podemos **arrastrar etiquetas desde la lista superior**, y el listado de ficheros se filtrará mostrando solo los ficheros que tengan asociadas todas las etiquetas de la lista inferior:

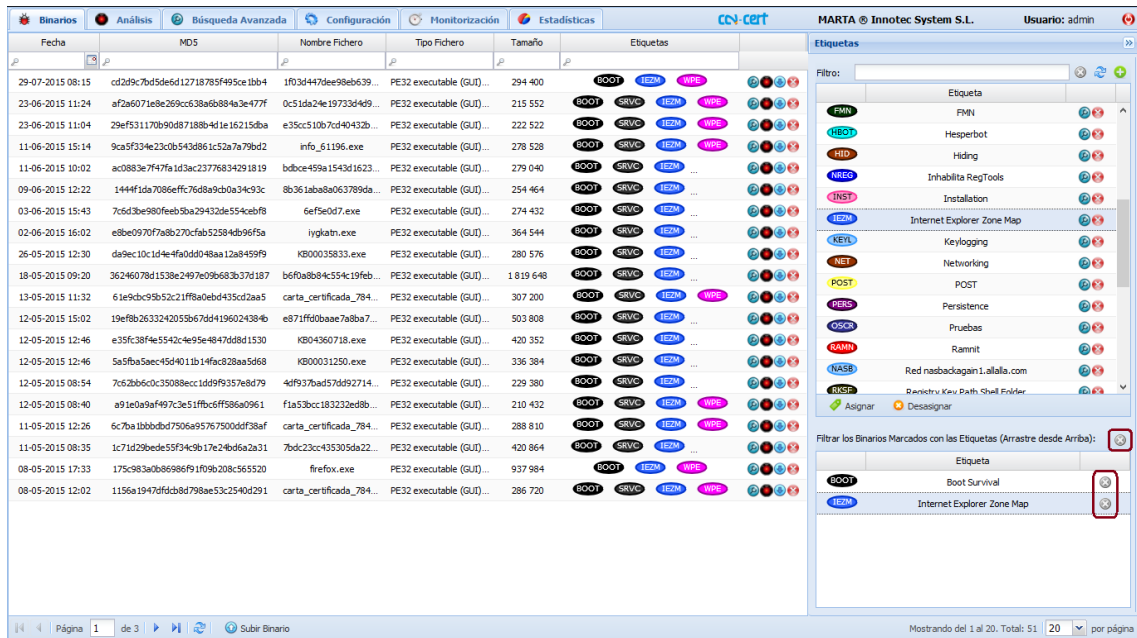


The screenshot shows the MARTA application interface. The top navigation bar includes tabs for Binarios, Análisis, Búsqueda Avanzada, Configuración, Monitorización, and Estadísticas. The 'Binarios' tab is active, displaying a table of files. The table has columns for Fecha, MD5, Nombre Fichero, Tipo Fichero, Tamaño, and Etiquetas. The 'Etiquetas' panel on the right shows a list of tags. A red box highlights the '1 etiqueta seleccionada' message at the bottom of the tags panel.



The screenshot shows the MARTA application interface. The top navigation bar includes tabs for Binarios, Análisis, Búsqueda Avanzada, Configuración, Monitorización, and Estadísticas. The 'Binarios' tab is active, displaying a table of files. The table has columns for Fecha, MD5, Nombre Fichero, Tipo Fichero, Tamaño, and Etiquetas. The 'Etiquetas' panel on the right shows a list of tags. A red box highlights the '1 etiqueta seleccionada' message at the bottom of the tags panel.

Se pueden quitar etiquetas de la lista de filtro arrastrándolas de nuevo a la lista superior, o clicando en la acción  **Quitar del Filtro** de la lista inferior. También se puede limpiar el filtro por completo clicando en el botón  **Quitar Todas las Etiquetas del Filtro**.



The screenshot displays the MARTA application interface. The main window shows a table of files with columns for Fecha, MD5, Nombre Fichero, Tipo Fichero, Tamaño, and Etiquetas. The Etiquetas column contains various tags like BOOT, SRV, and others. On the right side, there is a panel titled 'Etiquetas' which lists available tags and a section for filtering. The filter section has a button 'Filtrar los Binarios Marcados con las Etiquetas (Arrastre desde Arriba):' and a list of tags with checkboxes. A red box highlights the 'Quitar del Filtro' button (minus icon) next to the 'BOOT' tag in the filter list. Another red box highlights the 'Quitar Todas las Etiquetas del Filtro' button (minus icon) at the bottom of the filter panel.

## 6 PESTAÑA DE ANÁLISIS

Esta pestaña está diseñada para facilitar todas las gestiones relativas a los análisis dinámicos.

| ccn-cert MARTA © Innotec System S.L. Usuario: user_ccn |           |                                  |                |                |              |         |            |           |          |  |
|--------------------------------------------------------|-----------|----------------------------------|----------------|----------------|--------------|---------|------------|-----------|----------|--|
| Binarios                                               | Analisis  | Búsqueda Avanzada                | Configuración  | Monitorización | Estadísticas |         |            |           |          |  |
| Fecha                                                  | Organismo | MD5                              | Nombre Fichero | Sandbox        | Máq. Vir.    | Red     | Estado     | Etiquetas | Acciones |  |
| 03-10-2016 10:22                                       | CCN       | caf7d59508f5ab164c26bc3371c3a1c4 | irc.exe        | Cuckoo         | W7 32        | W7 32   | Finalizado | BIW, LSA  |          |  |
| 03-10-2016 10:22                                       | CCN       | caf7d59508f5ab164c26bc3371c3a1c4 | irc.exe        | Cuckoo         | WXP 32       | WXP 32  | Finalizado | BIW       |          |  |
| 03-10-2016 10:13                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W2k3 32      | W2k3 32 | Finalizado |           |          |  |
| 03-10-2016 09:57                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | WXP 32       | WXP 32  | Finalizado |           |          |  |
| 03-10-2016 09:42                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W7 32        | W7 32   | Finalizado |           |          |  |
| 03-10-2016 09:32                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W7 32        | W7 32   | Finalizado |           |          |  |
| 03-10-2016 08:58                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | WXP 32       | WXP 32  | Finalizado |           |          |  |
| 30-09-2016 14:48                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W2k8 32      | W2k8 32 | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W7 32        | W7 32   | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W8 32        | W8 32   | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W2k3 32      | W2k3 32 | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | WXP 32       | WXP 32  | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W2k8 32      | W2k8 32 | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W2k3 32      | W2k3 32 | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W8 32        | W8 32   | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W7 32        | W7 32   | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | WXP 32       | WXP 32  | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W7 32        | W7 32   | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W8 32        | W8 32   | Finalizado |           |          |  |
| 30-09-2016 14:47                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W2k3 32      | W2k3 32 | Finalizado |           |          |  |

### 6.1 LISTADO

La pestaña muestra una **lista** a modo de resumen con **todos los análisis dinámicos** de MARTA. Al igual que la lista de ficheros de la pestaña de binarios, la lista está paginada y ordenada por fecha del análisis, de más reciente a menos reciente.

En la lista se muestran los **atributos** más significativos de cada análisis: la fecha en la que realizó, la organización a la que pertenece le análisis, el MD5 y el nombre del fichero analizado, la sandbox, la máquina virtual, el tipo de red, el estado actual del análisis y sus etiquetas asociadas. Al igual que en la lista de ficheros, es posible **filtrar** por cualquiera de estos campos:

| ccn-cert MARTA © Innotec System S.L. Usuario: user_ccn |           |                                  |                |                |              |         |            |           |          |  |
|--------------------------------------------------------|-----------|----------------------------------|----------------|----------------|--------------|---------|------------|-----------|----------|--|
| Binarios                                               | Analisis  | Búsqueda Avanzada                | Configuración  | Monitorización | Estadísticas |         |            |           |          |  |
| Fecha                                                  | Organismo | MD5                              | Nombre Fichero | Sandbox        | Máq. Vir.    | Red     | Estado     | Etiquetas | Acciones |  |
| 03-10-2016 10:22                                       | CCN       | caf7d59508f5ab164c26bc3371c3a1c4 | irc.exe        | Cuckoo         | W7 32        | W7 32   | Finalizado | BIW, LSA  |          |  |
| 03-10-2016 10:22                                       | CCN       | caf7d59508f5ab164c26bc3371c3a1c4 | irc.exe        | Cuckoo         | WXP 32       | WXP 32  | Finalizado | BIW       |          |  |
| 03-10-2016 10:13                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | W2k3 32      | W2k3 32 | Finalizado |           |          |  |
| 03-10-2016 09:57                                       | IGAE      | e9ef9dfce577e957d08bf2f808ce346  | paflsh.binary  | Cuckoo         | WXP 32       | WXP 32  | Finalizado |           |          |  |

## 6.2 ESTADOS DE UN ANÁLISIS

Desde que se pide o se programa un análisis dinámico hasta que finaliza, pasa por una serie de diversos estados que se describen a continuación:

-  **Pendiente de Envío:** El análisis aún no ha sido enviado a su sandbox correspondiente. Esto puede deberse a que el análisis esté programado para una fecha y hora posterior a la actual, o a que el proceso que envía los análisis a las sandbox (el cual se ejecuta periódicamente cada poco tiempo) esté a punto de ejecutarse.
-  **Error en el Envío:** Se ha producido un error en la comunicación entre el servidor de MARTA y la sandbox en el momento del envío del análisis. Un análisis en este estado no llegará a ejecutarse nunca.
-  **Solicitado:** El análisis ha sido enviado a la sandbox, y ésta aún no ha enviado respuesta. Esto puede deberse a que el análisis se esté ejecutando (usualmente conlleva varios minutos), o a que la sandbox tenga otros análisis por delante.
-  **Error en el Análisis:** Se ha producido un error durante la ejecución del análisis.
-  **Error en la Respuesta:** El análisis se ha ejecutado correctamente en la sandbox, pero se ha producido un error en la comunicación entre el servidor de MARTA y la sandbox en el momento del envío de los datos del análisis.
-  **Finalizado:** El análisis se ha ejecutado correctamente y el servidor de MARTA ha recogido los datos del análisis, los cuales pueden ser consultados a través de la interfaz web.

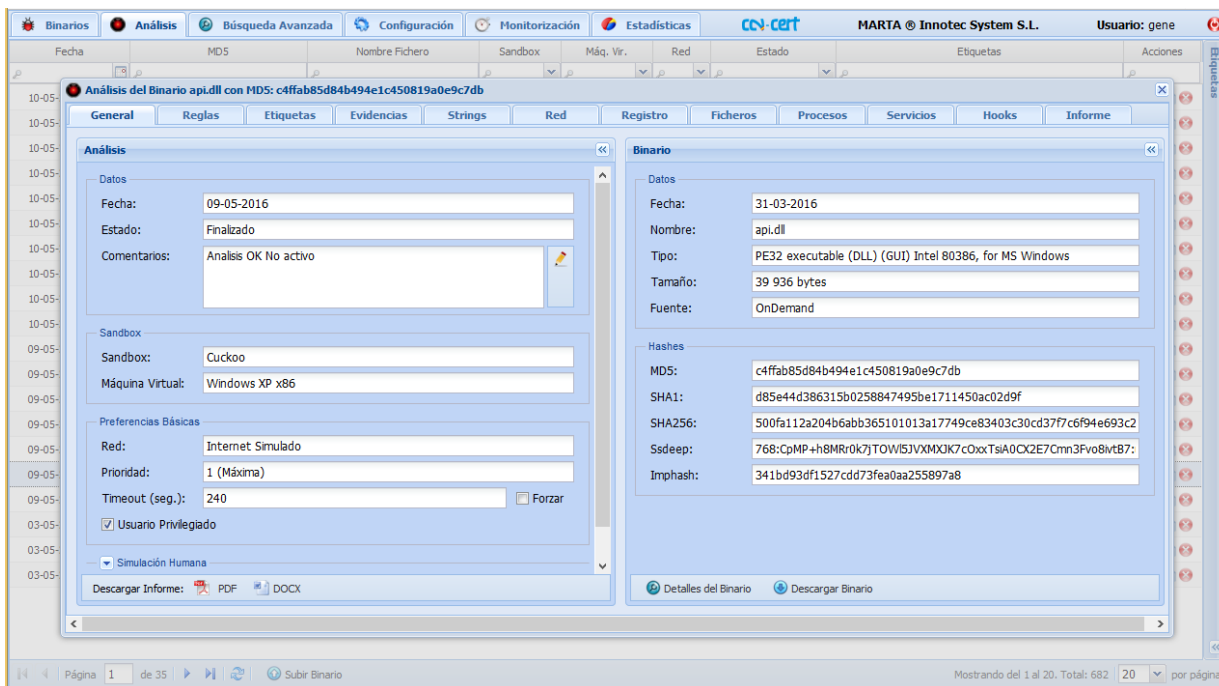
## 6.3 ACCIONES SOBRE LOS ANÁLISIS

La última columna de la lista de análisis es de **acciones**:

| Sandbox                                                                             | Máq. Vir.                                                                           | Red                                                                                 | Estado                                                                                         | Etiquetas                                                                                                                                                                  | Acciones                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  |  |             |                                                                                         |                                                                                                                                                                              |
| Cuckoo                                                                              | WXP 32                                                                              |  |  Finalizado |                                                                                       |    |
| Cuckoo                                                                              | WXP 32                                                                              |  |  Finalizado |   |    |
| Cuckoo                                                                              | WXP 32                                                                              |  |  Finalizado |   |    |

Permite realizar las siguientes acciones sobre un análisis:

-  **Ver Detalle:** Abre la vista de detalles del análisis seleccionado. Esta vista contiene toda la información extraída durante el análisis. Se describe en la sección [Vista de Detalle de un Análisis](#) de este documento.



-  **Reanalizar Binario:** Abre la vista de reanálisis del fichero correspondiente al análisis seleccionado. Esta vista permite lanzar o programar uno o varios análisis dinámicos de un fichero. Se describe en la sección [Vista de Reanálisis de un Binario](#) de este documento.

**Crear Reanálisis para el binario con MD5: 540b7275c35221468b077afdbdecb873** [X]

**Programación de los Reanálisis**

Fecha y Hora de Inicio del Primer Reanálisis

Fecha: 03/10/2016 Hora: 11 : 31

Número de Análisis e Intervalo de Tiempo entre Análisis

Nº Análisis: 1 Intervalo: 1 h : 00 m

☐ Incluir Triana

☒ Enviar email al usuario validado

☐ Enviar email a otra cuenta

☒ Cuckoo Sandbox ☐ Joe Sandbox

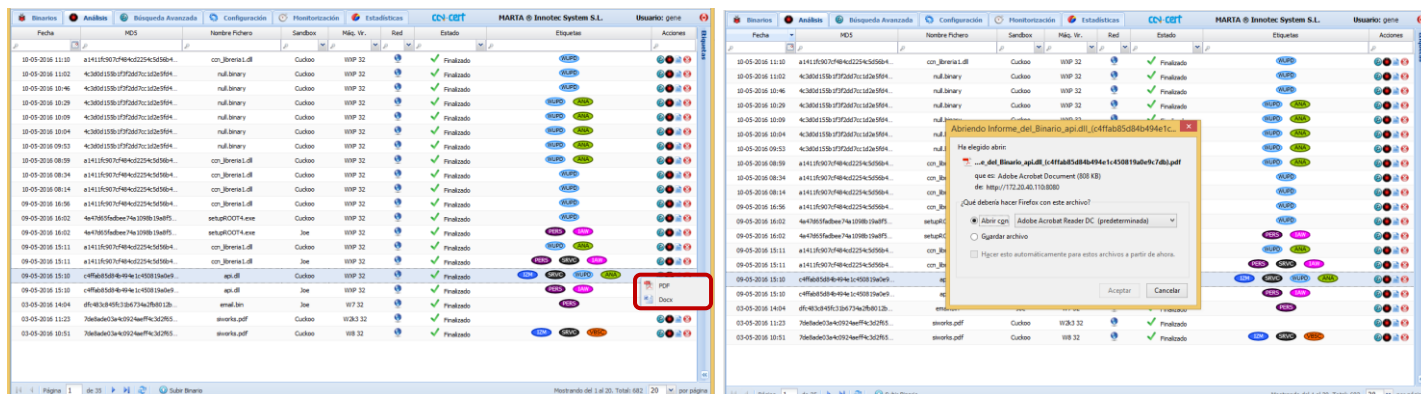
**Máquinas Virtuales**

|                          |                         |
|--------------------------|-------------------------|
| <input type="checkbox"/> | Windows XP x86          |
| <input type="checkbox"/> | Windows 7 x86           |
| <input type="checkbox"/> | Windows 8 x86           |
| <input type="checkbox"/> | Windows Server 2003 x86 |
| <input type="checkbox"/> | Windows Server 2008 x86 |

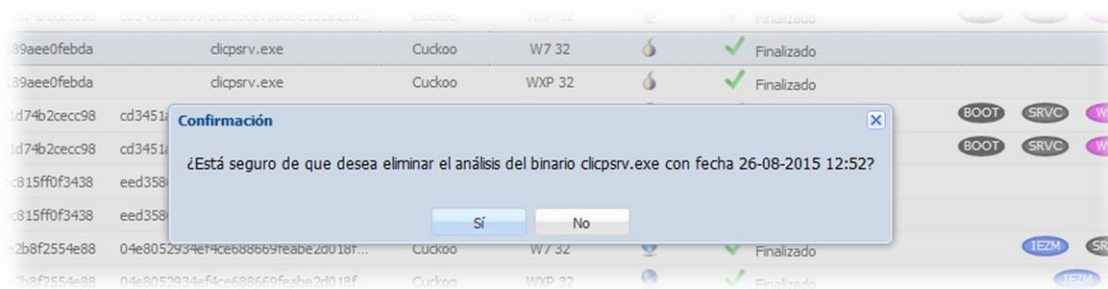
**Preferencias Básicas**

+ Crear Reanálisis

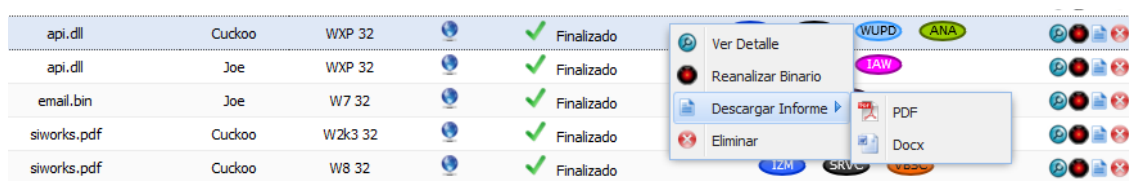
-  **Descargar Informe:** Descarga el informe del análisis seleccionado. Este informe incluye toda la información extraída del análisis, y también toda la información de los scripts estáticos. Es posible elegir el formato del informe entre PDF y Docx.



-  **Eliminar:** Elimina el análisis seleccionado. Pide confirmación antes de eliminar. Solo podremos eliminar los análisis de nuestra organización.



Al igual que en la lista de ficheros, todas estas acciones también pueden realizarse utilizando el botón derecho del ratón sobre un análisis de la lista.



## 6.4 ACCIONES GENERALES

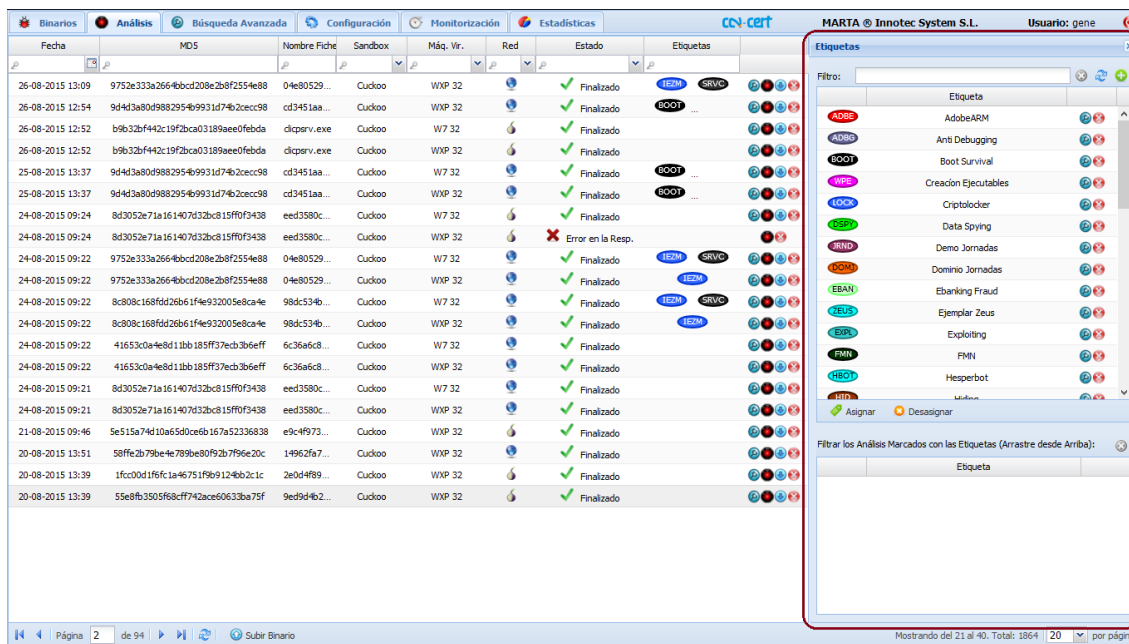
Al igual que en la pestaña de binarios, en la barra de herramientas de la parte inferior de la pestaña de análisis, hay botones que permiten realizar **gestiones** que no están directamente ligadas a un análisis:



Y, de nuevo, al igual que en la pestaña de binarios, en la de análisis sólo hay una: **Subir Binario**, que abre la vista de subida de un fichero.

## 6.5 ETIQUETAS

En la parte derecha de la pestaña, hay un panel desplegable que permite hacer **gestiones con las etiquetas** asociadas a los análisis, de forma totalmente similar al de la pestaña de binarios.



The screenshot displays the MARTA interface with the 'Análisis' tab selected. The main table lists analysis results with columns for Fecha, MD5, Nombre Fichero, Sandbox, Máq. Vr., Red, Estado, and Etiquetas. The 'Etiquetas' panel on the right is open, showing a list of tags (e.g., AdobeARM, Ant Debugging, Boot Survival) and buttons for 'Asignar' and 'Desasignar'. The bottom status bar indicates 'Mostrando del 21 al 40. Total: 1864 | 20 | por página'.

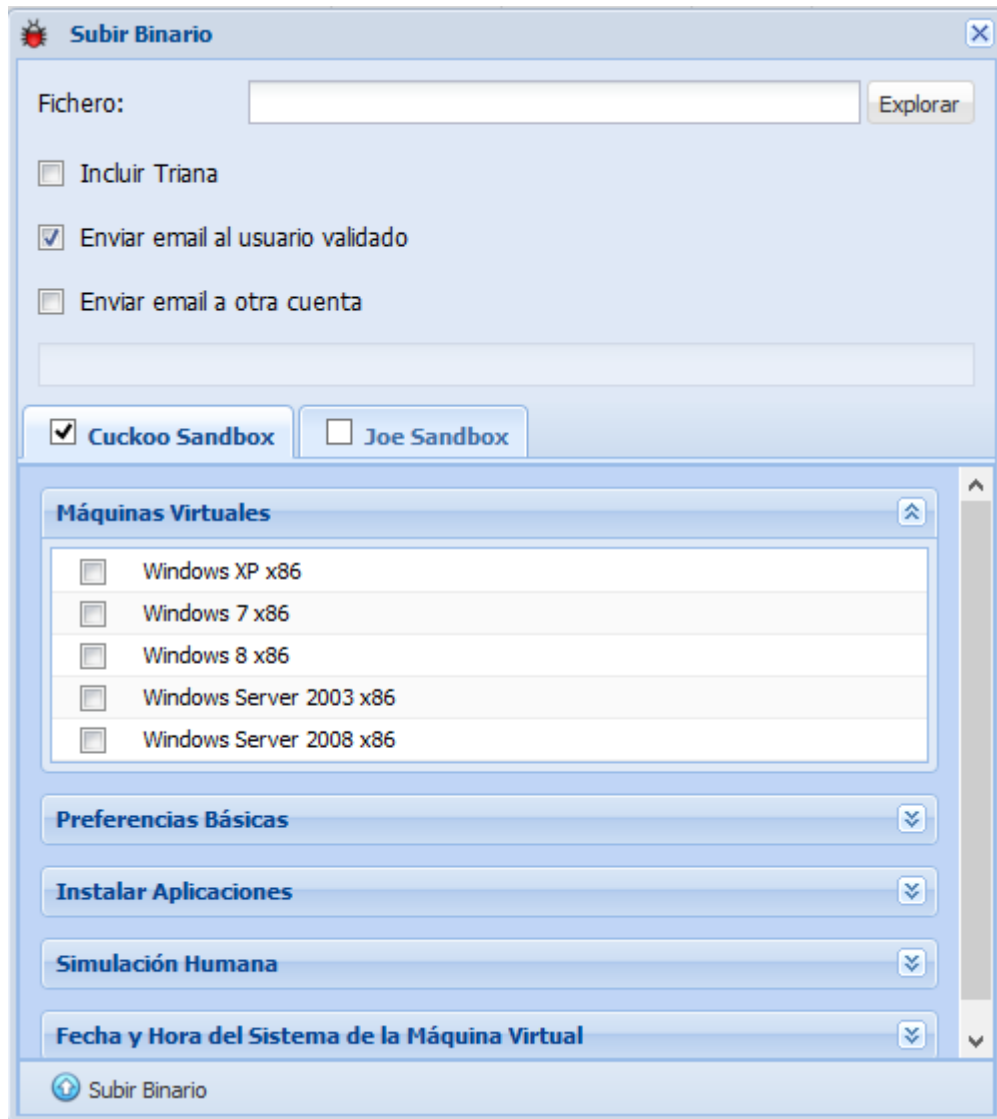
Permite crear, modificar y eliminar etiquetas, asignarlas y desasignarlas a múltiples análisis y filtrar los análisis por etiquetas. Véase la sección [Etiquetas de la Pestaña de Binarios](#).

A modo de recordatorio: un análisis tiene asociadas todas las etiquetas que se le asignen manualmente, más todas las etiquetas que asociadas a las reglas que cumple. Y un fichero tiene asignadas todas las etiquetas que se le asignen

manualmente, más todas las etiquetas que tengan asignadas todos sus análisis dinámicos.

## 7 VISTA DE SUBIDA DE UN BINARIO

Esta vista permite subir un fichero nuevo a MARTA y hacerle un análisis dinámico directamente (o varios si seleccionamos múltiples sandbox y/o máquinas virtuales).

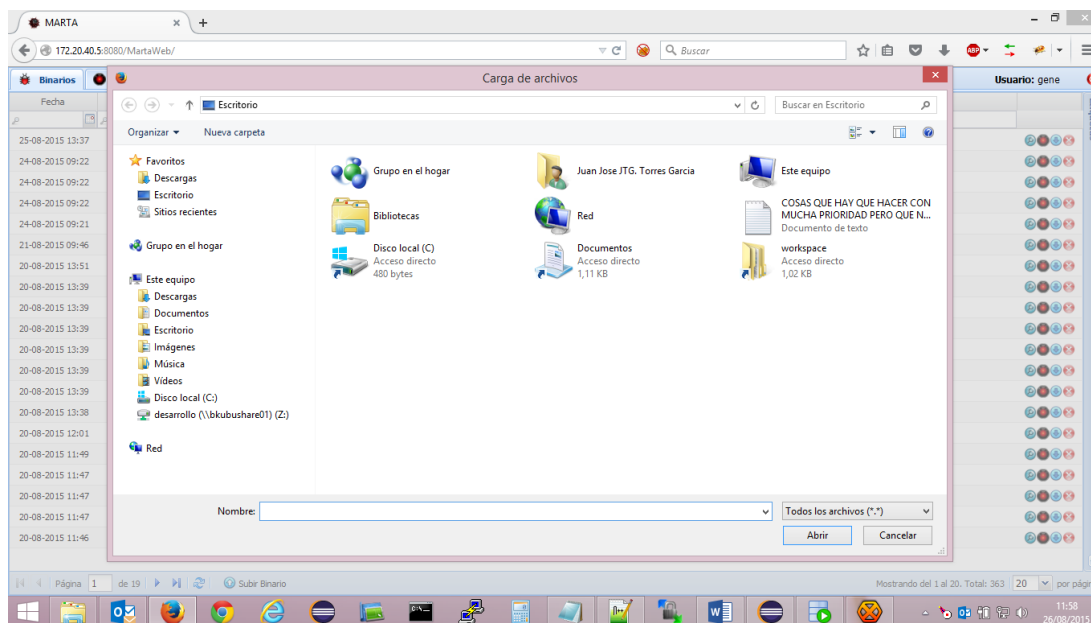


The screenshot shows the 'Subir Binario' window with the following elements:

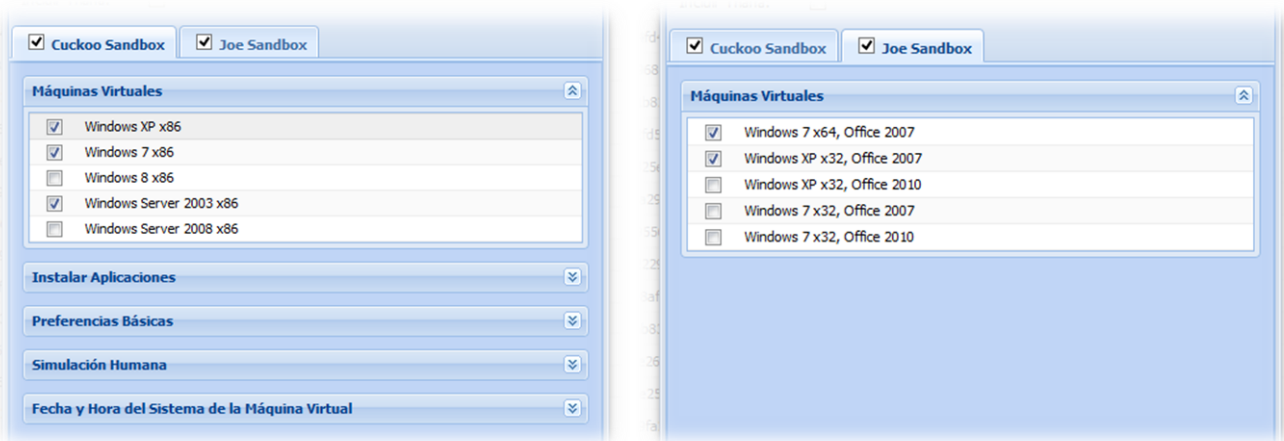
- Header:** A red bug icon and the title 'Subir Binario'.
- Fichero:** A text input field for the file name, followed by an 'Explorar' button.
- Options:**
  - ☐ Incluir Triana
  - ☒ Enviar email al usuario validado
  - ☐ Enviar email a otra cuenta
- Sandbox Selection:** Two buttons: ☒ Cuckoo Sandbox and ☐ Joe Sandbox.
- Máquinas Virtuales:** A list of virtual machines with checkboxes:
  - ☐ Windows XP x86
  - ☐ Windows 7 x86
  - ☐ Windows 8 x86
  - ☐ Windows Server 2003 x86
  - ☐ Windows Server 2008 x86
- Expandable Sections:** Four sections with expand/collapse arrows:
  - Preferencias Básicas
  - Instalar Aplicaciones
  - Simulación Humana
  - Fecha y Hora del Sistema de la Máquina Virtual
- Footer:** A blue button with an upload icon and the text 'Subir Binario'.

## 7.1 CAMPOS DEL FORMULARIO

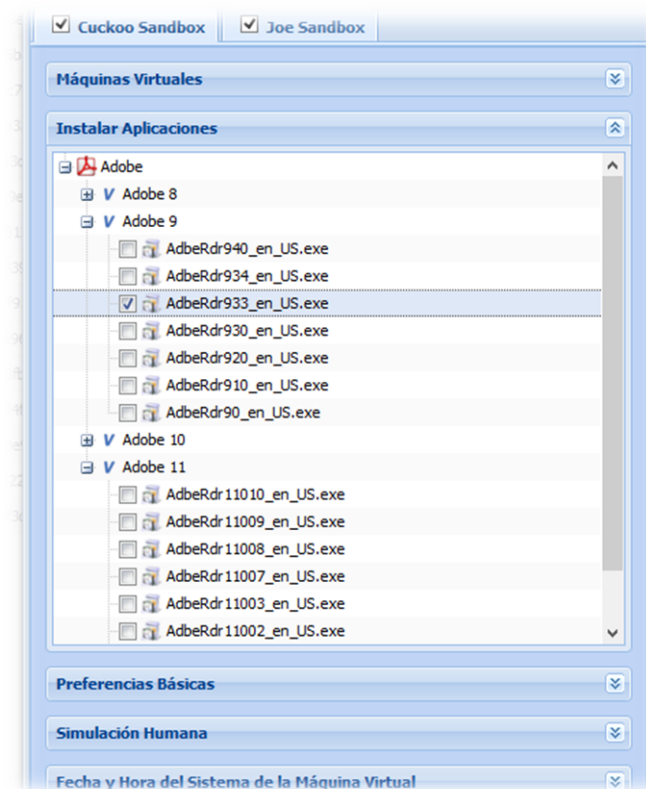
- En el campo **Fichero**, seleccionamos el fichero que queremos subir. Pinchando en el botón Explorar se nos abrirá el navegador:



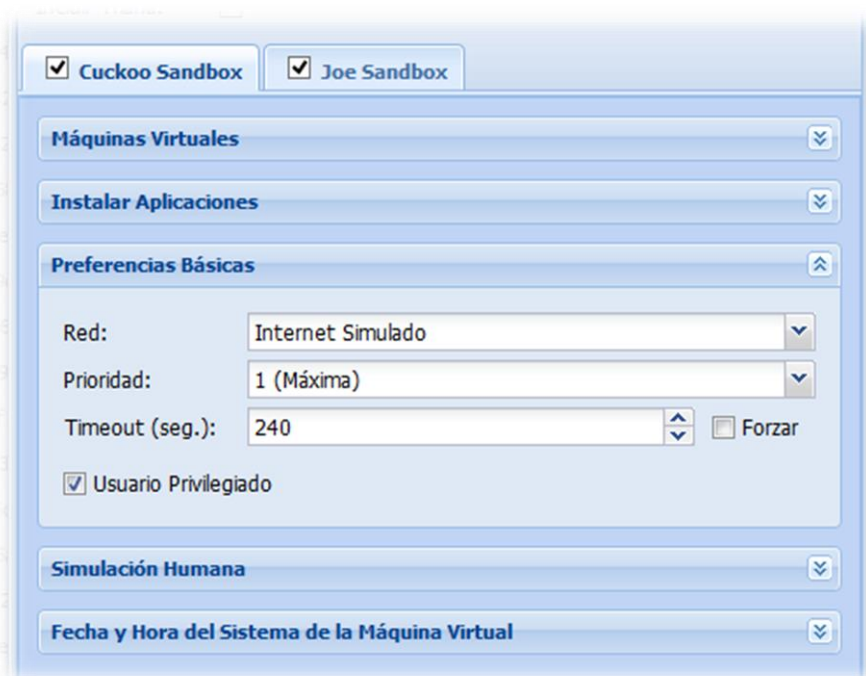
- En el campo **Enviar mail a otra cuenta**, podemos indicar un correo electrónico donde se enviará un informe de cada análisis automáticamente.
- Si marcamos el campo **Incluir Triana**, se realizará un análisis de Triana del MD5 del fichero seleccionado, y se asociará a los análisis dinámicos.
- Por cada **Sandbox** hay una pestaña con una casilla de selección. Es posible seleccionar ambas Sandbox para realizar uno o varios análisis en cada una de ellas. Cada pestaña incluye todas las opciones de análisis de la Sandbox. Para cada Sandbox debemos seleccionar las máquinas virtuales sobre las que queremos hacer análisis. Se realizará un análisis dinámico por cada máquina virtual seleccionada en cada Sandbox.



- Pestaña de **Cuckoo Sandbox**: En esta pestaña podemos seleccionar las máquinas virtuales de Cuckoo sobre las que queremos realizar análisis dinámicos, y elegir las opciones de Cuckoo para estos análisis, de entre las siguientes:
  - o Instalar Aplicaciones: Permite instalar versiones concretas de aplicaciones (como, por ejemplo, Adobe Reader) en la máquina virtual antes de la ejecución del malware. Esto es útil para la detección de códigos dañinos que explotan una vulnerabilidad de una versión concreta de una aplicación, o códigos dañinos que requieren que una aplicación concreta esté instalada para funcionar.



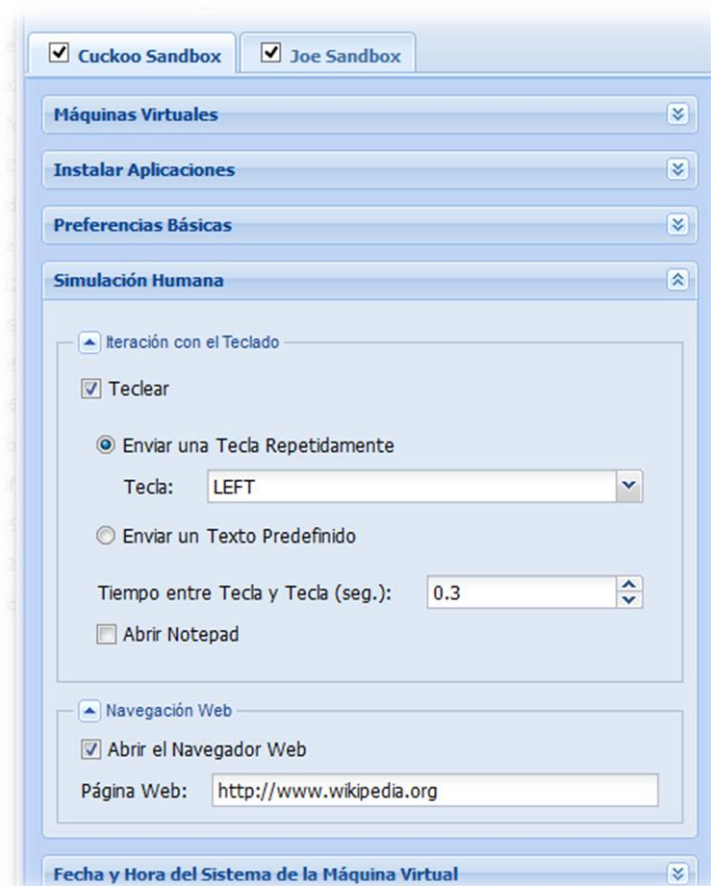
- Preferencias Básicas: Permite elegir el tipo de red de las máquinas virtuales, la prioridad del análisis, su duración máxima y los privilegios del usuario que ejecuta el malware.



- Tipos de Red: **Internet Simulado** debe utilizarse para analizar códigos dañinos que para funcionar necesiten hacer conexiones a Internet, pero no queramos que se hagan realmente. Con esta opción, la máquina estará totalmente aislada de internet, pero habrá un proceso que intentará hacer creer al código dañino que sí hay conexión. Resolverá correctamente las peticiones DNS que se hagan, y responderá a las peticiones a puertos conforme al protocolo estándar del puerto (el protocolo que se utilizará en cada puerto es configurable). Sin embargo, si el código dañino necesita descargarse datos de Internet o requiere una respuesta específica a una petición, es muy posible que no funcione con Internet Simulado. **Tor**, en cambio, permite la salida a Internet de forma real, pero lo hace a través de la red Tor para evitar el rastreo del análisis de forma externa.
- Prioridad: Esta opción es útil si queremos encolar múltiples análisis al mismo tiempo. Cuando Cuckoo termine un análisis y vaya a seleccionar de la cola de análisis el siguiente, siempre seleccionará primero el más prioritario. La escala de prioridades consta de 7 niveles, siendo 1 el más prioritario y 7 el menos.
- Duración Máxima: En el campo **Timeout** podemos indicar el tiempo máximo en segundos que durará el análisis. Si la ejecución del código

daño no ha terminado una vez cumplido este tiempo, la máquina virtual se detendrá inmediatamente. Marcando la opción **Forzar**, la máquina virtual seguirá en ejecución y siendo monitorizada durante el tiempo indicado en Timeout, incluso si la ejecución del código dañado ha terminado.

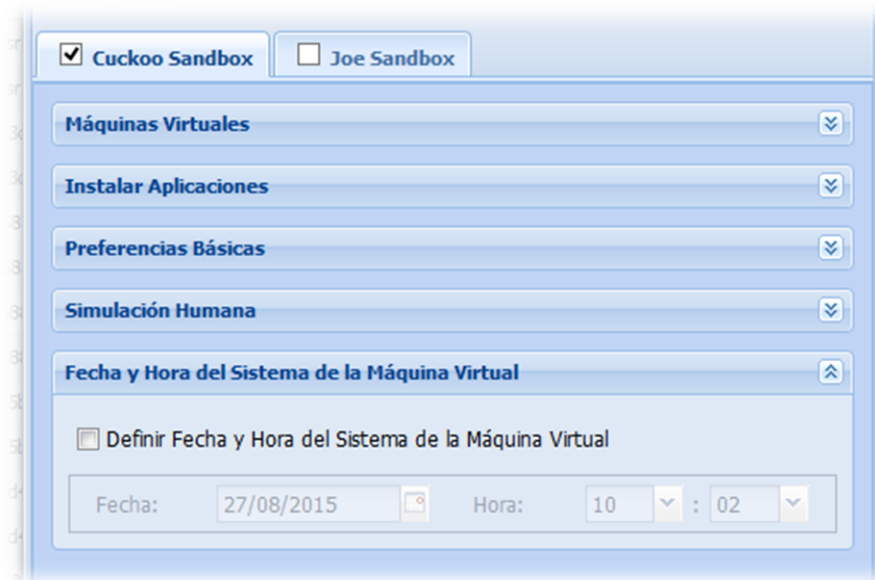
- Usuario Privilegiado: Marcando esta opción, el código dañado se ejecutará con privilegios de administrador.
- Simulación Humana: Cuckoo dispone de una serie de opciones que permiten simular el comportamiento humano durante la ejecución del malware.



- Iteración con el Teclado: Permite simular la pulsación de una tecla concreta cada cierto tiempo de forma constante, o la escritura de un texto predefinido (Lorem Ipsum), durante toda la ejecución de la máquina virtual. Si no se marca el campo Abrir Notepad, la escritura se hará sobre el escritorio, o sobre las ventanas que se abran durante la ejecución del malware. En cambio, si se marca, se abrirá la aplicación Notepad y se escribirá en ella.

- Navegación web: Permite abrir el navegador web y acceder a una página web en concreto durante la ejecución de la máquina virtual.

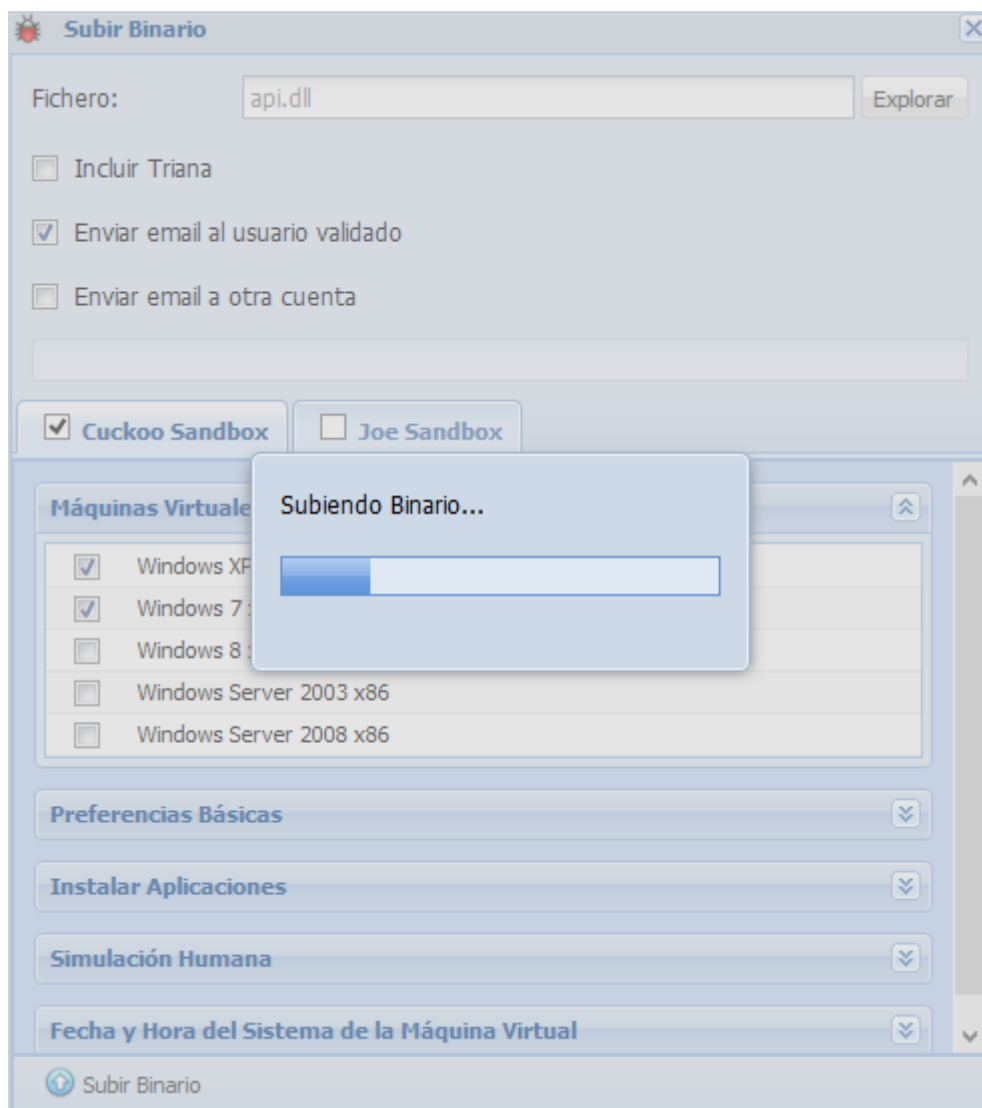
- Fecha y Hora del Sistema de la Máquina Virtual: Permite establecer la fecha y hora del sistema operativo de la máquina virtual justo antes de ejecutar el malware. Esto es útil para analizar códigos dañinos cuya ejecución depende de la fecha y hora.



- Pestaña de **Joe Sandbox**: En esta pestaña podemos seleccionar las máquinas virtuales de Joe sobre las que queremos realizar análisis dinámicos. Sin embargo, actualmente Joe no cuenta con opciones para los análisis.

## 7.2 SUBIDA DEL FICHERO

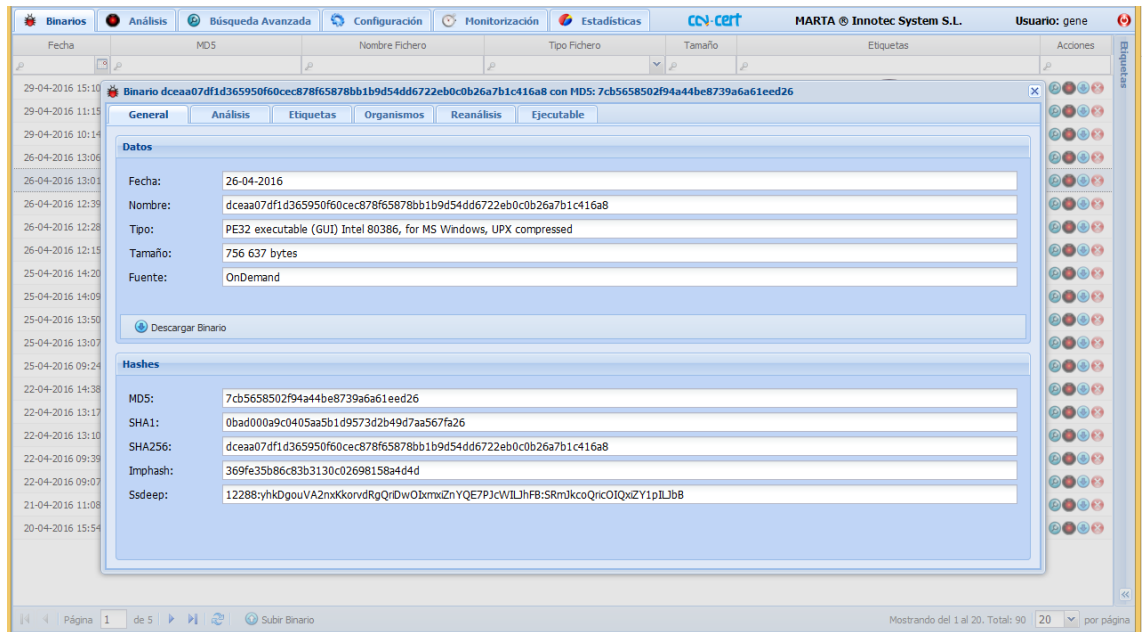
Una vez seleccionados todos los campos, hacemos clic en el botón **Subir Binario**. Esto hará que se suba el fichero a MARTA, se le pasen los scripts estáticos y se lance un análisis dinámico por cada máquina virtual marcada en cada sandbox.



Los scripts estáticos tardan muy poco tiempo en pasarse, así que se lanzan inmediatamente según se realiza la subida del fichero, y se espera a que terminen. Sin embargo, los análisis dinámicos normalmente conllevan varios minutos de análisis, por lo que en el momento de la subida del binario, simplemente se lanzan, pero no se espera a que terminen.

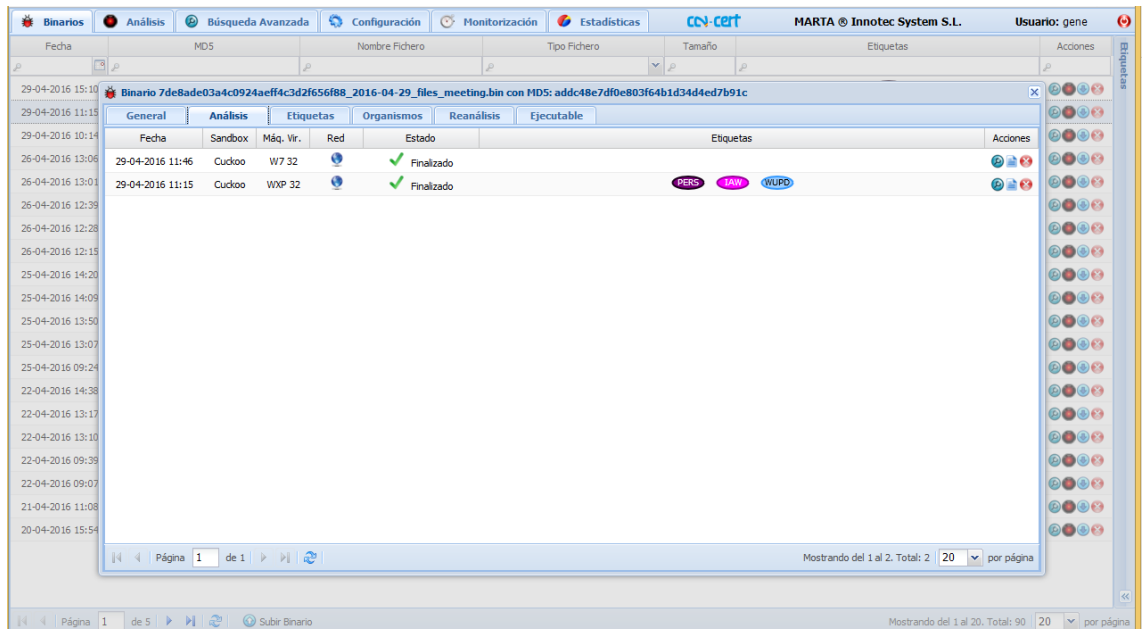
Una vez han terminado los scripts estáticos y se han lanzado los análisis dinámicos, la ventana muestra el MD5 del fichero subido, y permite las siguientes acciones:

-  **Detalles del Binario:** Abre la vista de detalles del fichero subido. Esta vista contiene toda la información relativa a dicho fichero, incluidos los datos extraídos de los scripts estáticos. Se describe en la sección [Vista de Detalle de un Binario](#) de este documento.



-  **Subir Otro:** Permite subir otro fichero a MARTA.
-  **Cerrar:** Cierra la ventana de subida de fichero.

Los análisis dinámicos pueden verse desde la propia vista de detalles del fichero:



Y también desde la pestaña de análisis:

El fichero subido aparecerá en la pestaña de binarios:

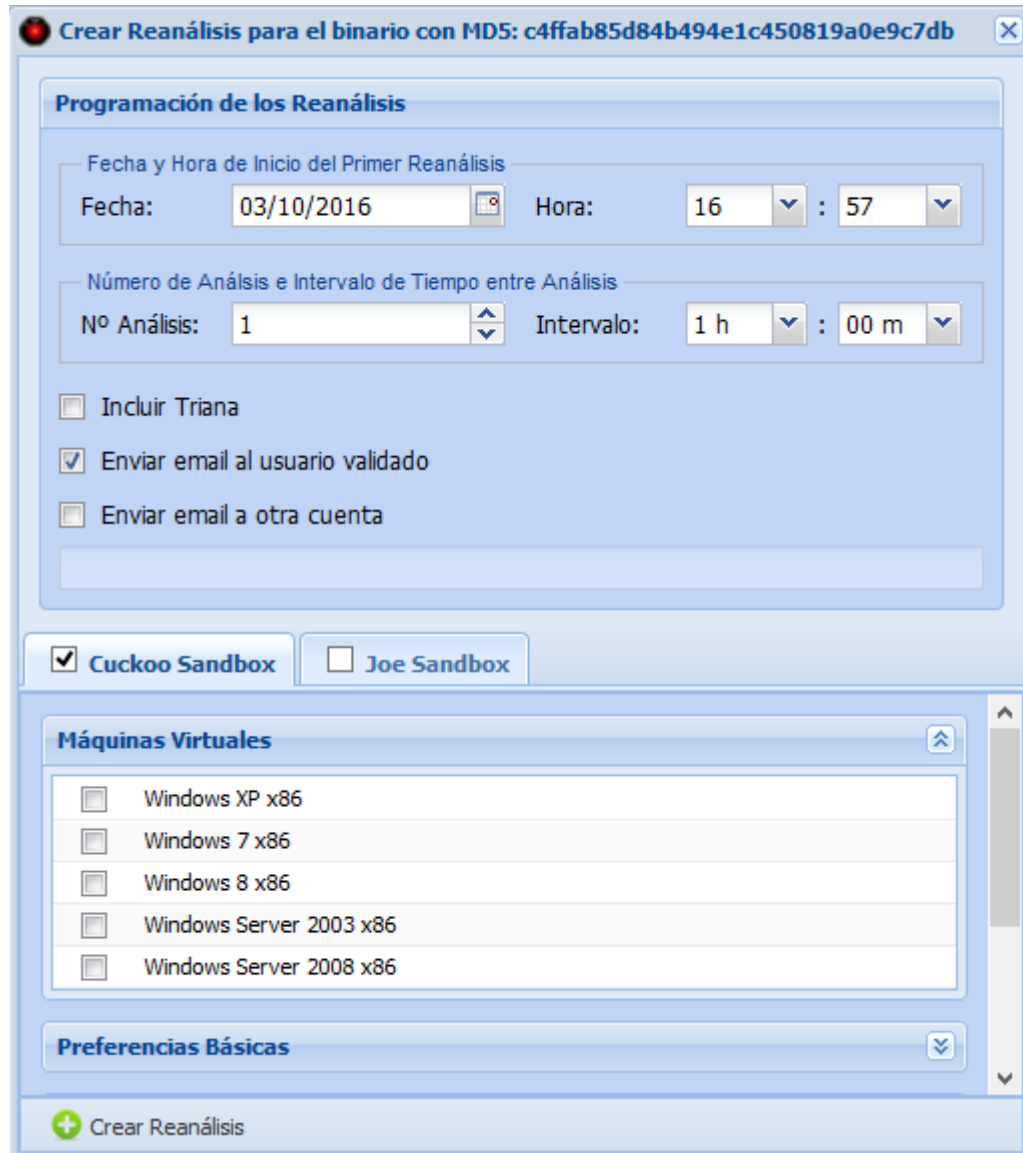
| MARTA © Innotec System S.L. Usuario: user_ccn |           |                                  |                          |         |           |     |            |           |          |  |
|-----------------------------------------------|-----------|----------------------------------|--------------------------|---------|-----------|-----|------------|-----------|----------|--|
| Fecha                                         | Organismo | MD5                              | Nombre Fichero           | Sandbox | Máq. Vir. | Red | Estado     | Etiquetas | Acciones |  |
| 03-10-2016 16:38                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll                  | Cuckoo  | W7 32     |     | Solicitado |           |          |  |
| 03-10-2016 16:38                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll                  | Cuckoo  | WXP 32    |     | Solicitado |           |          |  |
| 03-10-2016 16:38                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll                  | Cuckoo  | W7 32     |     | Finalizado |           |          |  |
| 03-10-2016 16:38                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll                  | Cuckoo  | WXP 32    |     | Finalizado |           |          |  |
| 03-10-2016 16:01                              | IGAP      | a80f4c5055e0d7e6fe59d4e14bd3c103 | Cronos_2.0.binary        | Cuckoo  | WXP 32    |     | Finalizado |           |          |  |
| 03-10-2016 16:01                              | IGAP      | a80f4c5055e0d7e6fe59d4e14bd3c103 | Cronos_2.0.binary        | Cuckoo  | W7 32     |     | Finalizado |           |          |  |
| 03-10-2016 16:01                              | IGAP      | a80f4c5055e0d7e6fe59d4e14bd3c103 | Cronos_2.0.binary        | Cuckoo  | W8 32     |     | Finalizado |           |          |  |
| 03-10-2016 16:01                              | IGAP      | a80f4c5055e0d7e6fe59d4e14bd3c103 | Cronos_2.0.binary        | Cuckoo  | W2k3 32   |     | Finalizado |           |          |  |
| 03-10-2016 16:00                              | IGAP      | a80f4c5055e0d7e6fe59d4e14bd3c103 | Cronos_2.0.binary        | Cuckoo  | WXP 32    |     | Finalizado |           |          |  |
| 03-10-2016 16:00                              | IGAP      | a80f4c5055e0d7e6fe59d4e14bd3c103 | Cronos_2.0.binary        | Cuckoo  | W7 32     |     | Finalizado |           |          |  |
| 03-10-2016 16:00                              | IGAP      | a80f4c5055e0d7e6fe59d4e14bd3c103 | Cronos_2.0.binary        | Cuckoo  | W8 32     |     | Finalizado |           |          |  |
| 03-10-2016 16:00                              | IGAP      | a80f4c5055e0d7e6fe59d4e14bd3c103 | Cronos_2.0.binary        | Cuckoo  | W2k3 32   |     | Finalizado |           |          |  |
| 03-10-2016 14:57                              | CCN       | 4c3d0d15b01f3f2dd7cc1d3e5f64c8f9 | null.binary              | Cuckoo  | WXP 32    |     | Finalizado |           |          |  |
| 03-10-2016 14:11                              | IGAP      | 6352645bb37025dc51e59ca4e3e9230  | ficherosRegistros.binary | Cuckoo  | W7 32     |     | Finalizado |           |          |  |
| 03-10-2016 14:11                              | IGAP      | 6352645bb37025dc51e59ca4e3e9230  | ficherosRegistros.binary | Cuckoo  | W8 32     |     | Finalizado |           |          |  |
| 03-10-2016 14:11                              | IGAP      | 6352645bb37025dc51e59ca4e3e9230  | ficherosRegistros.binary | Cuckoo  | W2k3 32   |     | Finalizado |           |          |  |
| 03-10-2016 14:11                              | IGAP      | 6352645bb37025dc51e59ca4e3e9230  | ficherosRegistros.binary | Cuckoo  | W2k8 32   |     | Finalizado |           |          |  |
| 03-10-2016 14:11                              | IGAP      | 6352645bb37025dc51e59ca4e3e9230  | ficherosRegistros.binary | Cuckoo  | WXP 32    |     | Finalizado |           |          |  |

Las listas de ficheros y de análisis están ordenadas por fecha de más reciente a menos reciente, por lo que en la lista de análisis, los análisis del fichero subido aparecerán los primeros. En la lista de ficheros, el fichero aparecerá también el primero si es la primera vez que se sube a MARTA. En cambio, si ya había sido subido con anterioridad, aparecerá en la posición correspondiente a la fecha en la que se subió.

Cuando se sube un fichero a MARTA que ya había sido subido anteriormente (identificado por MD5), no se le vuelven a pasar los scripts estáticos. Sin embargo, sí que se le hará un análisis dinámico nuevo por cada máquina virtual seleccionada en cada sandbox.

## 8 VISTA DE REANÁLISIS DE UN BINARIO

Esta vista permite lanzar o programar uno o varios análisis dinámicos de un fichero.



**Crear Reanálisis para el binario con MD5: c4ffab85d84b494e1c450819a0e9c7db**

**Programación de los Reanálisis**

Fecha y Hora de Inicio del Primer Reanálisis  
Fecha: 03/10/2016 Hora: 16 : 57

Número de Análisis e Intervalo de Tiempo entre Análisis  
Nº Análisis: 1 Intervalo: 1 h : 00 m

☐ Incluir Triana  
☒ Enviar email al usuario validado  
☐ Enviar email a otra cuenta

☒ Cuckoo Sandbox ☐ Joe Sandbox

**Máquinas Virtuales**

- ☐ Windows XP x86
- ☐ Windows 7 x86
- ☐ Windows 8 x86
- ☐ Windows Server 2003 x86
- ☐ Windows Server 2008 x86

**Preferencias Básicas**

 Crear Reanálisis

## 8.1 CAMPOS DEL FORMULARIO

La vista de reanálisis está pensada para programar una cantidad de análisis dinámicos para un fichero cada cierto tiempo, a partir de una fecha y hora determinadas. En la sección **Fecha y Hora de Inicio del Primer Reanálisis** podemos elegir el momento en el que se iniciará la cadena de análisis programados, lanzándose el primer análisis. En la sección **Número de Análisis e Intervalo de Tiempo entre Análisis** podemos elegir cuántos análisis queremos programar, y cada cuánto tiempo se lanzará un análisis.

Por ejemplo, podemos programar 5 análisis, empezando el día 28/08/2015 a las 8:00, con un intervalo de tiempo de media hora entre cada uno de ellos:



Crear Reanálisis para el binario con MD5: 9f4efa767708af6badca6f60ad2006ae

**Programación de los Reanálisis**

Fecha y Hora de Inicio del Primer Reanálisis

Fecha: 28/08/2015 Hora: 08 : 00

Número de Análisis e Intervalo de Tiempo entre Análisis

Nº Análisis: 5 Intervalo: 0 h : 30 m

Sin embargo, como el caso más habitual es querer lanzar un análisis dinámico de un fichero inmediatamente, por defecto estos campos están rellenos para programar un único análisis en el momento actual:



Crear Reanálisis para el binario con MD5: 9f4efa767708af6badca6f60ad2006ae

**Programación de los Reanálisis**

Fecha y Hora de Inicio del Primer Reanálisis

Fecha: 27/08/2015 Hora: 13 : 57

Número de Análisis e Intervalo de Tiempo entre Análisis

Nº Análisis: 1 Intervalo: 1 h : 00 m

El resto de campos son idénticos a los ya descritos en la sección [Vista de Subida de un Binario](#). Si se seleccionan múltiples sandbox y/o máquinas virtuales, se creará una cadena de reanálisis por cada máquina virtual seleccionada en cada sandbox.

## 8.2 CREACIÓN DE LOS REANÁLISIS

Una vez seleccionados todos los campos, hacemos clic en el botón **Crear Reanálisis**. Esto hará que se programen todos los análisis dinámicos con las opciones elegidas. Los análisis programados para una fecha y hora iguales o anteriores al momento actual, se lanzarán inmediatamente.



**Crear Reanálisis para el binario con MD5: c4ffab85d84b494e1c450819a0e9c7db**

**Programación de los Reanálisis**

Fecha y Hora de Inicio del Primer Reanálisis  
Fecha: 03/10/2016 Hora: 16 : 57

Número de Análisis e Intervalo de Tiempo entre Análisis  
Nº Análisis: 1 Intervalo: 1 h : 00 m

☐ Incluir Triana  
☒ Enviar email al usuario validado  
☐ Enviar email a otra cuenta

☒ Cuckoo Sandbox ☐ Joe Sandbox

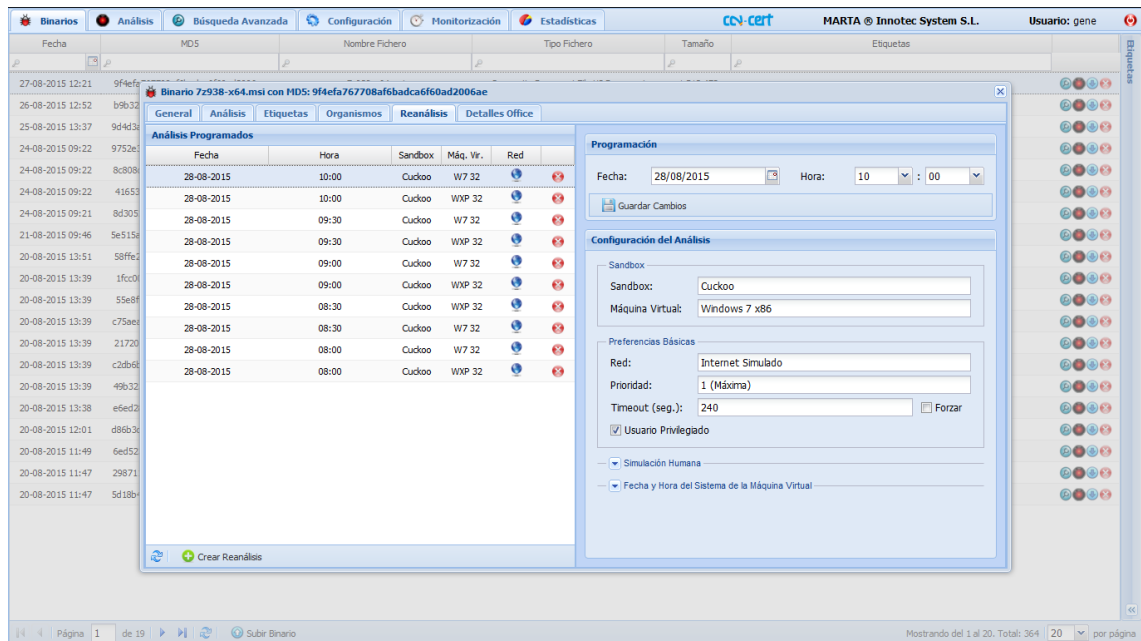
**Máquinas Virtuales**

- ☐ Windows XP x86
- ☐ Windows 7 x86
- ☐ Windows 8 x86
- ☐ Windows Server 2003 x86
- ☐ Windows Server 2008 x86

**Preferencias Básicas**

 Crear Reanálisis

Podemos consultar los reanálisis programados de un fichero en su **Vista de Detalles de un Binario**:



**Binario 72938-x64.msi con MD5: 9f4efa767708af6badca6f60ad2006ae**

| Fecha      | Hora  | Sandbox | Máq. Vr. | Red |
|------------|-------|---------|----------|-----|
| 28-08-2015 | 10:00 | Cuckoo  | W7 32    |     |
| 28-08-2015 | 10:00 | Cuckoo  | WXP 32   |     |
| 28-08-2015 | 09:30 | Cuckoo  | W7 32    |     |
| 28-08-2015 | 09:30 | Cuckoo  | WXP 32   |     |
| 28-08-2015 | 09:00 | Cuckoo  | W7 32    |     |
| 28-08-2015 | 09:00 | Cuckoo  | WXP 32   |     |
| 28-08-2015 | 08:30 | Cuckoo  | WXP 32   |     |
| 28-08-2015 | 08:30 | Cuckoo  | W7 32    |     |
| 28-08-2015 | 08:00 | Cuckoo  | W7 32    |     |
| 28-08-2015 | 08:00 | Cuckoo  | WXP 32   |     |

**Programación**

Fecha: 28/08/2015 Hora: 10 : 00

**Configuración del Análisis**

Sandbox: Cuckoo

Máquina Virtual: Windows 7 x86

**Preferencias Básicas**

Red: Internet Simulado

Prioridad: 1 (Máxima)

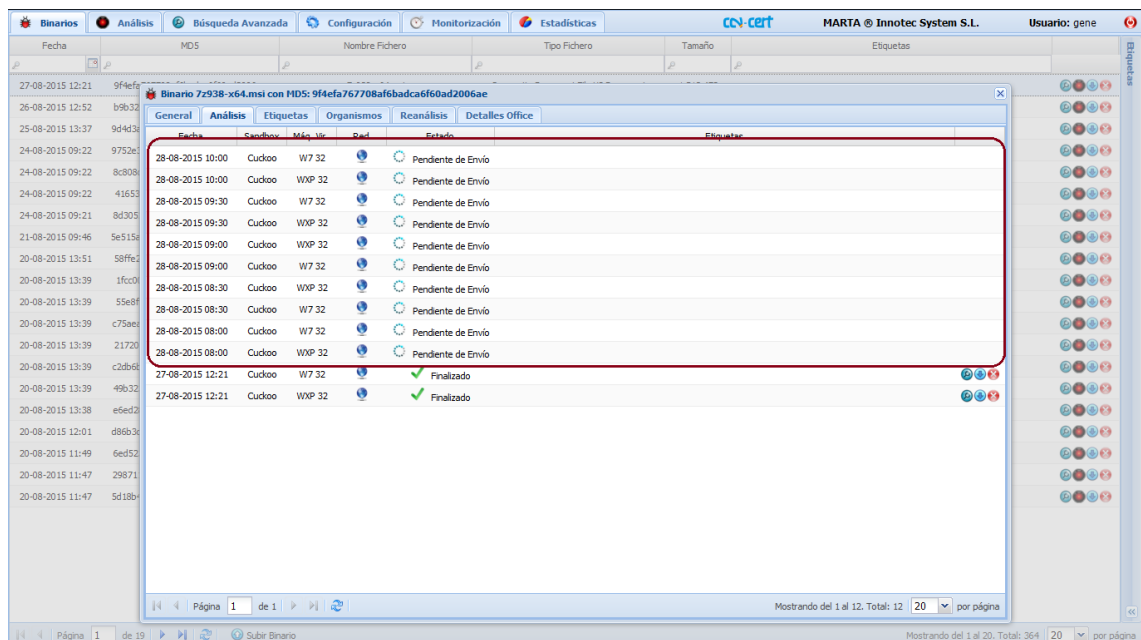
Timeout (seg.): 240 ☐ Forzar

☒ Usuario Privilegiado

☐ Simulación Humana

☐ Fecha y Hora del Sistema de la Máquina Virtual

Además, estos también aparecen en la lista de análisis de la propia Vista de Detalles del Binario:



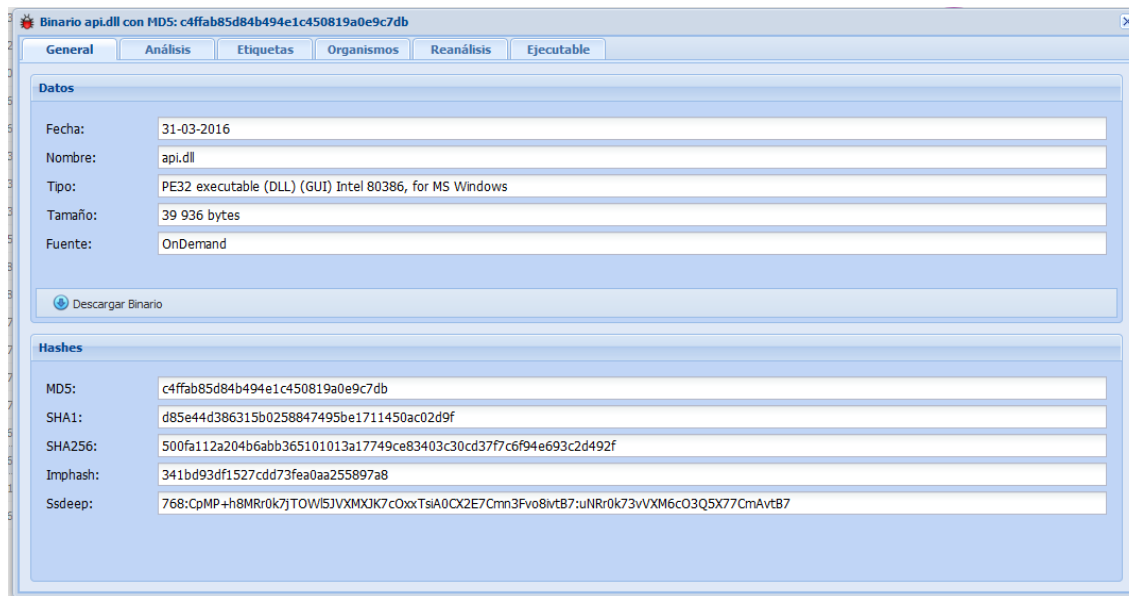
| Fecha            | Sandbox | Máq. Vr. | Red | Estado             |
|------------------|---------|----------|-----|--------------------|
| 28-08-2015 10:00 | Cuckoo  | W7 32    |     | Pendiente de Envío |
| 28-08-2015 10:00 | Cuckoo  | WXP 32   |     | Pendiente de Envío |
| 28-08-2015 09:30 | Cuckoo  | W7 32    |     | Pendiente de Envío |
| 28-08-2015 09:30 | Cuckoo  | WXP 32   |     | Pendiente de Envío |
| 28-08-2015 09:00 | Cuckoo  | WXP 32   |     | Pendiente de Envío |
| 28-08-2015 09:00 | Cuckoo  | W7 32    |     | Pendiente de Envío |
| 28-08-2015 08:30 | Cuckoo  | WXP 32   |     | Pendiente de Envío |
| 28-08-2015 08:30 | Cuckoo  | W7 32    |     | Pendiente de Envío |
| 28-08-2015 08:00 | Cuckoo  | W7 32    |     | Pendiente de Envío |
| 28-08-2015 08:00 | Cuckoo  | WXP 32   |     | Pendiente de Envío |
| 27-08-2015 12:21 | Cuckoo  | W7 32    |     | Finalizado         |
| 27-08-2015 12:21 | Cuckoo  | WXP 32   |     | Finalizado         |

Y también en la pestaña de análisis de MARTA:

| MARTA © Innotec System S.L. Usuario: gene |                                  |                                      |         |           |     |                    |           |  |  |
|-------------------------------------------|----------------------------------|--------------------------------------|---------|-----------|-----|--------------------|-----------|--|--|
| Fecha                                     | MDS                              | Nombre Fichero                       | Sandbox | Máq. Vir. | Red | Estado             | Etiquetas |  |  |
| 28-08-2015 10:00                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | WXP 32    |     | Pendiente de Envío |           |  |  |
| 28-08-2015 10:00                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | W7 32     |     | Pendiente de Envío |           |  |  |
| 28-08-2015 09:30                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | WXP 32    |     | Pendiente de Envío |           |  |  |
| 28-08-2015 09:30                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | W7 32     |     | Pendiente de Envío |           |  |  |
| 28-08-2015 09:00                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | WXP 32    |     | Pendiente de Envío |           |  |  |
| 28-08-2015 09:00                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | W7 32     |     | Pendiente de Envío |           |  |  |
| 28-08-2015 08:30                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | W7 32     |     | Pendiente de Envío |           |  |  |
| 28-08-2015 08:30                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | WXP 32    |     | Pendiente de Envío |           |  |  |
| 28-08-2015 08:00                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | WXP 32    |     | Pendiente de Envío |           |  |  |
| 28-08-2015 08:00                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | W7 32     |     | Pendiente de Envío |           |  |  |
| 27-08-2015 13:32                          | 00128613c86c0b9e23332eca1f99ba3  | Vacio.docx                           | Joe     | W7 32     |     | Error en la Resp.  |           |  |  |
| 27-08-2015 12:26                          | 4c3d0d155b1f3f2dd7cc1d2e5f64c8f9 | null.exe                             | Cuckoo  | W8 32     |     | Finalizado         |           |  |  |
| 27-08-2015 12:21                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | W7 32     |     | Finalizado         |           |  |  |
| 27-08-2015 12:21                          | 9f4efa767708af6badca6f60ad2006ae | 7z938-v64.msi                        | Cuckoo  | WXP 32    |     | Finalizado         |           |  |  |
| 27-08-2015 12:03                          | 4c3d0d155b1f3f2dd7cc1d2e5f64c8f9 | null.exe                             | Cuckoo  | W8 32     |     | Finalizado         |           |  |  |
| 27-08-2015 11:58                          | 4c3d0d155b1f3f2dd7cc1d2e5f64c8f9 | null.exe                             | Cuckoo  | W8 32     |     | Finalizado         |           |  |  |
| 27-08-2015 11:54                          | 4c3d0d155b1f3f2dd7cc1d2e5f64c8f9 | null.exe                             | Cuckoo  | W8 32     |     | Finalizado         |           |  |  |
| 27-08-2015 08:56                          | 4c3d0d155b1f3f2dd7cc1d2e5f64c8f9 | null.exe                             | Cuckoo  | W8 32     |     | Finalizado         |           |  |  |
| 27-08-2015 08:52                          | 4c3d0d155b1f3f2dd7cc1d2e5f64c8f9 | null.exe                             | Cuckoo  | W8 32     |     | Finalizado         |           |  |  |
| 26-08-2015 13:09                          | 9752e333a26646bcd208e2b8f2554e88 | 04e8052934ef4fce688669feabe2d018f... | Cuckoo  | WXP 32    |     | Finalizado         |           |  |  |

## 9 VISTA DE DETALLE DE UN BINARIO

Esta vista contiene toda la **información** relativa a un **fichero** subido a MARTA.



Dispone de múltiples pestañas:

- **General:** Muestra información básica acerca del fichero.
- **Análisis:** Muestra todos los análisis dinámicos realizados y programados del fichero.
- **Etiquetas:** Muestra y permite gestionar las etiquetas asociadas al fichero.
- **Organismos:** Muestra y permite gestionar los organismos relacionados con el fichero.
- **Reanálisis:** Muestra y permite gestionar los reanálisis programados del fichero.

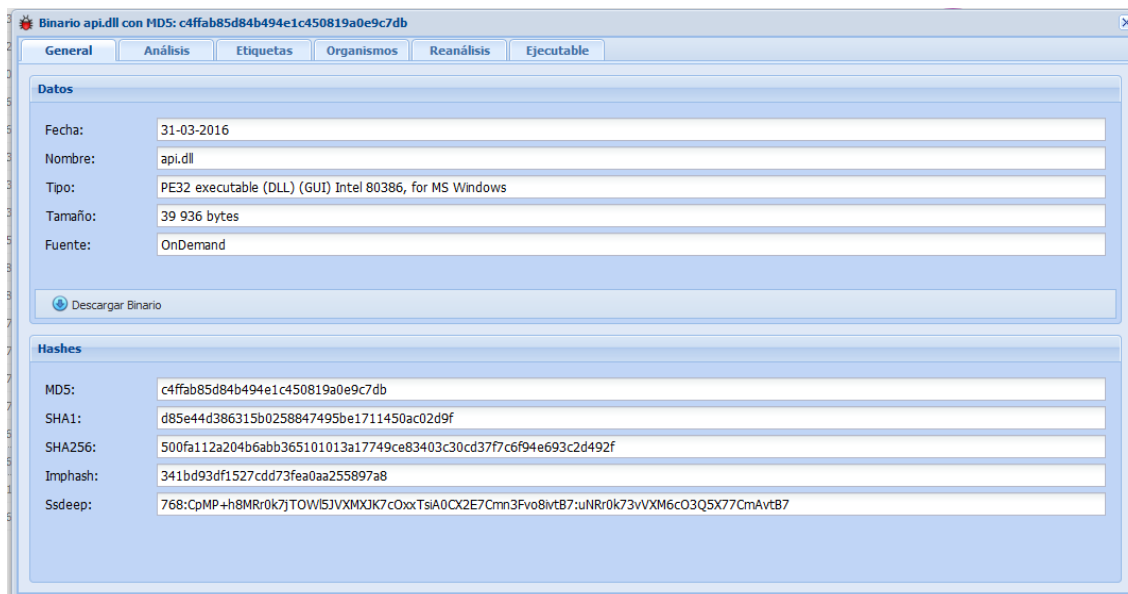
En función del tipo de fichero, aparecerá una pestaña más, diferente para cada tipo, mostrando toda la información extraída por los **scripts estáticos**.

- **Detalles Ejecutable:** Aparece sólo si el fichero es un ejecutable, como por ejemplo un exe, un msi, un bat, etc.
- **Detalles PDF:** Aparece sólo si el fichero es un pdf.
- **Detalles Office:** Aparece sólo si el fichero es un documento de Microsoft Office, como por ejemplo, un doc, un docx, un xlsx, un pptx, etc.

- **Detalles OpenOffice:** Aparece sólo si el fichero es un documento de OpenOffice, como por ejemplo, un odt.

## 9.1 GENERAL

Muestra **información básica acerca del fichero**: la fecha en la que se subió a MARTA, su nombre, su tipo, tu tamaño, la fuente (esto indica si se subió manualmente, "OnDemand", o si fue recolectado por un colector), y sus hashes: MD5, SHA1, SHA256, Imphash y Ssdeep.



The screenshot shows a web application window titled 'Binario api.dll con MD5: c4ffab85d84b494e1c450819a0e9c7db'. It has several tabs: 'General', 'Análisis', 'Etiquetas', 'Organismos', 'Reanálisis', and 'Ejecutable'. The 'General' tab is active, displaying the following information:

| Datos   |                                                         |
|---------|---------------------------------------------------------|
| Fecha:  | 31-03-2016                                              |
| Nombre: | api.dll                                                 |
| Tipo:   | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows |
| Tamaño: | 39 936 bytes                                            |
| Fuente: | OnDemand                                                |

Below the data table is a button labeled 'Descargar Binario' with a download icon. Underneath is a section titled 'Hashes' containing the following values:

|          |                                                                                         |
|----------|-----------------------------------------------------------------------------------------|
| MD5:     | c4ffab85d84b494e1c450819a0e9c7db                                                        |
| SHA1:    | d85e44d386315b0258847495be1711450ac02d9f                                                |
| SHA256:  | 500fa112a204b6abb365101013a17749ce83403c30cd37f7c6f94e693c2d492f                        |
| Imphash: | 341bd93df1527cdd73fea0aa255897a8                                                        |
| Ssdeep:  | 768:CpMP+h8MRr0k7JTOW/5JvXMXJK7cOxxTsiA0CX2E7Cmn3Fvo8ivtB7:uNRr0k73vVXM6c03Q5X77CmAvtB7 |

Además, permite descargar el binario con el botón  **Descargar Binario**. Esta acción debe realizarse con precaución ya que el fichero descargado podría ser un malware. El fichero se descarga con su MD5 como nombre, y con extensión .binary, para evitar que lo ejecutemos por error al descargarlo.

## 9.2 ANÁLISIS

Muestra una **lista** con todos los **análisis dinámicos** realizados y programados **del fichero**, muy similar a la de la pestaña de análisis de la vista principal de la aplicación.

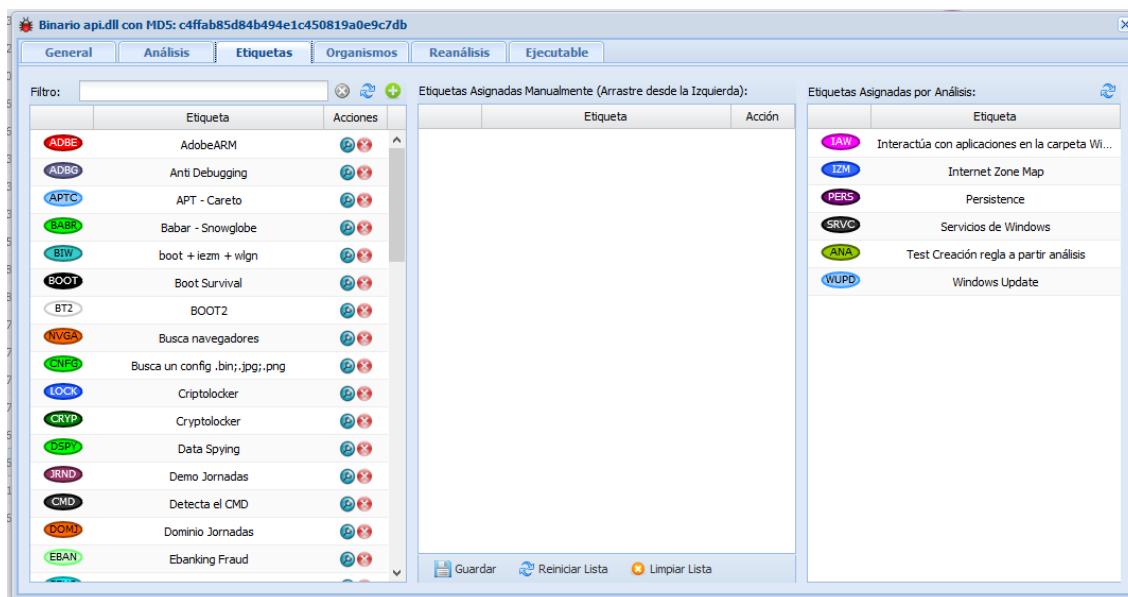
| MARTA © Innotec System S.L. Usuario: user_ccn |           |                                  |                       |         |           |     |            |           |      |          |
|-----------------------------------------------|-----------|----------------------------------|-----------------------|---------|-----------|-----|------------|-----------|------|----------|
| Fecha                                         | Organismo | MDS                              | Nombre Fichero        | Sandbox | Máq. Vir. | Red | Estado     | Etiquetas |      | Acciones |
| 04-10-2016 09:07                              | CCN       | 7c78f16f7db7a94ba070e2002de32833 | curl.exe              | Cuckoo  | WXP 32    | ✓   | Finalizado |           |      |          |
| 03-10-2016 16:38                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll               | Cuckoo  | W7 32     | ✓   | Finalizado |           |      |          |
| 03-10-2016 16:38                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll               | Cuckoo  | WXP 32    | ✓   | Finalizado |           |      |          |
| 03-10-2016 16:38                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll               | Cuckoo  | W7 32     | ✓   | Finalizado |           |      |          |
| 03-10-2016 16:38                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll               | Cuckoo  | WXP 32    | ✓   | Finalizado |           |      |          |
| 03-10-2016 14:57                              | CCN       | 4c3d0d155b1f3f3dd7cc1d2e5f4c8f9  | null.binary           | Cuckoo  | WXP 32    | ✓   | Finalizado |           |      |          |
| 03-10-2016 12:00                              | CCN       | 1472d0f7765fd2b2a302a77b2b065574 | informeMartaEXE.docx  | Cuckoo  | WXP 32    | ✓   | Finalizado |           |      |          |
| 03-10-2016 10:22                              | CCN       | ca7d59508fab164c26bc3371c3a1c4   | irc.exe               | Cuckoo  | W7 32     | ✓   | Finalizado | BTW       | EXL  |          |
| 03-10-2016 10:22                              | CCN       | ca7d59508fab164c26bc3371c3a1c4   | irc.exe               | Cuckoo  | WXP 32    | ✓   | Finalizado | BTW       | EXL  |          |
| 30-09-2016 11:00                              | CCN       | 438e9520d8e0e487e79f328e41f7e04  | TestMemoryFinal.exe   | Joe     | W7 32     | ✓   | Finalizado |           |      |          |
| 30-09-2016 11:00                              | CCN       | 438e9520d8e0e487e79f328e41f7e04  | TestMemoryFinal.exe   | Joe     | W7 64     | ✓   | Finalizado |           |      |          |
| 30-09-2016 10:58                              | CCN       | 9a3076f030741ef0322542ba6021b3ae | procesos.exe          | Cuckoo  | WXP 32    | ✓   | Finalizado |           |      |          |
| 30-09-2016 10:57                              | CCN       | 6a78093d68fe09f27feb369615b56cdf | persistence-files.exe | Joe     | W7 64     | ✓   | Finalizado | 12M       | PERS | 1AW      |
| 30-09-2016 10:31                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll               | Joe     | W7 32     | ✓   | Finalizado | 12M       | PERS | 1AW      |
| 30-09-2016 10:31                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll               | Joe     | W7 64     | ✓   | Finalizado | 12M       | PERS | 1AW      |
| 30-09-2016 10:20                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll               | Joe     | W7 32     | ✓   | Finalizado | 12M       | PERS | 1AW      |
| 30-09-2016 10:20                              | CCN       | c4ffab85d84b494e1c450819a0e9c7db | api.dll               | Joe     | W7 64     | ✓   | Finalizado | 12M       | PERS | 1AW      |
| 29-09-2016 11:53                              | CCN       | 6a78093d68fe09f27feb369615b56cdf | persistence-files.exe | Cuckoo  | W2k8 32   | ✓   | Solicitado |           |      |          |
| 29-09-2016 11:53                              | CCN       | 6a78093d68fe09f27feb369615b56cdf | persistence-files.exe | Cuckoo  | W2k3 32   | ✓   | Finalizado |           |      |          |
| 29-09-2016 11:53                              | CCN       | 6a78093d68fe09f27feb369615b56cdf | persistence-files.exe | Cuckoo  | W8 32     | ✓   | Finalizado |           |      |          |

Esta lista muestra los **atributos** más significativos de cada análisis: la fecha en la que se realizó (o para la que está programado), la sandbox, la máquina virtual, el tipo de red, el estado actual del análisis y sus etiquetas asociadas.

La última columna es de acciones. Permite realizar acciones sobre un análisis, similar a la de la pestaña de análisis de la vista principal de la aplicación. Véase la sección [Acciones sobre los Análisis](#).

### 9.3 ETIQUETAS

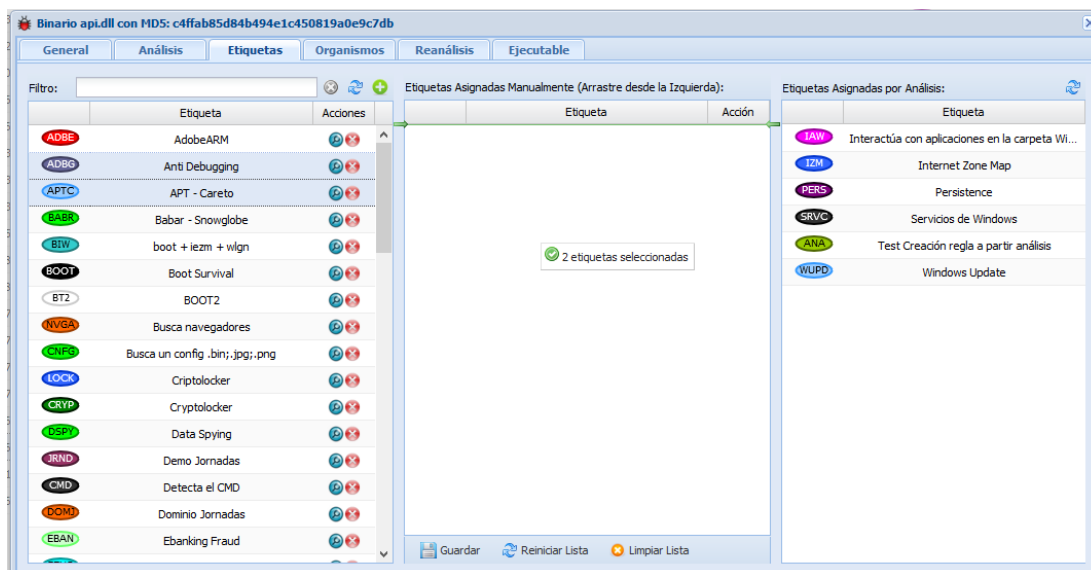
Muestra y permite gestionar las etiquetas asociadas al fichero.

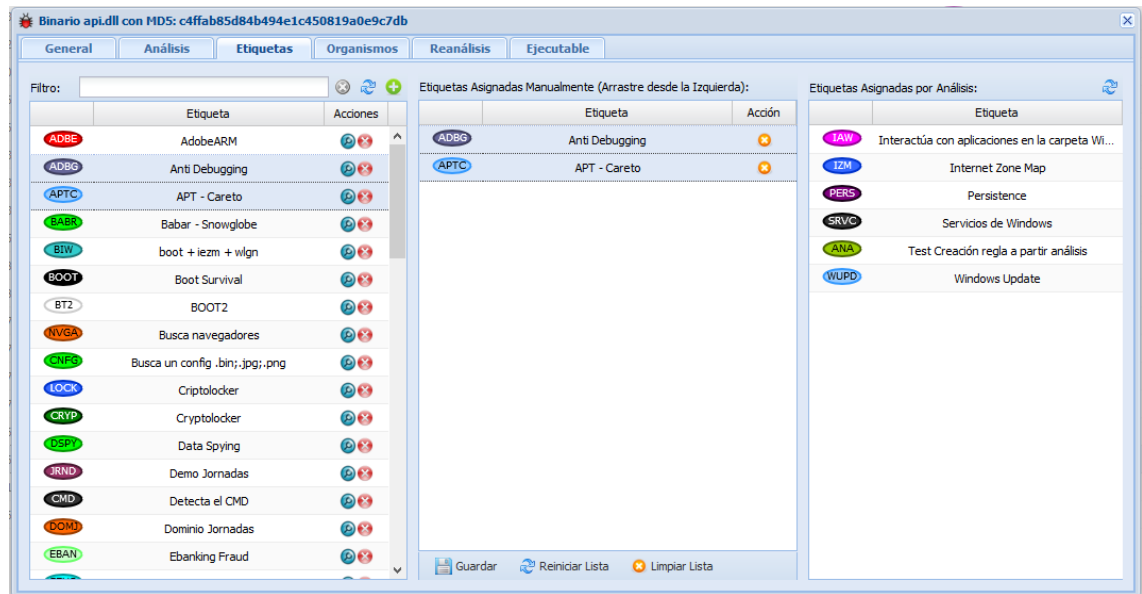


A modo de recordatorio: un fichero tiene asignadas todas las etiquetas que se le asignen manualmente, más todas las etiquetas que tengan asignadas todos sus análisis dinámicos.

La pestaña consta de tres listas:

- La lista de la izquierda muestra todas las etiquetas existentes y permite gestionarlas, de forma similar a la descrita en la sección [Etiquetas](#).
- La lista del centro muestra las etiquetas asignadas manualmente al fichero, y permite arrastrar desde o hacia la lista de la izquierda para añadir o quitar etiquetas.





También podemos quitar etiquetas de la lista clicando en la acción  **Quitar** de una etiqueta.

Debajo de la lista hay una barra de acciones, que permite las siguientes gestiones:

-  **Guardar:** Guarda las etiquetas manualmente asignadas al fichero, tal y como esté la lista en el momento de clicar en el botón.
  -  **Reiniciar Lista:** Reinicia la lista a las etiquetas que tenga el fichero asignadas manualmente en el momento de clicar en el botón.
  -  **Limpiar Lista:** Quita todas las etiquetas de la lista, pero no las desasigna del fichero (a no ser que a continuación hagamos clic en el botón Guardar).
- La lista de la derecha muestra las etiquetas asociadas al fichero debido a las etiquetas asociadas a sus análisis. Esta lista no es modificable. Es posible consultar concretamente qué etiquetas vienen de cada análisis desde la pestaña de Análisis:

Binario api.dll con MD5: c4ffab85d84b494e1c450819a0e9c7db

| General          |         | Análisis  | Etiquetas | Organismos   | Reanálisis        | Ejecutable |
|------------------|---------|-----------|-----------|--------------|-------------------|------------|
| Fecha            | Sandbox | Máq. Vir. | Red       | Estado       | Etiquetas         | Acciones   |
| 09-05-2016 15:10 | Joe     | WXP 32    |           | ✓ Finalizado | PERS IAW          |            |
| 09-05-2016 15:10 | Cuckoo  | WXP 32    |           | ✓ Finalizado | IZM SRVC WUPD ANA |            |
| 27-04-2016 19:23 | Cuckoo  | WXP 32    |           | ✓ Finalizado | IZM SRVC          |            |
| 27-04-2016 19:03 | Cuckoo  | WXP 32    |           | ✓ Finalizado | IZM SRVC WUPD     |            |
| 27-04-2016 19:03 | Cuckoo  | W2k3 32   |           | ✓ Finalizado | IZM SRVC          |            |
| 27-04-2016 19:03 | Cuckoo  | W8 32     |           | ✓ Finalizado | IZM SRVC          |            |
| 27-04-2016 19:03 | Cuckoo  | W7 32     |           | ✓ Finalizado | IZM SRVC          |            |
| 27-04-2016 19:03 | Cuckoo  | W2k8 32   |           | ✓ Finalizado | IZM SRVC          |            |
| 26-04-2016 10:34 | Cuckoo  | WXP 32    |           | ✓ Finalizado | IZM SRVC WUPD     |            |
| 05-04-2016 10:29 | Cuckoo  | WXP 32    |           | ✓ Finalizado | IZM SRVC          |            |
| 31-03-2016 10:16 | Cuckoo  | WXP 32    |           | ✓ Finalizado | IZM SRVC          |            |
| 31-03-2016 10:16 | Joe     | WXP 32    |           | ✓ Finalizado | PERS IAW          |            |

Página 1 de 1

Mostrando del 1 al 12. Total: 12 20 por página

## 9.4 REANÁLISIS

Muestra y permite gestionar los reanálisis programados del fichero.

Binario api.dll con MD5: c4ffab85d84b494e1c450819a0e9c7db

| General    |       | Análisis | Etiquetas | Organismos | Reanálisis | Ejecutable |
|------------|-------|----------|-----------|------------|------------|------------|
| Fecha      | Hora  | Sandbox  | Máq. Vir. | Red        | Acción     |            |
| 12-05-2016 | 19:29 | Joe      | WXP 32    |            |            |            |
| 12-05-2016 | 19:29 | Cuckoo   | W7 32     |            |            |            |
| 12-05-2016 | 19:29 | Cuckoo   | WXP 32    |            |            |            |
| 12-05-2016 | 19:29 | Joe      | W7 32     |            |            |            |
| 12-05-2016 | 17:29 | Joe      | WXP 32    |            |            |            |
| 12-05-2016 | 17:29 | Cuckoo   | W7 32     |            |            |            |
| 12-05-2016 | 17:29 | Cuckoo   | WXP 32    |            |            |            |
| 12-05-2016 | 17:29 | Joe      | W7 32     |            |            |            |
| 12-05-2016 | 15:29 | Joe      | WXP 32    |            |            |            |
| 12-05-2016 | 15:29 | Cuckoo   | W7 32     |            |            |            |
| 12-05-2016 | 15:29 | Cuckoo   | WXP 32    |            |            |            |
| 12-05-2016 | 15:29 | Joe      | W7 32     |            |            |            |
| 12-05-2016 | 13:29 | Joe      | WXP 32    |            |            |            |
| 12-05-2016 | 13:29 | Cuckoo   | W7 32     |            |            |            |
| 12-05-2016 | 13:29 | Cuckoo   | WXP 32    |            |            |            |
| 12-05-2016 | 13:29 | Joe      | W7 32     |            |            |            |

Crear Reanálisis

**Programación**

Fecha: 12/05/2016 Hora: 19 : 29

Guardar Cambios

**Configuración del Análisis**

**Sandbox**

Sandbox: Cuckoo

Máquina Virtual: Windows 7 x86

**Preferencias Básicas**

Red: Internet Simulado

Prioridad: 1 (Máxima)

Timeout (seg.): 240 ☐ Forzar

☒ Usuario Privilegiado

☐ Simulación Humana

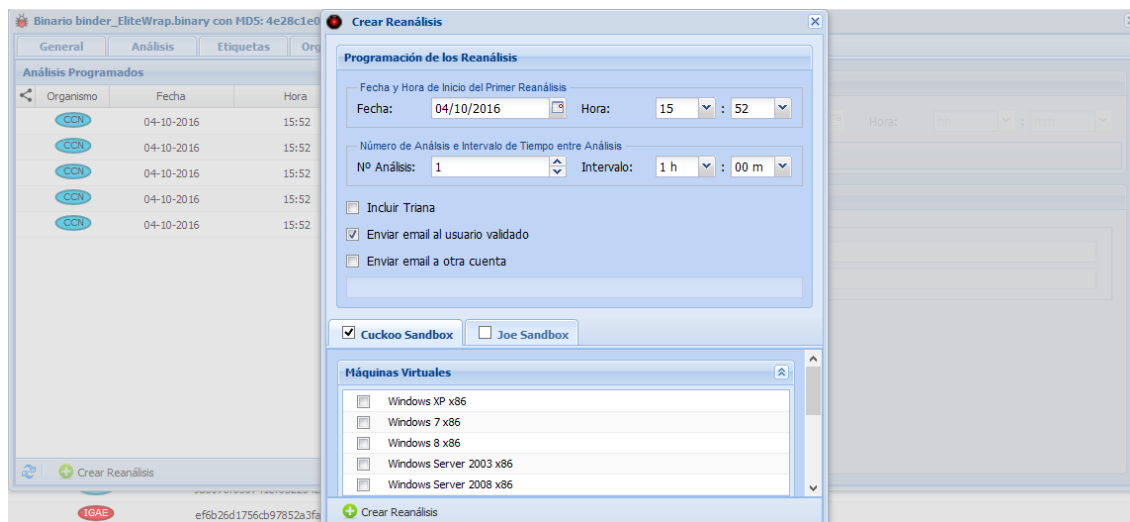
☐ Fecha y Hora del Sistema de la Máquina Virtual

En la parte de la izquierda, se muestra una lista con todos los reanálisis programados, con la fecha y hora para la que están programados, la sandbox, la máquina virtual y el tipo de red.

Si seleccionamos uno, en la parte de la derecha se muestran todos los detalles de la programación del análisis. La fecha y hora pueden ser modificados.

Un reanálisis programado puede ser eliminado clicando en la acción **Eliminar** de la lista de la izquierda. Se pide confirmación antes de eliminarlo.

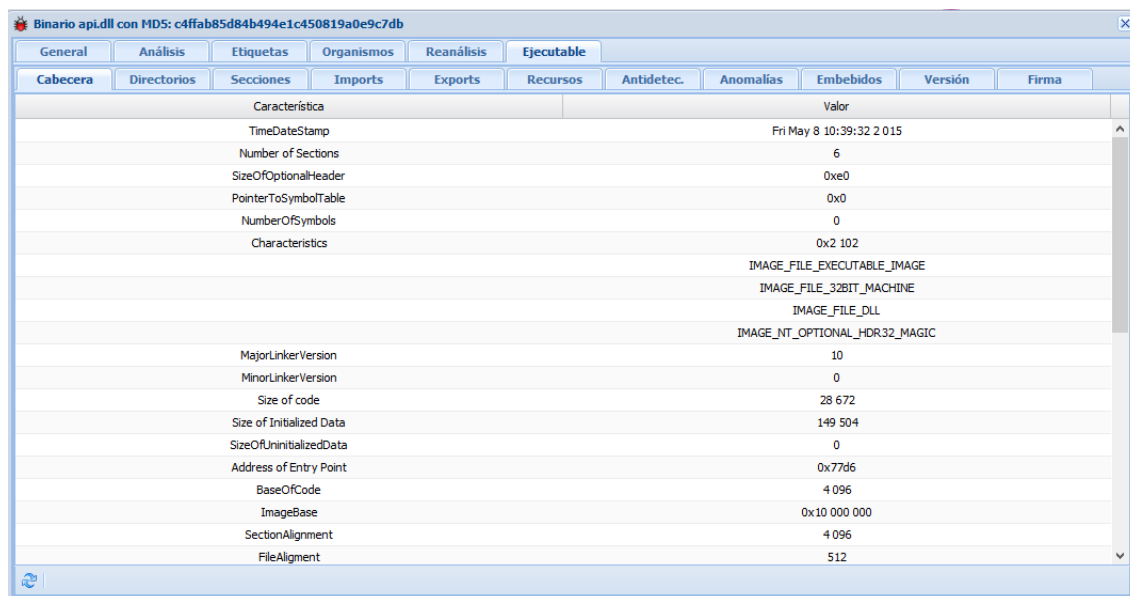
Podemos crear un reanálisis nuevo clicando en el botón  **Crear Reanálisis** de la barra de herramientas inferior de la lista de la izquierda. Esto abrirá la **vista de reanálisis**.



## 9.5 DETALLES EJECUTABLE

Esta pestaña aparece sólo si el fichero es un ejecutable, como por ejemplo un exe, un msi, un bat, etc. Muestra toda la información extraída por los **scripts estáticos** acerca del fichero.

- **Info. Cabecera:** Muestra toda la información extraíble de la cabecera del ejecutable.



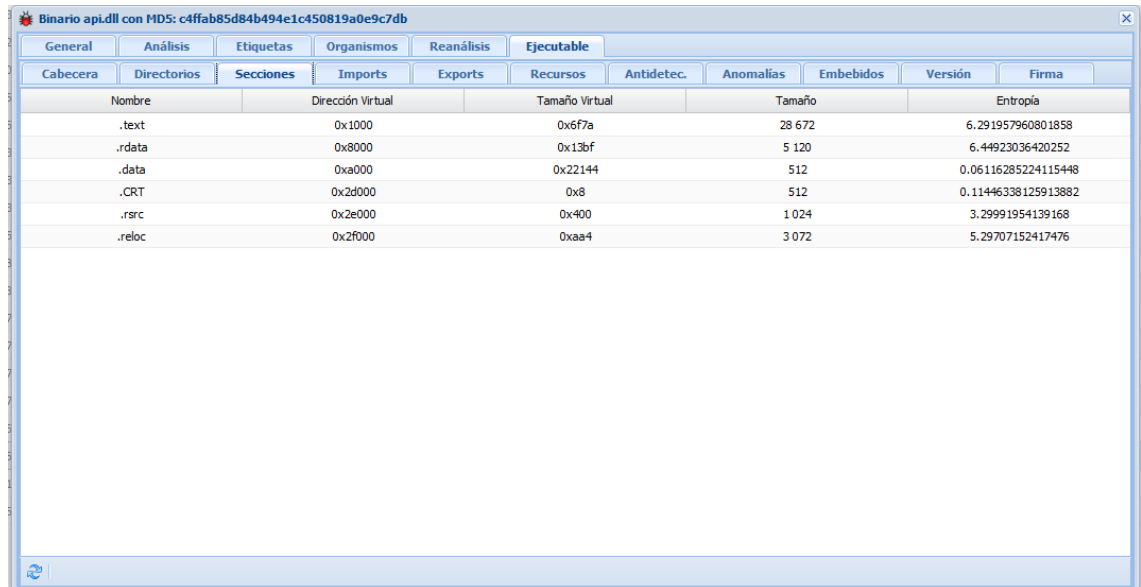
| Característica           | Valor                         |
|--------------------------|-------------------------------|
| TimeDateStamp            | Fri May 8 10:39:32 2015       |
| Number of Sections       | 6                             |
| SizeOfOptionalHeader     | 0xe0                          |
| PointerToSymbolTable     | 0x0                           |
| NumberOfSymbols          | 0                             |
| Characteristics          | 0x2 102                       |
|                          | IMAGE_FILE_EXECUTABLE_IMAGE   |
|                          | IMAGE_FILE_32BIT_MACHINE      |
|                          | IMAGE_FILE_DLL                |
|                          | IMAGE_NT_OPTIONAL_HDR32_MAGIC |
| MajorLinkerVersion       | 10                            |
| MinorLinkerVersion       | 0                             |
| Size of code             | 28 672                        |
| Size of Initialized Data | 149 504                       |
| SizeOfUninitializedData  | 0                             |
| Address of Entry Point   | 0x77d6                        |
| BaseOfCode               | 4 096                         |
| ImageBase                | 0x10 000 000                  |
| SectionAlignment         | 4 096                         |
| FileAlignment            | 512                           |

- **Tabla Directorios:** Muestra información sobre la tabla de directorios del ejecutable.

Binario api.dll con MD5: c4ffab85d84b494e1c450819a0e9c7db

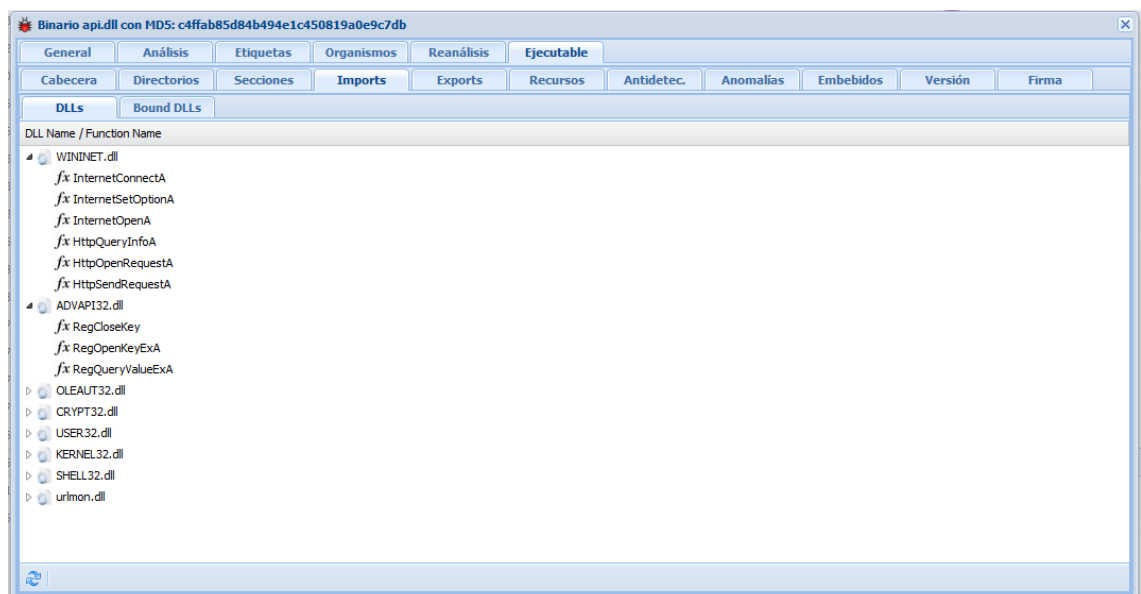
| General   | Análisis    | Etiquetas         | Organismos | Reanálisis | Ejecutable |             |           |           |         |       |  |
|-----------|-------------|-------------------|------------|------------|------------|-------------|-----------|-----------|---------|-------|--|
| Cabecera  | Directorios | Secciones         | Imports    | Exports    | Recursos   | Antidetect. | Anomalías | Embebidos | Versión | Firma |  |
| Nombre    |             | Dirección Virtual |            |            |            |             |           |           | Tamaño  |       |  |
| EXPORTS   |             | 37616             |            |            |            |             |           |           | 207     |       |  |
| IMPORT    |             | 35940             |            |            |            |             |           |           | 180     |       |  |
| RESOURCE  |             | 188416            |            |            |            |             |           |           | 1 024   |       |  |
| BASERELOC |             | 192512            |            |            |            |             |           |           | 2 052   |       |  |
| IAT       |             | 32768             |            |            |            |             |           |           | 300     |       |  |

- **Secciones:** Muestra información sobre las secciones del ejecutable.



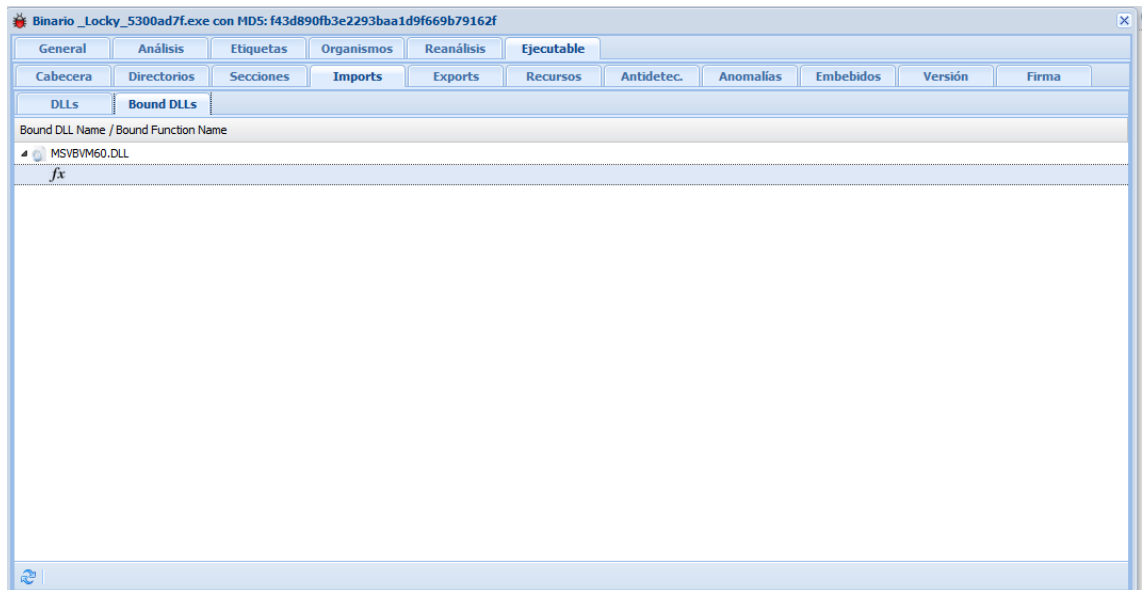
| Nombre | Dirección Virtual | Tamaño Virtual | Tamaño | Entropía            |
|--------|-------------------|----------------|--------|---------------------|
| .text  | 0x1000            | 0x6f7a         | 28 672 | 6.291957960801858   |
| .rdata | 0x8000            | 0x13bf         | 5 120  | 6.44923036420252    |
| .data  | 0xa000            | 0x22144        | 512    | 0.06116285224115448 |
| .CRT   | 0x2d000           | 0x8            | 512    | 0.11446338125913882 |
| .rsrc  | 0x2e000           | 0x400          | 1 024  | 3.29991954139168    |
| .reloc | 0x2f000           | 0xaa4          | 3 072  | 5.29707152417476    |

- **Imports.** Esta sección se compone de dos partes:
  - o **DLLs:** Muestra información sobre las librerías importadas por el ejecutable, y las funciones de dichas librerías.

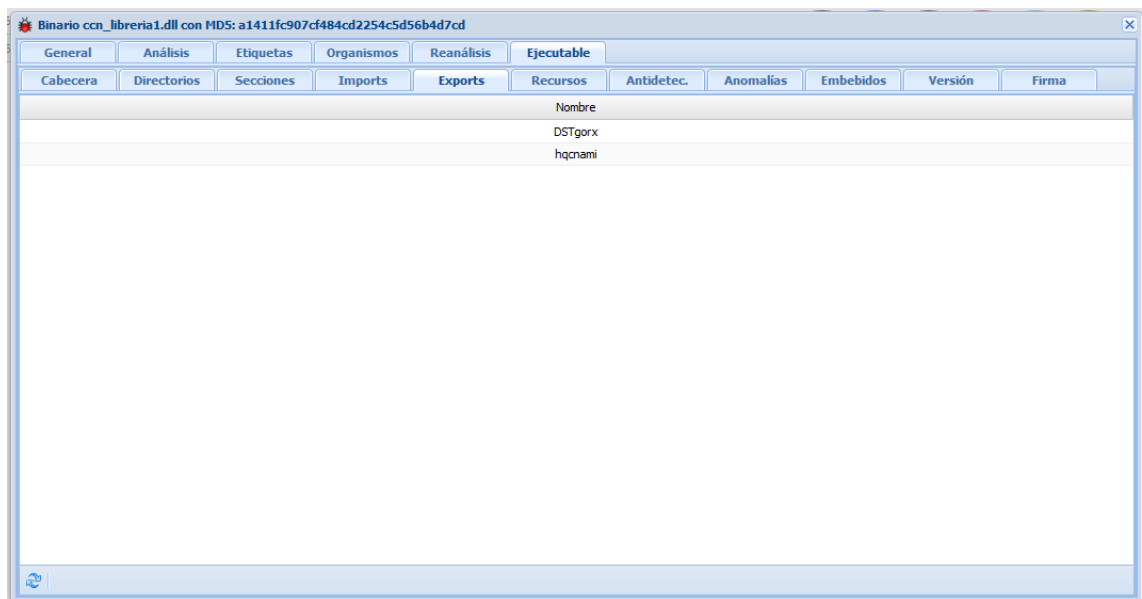


| DLL Name / Function Name |
|--------------------------|
| WININET.dll              |
| fx InternetConnectA      |
| fx InternetSetOptionA    |
| fx InternetOpenA         |
| fx HttpQueryInfoA        |
| fx HttpOpenRequestA      |
| fx HttpSendRequestA      |
| ADVAPI32.dll             |
| fx RegCloseKey           |
| fx RegOpenKeyExA         |
| fx RegQueryValueExA      |
| OLEAUT32.dll             |
| CRYPT32.dll              |
| USER32.dll               |
| KERNEL32.dll             |
| SHELL32.dll              |
| urlmon.dll               |

- **Bound DLLs:** Muestra información sobre las librerías bindeadas al ejecutable, y las funciones de dichas librerías.



- **Exports:** Muestra información sobre los exports del ejecutable.

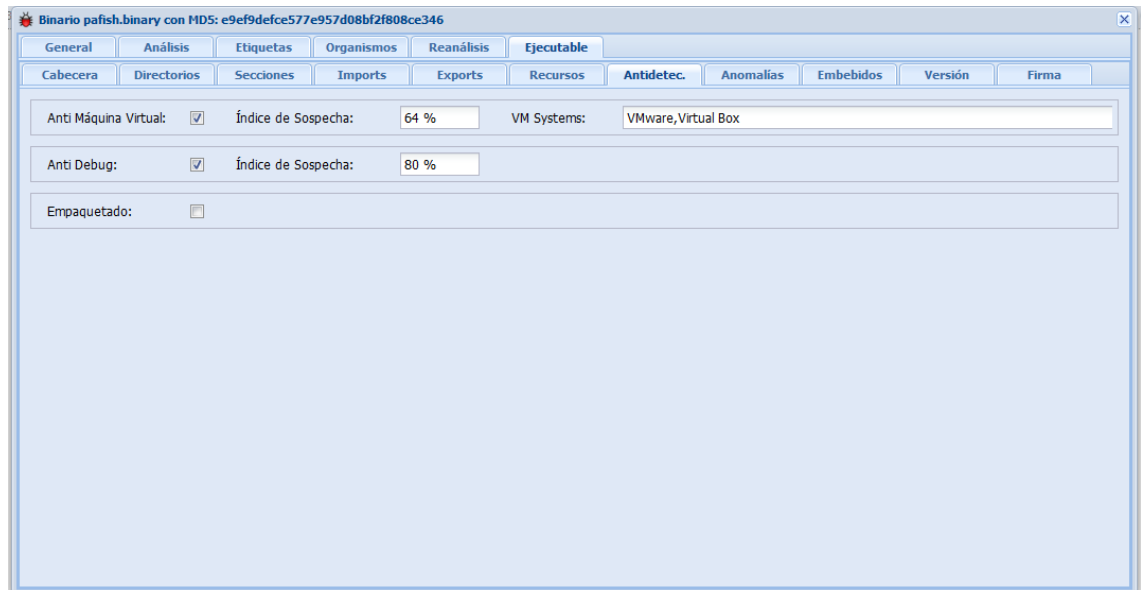


- **Recursos:** Muestra información sobre los recursos del ejecutable.

Binario 94b80736e79ac8846bde9ef1e99a8c80 con MD5: 94b80736e79ac8846bde9ef1e99a8c80

| General            | Análisis    | Etiquetas     | Organismos | Reanálisis         | Ejecutable |               |           |             |         |       |  |
|--------------------|-------------|---------------|------------|--------------------|------------|---------------|-----------|-------------|---------|-------|--|
| Cabecera           | Directorios | Secciones     | Imports    | Exports            | Recursos   | Antidetect.   | Anomalías | Embebidos   | Versión | Firma |  |
| Nombre del Recurso |             | Lenguaje      |            | Sublenguaje        |            | Codigo Página |           | Ocurrencias |         |       |  |
| RT_ICON            |             | LANG_ROMANIAN |            | SUBLANG_ROMANIAN   |            | 0             |           | 5           |         |       |  |
| RT_DIALOG          |             | LANG_ENGLISH  |            | SUBLANG_ENGLISH_US |            | 0             |           | 3           |         |       |  |
| RT_DIALOG          |             | LANG_ROMANIAN |            | SUBLANG_ROMANIAN   |            | 0             |           | 2           |         |       |  |
| RT_VERSION         |             | LANG_ENGLISH  |            | SUBLANG_ENGLISH_US |            | 0             |           | 1           |         |       |  |
| RT_GROUP_ICON      |             | LANG_ROMANIAN |            | SUBLANG_ROMANIAN   |            | 0             |           | 1           |         |       |  |
| RT_ICON            |             | LANG_ENGLISH  |            | SUBLANG_ENGLISH_US |            | 0             |           | 1           |         |       |  |
| RT_GROUP_ICON      |             | LANG_ENGLISH  |            | SUBLANG_ENGLISH_US |            | 0             |           | 1           |         |       |  |

- **Técnicas Antidetección:** Muestra información sobre las técnicas antidetección del ejecutable.



- **Anomalías:** Muestra información sobre las anomalías del ejecutable.



- **Ficheros Embebidos:** Muestra información sobre los ficheros embebidos del ejecutable.

Binario ping.binary con MD5: 6e9739b317fb6daacd482ce69c26b390

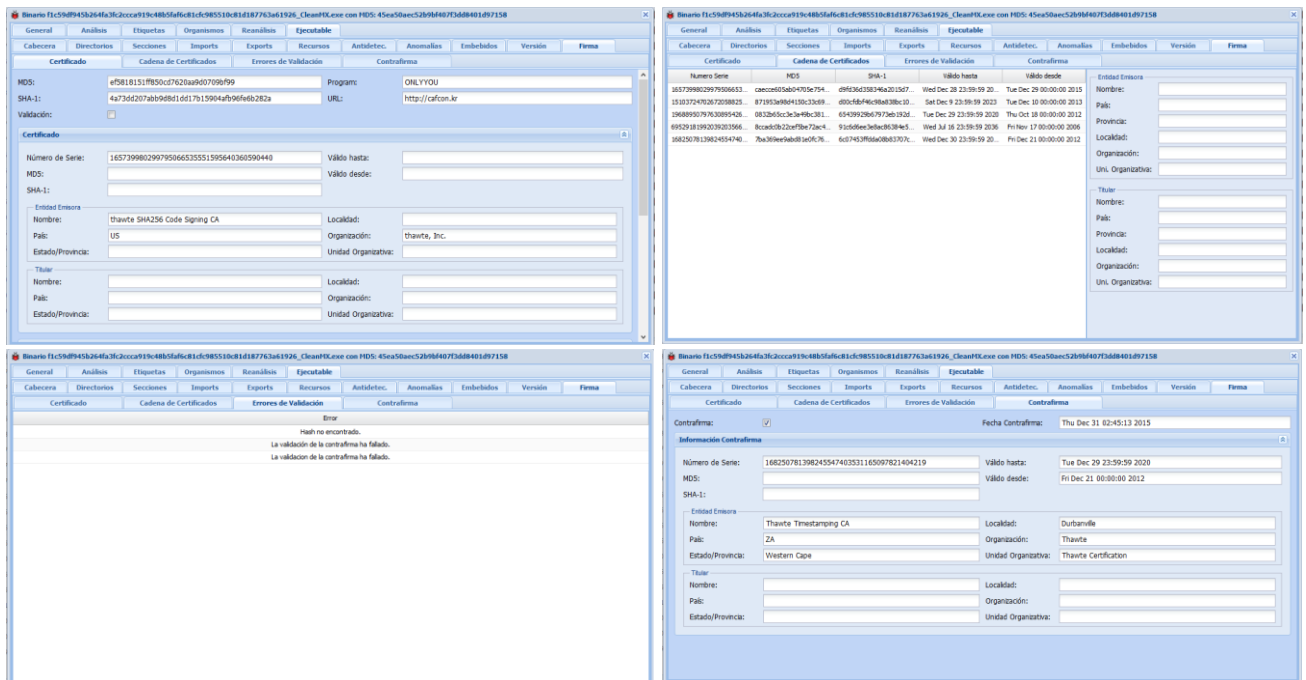
| Ejecutable                       |                       |                    |                                                       |         |
|----------------------------------|-----------------------|--------------------|-------------------------------------------------------|---------|
| Cabecera                         | Directorios           | Secciones          | Imports                                               | Exports |
| MD5                              | Tipo MIME             | Tamaño del Fichero | Tipo de Fichero                                       | Acción  |
| bb23c728d346448a392e9a8ed53a97f2 | application/x-dosexec | 2459648            | PE32 executable (console) Intel 80386, for MS Windows |         |
| 324761ca06eb9e4350307780959d8ebd | application/x-dosexec | 910336             | PE32 executable (console) Intel 80386, for MS Windows |         |
| 637aabdf24be92e33f3e71367e6e6a5  | application/x-dosexec | 46080              | PE32 executable (console) Intel 80386, for MS Windows |         |
| 6ba1564cd78ddb62900ff3327c18587c | application/x-dosexec | 1315328            | PE32 executable (console) Intel 80386, for MS Windows |         |
| 3478581db4eb3865282562c277f28b0a | application/x-dosexec | 68608              | PE32 executable (console) Intel 80386, for MS Windows |         |
| 5602701b02f8f8cac446ad4e4e05c317 | application/x-dosexec | 10240              | PE32 executable (console) Intel 80386, for MS Windows |         |
| ab90ebdeb35afd592dca1e3d7023da80 | application/x-dosexec | 686080             | PE32 executable (console) Intel 80386, for MS Windows |         |

- **Versión:** Muestra información sobre la versión del ejecutable.

Binario \_Locky\_5300ad7f.exe con MD5: f43d890fb3e2293baa1d9f669b79162f

| Versión                      |                 |
|------------------------------|-----------------|
| Copyright Legal:             |                 |
| Nombre Interno:              | Bolgsektor3     |
| Versión del Fichero:         | 1.00            |
| Nombre de la Compañía:       | Halon Krusk     |
| Marcas Registradas:          |                 |
| Comentarios:                 | Ropewalker2     |
| Nombre del Producto:         | Statuering0     |
| Versión del Producto:        | 1.00            |
| Descripción del Fichero:     | Reimmigrant1    |
| Nombre Original del Fichero: | Bolgsektor3.exe |

- **Información de Firma:** Muestra información sobre la firma del ejecutable.



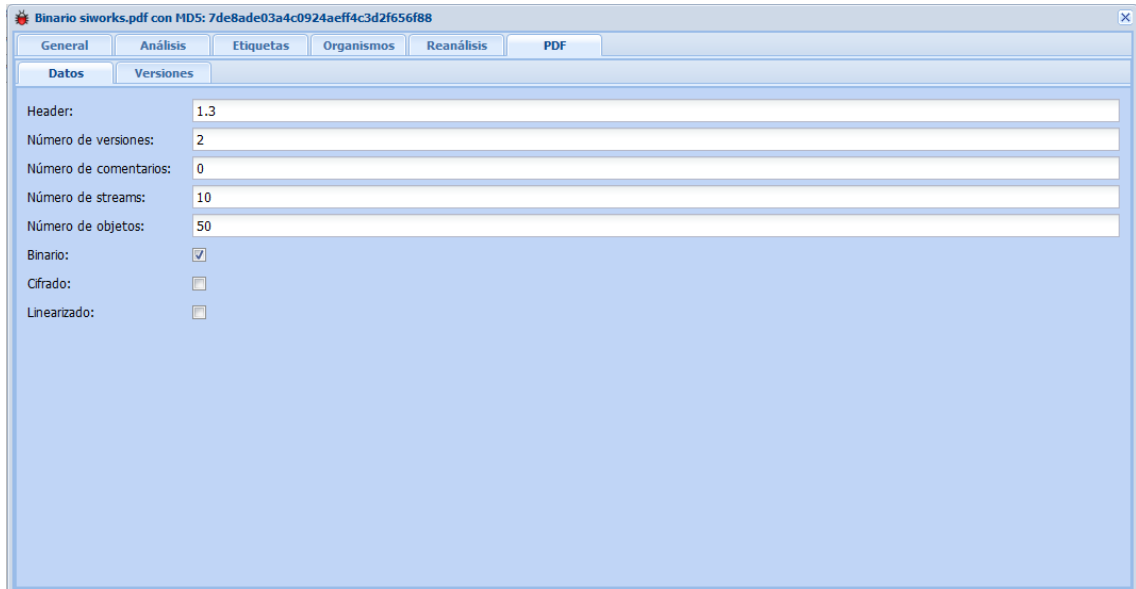
The screenshots show the 'Firma' tab in the MARTA application, which displays digital signature information for an executable file. The interface includes a menu bar with options like General, Análisis, Etiquetas, Organismos, Recursos, Análisis, Ejecutable, and Firma. The main content area is divided into several sections:

- General:** Displays the MD5 hash (e9818131f850c762ba940709f99) and the SHA-1 hash (4a736d207ab698d1d117915994af96f6282a). It also shows the program name (ONLYYOU) and the URL (http://crl.com.kr).
- Certificado:** Shows the certificate details, including the number of series (16573998029979506633551595640360590448), the MD5 hash, and the SHA-1 hash. It also displays the issuer information (thawte SHA256 Code Signing CA) and the subject information (thawte, Inc.).
- Errores de Validación:** Displays a list of validation errors, such as 'Hash no encontrado' and 'La validación de la contrasigna ha fallado'.
- Contrafirma:** Shows the counter-signature details, including the number of series (16825078139824554740331165007821404219), the MD5 hash, and the SHA-1 hash. It also displays the issuer information (Thawte Timestamping CA) and the subject information (Thawte Certification).

## 9.6 DETALLES PDF

Esta pestaña aparece sólo si el fichero es un pdf. Muestra toda la información extraída por los *scripts estáticos* acerca del fichero.

- **Datos:** Muestra datos generales acerca del documento pdf.



Binario siworks.pdf con MD5: 7de8ade03a4c0924aeff4c3d2f656f88

General | Análisis | Etiquetas | Organismos | Reanálisis | PDF

Datos | Versiones

Header: 1.3

Número de versiones: 2

Número de comentarios: 0

Número de streams: 10

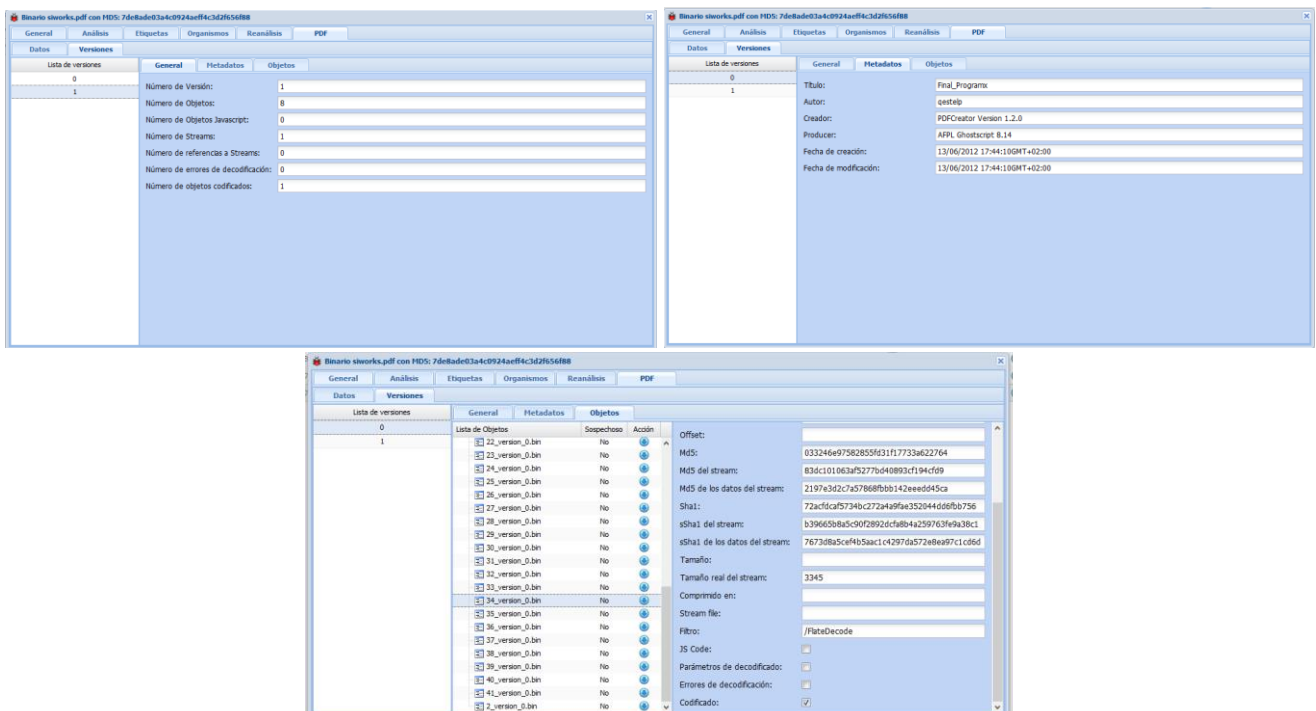
Número de objetos: 50

Binario: ☒

Cifrado: ☐

Linearizado: ☐

- **Versiones:** Muestra una lista con todas las versiones del documento pdf. Seleccionando cada versión, muestra sus datos generales, sus metadatos y sus objetos embebidos.



Binario siworks.pdf con MD5: 7de8ade03a4c0924aeff4c3d2f656f88

General | Análisis | Etiquetas | Organismos | Reanálisis | PDF

Datos | Versiones

Lista de versiones

| General                          | Metadatos                          | Objetos                                |
|----------------------------------|------------------------------------|----------------------------------------|
| Número de Versión: 1             | Número de Objetos: 8               | Número de Objetos Javascript: 0        |
| Número de Streams: 1             | Número de referencias a Streams: 0 | Número de errores de decodificación: 0 |
| Número de objetos codificados: 1 |                                    |                                        |

Binario siworks.pdf con MD5: 7de8ade03a4c0924aeff4c3d2f656f88

General | Análisis | Etiquetas | Organismos | Reanálisis | PDF

Datos | Versiones

Lista de versiones

| General                                         | Metadatos                                           | Objetos                  |
|-------------------------------------------------|-----------------------------------------------------|--------------------------|
| Título: Final_Programe                          | Autor: questip                                      | PDFCreator Version 1.2.0 |
| Fecha de creación: 13/06/2012 17:44:10GMT+02:00 | Fecha de modificación: 13/06/2012 17:44:10GMT+02:00 |                          |

Binario siworks.pdf con MD5: 7de8ade03a4c0924aeff4c3d2f656f88

General | Análisis | Etiquetas | Organismos | Reanálisis | PDF

Datos | Versiones

Lista de versiones

| General          | Metadatos | Objetos | Suspectos | Acción |
|------------------|-----------|---------|-----------|--------|
| 22_version_0_bin | No        |         |           |        |
| 23_version_0_bin | No        |         |           |        |
| 24_version_0_bin | No        |         |           |        |
| 25_version_0_bin | No        |         |           |        |
| 26_version_0_bin | No        |         |           |        |
| 27_version_0_bin | No        |         |           |        |
| 28_version_0_bin | No        |         |           |        |
| 29_version_0_bin | No        |         |           |        |
| 30_version_0_bin | No        |         |           |        |
| 31_version_0_bin | No        |         |           |        |
| 32_version_0_bin | No        |         |           |        |
| 33_version_0_bin | No        |         |           |        |
| 34_version_0_bin | No        |         |           |        |
| 35_version_0_bin | No        |         |           |        |
| 36_version_0_bin | No        |         |           |        |
| 37_version_0_bin | No        |         |           |        |
| 38_version_0_bin | No        |         |           |        |
| 39_version_0_bin | No        |         |           |        |
| 40_version_0_bin | No        |         |           |        |
| 41_version_0_bin | No        |         |           |        |
| 42_version_0_bin | No        |         |           |        |

Offset: 03246e97582855f31f17733a222764

MD5: 83dc101063a5277b040893cf194cf09

MD5 del stream: 2197e3d2c7a57868fbb142eeed045ca

MD5 de los datos del stream: 72acfdca5734bc272a49fa3252044d68fb756

Sha1: b39665b8a5c90f2892dcf8b4a259763f9a38c1

sha1 de los datos del stream: 76730ba5ca4b5aac1c42970a572e8ea97c1c0bd

Tamaño: 3345

Tamaño real del stream: 3345

Comprimido en: Stream file

Filtro: /FlateDecode

JS Code: ☐

Parámetros de decodificación: ☐

Errores de decodificación: ☐

Codificado: ☒



## 9.7 DETALLES OFFICE

Esta pestaña aparece sólo si el fichero es un documento de Microsoft Office, como por ejemplo, un doc, un docx, un xlsx, un pptx, etc. Muestra toda la información extraída por los *scripts estáticos* acerca del fichero.

- **Datos:** Muestra datos generales acerca del documento, y sus metadatos.

The screenshot shows the 'Office' tab in the MARTA application. The window title is 'Binario 6dd18e5b601406cfad3f076330cd63670d6e37a740530cba872d95a060b52dfb.doc con MD5: ba81bfe79fc31f4c2ef55ade47d0b1be'. The 'Office' tab is selected, and the 'Datos' sub-tab is active. The 'Datos' section contains the following fields:

| Field             | Value                               |
|-------------------|-------------------------------------|
| Aplicación:       | Microsoft Office Word               |
| Nº Objetos Flash: | 0                                   |
| Cifrado:          | <input type="checkbox"/>            |
| Info. de Sumario: | <input checked="" type="checkbox"/> |
| Pool de Objetos:  | <input type="checkbox"/>            |
| Formato OLE:      | <input checked="" type="checkbox"/> |
| Macros VBA:       | <input checked="" type="checkbox"/> |

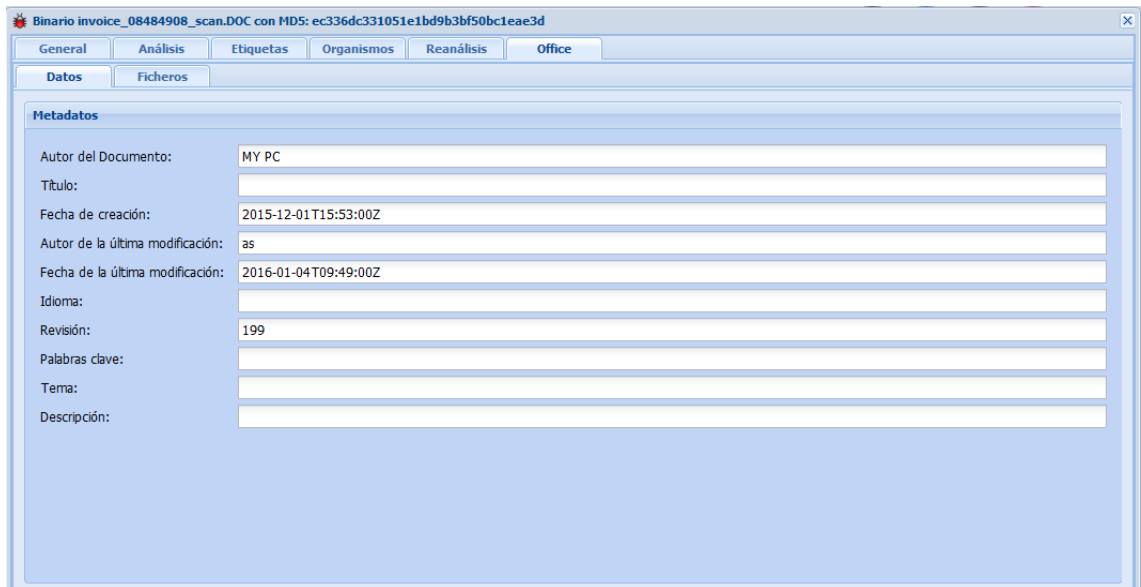
The 'Metadatos' section contains the following fields:

| Field                 | Value                 |
|-----------------------|-----------------------|
| Título:               |                       |
| Autor:                |                       |
| Compañía:             |                       |
| Aplic. de Creación:   | Microsoft Office Word |
| Modificado por:       |                       |
| Fecha de Creación:    | 2016-03-29 01:12:00   |
| Fecha de Modificac.:  | 2016-04-06 11:19:00   |
| Tiempo Total Edición: | 600                   |
| Versión:              | 730895                |
| Revisión:             | 12                    |
| Plantilla:            | Normal.dot            |
| Código de Página:     | 1251                  |
| Nº Caracteres:        | 29                    |
| Nº Caract. con Espac: | 33                    |
| Nº Líneas:            | 1                     |

## 9.8 DETALLES OPENOFFICE

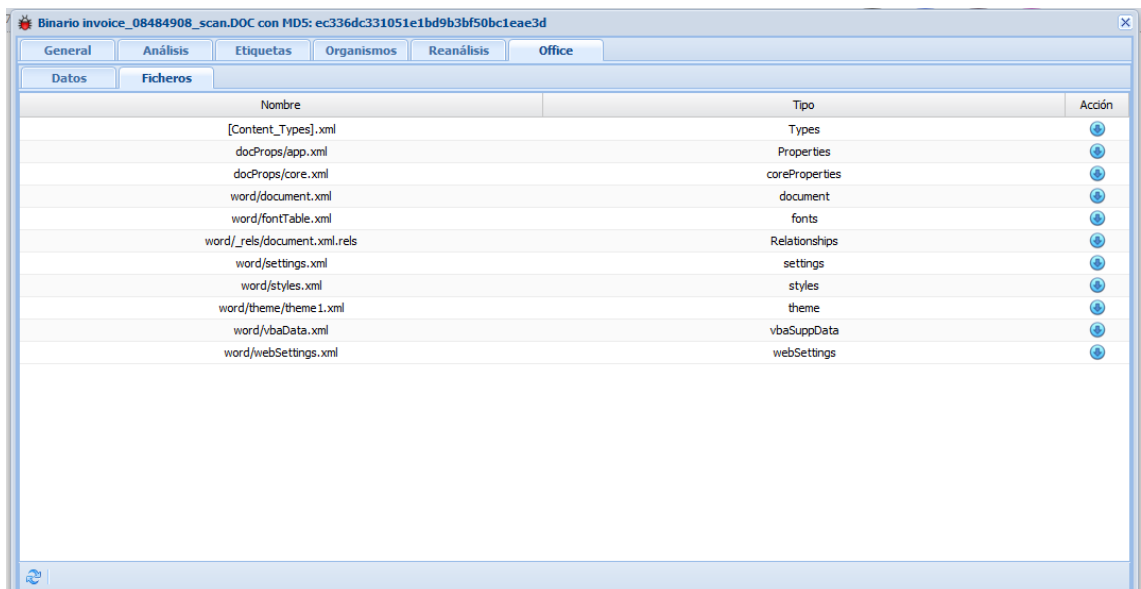
Esta pestaña aparece sólo si el fichero es un documento de OpenOffice, como por ejemplo, un odt. Muestra toda la información extraída por los *scripts estáticos* acerca del fichero.

- **Datos:** Muestra datos generales acerca del documento OpenOffice



| Metadatos                        |                      |
|----------------------------------|----------------------|
| Autor del Documento:             | MY PC                |
| Título:                          |                      |
| Fecha de creación:               | 2015-12-01T15:53:00Z |
| Autor de la última modificación: | as                   |
| Fecha de la última modificación: | 2016-01-04T09:49:00Z |
| Idioma:                          |                      |
| Revisión:                        | 199                  |
| Palabras clave:                  |                      |
| Tema:                            |                      |
| Descripción:                     |                      |

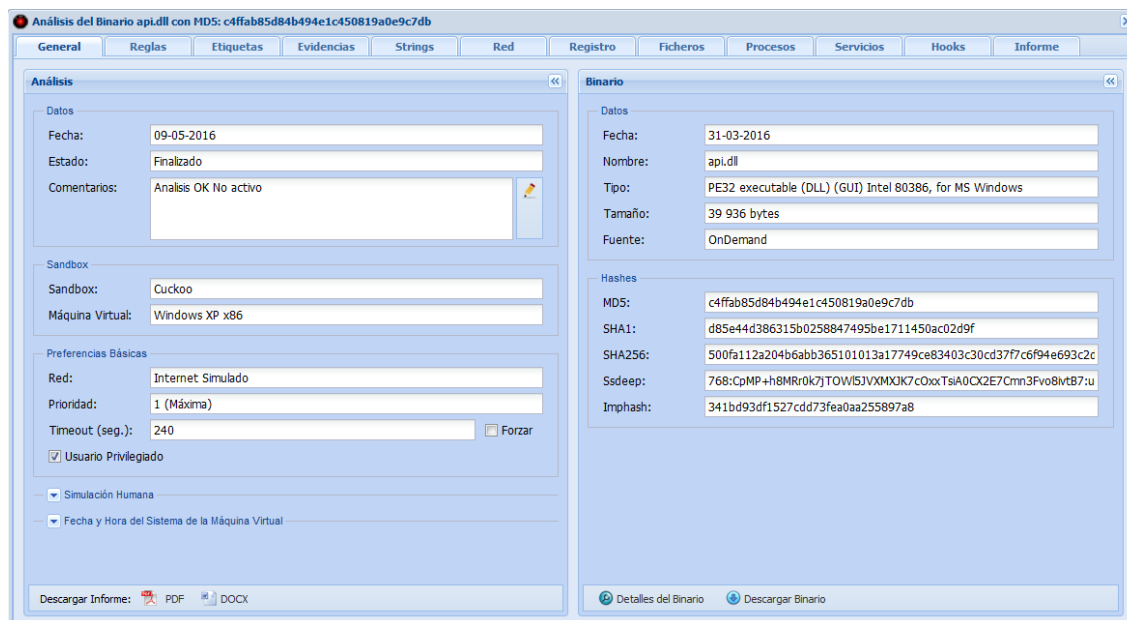
- **Ficheros:** Muestra una lista con todos los ficheros embebidos en el documento OpenOffice, y permite descargarlos:



| Nombre                       | Tipo           | Acción                                                                                |
|------------------------------|----------------|---------------------------------------------------------------------------------------|
| [Content_Types].xml          | Types          |  |
| docProps/app.xml             | Properties     |  |
| docProps/core.xml            | coreProperties |  |
| word/document.xml            | document       |  |
| word/fontTable.xml           | fonts          |  |
| word/_rels/document.xml.rels | Relationships  |  |
| word/settings.xml            | settings       |  |
| word/styles.xml              | styles         |  |
| word/theme/theme1.xml        | theme          |  |
| word/vbaData.xml             | vbaSuppData    |  |
| word/webSettings.xml         | webSettings    |  |

## 10 VISTA DE DETALLE DE UN ANÁLISIS

Esta vista contiene toda la **información** relativa a un **análisis dinámico** de un fichero subido a MARTA.



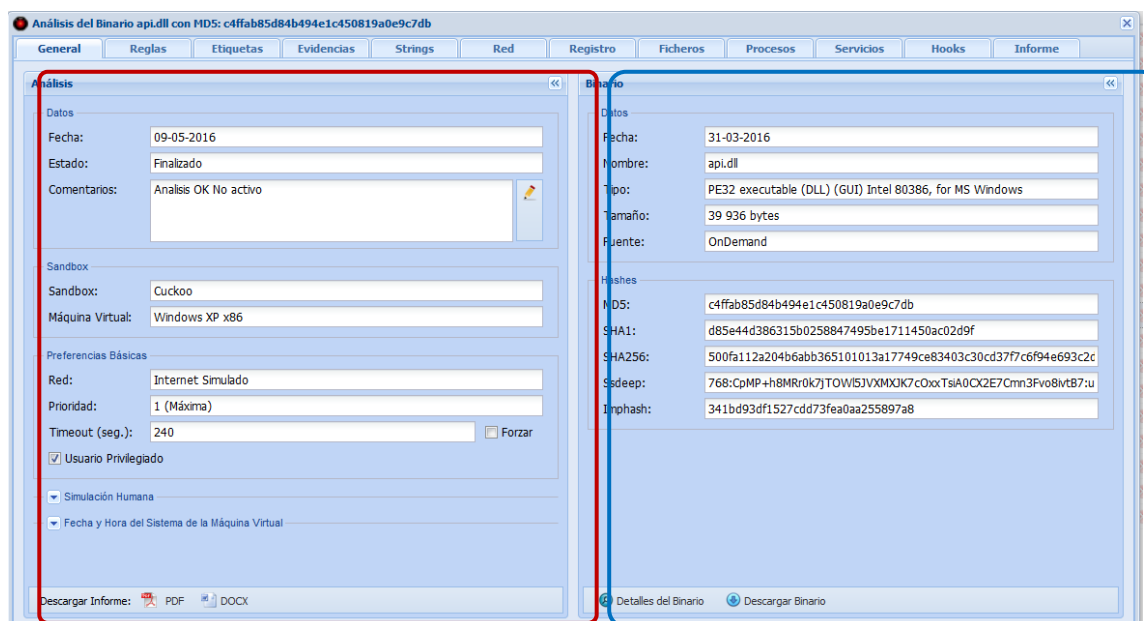
Dispone de múltiples pestañas:

- **General:** Muestra información básica acerca del análisis y del fichero analizado.
- **Reglas:** Muestra todas las reglas coincidentes con el análisis y permite generar reglas a partir de él.
- **Etiquetas:** Muestra y permite gestionar las etiquetas asociadas al análisis.
- **Evidencias:** Muestra una lista con diferentes recursos obtenidos por la sandbox durante la ejecución del análisis, como volcados de memoria o capturas de pantalla.
- **Strings:** Herramienta de búsqueda de cadenas de texto entre la memoria utilizada durante el análisis.
- **Red:** Muestra información acerca de las conexiones de red realizadas durante el análisis, agrupadas por protocolo.
- **Registro:** Muestra información acerca de las claves de registro abiertas, leídas, escritas y eliminadas durante el análisis.
- **Ficheros:** Muestra información acerca de los ficheros abiertos, leídos, escritos, eliminados, ejecutados, movidos y copiados durante el análisis.

- **Procesos:** Muestra información acerca de los procesos creados durante el análisis.
- **Servicios:** Muestra información acerca de los servicios de sistema operativo creados durante el análisis.
- **Informe:** Permite crear un informe a medida, eligiendo qué secciones se desea que aparezcan.

## 10.1 GENERAL

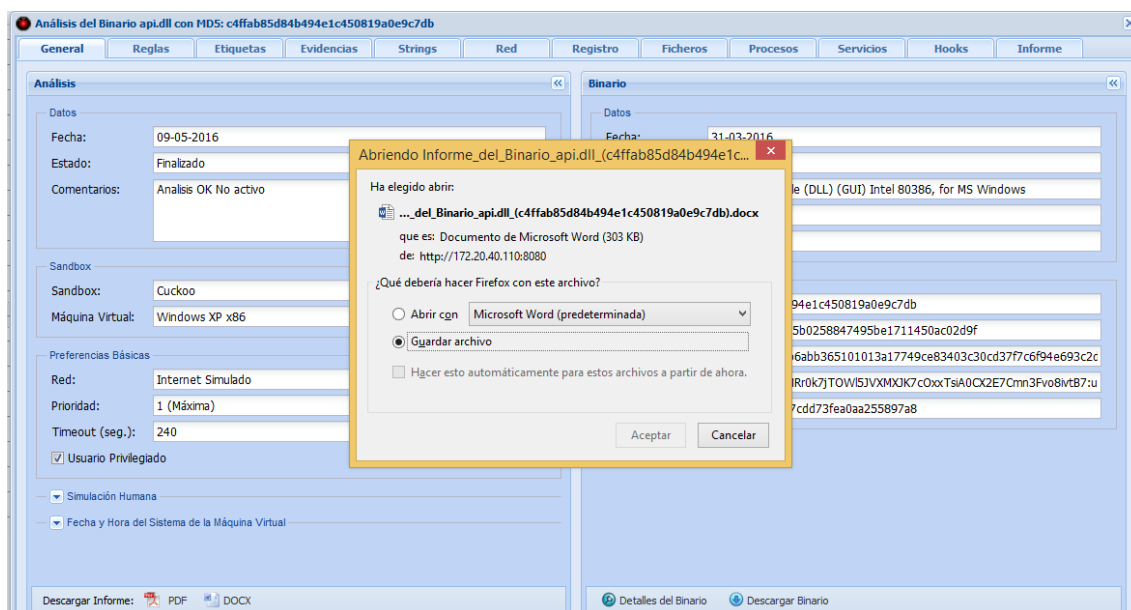
Muestra *información básica acerca del análisis y del fichero analizado*:



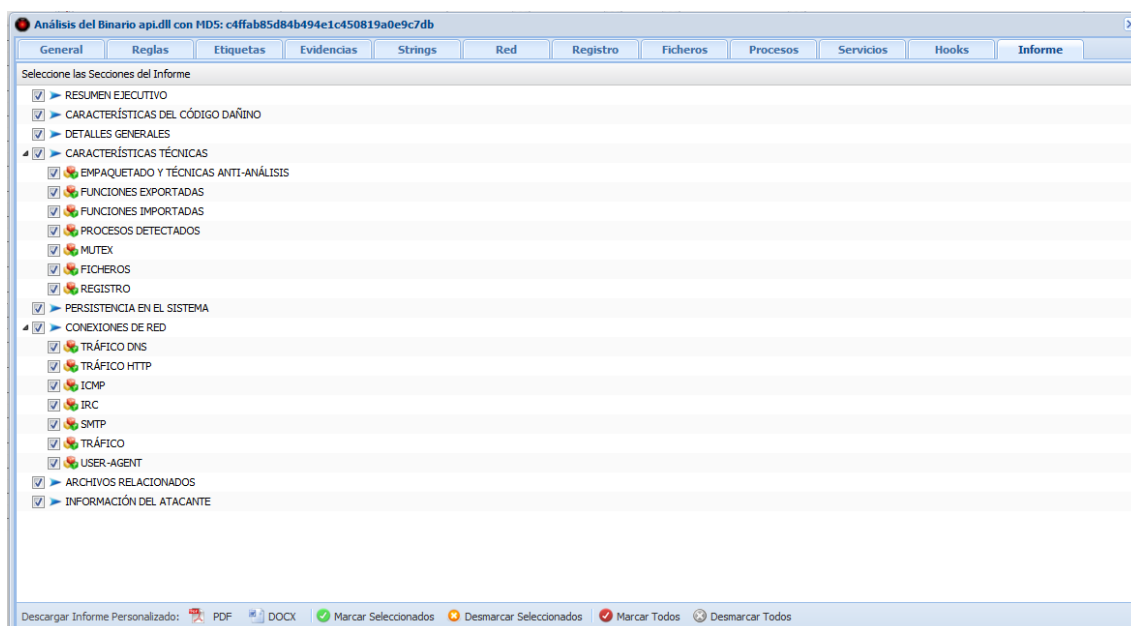
The screenshot shows the MARTA application interface with two main panels: 'Análisis' (left) and 'Binario' (right). The 'Análisis' panel is outlined in red and contains fields for 'Fecha' (09-05-2016), 'Estado' (Finalizado), 'Comentarios' (Análisis OK No activo), 'Sandbox' (Cuckoo), 'Máquina Virtual' (Windows XP x86), 'Red' (Internet Simulado), 'Prioridad' (1 (Máxima)), 'Timeout (seg.)' (240), and a checkbox for 'Usuario Privilegiado'. The 'Binario' panel is outlined in blue and contains fields for 'Fecha' (31-03-2016), 'Nombre' (api.dll), 'Tipo' (PE32 executable (DLL) (GUI) Intel 80386, for MS Windows), 'Tamaño' (39 936 bytes), 'Fuente' (OnDemand), and a list of hashes including MD5, SHA1, SHA256, Ssdeep, and Imphash. At the bottom of the 'Análisis' panel, there are buttons for 'Descargar Informe' (PDF, DOCX) and 'Detalles del Binario' (Descargar Binario).

La parte de la izquierda muestra información acerca del análisis: la fecha de cuando se realizó, su estado actual (Véase la sección [Estados de un Análisis](#)), sus comentarios (Editables haciendo clic en el botón  **Editar**), su sandbox, su máquina virtual y todas las opciones que se eligieron cuando se pidió el análisis (Véase la sección [Campos del Formulario de la Vista de Subida de un Binario](#)). Estas opciones son diferentes en función de la sandbox. Además, cuenta con una barra de herramientas en la parte inferior, que permite las siguientes acciones:

-   **Descargar Informe:** Descarga el informe del análisis. Este informe incluye toda la información extraída del análisis, y también toda la información de los scripts estáticos. Es posible elegir el formato del informe entre PDF y Docx.

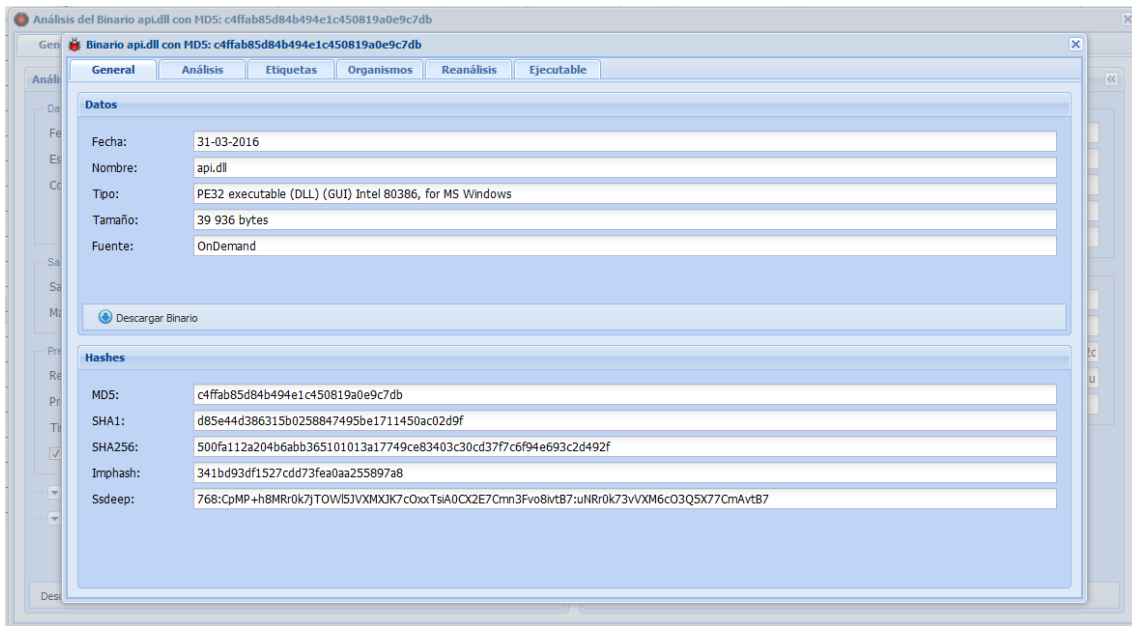


-  **Informe Personalizado:** Muestra la pestaña Informe Personalizado, que permite crear un informe a medida, eligiendo qué secciones se desea que aparezcan.

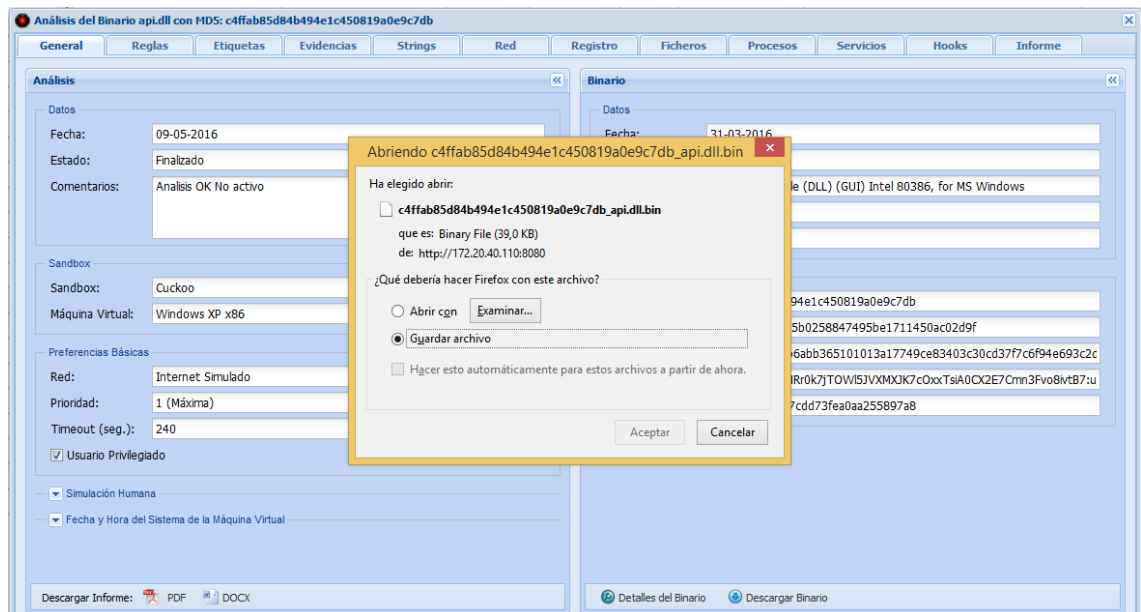


La parte de la derecha muestra información acerca del fichero, la misma que se muestra en la pestaña [General de la Vista de Detalle de un Binario](#). También cuenta con una barra de herramientas en la parte inferior, que permite las siguientes acciones:

-  **Detalles Binario:** Abre la vista de detalles del fichero:



-  **Descargar Binario:** Descarga el fichero. Esta acción debe realizarse con precaución ya que el fichero descargado podría ser un malware. El fichero se descarga con su MD5 como nombre, y con extensión .binary, para evitar que lo ejecutemos por error al descargarlo.

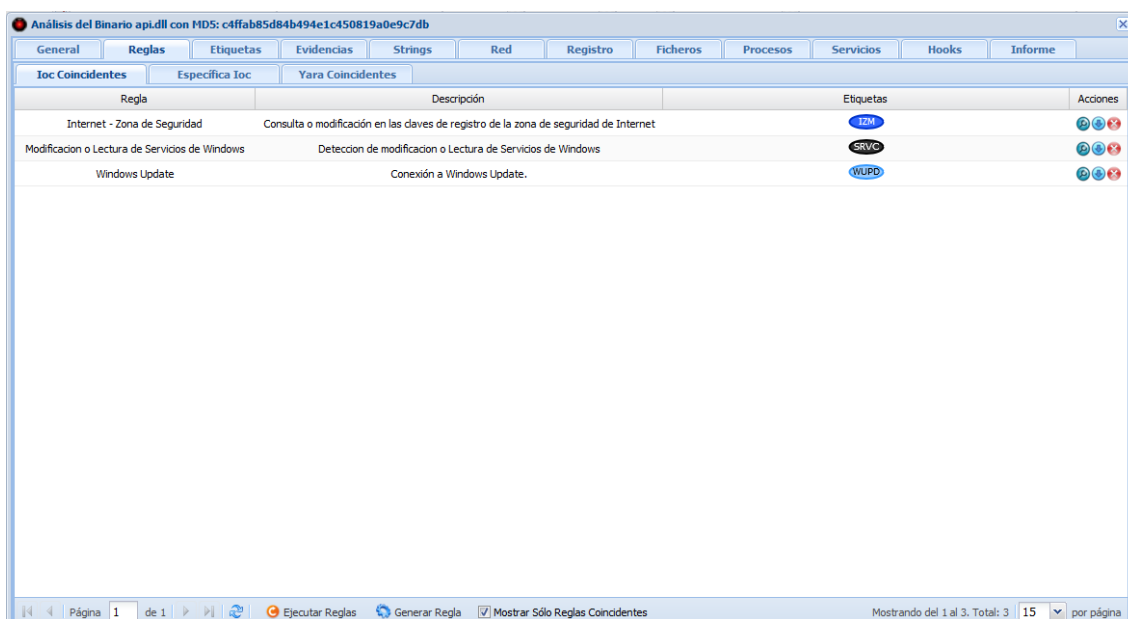


## 10.2 REGLAS

Esta pestaña permite gestionar las reglas relacionadas con el análisis. Cuenta con tres subpestañas:

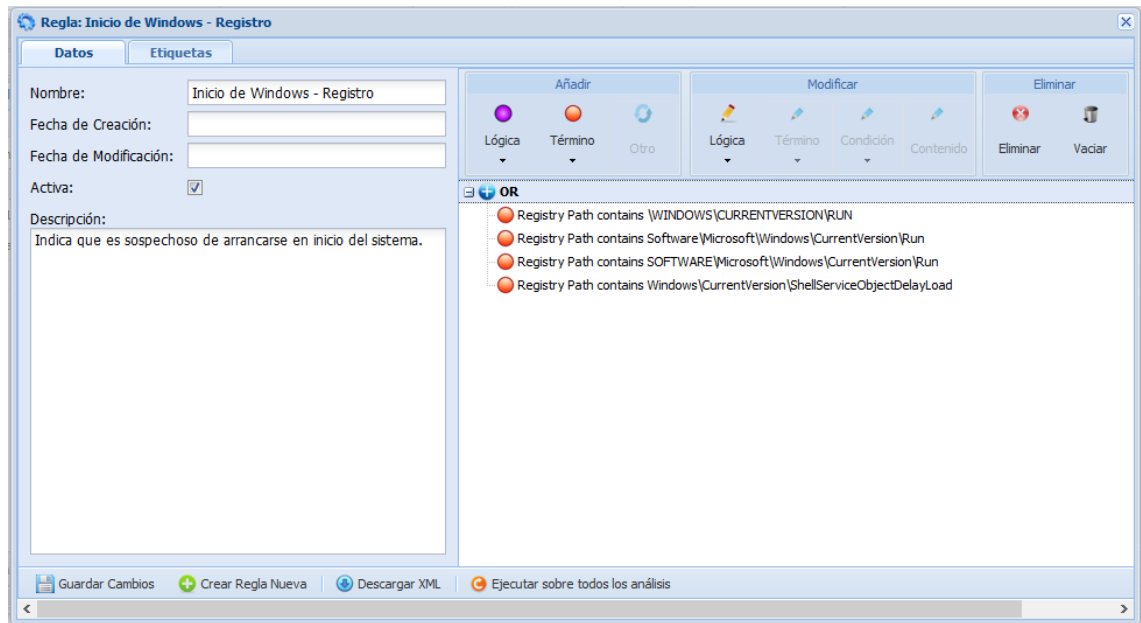
### *loc Coincidentes*

Muestra una lista paginada con todas las reglas activas cumplidas por el análisis, con su nombre, descripción y etiquetas (un análisis recibe todas las etiquetas asignadas a todas sus reglas coincidentes):

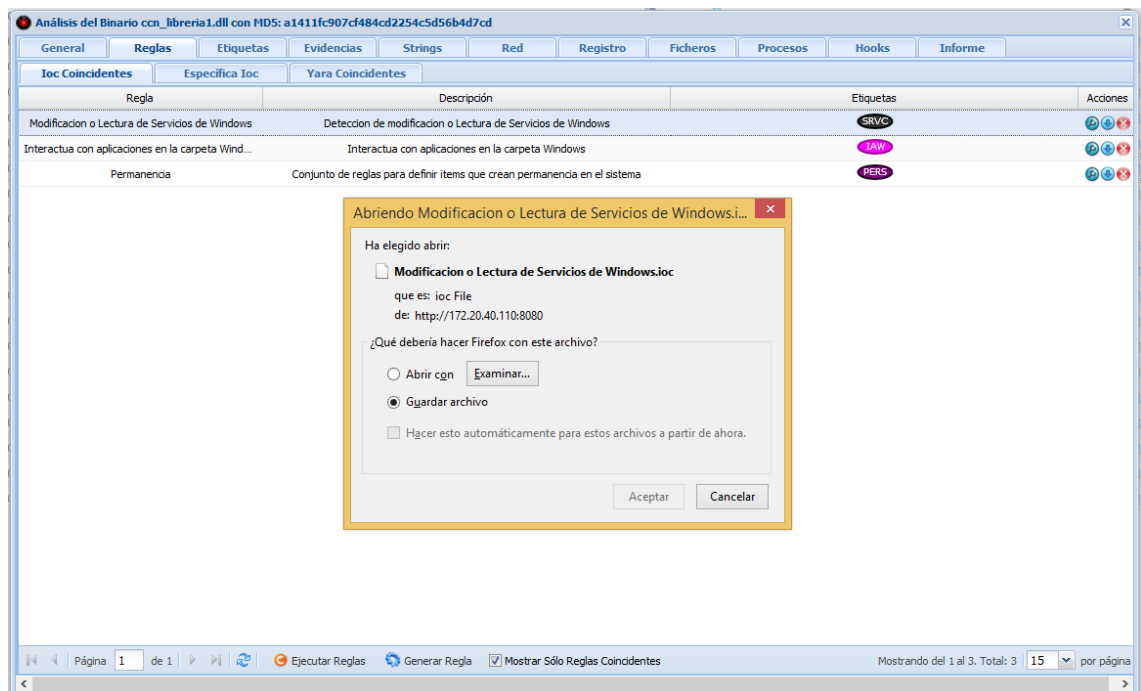


La última columna de la lista es de acciones. Permite realizar las siguientes gestiones:

-  **Ver Detalle:** Abre la vista de detalles de la regla seleccionada. Esta vista contiene toda la información relativa a la regla. Se describe en la sección [Vista de Detalle de una Regla](#) de este documento.

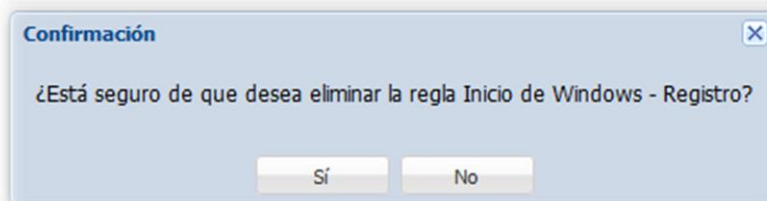


-  **Descargar Regla como XML:** Permite exportar la regla a un fichero con formato XML y descargarlo.

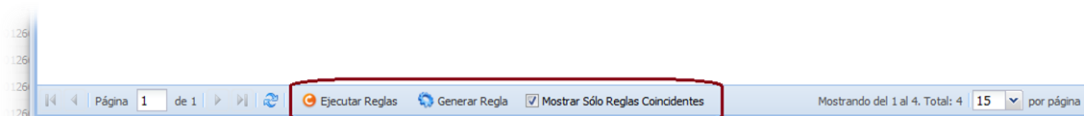


```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
id="" last-modified="2015-09-02T00:00:00" xmlns="http://schemas.mandiant.com/2010/ioc">
<short_description>Inicio de Windows - Registro</short_description>
<description>Inicio de Windows - Registro</description>
<authored_by>null</authored_by>
<authored_date>2015-09-02T00:00:00</authored_date>
<links />
<definition>
<Indicator operator="OR" id="">
<IndicatorItem id="" condition="contains">
<Context document="Registry Path" search="RegistryItem/Path" type="mir" />
<Content type="string">WINDOWS\CURRENTVERSION\RUN</Content>
</IndicatorItem>
<IndicatorItem id="" condition="contains">
<Context document="Registry Path" search="RegistryItem/Path" type="mir" />
<Content type="string">Software\Microsoft\Windows\CurrentVersion\Run</Content>
</IndicatorItem>
<IndicatorItem id="" condition="contains">
<Context document="Registry Path" search="RegistryItem/Path" type="mir" />
<Content type="string">SOFTWARE\Microsoft\Windows\CurrentVersion\Run</Content>
</IndicatorItem>
<IndicatorItem id="" condition="contains">
<Context document="Registry Path" search="RegistryItem/Path" type="mir" />
<Content type="string">Windows\CurrentVersion\ShellServiceObjectDelayLoad</Content>
</IndicatorItem>
</Indicator>
</definition>
</ioc>
```

-  **Eliminar:** Elimina la regla seleccionada. Pide confirmación antes de eliminar.

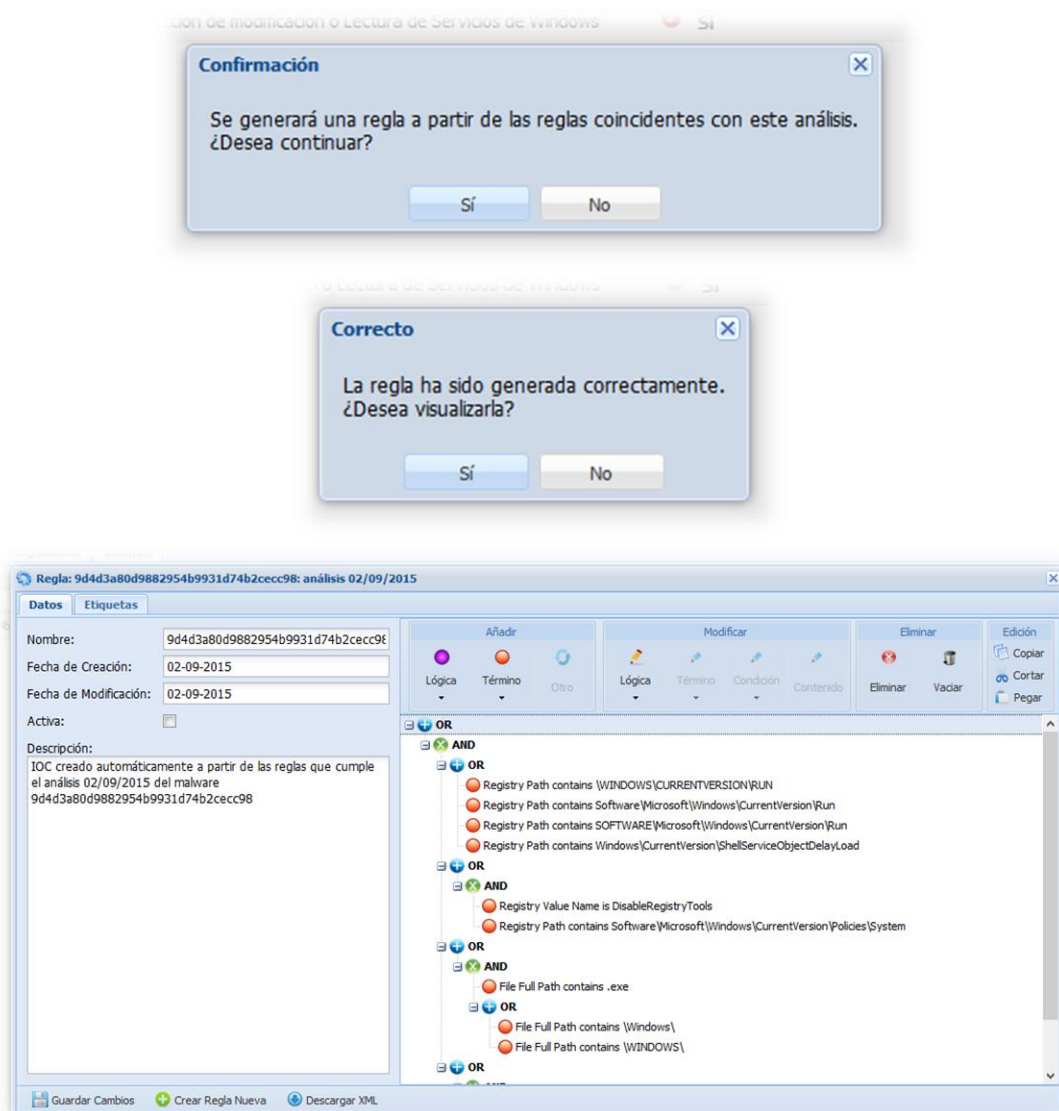


En la parte inferior de la subpestaña, hay una barra de herramientas con acciones:



Permite las siguientes gestiones:

-  **Ejecutar Reglas:** Vuelve a comprobar todas las reglas existentes contra este análisis. Esto es útil si se han modificado reglas o se han creado nuevas posteriormente al análisis, dado que las reglas se comprueban en el momento en el análisis finaliza.
-  **Generar Regla:** Genera una regla nueva combinando todas las reglas coincidentes con este análisis. Pide confirmación.



La regla generada por defecto estará inactiva, así que no se tendrá en cuenta a la hora de comprobar las reglas coincidentes con los próximos análisis. Puede activarse desde la pestaña de configuración, o desde la vista de detalle de una regla.

- ☒ **Mostrar Sólo Reglas Coincidentes:** Si se desactiva esta casilla, la lista mostrará todas las reglas activas, no sólo las coincidentes con el análisis. Aun así, es posible diferenciar las cumplidas por el análisis gracias a la columna Coincidencia.

Análisis del Binario ccn\_libreria1.dll con MD5: a1411fc907cf484cd2254c5d56b4d7cd

GeneralReglasEtiquetasEvidenciasStringsRedRegistroFicherosProcesosHooksInforme

Ioc CoincidentesEspecifica IocYara Coincidentes

| Regla                                             | Descripción                                                                               | Etiquetas | Acciones                                                                                                                                                                                                                                                    |
|---------------------------------------------------|-------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regla AdobeARM                                    | Regla detección de clave de registro AdobeARM                                             | ADBE      |    |
| Consulta DNS a nasbackagain1.allalla.com          | Consulta DNS asbackagain1.allalla.com                                                     | NASB      |    |
| Internet - Zona de Seguridad                      | Consulta o modificación en las claves de registro de la zona de seguridad de Intern...    | IZM       |    |
| Inicio de Windows - Registro                      | Indica que es sospechoso de arrancarse en inicio del sistema.                             | BOOT      |    |
| WinLogon                                          | El código dañino Interactúa con el valor UserInit de la clave de registro winlogon. ...   | WLGK      |    |
| Modificación o Lectura de Servicios de Windows    | Detección de modificación o Lectura de Servicios de Windows                               | SRVC      |    |
| Ejecución de Tarea Programada                     | El binario utiliza schtasks.exe or at.exe para modificar la programación de tareas.       | SCHT      |    |
| Interactua con aplicaciones en la carpeta Wind... | Interactua con aplicaciones en la carpeta Windows                                         | IAW       |    |
| Deshabilita Registro                              | Deshabilita las herramientas de edición de registro de windows dificultando la capa...    | NREG      |    |
| Deshabilita TaskManager                           | Deshabilita el gestor de tareas de Windows.                                               | TASK      |    |
| Modificación de Configuración de Red              | El código dañino utiliza la aplicación netsh.exe para realizar modificaciones en la co... | NET       |    |
| Permanencia                                       | Conjunto de reglas para definir items que crean permanencia en el sistema                 | PERS      |    |
| PRUEBA                                            |                                                                                           | CCN       |    |



Página 1 de 1



 Ejecutar Reglas

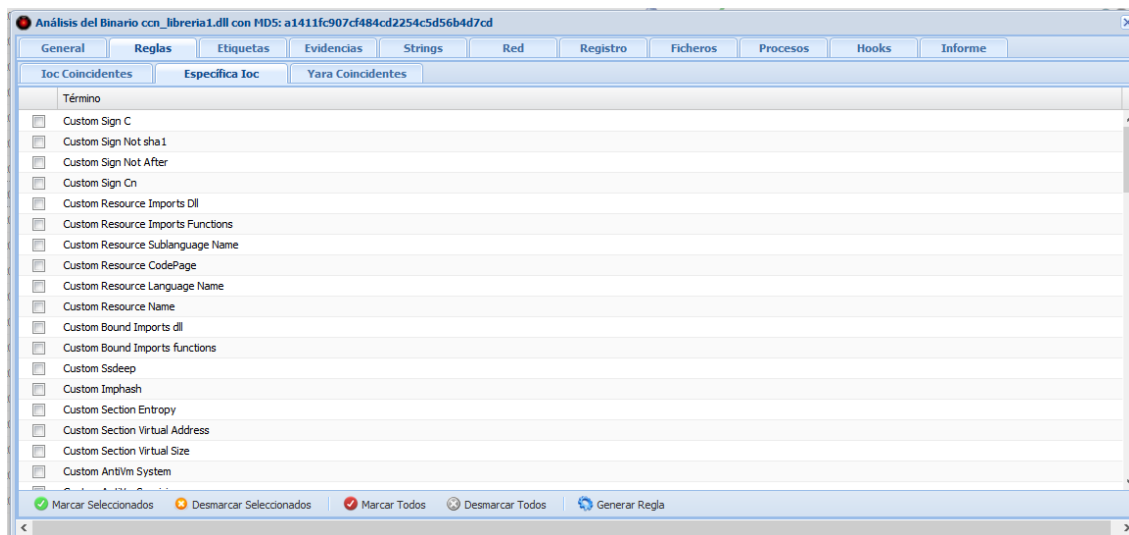
 Generar Regla

☐ Mostrar Sólo Reglas Coincidentes

Mostrando del 1 al 13, Total: 1315 por página

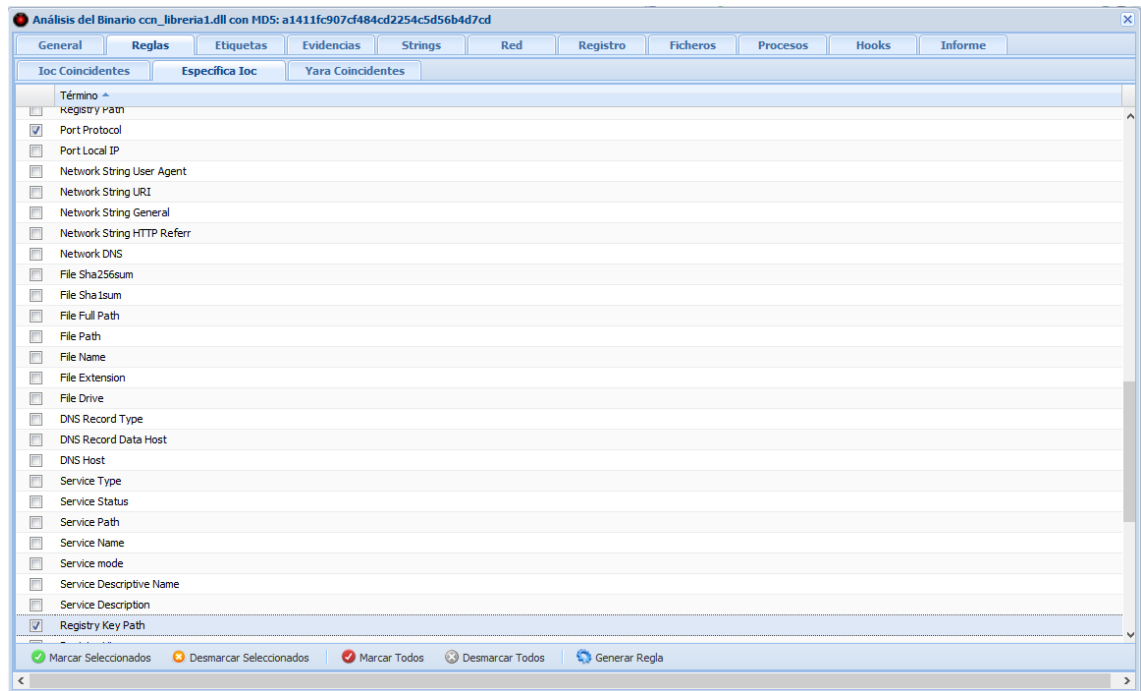
### Específica loc

Permite generar una regla nueva a partir de los datos obtenidos de este análisis. Esto es útil para generar una regla específica del fichero correspondiente al análisis, de forma que si se sube otro fichero a MARTA con un comportamiento muy similar, cumplirá la regla generada y podrá ser detectado rápidamente.

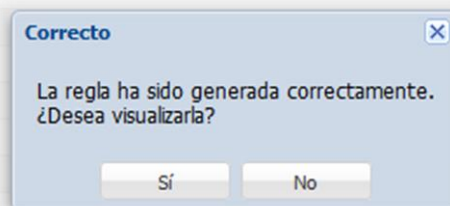
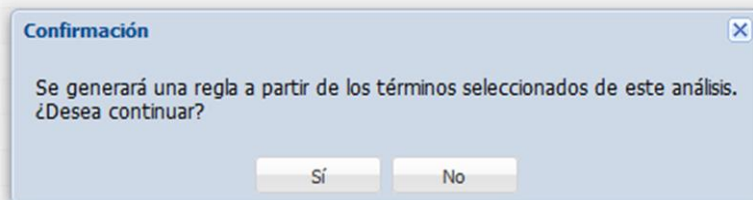


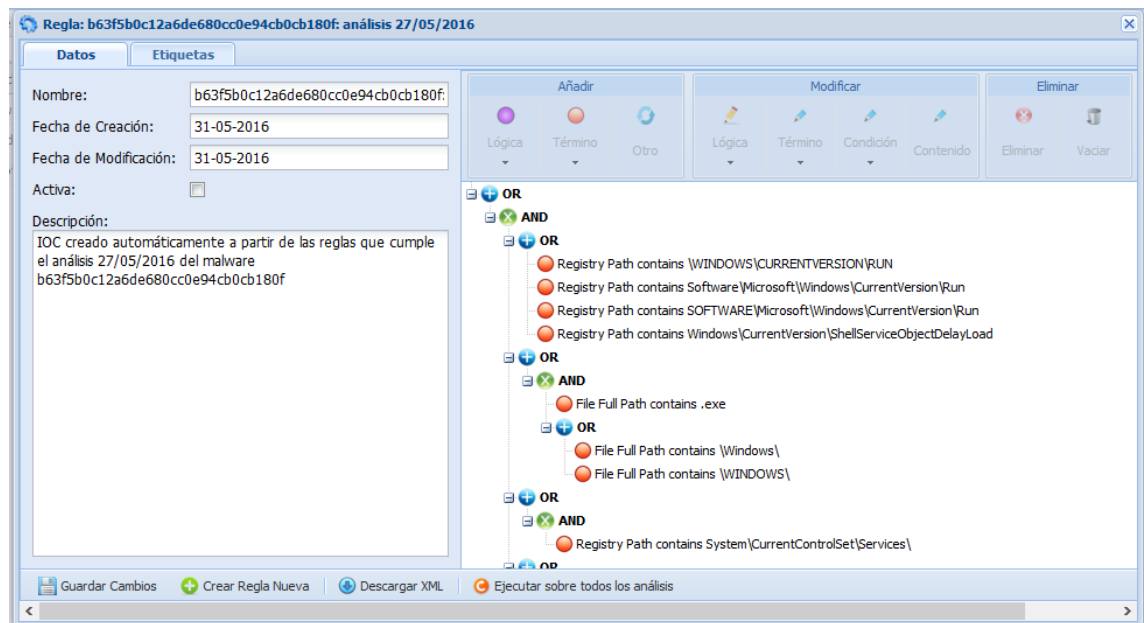
Para generar la regla, debemos elegir qué términos del análisis queremos incluir en ella, marcando las casillas de selección de la lista. Se generará una regla combinando toda la información del análisis acerca de los términos marcados.

Por ejemplo, si marcamos "Registry Key Path" y "Port Protocol", se generará una regla con los key path de las claves de registro con las que se ha interactuado (de cualquier forma), y los protocolos de los puertos accedidos durante el análisis:



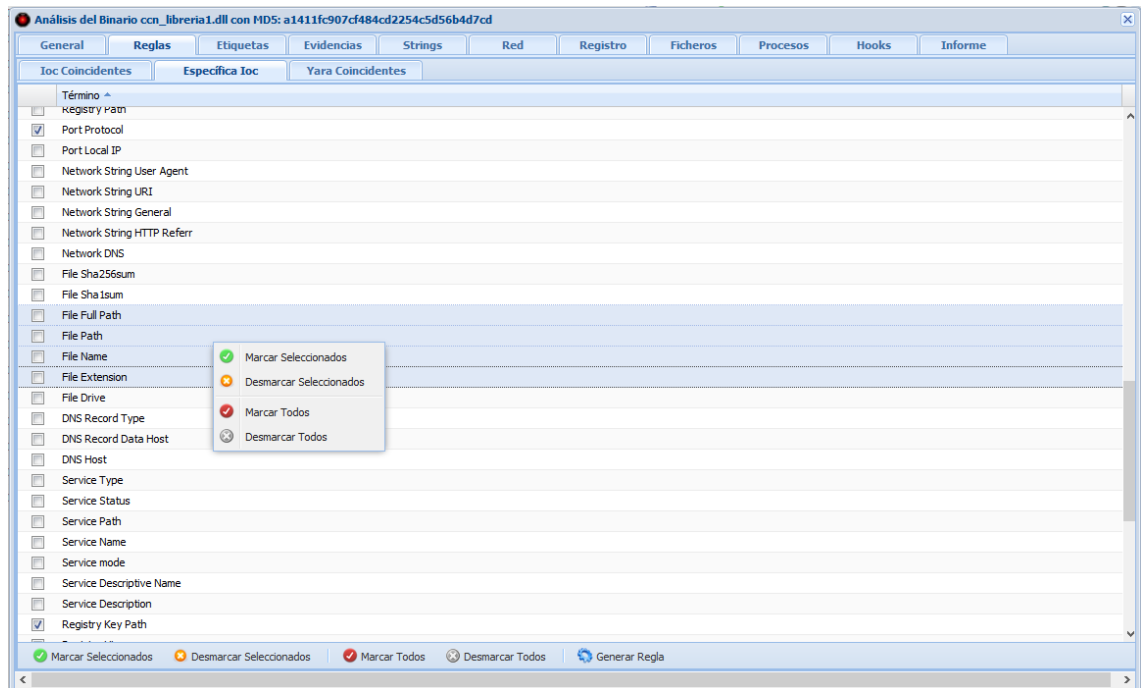
Para generar la regla, debemos clicar en el botón  **Generar Regla** de la barra de herramientas de la parte inferior de la subpestaña.





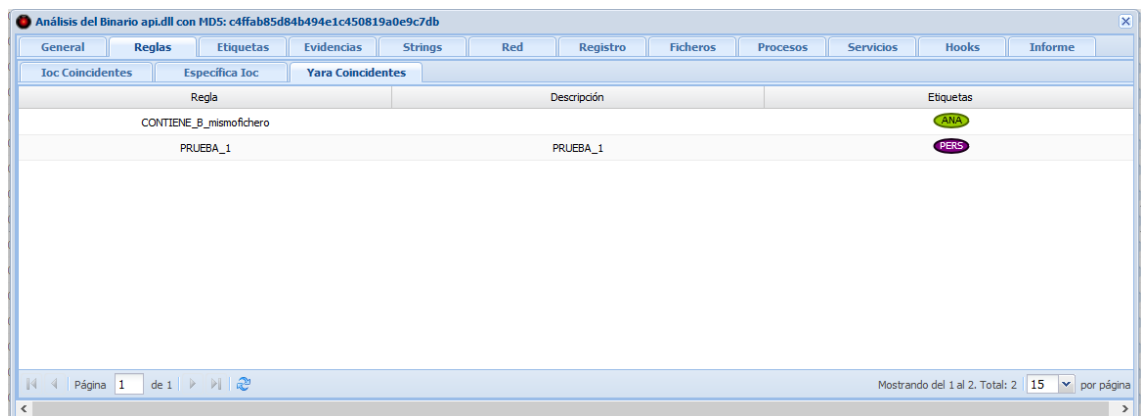
La regla generada por defecto estará inactiva, así que no se tendrá en cuenta a la hora de comprobar las reglas coincidentes con los próximos análisis. Puede activarse desde la pestaña de configuración, o desde la vista de detalle de una regla.

La de herramientas, además, cuenta con botones que nos facilitan el marcado de las casillas de selección:  **Marcar Seleccionados**,  **Desmarcar Seleccionados**,  **Marcar Todos** y  **Desmarcar Todos**. Estas acciones también están disponibles haciendo clic con el botón derecho del ratón sobre la lista de términos.



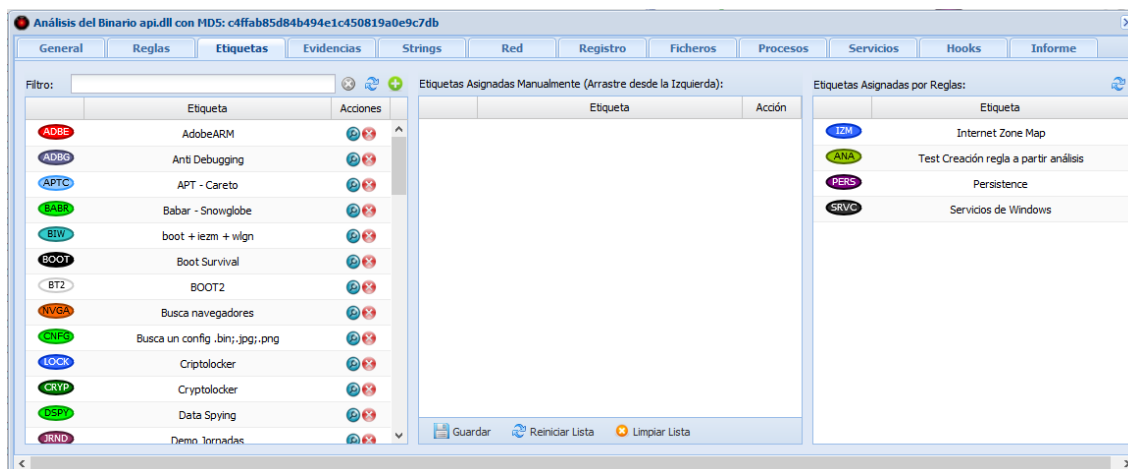
### Yara coincidentes

En esta sección aparecen las reglas yara activas coincidentes y sus etiquetas asociadas. Son las reglas activas que han casado sobre el contenido de la muestra o sobre el contenido de los "dumps" de los procesos creados en la ejecución del análisis dinámico de dicha muestra.



### 10.3 ETIQUETAS

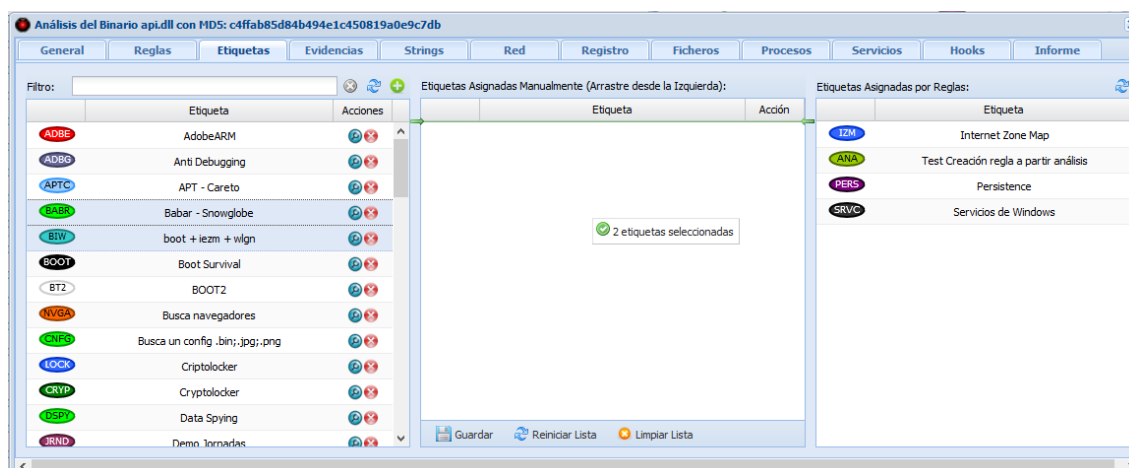
Muestra y permite gestionar las etiquetas asociadas al análisis.

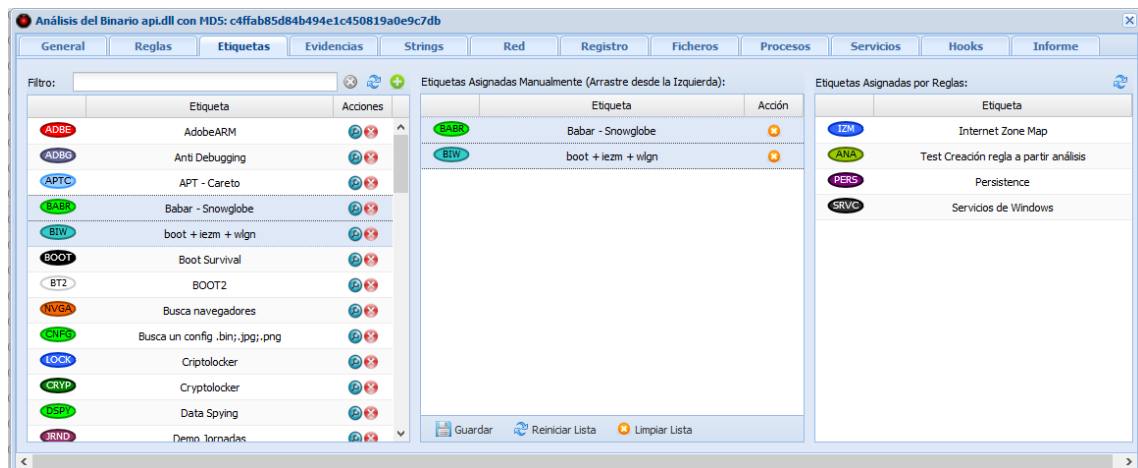


A modo de recordatorio: un análisis tiene asignadas todas las etiquetas que se le asignen manualmente, más todas las etiquetas que tengan asignadas todas sus reglas coincidentes.

Esta pestaña, de forma similar a la de Etiquetas de la Vista de Detalle de un Binario, consta de tres listas:

- La lista de la izquierda muestra todas las etiquetas existentes y permite gestionarlas, de forma similar a la descrita en la sección [Etiquetas](#).
- La lista del centro muestra las etiquetas asignadas manualmente al análisis, y permite arrastrar desde o hacia la lista de la izquierda para añadir o quitar etiquetas.

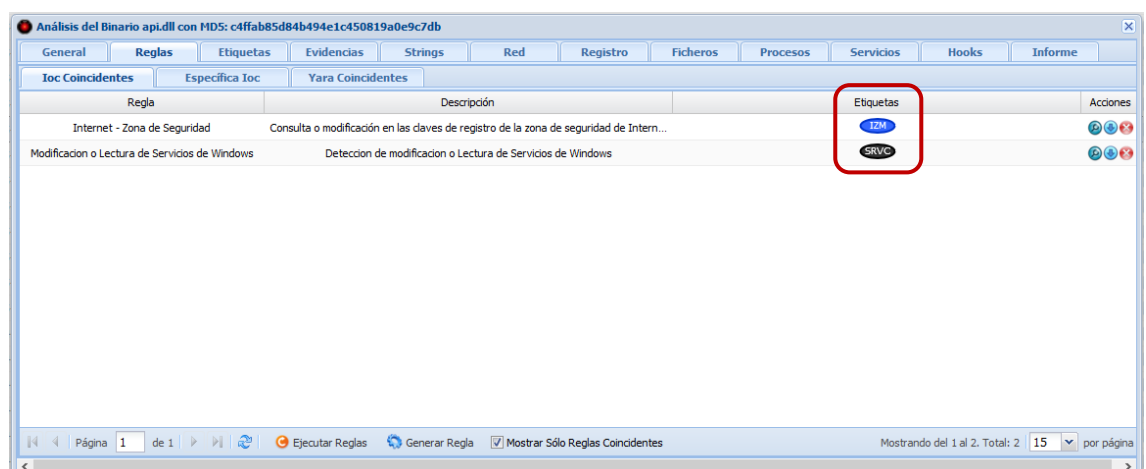


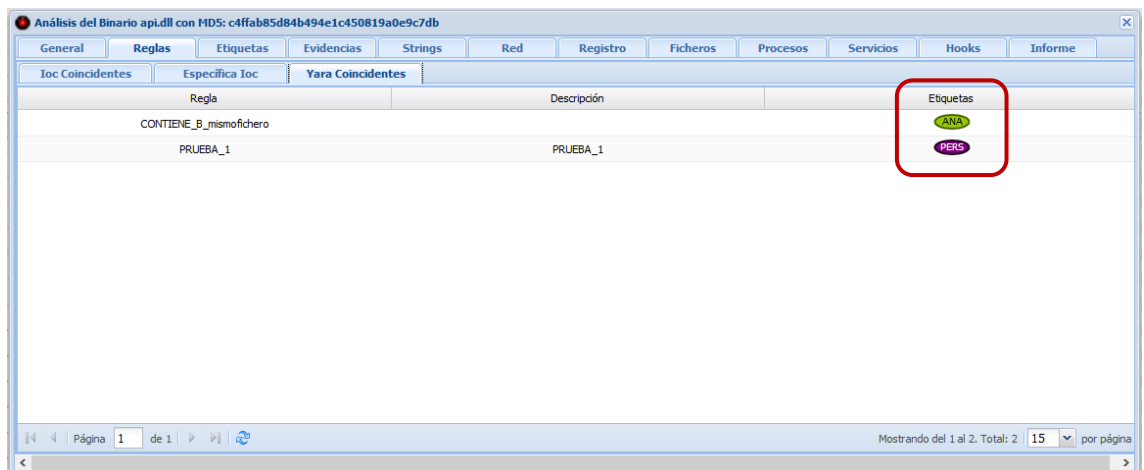


También podemos quitar etiquetas de la lista clicando en la acción  **Quitar** de una etiqueta.

Debajo de la lista hay una barra de acciones, que permite las siguientes gestiones:

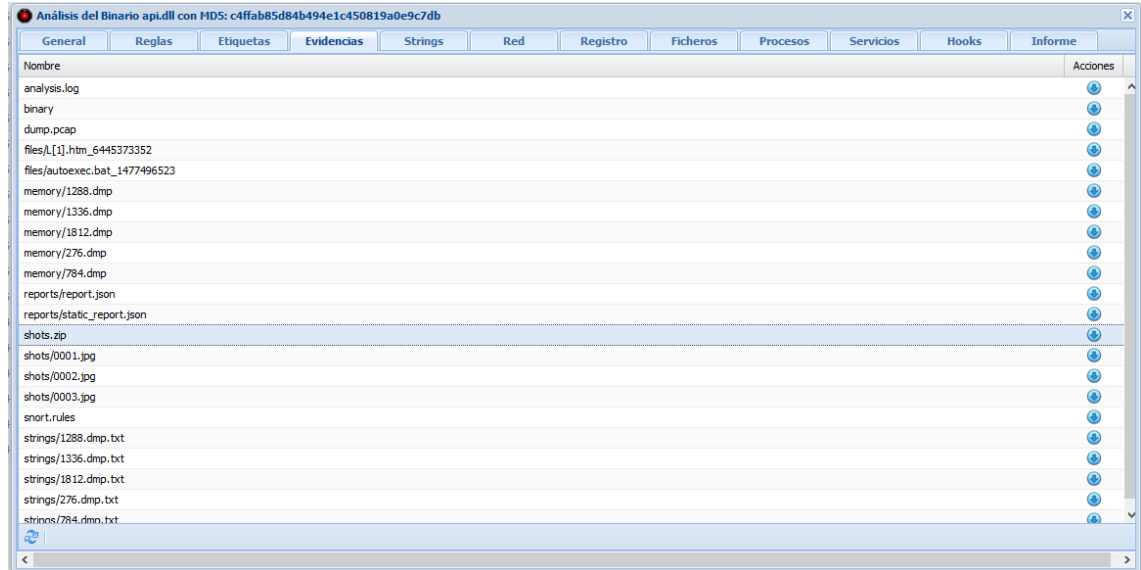
-  **Guardar:** Guarda las etiquetas manualmente asignadas al análisis, tal y como esté la lista en el momento de clicar en el botón.
  -  **Reiniciar Lista:** Reinicia la lista a las etiquetas que tenga el análisis asignadas manualmente en el momento de clicar en el botón.
  -  **Limpiar Lista:** Quita todas las etiquetas de la lista, pero no las desasigna del análisis (a no ser que a continuación hagamos clic en el botón Guardar).
- La lista de la derecha muestra las etiquetas asociadas al análisis debido a las etiquetas asociadas a sus reglas coincidentes. Esta lista no es modificable. Es posible consultar concretamente qué etiquetas vienen de cada regla desde la pestaña de Reglas subsecciones loc coincidentes y Yara coincidentes.



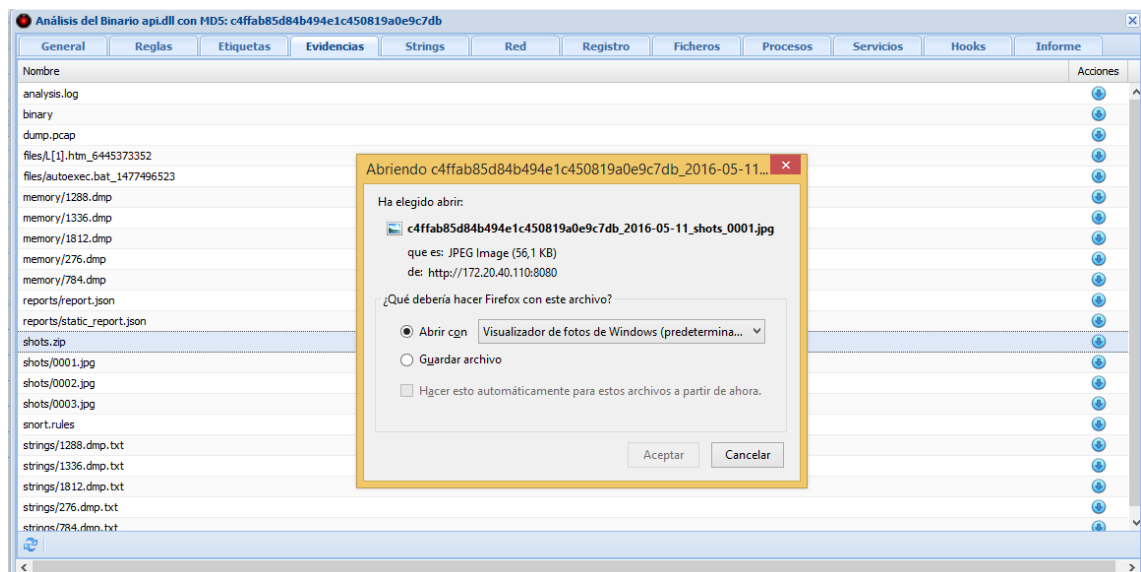


## 10.4 EVIDENCIAS

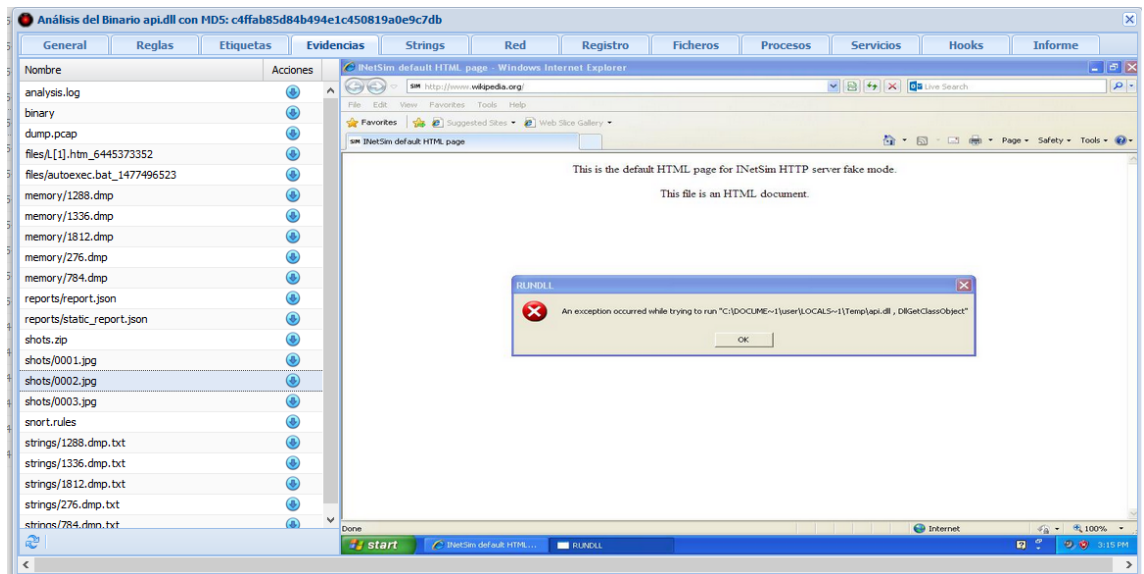
Muestra una lista con diferentes recursos obtenidos por la sandbox durante la ejecución del análisis:



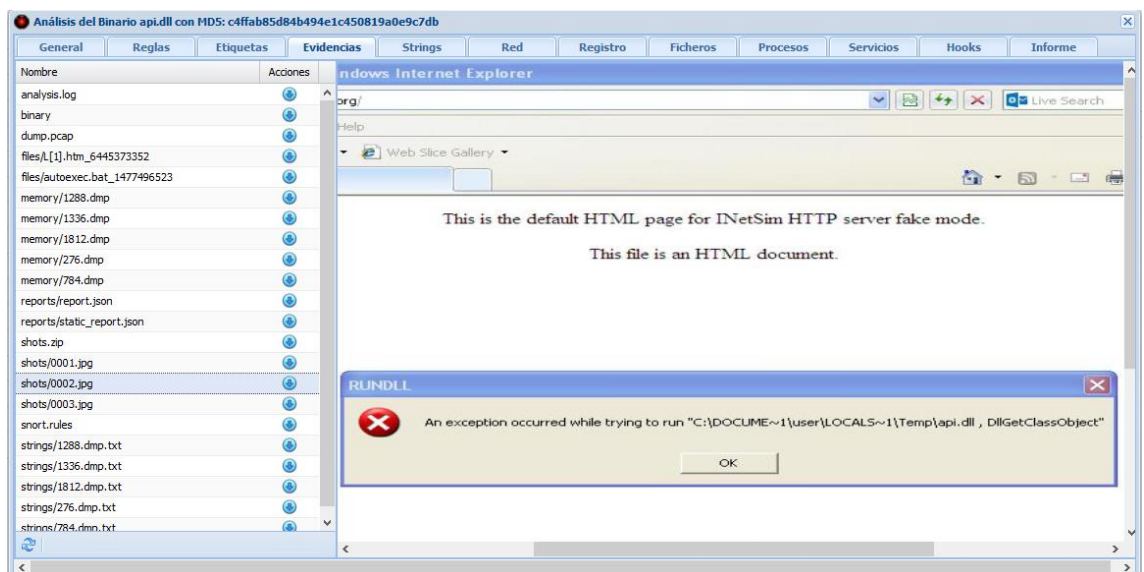
Todos pueden descargarse utilizando la acción  **Descargar**.



Los que son de tipo imagen, como las capturas de pantalla, pueden visualizarse clicando en ellos.



Y se puede aumentar y reducir el zoom haciendo clic con el botón izquierdo y derecho del ratón, respectivamente:

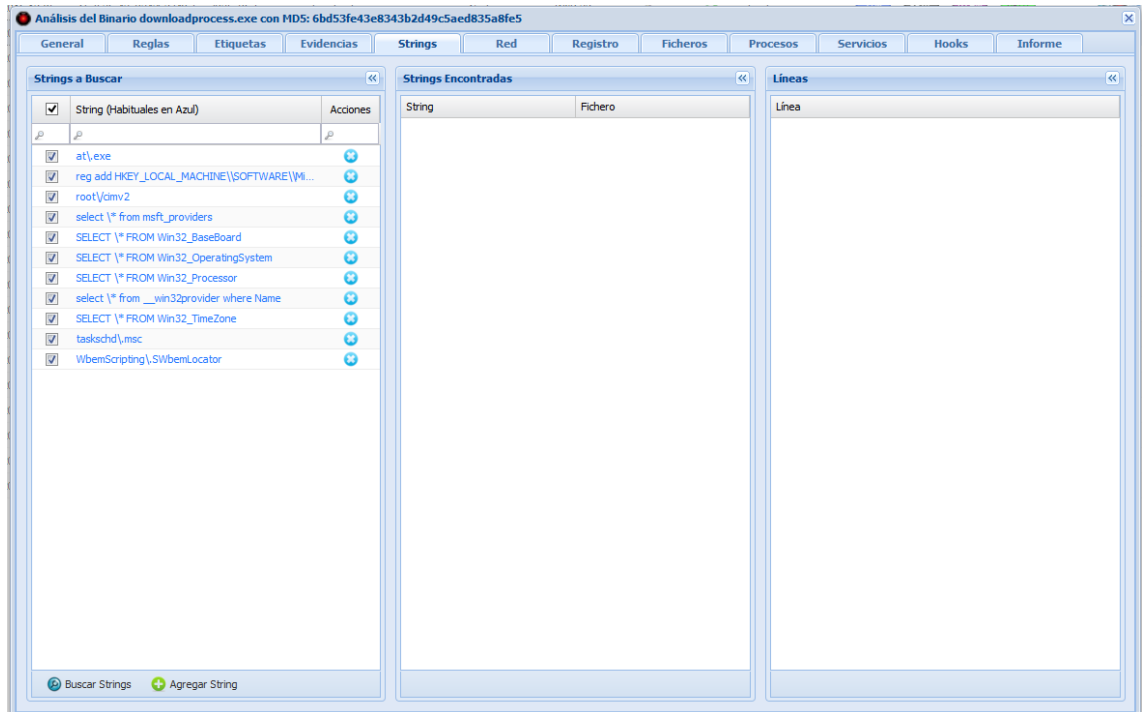


Lista de posibles evidencias:

- **binary:** El fichero analizado.
- **report.json:** Resultado completo del análisis dinámico, en formato json.
- **static\_report.json:** Resultado completo de los scripts estáticos, en formato json.
- **analysis.log:** Log de la sandbox durante la ejecución del análisis.
- **dump.pcap:** Volcado de red de la máquina durante la ejecución del análisis.
- **strings:** Cadenas de texto en la memoria de la máquina durante la ejecución del análisis. Puede haber varios ficheros de strings, uno por cada proceso.
- **files:** Ficheros creados en la máquina durante la ejecución del análisis.
- **shots:** Capturas de pantalla de la máquina durante la ejecución del análisis.
- **snort.rules:** Reglas de Snort sobre las conexiones de red maliciosas del fichero analizado.

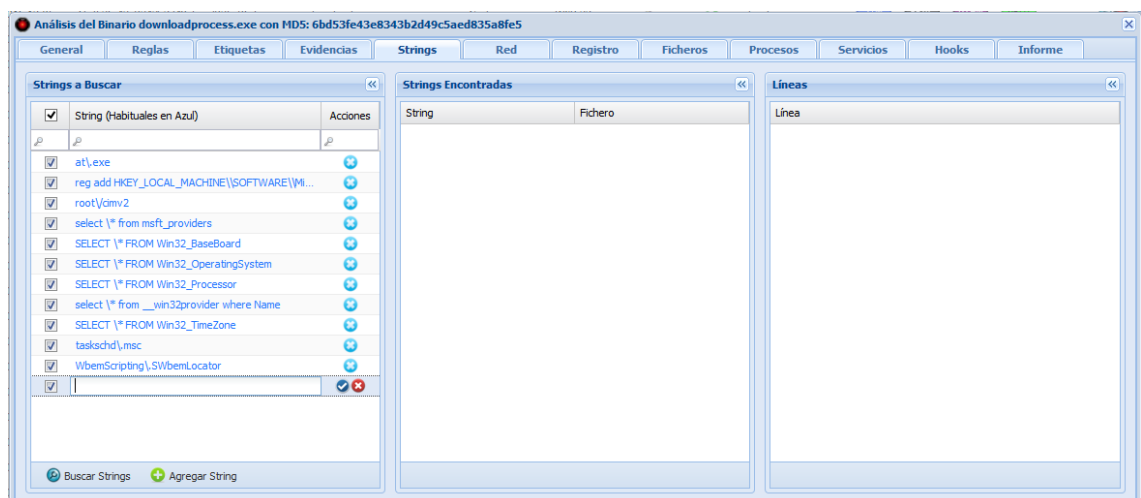
## 10.5 STRINGS

Esta pestaña es una herramienta que facilita la búsqueda de cadenas de texto (strings) específicas en la memoria de la máquina durante la ejecución del análisis.

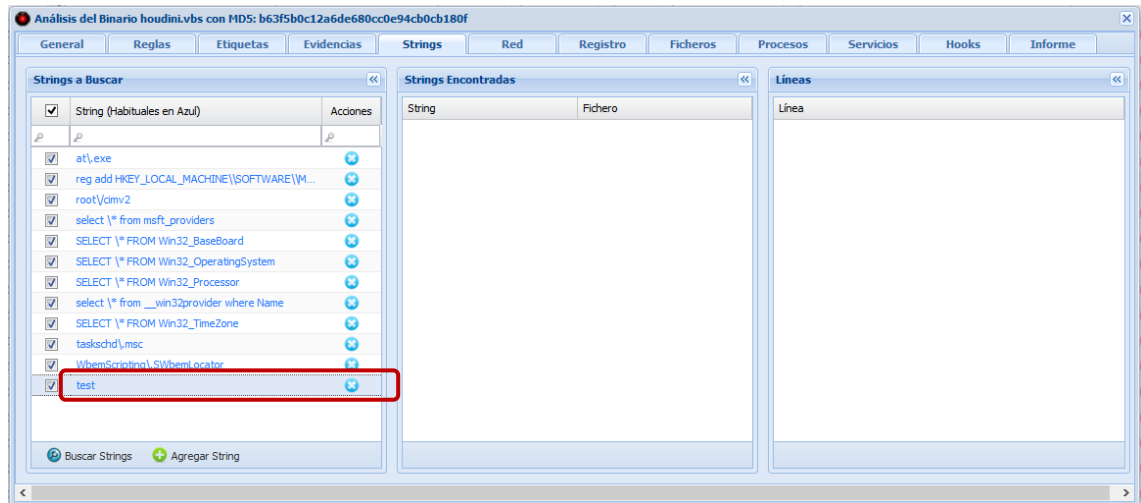


Consta de tres listas:

- La lista de la izquierda contiene las strings que queremos buscar. Por defecto, viene rellena con un conjunto de strings habituales (en azul). Podemos añadir otras strings (no habituales, sólo para esta búsqueda) haciendo clic en el botón **+ Agregar String** de la barra de herramientas inferior de la lista, y a continuación escribiendo el texto de la string y pulsando enter.



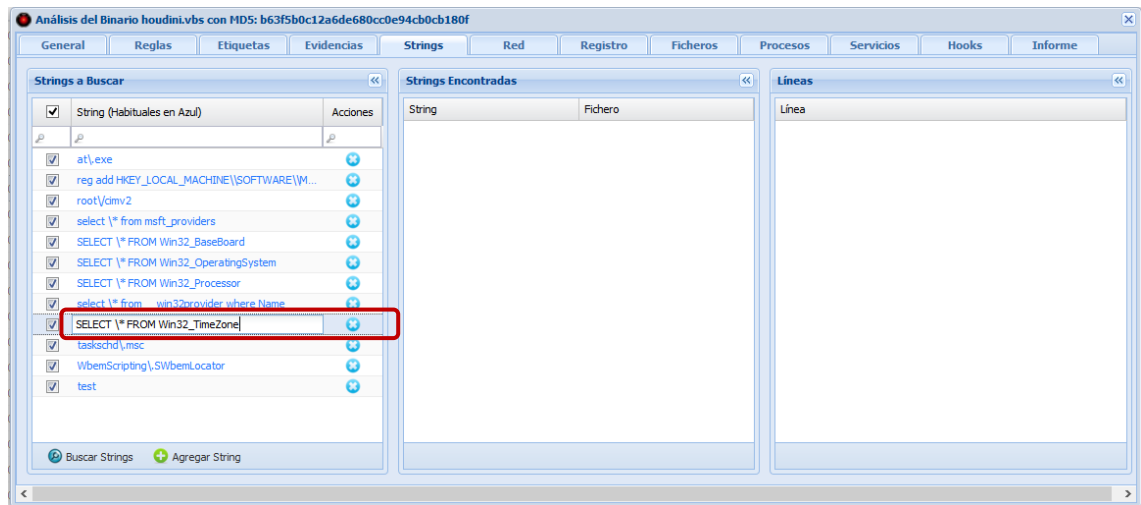
Podemos convertir una string no habitual en habitual clicando en la acción  **Marcar como Habitual**.



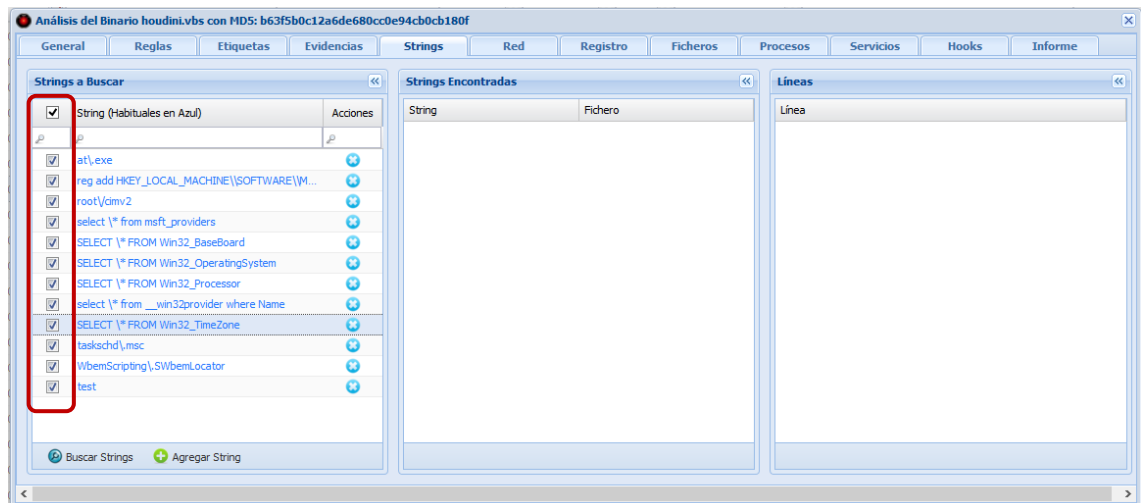
O hacer que una string habitual deje de serlo clicando en la acción  **Desmarcar como Habitual**.

También podemos quitar una string no habitual de la lista clicando en la acción  **Quitar**.

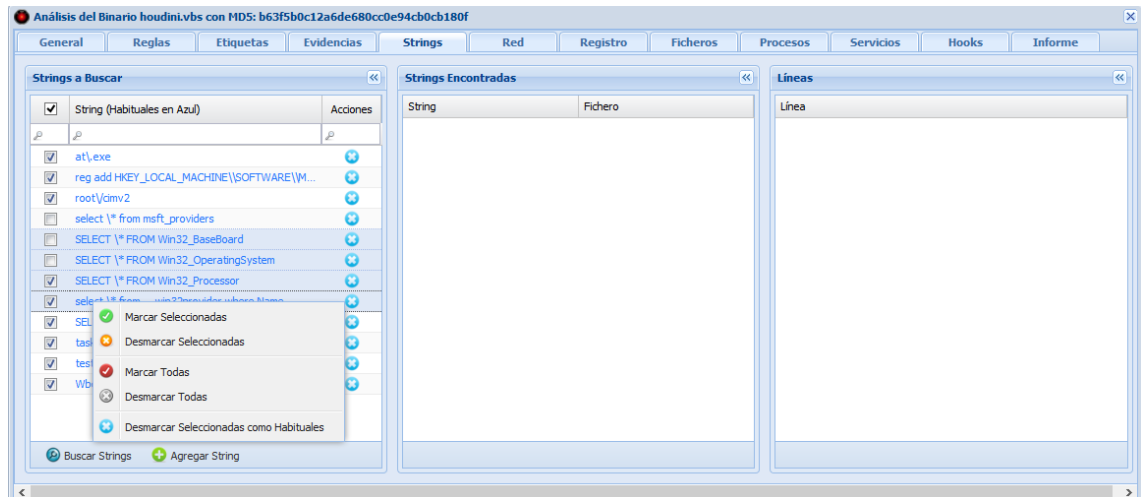
Podemos modificar cualquier string haciendo doble clic sobre ella, escribiendo su nuevo texto y pulsando enter.



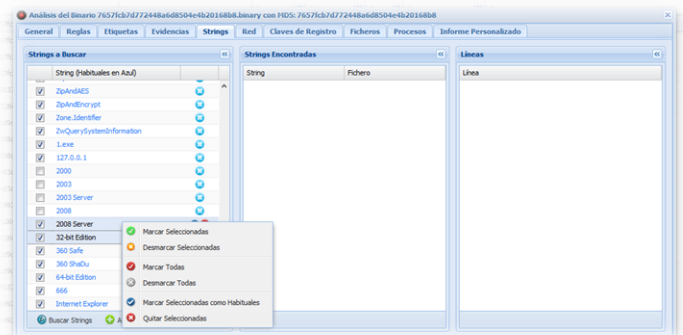
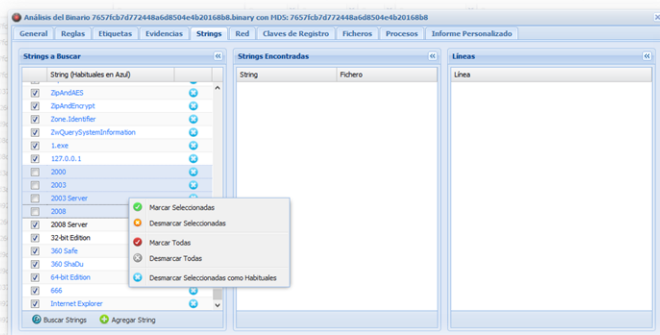
Además, podemos marcar y desmarcar las casillas de selección de cada string para tenerla o no tenerla en cuenta para la siguiente búsqueda.



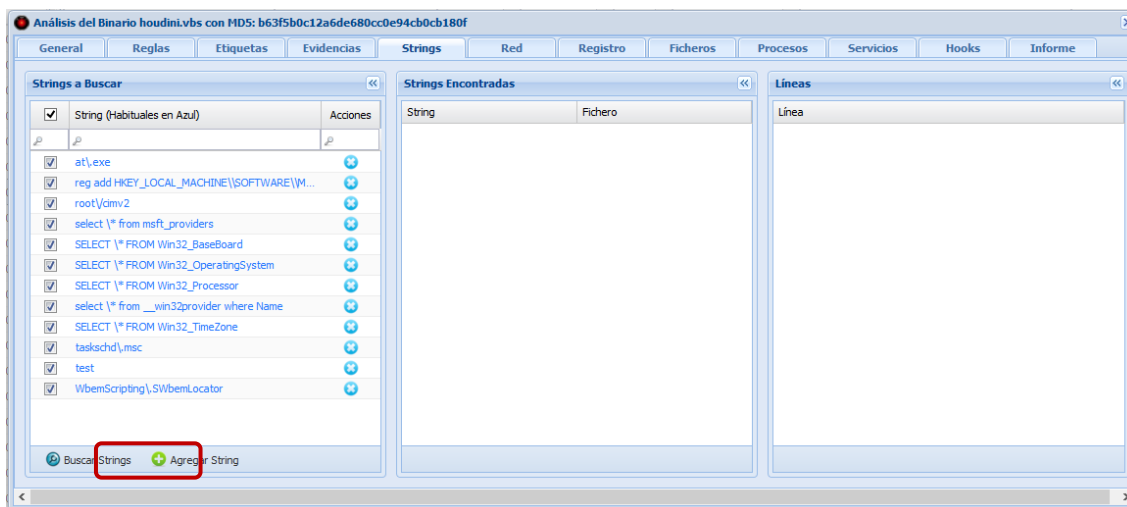
Haciendo clic con el botón derecho del ratón sobre la lista podemos desplegar un menú con las siguientes acciones sobre las strings:  **Marcar Seleccionadas**,  **Desmarcar Seleccionadas**,  **Marcar Todas**,  **Desmarcar Todos**.



Si sólo hemos seleccionado strings habituales, este menú también mostrará la acción  **Desmarcar Seleccionadas como Habituales**. Y si sólo hemos seleccionado strings no habituales, mostrará las acciones  **Marcar Seleccionadas como Habituales** y  **Quitar Seleccionadas**.

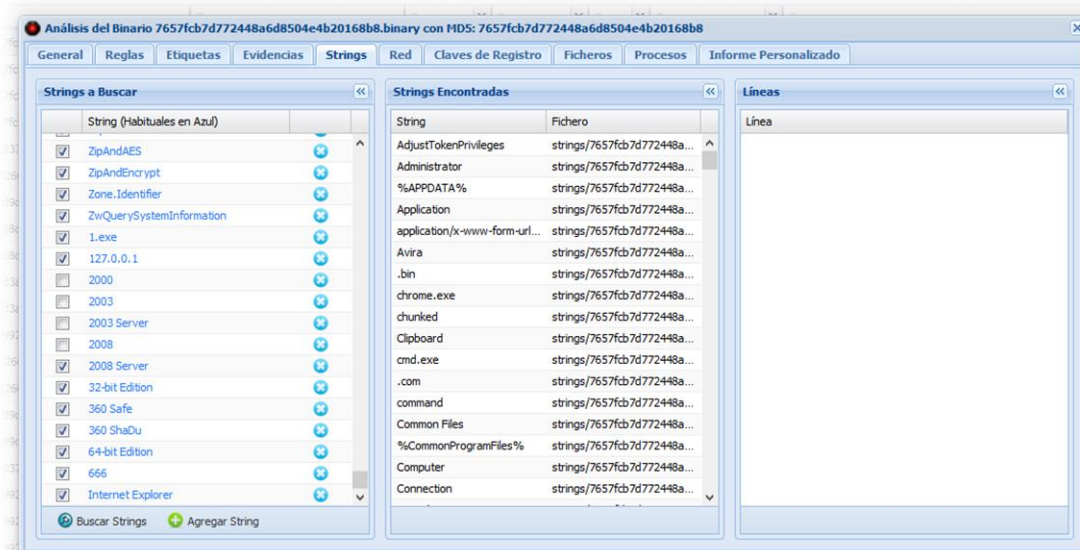


Una vez hemos determinado las strings que queremos buscar, hacemos clic en el botón **Buscar Strings** de la barra de herramientas inferior de la lista.

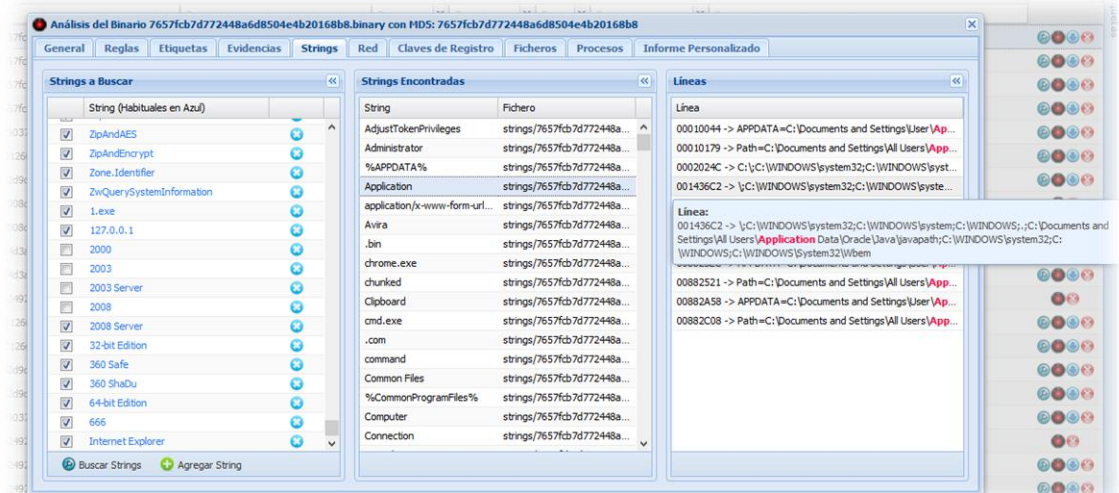
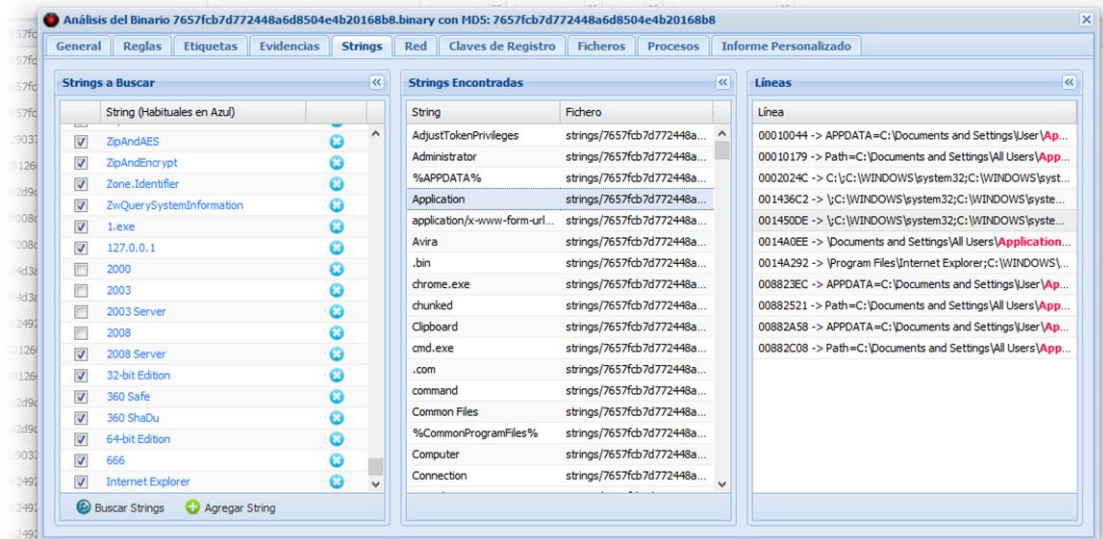


Esto iniciará la búsqueda de las strings por todos los ficheros de strings de memoria del análisis (hay un fichero de strings por cada proceso; pueden descargarse desde la pestaña de evidencias). Este proceso habitualmente dura unos segundos.

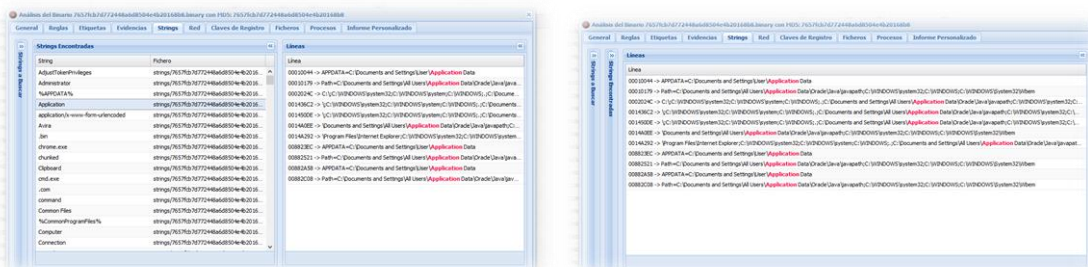
- Al finalizar la búsqueda de strings, la lista del medio se rellenará con todas las strings encontradas en cada fichero de strings.



- Seleccionando una string de la lista del medio, la lista de la derecha mostrará en qué líneas del fichero se encuentra la string.

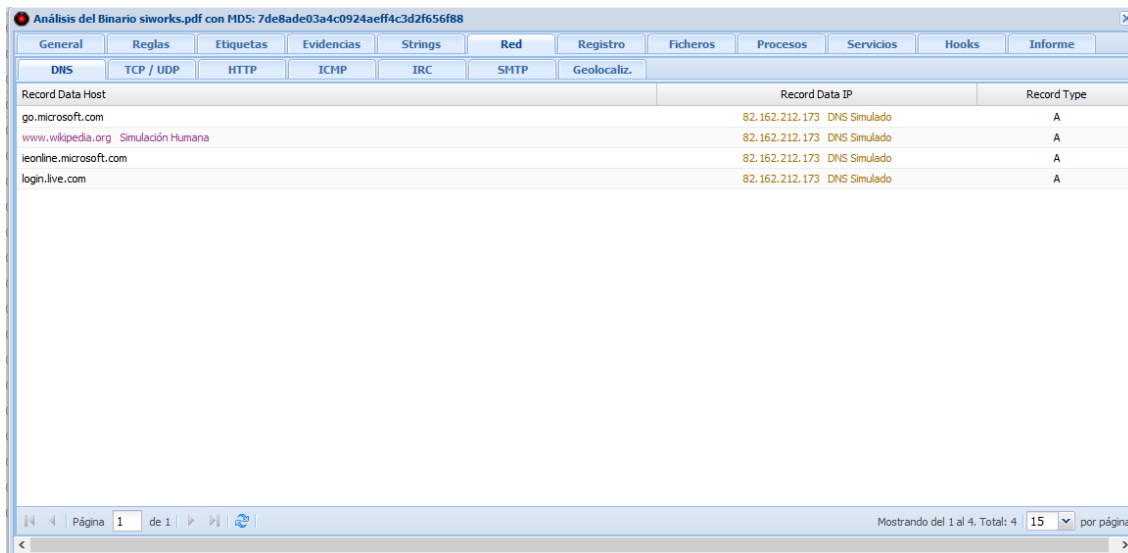


Por comodidad, las tres listas son plegables:



## 10.6 RED

Muestra información acerca de las conexiones de red realizadas durante el análisis, agrupadas por protocolo:



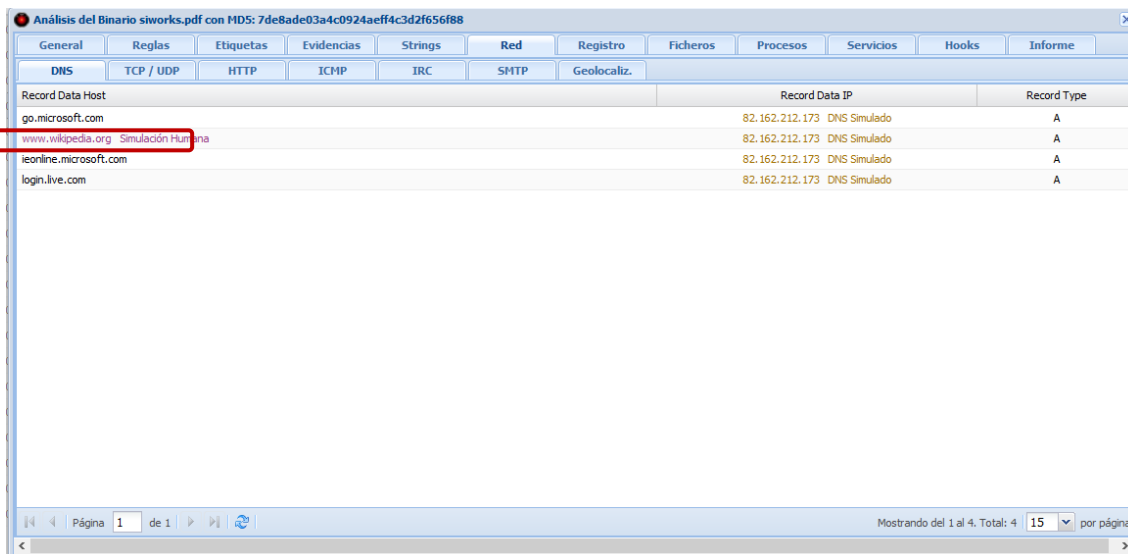
| Análisis del Binario siworks.pdf con MD5: 7de8ade03a4c0924aef4c3d2f656f88                          |                             |             |  |
|----------------------------------------------------------------------------------------------------|-----------------------------|-------------|--|
| General Reglas Etiquetas Evidencias Strings Red Registro Ficheros Procesos Servicios Hooks Informe |                             |             |  |
| DNS TCP / UDP HTTP ICMP IRC SMTP Geolocaliz.                                                       |                             |             |  |
| Record Data Host                                                                                   | Record Data IP              | Record Type |  |
| go.microsoft.com                                                                                   | 82.162.212.173 DNS Simulado | A           |  |
| www.wikipedia.org Simulación Humana                                                                | 82.162.212.173 DNS Simulado | A           |  |
| ieonline.microsoft.com                                                                             | 82.162.212.173 DNS Simulado | A           |  |
| login.live.com                                                                                     | 82.162.212.173 DNS Simulado | A           |  |

Mostrando del 1 al 4. Total: 4 15 por página

Por cada protocolo, hay una subpestaña.

### DNS

Muestra todas las resoluciones DNS realizadas durante el análisis, indicando su Host, su IP y su tipo. Si en las opciones del análisis se ha seleccionado la opción “Abrir el navegador web” en la sección “Simulación humana” (opción por defecto) entonces el registro DNS correspondiente a la resolución de la URL tecleada aparecerá en color morado.



| Análisis del Binario siworks.pdf con MD5: 7de8ade03a4c0924aef4c3d2f656f88                          |                             |             |  |
|----------------------------------------------------------------------------------------------------|-----------------------------|-------------|--|
| General Reglas Etiquetas Evidencias Strings Red Registro Ficheros Procesos Servicios Hooks Informe |                             |             |  |
| DNS TCP / UDP HTTP ICMP IRC SMTP Geolocaliz.                                                       |                             |             |  |
| Record Data Host                                                                                   | Record Data IP              | Record Type |  |
| go.microsoft.com                                                                                   | 82.162.212.173 DNS Simulado | A           |  |
| www.wikipedia.org Simulación Humana                                                                | 82.162.212.173 DNS Simulado | A           |  |
| ieonline.microsoft.com                                                                             | 82.162.212.173 DNS Simulado | A           |  |
| login.live.com                                                                                     | 82.162.212.173 DNS Simulado | A           |  |

Mostrando del 1 al 4. Total: 4 15 por página

## TCP / UDP

Muestra todas las conexiones TCP y UDP realizadas durante el análisis, indicando la IP y el puerto local y remoto. Las IPs de Internet Simulado, Tor y la Sandbox están marcadas para que sean fácilmente identificables.

| Análisis del Puerto 364d4090368/752173c456467d3 con MD5: 364d4090368/752173c456467d3 |           |           |               |         |      |               |          |                |           |           |         |  |
|--------------------------------------------------------------------------------------|-----------|-----------|---------------|---------|------|---------------|----------|----------------|-----------|-----------|---------|--|
| Acción                                                                               | Reglas    | Etiquetas | Evidencias    | Strings | Red  | Registro      | Archivos | Procesos       | Servicios | Huella    | Informe |  |
| DMS                                                                                  | TCP / UDP | HTTP      | ICMP          | IRC     | SFTP | Geolocaliz.   |          |                |           |           |         |  |
| IP Origen                                                                            |           |           | Puerto Origen |         |      | IP Destino    |          | Puerto Destino |           | Protocolo |         |  |
| 172.20.40.120                                                                        | Sandbox   |           | 65189         |         |      | 172.20.40.130 | Gateway  | 53             |           | UDP       |         |  |
| 172.20.40.130                                                                        | Gateway   |           | 53            |         |      | 172.20.40.120 | Sandbox  | 65189          |           | UDP       |         |  |
| 172.20.40.120                                                                        | Sandbox   |           | 63127         |         |      | 172.20.40.130 | Gateway  | 53             |           | UDP       |         |  |
| 172.20.40.130                                                                        | Gateway   |           | 53            |         |      | 172.20.40.120 | Sandbox  | 63127          |           | UDP       |         |  |
| 172.20.40.120                                                                        | Sandbox   |           | 51973         |         |      | 172.20.40.130 | Gateway  | 53             |           | UDP       |         |  |
| 172.20.40.130                                                                        | Gateway   |           | 53            |         |      | 172.20.40.120 | Sandbox  | 51973          |           | UDP       |         |  |
| 172.20.40.120                                                                        | Sandbox   |           | 52120         |         |      | 172.20.40.130 | Gateway  | 53             |           | UDP       |         |  |
| 172.20.40.130                                                                        | Gateway   |           | 53            |         |      | 172.20.40.120 | Sandbox  | 52120          |           | UDP       |         |  |
| 172.20.40.120                                                                        | Sandbox   |           | 58125         |         |      | 172.20.40.130 | Gateway  | 53             |           | UDP       |         |  |
| 172.20.40.130                                                                        | Gateway   |           | 53            |         |      | 172.20.40.120 | Sandbox  | 58125          |           | UDP       |         |  |
| 172.20.40.120                                                                        | Sandbox   |           | 63128         |         |      | 172.20.40.130 | Gateway  | 53             |           | UDP       |         |  |
| 172.20.40.130                                                                        | Gateway   |           | 53            |         |      | 172.20.40.120 | Sandbox  | 63128          |           | UDP       |         |  |
| 172.20.40.120                                                                        | Sandbox   |           | 57952         |         |      | 172.20.40.130 | Gateway  | 53             |           | UDP       |         |  |
| 172.20.40.130                                                                        | Gateway   |           | 53            |         |      | 172.20.40.120 | Sandbox  | 57952          |           | UDP       |         |  |
| 172.20.40.120                                                                        | Sandbox   |           | 49688         |         |      | 172.20.40.130 | Gateway  | 53             |           | UDP       |         |  |

24

Página 1 de 147

Mostrando del 1 al 15. Total: 204415 de 15 por página

| Análisis del Movimiento sinérgico por PDS: Yalobá de la 09/02/2019 a la 06/02/2019 |           |           |               |         |      |                                  |          |                |           |        |           |
|------------------------------------------------------------------------------------|-----------|-----------|---------------|---------|------|----------------------------------|----------|----------------|-----------|--------|-----------|
| General                                                                            | Región    | Etiquetas | Evidencias    | Shtraps | Red  | Registro                         | Ficheros | Procesos       | Servicios | Hotels | Informes  |
| DMS                                                                                | TCP / UDP | HTTP      | ICMP          | IRC     | SMTP | Genérica                         |          |                |           |        |           |
| IP Origen                                                                          |           |           | Puerto Origen |         |      | IP Destino                       |          | Puerto Destino |           |        | Protocolo |
| 192.168.57.120                                                                     | Sandbox   |           | 50055         |         |      | 192.168.57.1 Gateway             |          | 50055          |           |        | UDP       |
| 192.168.57.1 Gateway                                                               |           |           | 53022         |         |      | 192.168.57.120 Sandbox           |          | 53025          |           |        | UDP       |
| 192.168.57.120 Sandbox                                                             |           |           | 53022         |         |      | 192.168.57.1 Gateway             |          | 53             |           |        | UDP       |
| 192.168.57.1 Gateway                                                               |           |           | 53            |         |      | 192.168.57.120 Sandbox           |          | 53922          |           |        | UDP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 443           |         |      | 192.168.57.120 Sandbox           |          | 15948          |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 443           |         |      | 192.168.57.120 Sandbox           |          | 15403          |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 443           |         |      | 192.168.57.120 Sandbox           |          | 15403          |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 1041          |         |      | 208.80.134.224 Simulación Humana |          | 80             |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 80            |         |      | 192.168.57.120 Sandbox           |          | 1041           |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 1042          |         |      | 208.80.134.224 Simulación Humana |          | 443            |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 443           |         |      | 192.168.57.120 Sandbox           |          | 1042           |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 1043          |         |      | 208.80.134.224 Simulación Humana |          | 1043           |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 443           |         |      | 192.168.57.120 Sandbox           |          | 1043           |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 1044          |         |      | 208.80.134.224 Simulación Humana |          | 443            |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 1044          |         |      | 192.168.57.120 Sandbox           |          | 1044           |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 1052          |         |      | 82.92.212.179 FPG Simulada       |          | 443            |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 1075          |         |      | 21.204.181.24 Externa            |          | 443            |           |        | TCP       |
| 23.204.181.24 Externa                                                              |           |           | 1075          |         |      | 192.168.57.120 Sandbox           |          | 1075           |           |        | TCP       |
| 208.80.134.224 Simulación Humana                                                   |           |           | 1076          |         |      | 82.92.212.179 FPG Simulada       |          | 443            |           |        | TCP       |

28

Página 1 de 1

Mostrando del 1 al 39. Total: 39

28

por página

## HTTP

Muestra todas las conexiones HTTP y HTTPS realizadas durante el análisis, indicando la URI, el dominio DNS, el Referer y el User Agent.

<

## ICMP

Muestra todas las conexiones ICMP realizadas durante el análisis, indicando los la IP de origen y de destino, el tipo, los datos y el código.

Análisis del Binario ccn\_libreria1.dll con MD5: a1411fc907cf484cd2254cd56b4d7cd

General

Reglas

Etiquetas

Evidencias

Strings

Red

Registro

Ficheros

Procesos

Hooks

Informe

DNS

TCP / UDP

HTTP

ICMP

IRC

SMTP

Geolocaliz.

IP Origen

IP Destino

Tipo

Código

Data

172.20.41.6

Sandbox

172.20.40.254

Gateway

Destination Unreachable

(Port unreachable)

172.20.40.254

Gateway

172.20.41.6

Sandbox

Destination Unreachable

(Port unreachable)

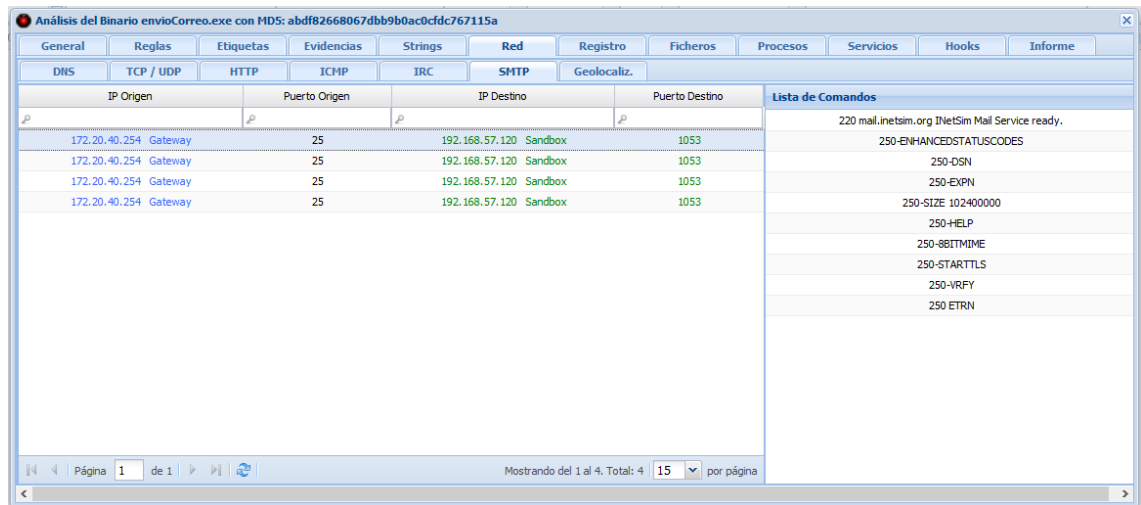
</

## IRC

Muestra todas las conexiones IRC realizadas durante el análisis. Seleccionando cada una de ellas, se muestran los comandos invocados.

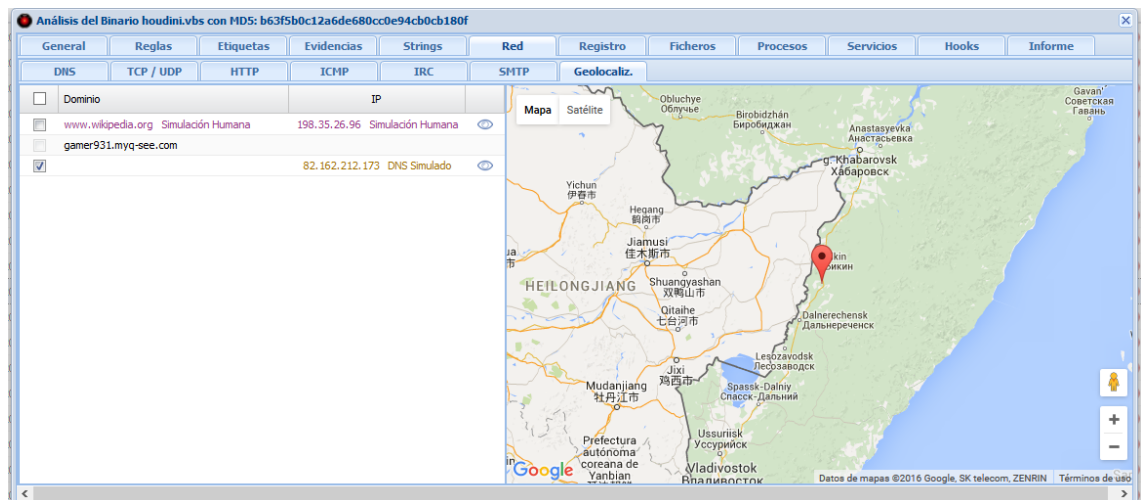
## SMTP

Muestra todas las conexiones SMTP realizadas durante el análisis. Seleccionando cada una de ellas, se muestran los comandos invocados.



### Geolocalización

Muestra los dominios e IP's del análisis, si se seleccionan de forma individual o múltiple los registros es posible ver en la parte derecha la geolocalización de los mismos.



## 10.7 CLAVES DE REGISTRO

Muestra información acerca de las claves de registro con las que se interactuó durante el análisis, separadas en subpestañas por acción: Abiertas, Leídas, Escritas y Eliminadas.

**Análisis del Binario 3f4db4b9036fbc752177ac14564f7c62 con MD5: 3f4db4b9036fbc752177ac14564f7c62**

| General                                                                                                                                 | Reglas | Etiquetas | Evidencias | Strings | Red | Registro | Ficheros | Procesos | Servicios | Hooks | Informe |
|-----------------------------------------------------------------------------------------------------------------------------------------|--------|-----------|------------|---------|-----|----------|----------|----------|-----------|-------|---------|
| Abiertas                                                                                                                                |        |           |            |         |     |          |          |          |           |       |         |
| Path                                                                                                                                    | Status |           |            |         |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\                                                                                                                      | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cryptography\Providers\Type 024\                                                                   | ✗      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)\ | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\                                                                    | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Offload\                                                                             | ✗      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\DESHashSessionKeyBackward\                                                           | ✗      |           |            |         |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\SOFTWARE\Microsoft\Cryptography\Providers\Type 001\                                                                   | ✗      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider\                           | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\                                                                                     | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName\                                                                       | ✓      |           |            |         |     |          |          |          |           |       |         |
| ActiveComputerName\                                                                                                                     | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\                                                                        | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\                                                                                     | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\                                                            | ✓      |           |            |         |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-57989841-1606980848-1957994488-1003\               | ✓      |           |            |         |     |          |          |          |           |       |         |

Página 1 de 5 | Mostrando del 1 al 15. Total: 71 | 15 por página

**Análisis del Binario 3f4db4b9036fbc752177ac14564f7c62 con MD5: 3f4db4b9036fbc752177ac14564f7c62**

| General                                                                 | Reglas            | Etiquetas                    | Evidencias | Strings | Red | Registro | Ficheros | Procesos | Servicios | Hooks | Informe |
|-------------------------------------------------------------------------|-------------------|------------------------------|------------|---------|-----|----------|----------|----------|-----------|-------|---------|
| Escritas                                                                |                   |                              |            |         |     |          |          |          |           |       |         |
| Path                                                                    | Name              | Data                         | Type       | Status  |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\       |                   |                              |            | ✓       |     |          |          |          |           |       |         |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\       | ofawygrn          | "C:\WINDOWS\phihiefiz.exe"   | REG_SZ     | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PhishingFilter\  |                   |                              |            | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PhishingFilter\  | EnabledV8         | 0                            | REG_DWORD  | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PhishingFilter\  | EnabledV9         | 0                            | REG_DWORD  | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name\            |                   |                              |            | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name\            |                   | C:\Documents and Settings... | REG_SZ     | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\                          |                   |                              |            | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\                          | OlkContactRefresh | 0                            | REG_DWORD  | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\                          | OlkFolderRefresh  | 0                            | REG_DWORD  | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Identities\                                           |                   |                              |            | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Identities\{C4FA31F4-BF1B-4FF1-978A-58670F63938C}\    | Identity Ordinal  | 1                            | REG_DWORD  | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Identities\                                           | Identity Ordinal  | 2                            | REG_DWORD  | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\ |                   |                              |            | ✓       |     |          |          |          |           |       |         |
| HKEY_CURRENT_USER\Software\Microsoft\Internet Account Manager\Accounts\ | AssociatedID      |                              | REG_BINARY | ✓       |     |          |          |          |           |       |         |

Página 1 de 5 | Mostrando del 1 al 15. Total: 66 | 15 por página

Se indica la ruta completa de la clave de registro, el nombre, el valor, el tipo y el estado de la acción (✓ *Correcto* o ✗ *Incorrecto*; por ejemplo, si se intentó abrir una clave y no existía, aparecerá en Abiertas con estado Incorrecto). Es posible filtrar por cualquiera de estos campos.

## 10.8 FICHEROS

Muestra información acerca de los ficheros con los que se interactuó durante el análisis separados en subpestañas por acción: Abiertos, Leídos, Escritos y Eliminados.

Análisis del Binario ccn\_malo33.exe con MD5: 6f2b84cb1f3a256c62d9561cb7e3e9b1

General

Reglas

Etiquetas

Evidencias

Strings

Red

Registro

Ficheros

Procesos

Servicios

Hooks

Informe

Abiertos

Leídos

Escritos

Eliminados

Ejecutados

Movidos

Copiados

| Nombre del Fichero | Ruta Completa                                       | MD5                               | Tamaño    | Estado |
|--------------------|-----------------------------------------------------|-----------------------------------|-----------|--------|
|                    | PIPE\lsarpc                                         | 9e6c8eab97aa64260b272fd77fa88ca2  | 200 bytes |        |
| wtray.exe          | C:\DOCUME~1\User\LOCALS~1\Temp\XP000.TMP\wtray.exe  | 5e998c060005f2fbbad07e5f7e1d57e7  | 332 KB    |        |
| type.dll           | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\type.dll   | 98e83379d45538379c2ac4e47c3be81d  | 3 bytes   |        |
| ass.dll            | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\ass.dll    | a87ff679a2f3e71d9181a67b7542122c  | 1 bytes   |        |
| sdcc.dll           | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\sdcc.dll   | 0af629b1df207fd25f221a50059140a5  | 36 bytes  |        |
| mail.dll           | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\mail.dll   | f78dc2c2f7c86ce6964bda1c879facc   | 17 bytes  |        |
| webas.dll          | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\webas.dll  | c4ca4238a0b923820dccc509a6f75849b | 1 bytes   |        |
| resu.dll           | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\resu.dll   | 73acd9a5972130b75066c82595a1fae3  | 5 bytes   |        |
| ssap.dll           | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\ssap.dll   | 73acd9a5972130b75066c82595a1fae3  | 5 bytes   |        |
| seek.dll           | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\seek.dll   | c4ca4238a0b923820dccc509a6f75849b | 1 bytes   |        |
| seekl.dll          | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\seekl.dll  | cfcd208495d565ef66e7dfff9f8764da  | 1 bytes   |        |
| scen.dll           | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\scen.dll   | c4ca4238a0b923820dccc509a6f75849b | 1 bytes   |        |
| scint.dll          | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\scint.dll  | c0c7c76d30bd3dcaefc96f40275bdc0a  | 2 bytes   |        |
| scint2.dll         | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\scint2.dll | c4ca4238a0b923820dccc509a6f75849b | 1 bytes   |        |
| scde.dll           | C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\scde.dll   | cfcd208495d565ef66e7dfff9f8764da  | 1 bytes   |        |

Página 1 de 4

Mostrando del 1 al 15. Total: 54

15

por página

Si el análisis proviene de la sandbox Cuckoo, también se muestra información de los ficheros Ejecutados, Movidos y Copiados.

●

Análisis del Binario ccn\_malo33.exe con MD5: 6f2b84cb1f3a256c62d9561cb7e3e9b1

General

Reglas

Etiquetas

Evidencias

Strings

Red

Registro

Ficheros

Procesos

Servicios

Hooks

Informe

Abiertos

Leídos

Escritos

Eliminados

Ejecutados

Movidos

Copiados

| Nombre del Fichero                                     | Ruta Completa                                         | MD5                              | Tamaño    | Estado |
|--------------------------------------------------------|-------------------------------------------------------|----------------------------------|-----------|--------|
| wtray.exe                                              | C:\DOCUME~1\User\LOCALS~1\Temp\XP000.TMP\wtray.exe    | 5e998c060005f2ffb07e5f7e1d57e7   | 332 KB    | ✓      |
| Korekars.exe                                           | C:\DOCUME~1\User\LOCALS~1\Temp\XP000.TMP\Korekars.exe | b0c4fc6957f6b8628f42886d880df2f7 | 1 MB      | ✓      |
| "C:\DOCUME~1\User\LOCALS~1\Temp\Compresso\desktop.exe" |                                                       |                                  |           | ✓      |
| cmd /c echo y                                          | C:\WINDOWS\system32\cmd.exe /S /D /c echo y           |                                  |           | ✓      |
| cmd /c echo y                                          | C:\WINDOWS\system32\cmd.exe /S /D /c echo y           |                                  |           | ✓      |
| csrss.exe                                              | C:\WINDOWS\system32\csrss.exe                         |                                  |           | ✓      |
| services.exe                                           | C:\WINDOWS\system32\services.exe                      |                                  |           | ✓      |
| c" echo y"                                             | C:\WINDOWS\system32\cmd.exe /S /D /c echo y"          |                                  |           | ✓      |
| c" echo y"                                             | C:\WINDOWS\system32\cmd.exe /S /D /c echo y"          | 9e6c8eab97aa64260b272fd77fa88ca2 | 200 bytes | ✓      |
| services.exe                                           | C:\WINDOWS\system32\services.exe                      | 9e6c8eab97aa64260b272fd77fa88ca2 | 200 bytes | ✓      |
| taskmgr.exe                                            | C:\WINDOWS\system32\taskmgr.exe                       |                                  |           | ✓      |
| msn64.exe                                              | C:\WINDOWS\system32\msn64.exe                         |                                  |           | ✓      |
| taskmgr.exe                                            | C:\WINDOWS\system32\taskmgr.exe                       | 9e6c8eab97aa64260b272fd77fa88ca2 | 200 bytes | ✓      |

1

de 1

Mostrando del 1 al 15. Total: 15

15

por página

Se indica el nombre del fichero, la ruta completa, el MD5, el tamaño y el estado de la acción (✓ Correcto o ✗ Incorrecto; por ejemplo, si se intentó abrir un fichero y no existía, aparecerá en Abiertos con estado Incorrecto). Es posible filtrar por cualquiera de estos campos.

## 10.9 PROCESOS

Muestra información acerca de los procesos creados durante el análisis.

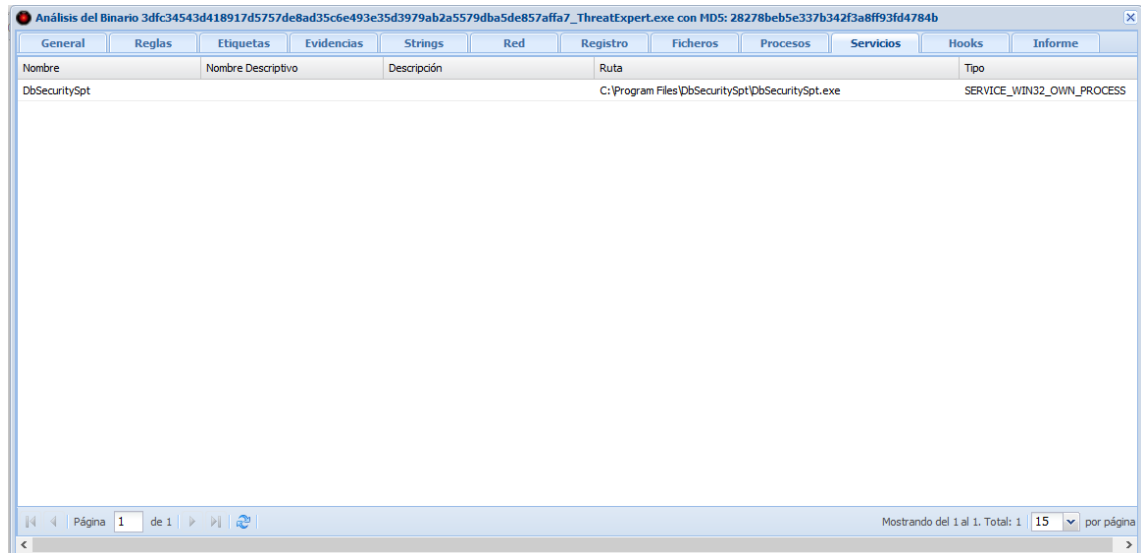
Análisis del Binario 64bbe260b9ff2fe877ade2dac2eac000 con MD5: 64bbe260b9ff2fe877ade2dac2eac000

| General                                                      | Reglas | Etiquetas | Evidencias | Strings                                                           | Red | Registro | Ficheros | Procesos          | Servicios | Hooks     | Informe |  |
|--------------------------------------------------------------|--------|-----------|------------|-------------------------------------------------------------------|-----|----------|----------|-------------------|-----------|-----------|---------|--|
| Process Name / Handle Name                                   |        |           |            | Process Path / Handle Type                                        |     | PID      | Parent   | Process Arguments |           | Terminado |         |  |
| 64bbe260b9ff2fe877ade2dac2eac000.exe                         |        |           |            | C:\DOCUME~1\user\LOCALS~1\Temp\64bbe260b9ff2fe877ade2dac2eac00... |     | 1312     | 192      |                   |           | ✓         |         |  |
| 64bbe260b9ff2fe877ade2dac2eac000.exe                         |        |           |            | C:\DOCUME~1\user\LOCALS~1\Temp\64bbe260b9ff2fe877ade2dac2eac00... |     | 1732     | 1312     |                   |           | ✓         |         |  |
| explorer.exe                                                 |        |           |            | C:\WINDOWS\explorer.exe                                           |     | 236      | 1732     |                   |           | ✓         |         |  |
| vssadmin.exe                                                 |        |           |            | C:\WINDOWS\system32\vssadmin.exe                                  |     | 460      | 236      |                   |           | ✓         |         |  |
| Global\luhegonaguholahevevupotrajlo                          |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |
| CTF.TimListCache.FMPDefaultS-1-5-21-57989841-160698084       |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |
| MPSWabDataAccessMutex                                        |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |
| MPSWABOlkStoreNotifyMutex                                    |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |
| Global\ufutuvikomefykjibidohi                                |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |
| Global\luhegonaguholahevevupotrajlo                          |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |
| CTF.TimListCache.FMPDefaultS-1-5-21-57989841-1606980848-1957 |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |
| ShimCacheMutex                                               |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |
| qazwsxedc                                                    |        |           |            | Mutant                                                            |     |          |          |                   |           |           |         |  |

Se indica el nombre del proceso, la ruta completa a su ejecutable, el PID y los argumentos de ejecución. Si se despliega un proceso, se pueden ver sus mutex. Se indica su nombre y su tipo.

## 10.10 SERVICIOS

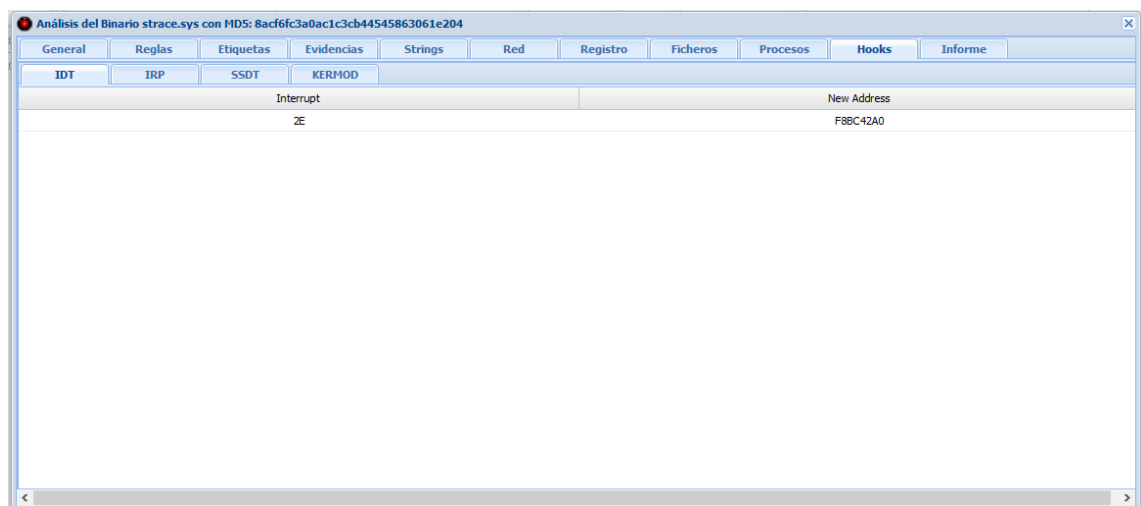
Muestra información acerca de los servicios de sistema operativo creados durante el análisis.



Se indica el nombre del servicio, el nombre descriptivo, la descripción, la ruta completa a su ejecutable y el tipo de servicio.

## 10.11 HOOKS

Muestra información de los hooks creados por la muestra. Actualmente se detectan 4 tipos de hooks IDT, IRP, SSDT y KERMID.

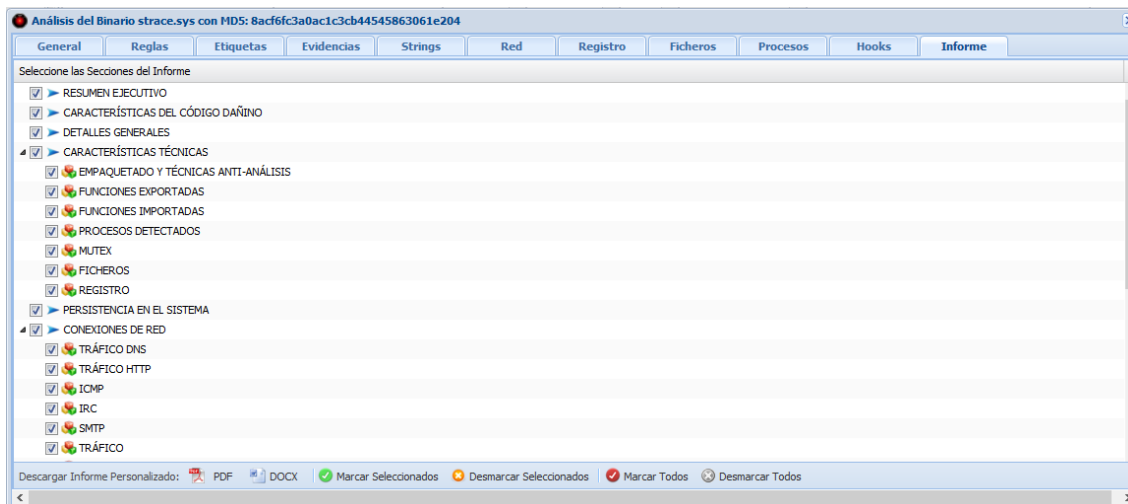


● Análisis del Binario strace.sys con MD5: 8acf6fc3a0ac1c3cb44545863061e204

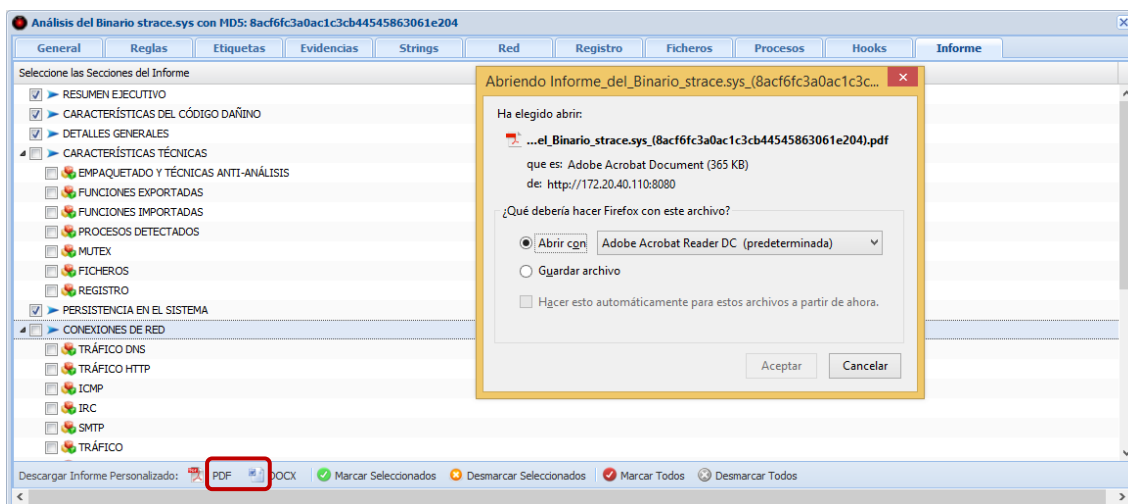
| General                        | Reglas | Etiquetas | Evidencias        | Strings | Red      | Registro | Ficheros | Procesos | Hooks | Informe |
|--------------------------------|--------|-----------|-------------------|---------|----------|----------|----------|----------|-------|---------|
| IDT                            | IRP    | SSDT      | KERMOD            |         |          |          |          |          |       |         |
| Handler Function               |        |           | Driver            |         | Address  |          |          |          |       |         |
| IRP_MJ_CLEANUP                 |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_CLOSE                   |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_CREATE                  |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_CREATE_MAILSLOT         |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_CREATE_NAMED_PIPE       |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_DEVICE_CHANGE           |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_DEVICE_CONTROL          |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_DIRECTORY_CONTROL       |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_FILE_SYSTEM_CONTROL     |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_FLUSH_BUFFERS           |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_INTERNAL_DEVICE_CONTROL |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_LOCK_CONTROL            |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_PNP                     |        |           | \Driver\pLlYTrDXY |         | 804F354A |          |          |          |       |         |
| IRP_MJ_POWER                   |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_QUERY_EA                |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_QUERY_INFORMATION       |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_QUERY_QUOTA             |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |
| IRP_MJ_QUERY_SECURITY          |        |           | \Driver\pLlYTrDXY |         | F88C47AA |          |          |          |       |         |

## 10.12 INFORME PERSONALIZADO

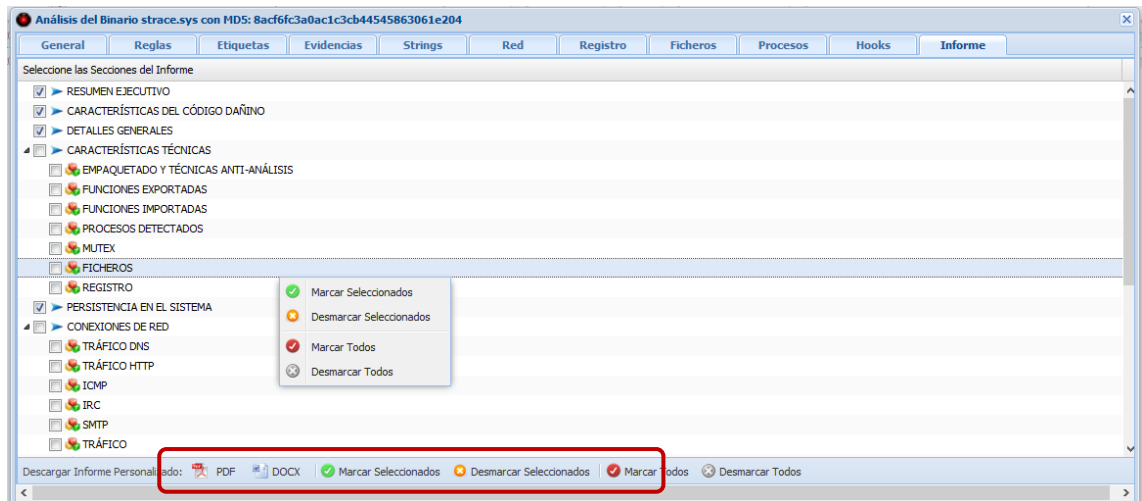
Permite crear un informe del análisis a medida, eligiendo qué secciones se desea que aparezcan.



Para generar el informe, debemos seleccionar qué secciones queremos incluir en él marcando las casillas de selección de la lista y a continuación hacer clic en uno de los botones de   **Descargar Informe Personalizado** de la barra de herramientas de la parte inferior de la pestaña, en función del formato en el que queramos descargar el informe, entre PDF y Docx.

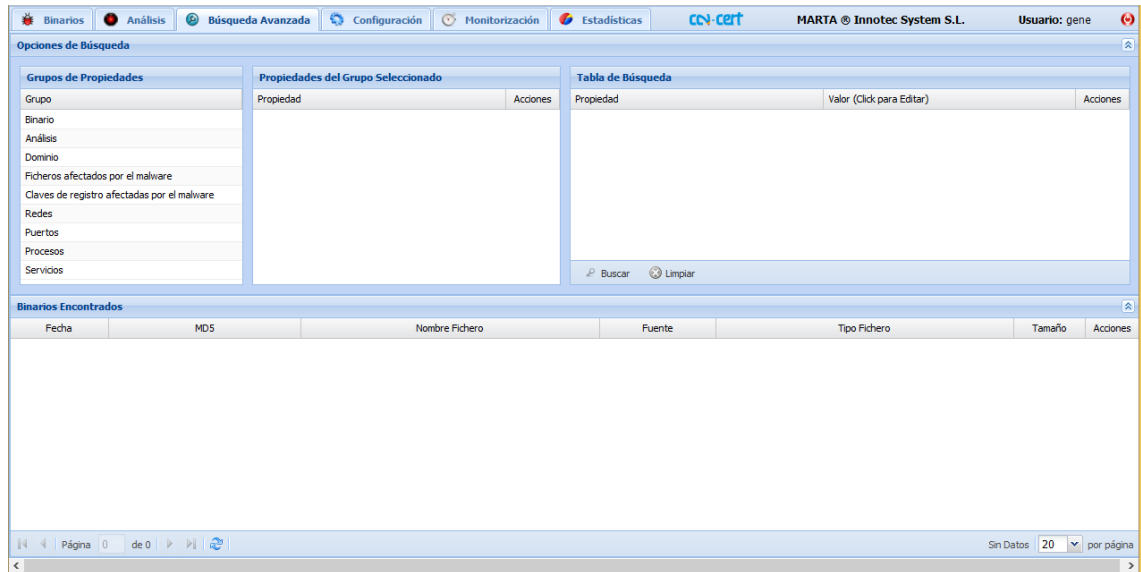


La de herramientas, además, cuenta con botones que nos facilitan el marcado de las casillas de selección:  **Marcar Seleccionados**,  **Desmarcar Seleccionados**,  **Marcar Todos** y  **Desmarcar Todos**. Estas acciones también están disponibles haciendo clic con el botón derecho del ratón sobre la lista de secciones.

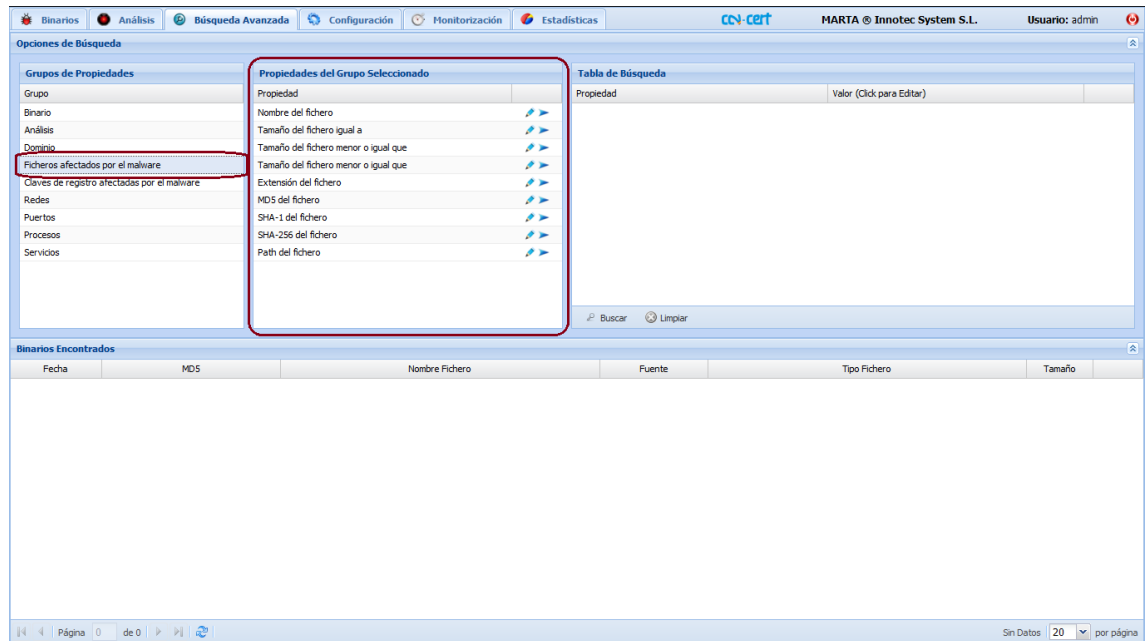


## 11 PESTAÑA DE BÚSQUEDA AVANZADA

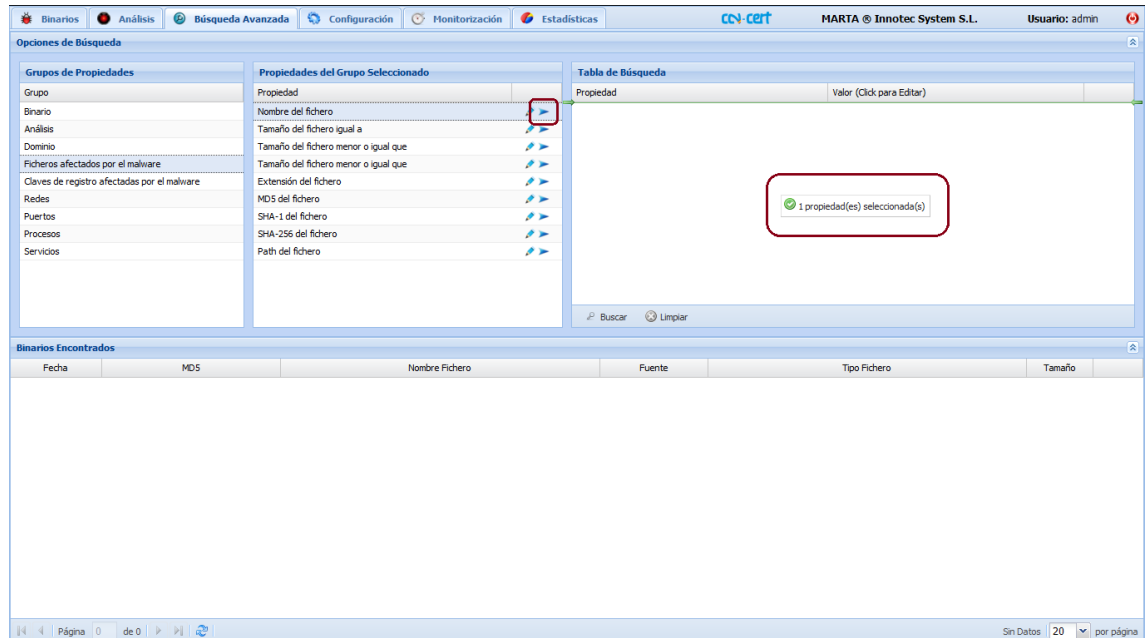
Esta pestaña está diseñada para facilitar la búsqueda de ficheros con unos atributos o un comportamiento o determinado. Permite buscar ficheros filtrando por cualquier dato que pudiera obtenerse tanto de los resultados de los scripts estáticos como de los análisis dinámicos.



Como hay una gran cantidad de posibles datos diferentes, se agrupan en Grupos de Propiedades, que podemos ver en la lista de la izquierda de la parte superior. Seleccionando un grupo de propiedades, se cargan todas sus propiedades en la lista central de la parte superior.



Ahora podemos seleccionar una propiedad y arrastrarla a la lista de la derecha de la de la parte superior (o pasarla haciendo clic en la acción ➤ **Agregar Propiedad a la Tabla de Búsqueda** de la tabla central). La lista de la derecha es la **Tabla de Búsqueda**. En esta tabla ponemos los criterios por los que queremos buscar.



Binarios | **Análisis** | Búsqueda Avanzada | Configuración | Monitorización | Estadísticas | CN-CERT | MARTA © Innotec System S.L. | Usuario: admin

**Opciones de Búsqueda**

| Grupo                                       | Propiedad                            | Valor (Click para Editar) |
|---------------------------------------------|--------------------------------------|---------------------------|
| Binario                                     | Nombre del fichero                   | Nombre del fichero        |
| Análisis                                    | Tamaño del fichero igual a           |                           |
| Dominio                                     | Tamaño del fichero menor o igual que |                           |
| Ficheros afectados por el malware           | Extensión del fichero                |                           |
| Claves de registro afectadas por el malware | MDS del fichero                      |                           |
| Redes                                       | SHA-1 del fichero                    |                           |
| Puertos                                     | SHA-256 del fichero                  |                           |
| Procesos                                    | Path del fichero                     |                           |
| Servicios                                   |                                      |                           |

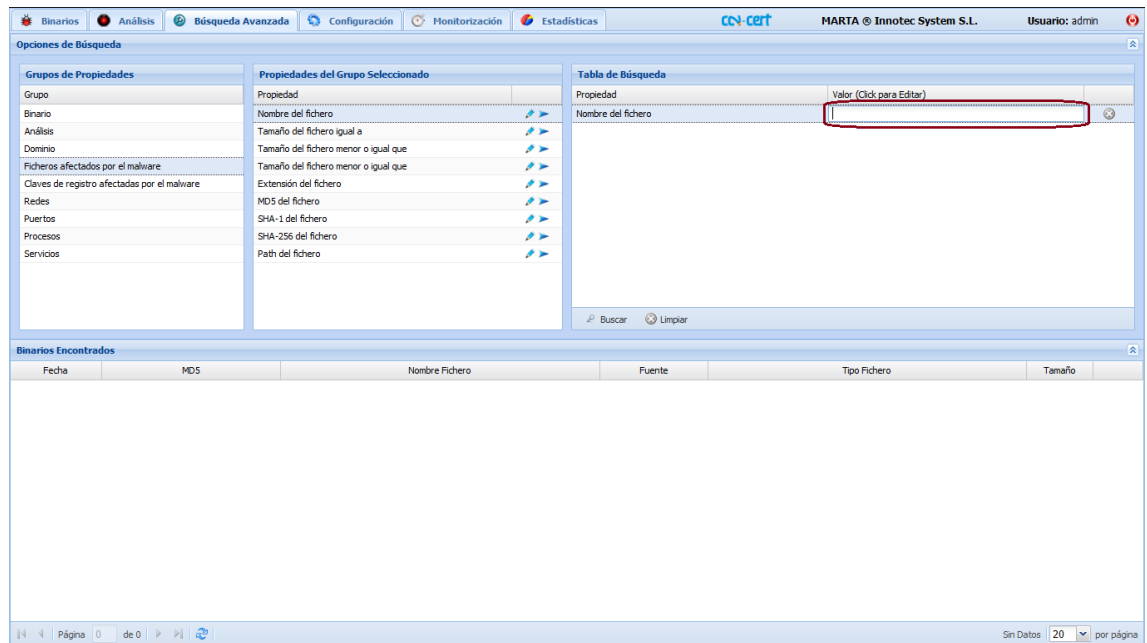
Buscar Limpia

**Binarios Encontrados**

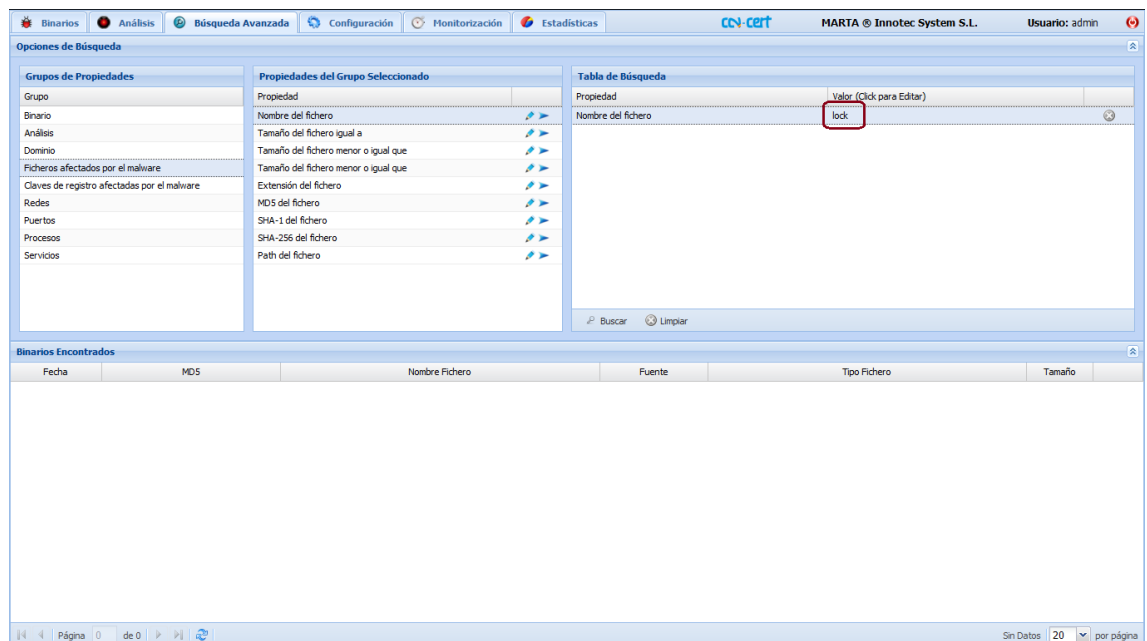
| Fecha | MDS | Nombre Fichero | Fuente | Tipo Fichero | Tamaño |
|-------|-----|----------------|--------|--------------|--------|
|-------|-----|----------------|--------|--------------|--------|

Página 0 de 0 | Sin Datos: 20 por página

Haciendo clic en el Valor de una propiedad de la tabla de búsqueda, podemos editarlo:



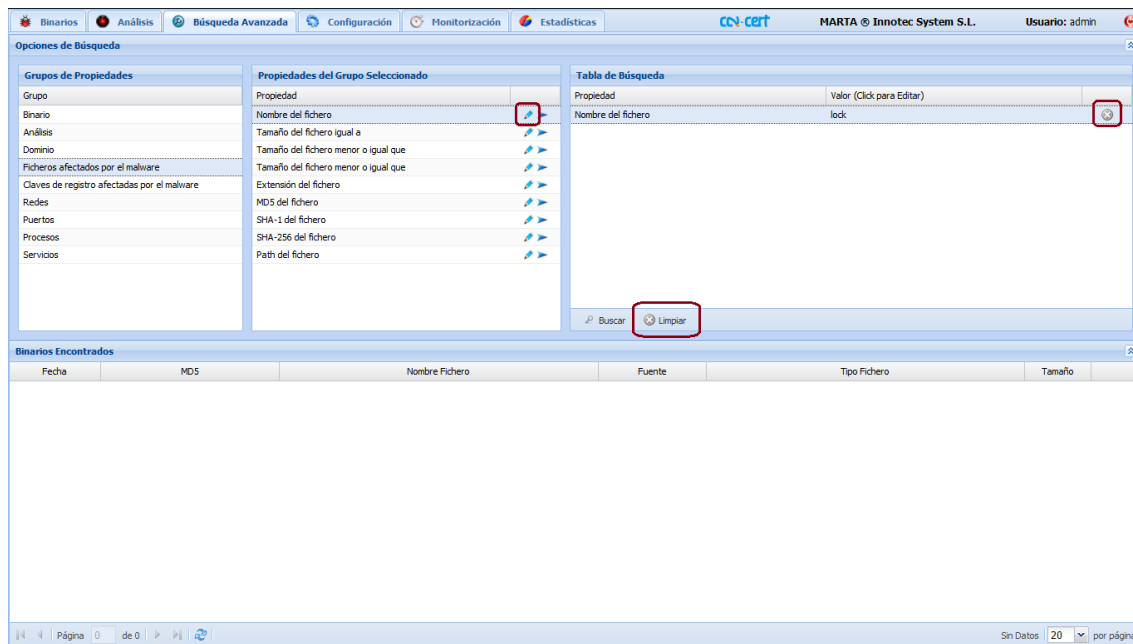
The screenshot shows the MARTA application interface. The top navigation bar includes tabs for Binarios, Análisis, Búsqueda Avanzada (selected), Configuración, Monitorización, and Estadísticas. The user is logged in as 'admin'. The 'Opciones de Búsqueda' section is active, displaying a list of properties on the left and a table of search results on the right. The table has columns for Propiedad, Valor (Click para Editar), and a search icon. The 'Valor' column for the first row is highlighted with a red box.



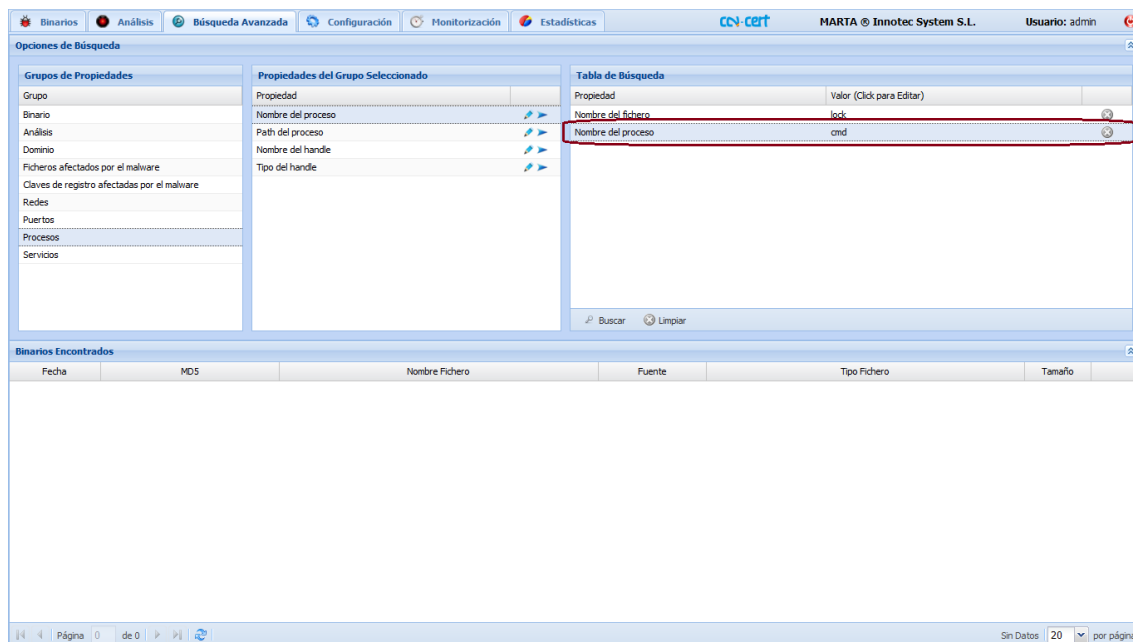
The screenshot shows the same MARTA application interface. In the 'Tabla de Búsqueda' table, the 'lock' value in the 'Valor' column is highlighted with a red box, indicating the search criteria. The 'lock' value is entered in the 'Valor (Click para Editar)' field.

En este momento, tenemos un criterio: buscar todos los códigos dañinos que interactúen con un fichero que contenga la palabra "lock" en su nombre.

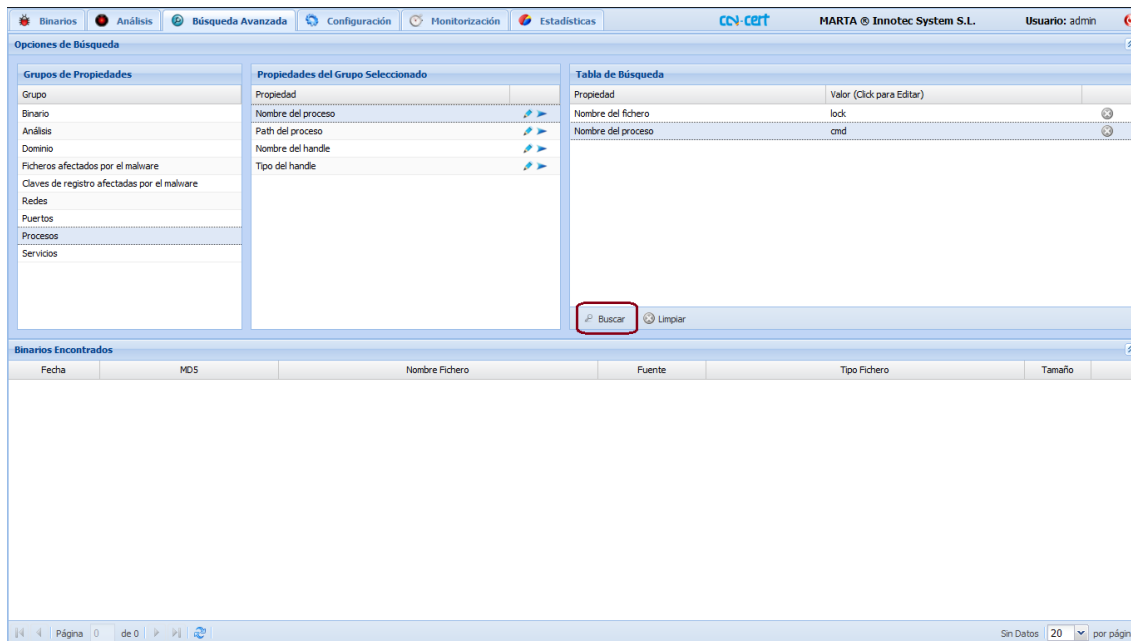
Podemos quitar criterios de la tabla de búsqueda arrastrándolos hacia la tabla central de la parte superior, o clicando en la acción  **Quitar Propiedad de la Tabla de Búsqueda**. O podemos quitarlos todos haciendo clic en el botón  **Limpiar** de la barra de herramientas inferior de la tabla de búsqueda. También podemos sustituir una propiedad de la tabla de búsqueda por otra de la tabla central haciendo clic en la acción  **Modificar las Propiedades Seleccionadas de la Tabla de Búsqueda**.



Vamos a añadir un segundo criterio: buscar todos los códigos dañinos que creen un proceso que contenga la palabra "cmd" en su nombre.



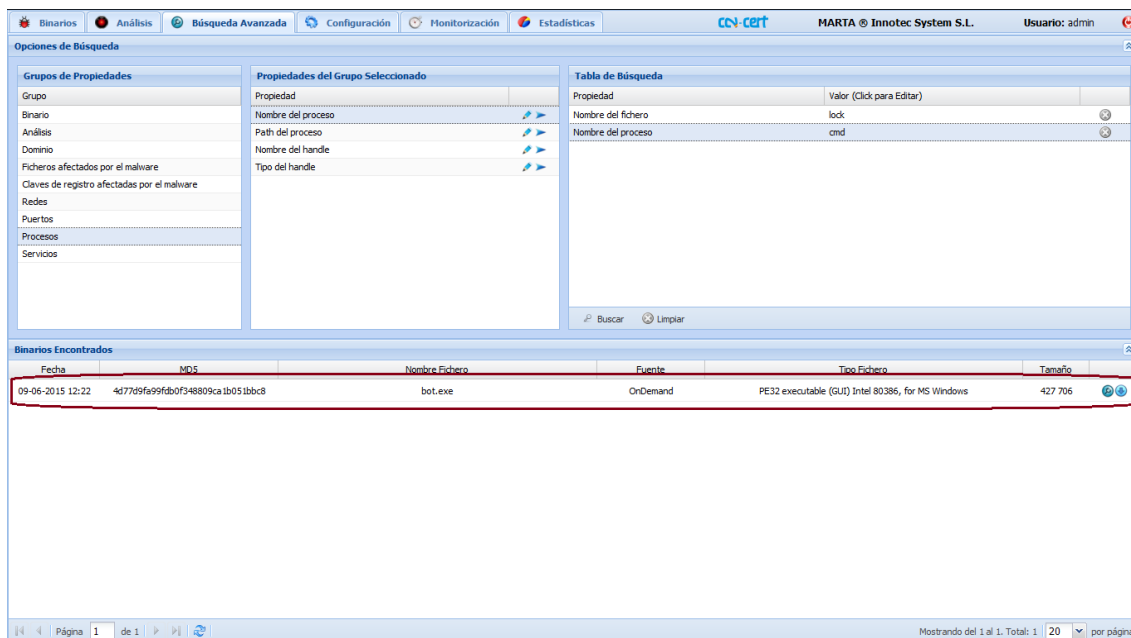
Una vez hemos definido los criterios de búsqueda, hacemos clic en el botón  **Buscar** de la barra de herramientas inferior de la tabla de búsqueda. En este caso, buscaremos códigos dañinos que interactúen con un fichero llamado lock y creen un proceso llamado cmd.



The screenshot shows the 'Opciones de Búsqueda' (Search Options) section. On the left, under 'Grupos de Propiedades', the 'Procesos' (Processes) group is selected. In the center, 'Propiedades del Grupo Seleccionado' (Properties of the Selected Group) lists: Nombre del proceso, Path del proceso, Nombre del handle, and Tipo del handle. On the right, the 'Tabla de Búsqueda' (Search Table) has two rows: 'Nombre del fichero' with value 'lock' and 'Nombre del proceso' with value 'cmd'. At the bottom of this table, the 'Buscar' button is highlighted with a red rectangle. Below the search options is the 'Binarios Encontrados' (Found Binaries) table, which is currently empty.

| Fecha | MD5 | Nombre Fichero | Fuente | Tipo Fichero | Tamaño |
|-------|-----|----------------|--------|--------------|--------|
|-------|-----|----------------|--------|--------------|--------|

La búsqueda suele tardar un par de segundos. Cuando finaliza, se rellena la tabla inferior con los códigos dañinos encontrados.



This screenshot shows the same search interface as the previous one, but now the 'Binarios Encontrados' table contains one result. The 'Buscar' button is still highlighted with a red rectangle.

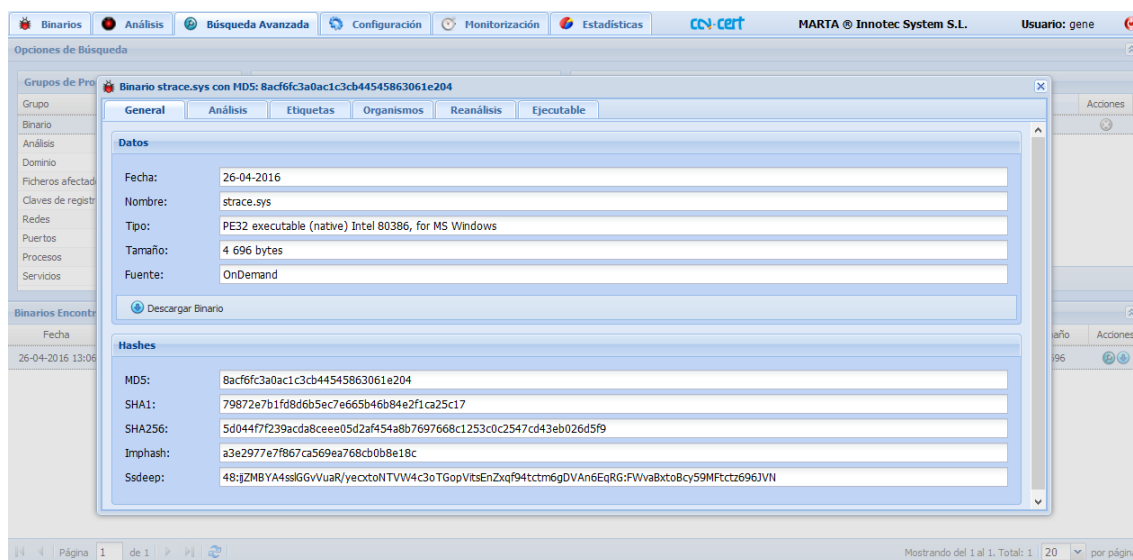
| Fecha            | MD5                              | Nombre Fichero | Fuente   | Tipo Fichero                                      | Tamaño  |
|------------------|----------------------------------|----------------|----------|---------------------------------------------------|---------|
| 09-06-2015 12:22 | 4d7709fa99fdb0f348809ca1b051bbc8 | bot.exe        | OnDemand | PE32 executable (GUI) Intel 80386, for MS Windows | 427 706 |

En este caso sólo hay uno: bot.exe.

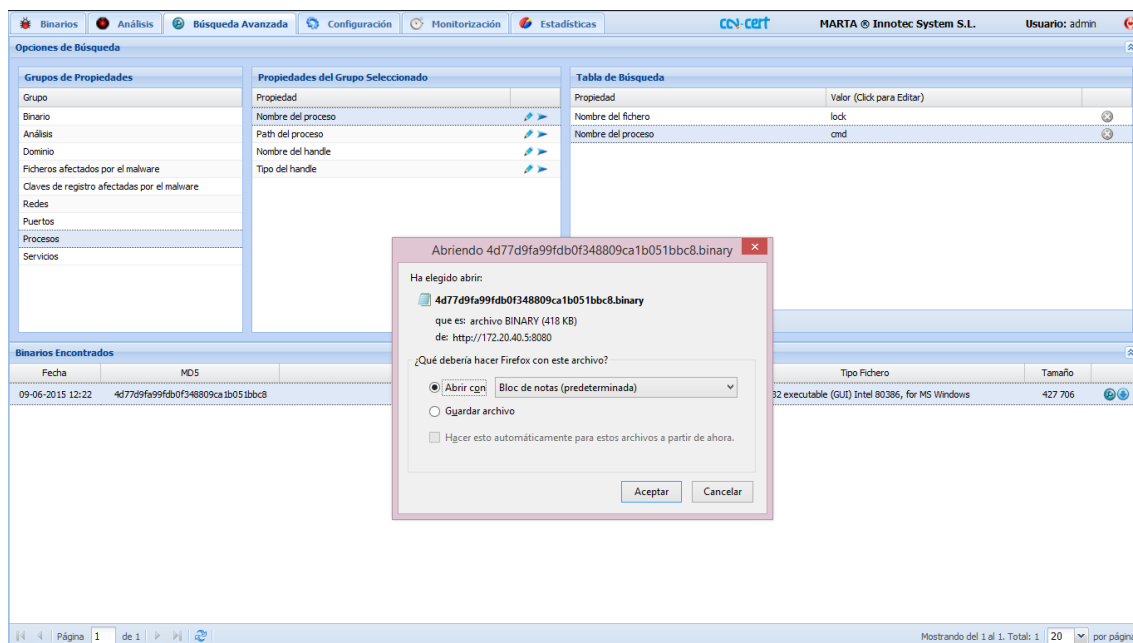


La tabla inferior muestra los datos más relevantes de los ficheros que cumplen los criterios de búsqueda definidos: la fecha en la que se subió, su MD5, su nombre, su fuente, su tipo y su tamaño. Además, permite realizar acciones sobre ellos:

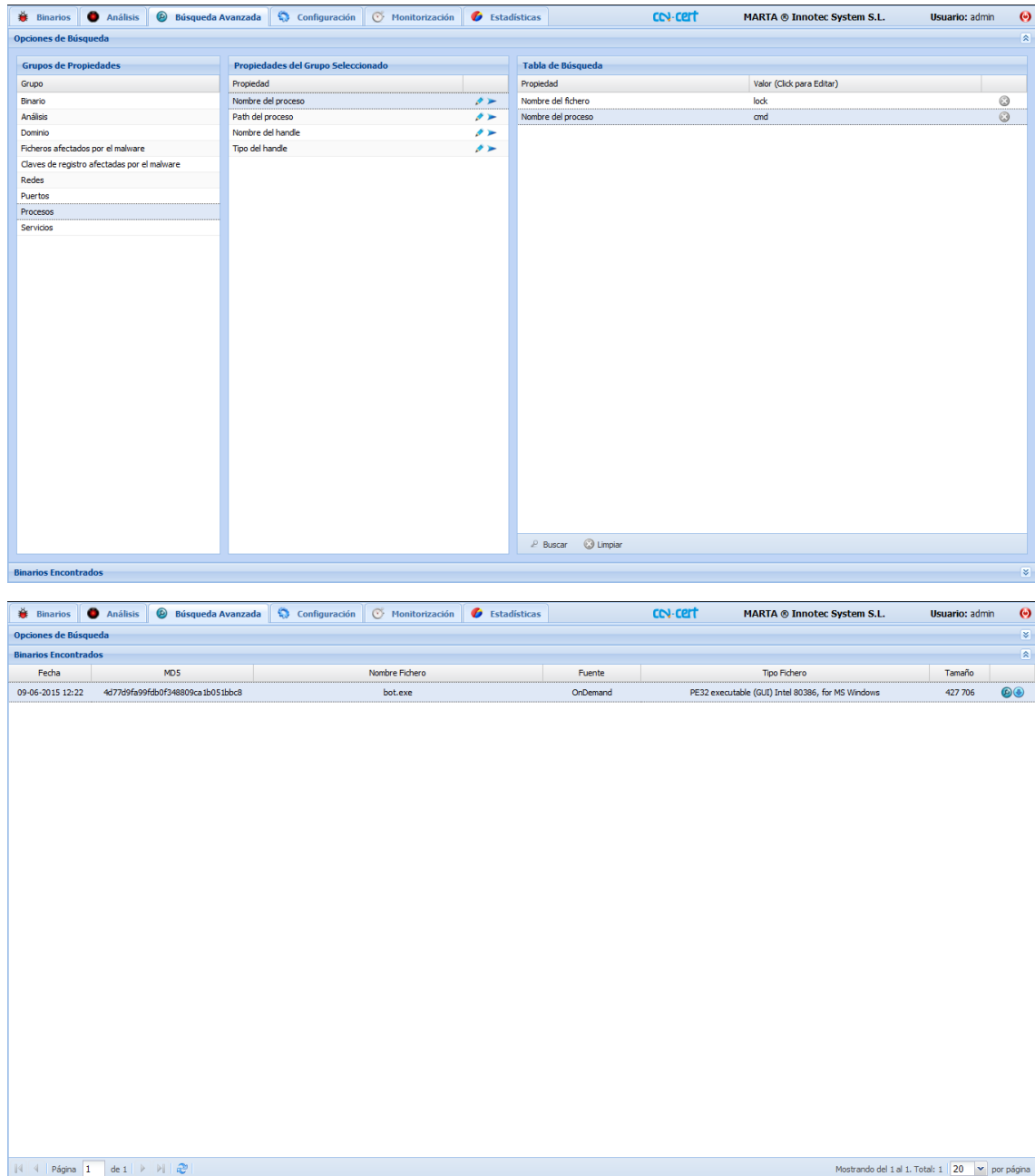
-  **Ver Detalle:** Abre la vista de detalles del fichero seleccionado. Esta vista contiene toda la información relativa a un fichero. Se describe en la sección [Vista de Detalle de un Binario](#) de este documento.



-  **Descargar Binario:** Descarga el fichero seleccionado. Esta acción debe realizarse con precaución ya que el fichero descargado podría ser un malware. El fichero se descarga con su MD5 como nombre, y con extensión .binary, para evitar que lo ejecutemos por error al descargarlo.



Por comodidad, tanto las partes de las tres listas superiores como la lista inferior son plegables:



**Opciones de Búsqueda**

**Grupos de Propiedades**

Grupo

Binario

Análisis

Dominio

Ficheros afectados por el malware

Claves de registro afectadas por el malware

Redes

Puertos

Procesos

Servicios

**Propiedades del Grupo Seleccionado**

Propiedad

Nombre del proceso

Path del proceso

Nombre del handle

Tipo del handle

**Tabla de Búsqueda**

| Propiedad          | Valor (Click para Editar) |
|--------------------|---------------------------|
| Nombre del fichero | lock                      |
| Nombre del proceso | cmd                       |

Buscar Limpiar

**Binarios Encontrados**

| Fecha            | MD5                              | Nombre Fichero | Fuente   | Tipo Fichero                                      | Tamaño  |
|------------------|----------------------------------|----------------|----------|---------------------------------------------------|---------|
| 09-06-2015 12:22 | 4d77d9fa99fdb0f348809ca1b051bbc8 | bot.exe        | OnDemand | PE32 executable (GUI) Intel 80386, for MS Windows | 427 706 |

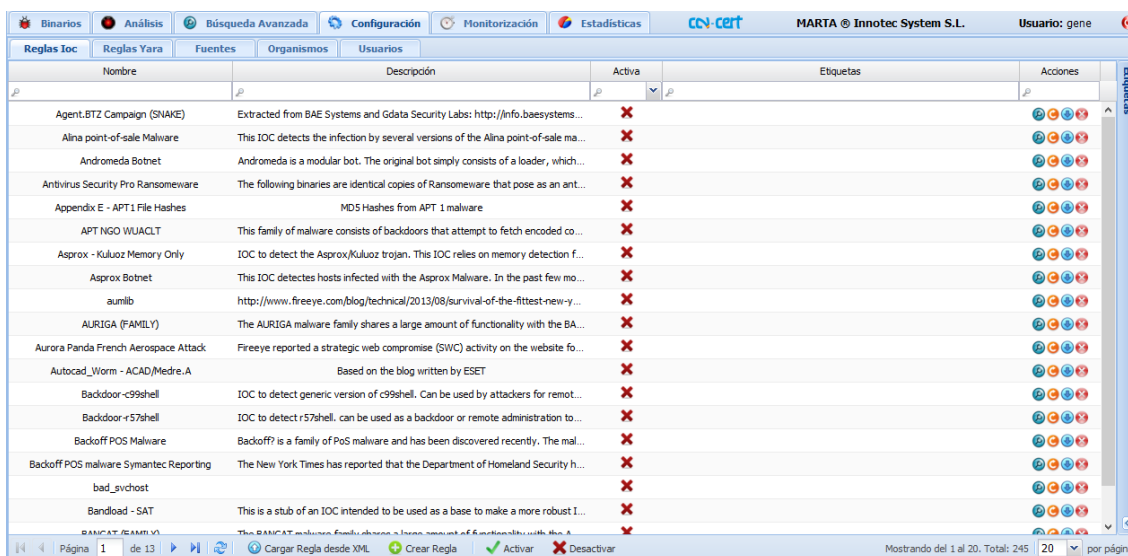
Página 1 de 1

Mostrando del 1 al 1. Total: 1 20 por página

## 12 PESTAÑA DE CONFIGURACIÓN

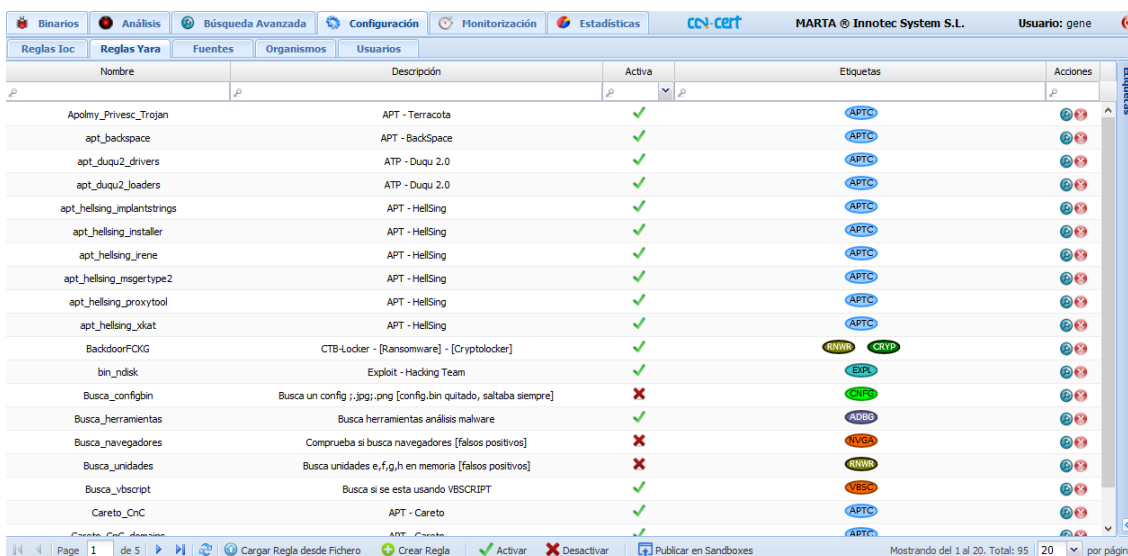
Esta pestaña engloba un conjunto de pestañas relacionadas con la configuración de MARTA:

- **Reglas Ioc:** Facilita todas las gestiones relacionadas con el motor de reglas de IOC's.



| Nombre                                 | Descripción                                                                         | Activa | Etiquetas | Acciones |
|----------------------------------------|-------------------------------------------------------------------------------------|--------|-----------|----------|
| Agent.BTZ Campaign (SNAKE)             | Extracted from BAE Systems and Gdata Security Labs: http://info.baesystems...       | ✗      |           |          |
| Alina point-of-sale Malware            | This IOC detects the infection by several versions of the Alina point-of-sale ma... | ✗      |           |          |
| Andromeda Botnet                       | Andromeda is a modular bot. The original bot simply consists of a loader, which...  | ✗      |           |          |
| Antivirus Security Pro Ransomware      | The following binaries are identical copies of Ransomware that pose as an ant...    | ✗      |           |          |
| Appendix E - APT1 File Hashes          | MDS Hashes from APT 1 malware                                                       | ✗      |           |          |
| APT NGO WUACLT                         | This family of malware consists of backdoors that attempt to fetch encoded co...    | ✗      |           |          |
| Asprox - Kuluoz Memory Only            | IOC to detect the Asprox/Kuluoz trojan. This IOC relies on memory detection f...    | ✗      |           |          |
| Asprox Botnet                          | This IOC detects hosts infected with the Asprox Malware. In the past few mo...      | ✗      |           |          |
| aurmb                                  | http://www.freeeye.com/blog/technical/2013/08/survival-of-the-fittest-new-y...      | ✗      |           |          |
| AURIGA (FAMILY)                        | The AURIGA malware family shares a large amount of functionality with the BA...     | ✗      |           |          |
| Aurora Panda French Aerospace Attack   | Freeeye reported a strategic web compromise (SWC) activity on the website fo...     | ✗      |           |          |
| Autocad_Worm - ACAD/Medre.A            | Based on the blog written by ESET                                                   | ✗      |           |          |
| Backdoor-c99shell                      | IOC to detect generic version of c99shell. Can be used by attackers for remot...    | ✗      |           |          |
| Backdoor-r57shell                      | IOC to detect r57shell. can be used as a backdoor or remote administration to ...   | ✗      |           |          |
| Backoff POS Malware                    | Backoff? is a family of PoS malware and has been discovered recently. The mal...    | ✗      |           |          |
| Backoff POS malware Symantec Reporting | The New York Times has reported that the Department of Homeland Security h...       | ✗      |           |          |
| bad_svchost                            |                                                                                     | ✗      |           |          |
| Bandload - SAT                         | This is a stub of an IOC intended to be used as a base to make a more robust I...   | ✗      |           |          |
| BANCAT FAMILY                          | The BANCAT malware family shares a large amount of functionality with the A...      | ✗      |           |          |

- **Reglas Yara:** Facilita todas las gestiones relacionadas con el motor de reglas Yara.



| Nombre                      | Descripción                                                      | Activa | Etiquetas  | Acciones |
|-----------------------------|------------------------------------------------------------------|--------|------------|----------|
| Apolmy_Privesc_Trojan       | APT - Terracota                                                  | ✓      | APT        |          |
| apt_backspace               | APT - BackSpace                                                  | ✓      | APT        |          |
| apt_duqu2_drivers           | ATP - Duqu 2.0                                                   | ✓      | APT        |          |
| apt_duqu2_loaders           | ATP - Duqu 2.0                                                   | ✓      | APT        |          |
| apt_hellsing_implantstrings | APT - Hellsing                                                   | ✓      | APT        |          |
| apt_hellsing_installer      | APT - Hellsing                                                   | ✓      | APT        |          |
| apt_hellsing_irene          | APT - Hellsing                                                   | ✓      | APT        |          |
| apt_hellsing_msgertype2     | APT - Hellsing                                                   | ✓      | APT        |          |
| apt_hellsing_proxytool      | APT - Hellsing                                                   | ✓      | APT        |          |
| apt_hellsing_xlat           | APT - Hellsing                                                   | ✓      | APT        |          |
| BackdoorFCG                 | CTB-Locker - [Ransomware] - [Cryptolocker]                       | ✓      | RNWR, CRYP |          |
| bin_ndisk                   | Exploit - Hacking Team                                           | ✓      | EXPL       |          |
| Busca_configbin             | Busca un config .jpg; .png [config.bin quitado, saltaba siempre] | ✗      | EXPL       |          |
| Busca_herramientas          | Busca herramientas análisis malware                              | ✓      | ADBD       |          |
| Busca_navegadores           | Comprueba si busca navegadores [falsos positivos]                | ✗      | MYGA       |          |
| Busca_unidades              | Busca unidades e,f,g,h en memoria [falsos positivos]             | ✗      | RNWR       |          |
| Busca_vbscript              | Busca si se esta usando VBSCRIPT                                 | ✓      | VESC       |          |
| Careto_CnC                  | APT - Careto                                                     | ✓      | APT        |          |
| Careto_CnC                  | APT - Careto                                                     | ✓      | APT        |          |

## 13 PESTAÑA DE REGLAS IOC

Esta pestaña está diseñada para facilitar todas las gestiones relativas al motor de reglas de MARTA.

| Reglas IOC                             |                                                                                     |        |           |  |          |  |
|----------------------------------------|-------------------------------------------------------------------------------------|--------|-----------|--|----------|--|
| Nombre                                 | Descripción                                                                         | Activa | Etiquetas |  | Acciones |  |
| Agent.BTZ Campaign (SNAKE)             | Extracted from BAE Systems and Gdata Security Labs: http://info.baesystems...       | ✗      |           |  |          |  |
| Alina point-of-sale Malware            | This IOC detects the infection by several versions of the Alina point-of-sale ma... | ✗      |           |  |          |  |
| Andromeda Botnet                       | Andromeda is a modular bot. The original bot simply consists of a loader, which...  | ✗      |           |  |          |  |
| Antivirus Security Pro Ransomware      | The following binaries are identical copies of Ransomware that pose as an ant...    | ✗      |           |  |          |  |
| Appendix E - APT1 File Hashes          | MDS Hashes from APT 1 malware                                                       | ✗      |           |  |          |  |
| APT NGO WUACLT                         | This family of malware consists of backdoors that attempt to fetch encoded co...    | ✗      |           |  |          |  |
| Asprox - Kuloz Memory Only             | IOC to detect the Asprox/Kuloz trojan. This IOC relies on memory detection f...     | ✗      |           |  |          |  |
| Asprox Botnet                          | This IOC detects hosts infected with the Asprox Malware. In the past few mo...      | ✗      |           |  |          |  |
| aulmb                                  | http://www.freeeye.com/blog/technical/2013/08/survival-of-the-fittest-new-y...      | ✗      |           |  |          |  |
| AURIGA (FAMILY)                        | The AURIGA malware family shares a large amount of functionality with the BA...     | ✗      |           |  |          |  |
| Aurora Panda French Aerospace Attack   | Freeeye reported a strategic web compromise (SWC) activity on the website fo...     | ✗      |           |  |          |  |
| Autocad_Worm - ACAD/Medre.A            | Based on the blog written by ESET                                                   | ✗      |           |  |          |  |
| Backdoor-c99shell                      | IOC to detect generic version of c99shell. Can be used by attackers for remot...    | ✗      |           |  |          |  |
| Backdoor-r57shell                      | IOC to detect r57shell. can be used as a backdoor or remote administration to...    | ✗      |           |  |          |  |
| Backoff POS Malware                    | Backoff is a family of PoS malware and has been discovered recently. The mal...     | ✗      |           |  |          |  |
| Backoff POS malware Symantec Reporting | The New York Times has reported that the Department of Homeland Security h...       | ✗      |           |  |          |  |
| bad_gvchost                            |                                                                                     | ✗      |           |  |          |  |
| Bandload - SAT                         | This is a stub of an IOC intended to be used as a base to make a more robust I...   | ✗      |           |  |          |  |

### 13.1 LISTADO

La pestaña muestra una **lista** a modo de resumen con **todas las reglas** de MARTA. Al igual que las listas de ficheros y de análisis, esta lista está paginada.

En la lista se muestran los atributos más significativos de cada regla: el nombre, la descripción, si está activa (**una regla no activa no se tendrá en cuenta para las comprobaciones de reglas coincidentes de un análisis**) y sus etiquetas asociadas. Al igual que en las listas de ficheros y de análisis, es posible **filtrar** por cualquiera de estos campos.

| Reglas IOC                                        |                                                                                      |        |           |  |          |  |
|---------------------------------------------------|--------------------------------------------------------------------------------------|--------|-----------|--|----------|--|
| Nombre                                            | Descripción                                                                          | Activa | Etiquetas |  | Acciones |  |
| Deshabilita Registro                              | Deshabilita las herramientas de edición de registro de windows dificultando la ca... | ✓      |           |  |          |  |
| Deshabilita TaskManager                           | Deshabilita el gestor de tareas de Windows.                                          | ✓      |           |  |          |  |
| Interactua con aplicaciones en la carpeta Wind... | Interactua con aplicaciones en la carpeta Windows                                    | ✓      |           |  |          |  |
| Modificación o Lectura de Servicios de Windows    | Detección de modificación o Lectura de Servicios de Windows                          | ✓      |           |  |          |  |

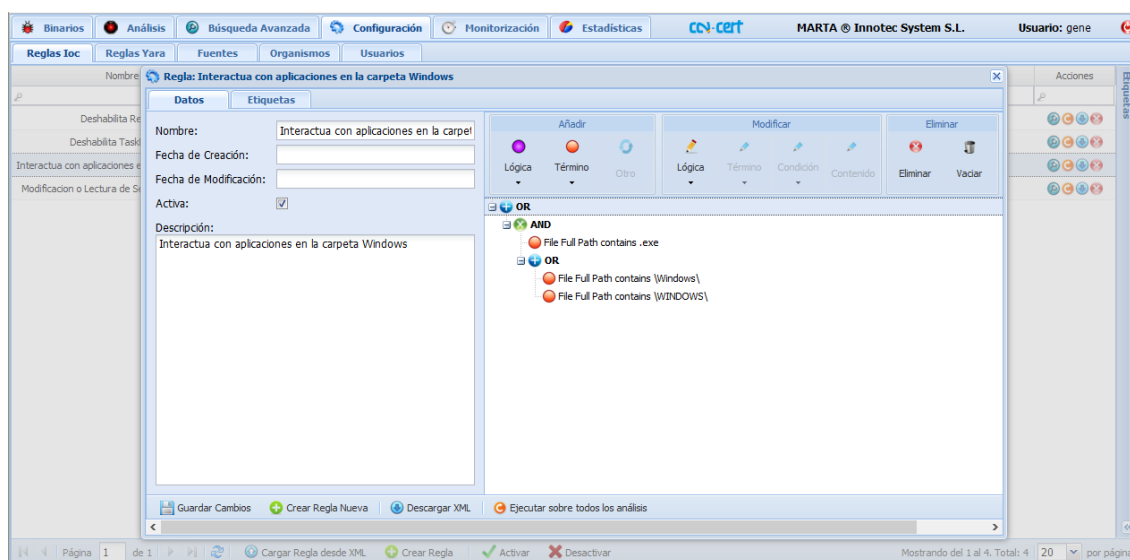
## 13.2 ACCIONES SOBRE LAS REGLAS

La última columna de la lista de reglas es de **acciones**:

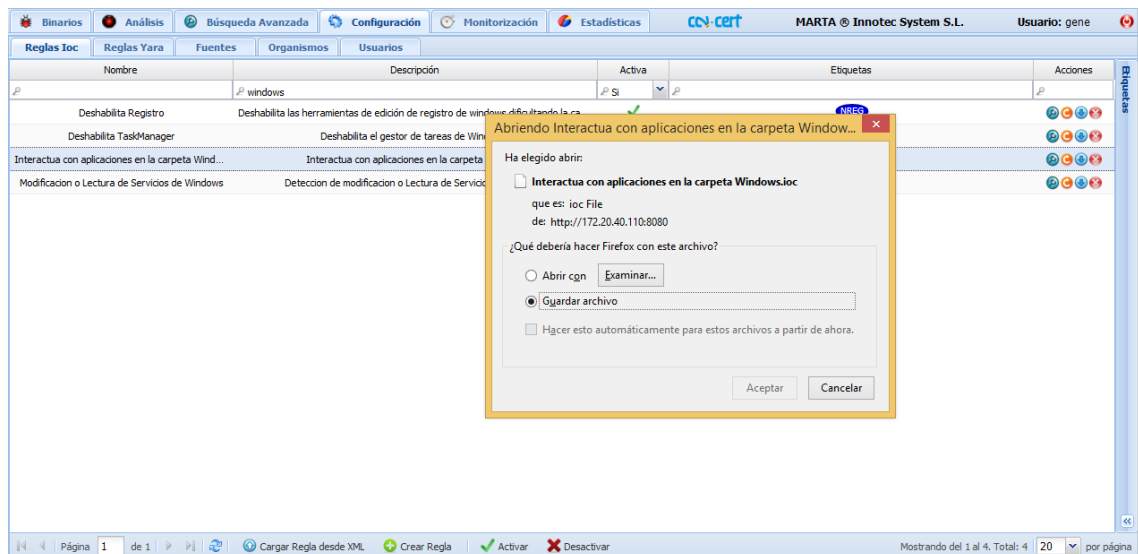
| Reglas Ioc | Reglas Yara | Fuentes | Organismos | Usuarios | Nombre                                            | Descripción                                                                          | Activa | Etiquetas | Acciones |
|------------|-------------|---------|------------|----------|---------------------------------------------------|--------------------------------------------------------------------------------------|--------|-----------|----------|
|            |             |         |            |          | Deshabilita Registro                              | Deshabilita las herramientas de edición de registro de windows dificultando la ca... | ✓      | NREG      |          |
|            |             |         |            |          | Deshabilita TaskManager                           | Deshabilita el gestor de tareas de Windows.                                          | ✓      | TMGR      |          |
|            |             |         |            |          | Interactua con aplicaciones en la carpeta Wind... | Interactua con aplicaciones en la carpeta Windows                                    | ✓      | LAW       |          |
|            |             |         |            |          | Modificacion o Lectura de Servicios de Windows    | Deteccion de modificacion o Lectura de Servicios de Windows                          | ✓      | SRVC      |          |

Permite realizar las siguientes acciones sobre una regla:

-  **Ver Detalle:** Abre la vista de detalles de la regla seleccionada. Esta vista contiene toda la información relativa a la regla. Se describe en la sección [Vista de Detalle de una Regla](#) de este documento.

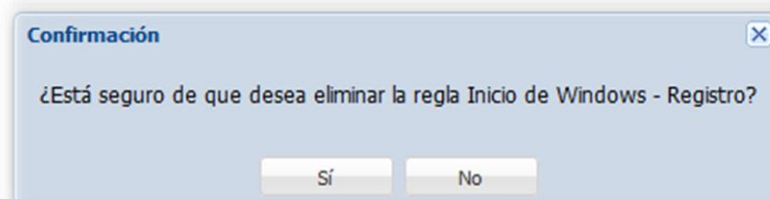


-  **Descargar Regla como XML:** Permite exportar la regla a un fichero con formato XML y descargarlo.

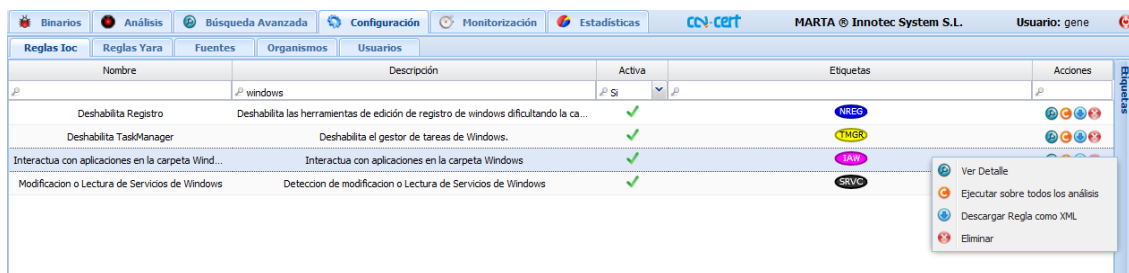


```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="" last-modified="2015-09-04T00:00:00"
xmlns="http://schemas.mandiant.com/2010/ioc">
<short_description>Creación de Ejecutables en carpeta Windows</short_description>
<description>Creación de Ejecutables en carpeta Windows</description>
<authored_by>null</authored_by>
<authored_date>2015-09-04T00:00:00</authored_date>
<links />
<definition>
<Indicator operator="OR" id="">
<IndicatorItem id="" condition="contains">
<Context document="File Full Path" search="FileItem/FullPath" type="mir" />
<Content type="string">.exe</Content>
</IndicatorItem>
<Indicator operator="OR" id="">
<IndicatorItem id="" condition="contains">
<Context document="File Full Path" search="FileItem/FullPath" type="mir" />
<Content type="string">\Windows</Content>
</IndicatorItem>
<IndicatorItem id="" condition="contains">
<Context document="File Full Path" search="FileItem/FullPath" type="mir" />
<Content type="string">\WINDOWS</Content>
</IndicatorItem>
</Indicator>
</Indicator>
</Indicator>
</definition>
</ioc>
```

-  **Eliminar:** Elimina la regla seleccionada. Pide confirmación antes de eliminar.

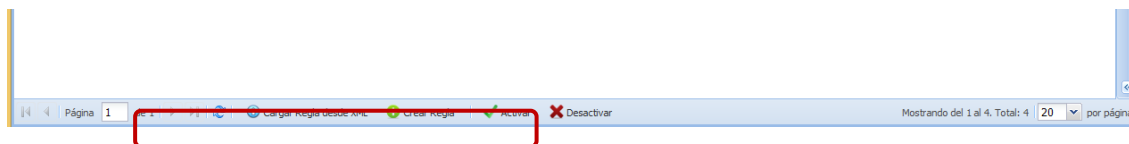


Al igual que en las listas de ficheros y de análisis, todas estas acciones también pueden realizarse utilizando el botón derecho del ratón sobre una regla de la lista.

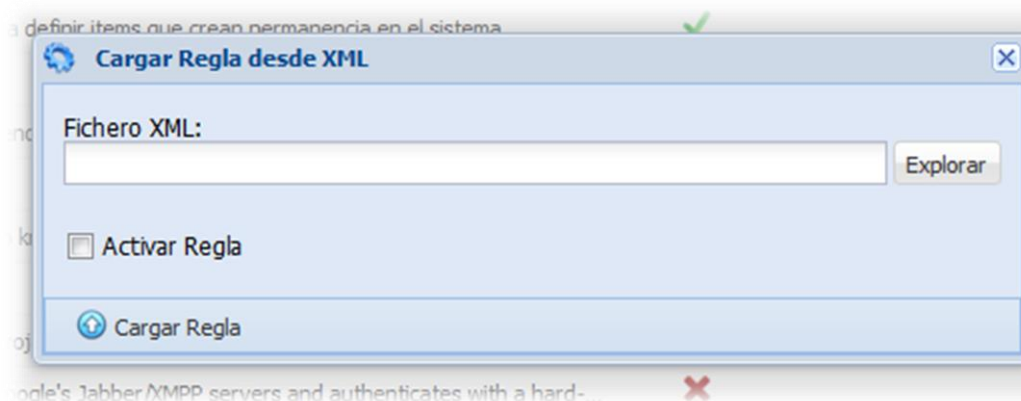


### 13.3 ACCIONES GENERALES

Al igual que en las pestañas de binarios y de análisis, en la barra de herramientas de la parte inferior de la pestaña de reglas hay botones que permiten realizar **gestiones** que no están directamente ligadas a una regla:

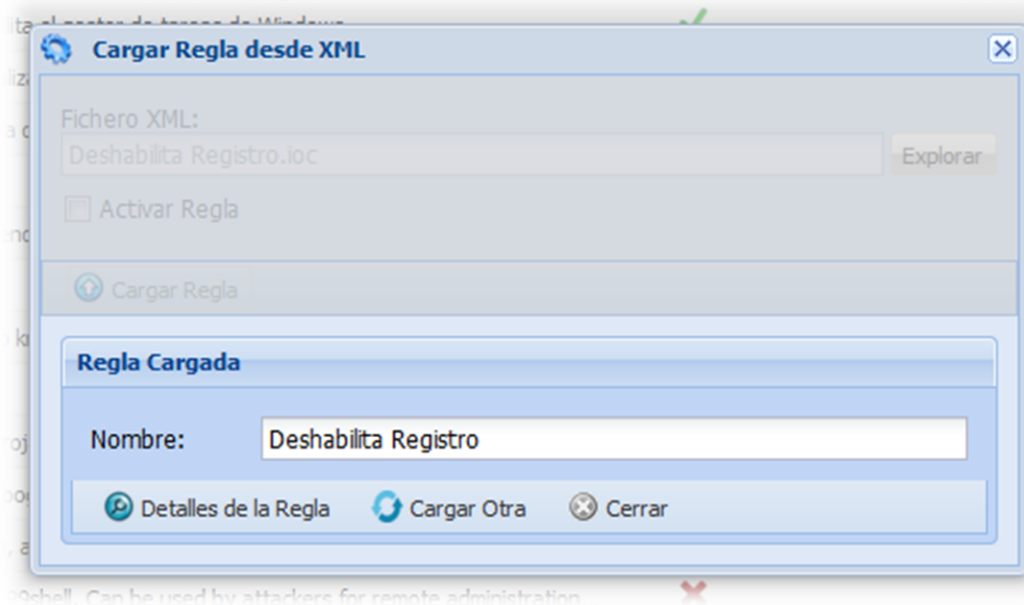


-  **Cargar Regla desde XML:** Abre una vista que permite cargar una regla desde un fichero XML con formato IOC (equivalente al formato en el que se descargan las reglas de MARTA).

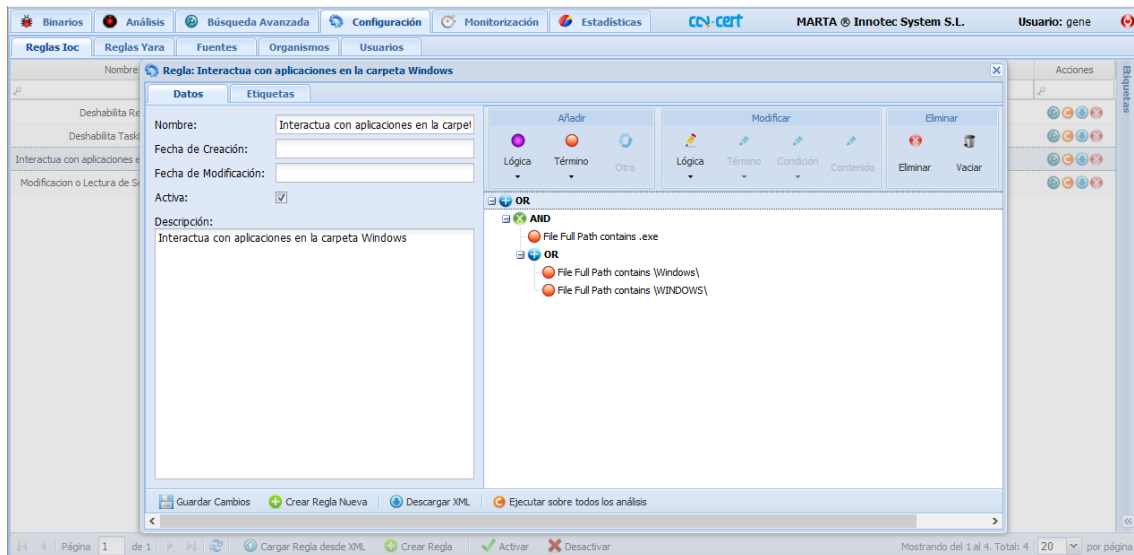


Se debe seleccionar el fichero con el campo **Fichero XML**, elegir si se desea activar la regla con la casilla de selección **Activar Regla**, y clicar en el botón  **Cargar Regla**. Esto hará que se suba el fichero XML a MARTA y se cree la regla a partir de su contenido.

Una vez hecho todo esto, la ventana muestra el nombre de la regla cargada, y permite las siguientes acciones:

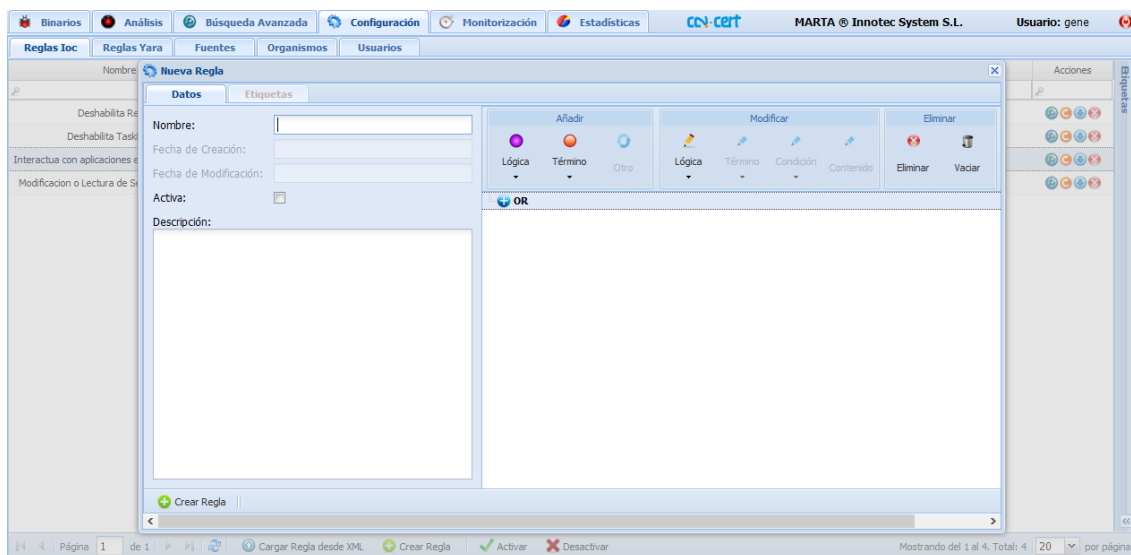


- **Detalles de la Regla:** Abre la vista de detalles de la regla cargada. Esta vista contiene toda la información relativa a la regla. Se describe en la sección [Vista de Detalle de una Regla](#) de este documento.

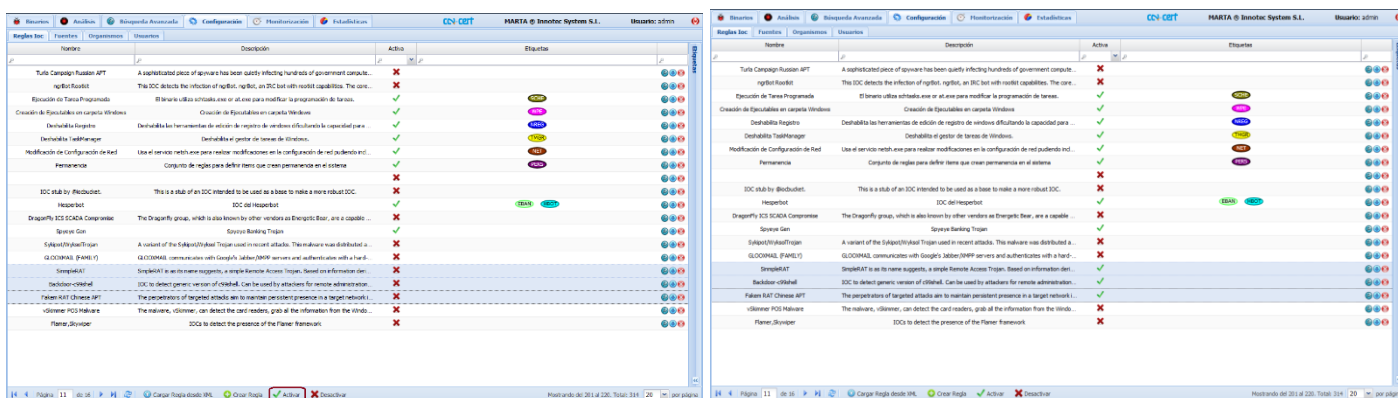


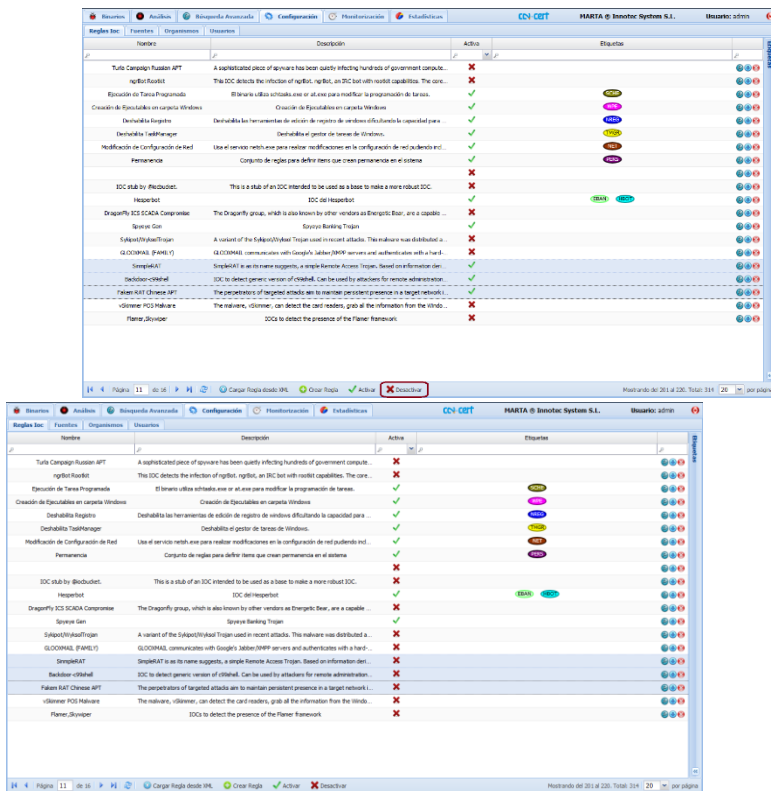
- **Cargar Otra:** Permite cargar otra regla.

-  **Cerrar:** Cierra la ventana de carga de reglas.
-  **Crear Regla:** Abre la vista de detalles de una regla, vacía, para crear una regla nueva desde cero. Esta vista se describe en la sección [Vista de Detalle de una Regla](#) de este documento.



-  **Activar** /  **Desactivar:** Activa / Desactiva todas las reglas seleccionadas de la lista de reglas.



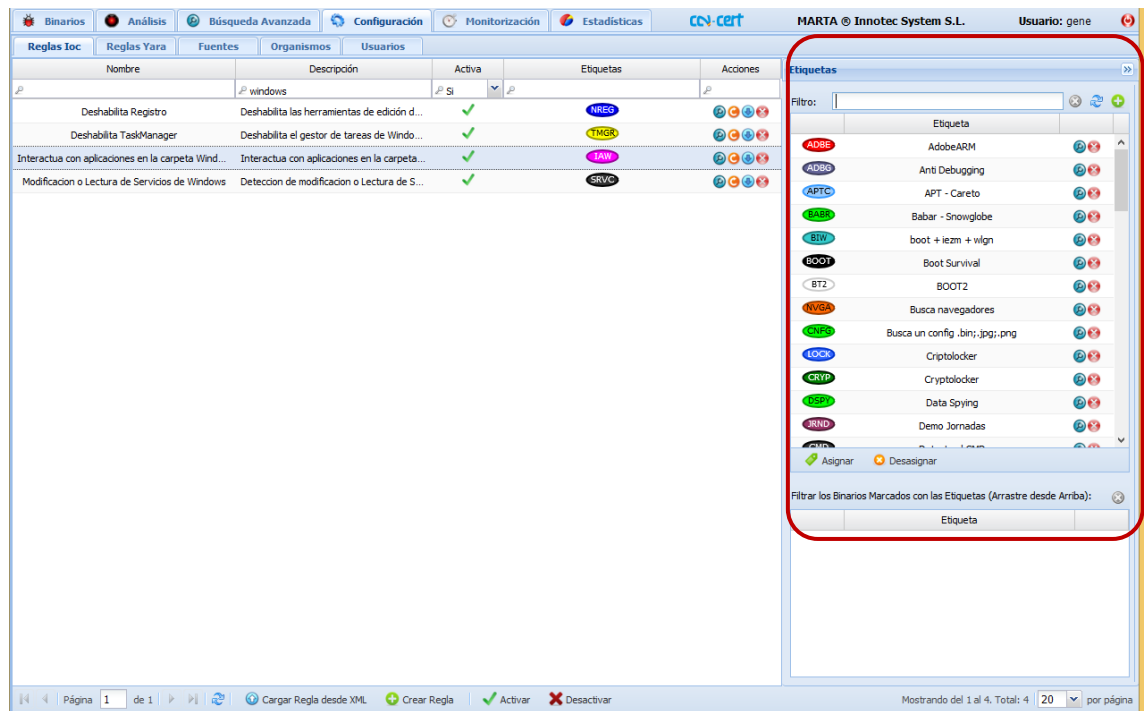


The screenshot shows the MARTA @ Insoctec System S.L. interface. The 'Reglas de' tab is active, displaying a list of rules. The 'Etiquetas' column is highlighted, showing a dropdown menu with various tags. The 'Activo' column shows a status of 'Activo' (Active) for the selected rule.

| Nombre                                     | Descripción                                                                                      | Activo | Etiquetas |
|--------------------------------------------|--------------------------------------------------------------------------------------------------|--------|-----------|
| Trojan Campaign Russian APT                | A sophisticated piece of spyware has been quietly infecting hundreds of government computers...  | ✗      |           |
| NgBot Ransomware                           | The IOC detects the infection of ngbot, a botnet with various capabilities. The core...          | ✗      |           |
| Exención de Tareas Programada              | El sistema utiliza esta regla para modificar la programación de tareas.                          | ✓      |           |
| Creación de Ejecutables en carpeta Windows | Creación de Ejecutables en carpeta Windows                                                       | ✓      |           |
| Deshabilita Registro                       | Deshabilita las herramientas de edición de registro de Windows dificultando la capacidad para... | ✓      |           |
| Deshabilita TaskManager                    | Deshabilita el gestor de tareas de Windows.                                                      | ✓      |           |
| Modificación de Configuración de Red       | Usa el servicio netsh para realizar modificaciones en la configuración de red pudiendo incl...   | ✓      |           |
| Permanencia                                | Conjunto de reglas para definir items que crean permanencia en el sistema                        | ✓      |           |
| IOC stub by @bluec0d3r                     | This is a stub of an IOC intended to be used as a base to make a more robust IOC.                | ✗      |           |
| Heapsort                                   | IOC del Heapsort                                                                                 | ✓      |           |
| Dragonfly ICS SCADA Compromise             | The Dragonfly group, which is also known by other vendors as Energetic Bear, are a capab...      | ✗      |           |
| Spurva Coin                                | Spurva Banking Trojan                                                                            | ✓      |           |
| FakeWinMailbox Trojan                      | A variant of the FakeWinMailbox Trojan used in recent attacks. This malware was distributed a... | ✗      |           |
| GLOOMY (FAME-1)                            | GLOOMY communicates with Google's Talker/SMTP servers and authenticates with a hard...           | ✗      |           |
| SimpleMail                                 | SimpleMail is a malware suggestion, a simple Remote Access Trojan. Based on information der...   | ✗      |           |
| Backdoor-citibank                          | IOC to detect generic version of citibank. Can be used by attackers for remote administration... | ✗      |           |
| FakeWinMailbox APT                         | The perpetrators of targeted attacks aim to maintain persistent presence in a target network...  | ✗      |           |
| vitamer FQDN Malware                       | The malware, vitamer, can detect the card readers, grab all the information from the cards...    | ✗      |           |
| Flamer/Slurper                             | IOC to detect the presence of the Flamer framework                                               | ✗      |           |

## 13.4 ETIQUETAS

En la parte derecha de la pestaña, hay un panel desplegable que permite hacer **gestiones con las etiquetas** asociadas a los análisis, de forma totalmente similar a los de las pestañas de binarios y análisis.

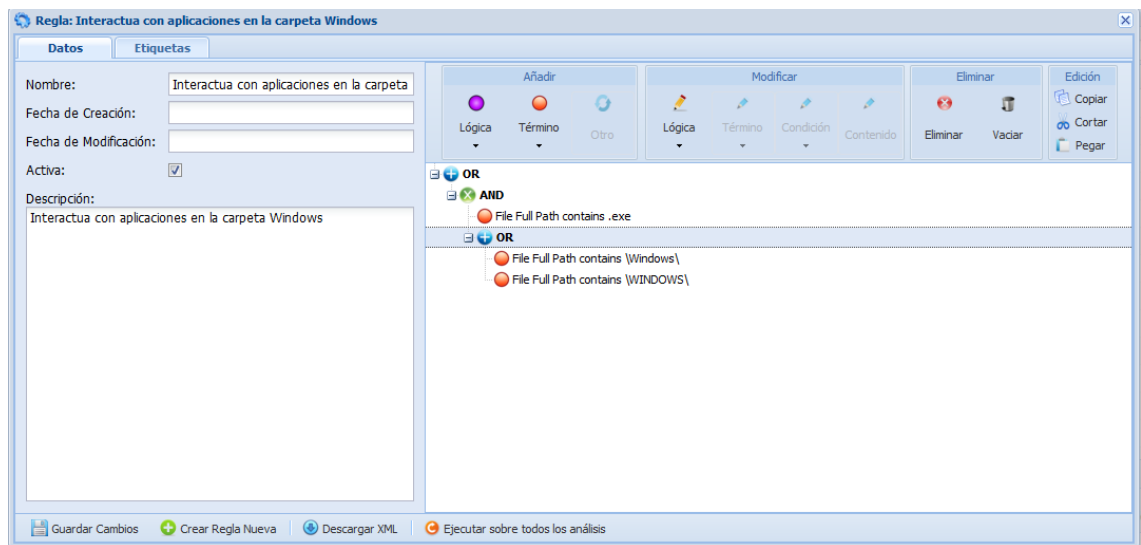


Permite crear, modificar y eliminar etiquetas, asignarlas y desasignarlas a múltiples reglas y filtrar las reglas por etiquetas. Véase la sección [Etiquetas de la Pestaña de Pestaña de Binarios](#).

A modo de recordatorio, un análisis tiene asociadas todas las etiquetas asociadas a las reglas que cumple. Y un fichero tiene asignadas todas las etiquetas que tengan asignadas todos sus análisis.

## 14 VISTA DE DETALLE DE UNA REGLA

Esta vista contiene toda la información relativa a una regla, y permite gestionarla.

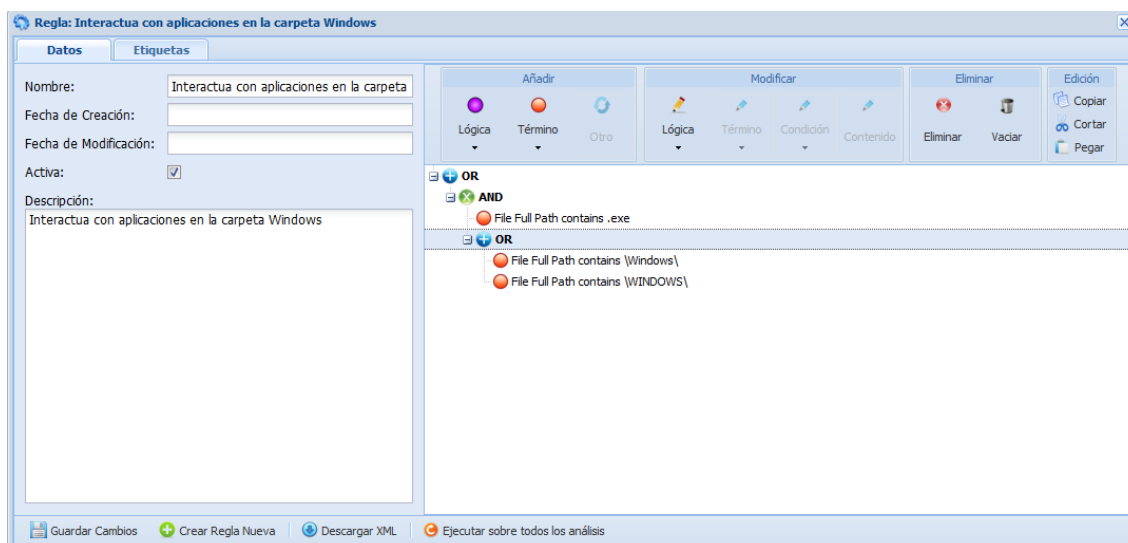


Dispone de dos pestañas:

- **Datos:** Muestra y permite gestionar la definición de la regla.
- **Etiquetas:** Muestra y permite gestionar las etiquetas asociadas a la regla.

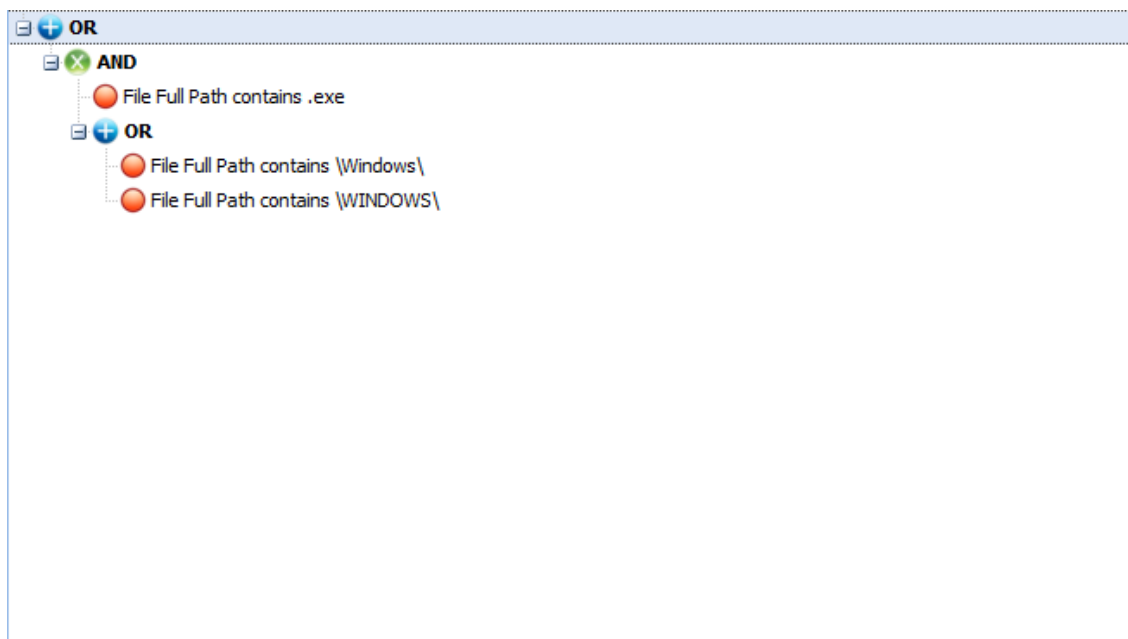
## 14.1 DATOS

Muestra y permite gestionar la *definición de la regla*.



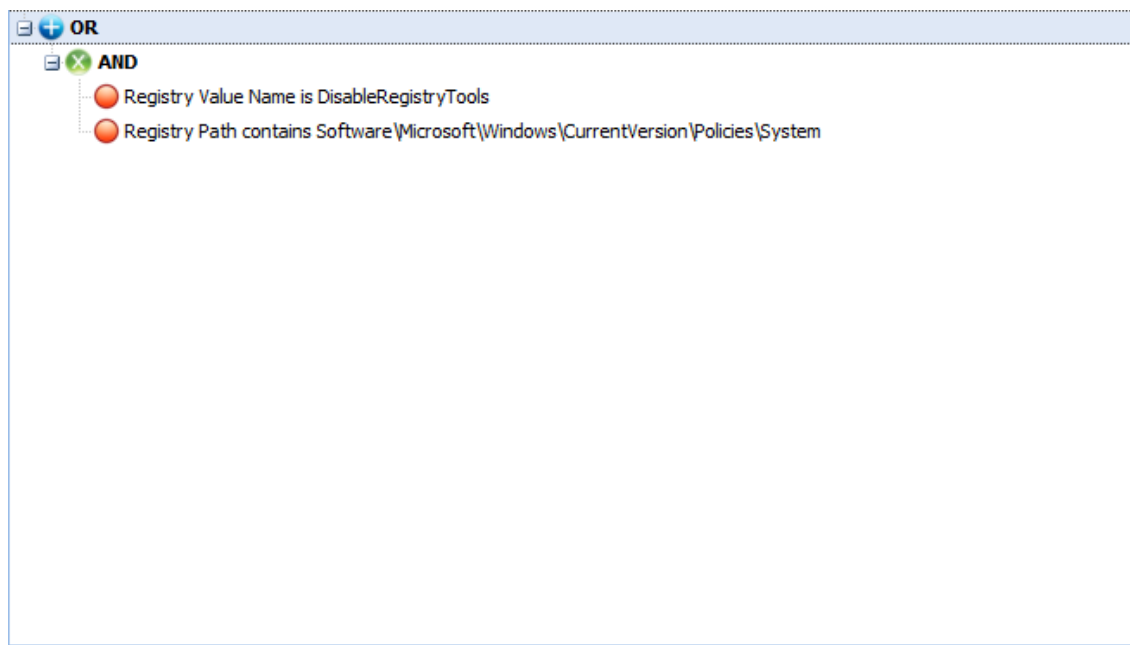
La parte de la izquierda contiene los datos básicos de la regla: el nombre, la fecha de creación y de última modificación, si está activa (**una regla no activa no se tendrá en cuenta para las comprobaciones de reglas coincidentes de un análisis**), y la descripción. Todos estos campos son editables, excepto las fechas, que se calculan de forma automática. Si una regla no tiene fecha de creación es debido a que fue importada desde un XML que no contenía esta información.

La parte de la derecha contiene el árbol lógico de la regla. Las reglas de MARTA tienen estructura de IOC. Es decir, están basadas en comprobaciones de términos anidados con operaciones AND y OR.



Por ejemplo, esta regla, sería cumplida por análisis en los que se interaccione con un fichero cuya ruta completa (File Full Path) contenga ".exe", y además, o bien la ruta contenga "\Windows\", o "\WINDOWS\".

Esta otra, en cambio:

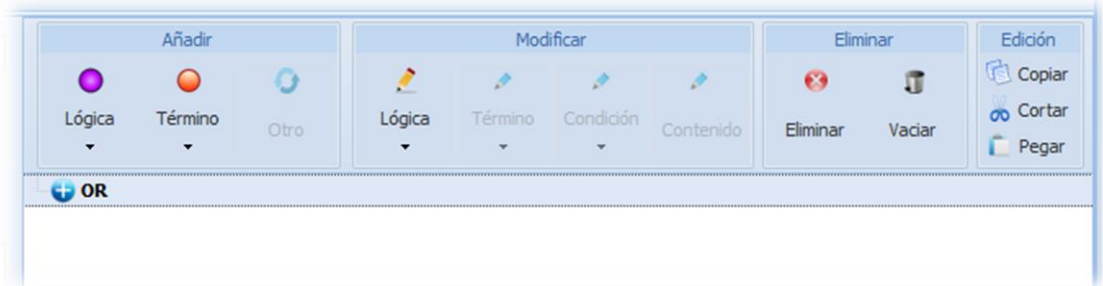


Sería cumplida por análisis en los que se interaccione con una clave de registro cuyo nombre (Registry Value Name) sea "DisableRegistryTools", y además, su ruta (Registry Path) contenga "Software\Microsoft\Windows\CurrentVersion\Policies\System".

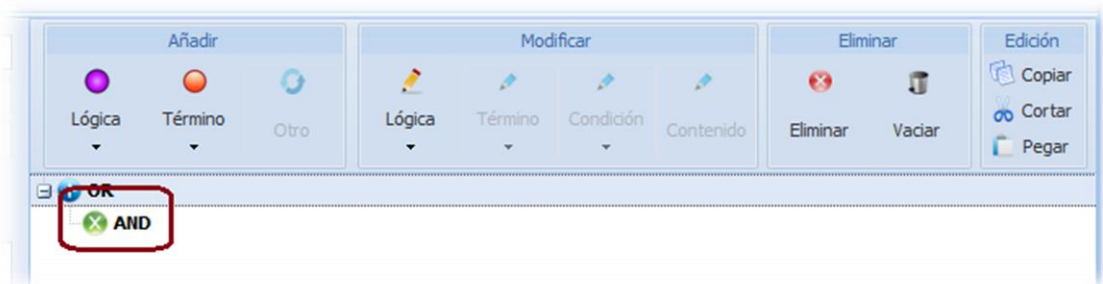
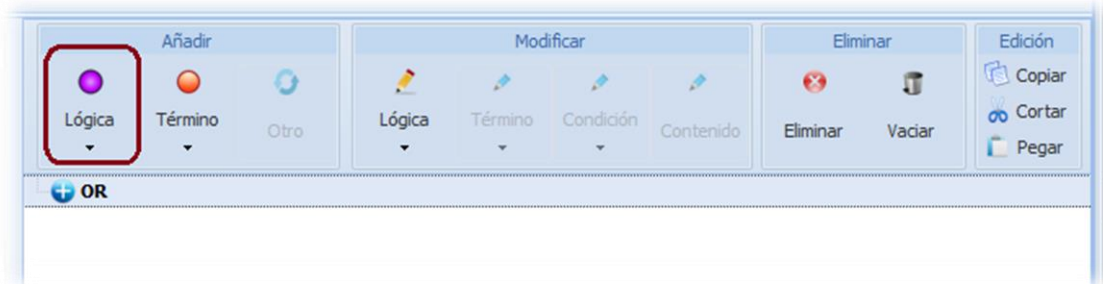
File Full Path, Registry Value Name y Registry Path son **términos**, que se pueden comparar con un **contenido** en concreto (como ".exe" o "Software\Microsoft\Windows\CurrentVersion\Policies\System") a través de cuatro posibles **condiciones**: contains (contiene), contains not (no contiene), is (es exactamente), is not (no es). Los términos se anidan en un árbol lógico utilizando los **operadores**: AND (y), OR (o).

Hay una gran cantidad de términos diferentes, Valor de Registro (Registry Value), Nombre de Proceso (Process Name), URI, Extensión de Fichero (File Extension), Servidor DNS (DNS Host), Nombre de Servicio (Service Name), Puerto Remoto (Remote Port), y un largo etcétera. Entre todos ellos, se puede definir cualquier comportamiento que MARTA pueda analizar. Y las reglas se pueden hacer tan complicadas como sea necesario, anidando términos con operadores lógicos. Es decir, es posible definir reglas que detecten comportamientos muy complejos o muy concretos.

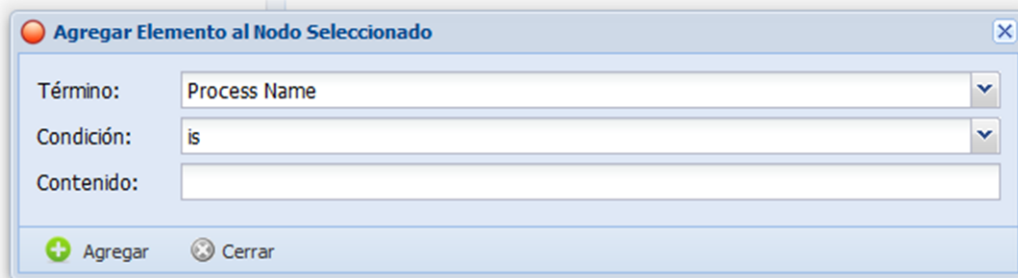
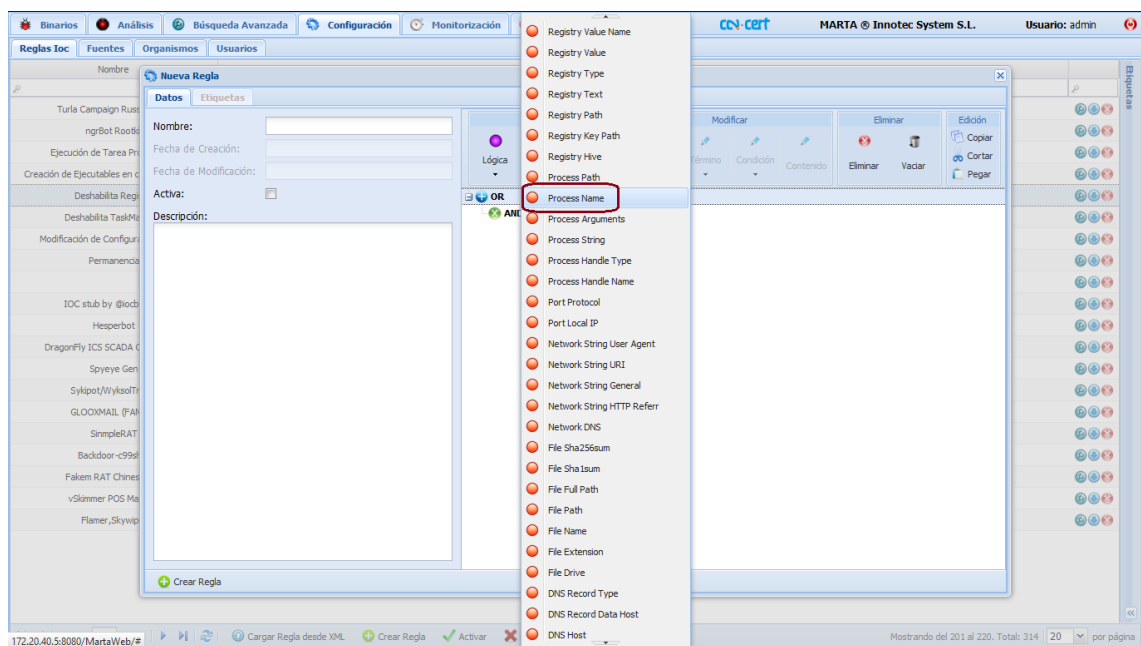
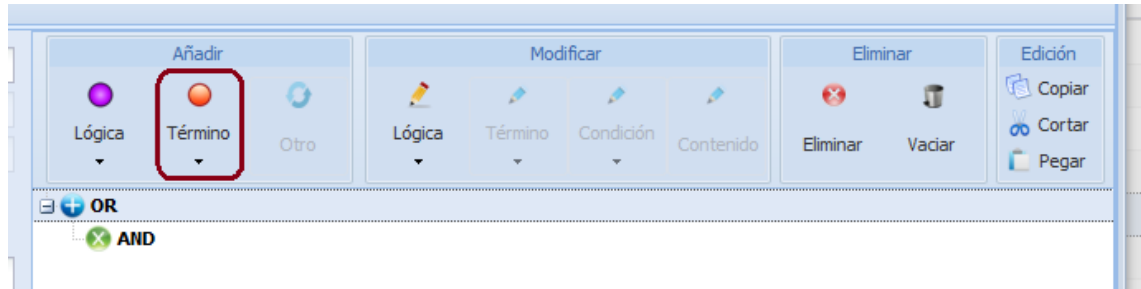
El árbol lógico cuenta con una barra de herramientas en la parte superior, que nos permite gestionar los términos y operadores. Todas las reglas comienzan con un nodo OR.



A un nodo de operador lógico (AND u OR) se le pueden añadir otros nodos lógicos, utilizando el botón de **Lógica**.



También se le pueden añadir nodos de término, utilizando el botón de  **Término**. Se desplegará una lista con todos los posibles términos, y, al clicar en uno de ellos, se abrirá una ventana que nos permitirá introducir la condición y el contenido.



**Agregar Elemento al Nodo Seleccionado**

Término:

Condición:

Contenido:

**Agregar Elemento al Nodo Seleccionado**

Término:

Condición:

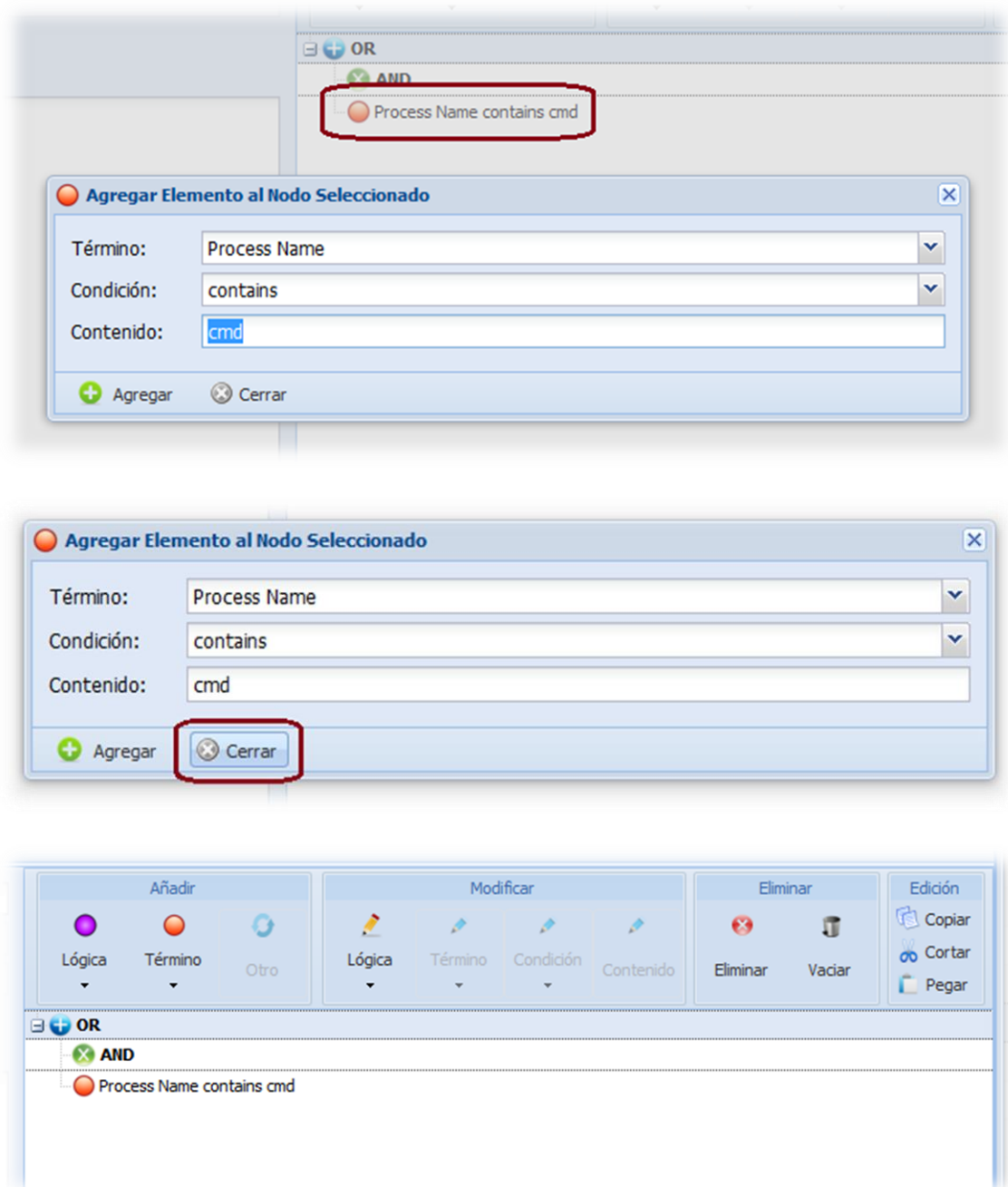
Contenido:

**Agregar Elemento al Nodo Seleccionado**

Término:

Condición:

Contenido:



Acabamos de añadir un término que detecta interacción con un proceso cuyo nombre contiene "cmd" al nodo OR principal de la regla.

La ventana de agregar términos no se cierra al agregar un término, sino al hacer clic en el botón de cerrar para poder agregar múltiples términos a un mismo nodo cómodamente.

Si seleccionamos en el término que acabamos de agregar y clicamos en el botón  **Otro**, se nos abrirá de nuevo la ventana de agregar términos para que

añadamos otro término al nodo padre del nodo que hemos seleccionado, en este caso, al nodo OR principal de la regla.



**Agregar Elemento al Nodo Padre del Seleccionado**

Término:

Condición:

Contenido:

**Agregar Elemento al Nodo Padre del Seleccionado**

Término:

Condición:

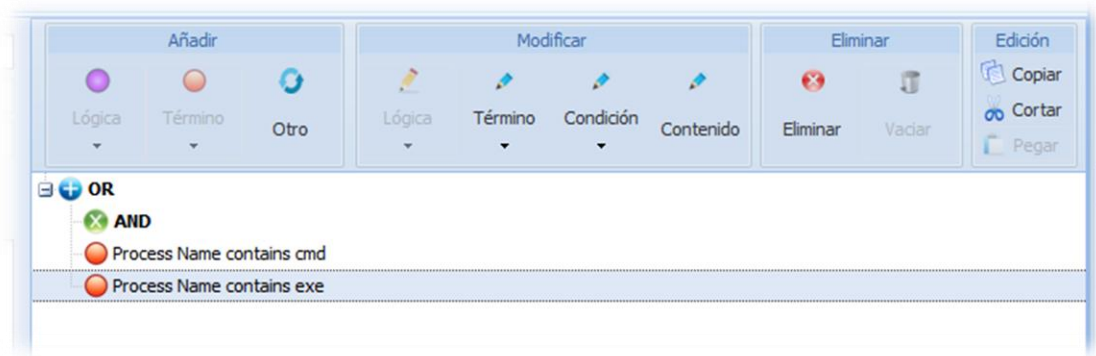
Contenido:

**Agregar Elemento al Nodo Padre del Seleccionado**

Término:

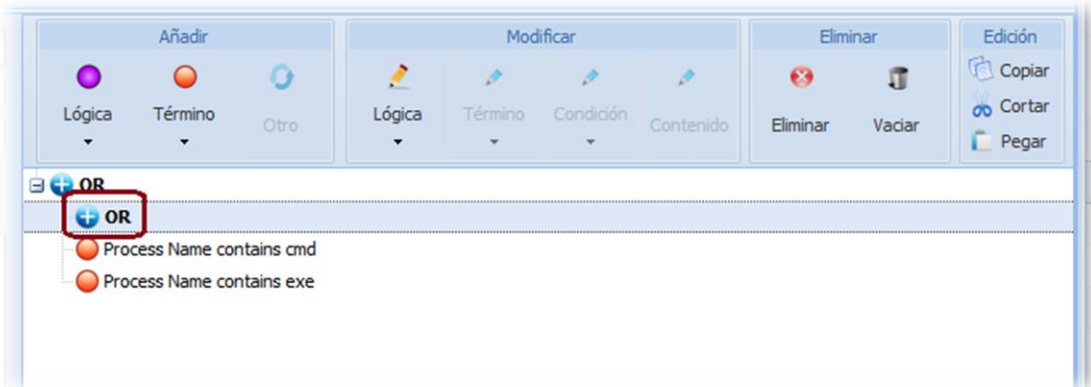
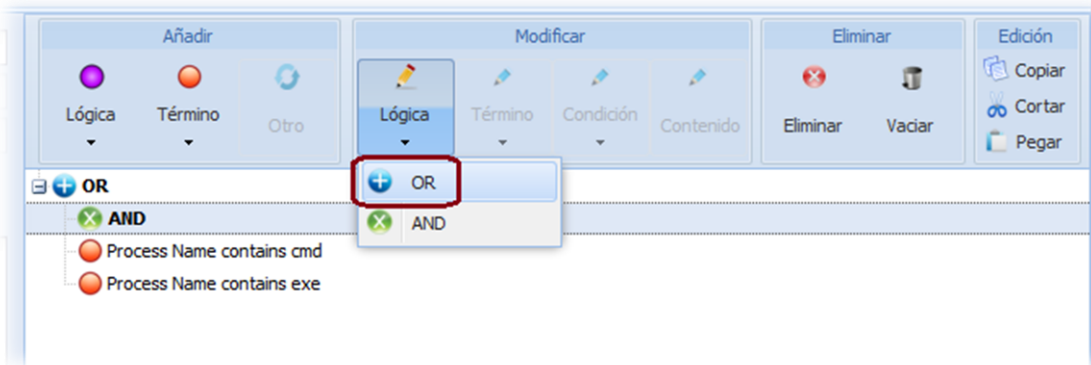
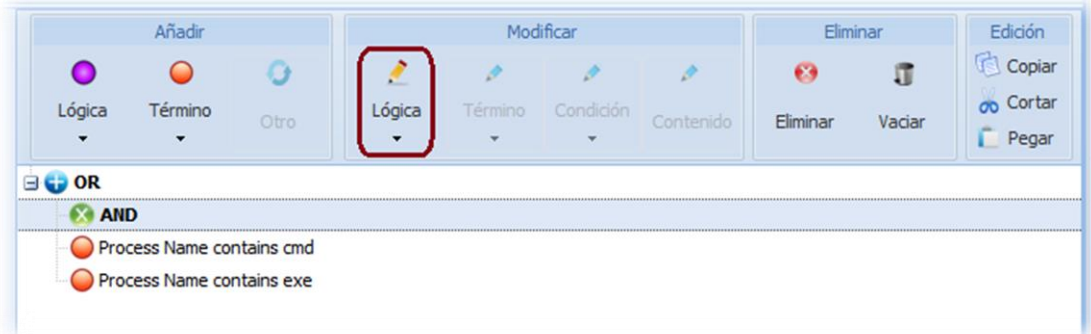
Condición:

Contenido:

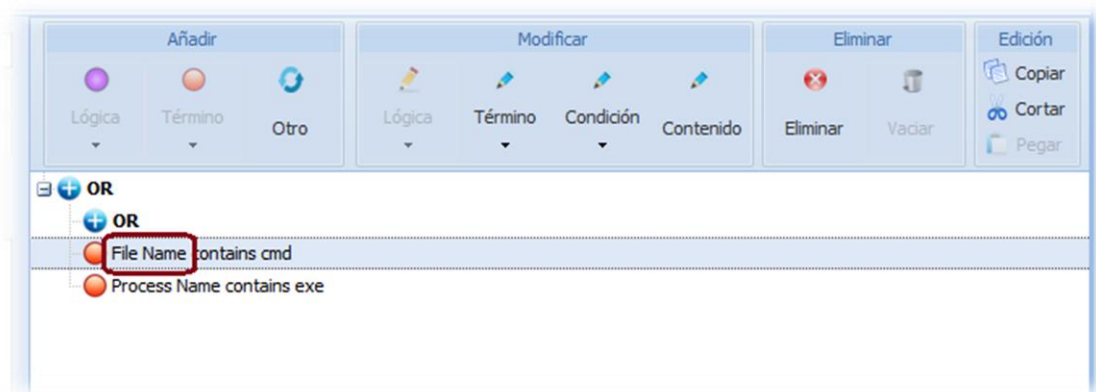
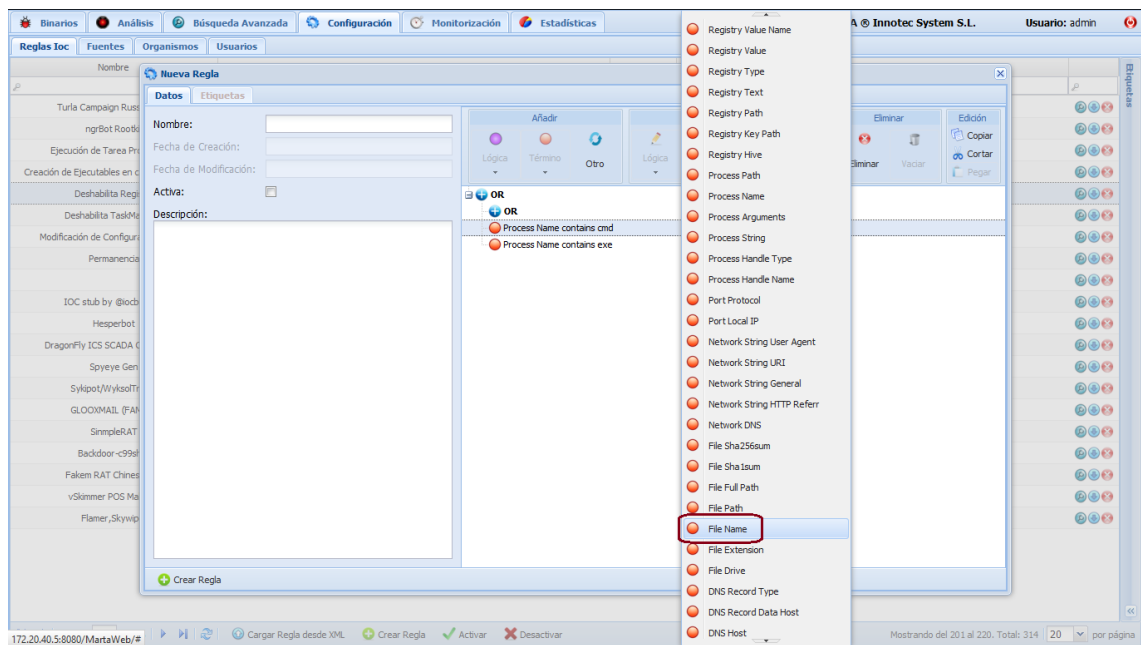
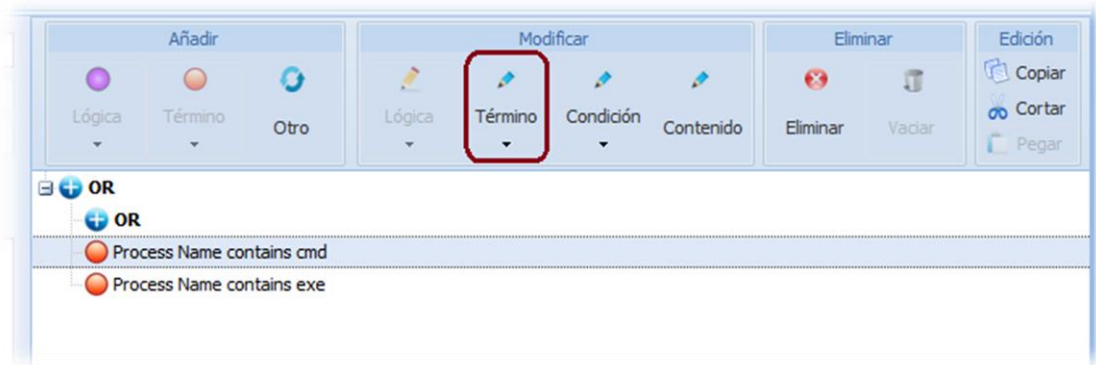


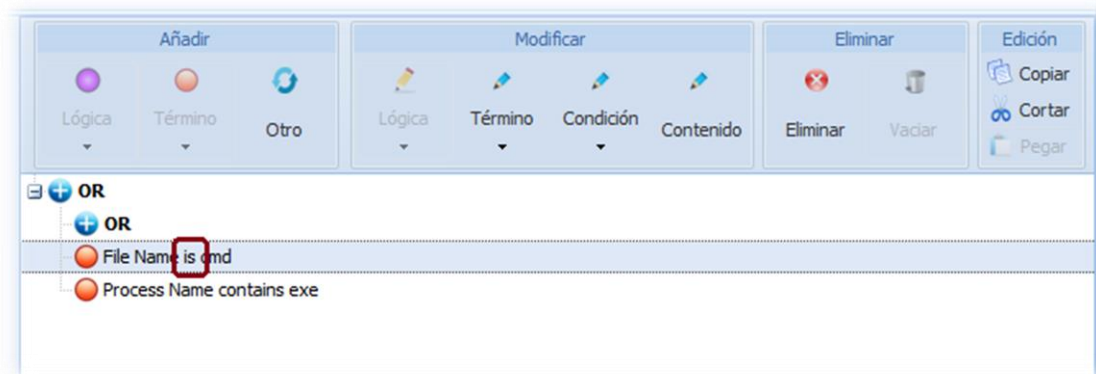
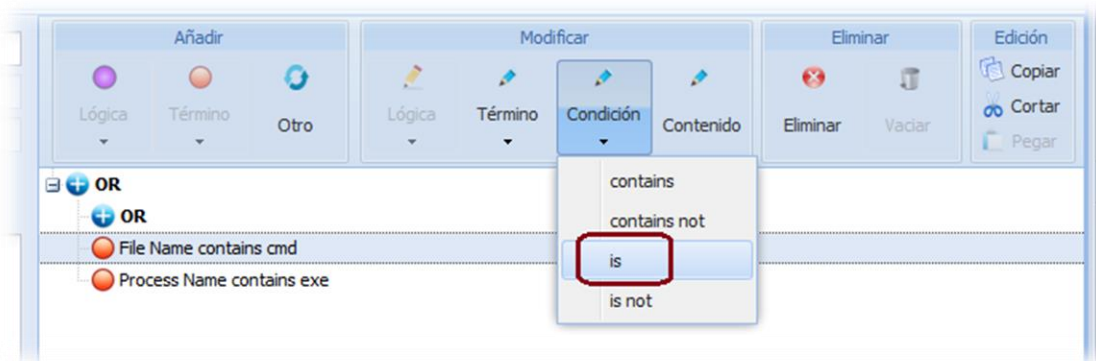
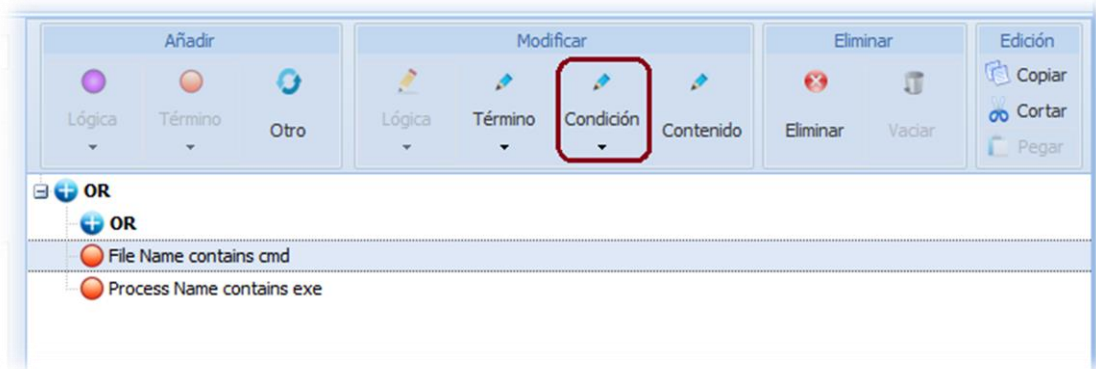
Acabamos de añadir otro término que detecta interacción con un proceso cuyo nombre contiene, en este caso, “exe” al nodo OR principal de la regla.

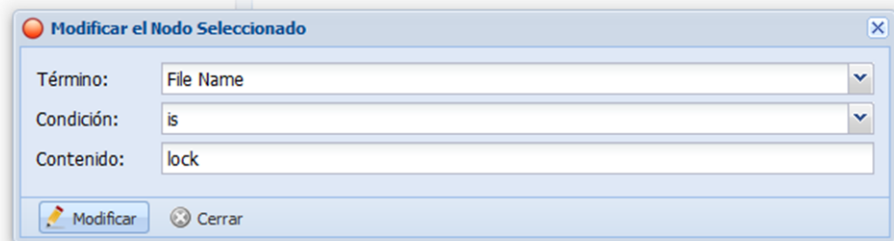
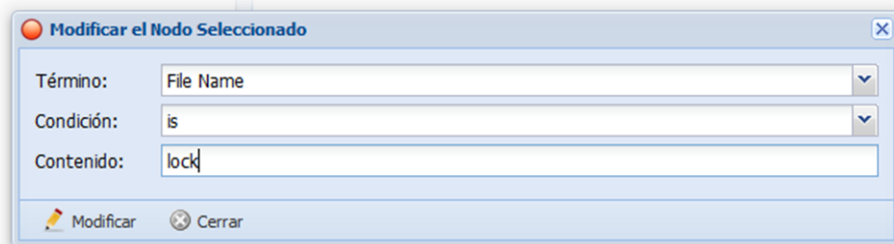
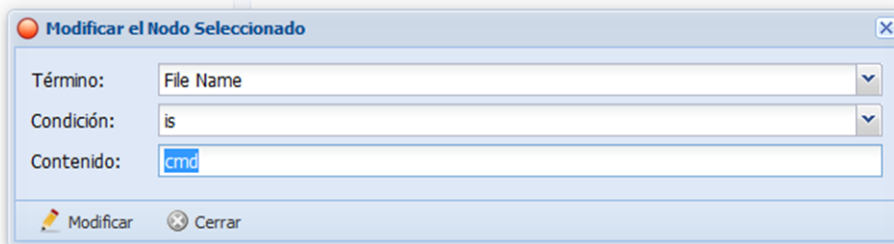
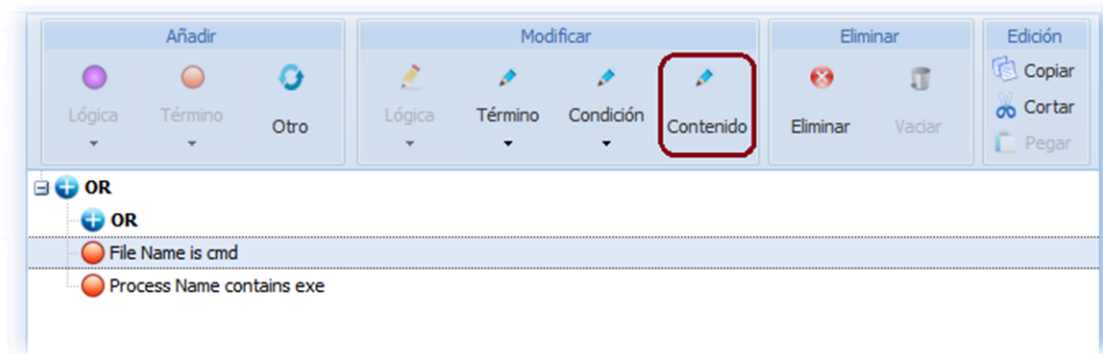
Si seleccionamos un nodo de lógica, podemos cambiarlo a AND u OR haciendo clic en el botón  **Lógica** (excepto el nodo principal, que siempre debe ser OR).

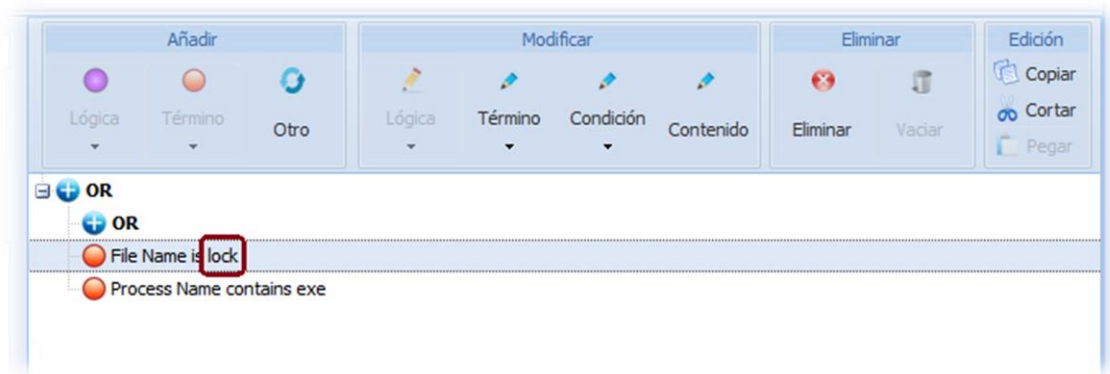


Si seleccionamos un nodo de término, podemos modificar su término, condición o contenido clicando en los botones de  **Término**,  **Condición** y  **Contenido**.

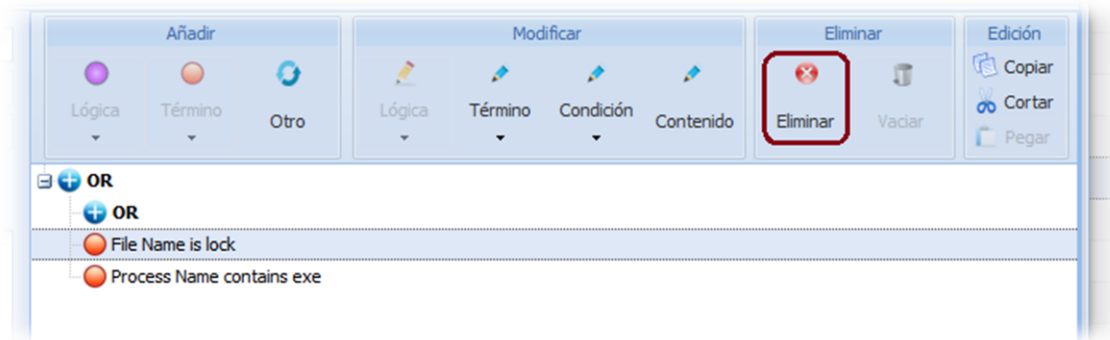




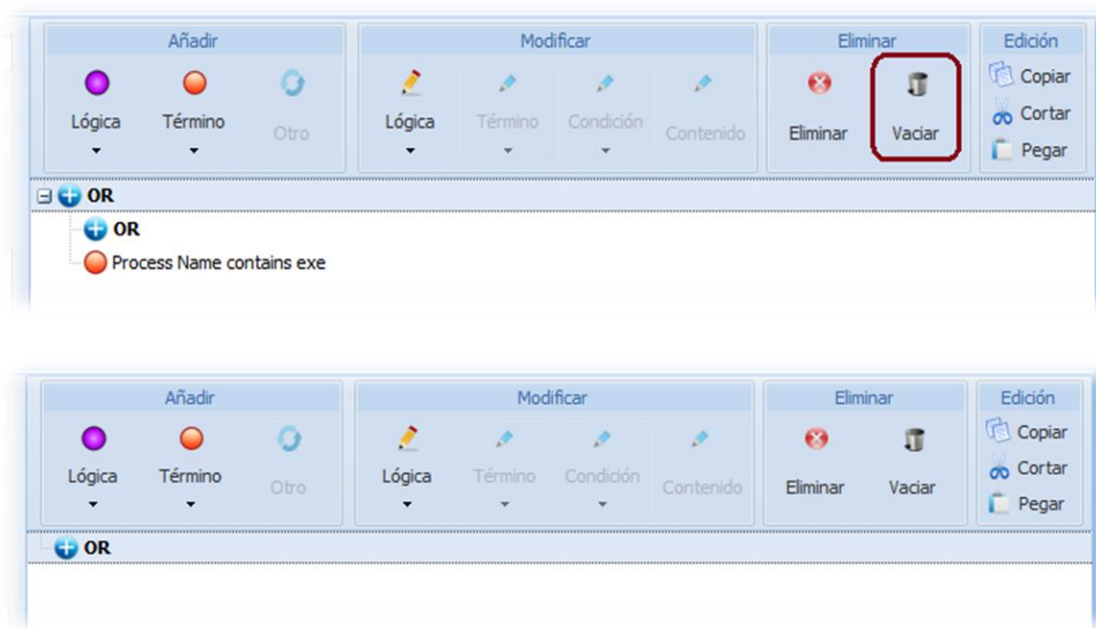




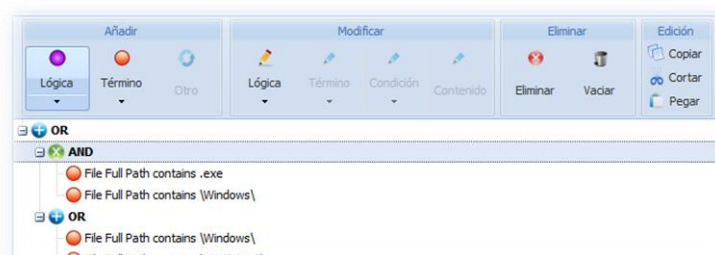
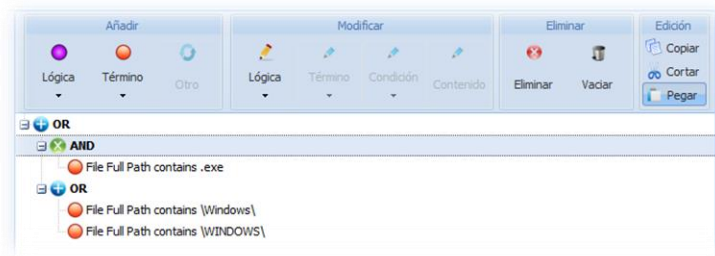
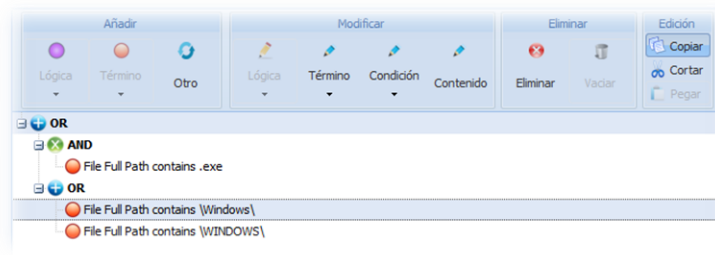
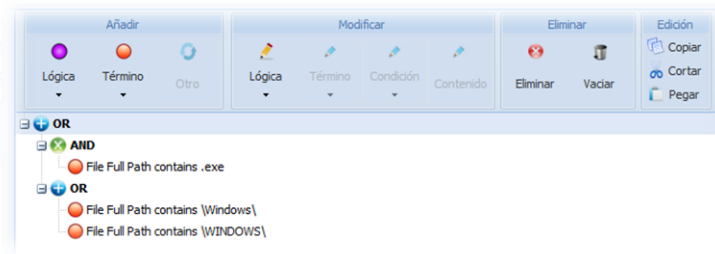
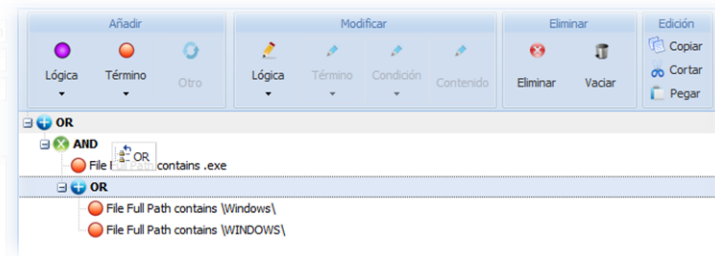
Si seleccionamos un nodo cualquiera, podemos eliminarlo haciendo clic en el botón  **Eliminar**.



Y si seleccionamos un nodo lógico, podemos eliminar todos sus hijos haciendo clic en el botón  **Vaciar**.

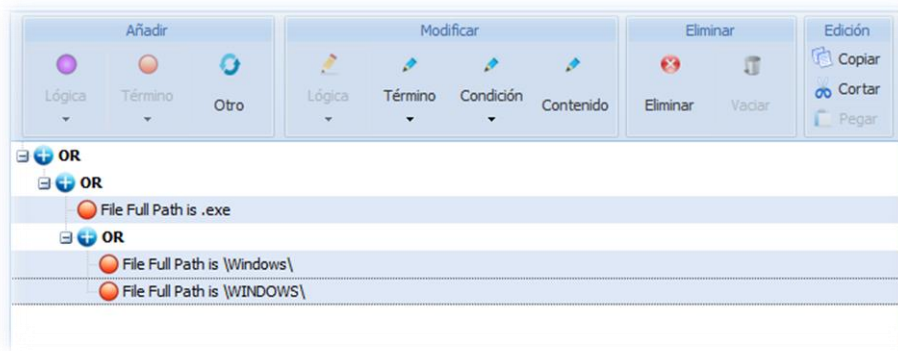
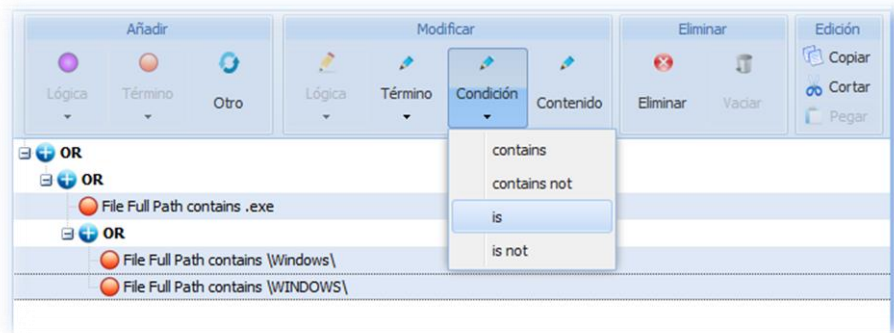
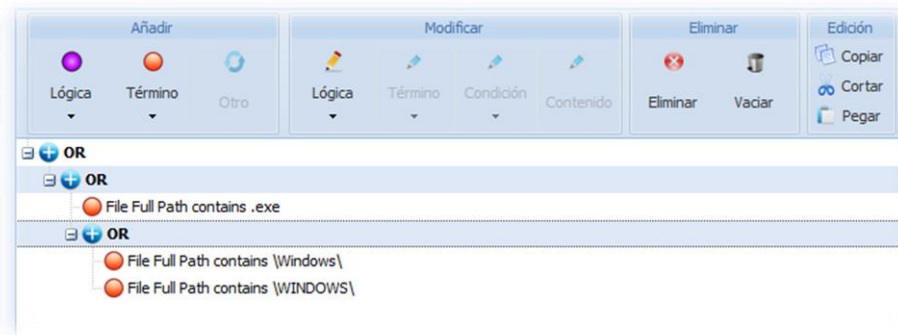
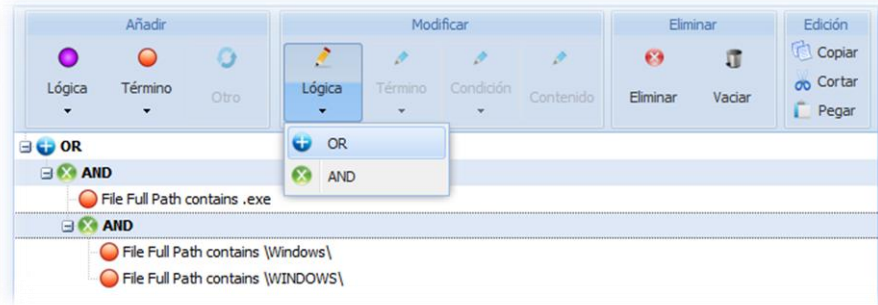


Un nodo puede ser movido (arrastrando), copiado, cortado y pegado (haciendo clic en los botones de  **Copiar**,  **Cortar** y  **Pegar**). Cualquiera de estas acciones sobre un nodo de término mueve el nodo en sí, y sobre un nodo de lógica mueve el nodo y todos sus hijos.



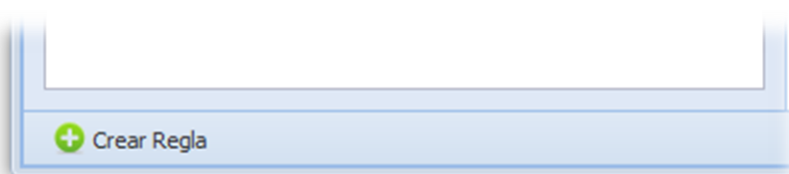
Los nodos copiados se quedan guardados incluso aunque se cierre la vista de de la regla. De esta forma, podemos copiar nodos de una regla a otra.

Cualquier acción que se pueda realizar sobre un nodo, también se puede realizar sobre todos los seleccionados, incluso copiar múltiples nodos y pegarlos sobre múltiples nodos.



La pestaña de datos cuenta con una barra de herramientas en la parte inferior, con **acciones**. Estas acciones dependen de si estamos creando una regla nueva, o editando una existente.

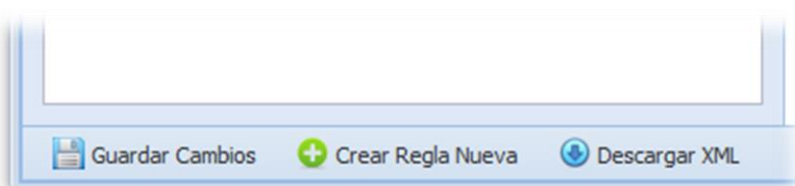
### *Creación de una Regla Nueva*



En este caso sólo hay una acción:

-  **Crear Regla:** Crea una regla con los datos introducidos.

### *Edición de una Regla Existente*



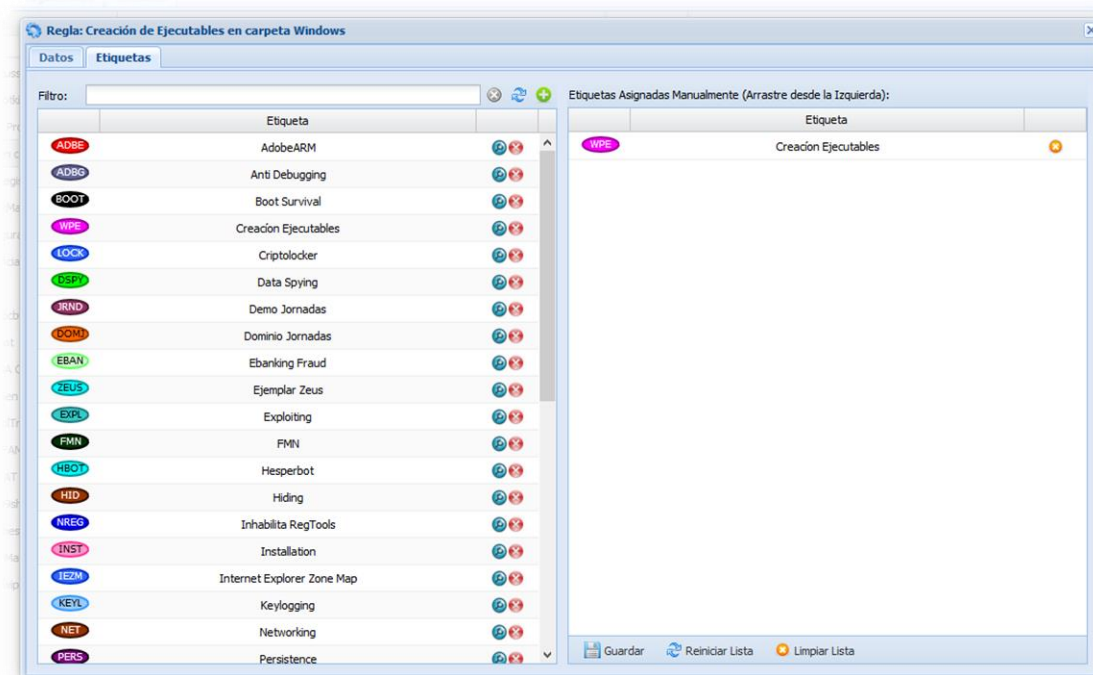
En este caso hay 3 acciones:

-  **Guardar Cambios:** Guarda los cambios efectuados en la regla.
-  **Crear Regla Nueva:** Crea una regla nueva a partir de la regla ya existente. Debe cambiarse el nombre.

-  **Descargar XML:** Exporta la regla a un fichero con formato XML y lo descarga. La exportación se hace tal y como esté la regla guardada. Si se han hecho modificaciones en ella, se deben guardar los cambios antes de descargar el XML.

## 14.2 ETIQUETAS

Muestra y permite gestionar las etiquetas asociadas a la regla. Esta pestaña sólo está activa si estamos editando una regla existente. No se pueden asignar etiquetas a una regla durante su creación, primero se debe crear la regla y a continuación asignarla etiquetas.



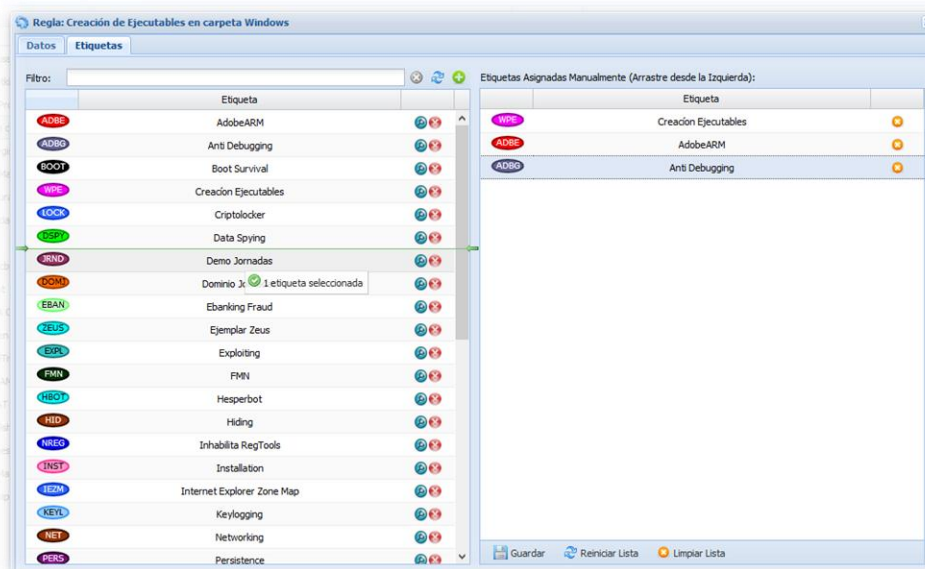
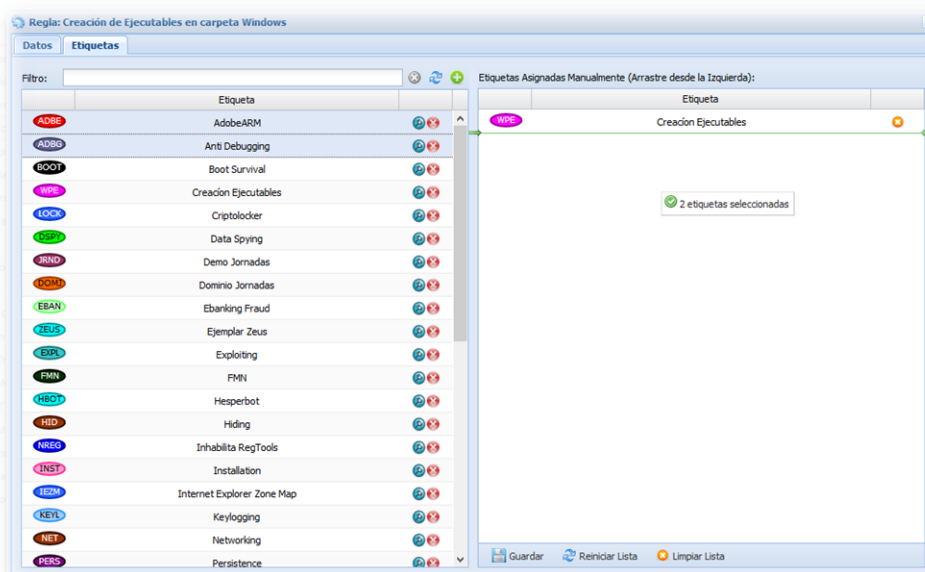
La asignación de **etiquetas** a **reglas** es **muy importante**, dado que las reglas definen los comportamientos que queremos detectar en los códigos dañinos analizados. Los análisis de códigos dañinos reciben todas las etiquetas asociadas a las reglas que cumplen. Y los propios ficheros de código dañino reciben todas las etiquetas asociadas a sus análisis. Por tanto, las **etiquetas** que asociemos a reglas que definan comportamientos que queremos detectar, estarán **asociadas** a los ficheros de código dañino que tengan esos **comportamientos**.

De esta forma, podremos reconocer rápidamente el **comportamiento** de un **fichero** echando un **vistazo a sus etiquetas**. O podremos **buscar códigos dañinos** con un comportamiento específico **filtrando ficheros por etiquetas**.

Esta pestaña consta de dos listas:

- La lista de la izquierda muestra todas las etiquetas existentes y permite gestionarlas, de forma similar a la descrita en la sección [Etiquetas](#).

- La lista de la derecha muestra las etiquetas asociadas a la regla, y permite arrastrar desde o hacia la lista de la izquierda para añadir o quitar etiquetas.



También podemos quitar etiquetas de la lista clicando en la acción  **Quitar** de una etiqueta.

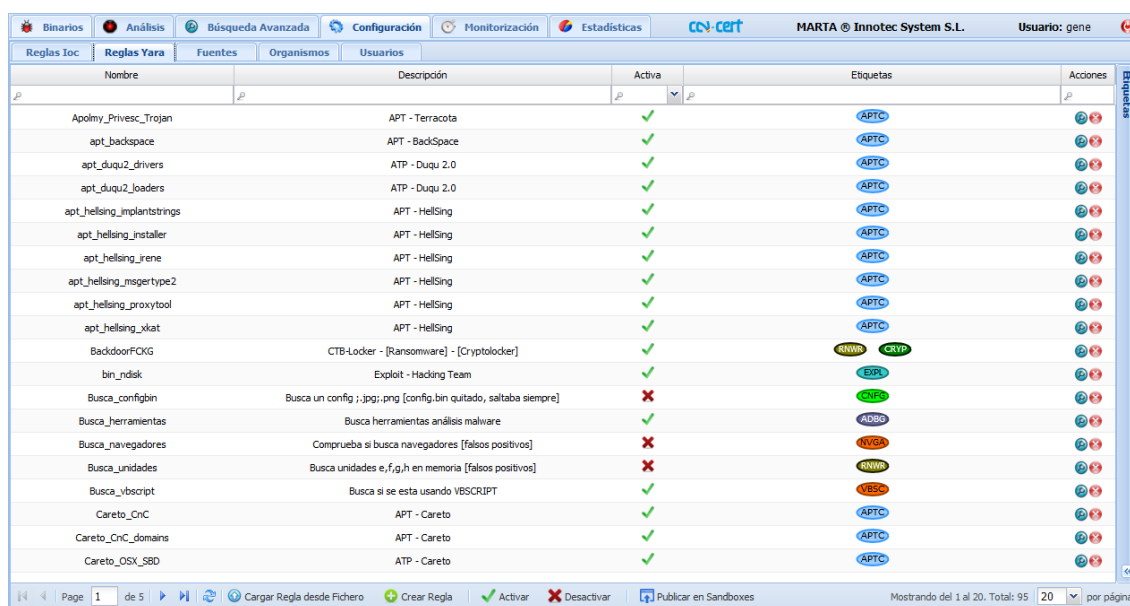
Debajo de la lista hay una barra de acciones, que permite las siguientes gestiones:

-  **Guardar:** Guarda las etiquetas asignadas a la regla, tal y como esté la lista en el momento de clicar en el botón.
-  **Reiniciar Lista:** Reinicia la lista a las etiquetas que tenga la regla asignadas en el momento de clicar en el botón.

-  **Limpiar Lista:** Quita todas las etiquetas de la lista, pero no las desasigna de la regla (a no ser que a continuación hagamos clic en el botón Guardar).

## 15 REGLAS YARA

En esta sección el usuario puede hacer todas las gestiones relativas al motor de reglas Yara de MARTA.



| Nombre                      | Descripción                                                      | Activa | Etiquetas  | Acciones                                                                                                                                                                    |
|-----------------------------|------------------------------------------------------------------|--------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apolmy_Privesc_Trojan       | APT - Terracota                                                  | ✓      | APT        |       |
| apt_backspace               | APT - BackSpace                                                  | ✓      | APT        |       |
| apt_duqu2_drivers           | ATP - Duqu 2.0                                                   | ✓      | APT        |       |
| apt_duqu2_loaders           | ATP - Duqu 2.0                                                   | ✓      | APT        |       |
| apt_hellsing_implantstrings | APT - HellSIng                                                   | ✓      | APT        |       |
| apt_hellsing_installer      | APT - HellSIng                                                   | ✓      | APT        |       |
| apt_hellsing_irene          | APT - HellSIng                                                   | ✓      | APT        |       |
| apt_hellsing_msgertype2     | APT - HellSIng                                                   | ✓      | APT        |       |
| apt_hellsing_proxytool      | APT - HellSIng                                                   | ✓      | APT        |       |
| apt_hellsing_xkat           | APT - HellSIng                                                   | ✓      | APT        |       |
| BackdoorFCKG                | CTB-Locker - [Ransomware] - [Cryptolocker]                       | ✓      | RNWR, CRYP |       |
| bin_ndisk                   | Exploit - Hacking Team                                           | ✓      | EXP        |       |
| Busca_configbin             | Busca un config ;.jpg;.png [config.bin quitado, saltaba siempre] | ✗      | EXP        |       |
| Busca_herramientas          | Busca herramientas análisis malware                              | ✓      | ADBB       |     |
| Busca_navegadores           | Comprueba si busca navegadores [falsos positivos]                | ✗      | RVGA       |   |
| Busca_unidades              | Busca unidades e,f,g,h en memoria [falsos positivos]             | ✗      | RNWR       |   |
| Busca_vbscript              | Busca si se esta usando VBSCRIPT                                 | ✓      | VBSC       |   |
| Careto_CnC                  | APT - Careto                                                     | ✓      | APT        |   |
| Careto_CnC_domains          | APT - Careto                                                     | ✓      | APT        |   |
| Careto_OSX_SBD              | ATP - Careto                                                     | ✓      | APT        |   |

### 15.1 LISTADO

En el listado el usuario puede ver paginadas las reglas Yara que hay en el sistema. También puede filtrar los resultados por uno o varios de los campos del listado.

En la lista se pueden ver los atributos más significativos de cada regla: el nombre, la descripción, si está activa (**una regla no activa no se tendrá en cuenta para las comprobaciones de reglas coincidentes de un análisis**) y sus etiquetas asociadas. Al igual que en las listas de ficheros y de análisis, es posible **filtrar** por cualquiera de estos campos.

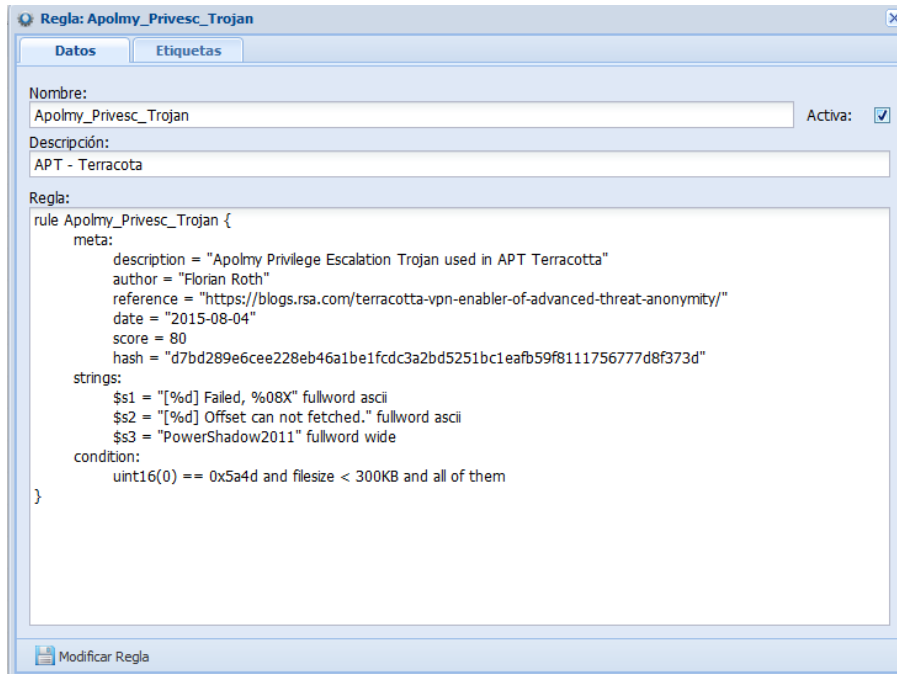
### 15.2 ACCIONES REGLAS YARA

Las acciones disponibles desde esta pantalla son las siguientes:

- Ver detalle de una regla
- Eliminar una regla
- Crear una regla
- Activar reglas seleccionadas
- Desactivar reglas seleccionadas
- Cargar reglas desde un fichero
- Gestionar etiquetas asociadas a las reglas Yara.

### 15.2.1 DETALLE REGLA YARA

Se accede al detalle de una regla desde el icono de detalle (lupa) en la columna de acciones . Desde esta opción el usuario puede ver el detalle de una regla Yara, modificar sus propiedades y etiquetas. La vista consta de dos partes, datos y etiquetas.



**Regla: Apolmy\_Privesc\_Trojan**

**Datos** | Etiquetas

Nombre: Apolmy\_Privesc\_Trojan Activa: ☒

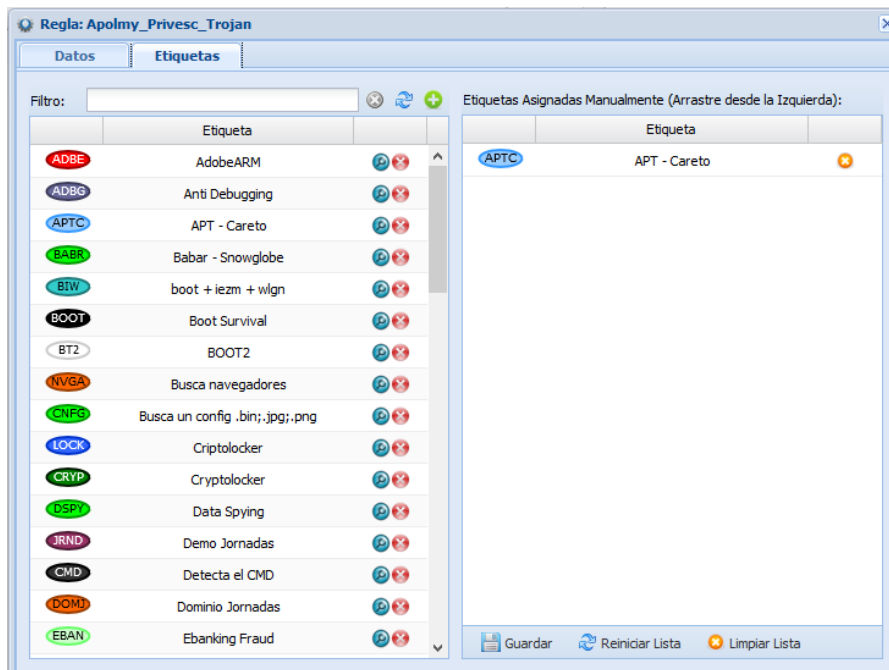
Descripción: APT - Terracota

Regla:

```
rule Apolmy_Privesc_Trojan {
  meta:
    description = "Apolmy Privilege Escalation Trojan used in APT Terracotta"
    author = "Florian Roth"
    reference = "https://blogs.rsa.com/terracotta-vpn-enabler-of-advanced-threat-anonymity/"
    date = "2015-08-04"
    score = 80
    hash = "d7bd289e6cee228eb46a1be1fcdc3a2bd5251bc1eafb59f8111756777d8f373d"
  strings:
    $s1 = "[%d] Failed, %08X" fullword ascii
    $s2 = "[%d] Offset can not fetched." fullword ascii
    $s3 = "PowerShadow2011" fullword wide
  condition:
    uint16(0) == 0x5a4d and filesize < 300KB and all of them
}
```

 Modificar Regla

El usuario puede fácilmente gestionar las etiquetas asociadas a una regla Yara arrastrando de un lado a otro una o varias etiquetas seleccionadas desde cada una de las partes.



**Regla: Apolmy\_Privesc\_Trojan**

**Datos** | **Etiquetas**

Filtro:

| Etiqueta                                                                                                           |                                                                                     |
|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|  AdobeARM                       |  |
|  Anti Debugging                 |  |
|  APT - Careto                   |  |
|  Babar - Snowglobe              |  |
|  boot + iezm + wlgm             |  |
|  Boot Survival                  |  |
|  BOOT2                          |  |
|  Busca navegadores              |  |
|  Busca un config .bin;.jpg;.png |  |
|  Criptolocker                   |  |
|  Cryptolocker                   |  |
|  Data Spying                    |  |
|  Demo Jornadas                  |  |
|  Detecta el CMD                 |  |
|  Dominio Jornadas               |  |
|  Ebanking Fraud                 |  |

Etiquetas Asignadas Manualmente (Arrastre desde la Izquierda):

| Etiqueta                                                                                         |                                                                                       |
|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
|  APT - Careto |  |

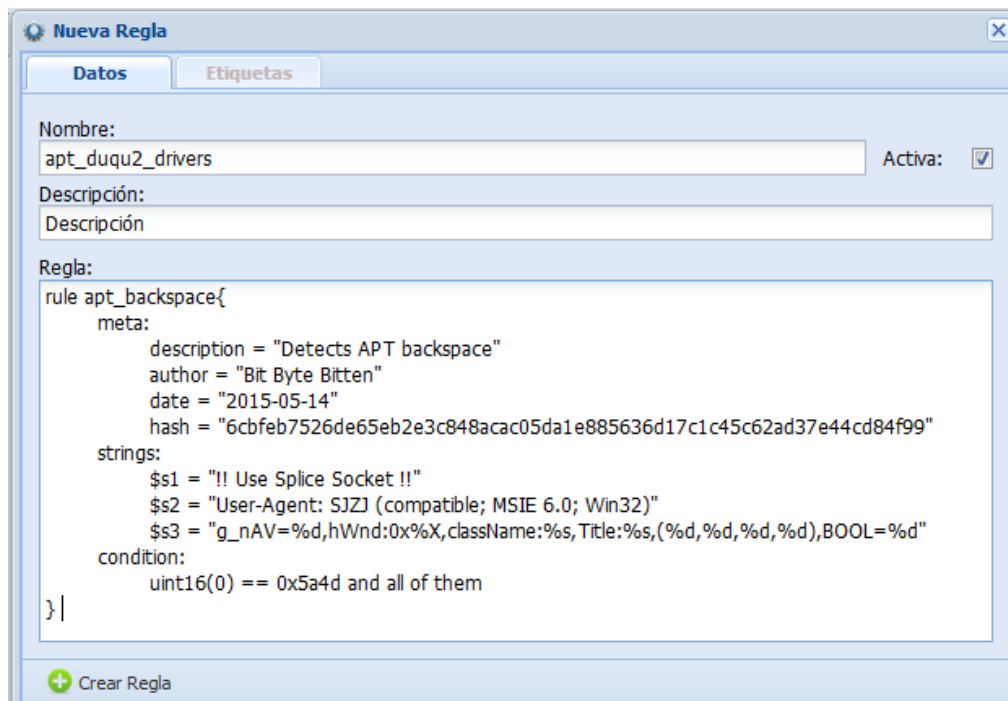
 Guardar  Reiniciar Lista  Limpiar Lista

### 15.2.2 ELIMINAR REGLA YARA

El usuario puede eliminar una regla el icono rojo en la columna de acciones . La aplicación pide al usuario confirmación antes de hacer el borrado de la regla.

### 15.2.3 CREAR REGLA YARA

Se puede crear una nueva regla desde el icono  Crear Regla situado en la barra inferior de menú.



The screenshot shows a dialog box titled "Nueva Regla" with two tabs: "Datos" and "Etiquetas". The "Datos" tab is active. It contains the following fields and controls:

- Nombre:** A text box containing "apt\_duqu2\_drivers".
- Activa:** A checkbox that is checked.
- Descripción:** A text box containing "Descripción".
- Regla:** A large text area containing YARA code:
 

```
rule apt_backspace{
  meta:
    description = "Detects APT backspace"
    author = "Bit Byte Bitten"
    date = "2015-05-14"
    hash = "6cbfeb7526de65eb2e3c848acac05da1e885636d17c1c45c62ad37e44cd84f99"
  strings:
    $s1 = "!! Use Splice Socket !!"
    $s2 = "User-Agent: SJZJ (compatible; MSIE 6.0; Win32)"
    $s3 = "g_nAV=%d,hWnd:0x%X,className:%s,Title:%s,(%d,%d,%d,%d),BOOL=%d"
  condition:
    uint16(0) == 0x5a4d and all of them
}
```

At the bottom of the dialog is a button with a green plus icon and the text "Crear Regla".

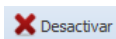
### 15.2.4 ACTIVAR REGLAS SELECCIONADAS

El usuario puede activar una o varias reglas seleccionadas utilizando el icono  Activar situado en la barra inferior de menú.

| Reglas Ioc                  | Reglas Yara                                                      | Fuentes                             | Organismos | Usuarios |
|-----------------------------|------------------------------------------------------------------|-------------------------------------|------------|----------|
| Nombre                      | Descripción                                                      | Activa                              | Etiquetas  | Acciones |
| Apolmy_Privesc_Trojan       | APT - Terracota                                                  | <input checked="" type="checkbox"/> | APTc       |          |
| apt_backspace               | APT - BackSpace                                                  | <input checked="" type="checkbox"/> | APTc       |          |
| apt_duqu2_drivers           | ATP - Duqu 2.0                                                   | <input checked="" type="checkbox"/> | APTc       |          |
| apt_duqu2_loaders           | ATP - Duqu 2.0                                                   | <input checked="" type="checkbox"/> | APTc       |          |
| apt_hellsing_implantstrings | APT - HellSIng                                                   | <input checked="" type="checkbox"/> | APTc       |          |
| apt_hellsing_installer      | APT - HellSIng                                                   | <input checked="" type="checkbox"/> | APTc       |          |
| apt_hellsing_irene          | APT - HellSIng                                                   | <input checked="" type="checkbox"/> | APTc       |          |
| apt_hellsing_msgrtype2      | APT - HellSIng                                                   | <input checked="" type="checkbox"/> | APTc       |          |
| apt_hellsing_proxytool      | APT - HellSIng                                                   | <input checked="" type="checkbox"/> | APTc       |          |
| apt_hellsing_xkat           | APT - HellSIng                                                   | <input checked="" type="checkbox"/> | APTc       |          |
| BackdoorFCGK                | CTB-Locker - [Ransomware] - [Cryptolocker]                       | <input checked="" type="checkbox"/> | RNWR CKYP  |          |
| bin_ndsk                    | Exploit - Hacking Team                                           | <input checked="" type="checkbox"/> | EXPL       |          |
| Busca_configbin             | Busca un config ;jogg.png [config.bin quitado , saltaba siempre] | <input checked="" type="checkbox"/> | CSTC       |          |
| Busca_herramientas          | Busca herramientas análisis malware                              | <input checked="" type="checkbox"/> | ADBB       |          |
| Busca_navegadores           | Comprueba si busca navegadores [falsos positivos]                | <input checked="" type="checkbox"/> | NVGA       |          |
| Busca_unidades              | Busca unidades e,f,g,h en memoria [falsos positivos]             | <input checked="" type="checkbox"/> | RNWR       |          |
| Busca_vbscript              | Busca si se esta usando VBSCRIPT                                 | <input checked="" type="checkbox"/> | VESC       |          |
| Careto_CnC                  | APT - Careto                                                     | <input checked="" type="checkbox"/> | APTc       |          |
| Careto_CnC_domains          | APT - Careto                                                     | <input checked="" type="checkbox"/> | APTc       |          |
| Careto_OSX_SBD              | ATP - Careto                                                     | <input checked="" type="checkbox"/> | APTc       |          |

### 15.2.5 DESACTIVAR REGLAS SELECCIONADAS

El usuario puede desactivar una o varias reglas seleccionadas utilizando el icono



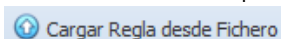
situado en la barra inferior de menú.

| Reglas Toc                  | Reglas Yara                                                     | Fuentes | Organismos | Usuarios |
|-----------------------------|-----------------------------------------------------------------|---------|------------|----------|
| Nombre                      | Descripción                                                     | Activa  | Etiquetas  | Acciones |
| Apolmy_Privesc_Trojan       | APT - Terracota                                                 | ✓       | APTC       | [Icono]  |
| apt_backspace               | APT - BackSpace                                                 | ✓       | APTC       | [Icono]  |
| apt_duqu2_drivers           | ATP - Duqu 2.0                                                  | ✓       | APTC       | [Icono]  |
| apt_duqu2_loaders           | ATP - Duqu 2.0                                                  | ✓       | APTC       | [Icono]  |
| apt_hellsing_implantstrings | APT - HellSing                                                  | ✓       | APTC       | [Icono]  |
| apt_hellsing_installer      | APT - HellSing                                                  | ✓       | APTC       | [Icono]  |
| apt_hellsing_rene           | APT - HellSing                                                  | ✓       | APTC       | [Icono]  |
| apt_hellsing_msrger type2   | APT - HellSing                                                  | ✓       | APTC       | [Icono]  |
| apt_hellsing_proxytool      | APT - HellSing                                                  | ✓       | APTC       | [Icono]  |
| apt_hellsing_xkat           | APT - HellSing                                                  | ✓       | APTC       | [Icono]  |
| BackdoorFCGK                | CTB-Locker - [Ransomware] - [Cryptolocker]                      | ✓       | RNMR CRYP  | [Icono]  |
| bin_ndsk                    | Exploit - Hacking Team                                          | ✓       | EXPL       | [Icono]  |
| Busca_configbin             | Busca un config ;pgg.png [config.bin quitado , saltaba siempre] | ✓       | CONF       | [Icono]  |
| Busca_herramientas          | Busca herramientas análisis malware                             | ✓       | ANBO       | [Icono]  |
| Busca_navegadores           | Comprueba si busca navegadores [falsos positivos]               | ✓       | NVGA       | [Icono]  |
| Busca_unidades              | Busca unidades e,f,g,h en memoria [falsos positivos]            | ✗       | RNMR       | [Icono]  |
| Busca_vbscript              | Busca si se esta usando VBSCRIPT                                | ✓       | VBSO       | [Icono]  |
| Careto_CnC                  | APT - Careto                                                    | ✓       | APTC       | [Icono]  |
| Careto_CnC_domains          | APT - Careto                                                    | ✓       | APTC       | [Icono]  |
| Careto_OSX_SBD              | ATP - Careto                                                    | ✓       | APTC       | [Icono]  |

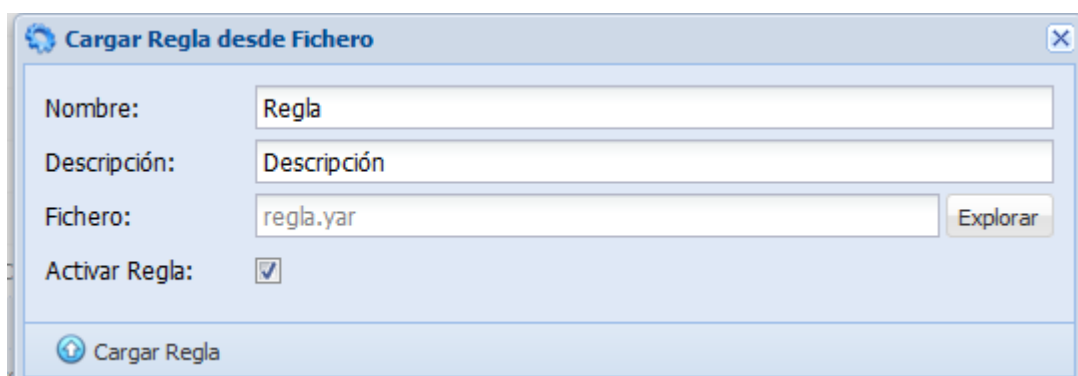
Page 1 de 5
Cargar Regla desde Fichero
Crear Regla
Activar
Desactivar
Publicar en Sandboxes
Mostrando del 1 al 20, Total: 96
20
por página

### 15.2.6 CARGAR REGLAS DESDE UN FICHERO

El usuario puede cargar una regla desde un fichero utilizando el icono

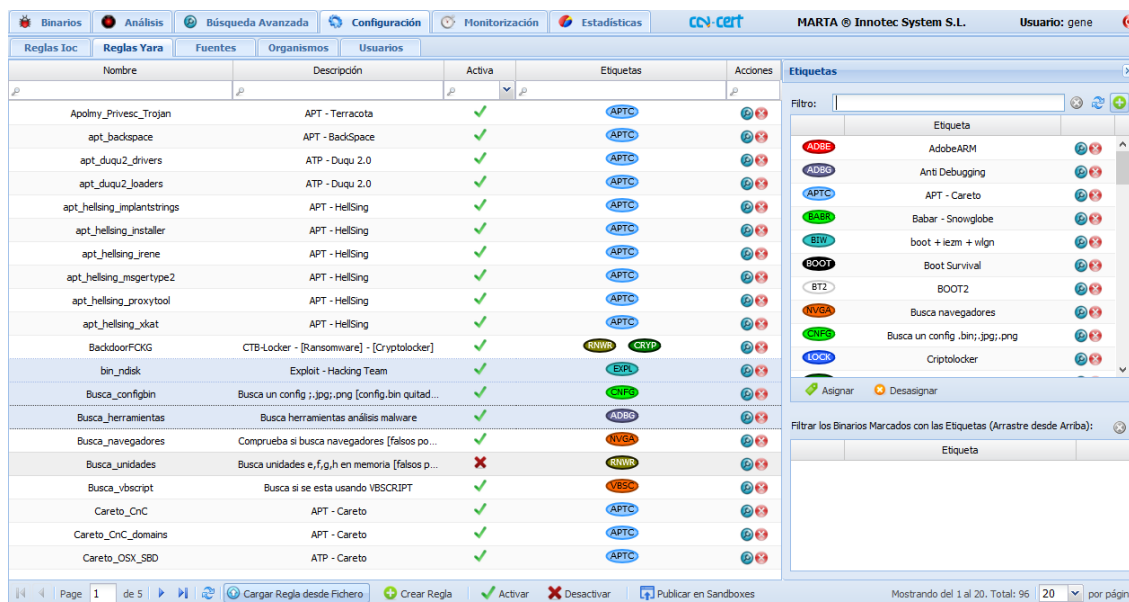


situado en la barra inferior de menú.



### 15.2.7 ETIQUETAS

En la parte derecha de la pestaña, hay un panel desplegable que permite al usuario hacer **gestiones con las etiquetas** asociadas a los análisis, de forma totalmente similar a los de las pestañas de binarios y análisis.



| Nombre                      | Descripción                                      | Activa | Etiquetas  | Acciones |
|-----------------------------|--------------------------------------------------|--------|------------|----------|
| Apolmy_Privesc_Trojan       | APT - Terracota                                  | ✓      | APT-C      | [+/-]    |
| apt_backspace               | APT - BackSpace                                  | ✓      | APT-C      | [+/-]    |
| apt_duqu2_drivers           | ATP - Duqu 2.0                                   | ✓      | APT-C      | [+/-]    |
| apt_duqu2_loaders           | ATP - Duqu 2.0                                   | ✓      | APT-C      | [+/-]    |
| apt_hellsing_implantstrings | APT - HellSing                                   | ✓      | APT-C      | [+/-]    |
| apt_hellsing_installer      | APT - HellSing                                   | ✓      | APT-C      | [+/-]    |
| apt_hellsing_jrene          | APT - HellSing                                   | ✓      | APT-C      | [+/-]    |
| apt_hellsing_msgrtype2      | APT - HellSing                                   | ✓      | APT-C      | [+/-]    |
| apt_hellsing_proxytool      | APT - HellSing                                   | ✓      | APT-C      | [+/-]    |
| apt_hellsing_xkat           | APT - HellSing                                   | ✓      | APT-C      | [+/-]    |
| BackdoorFCG                 | CTB-Locker - [Ransomware] - [Cryptolocker]       | ✓      | RNWR, CRYP | [+/-]    |
| bin_ndisk                   | Exploit - Hacking Team                           | ✓      | EXP        | [+/-]    |
| Busca_configbin             | Busca un config ;.jpg;.png [config.bin quitad... | ✓      | CRYP       | [+/-]    |
| Busca_herramientas          | Busca herramientas análisis malware              | ✓      | ADBG       | [+/-]    |
| Busca_navegadores           | Comprueba si busca navegadores [falsos po...     | ✓      | NVGA       | [+/-]    |
| Busca_unidades              | Busca unidades e,f,g,h en memoria [falsos p...   | ✗      | RNWR       | [+/-]    |
| Busca_vbscript              | Busca si se esta usando VBSCRIPT                 | ✓      | VBS        | [+/-]    |
| Careto_CnC                  | APT - Careto                                     | ✓      | APT-C      | [+/-]    |
| Careto_CnC_domains          | APT - Careto                                     | ✓      | APT-C      | [+/-]    |
| Careto_OSX_SBD              | ATP - Careto                                     | ✓      | APT-C      | [+/-]    |

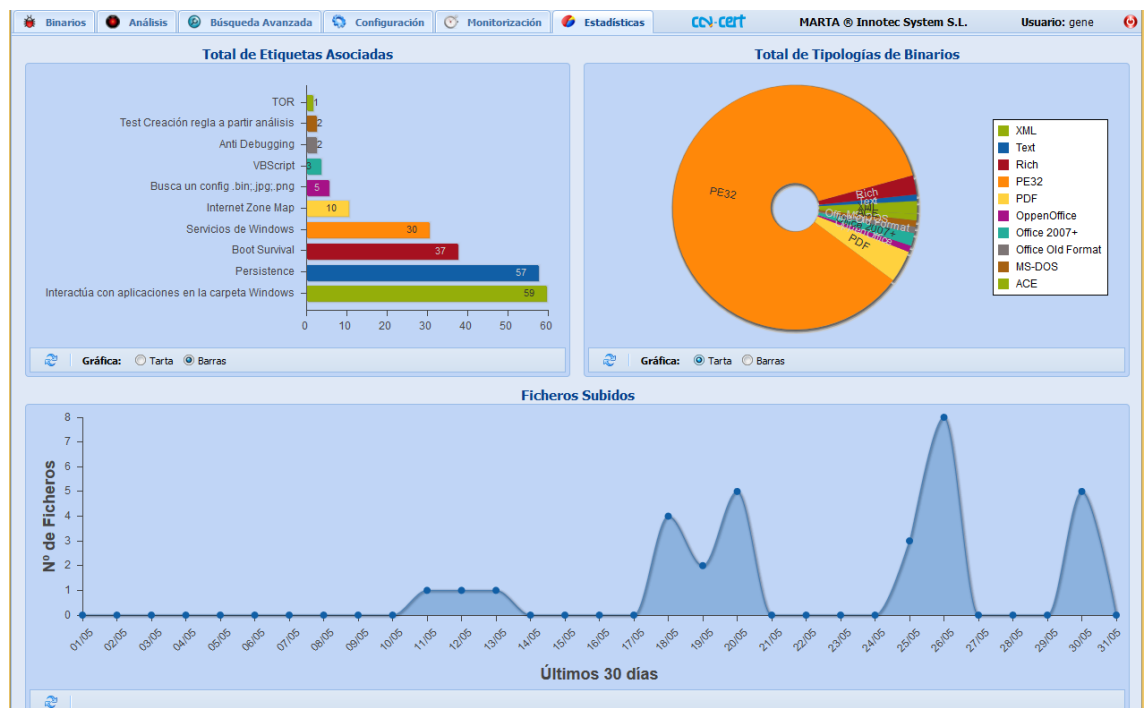
La asignación de **etiquetas** a **reglas** es **muy importante**, dado que las reglas definen los comportamientos que queremos detectar en las muestras analizadas. Los análisis de muestras reciben todas las etiquetas asociadas a las reglas que cumplen. Y los propios ficheros de código dañino reciben todas las etiquetas asociadas a sus análisis. Por tanto, las **etiquetas** que asociemos a reglas que definan comportamientos que queremos detectar, estarán **asociadas** a los ficheros de código dañino que tengan esos **comportamientos**.

De esta forma, podremos reconocer rápidamente el **comportamiento** de un **fichero** echando un **vistazo a sus etiquetas**. O podremos **buscar muestras** con un comportamiento específico **filtrando ficheros por etiquetas**.

| Reglas Yara | Fuentes                    | Organismos                                     | Persistencia | Reglas Yara | Fuentes  | Organismos | Persistencia |
|-------------|----------------------------|------------------------------------------------|--------------|-------------|----------|------------|--------------|
| Organismo   | Nombre                     | Descripción                                    | Activa       | Etiquetas   | Acciones | Etiquetas  |              |
| CCN         | Apolmy_Privesc_Trojan      | APT - Terracota                                | ✓            | APTTC       |          |            |              |
| CCN         | apt_backspace              | APT - BackSpace                                | ✓            | APTTC       |          |            |              |
| CCN         | apt_duqu2_drivers          | ATP - Duqu 2.0                                 | ✓            | APTTC       |          |            |              |
| CCN         | apt_duqu2_loaders          | ATP - Duqu 2.0                                 | ✓            | APTTC       |          |            |              |
| CCN         | apt_helsing_implantstrings | APT - Helsing                                  | ✓            | APTTC       |          |            |              |
| CCN         | apt_helsing_installer      | APT - Helsing                                  | ✓            | APTTC       |          |            |              |
| CCN         | apt_helsing_rene           | APT - Helsing                                  | ✓            | APTTC       |          |            |              |
| CCN         | apt_helsing_msgrtype2      | APT - Helsing                                  | ✓            | APTTC       |          |            |              |
| CCN         | apt_helsing_proxytool      | APT - Helsing                                  | ✓            | APTTC       |          |            |              |
| CCN         | apt_helsing_xlat           | APT - Helsing                                  | ✓            | APTTC       |          |            |              |
| CCN         | BackdoorFCXG               | CTB-Locker - [Ransomware] - [Cryptolocker]     | ✓            | RMWR        |          |            |              |
| CCN         | bin_ndisk                  | Exploit - Hacking Team                         | ✓            | EXPL        |          |            |              |
| CCN         | Busca_configbin            | Busca un config .jpg;.png [config.bin quita... | ✓            | CONF        |          |            |              |
| CCN         | Busca_herramientas         | Busca herramientas an [falsos malware          | ✓            | ADBS        |          |            |              |
| CCN         | Busca_navegadores          | Comprueba si busca navegadores [falsos p...    | ✓            | NVSA        |          |            |              |
| CCN         | Busca_unidades             | Busca unidades e,f,g,h en memoria [falsos ...  | ✗            | YVSA        |          |            |              |
| CCN         | Busca_vbscript             | Busca si se esta usando VBSCRIPT               | ✓            | VBSA        |          |            |              |
| CCN         | Careto_CnC                 | APT - Careto                                   | ✓            | APTTC       |          |            |              |
| CCN         | Careto_CnC_domains         | APT - Careto                                   | ✓            | APTTC       |          |            |              |

## 16 PESTAÑA DE ESTADÍSTICAS

Esta pestaña muestra estadísticas sobre las etiquetas más comunes (Total de Etiquetas Asociadas), los tipos de ficheros más comunes (Total de Tipologías de Binarios), y la cantidad de ficheros subidos a MARTA por días durante los últimos 30 días.



Las gráficas de Total de Etiquetas Asociadas y Total de Tipologías de Binarios pueden consultarse en formato de tarta o de barras.

