



HERRAMIENTAS

## MARTA: Manual de Usuario

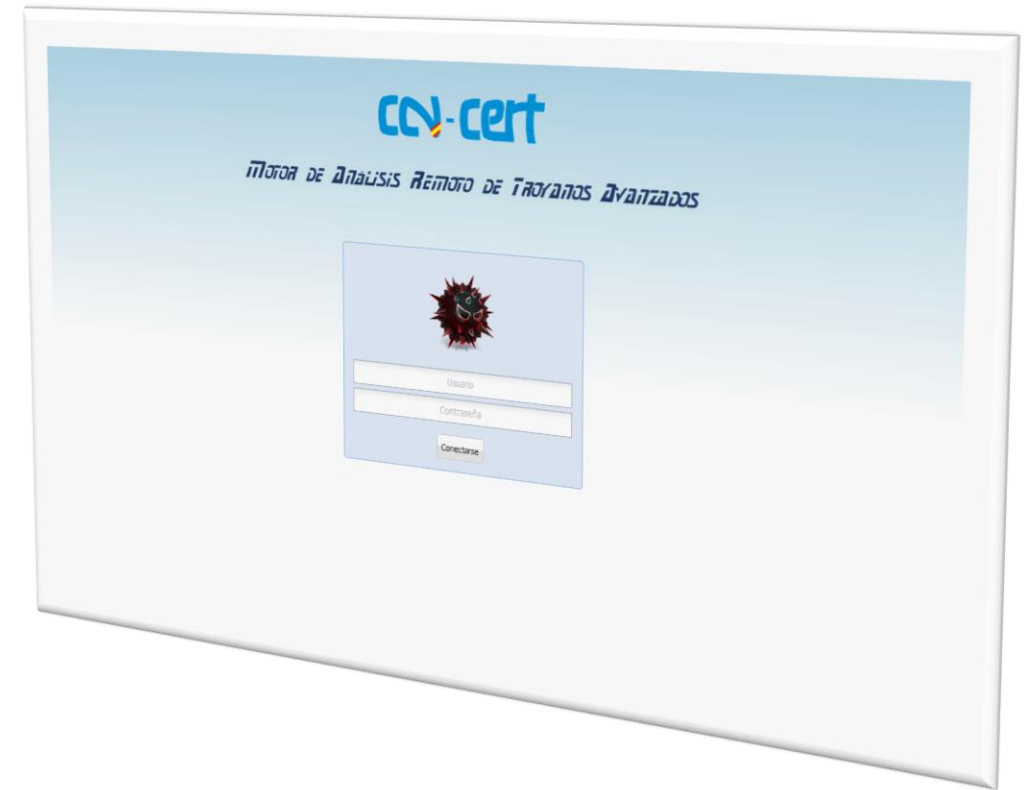
Motor de Análisis Remoto  
de Troyanos Avanzados

<https://marta.ccn-cert.cni.es>

[marta@ccn-cert.cni.es](mailto:marta@ccn-cert.cni.es)

## Índice

1. Introducción
2. Interfaz principal de MARTA
3. Subir binario a MARTA
  - 3.1. Elementos de la interfaz “Subir Binario”
  - 3.2. Opciones de las Sandbox Cuckoo y Joe
4. Análisis Estáticos
  - 4.1. Pestaña General
  - 4.2. Pestaña de Detalles
5. Análisis Dinámicos
6. Reglas
  - 6.1. Reglas IOC
  - 6.2. Reglas YARA
7. Etiquetas
  - 7.1. Operaciones
  - 7.2. Acciones



## 1. Introducción

- La herramienta MARTA, desarrollada por el CCN-CERT, es una plataforma avanzada de **sandboxing**, dedicada al **análisis automatizado** de múltiples tipos de ficheros, que podrían tener un comportamiento malicioso y que no son detectados por los programas antivirus.
- El análisis de ficheros incluye **ejecutables**, documentos de **office** o **pdf**, entre otros.
- En una primera fase, esta herramienta está destinada a todas las organizaciones que se encuentren adheridas al **Sistema de Alerta Temprana** del CCN-CERT que pueden acceder a ella a través de la dirección: <https://marta.ccn-cert.cni.es>

### Ventajas para el usuario

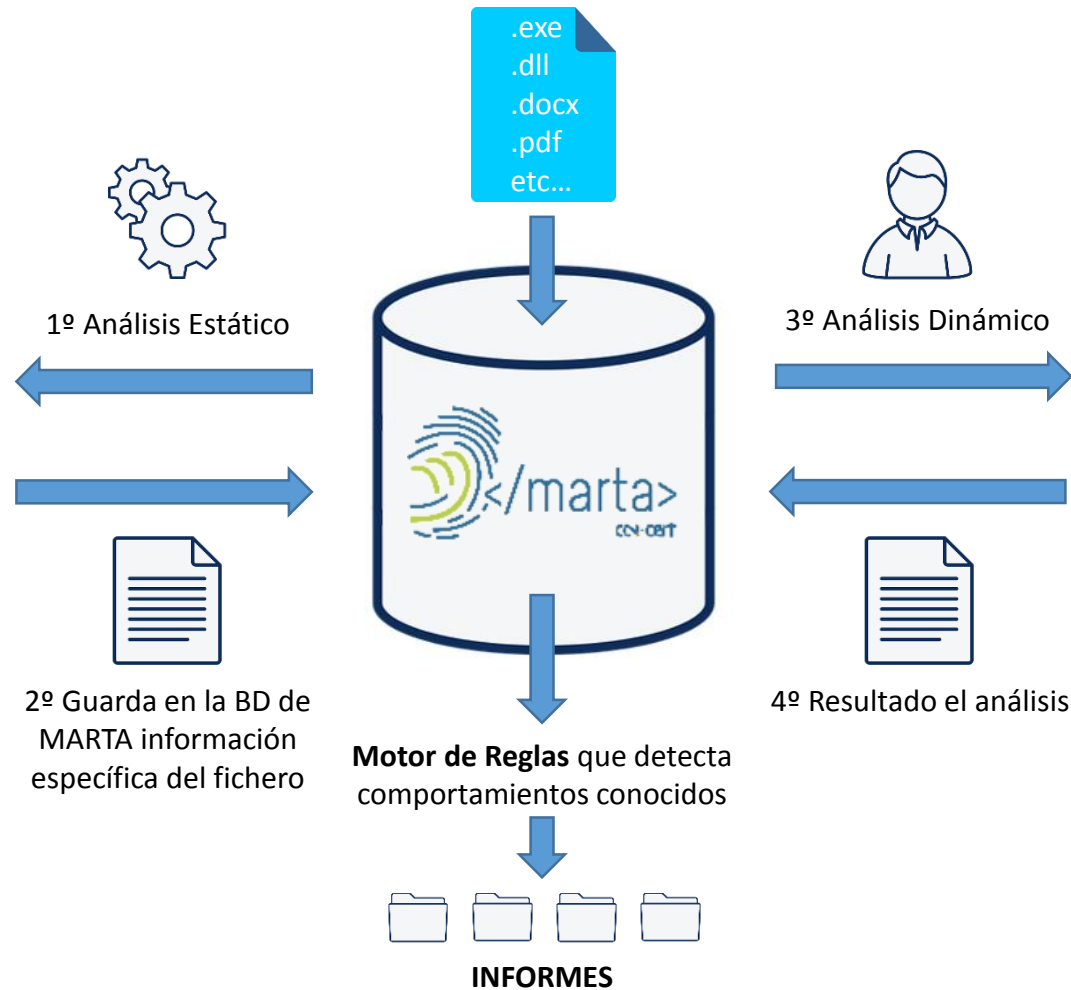
- Detección precoz de amenazas provenientes de código dañino, analizando las características de un fichero más allá de la información facilitada por un antivirus.
- Utilización de un sitio centralizado y seguro en el que albergar las muestras de malware de un modo organizado y con una herramienta de búsqueda avanzada.
- Organización, a través de un sistema de etiquetas, de toda la información a través de un modo visual y ágil de ficheros, análisis y reglas.

## 1. Introducción

El siguiente esquema muestra las fases del análisis

### Análisis Estático

Lo primero que hace la aplicación cuando recibe un fichero, es pasarle una serie de **scripts "estáticos"** (el código dañino no se ejecuta en ningún momento mientras se le analiza con estos scripts)




### Análisis Dinámico


Consiste en **infectar una máquina virtual** que tenga instalado un sistema operativo concreto con el fichero sospechoso (clonado de máquina virtual, copiado del fichero y ejecución del mismo)







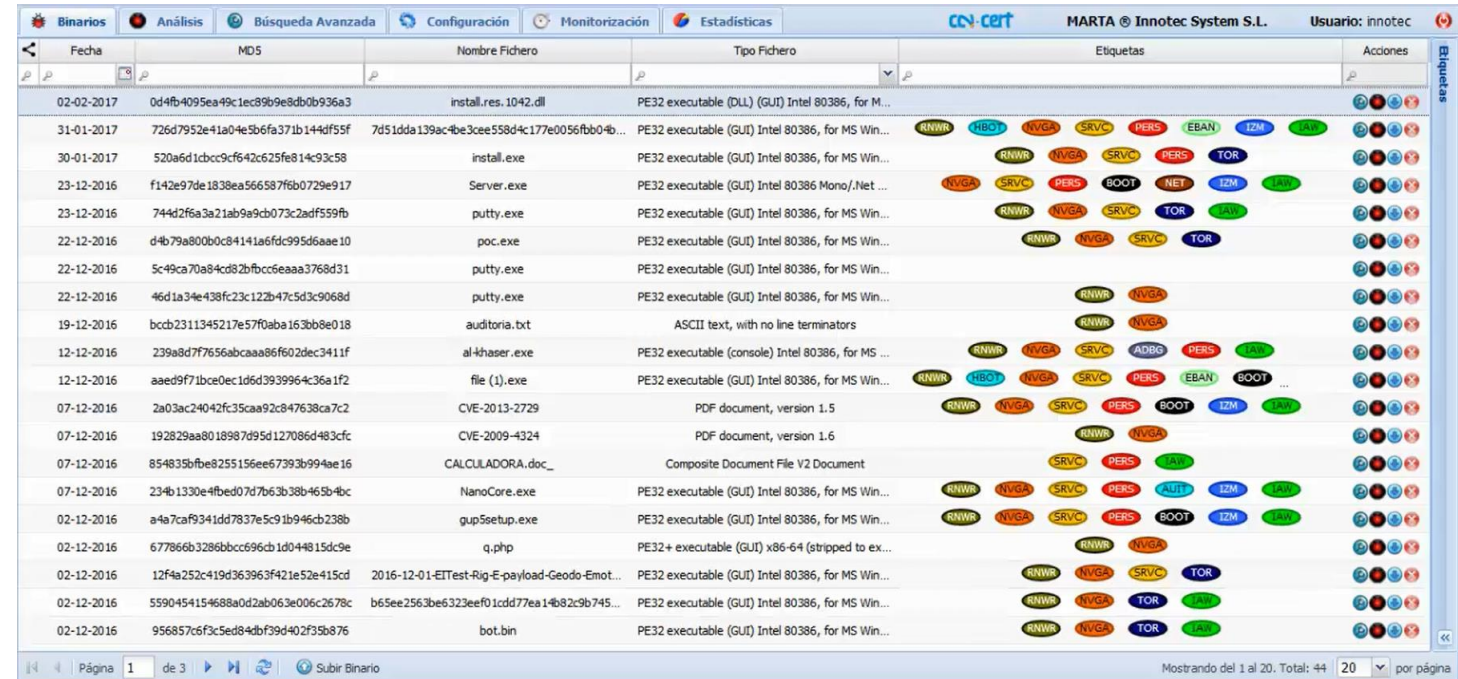
## 2. Interfaz principal de MARTA

 **Binarios:** Muestra una lista con todos los ficheros subidos a MARTA. Permite subir nuevas muestras, crear análisis dinámicos y filtrar resultados.

 **Análisis:** Muestra una lista con todos los análisis de ficheros realizados. Permite hacer filtros rápidos sobre los análisis, ver sus detalles y también reanalizar las muestras.

 **Búsqueda Avanzada:** Permite hacer búsquedas de binarios que cumplan una serie de directrices.

 **Configuración:** Permite la gestión de Reglas, Fuentes, Organismos y Usuarios de la aplicación.



Fecha	MD5	Nombre Fichero	Tipo Fichero	Etiquetas	Acciones
02-02-2017	0d4fb4095ea49c1ec89b9e8db0b936a3	install.res.1042.dll	PE32 executable (DLL) (GUI) Intel 80386, for M...		
31-01-2017	726d7952e41a04e5b6fa371b144df55f	7d51dda139ac4be3cee558d4c177e0056fbb04b...	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, SRVC, PERS, EBAN, IZM, SAV	
30-01-2017	520a6d1c9cc9cf642c625fe814c93c58	install.exe	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, SRVC, PERS, TOR	
23-12-2016	f142e97de1838ea566587f6b0729e917	Server.exe	PE32 executable (GUI) Intel 80386 Mono/.Net ...	NCVGA, SRVC, PERS, BOOT, NET, IZM, SAV	
23-12-2016	744d2f6a3a21ab9a9cb073c2adff559fb	putty.exe	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, SRVC, TOR, SAV	
22-12-2016	d4b79a800b0c84141a6fcd995d6aae10	poc.exe	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, SRVC, TOR	
22-12-2016	5c49ca70a84cd82bfcc6eaaa3768d31	putty.exe	PE32 executable (GUI) Intel 80386, for MS Win...		
22-12-2016	46d1a34e438fc23c122b47c5d3c9068d	putty.exe	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA	
19-12-2016	bcd2311345217e57f0aba163bb8e018	auditoria.txt	ASCII text, with no line terminators	RNWR, NCVGA	
12-12-2016	239a8d7f7656abcaaa86f602dec3411f	al-khaser.exe	PE32 executable (console) Intel 80386, for MS ...	RNWR, NCVGA, SRVC, ADBG, PERS, EBAN, BOOT	
12-12-2016	aaed9f71bce0ec1d6d3993964c36a1f2	file (1).exe	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, SRVC, PERS, EBAN, BOOT	
07-12-2016	2a03ac24042fc35caa92c847638ca7c2	CVE-2013-2729	PDF document, version 1.5	RNWR, NCVGA, SRVC, PERS, BOOT, IZM, SAV	
07-12-2016	192829aa8018987d95d127086d483cf	CVE-2009-4324	PDF document, version 1.6	RNWR, NCVGA	
07-12-2016	854835fbfe8255156ee67393b994ae16	CALCULADORA.doc_	Composite Document File V2 Document	SRVC, PERS, EBAN	
07-12-2016	234b1330e4fbed07d7b63b38b465b4bc	NanoCore.exe	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, SRVC, PERS, EBAN, IZM, SAV	
02-12-2016	a4a7caf9341dd7837e5c91b946cb238b	gup5etup.exe	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, SRVC, PERS, BOOT, IZM, SAV	
02-12-2016	677866b3286bcc696cd1d044815dc9e	q.php	PE32+ executable (GUI) x86-64 (stripped to ex...	RNWR, NCVGA	
02-12-2016	12f4a252c419d363963f421e52e415cd	2016-12-01-ETTest-Rig-E-payload-Geodo-Emot...	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, SRVC, TOR	
02-12-2016	5590454154688a0d2ab063e006c2678c	b65ee2563be322eef01cdd77ea14b82c9b745...	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, TOR, EBAN	
02-12-2016	956857c6f3c5ed84dbf39d402f35b876	bot.bin	PE32 executable (GUI) Intel 80386, for MS Win...	RNWR, NCVGA, TOR, EBAN	

 **Monitorización:** Proporciona información sobre el estado de los análisis en proceso.

 **Estadísticas:** Proporciona información visual a través de gráficos sobre estadísticas.

### 3. Subir binario a MARTA

Para subir un binario hacemos clic en el botón **Subir Binario** situado en la parte inferior de la aplicación:

Esta vista permite **subir un fichero nuevo** a MARTA y hacerle uno o varios análisis dinámicos directamente.

#### 3.1 Elementos de la interfaz “Subir Binario”

**Fichero:** elegimos el fichero que queremos analizar.

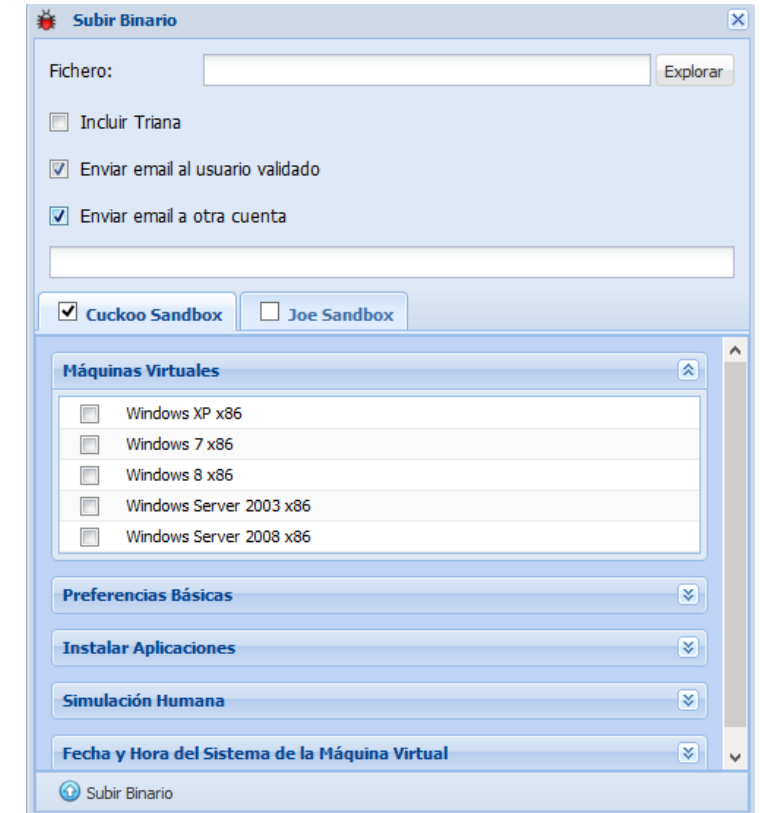
**Enviar email al usuario validado:** envía un mail cuando solicitamos el análisis y otro mail cuando termina.

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

#### 3.2 Opciones de las Sandbox Cuckoo y Joe

Permite configurar las opciones de análisis tanto de Cuckoo Sandbox como de Joe Sandbox.

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.



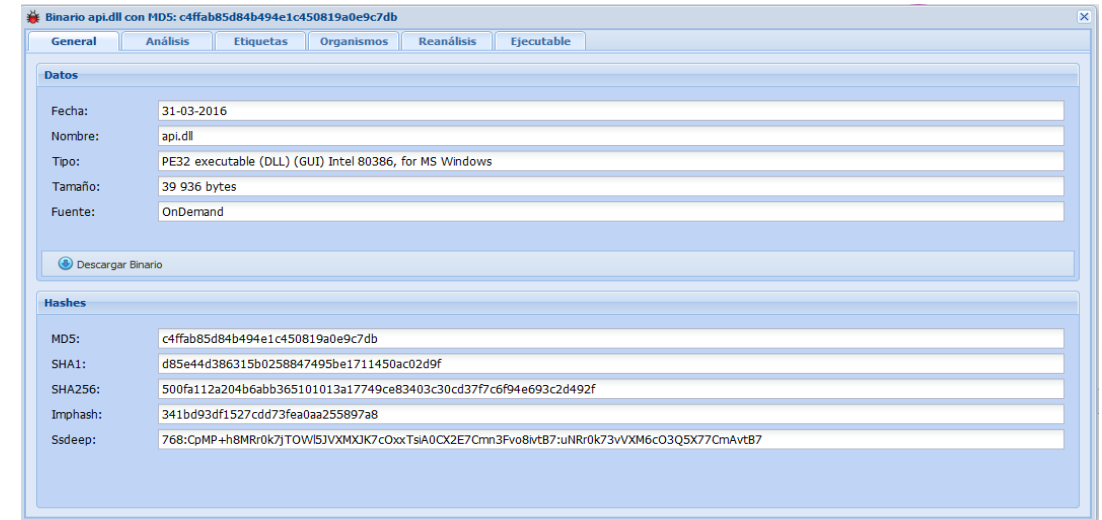
## 4. Análisis estáticos

Una vez subido el fichero es posible consultar diversa información del mismo, proveniente de su **análisis estático**.

### 4.1 Pestaña General

Muestra **información básica acerca del fichero**:

- Fecha en la que se subió a MARTA
- Nombre
- Tipo
- Tamaño
- Fuente (esto indica si se subió manualmente, “OnDemand”, o si fue recolectado por un colector)
- Hashes: MD5, SHA1, SHA256, Imphash y Ssdeep.



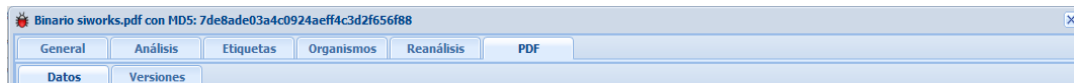
### 4.2 Pestaña de Detalles

En función del fichero subido (ejecutable, .docx, .odt, .pdf, etc.), muestra toda la información extraída por los **scripts estáticos** acerca del fichero.

- Detalles Ejecutable:



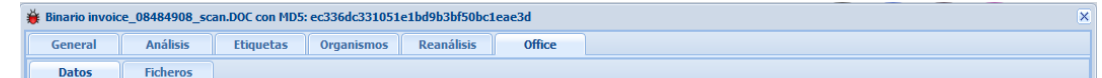
- Detalles PDF:



- Detalles Office:



- Detalles OpenOffice:


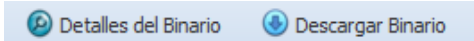


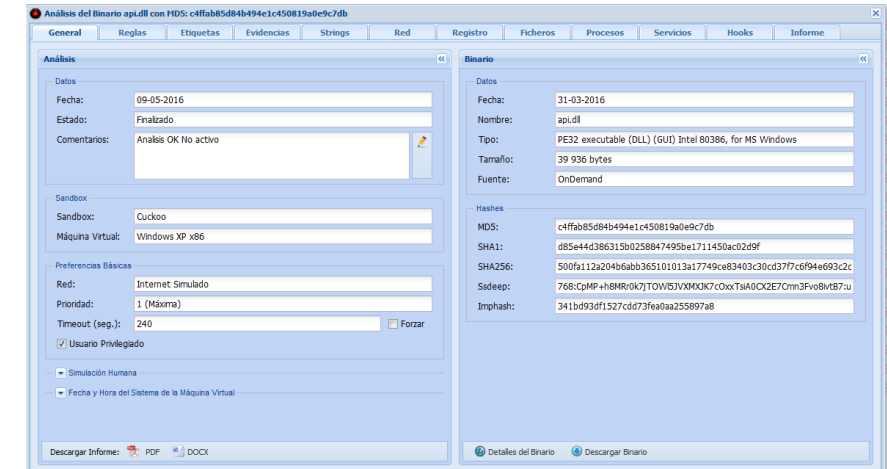
## 5. Análisis dinámicos

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

Se obtiene pinchando con el botón derecho del ratón sobre el fichero y seleccionando **Ver Detalle**.

Dispone de múltiples pestañas:

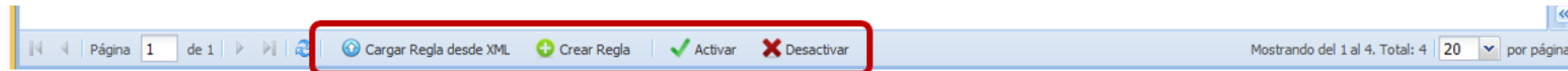
- **General:** Información del análisis y del fichero analizado. Permite:
  - Descargar el informe en PDF o DOCX: 
  - Descargar y ver los detalles del binario: 
- **Reglas:** Reglas coincidentes con el análisis y permite generar reglas a partir de él.
- **Etiquetas:** etiquetas asociadas al análisis.
- **Evidencias:** 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:** Claves de registro abiertas, leídas, escritas y eliminadas durante el análisis.
- **Ficheros:** Ficheros abiertos, leídos, escritos, eliminados, ejecutados, movidos y copiados durante el análisis.
- **Procesos:** Procesos creados durante el análisis.
- **Servicios:** Servicios de sistema operativo creados durante el análisis.
- **Informe:** Generación de informes a medida.





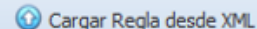
## 6. Reglas en MARTA


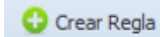
MARTA cuenta con un **Motor de Reglas** que permite definir **comportamientos reconocidos**. Se puede acceder a las reglas desde la pestaña **Configuración**. En la barra inferior de la pestaña de reglas hay botones que permiten realizar **gestiones** que no están directamente ligadas a una regla:



### 6.1 Reglas IOC / Yara




Facilita todas las gestiones relacionadas con el motor de reglas IOC / Yara.

 **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). 

 **Crear Regla:** Abre la vista de detalles de una regla, vacía, para crear una regla nueva desde cero. 

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

Una vez creada una regla, se pueden hacer varias operaciones con ella:

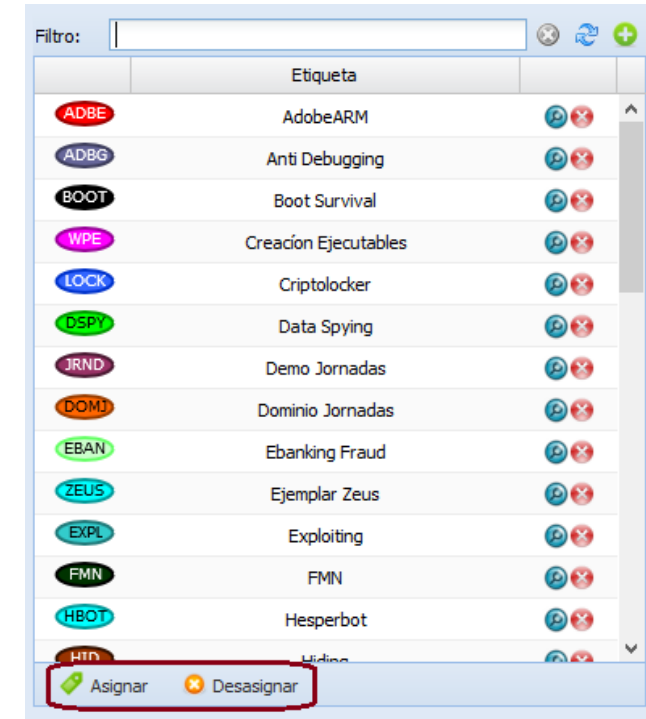
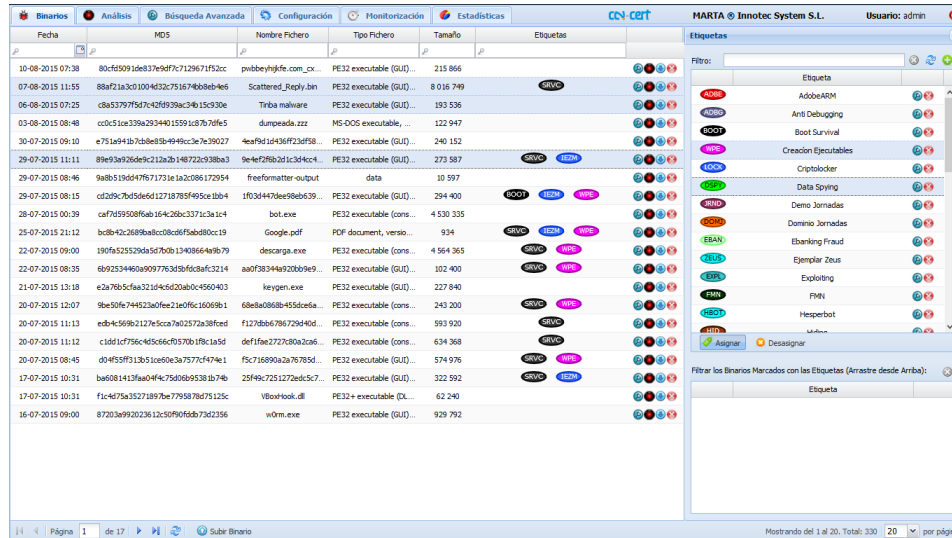
-  **Ver Detalle:** Abre la vista de detalles de la regla seleccionada. Esta vista contiene toda la información relativa a la regla.
-  **Descargar Regla como XML:** Permite exportar la regla a un fichero con formato XML y descargarlo.
-  **Eliminar:** Elimina la regla seleccionada. Pide confirmación antes de eliminar.

## 7. Etiquetas en MARTA

MARTA dispone de un **Sistema de Etiquetas** que permite una organización rápida y sencilla.

### Acciones:

- 📌 **Asignar:** Permite asignar todas las etiquetas seleccionadas a todos los ficheros seleccionados. Solo se podrán asignar etiquetas creadas por nuestra organización.



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

➤ **Acceso a MARTA**

➤ <https://marta.ccn-cert.cni.es>

➤ **Correo electrónico**

➤ [marta@ccn-cert.cni.es](mailto:marta@ccn-cert.cni.es)

➤ **Más información**

➤ <https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/marta.html>

➤ **Síguenos en**

