

# microCLAUDIA

Centro de vacunación



## Manual de usuario

Versión Septiembre 2023



## Índice

<b>1</b>	<b>SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL</b>	<b>6</b>
<b>2</b>	<b>INTRODUCCIÓN</b>	<b>7</b>
2.1	¿Qué es el ransomware? . . . . .	7
2.2	¿Cómo infecta el ransomware? . . . . .	7
2.3	¿Qué es microCLAUDIA? . . . . .	7
2.4	¿Qué es una vacuna? . . . . .	8
<b>3</b>	<b>Agente de microCLAUDIA</b>	<b>9</b>
3.1	Versión 1.x.x . . . . .	9
3.2	Versión 2.x.x . . . . .	10
3.2.1	Migración 1.x.x a 2.x.x . . . . .	11
3.3	Postinstalación . . . . .	12
<b>4</b>	<b>Acceso al panel central de microCLAUDIA</b>	<b>13</b>
4.1	Registro . . . . .	14
4.2	Secciones . . . . .	14
4.2.1	Interfaz para usuarios que tienen varios organismos. . . . .	14
4.2.2	Interfaz para usuarios que tienen un único organismo. . . . .	15
4.3	Listados . . . . .	16
4.4	Cuadro de Mando . . . . .	16
4.5	Organismos . . . . .	18
4.6	Equipos de un organismo . . . . .	18
4.6.1	Eliminar equipos . . . . .	24
4.6.2	Desinstalar de todos los equipos . . . . .	24
4.6.3	Activar selección . . . . .	24
4.7	Vacunas . . . . .	25
4.7.1	Tipos de vacunas . . . . .	25
4.7.2	Vacunación de equipos . . . . .	26
4.7.3	Vacunas con posibles reacciones adversas . . . . .	28
4.8	Alertas . . . . .	30
4.8.1	Activar selección . . . . .	30
4.9	Noticias . . . . .	32
4.10	Descarga de listados en formato CSV . . . . .	33
4.11	Buscador . . . . .	34
<b>5</b>	<b>POC</b>	<b>35</b>

<b>6</b>	<b>ANEXO. PREGUNTAS MÁS FRECUENTES</b>	<b>36</b>
<b>7</b>	<b>Despliegue y/o actualización por GPO</b>	<b>38</b>
7.1	Versión 1.x.x . . . . .	38
7.2	Versión 2.x.x . . . . .	44
7.2.1	Otras configuraciones de la GPO . . . . .	49

Edita:



© Centro Criptológico Nacional, 2023

Fecha de Edición: Septiembre de 2023

**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.



## 1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación 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.

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, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

## 2. INTRODUCCIÓN

### 2.1. ¿Qué es el ransomware?

El Ransomware (o malware de rescate), es un tipo de código dañino que tiene como objetivo bloquear el acceso a un equipo o a sus archivos (generalmente mediante el cifrado de estos), para posteriormente exigir el pago de un rescate para poder recuperar la información secuestrada.

### 2.2. ¿Cómo infecta el ransomware?

Para prevenir las infecciones, lo más conveniente es conocer el medio de entrada de la amenaza, así como sus mecanismos de propagación. Sin embargo, tras una infección, no siempre es posible determinar con exactitud cuál ha sido el origen o las causas de la infección. Los mecanismos y posibilidades para que la infección se produzca son variados, siendo importante conocer los vectores de infección más comunes. En algunos casos, el código dañino puede permanecer latente en el sistema durante cierto tiempo y manifestarse a raíz de una acción concreta o determinación de una fecha específica, lo cual hace difícil esclarecer con exactitud el momento de la infección<sup>1</sup>.

Aunque el método de infección más habitual es mediante phishing con un adjunto dañino, existen también otros métodos utilizados para llevar a cabo la infección mediante malware de este tipo:

- Mediante la visita a una web dañina
- A través de ataques por RDP
- Ataques sin interacción del usuario
- Por medio de otro malware

Puede ampliar esta información consultando el Informe de Buenas Prácticas CCN-CERT BP/04 sobre Ransomware.

### 2.3. ¿Qué es microCLAUDIA?

Basado en el motor de CLAUDIA, es el centro de vacunación del CCN-CERT que proporciona protección contra malware de tipo ransomware a sistemas Windows™ mediante la instalación de un agente ligero que despliega vacunas en el equipo.

Se compone de un agente que se instala en los equipos Windows™ del organismo, y una interfaz web desde dónde se pueden gestionar las vacunas de los equipos donde está instalado microCLAUDIA.

---

<sup>1</sup><https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2088-ccn-cert-bp-04-ransomware/file.html>



## 2.4. ¿Qué es una vacuna?

Se denomina vacuna a un mecanismo que impide que el malware se ejecute en un equipo. A diferencia de un antivirus o EDR, en donde la detección se realiza tras la ejecución de alguna acción por parte del malware, lo que se persigue con microCLAUDIA es evitar que éste ni siquiera llegue a ejecutarse en el equipo.

En estos momentos microCLAUDIA tiene varios tipos de vacunas:

- Las de tipo mutex, para hacer creer a un ransomware que ya se está ejecutando en un equipo.
- Las de tipo fichero, en las que se crea un fichero que hace creer al ransomware que se está ejecutando en un entorno de análisis de malware, para evitar su ejecución.
- Las que evitan que un proceso se ejecute. Por ejemplo, la ejecución de powershell desde un documento ofimático, típicamente utilizado en campañas de phishing por multitud de malware.

### 3. Agente de microCLAUDIA

Para instalar la herramienta hace falta el software de instalación y una clave de activación, única por organismo. Esta clave puede obtenerse mediante solicitud al correo electrónico **microclaudia@ccn-cert.cni.es**

Tras la validación de la solicitud, se facilitan las instrucciones de descarga e instalación de microCLAUDIA en los equipos Windows™ de la organización.

La forma de instalación difiere entre las versiones 1.x.x y 2.x.x utilizándose en las primeras un ejecutable “.exe” y en las segundas un instalador “.msi”.

#### 3.1. Versión 1.x.x

El agente puede instalarse en modo atendido, ejecutando directamente el instalador, y siguiendo los pasos para la instalación de software, introduciendo la clave de activación proporcionada y los datos del proxy, en caso de ser necesarios o también puede realizarse la instalación mediante línea de comandos, proporcionando los mismos datos que en el instalador:

```
microclaudia-setup.exe /apikey=<su_apikey> /server=<serverCentral_vacunas>  
↪ /tags=<tag1,tag2> /proxyhost=<dominio_o_ip_del_proxy>  
↪ /proxyport=<puerto_del_proxy> /verysilent
```

Por ejemplo, sin proxy:

```
microclaudia-setup.exe /apikey=7c832b57e9a1c8111c972db7f1d9df8d  
↪ /server=<dominio_microclaudia> /verysilent
```

Por ejemplo, con proxy:

```
microclaudia-setup.exe /apikey=7c832b57e9a1c8111c972db7f1d9df8d  
↪ /server=<dominio_microclaudia> /proxyhost=10.120.10.128 /proxyport=3128  
↪ /verysilent
```

Por ejemplo, con etiquetas:

```
microclaudia-setup.exe /apikey=7c832b57e9a1c8111c972db7f1d9df8d  
↪ /server=<dominio_microclaudia> /tags=tag1,tag2 /proxyhost=10.120.10.128  
↪ /proxyport=3128 /verysilent
```

### 3.2. Versión 2.x.x

Al igual que la versión anterior, el agente puede instalarse directamente utilizando el instalador, siendo los parámetros similares aunque se introduce uno nuevo que indica el tipo de instalación:

**Figura 1:** Ventana de instalación de microclaudia

- **Vdi:** Para instancias de escritorios virtuales de trabajo.
- **Golden:** Para plantillas usadas para la maquetación de equipos en la organización.
- **Offline:** Equipos aislados de la red.
- **Normal:** Para el resto de instalaciones.

Para su instalación de forma desatendida habrá que hacer uso del ejecutable “msiexec.exe” que viene con todas las versiones de Windows.

```
Start-Process C:\Windows\System32\msiexec.exe -ArgumentList "/i
↳  `\"microclaudia-x86_64.msi`\" API_KEY=7c832b57e9a1c8111c972db7f1d9df8d
↳  SERVER=microclaudia.dominio.com AGENT_MODE=Normal DEBUG=False
↳  TAGS=tag1,tag2,tag3 PROXY=servidor.proxy.com:3128 /qn\" -Wait
```

Además de los parámetros propios que se le pueden pasar al propio programa de Windows Installer, se necesitan los propios de microclaudia:

- **API\_KEY**: Clave de la organización.
- **SERVER**: Servidor de microclaudia. Formato: “subdominio.dominio.com”. No se debe incluir en ningún caso el esquema de conexión (http/https).
- **AGENT\_MODE** (Opcional): Modo de instalación: Vdi/Golden/Offline/Normal. Por defecto Normal.
- **TAGS** (Opcional): Listado de tags separados por comas. Ejemplo: dc,servidor,critical
- **PROXY** (Opcional): Proxy de comunicaciones. Formato: “subdominio.dominio:puerto” o “ip:puerto”, siendo el puerto opcional.
- **DEBUG** (Opcional): Iniciar el agente con el log level a debug: True/False. Por defecto el modo debug está desactivado.

La principal variación del agente con respecto a anteriores versiones es la recogida de información de la placa base del equipo, que en el caso de sistemas VDI permite identificar si una máquina se ha instanciado a partir de otra o es la original.

### Otros ejemplos de instalación:

Si la instalación falla, se le puede indicar a Windows Installer que genere un archivo de logs con el motivo del fallo:

```
Start-Process C:\Windows\System32\msiexec.exe -ArgumentList "/l*v
↳  install.log /i `\"microclaudia-x86_64.msi`\"
↳  API_KEY=7c832b57e9a1c8111c972db7f1d9df8d
↳  SERVER=microclaudia.dominio.com AGENT_MODE=Normal DEBUG=False
↳  TAGS=tag1,tag2,tag3 PROXY=servidor.proxy.com:3128 /qn\" -Wait
```

#### 3.2.1. Migración 1.x.x a 2.x.x

La migración de equipos se irá haciendo progresivamente hacia la versión 2.x.x, no obstante se puede hacer uso del ejecutable “microclaudia-updater.exe” para que se encargue de esta migración. Solo se necesita ejecutar con permisos de administración y no hace uso de ningún parámetro de entrada.

### 3.3. Postinstalación

Una vez instalado, aparecerá un icono en la barra de acciones del sistema que confirma que la herramienta ha sido instalada correctamente.

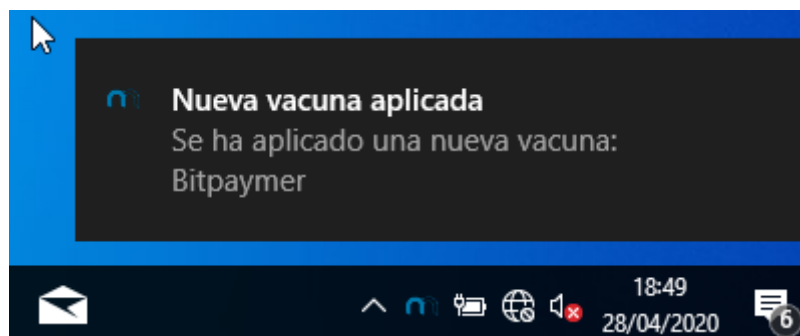


**Figura 2:** Icono de Microclaudia

La herramienta se comunica periódicamente en intervalos aleatorios configurables con el servidor central de vacunas:

**`https://<dominio_microclaudia>`**

Desde donde se descarga las vacunas que estén asignadas al equipo, notificando dicha descarga en el panel de notificaciones, siempre y cuando el organismo tenga habilitada la opción **Notificar a los agentes**.



**Figura 3:** Panel de notificaciones

La primera vez que el agente se comunica con el servidor central de vacunas, se registra la información del usuario que realiza la acción. Si se hace de forma desatendida, no se recoge información del usuario. En las siguientes comunicaciones que se realizan en intervalos aleatorios, el agente envía la información del equipo y del usuario logado. Si hay usuario logado cuando conecta, se sobrescribe el usuario, sino se deja vacío.

## 4. Acceso al panel central de microCLAUDIA

El acceso al panel central se realiza mediante navegador, accediendo al siguiente website:

**`https://<dominio_microclaudia>`**

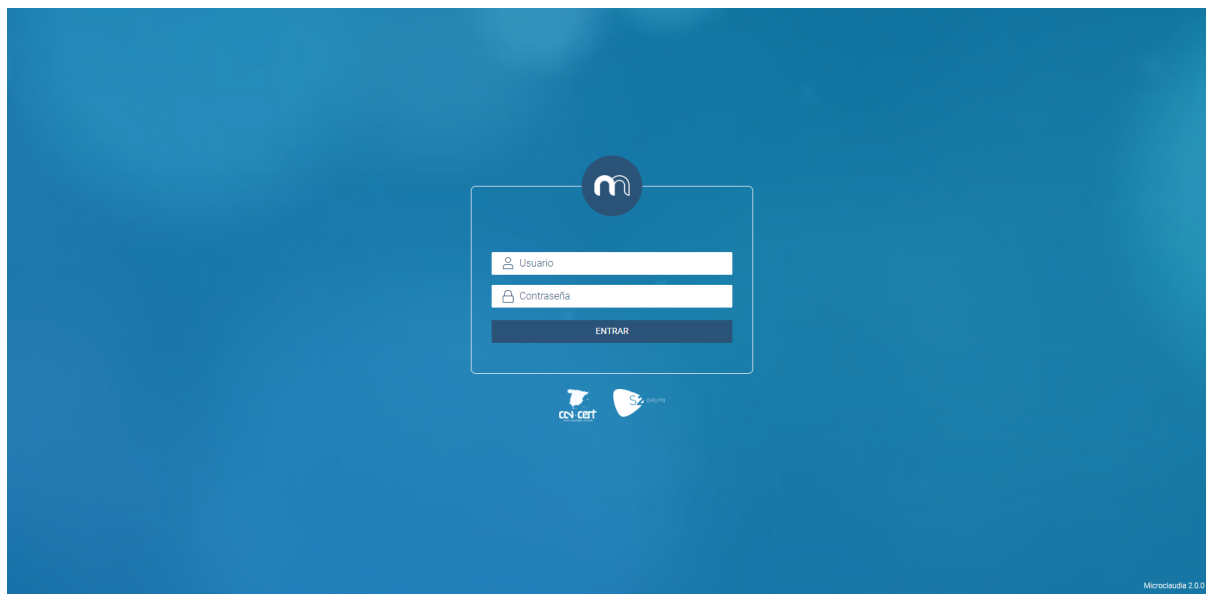


**Figura 4:** Pantalla de presentación

En la pantalla de presentación se muestra un resumen sobre la herramienta, la descarga de un documento de FAQ con las dudas más repetidas, y el acceso a la plataforma.

Para acceder al panel central se deberá pulsar sobre ACCEDER, tras lo cual, se nos redirigirá a la siguiente pantalla, en la que se deberán introducir el nombre de usuario y la contraseña de acceso con el fin de validar la identidad de la persona que desea autenticarse en el sistema.

Una vez que un usuario se ha identificado correctamente, se accederá automáticamente a la pantalla principal de microCLAUDIA, formada por un menú de opciones y un escritorio.



**Figura 5:** Pantalla de acceso





#### 4.1. Registro

El registro en la aplicación se realiza mediante solicitud a la cuenta de correo electrónico: **microclaudia@ccn-cert.cni.es**





#### 4.2. Secciones

La interfaz de usuario presenta un aspecto distinto si el usuario pertenece a varios organismos o a un único organismo





##### 4.2.1. Interfaz para usuarios que tienen varios organismos.

-  Un cuadro de mando que proporciona una vista general de los organismos.
-  La pantalla de sectores/organismos que permite acceder a los organismos gestionados por el usuario.
-  La pantalla de alertas provenientes de los agentes.
-  La pantalla de noticias de la herramienta.

#### 4.2.2. Interfaz para usuarios que tienen un único organismo.

-  Un cuadro de mando que proporciona una vista general de los organismos.
-  La pantalla del organismo del usuario.
-  La pantalla de alertas provenientes de los agentes.
-  La pantalla de noticias de la herramienta.

Además, desde la parte inferior izquierda se pueden realizar las siguientes acciones:

-  Activar/desactivar notificaciones y cambio de contraseña del usuario.
-  Preguntas frecuentes.
-  Descargar este manual.
-  Cerrar la sesión.

Al activar las notificaciones de usuario, éste recibirá por correo electrónico las alertas asociadas a los equipos de sus organismos.



### 4.3. Listados

En todos los listados de datos se **permite almacenar el tamaño de página por usuario** a la hora de mostrar el número de registros por página.

# Alertas

¿Qué alerta estás buscando?

Alertas (10615) ↑

Borrado de logs con wevutil • EQUIPO1

Advanced Port Scanner • EQUIPO2

Advanced Port Scanner • EQUIPO3

Advanced Port Scanner • EQUIPO4

Borrado de logs con wevutil • EQUIPO5

ARYUKHASH • EQUIPO6

ARYUKHASH • EQUIPO7

ARYUKHASH • EQUIPO8

ARYUKHASH • EQUIPO9

ARYUKHASH • EQUIPO10

ARYUKHASH • EQUIPO11

ARYUKHASH • EQUIPO12

ARYUKHASH • EQUIPO13

ARYUKHASH • EQUIPO14

ARYUKHASH • EQUIPO15

ARYUKHASH • EQUIPO16

ARYUKHASH • EQUIPO17

ARYUKHASH • EQUIPO18

ARYUKHASH • EQUIPO19

ARYUKHASH • EQUIPO20

Mensaje ↑

Fecha ↑

Alerta de proceso: executable\_path=C:\Users\aaaa\AppData\Local\T...

Se ha terminado el proceso executable\_path=C:\Users\aaaa\AppData...

Could not kill process: <\_xmli: Unexpected COM Error (-2147352567, '...

Se ha terminado el proceso executable\_path=C:\Users\aaaa\AppData...

Alerta de proceso: executable\_path=C:\Users\aaaa\AppData\Local\T...

Alerta de proceso: executable\_path=C:\Windows\System32\Runtime...

Alerta de proceso: executable\_path=C:\Windows\System32\Runtime...

Alerta de proceso: executable\_path=C:\Windows\System32\Runtime...

Alerta de proceso: executable\_path=C:\Program Files\WindowsApps\...

Alerta de proceso: executable\_path=C:\Windows\system32\backgrou...

Alerta de proceso: executable\_path=C:\Windows\system32\backgrou...

Alerta de proceso: executable\_path=C:\Windows\system32\backgrou...

Alerta de proceso: executable\_path=C:\Program Files (x86)\Microsoft...

Alerta de proceso: executable\_path=unknown command\_line=unkno...

Alerta de proceso: executable\_path=C:\Windows\System32\mouseco...

Alerta de proceso: executable\_path=C:\Program Files (x86)\Microsoft...

Alerta de proceso: executable\_path=C:\Windows\System32\Runtime...

Alerta de proceso: executable\_path=C:\Program Files (x86)\Microsoft...

Alerta de proceso: executable\_path=C:\Windows\System32\svchost...

12345...531

mostrar 20

Figura 6: Listado

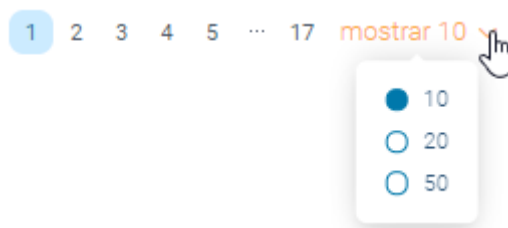
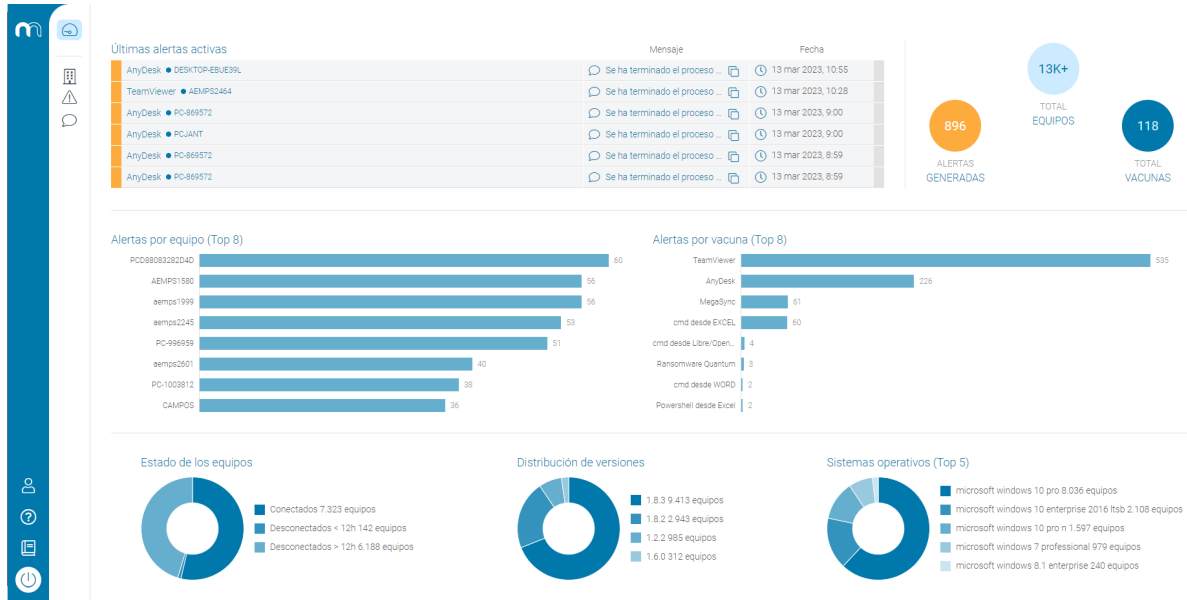


Figura 7: Configuración del tamaño de página

### 4.4. Cuadro de Mando

La sección de **Cuadro de mando** muestra un resumen del estado del organismo. En ella se pueden consultar las últimas 4 noticias, las seis últimas alertas que se han generado y las estadísticas generales del despliegue (alertas generadas, equipos donde está instalado microCLAUDIA y vacunas desplegadas en el sistema). En la parte inferior, se muestran unas gráficas con los ocho equipos que más alertas generan, así como las ocho alertas que se dan con más frecuencia. Por último se muestran también 3

gráficas con los estados de conexión de los equipos, las diferentes versiones de agentes y los diferentes sistemas operativos.

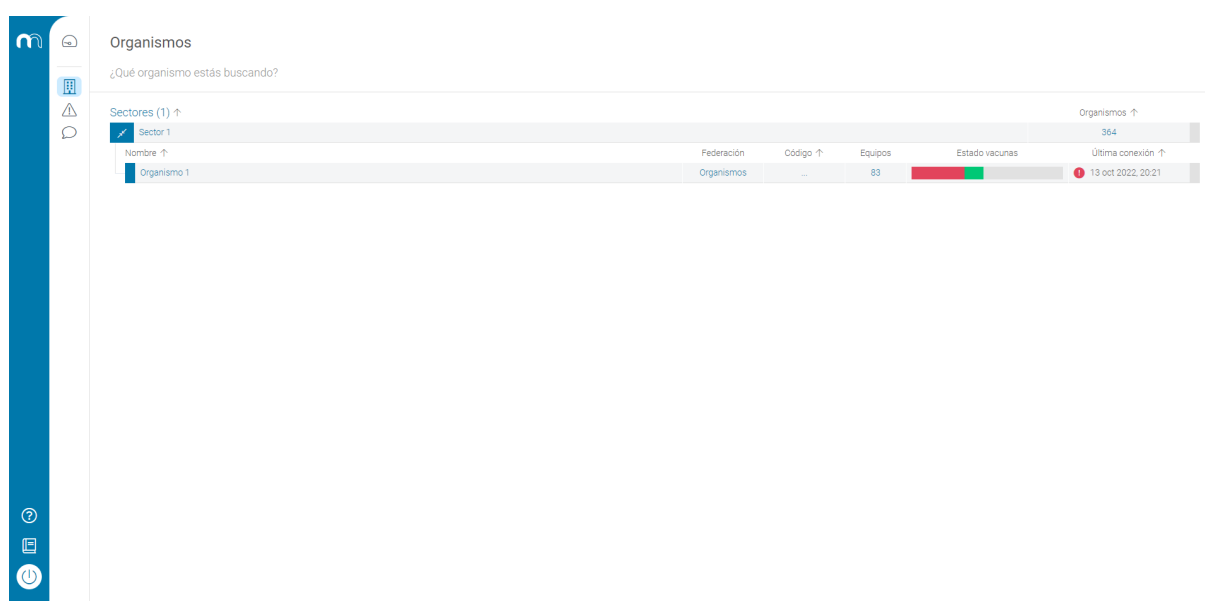


**Figura 8:** Cuadro de mandos

## 4.5. Organismos

Los usuarios con más de un organismo accederán a la sección de organismos pulsando en el icono de organismos en la barra lateral. Accederemos así a la página que muestra los sectores de los que tiene visibilidad nuestro usuario y desplegaremos para acceder al organismo del que deseamos mostrar su información. Para acceder a las diferentes secciones del organismo (Equipos, Vacunas) nos situaremos sobre la sección azul delante del nombre del organismo y aparecerá un ojo sobre el cuál podremos pulsar.

Los usuarios con un único organismo no tienen acceso a esta sección ya que pueden elegir su organismo desde la barra lateral de la izquierda.



**Figura 9:** Listado de sectores para usuarios con varios organismos

## 4.6. Equipos de un organismo

La sección de equipos de un organismo muestra un listado de los equipos donde se ha instalado la herramienta microCLAUDIA, así como su estado de vacunación.

Equipos

¿Qué equipos estás buscando?

ORGANISMO 1

Equipos (83) ↑	Dirección IP	Sistema operativo ↑	Agente ↑	Aplicadas	Estado vacunas	Última conexión ↑
EQUIPO 1	10.240.217.118...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122		14 oct 2022, 11:04
EQUIPO 2	10.240.254.57...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122		14 oct 2022, 4:59
EQUIPO 3	10.240.216.109...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122		14 oct 2022, 11:10
EQUIPO 4	192.168.6.13...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122		14 oct 2022, 11:14
EQUIPO 5	10.240.214.93...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122		14 oct 2022, 10:15
EQUIPO 6	10.240.217.82...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122		14 oct 2022, 10:22
EQUIPO 7	10.240.217.198...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122		14 oct 2022, 9:38
EQUIPO 8	10.240.217.199...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122		14 oct 2022, 9:35
EQUIPO 9	10.240.217.28...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122		14 oct 2022, 11:16
EQUIPO 10	10.240.216.50...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122		14 oct 2022, 9:22
EQUIPO 11	10.240.216.51...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122		14 oct 2022, 6:24
EQUIPO 12	10.240.207.67...	Microsoft Windows Server 2008 ..	1.8.2	0 / 122		14 oct 2022, 11:31
EQUIPO 13	10.240.207.68...	Microsoft Windows Server 2008 ..	1.8.2	0 / 122		14 oct 2022, 10:04
EQUIPO 14	10.240.216.222...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122		14 oct 2022, 9:21
EQUIPO 15	10.240.216.223...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122		14 oct 2022, 11:03
EQUIPO 16	10.240.218.43...	Microsoft Windows Server 2008 ..	1.8.2	0 / 122		14 oct 2022, 9:31
EQUIPO 17	10.240.234.19...	Microsoft Windows Server 2008 ..	1.8.2	0 / 122		14 oct 2022, 7:06
EQUIPO 18	192.168.6.168...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122		14 oct 2022, 8:12
EQUIPO 19	10.240.234.135...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122		14 oct 2022, 9:57
EQUIPO 20	10.240.234.35...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122		14 oct 2022, 11:02

1 2 3 4 5 mostrar 20

**Figura 10:** Listado de equipos para usuarios con un único organismo

En la tabla de equipos se muestra el nombre de éste, la IP o IPs asociadas al equipo, el sistema operativo que tiene **instalado**, la versión del agente, la cantidad de vacunas que se le han aplicado, el estado de sus vacunas y un icono que advierte del tiempo de inactividad de los equipos.

Existen tres tipos de estado diferentes, representados por los siguientes iconos:



Hace menos de doce horas que el equipo ha notificado que está activo.



Hace entre doce horas y un día que el equipo se ha comunicado con el servidor de microCLAUDIA.



Hace más de un día que el equipo no se comunica con el servidor de microCLAUDIA.

Es posible obtener información más detallada sobre las vacunas aplicadas al equipo en cuestión pulsando sobre el desplegable situado junto al nombre de cada equipo.

En esta nueva vista se muestra el nombre de la vacuna, el tipo, el estado y la fecha en la que fue lanzada dicha vacuna.

Los equipos pueden ser etiquetados desde el panel de edición. Para abrir dicho panel se deberá pulsar en el icono del lápiz del equipo seleccionado. Desde dicho panel será posible excluir o incluir las etiquetas deseadas o incluso crear nuevas etiquetas.

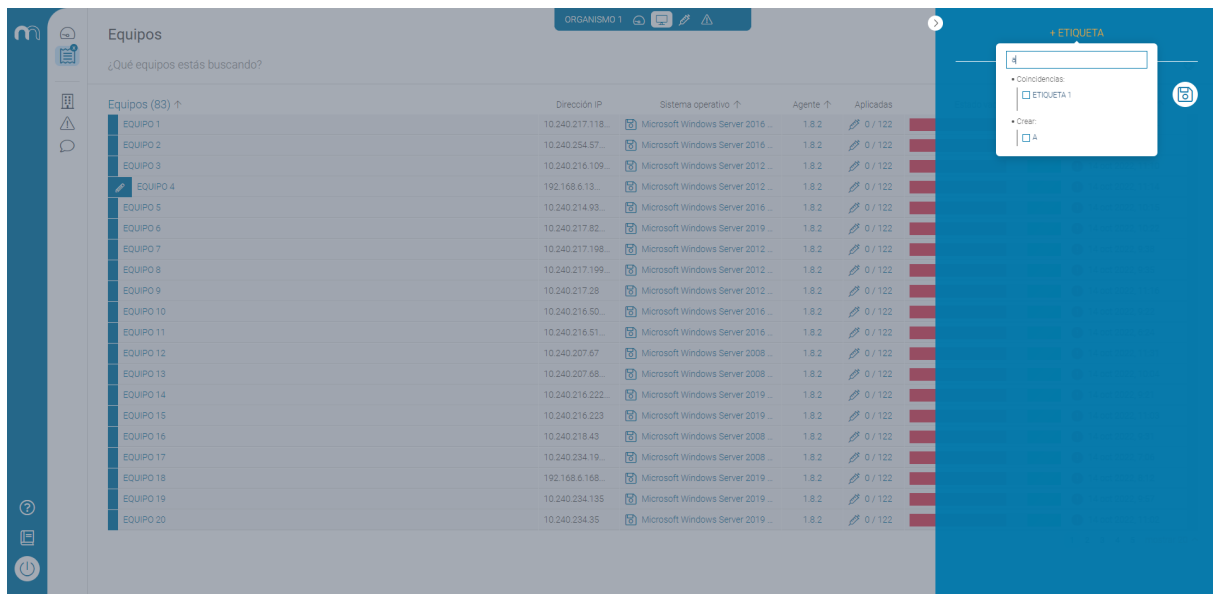


Figura 11: Asignar etiquetas

Una vez que alguno de los equipos haya sido etiquetado con una o más etiquetas, será posible filtrar el listado de equipos por etiquetas. Para desplegar el menú se deberá pulsar en el icono etiquetas. Una vez abierto dicho menú se podrán seleccionar las etiquetas deseadas.

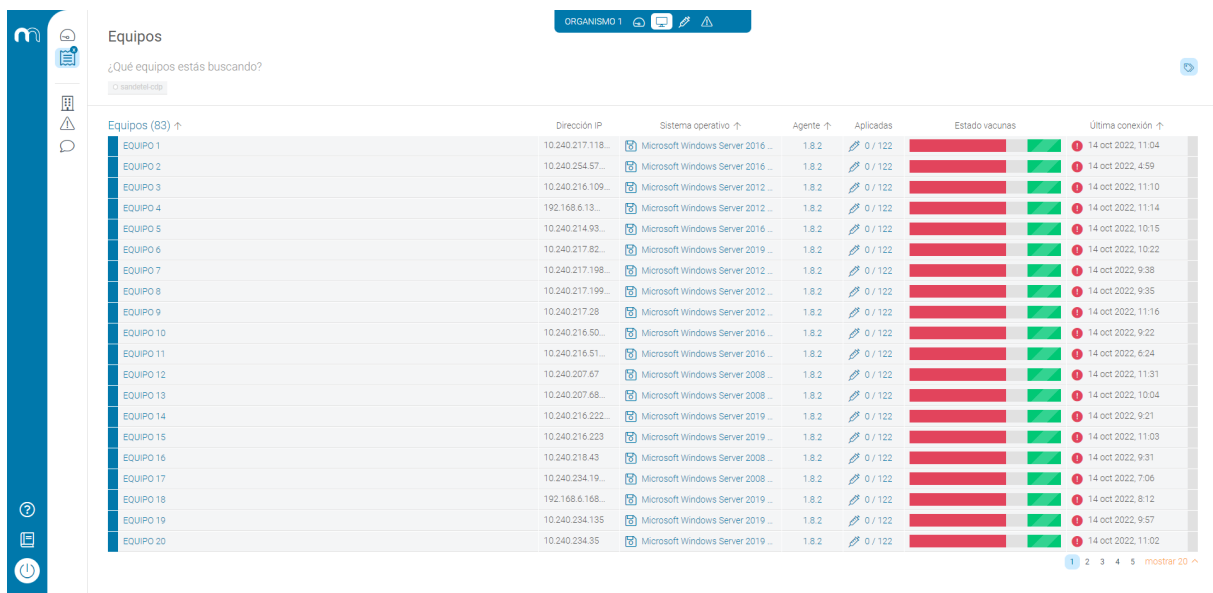
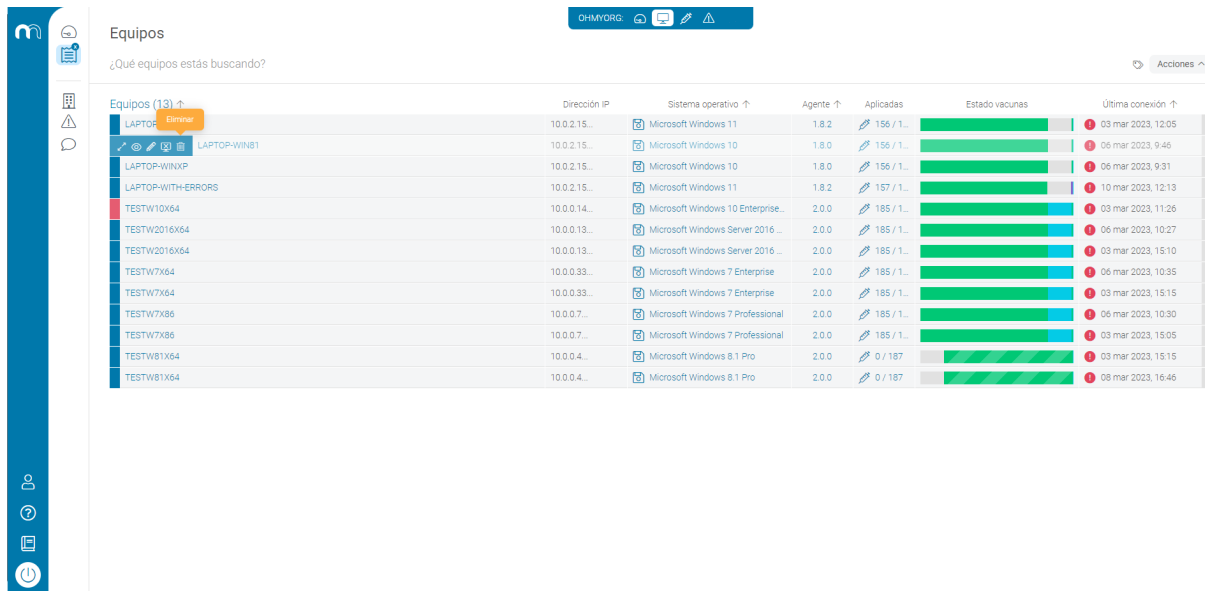


Figura 12: Listado con etiquetas

Si se desea **eliminar** alguno de los equipos de nuestra organización del centro de vacunación, se

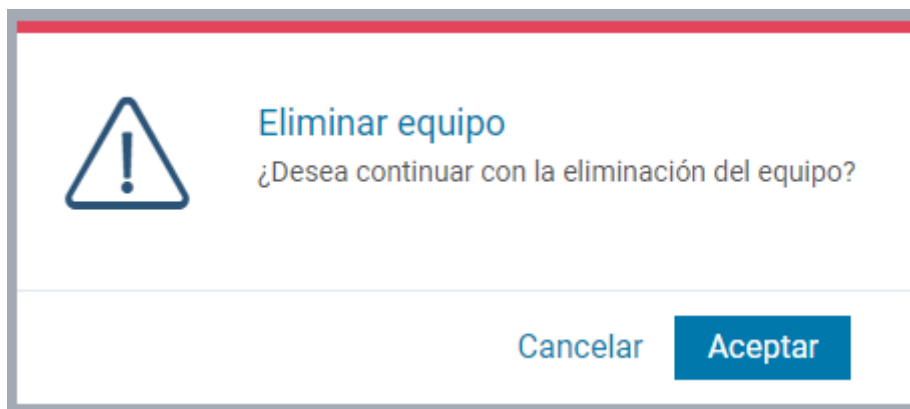
deberá pulsar sobre la papelera del equipo en cuestión. **Esta acción no desinstala el agente de microClaudia.**



Equipos (13) ↑	Dirección IP	Sistema operativo ↑	Agente ↑	Aplicadas	Estado vacunas	Última conexión ↑
LAPTOP-WIN81	10.0.2.15...	Microsoft Windows 11	1.8.2	156 / 1...		03 mar 2023, 12:05
LAPTOP-WIN81	10.0.2.15...	Microsoft Windows 10	1.8.0	156 / 1...		06 mar 2023, 9:46
LAPTOP-WINXP	10.0.2.15...	Microsoft Windows 10	1.8.0	156 / 1...		06 mar 2023, 9:31
LAPTOP-WITH-ERRORS	10.0.2.15...	Microsoft Windows 11	1.8.2	157 / 1...		10 mar 2023, 12:13
TESTW10X64	10.0.0.14...	Microsoft Windows 10 Enterprise...	2.0.0	185 / 1...		03 mar 2023, 11:26
TESTW2016X64	10.0.0.13...	Microsoft Windows Server 2016...	2.0.0	185 / 1...		06 mar 2023, 10:27
TESTW2016X64	10.0.0.13...	Microsoft Windows Server 2016...	2.0.0	185 / 1...		03 mar 2023, 15:10
TESTW7X64	10.0.0.33...	Microsoft Windows 7 Enterprise	2.0.0	185 / 1...		06 mar 2023, 10:35
TESTW7X64	10.0.0.33...	Microsoft Windows 7 Enterprise	2.0.0	185 / 1...		03 mar 2023, 15:15
TESTW7X86	10.0.0.7...	Microsoft Windows 7 Professional	2.0.0	185 / 1...		06 mar 2023, 10:30
TESTW7X86	10.0.0.7...	Microsoft Windows 7 Professional	2.0.0	185 / 1...		03 mar 2023, 15:05
TESTW81X64	10.0.0.4...	Microsoft Windows 8.1 Pro	2.0.0	0 / 187		03 mar 2023, 15:15
TESTW81X64	10.0.0.4...	Microsoft Windows 8.1 Pro	2.0.0	0 / 187		08 mar 2023, 16:46

**Figura 13:** Eliminar equipo

A continuación, aparecerá una ventana de confirmación.



**Figura 14:** Confirmación de eliminación de un equipo

Para indicar en el equipo, que **se desinstale el agente de microClaudia (a partir de la versión 1.8.0)**, se deberá hacer clic sobre el siguiente icono:

Equipos

¿Qué equipos estás buscando?

Acciones

Equipos (12) ↑	Dirección IP	Sistema operativo ↑	Agente ↑	Aplicadas	Estado vacunas	Última conexión ↑
LAPTOP-WIN11	10.0.2.15...	Microsoft Windows 11	1.8.2	156 / 1...		03 mar 2023, 12:05
Desinstalar Microclaudia en este equipo	10.0.2.15...	Microsoft Windows 10	1.8.0	156 / 1...		06 mar 2023, 9:31
LAPTOP-WITH-ERRORS	10.0.2.15...	Microsoft Windows 11	1.8.2	157 / 1...		10 mar 2023, 12:13
TESTW10X64	10.0.0.14...	Microsoft Windows 10 Enterprise...	2.0.0	185 / 1...		03 mar 2023, 11:26
TESTW2016X64	10.0.0.13...	Microsoft Windows Server 2016 ...	2.0.0	185 / 1...		06 mar 2023, 10:27
TESTW2016X64	10.0.0.13...	Microsoft Windows Server 2016 ...	2.0.0	185 / 1...		03 mar 2023, 15:10
TESTW7X64	10.0.0.33...	Microsoft Windows 7 Enterprise	2.0.0	185 / 1...		06 mar 2023, 10:35
TESTW7X64	10.0.0.33...	Microsoft Windows 7 Enterprise	2.0.0	185 / 1...		03 mar 2023, 15:15
TESTW7X86	10.0.0.7...	Microsoft Windows 7 Professional	2.0.0	185 / 1...		06 mar 2023, 10:30
TESTW7X86	10.0.0.7...	Microsoft Windows 7 Professional	2.0.0	185 / 1...		03 mar 2023, 15:05
TESTW81X64	10.0.0.4...	Microsoft Windows 8.1 Pro	2.0.0	0 / 187		03 mar 2023, 15:15
TESTW81X64	10.0.0.4...	Microsoft Windows 8.1 Pro	2.0.0	0 / 187		08 mar 2023, 16:46

Figura 15: Desinstalar agente

A continuación, aparecerá una ventana de confirmación.

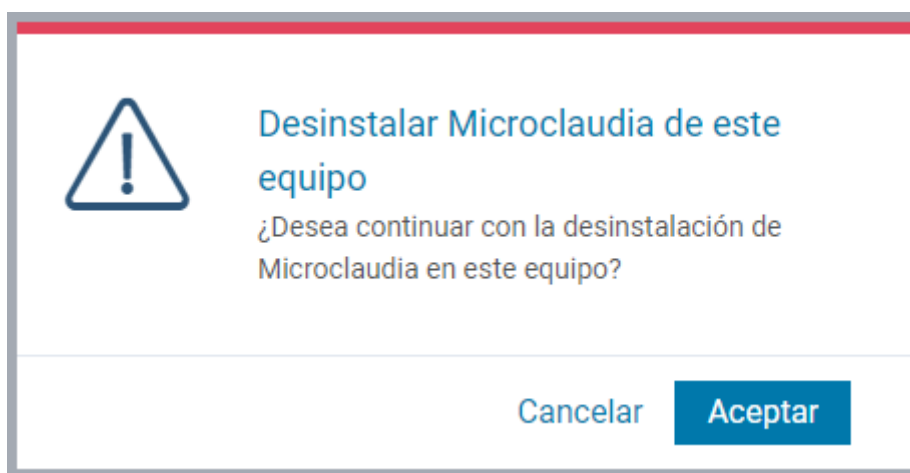


Figura 16: Confirmación de desinstalación de un agente

Automáticamente, la fila del equipo aparecerá en rojo indicando que no puede realizarse ninguna acción sobre el mismo. Cuando el agente microClaudia (*a partir de la versión 1.8.0*) se desinstale de dicho equipo, el mismo no aparecerá en la interfaz web y se habrá eliminado de nuestra organización del centro de vacunación.

Si se desea **ver la información del equipo**, se deberá pulsar sobre la lupa del equipo en cuestión. Y aparecerá dicha información en el panel de la derecha:

**Equipos**

¿Qué equipos estás buscando?

Equipos (83) ↑

	Dirección IP	Sistema operativo ↑	Agente ↑	Aplicadas
EQUIPO 1	10.240.217.118...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122
EQUIPO 2	10.240.254.57...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122
EQUIPO 3	10.240.216.109...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122
EQUIPO 4	192.168.6.13...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122
EQUIPO 5	10.240.214.93...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122
EQUIPO 6	10.240.217.82...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122
EQUIPO 7	10.240.217.198...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122
EQUIPO 8	10.240.217.199...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122
EQUIPO 9	10.240.217.28...	Microsoft Windows Server 2012 ..	1.8.2	0 / 122
EQUIPO 10	10.240.216.50...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122
EQUIPO 11	10.240.216.51...	Microsoft Windows Server 2016 ..	1.8.2	0 / 122
EQUIPO 12	10.240.207.67...	Microsoft Windows Server 2008 ..	1.8.2	0 / 122
EQUIPO 13	10.240.207.68...	Microsoft Windows Server 2008 ..	1.8.2	0 / 122
EQUIPO 14	10.240.216.222...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122
EQUIPO 15	10.240.216.223...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122
EQUIPO 16	10.240.218.43...	Microsoft Windows Server 2008 ..	1.8.2	0 / 122
EQUIPO 17	10.240.234.19...	Microsoft Windows Server 2008 ..	1.8.2	0 / 122
EQUIPO 18	192.168.6.168...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122
EQUIPO 19	10.240.234.135...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122
EQUIPO 20	10.240.234.35...	Microsoft Windows Server 2019 ..	1.8.2	0 / 122

**EQUIPO 7**  
Versión: 1.8.2  
4 GB

**Interfaces**

Dirección MAC: 00:50:56:98:30:7E  
Descripción: Conexión de red Gigabit Intel(R) 8257...  
Direcciones IP: 10.240.217.198

Dirección MAC: 00:50:56:98:58:25  
Descripción: Conexión de red Gigabit Intel(R) 8257...  
Direcciones IP: 192.168.7.65

**CPU**

Núcleo: 1  
Nombre: AMD Opteron(tm) Processor 6366 HE

Núcleo: 1  
Nombre: AMD Opteron(tm) Processor 6366 HE

**Discos**

Tamaño: 60 GB  
Etiqueta: VMware Virtual disk SCSI Disk Device

**Discos lógicos**

Tamaño: 0 Bytes  
Etiqueta: A:

Tamaño: 59.66 GB  
Etiqueta: C:

**Figura 17:** Información de un equipo

Desde un equipo podemos aplicar (presionando en el icono de “play”) o parar (presionando en icono de “stop”) una vacuna. (Ver apartado **Vacunación de Equipos**)

**EQUIPO 3**  
10.240.216.109... Microsoft Windows Server 2012 ... 1.8.2 0 / 122 14 oct 2022, 11:10

Vacunas (122)

	Tipo	Estado	Vacunación
Vacuna 1	vssprotect	✓	...
Vacuna 2	procomon	✓	...
Vacuna 3	file	✓	...
Vacuna 4	registry	✓	...
Vacuna 5	evento	✓	...
Vacuna 6	procomon	✓	...
Vacuna 7	mutex	✓	...
Vacuna 8	procomon	✓	...
Vacuna 9	mutex	✓	...
Vacuna 10	mutex	✓	...

**Figura 18:** Aplicar vacuna

**EQUIPO 3**  
10.240.216.109... Microsoft Windows Server 2012 ... 1.8.2 0 / 122 14 oct 2022, 11:10

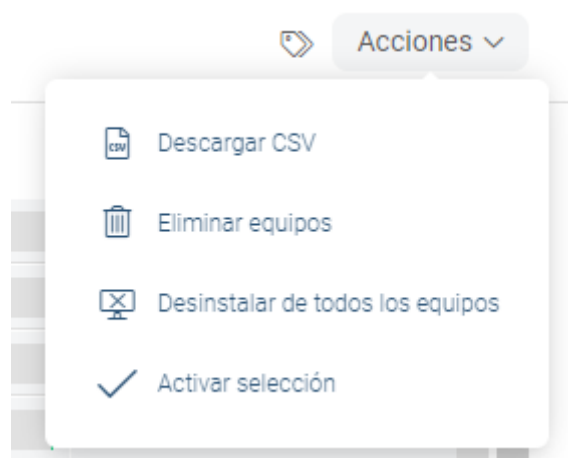
Vacunas (122)

	Tipo	Estado	Vacunación
Vacuna 1	vssprotect	✓	...
Vacuna 2	procomon	✓	...
Vacuna 3	file	✓	...
Vacuna 4	registry	✓	...
Vacuna 5	evento	✓	...
Vacuna 6	procomon	✓	...
Vacuna 7	mutex	✓	...
Vacuna 8	procomon	✓	...
Vacuna 9	mutex	✓	...
Vacuna 10	mutex	✓	...

**Figura 19:** Parar vacuna



Además, existen otras acciones disponibles para el listado de equipos, en la esquina superior derecha:



**Figura 20:** Acciones disponibles para el listado de equipos

#### 4.6.1. Eliminar equipos

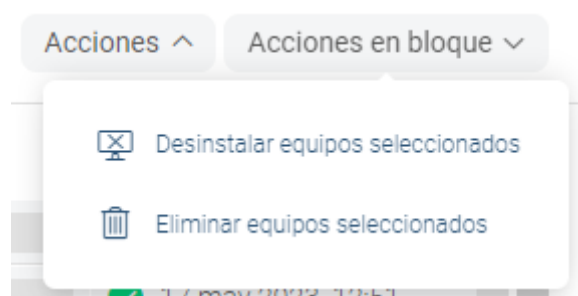
- Esta acción elimina TODOS los equipos del listado, al igual que la acción individual por cada equipo. Si los equipos posteriormente vuelven a sincronizar con el servidor de vacunas, éstos volverán a aparecer.

#### 4.6.2. Desinstalar de todos los equipos

- Esta acción marca TODOS los equipos del listado para su desinstalación, al igual que la acción individual por cada equipo.

#### 4.6.3. Activar selección

- Esta acción sirve para habilitar la selección múltiple de los diferentes equipos del listado y poder ejecutar acciones en bloque, sobre un conjunto concreto de equipos. Actualmente existen varias acciones de este tipo:



**Figura 21:** Acciones en bloque para el listado de equipos

#### 4.6.3.1. Desinstalar equipos seleccionados

- Desplegar el menú de acciones y seleccionar la opción **Activar selección**. Esta acción habilitará una cajita delante de los equipos para realizar la selección de aquellos sobre los que se desea realizar la acción.
- Tras realizar la selección de los equipos, se habilita un nuevo menú de acciones en bloque, y al pulsar sobre la acción **Desinstalar equipos seleccionados** se marcan para desinstalar los equipos seleccionados.

#### 4.6.3.2. Eliminar equipos seleccionados

- Desplegar el menú de acciones y seleccionar la opción **Activar selección**. Esta acción habilitará una cajita delante de los equipos para realizar la selección de aquellos sobre los que se desea realizar la acción.
- Tras realizar la selección de los equipos, se habilita un nuevo menú de acciones en bloque, y al pulsar sobre la acción **Eliminar equipos seleccionados** se eliminan del listado los equipos seleccionados.

### 4.7. Vacunas

La sección de vacunas muestra todas las vacunas existentes en la plataforma y permite lanzarlas en nuestro organismo.

#### 4.7.1. Tipos de vacunas

Existen varios tipos de vacunas desplegadas:

- **MUTEX:** la vacuna consiste en crear un *mutex* en la memoria del equipo para hacer creer al malware que ya se ha ejecutado.
- **FILE:** la vacuna crea un fichero en cierta ruta del equipo para hacer creer al malware que se está ejecutando en un entorno de análisis de malware.
- **PROCMON:** es la abreviación de “*process monitor*” o monitor de procesos. Permite establecer cuándo un proceso potencialmente dañino se va a ejecutar y lo para. Por ejemplo, si un documento Word™ trata de ejecutar un script de powershell.
- **VSSPROTECT:** protege de la eliminación de las “*shadow copies*” o puntos de restauración del sistema, por parte del malware.
- **PROCMON RYUK HASH y PROCMON RYUK TEXT:** ofrecen protección frente a variantes del ransomware Ryuk.
- **REGISTRY:** protección basada en la modificación del registro de Windows™.
- **EVENT:** crean objetos de tipo “*event*” en la memoria del equipo. Algunas familias de malware utilizan este tipo de objetos de Windows™ de forma similar a los mutex.

#### 4.7.2. Vacunación de equipos



Para vacunar un equipo accederemos a la sección vacunas del organismo. Disponemos de un listado con las vacunas disponibles.

Vacuna	Sistema operativo	Tipo	No aplicar/aplicar	Versión	Actualización	Válida hasta
Vacuna 1	microsoft windows xp	vssprotect	<input checked="" type="checkbox"/>	1.8.2	...	...
Vacuna 2	...	procmmon	<input checked="" type="checkbox"/>	1.8.2	...	...
Vacuna 3	...	file	<input checked="" type="checkbox"/>	1.8.2	...	...
Vacuna 4	...	registry	<input checked="" type="checkbox"/>	1.8.2	...	...
Vacuna 5	...	evento	<input checked="" type="checkbox"/>	1.8.2	...	...
Vacuna 6	...	procmmon	<input checked="" type="checkbox"/>	1.6.0	...	...
Vacuna 7	...	procmmon ryuk text	<input checked="" type="checkbox"/>	1.8.2	...	...
Vacuna 8	...	mutex	<input checked="" type="checkbox"/>	1.8.2	...	...
Vacuna 9	...	procmmon	<input checked="" type="checkbox"/>	1.4.0	...	...
Vacuna 10	...	mutex	<input checked="" type="checkbox"/>	1.4.0	...	...
Vacuna 11	...	mutex	<input checked="" type="checkbox"/>	1.0.0	...	...
Vacuna 12	...	file	<input checked="" type="checkbox"/>	1.0.4	...	...
Vacuna 13	...	procmmon	<input checked="" type="checkbox"/>	1.6.0	...	...
Vacuna 14	...	procmmon	<input checked="" type="checkbox"/>	1.4.0	...	...
Vacuna 15	...	procmmon	<input checked="" type="checkbox"/>	1.4.0	...	...
Vacuna 16	...	procmmon	<input checked="" type="checkbox"/>	1.0.4	...	...
Vacuna 17	...	procmmon	<input checked="" type="checkbox"/>	1.0.4	...	...
Vacuna 18	...	procmmon	<input checked="" type="checkbox"/>	1.0.4	...	...
Vacuna 19	...	procmmon	<input checked="" type="checkbox"/>	1.0.4	...	...
Vacuna 20	...	procmmon	<input checked="" type="checkbox"/>	1.0.4	...	...








**Figura 22:** Vacunación de equipos para usuarios con un único organismo

Si desplegamos una vacuna podremos ver un listado de equipos que nos muestra su estado de aplicación.

**Figura 23:** Vacunación: aplicación a equipos para usuarios con un único organismo

Podemos aplicar  o parar  una vacuna en un equipo concreto desde el área de acciones del equipo deseado.

Al realizar cualquiera de estas opciones cambiará el estado de la vacuna. A continuación se muestra el listado de los posibles estados.

-  Vacuna obligatoria y no aplicada.
-  Vacuna obligatoria y aplicada.
-  Vacuna no obligatoria y aplicada.
-  Vacuna no obligatoria y no aplicada.
-  Vacuna aplicada con error.
-  Vacuna obligatoria y pendiente de aplicación.
-  Vacuna no obligatoria y pendiente de aplicación.

Es posible realizar la acción inversa y aplicar o parar una vacuna en un equipo concreto. Para ello desde la vista equipos del organismo desplegaremos el equipo deseado y realizaremos la acción sobre un equipo. Los estados posibles son los mismos que en la opción anterior.

Los terminos “obligatorio” y “no obligatorio” se refieren a la recomendación por parte del CCN con respecto a la aplicación de vacunas concretas.

Las no obligatorias son recomendables de aplicar pero pueden afectar a organismos legítimos y se deja a decisión del organismo aplicarla o no.

En cuanto a los términos “no aplicada” y “pendiente de aplicación”, “no aplicada” significa que la vacuna no está aplicada mientras que “pendiente de aplicación” significa que está configurada para ser aplicada pero está pendiente de que el agente de Microclaudia contacte con el servidor para recibir la orden.

Equipos (83) ↑	Dirección IP	Sistema operativo ↑	Agente ↑	Aplicadas	Estado vacunas	Última conexión ↑
Equipo 1	10.240.217.118...	Microsoft Windows Server 2016 ...	1.8.2	0 / 123		14 oct 2022, 11:04
Vacunas (123)						
Vacuna 1					vssprotect	...
Vacuna 2					procomon	...
Vacuna 3					file	...
Vacuna 4					registry	...
Vacuna 5					evento	...
Vacuna 6					procomon	...
Vacuna 7					procomon ryuk text	...
Vacuna 8					mutex	...
Vacuna 9					procomon	...
Vacuna 10					mutex	...
Equipo 2	10.240.254.57...	Microsoft Windows Server 2016 ...	1.8.2	0 / 123		14 oct 2022, 4:59
Equipo 3	10.240.216.109...	Microsoft Windows Server 2012 ...	1.8.2	0 / 123		14 oct 2022, 11:10
Equipo 4	192.168.6.13...	Microsoft Windows Server 2012 ...	1.8.2	0 / 123		14 oct 2022, 11:14
Equipo 5	10.240.214.93...	Microsoft Windows Server 2016 ...	1.8.2	0 / 123		14 oct 2022, 10:15
Equipo 6	10.240.217.82...	Microsoft Windows Server 2019 ...	1.8.2	0 / 123		14 oct 2022, 10:22
Equipo 7	10.240.217.198...	Microsoft Windows Server 2012 ...	1.8.2	0 / 123		14 oct 2022, 9:38
Equipo 8	10.240.217.199...	Microsoft Windows Server 2012 ...	1.8.2	0 / 123		14 oct 2022, 9:35
Equipo 9	10.240.217.28...	Microsoft Windows Server 2012 ...	1.8.2	0 / 123		14 oct 2022, 11:16
Equipo 10	10.240.216.50...	Microsoft Windows Server 2016 ...	1.8.2	0 / 123		14 oct 2022, 11:16

**Figura 24:** Vacunación: aplicación de vacunas concretas a equipos para usuarios con un único organismo

#### 4.7.3. Vacunas con posibles reacciones adversas

Algunas vacunas pueden provocar reacciones adversas en los equipos, es por ello que, incluyen un mensaje informando al usuario de las acciones que estas vacunas pueden implicar, de modo que, el propio usuario pueda elegir asumir dichas reacciones adversas en la ejecución de esta vacuna.

Cuando se intente ejecutar una vacuna que tenga reacciones adversas, aparece un mensaje modal para confirmar su ejecución. Este mensaje informa con un aviso sobre las consecuencias que puede ocasionar ejecutar dicha vacuna, y da la opción de elegir entre continuar con la ejecución o cancelarla.

**Vacunas**

¿Qué vacuna estás buscando?

Vacunas (123) ↑

Sistema operativo ↑	Tipo ↑	No aplicar/aplicar	Versión ↑	Actualización ↑	Válida hasta ↑
microsoft windows xp	vssprotect	●	1.8.2	...	...

Equipos (83)

- Equipo 1
- Equipo 2
- Equipo 3
- Equipo 4
- Equipo 5
- Equipo 6
- Equipo 7
- Equipo 8
- Equipo 9
- Equipo 10

**Información de interés**

¿Desea continuar con la ejecución?

Puede generar problemas con las shadow copies

Cancelar Aceptar

Estado	Vacunación
✓	14 oct 2022, 11:04
✓	14 oct 2022, 4:59
✓	14 oct 2022, 11:10
✓	14 oct 2022, 11:14
✓	14 oct 2022, 10:15
✓	14 oct 2022, 10:22
✓	14 oct 2022, 9:38
✓	14 oct 2022, 9:35
✓	14 oct 2022, 11:16
✓	14 oct 2022, 9:22

1 2 3 4 5 - 9

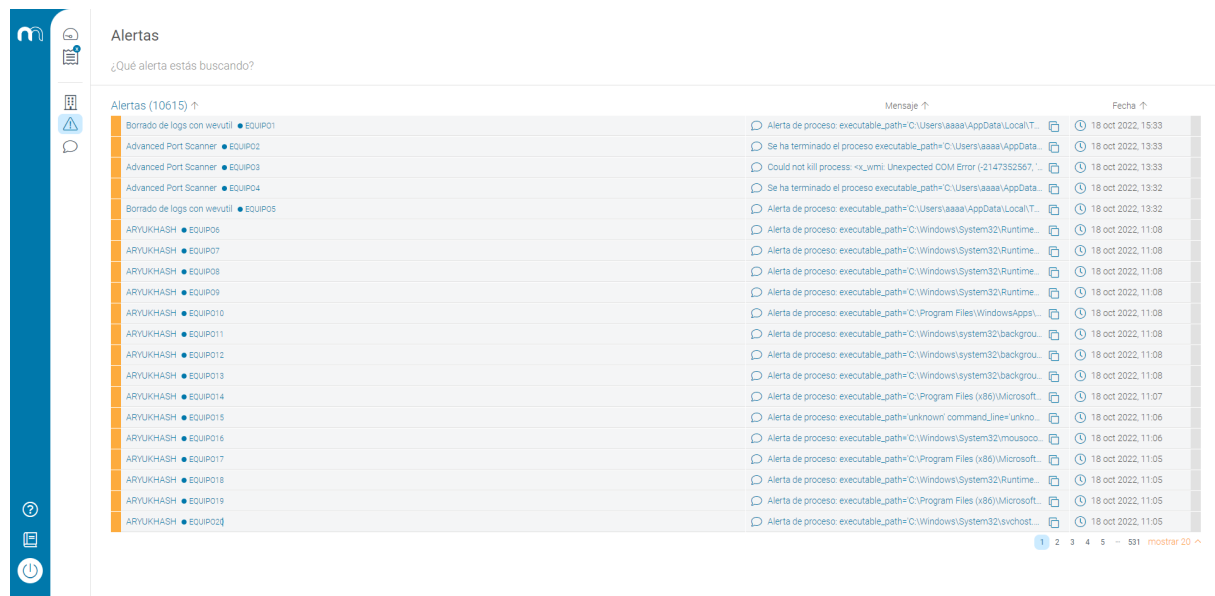
Vacuna 1	...	procomon	●	1.8.2	...	...
Vacuna 3	...	file	●	1.8.2	...	...
Vacuna 4	...	registry	●	1.8.2	...	...
Vacuna 5	...	evento	●	1.8.2	...	...
Vacuna 6	...	procomon	●	1.6.0	...	...
Vacuna 7	...	procomon ryuk text	●	1.8.2	...	...
Vacuna 8	...	mutex	●	1.8.2	...	...
Vacuna 9	...	procomon	●	1.4.0	...	...
Vacuna 10	...	mutex	●	1.4.0	...	...

1 2 3 4 5 6 7 mostrar 20

**Figura 25:** Vacuna con posibles efectos adversos

## 4.8. Alertas

La sección de alertas muestra un listado de las alertas que han generado las vacunas en los equipos de la organización.

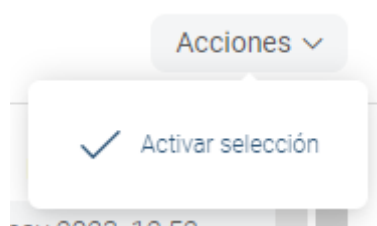


	Mensaje	Fecha
Borrado de logs con weutil • EQUIPO1	Alerta de proceso: executable_path=C:\Users\aaaa\AppData\Local\T...	18 oct 2022, 15:33
Advanced Port Scanner • EQUIPO2	Se ha terminado el proceso executable_path=C:\Users\aaaa\AppData...	18 oct 2022, 13:33
Advanced Port Scanner • EQUIPO3	Could not kill process: <_wmi> Unexpected COM Error (-2147352567, ...)	18 oct 2022, 13:33
Advanced Port Scanner • EQUIPO4	Se ha terminado el proceso executable_path=C:\Users\aaaa\AppData...	18 oct 2022, 13:32
Borrado de logs con weutil • EQUIPO5	Alerta de proceso: executable_path=C:\Users\aaaa\AppData\Local\T...	18 oct 2022, 13:32
ARYUKHASH • EQUIPO6	Alerta de proceso: executable_path=C:\Windows\System32\Runtime...	18 oct 2022, 11:08
ARYUKHASH • EQUIPO7	Alerta de proceso: executable_path=C:\Windows\System32\Runtime...	18 oct 2022, 11:08
ARYUKHASH • EQUIPO8	Alerta de proceso: executable_path=C:\Windows\System32\Runtime...	18 oct 2022, 11:08
ARYUKHASH • EQUIPO9	Alerta de proceso: executable_path=C:\Windows\System32\Runtime...	18 oct 2022, 11:08
ARYUKHASH • EQUIPO10	Alerta de proceso: executable_path=C:\Program Files\WindowsAppsi...	18 oct 2022, 11:08
ARYUKHASH • EQUIPO11	Alerta de proceso: executable_path=C:\Windows\system32\backgrou...	18 oct 2022, 11:08
ARYUKHASH • EQUIPO12	Alerta de proceso: executable_path=C:\Windows\system32\backgrou...	18 oct 2022, 11:08
ARYUKHASH • EQUIPO13	Alerta de proceso: executable_path=C:\Windows\system32\backgrou...	18 oct 2022, 11:08
ARYUKHASH • EQUIPO14	Alerta de proceso: executable_path=C:\Program Files (x86)\Microsoft...	18 oct 2022, 11:07
ARYUKHASH • EQUIPO15	Alerta de proceso: executable_path=unknown command_line=unkno...	18 oct 2022, 11:06
ARYUKHASH • EQUIPO16	Alerta de proceso: executable_path=C:\Windows\System32\mouseco...	18 oct 2022, 11:06
ARYUKHASH • EQUIPO17	Alerta de proceso: executable_path=C:\Program Files (x86)\Microsoft...	18 oct 2022, 11:05
ARYUKHASH • EQUIPO18	Alerta de proceso: executable_path=C:\Windows\System32\Runtime...	18 oct 2022, 11:05
ARYUKHASH • EQUIPO19	Alerta de proceso: executable_path=C:\Program Files (x86)\Microsoft...	18 oct 2022, 11:05
ARYUKHASH • EQUIPO20	Alerta de proceso: executable_path=C:\Windows\System32\svchost...	18 oct 2022, 11:05

**Figura 26:** Listado de alertas

Se muestra el nombre de la alerta, el nombre del equipo, el mensaje y la fecha de creación de la alerta.

Además, existen otras acciones disponibles para el listado de alertas, en la esquina superior derecha:



**Figura 27:** Acciones disponibles para el listado de alertas

### 4.8.1. Activar selección

- Esta acción sirve para habilitar la selección múltiple de las diferentes alertas del listado y poder ejecutar acciones en bloque, sobre un conjunto concreto de alertas. Actualmente existen varias

acciones de este tipo:



**Figura 28:** Acciones en bloque para el listado de alertas

#### 4.8.1.1. Resolver alertas seleccionadas

- Desplegar el menú de acciones y seleccionar la opción **Activar selección**. Esta acción habilitará una cajita delante de las alertas para realizar la selección de aquellas sobre las que se desea realizar la acción.
- Tras realizar la selección de las alertas, se habilita un nuevo menú de acciones en bloque, y al pulsar sobre la acción **Resolver alertas seleccionadas** se marcan como resueltas las alertas seleccionadas.













#### 4.8.1.2. Marcar como falso positivo las alertas seleccionadas

- Desplegar el menú de acciones y seleccionar la opción **Activar selección**. Esta acción habilitará una cajita delante de las alertas para realizar la selección de aquellas sobre las que se desea realizar la acción.
- Tras realizar la selección de las alertas, se habilita un nuevo menú de acciones en bloque, y al pulsar sobre la acción **Marcar como falso positivo las alertas seleccionadas** se marcan como falso positivo las alertas seleccionados.



## 4.9. Noticias

La sección de noticias muestra un listado de las noticias generadas por la herramienta Microclaudia.

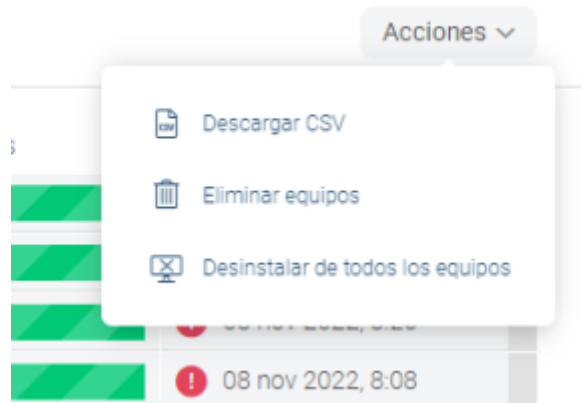
Noticias		
<b>Vacuna 1</b> Detecta la ejecución del ransomware Quantum		22 ago 2022, 13:18
<b>Vacuna 2</b> Detecta patrón de ejecución identificado en incidente de ransomware.		04 ago 2022, 11:41
<b>Vacuna 3</b> Mutex para Ransomware Lockbit 3.0		27 jul 2022, 10:36
<b>Vacuna 4</b> Manipulación de la tarea programada "lockertask"		27 jul 2022, 10:36
<b>Vacuna 5</b> Delete backup with wbadmin		27 jul 2022, 10:35
<b>Vacuna 6</b> Herramienta para la infección de ejecutables identificada en incidentes de ransomware		20 jul 2022, 13:39
<b>Vacuna 7</b> Detecta la ejecución del software legítimo MeshAgent. Puede producir falsos positivos si esta herramienta se usa a nivel corporativo.		14 jul 2022, 13:26
<b>Vacuna 8</b> Detecta la ejecución de binario relacionado con MedusaLocker		01 jul 2022, 11:29
<b>Vacuna 9</b> Detecta la ejecución de binarios relacionados con MedusaLocker		01 jul 2022, 11:29
<b>Vacuna 10</b> No existe software legítimo que se ejecute bajo esta ruta, usado habitualmente por actores de ransomware		07 jun 2022, 17:50
<b>Vacuna 11</b> Detecta binario empleado por Hive		
<b>Vacuna 12</b> Detecta binario empleado por Hive		

**Figura 29:** Listado de noticias

Se muestra el título de la noticia, su contenido formateado como html y la fecha de actualización.

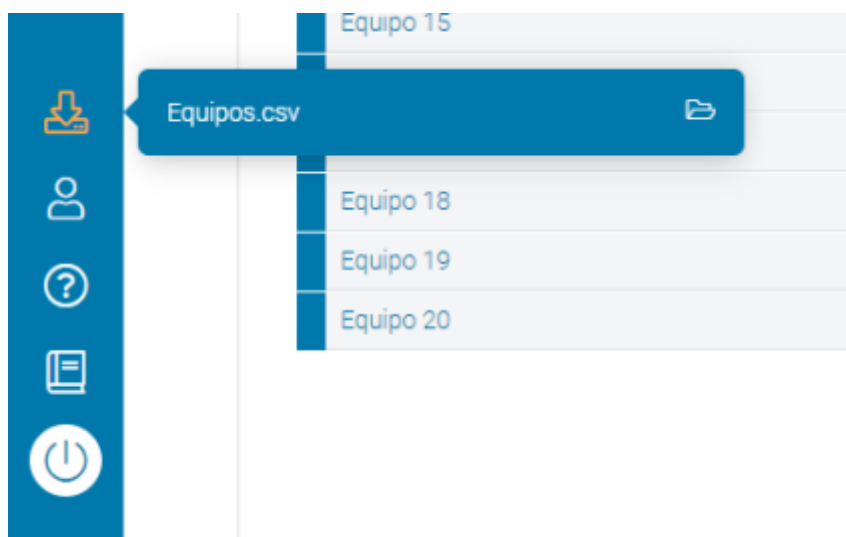
#### 4.10. Descarga de listados en formato CSV

Es posible descargar listados en formato CSV de las siguientes secciones: Equipos, alertas, organismos y vacunas. Para ello, iremos al menú de acciones de la sección deseada y pincharemos en la opción “Descargar CSV”.



**Figura 30:** Descargar CSV

Una vez iniciado el proceso de descarga. Las descargas activas aparecerán en el widget de la barra lateral con un indicador de precarga si están todavía en proceso. Cuando alguna de las descargas acabe de procesarse, ésta será clickable y al pinchar sobre ella nos descargará el archivo correspondiente.



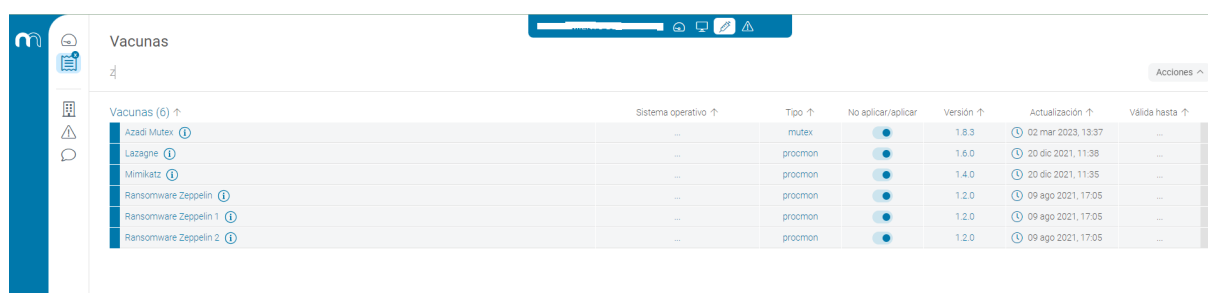
**Figura 31:** Descargar CSV

## 4.11. Buscador

Es posible realizar búsquedas en todas las pantallas, a excepción del cuadro de mando. Para ello, simplemente colocamos el cursor en el campo de texto ubicado debajo del título de la pantalla.

La búsqueda se realizará sobre todos los campos basados en texto que componen la tabla. La búsqueda permite el uso de comodines (\*).

A modo de ejemplo, a continuación, filtramos las vacunas que contienen la letra 'z'.



The screenshot shows a web application titled 'Vacunas'. At the top, there is a search bar containing the letter 'z'. Below the search bar, a table lists vaccine updates. The table has columns for 'Sistema operativo', 'Tipo', 'No aplicar/aplicar', 'Versión', 'Actualización', and 'Válida hasta'. The table contains six rows of data, including 'Azadi Mutev', 'Lazagne', 'Mimikatz', and two instances of 'Ransomware Zeppelin'.

	Sistema operativo ↑	Tipo ↑	No aplicar/aplicar	Versión ↑	Actualización ↑	Válida hasta ↑
Azadi Mutev ⓘ	...	mutex	<input checked="" type="checkbox"/>	1.8.3	🕒 02 mar 2023, 13:37	...
Lazagne ⓘ	...	procomon	<input checked="" type="checkbox"/>	1.6.0	🕒 20 dic 2021, 11:38	...
Mimikatz ⓘ	...	procomon	<input checked="" type="checkbox"/>	1.4.0	🕒 20 dic 2021, 11:35	...
Ransomware Zeppelin ⓘ	...	procomon	<input checked="" type="checkbox"/>	1.2.0	🕒 09 ago 2021, 17:05	...
Ransomware Zeppelin 1 ⓘ	...	procomon	<input checked="" type="checkbox"/>	1.2.0	🕒 09 ago 2021, 17:05	...
Ransomware Zeppelin 2 ⓘ	...	procomon	<input checked="" type="checkbox"/>	1.2.0	🕒 09 ago 2021, 17:05	...

**Figura 32:** Listado de noticias

## 5. POC

Puede dirigir cualquier consulta, duda o sugerencia a la siguiente dirección de correo electrónico:

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

## 6. ANEXO. PREGUNTAS MÁS FRECUENTES

### **¿Con qué sistemas operativos es compatible la herramienta?**

Con todos los sistemas operativos Windows™ desde Windows XP™ (incluido) en adelante.

### **¿Existe alguna incompatibilidad con soluciones antivirus o EDR?**

Hasta la fecha no se han encontrado incompatibilidades con ningún antivirus o EDR comercial. No obstante, para garantizar el correcto funcionamiento de la herramienta, se recomienda que ésta se excepcione en dichas soluciones de seguridad.

### **Si tengo ya una solución de EDR o antivirus, ¿podría desinstalarlos y utilizar sólo microCLAUDIA?**

No se recomienda. Se considera que microCLAUDIA es una solución de seguridad complementaria a las soluciones de seguridad existentes, proporcionando una capa de protección adicional frente a las amenazas de tipo ransomware.

### **Cuando se libere una nueva versión, ¿habrá que volver a instalarlo en todos los equipos?**

No, microCLAUDIA se actualiza de forma automática sin necesidad de realizar ninguna acción adicional por parte del organismo.

### **¿Cuántos recursos del equipo consume?**

En términos de memoria RAM el agente de microCLAUDIA consume en torno a 15 MB de memoria y en cuanto a CPU, su consumo es inapreciable.

### **¿Como afectan las vacunas en los equipos?**

Puede consultarlo en el apartado de Noticias.

### **¿Cuál es la diferencia con CLAUDIA?**

La herramienta microCLAUDIA podría considerarse una versión simplificada de CLAUDIA, en la que se ha puesto el foco en el despliegue de vacunas para la prevención de ransomware. A corto/medio plazo, toda la funcionalidad de microCLAUDIA, si bien podría ser implementada mediante sensores en CLAUDIA, estará incluida dentro de CLAUDIA.

CLAUDIA, por otro lado, está diseñada para la detección de amenazas persistentes avanzadas (APTs) en el puesto de usuario y para su funcionamiento requiere disponer previamente de la herramienta CARMEN.

### **¿Por qué en ocasiones no aparece información en el detalle del equipo (Interfaces, Discos, Usuarios...)?**

Para obtener la información del equipo se utiliza WMI, que es una herramienta de Microsoft para obtener información de Windows. Entre versiones de Windows cambian los formatos de las tablas de WMI, incluso con la misma versión de Windows, hay variaciones entre 32 y 64 bits, además de entre builds.

Por todo ello, en ocasiones WMI es incapaz de obtener dicha información y por eso no se muestra en la consola de microCLAUDIA. A partir de la versión 2.x del agente de microCLAUDIA se va a usar directamente llamadas al API de Windows y se resolverán todos estos problemas.

## 7. Despliegue y/o actualización por GPO

### 7.1. Versión 1.x.x

Para el despliegue de microCLAUDIA mediante una política de dominio (GPO), copiar el ejecutable de microclaudia-setup.exe en un recurso compartido accesible por los equipos de la organización junto con un fichero instalarclaudia.bat con el siguiente contenido: (Nota: Es importante que este contenido este únicamente en dos líneas, una para el @echo off y otra que incluya el resto del contenido, en una misma línea.)

```
@echo off

if exist "C:\Program Files\microclaudia" (echo microclaudia instalado >
↪ C:\Windows\Temp\microclaudia.log) else
↪ (\\<dominio>\NETLOGON\<dominio>\scripts\Microclaudia\microclaudia-
↪ setup.exe /VerySilent /apikey=<api_key> /server=<serverCentral_vacunas>
↪ /proxyhost=<proxy_host> /proxyport=<proxy_port> /tags=<tag1,tag2>)
```

En el comando, se deben modificar los siguientes valores:

- <dominio> dominio de la organización.
- <api\_key> apikey de activación, facilitada por email al responsable.
- <serverCentral\_vacunas> Servidor central de vacunas al que conectar.
- <proxy\_host> proxy de la organización. En caso de no utilizar, no incluir dicho elemento.
- <proxy\_port> puerto de la organización. En caso de no utilizar, no incluir dicho elemento.
- <tag1, tag2> Listado de etiquetas. En caso de no utilizar, no incluir dicho elemento.

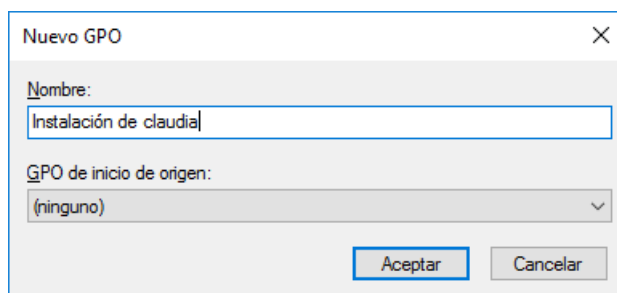
Ejemplo de instalación sin proxy:

```
microclaudia-setup.exe /apikey=7c832...d9df8d
↪ /server=<dominio_microclaudia> /verysilent
```

Ejemplo de instalación con proxy:

```
microclaudia-setup.exe /apikey=7c832...d9df8d
↪ /server=<dominio_microclaudia> /proxyhost=10.120.10.128 /proxyport=3128
↪ /verysilent
```

Seguidamente se deberá crear una GPO que ejecute el fichero .bat al arrancar el equipo. Para ello se deberá ejecutar el administrador de directivas de grupo y crear una política aplicada sobre la unidad organizativa que contenga los equipos en los que se desea instalar microCLAUDIA.

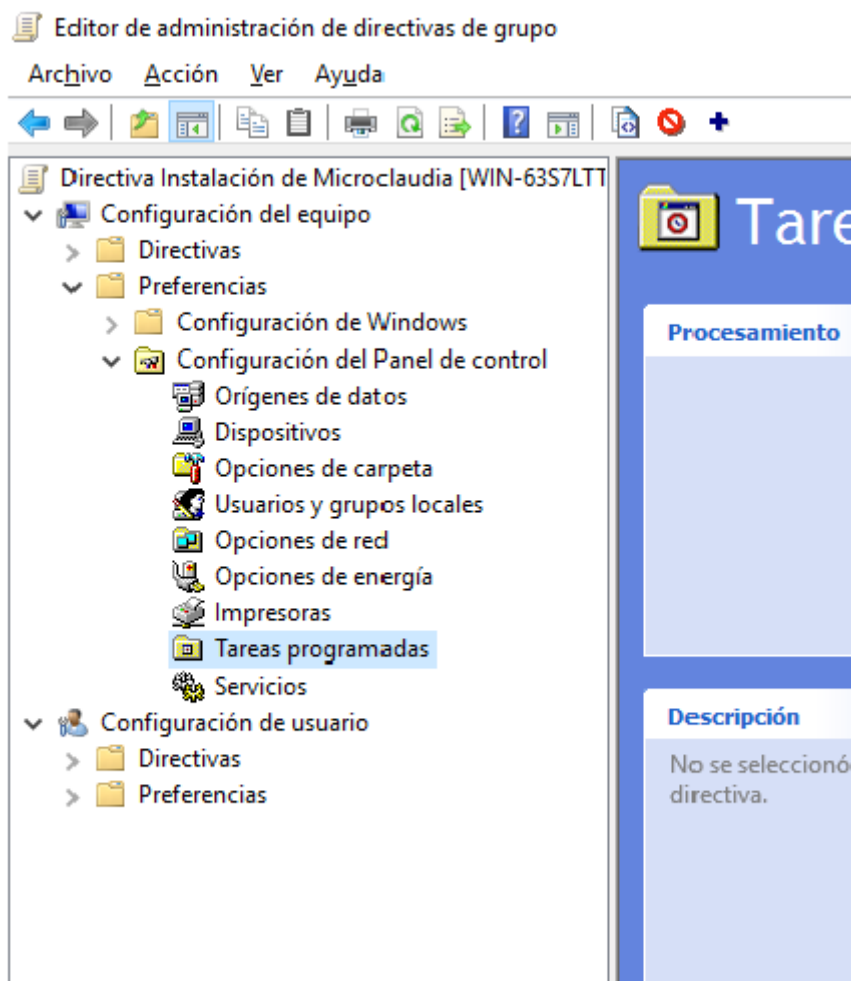


**Figura 33:** Nuevo GPO

Una vez creada la política se procederá a su edición pulsando botón derecho sobre el nombre de la política y seleccionando la opción Editar. En la pantalla de edición se deberá elegir:

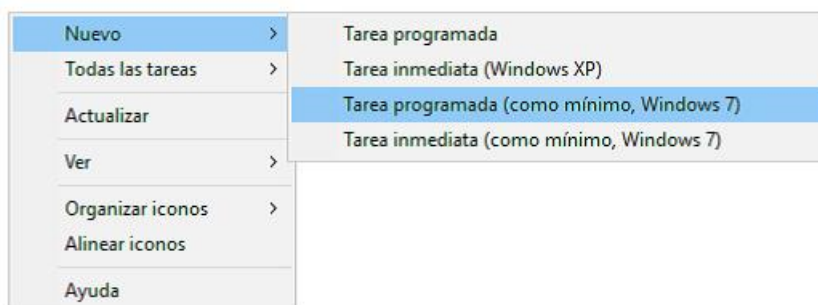
*Configuración del equipo → Preferencias → Panel de control → Tareas Programadas*





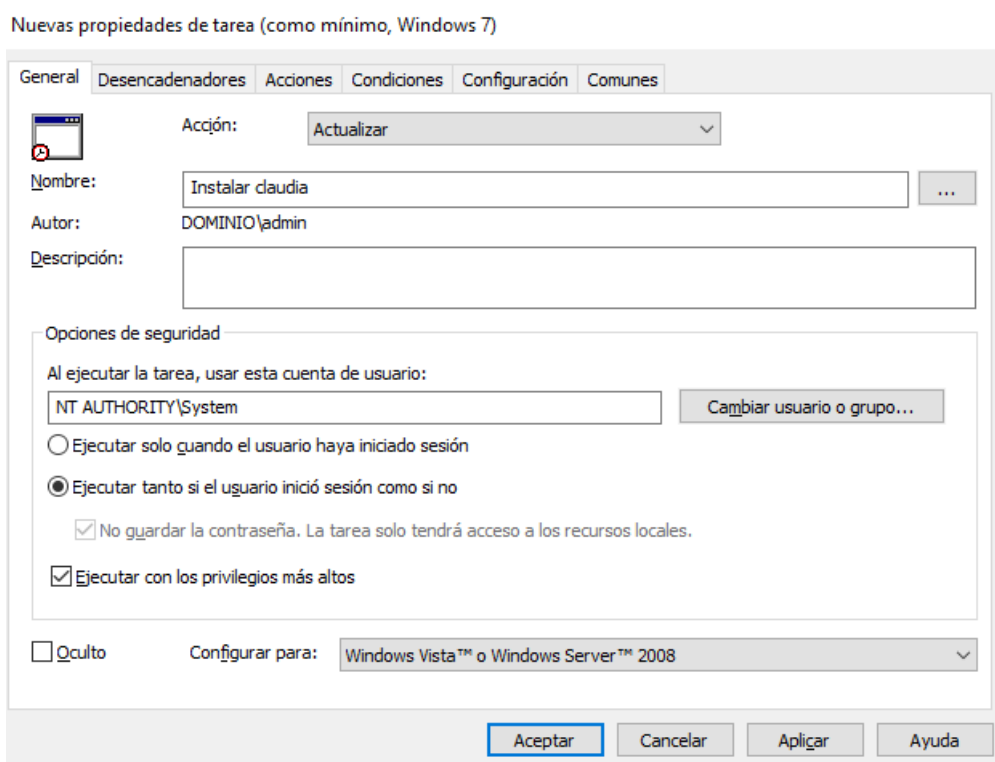
**Figura 34:** Editor de administración de directivas de grupo

Y se procederá a crear una nueva tarea programada pulsando botón derecho y eligiendo la siguiente opción:

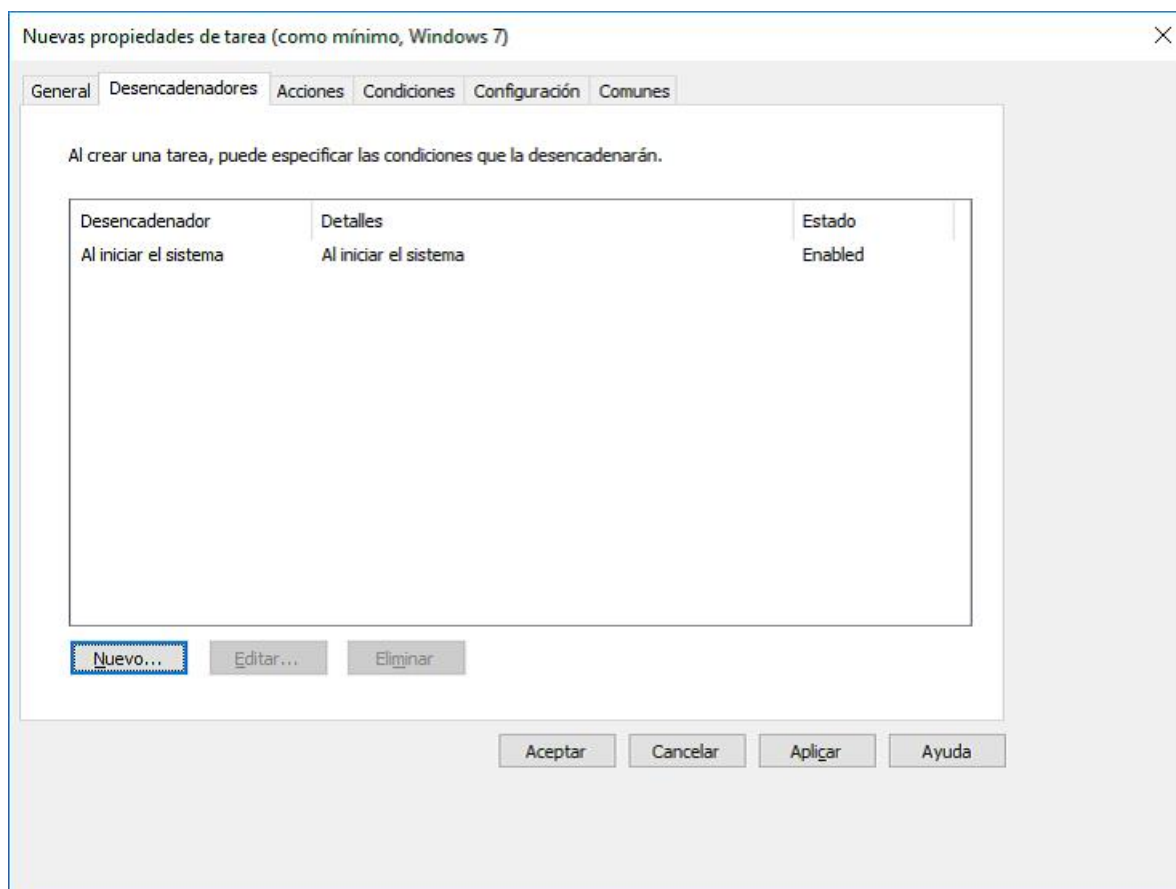


**Figura 35:** Nueva tarea programada

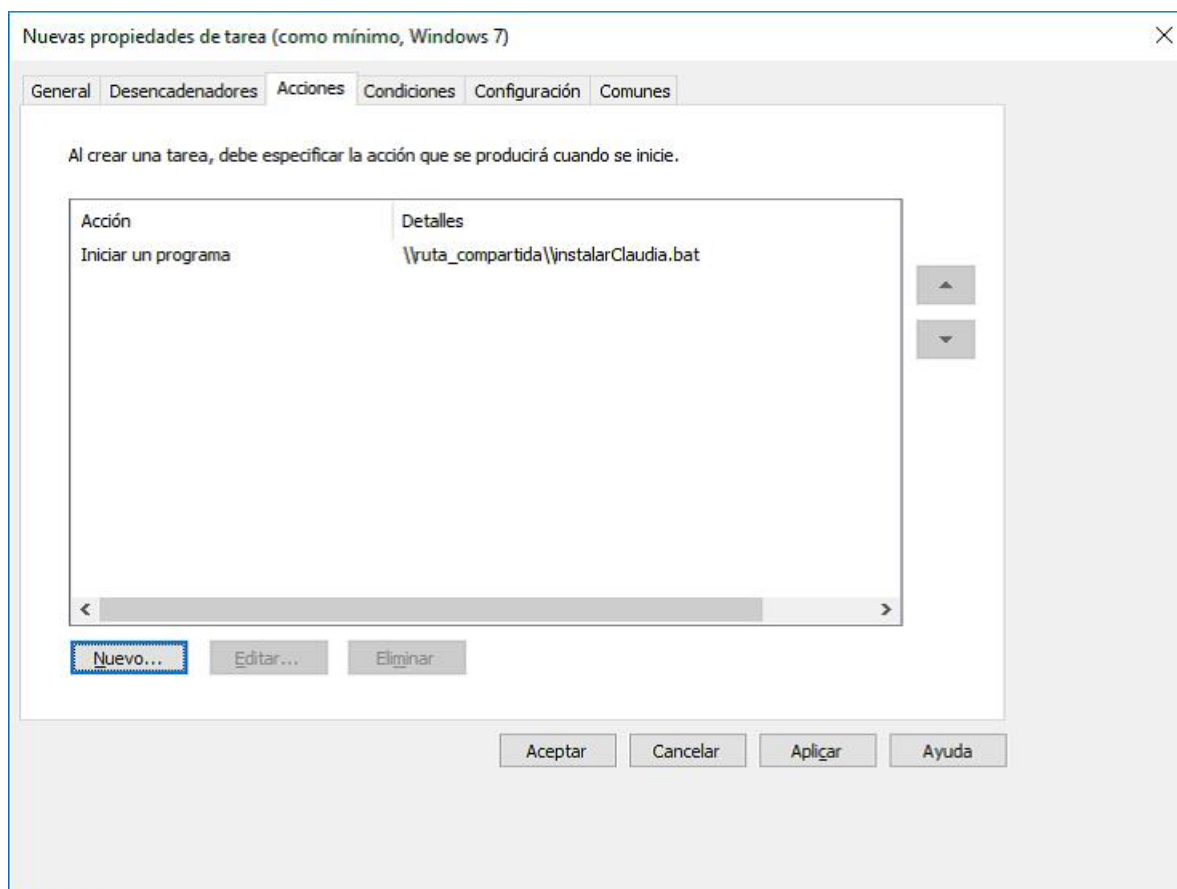
Finalmente, se escogerán las opciones para la tarea como se indica en las siguientes imágenes:



**Figura 36:** Propiedades generales de la tarea



**Figura 37:** Desencadenadores



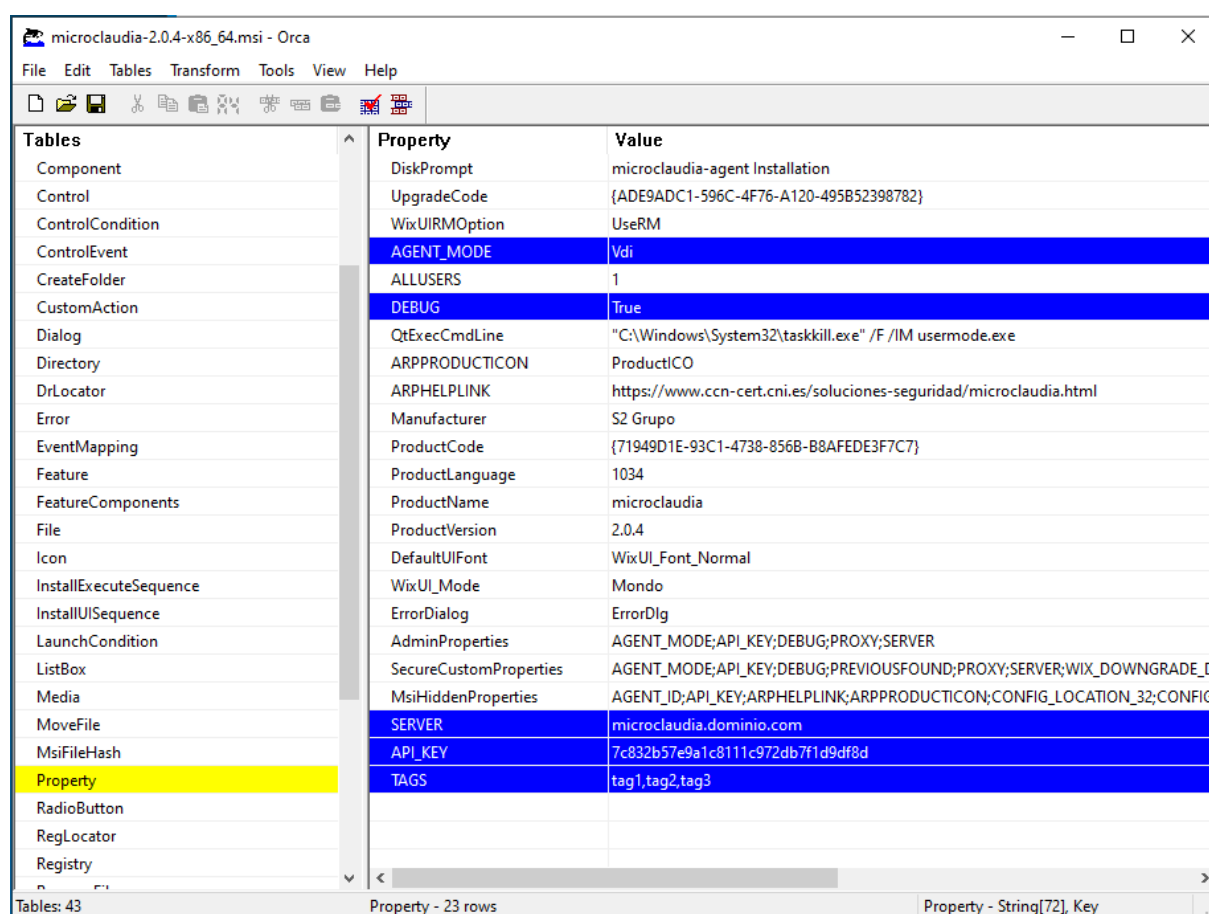
**Figura 38:** Acciones

## 7.2. Versión 2.x.x

Para la creación de la GPO es necesario hacer modificaciones sobre el MSI, siendo necesario el software Orca incluido en el SDK de Windows. Estas modificaciones contendrán los parámetros que se le pasan al MSI.

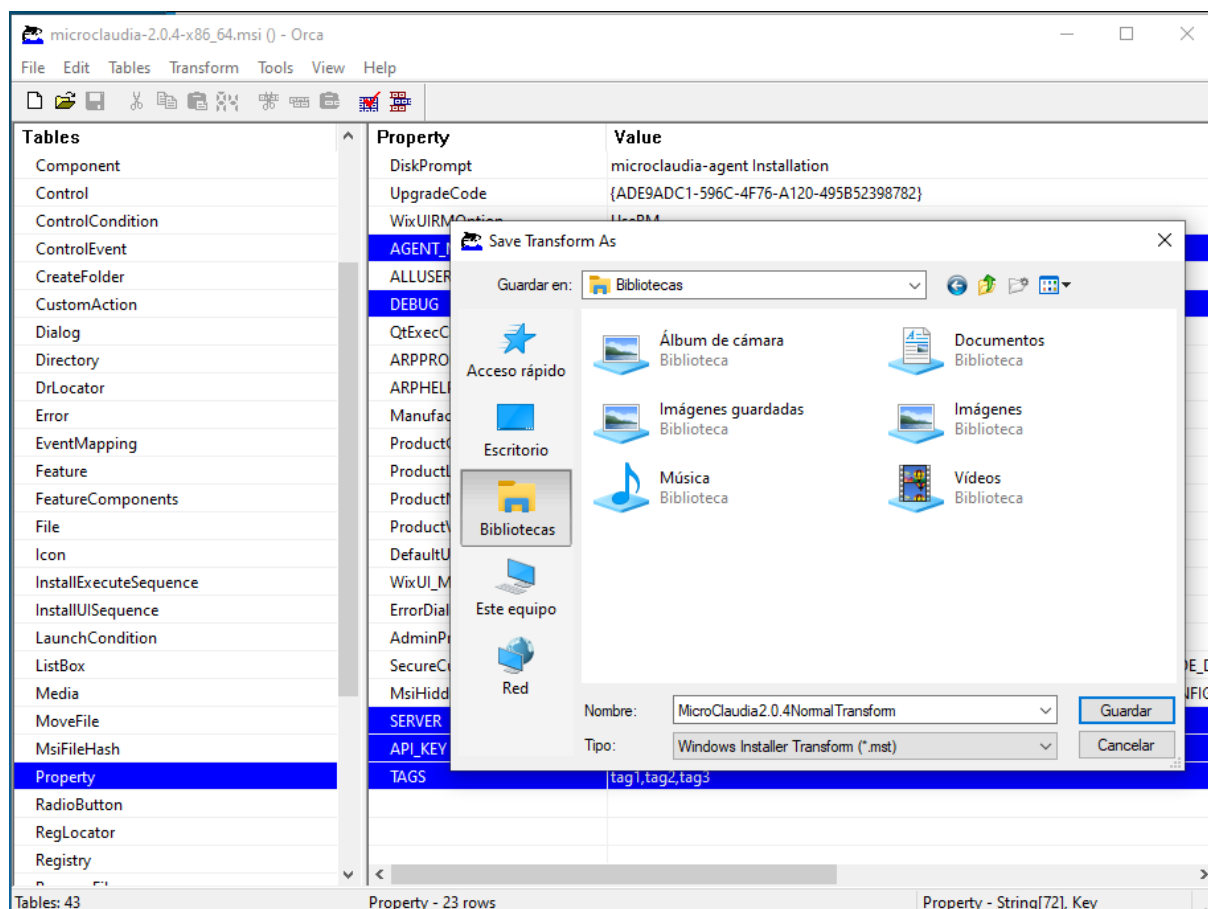
Se deben abrir los MSIs de Microclaudia con la herramienta Orca y desde el apartado *Transform* se deberá iniciar una modificación con *New Transform*.

En la lista de tablas, el apartado *Property* almacena todas las propiedades del MSI, pudiendose modificar el valor de cada una, si estas no aparecen, será necesario crearlas.



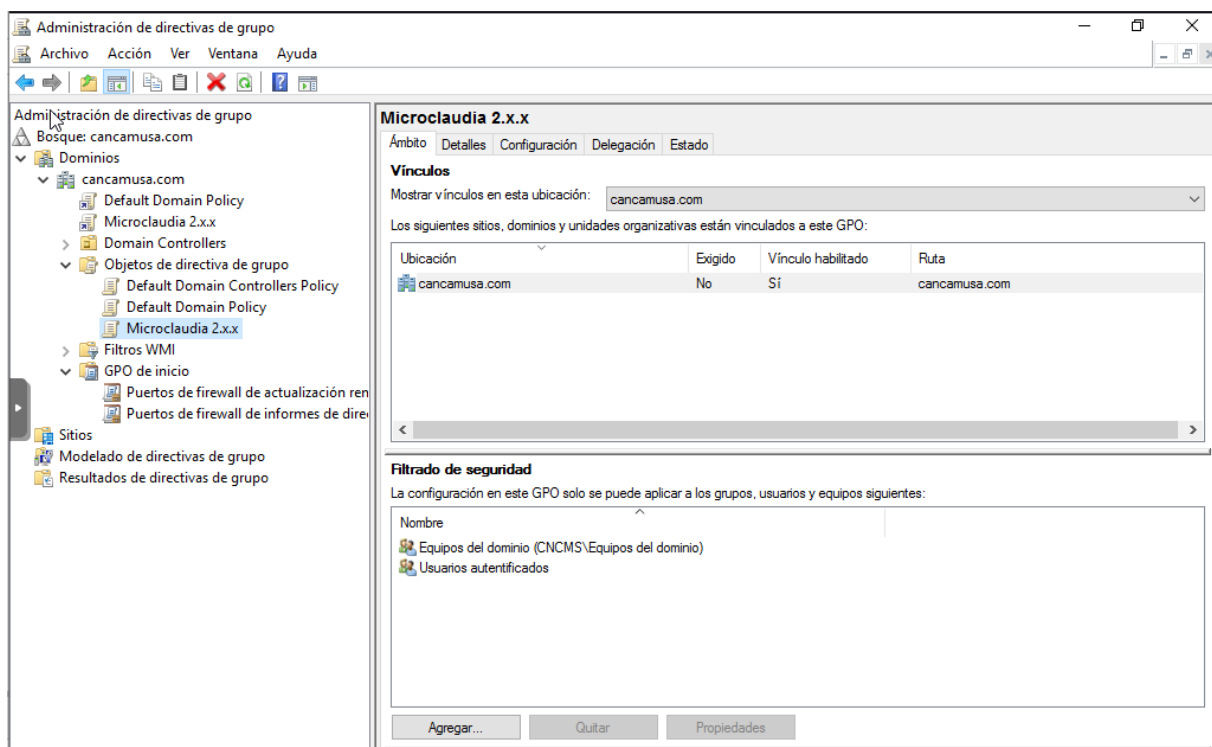
**Figura 39:** Añadir parámetros con Orca

Una vez ajustados los parámetros correctamente, se crea la modificación desde *Transform > Generate Transform*.



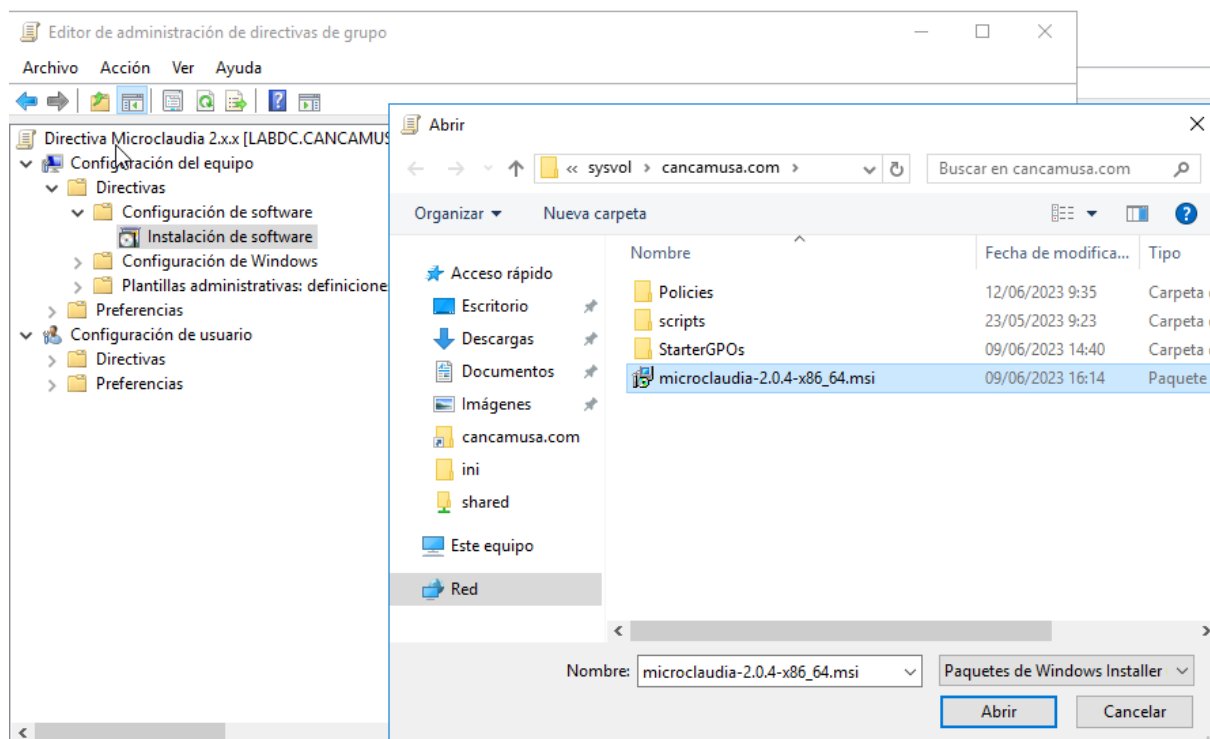
**Figura 40:** Generar una modificación

Como resultado se obtendrán unos ficheros *.mst* que se utilizarán durante la creación de la GPO. En el ejemplo se hace para *equipos de dominio*, pero se pueden crear distintas GPOs en función de los casos de uso que se manejen. Por ejemplo una GPO distinta para servidores y equipos de una red que necesitan un proxy de navegación frente a otra red que no lo necesita.



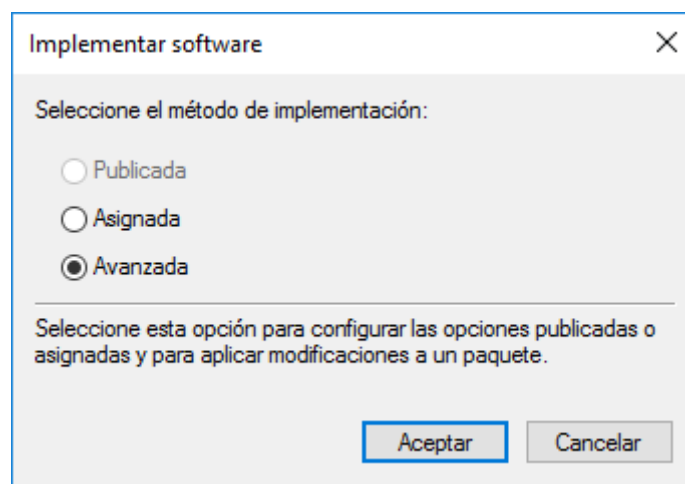
**Figura 41:** Creación de la GPO de microclaudia 2.x.x

Se crea una instalación de microclaudia de 64 bits. Es importante que el instalador esté en una carpeta compartida accesible por todos los equipos y con los permisos apropiados.



**Figura 42:** Instalación de microclaudia 64 bits

Se debe marcar la opción *Avanzada* puesto que se quiere modificar ligeramente la instalación.

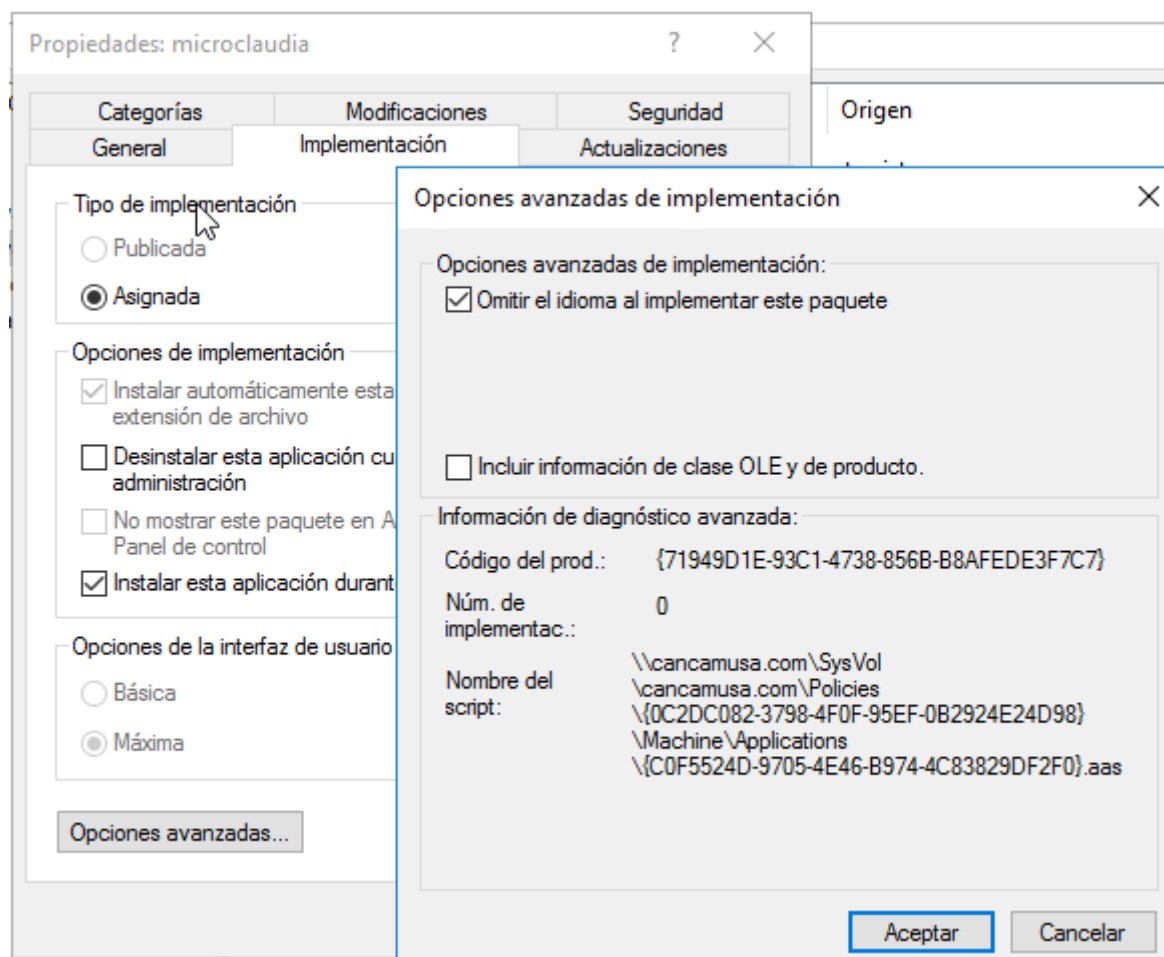


**Figura 43:** Implementación de software Avanzada

En el apartado de implementación se podrá marcar la opción para que se instale durante el inicio de sesión, aunque dependerá, de nuevo, de los casos de uso concretos, en el caso aplicarse sobre

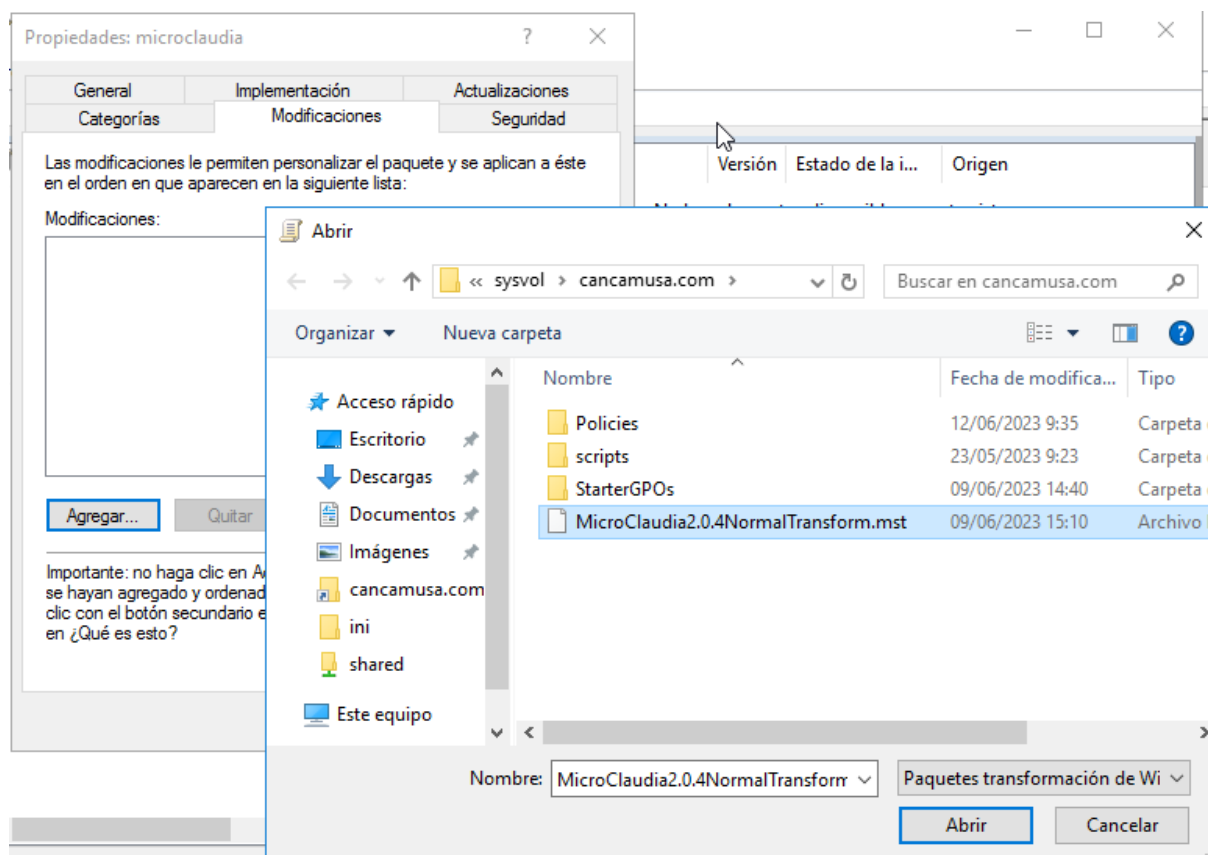


servidores no se instalará hasta que haya un reinicio, lo cual puede, en algún caso, no ocurrir en meses. La opción que sí se debe marcar es la de *Omitir el idioma al implementar el paquete* dentro de *Opciones avanzadas...* para que se pueda desplegar en toda la organización independientemente del idioma.



**Figura 44:** Configuración de la implementación

Ahora en la pestaña *Modificaciones* se añade el archivo *.mst* que se ha creado con Orca. Es importante que tanto los *.mst* como los *.msi* estén en carpetas compartidas accesibles por los equipos.



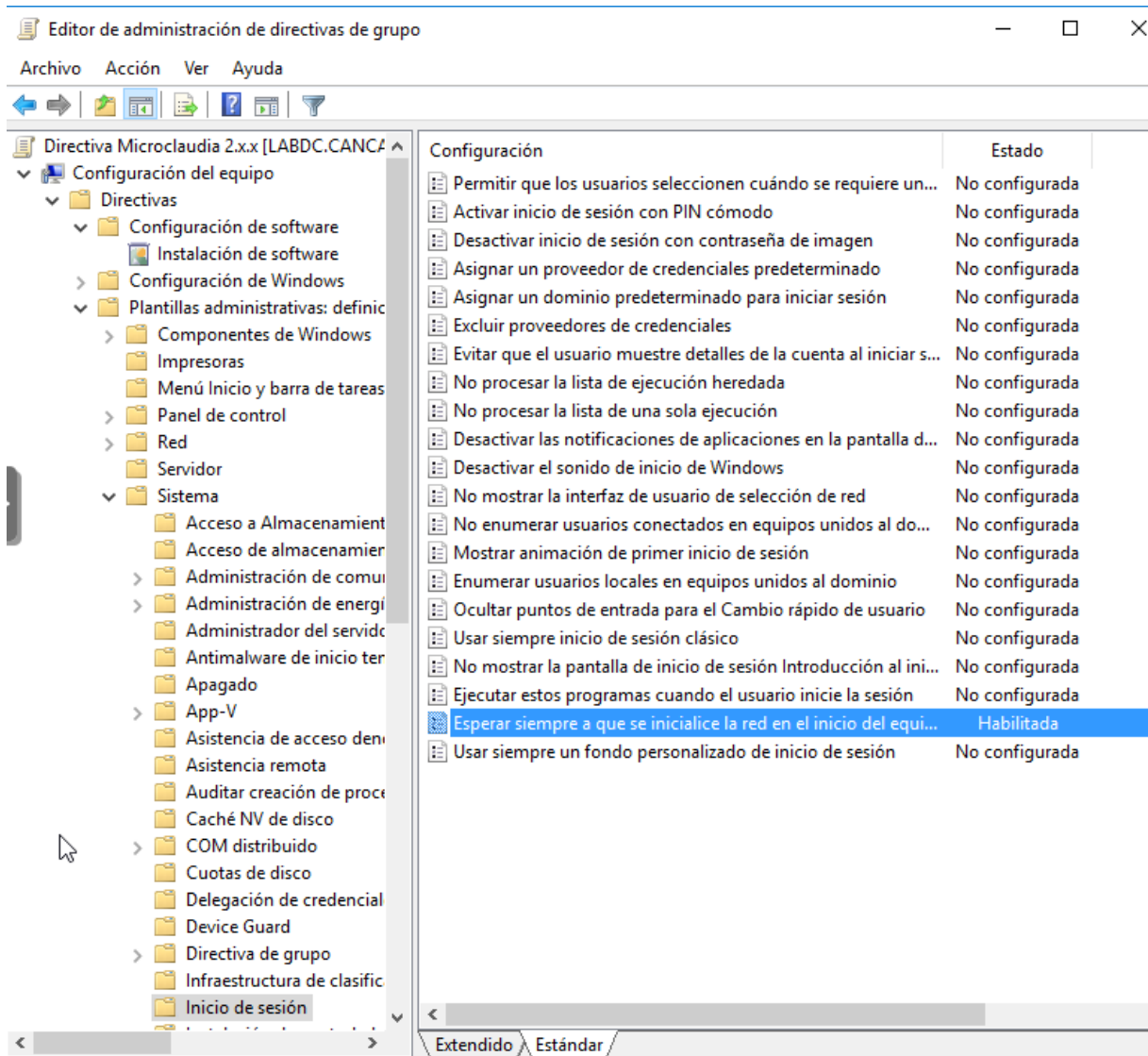
**Figura 45:** Añadir la modificación

Se debe repetir el proceso para el instalador de 32 bits, recordando usar un *mst* específico para la versión de 32 bits.

### 7.2.1. Otras configuraciones de la GPO

Para evitar errores de conectividad a la hora de procesar las GPOs, se pueden configurar los siguientes parámetros:

- Habilitar *Esperar siempre a que se inicie la red en el inicio del equipo y el inicio de sesión*
  - Configuración del Equipo > Plantillas administrativas > Sistema > Inicio de Sesión > Esperar siempre a que se inicie la red en el inicio del equipo y el inicio de sesión > Habilitada.
  - Computer Settings > Policies > Administrative Templates > System > Logon > Always wait for the network at computer startup and logon > Enabled.



**Figura 46:** Especificar que haya conectividad de red para procesar la GPO

- Habilitar *Especificar el tiempo de espera de conectividad de área de trabajo para el procesamiento de directivas*:
  - Configuración del Equipo > Plantillas administrativas > Sistema > Directivas de grupo > Esperar siempre a que se inicie la red en el inicio del equipo y el inicio de sesión > Habilitada y 90 segundos de tiempo de espera.
  - Computer Settings > Políticas > Administrative Templates > System > Group Policy > Startup policy processing wait time > Enabled with 90 seconds of wait time.

