

panda

Malware**Rad**ar



Guía de uso



## Introducción

Panda Malware Radar es un servicio de auditoría automatizada que identifica las amenazas que están pasando desapercibidas para su actual software de seguridad. Le permite evaluar la seguridad de su parque informático generando informes exhaustivos y recomendaciones que le permitirán orientar su estrategia de seguridad. Además, Panda Malware Radar le ofrece la posibilidad de realizar una limpieza para eliminar todas las amenazas encontradas.



## Tipos de auditorías

### Prueba gratuita (Trial)

La prueba gratuita de Panda Malware Radar le permite auditar una vez su parque informático, sin límite en el número de equipos analizados.

Este tipo de auditoría le presenta un resumen de resultados y un ejemplo de informe detallando los resultados obtenidos en uno de los equipos auditados.

### Auditoría única

Si adquiere una auditoría única podrá auditar su parque informático una sola vez. Dispone de dos tipos de auditoría única: **Con limpieza del malware detectado o sin limpieza del malware detectado.**

Al finalizar la auditoría, obtendrá dos informes detallados: el **informe ejecutivo** y el **informe técnico.**

Si desea adquirir una auditoría única, visite la [web de Panda Malware Radar](#) y solicite las licencias que necesite.

### Suscripción

Al adquirir una suscripción puede realizar un número ilimitado de auditorías en un conjunto fijo de equipos durante el tiempo contratado (uno, dos o tres años).

Al finalizar cada auditoría obtendrá dos informes: un **informe ejecutivo** y un **informe técnico.**

Si desea disponer de acceso ilimitado a los servicios, visite la [web de Panda Malware Radar](#) y adquiera las licencias que necesite por el periodo que prefiera.



## Pasos previos

Para realizar la auditoría es necesario distribuir el programa de análisis de Panda Malware Radar en la red.

- Para utilizar la herramienta de distribución automática es imprescindible que el equipo en el que se utilice dicha herramienta disponga de conexión a Internet. No es imprescindible que el resto de los equipos de la red dispongan de dicha conexión. La herramienta de distribución automática le permite seleccionar los equipos que desee auditar en su red.
- Si desea auditar una red aislada en la que ningún puesto dispone de conexión a Internet, o equipos aislados sin dicha conexión, deberá descargar el programa de análisis y ejecutarlo manualmente en cada uno de los equipos a auditar. Para más información, consulte el apartado **Auditorías con despliegue manual**. El programa de análisis no deja ningún componente instalado en los equipos a auditar.

### Requisitos

#### Requisitos para acceder a la consola web:

Internet Explorer 5.5 o superior.

Mozilla Firefox 1.5 o superior.

Conexión a Internet, bien directa o a través de una red local.

Conexión HTTPS (puerto 443).

#### Requisitos en el equipo desde el que se realiza el despliegue:

**Sistema operativo:** Windows Vista (32 y 64 Bits) / XP Professional (32 y 64 bits) / 2000 Pro / . Servidores Windows 2000 /2003 (32 y 64 bits).

**Procesador:** Pentium a 166 MHz o superior.

**Memoria RAM:** 128 MB.

**Disco duro:** 70 MB de espacio libre.

**Navegador:** Internet Explorer 5.0 o superior.

Conexión a Internet.

Tener acceso al recurso *Admin\$* de los equipos a auditar.

Realizar el análisis con un usuario que disponga de derechos de administrador sobre los equipos a auditar.

#### Requisitos en los equipos a auditar:

**Sistema operativo:** Windows Vista (32 y 64 Bits) / XP /2000 Pro /NT 4.0 /Me/ 98 /95 / . Servidores Windows 2003/2000/NT 4.0.

**Procesador:** 486 a 66 MHz o superior.

**Memoria RAM:** 128 MB.

**Disco duro:** 70 MB de espacio libre.

**Navegador:** Internet Explorer 5.0 o superior.

Tener instalado **Compartir impresoras y archivos para redes Microsoft**.

Tener desactivado el **uso compartido simple de archivos** (en Windows XP, **Herramientas > Opciones de carpeta > Utilizar uso compartido simple de archivos**).

Deshabilitar el firewall de Windows, o bien configurar la excepción **Compartir archivos e impresoras**.

Contar con derechos de administrador en los equipos a auditar.

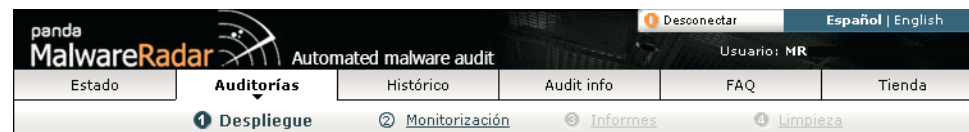


## Introducción a la consola de Panda Malware Radar

Para acceder a la consola de Panda Malware Radar visite la página <http://private.malwareradar.com/> e introduzca el nombre de usuario y la contraseña que le enviamos por correo electrónico tras realizar el registro. Tras aceptar el acuerdo de licencia, haga clic en **Acceder** para entrar en la consola.

Si no recuerda estos datos acceda al recordatorio de claves en <http://www.pandasecurity.com/spain/enterprise/support/details/password/>. Le enviaremos un nuevo correo electrónico con su nombre de usuario y contraseña.

La consola de Panda Malware Radar consta de varios apartados a modo de fichas en la parte superior de la consola, que le guiarán a lo largo del proceso de auditoría.



Las fichas disponibles son las siguientes:

- **Estado:** Muestra las auditorías disponibles, la situación de las auditorías en curso, las alertas, etc.
- **Auditorías:**
  - **Despliegue:** Le permite descargar **la herramienta de distribución automática** (debe utilizarse en un equipo con conexión a Internet), o el **programa de análisis**. Si desea utilizar su propio método de distribución deberá descargar el programa de análisis.
  - **Monitorización:** Muestra el estado de la auditoría en curso: equipos analizados, número de análisis finalizados, códigos maliciosos encontrados hasta el momento de la consulta, nivel de protección del parque, etc.
  - **Informes:** Le proporcionan información detallada sobre el software malicioso detectado (tanto activo como latente), fallos de seguridad, nivel de protección de su parque, etc. Existen dos tipos de informes con distinto nivel de detalle que podrá consultar en la consola, o bien descargar en PDF o XML.
  - **Limpieza:** Le permite distribuir el **programa de desinfección** en su red, bien mediante la herramienta de distribución automática, o descargando el programa de desinfección.



Una vez concluido el proceso en cada una de estas fichas, haga clic en la siguiente para continuar el proceso.

- **Histórico:** Contiene un archivo histórico de las auditorías realizadas para su posterior consulta. Además, permite crear un informe consolidado, combinando los resultados de las diferentes auditorías realizadas.
- **Audit Info:** Muestra estadísticas generales con datos significativos sobre los resultados obtenidos por Panda Malware Radar en otras empresas. En esta sección también es posible acceder a un glosario de términos.

- **FAQ:** En esta sección puede encontrar las respuestas a las preguntas planteadas con más frecuencia.

- **Tienda:** En la tienda puede adquirir el tipo de auditoría que prefiera:

- **Auditoría única:** Le permitirá auditar todo su parque una sola vez.
- **Suscripción:** Le permitirá realizar un número ilimitado de auditorías.

Además, también podrá contratar las limpiezas durante el periodo contratado (uno, dos o tres años).



## Cómo realizar la auditoría en unos pasos

El primer paso para auditar una red consiste en distribuir el programa de análisis a cada uno de los equipos.

Las posibilidades son las siguientes:

- Para utilizar la herramienta de distribución automática es imprescindible que el equipo en el que se utilice disponga de conexión a Internet.
- Si desea auditar una red aislada en la que ningún puesto dispone de conexión a Internet, o equipos aislados sin dicha conexión, deberá descargar el programa de análisis y ejecutarlo manualmente en cada uno de los equipos a auditar. Para más información, consulte el apartado **Despliegue manual**. El programa de análisis no deja ningún componente instalado en los equipos a auditar.
- Si desea realizar la distribución mediante otros medios (login script, Tivoli, etc.), deberá descargar el programa de análisis y distribuirlo en su red utilizando el método deseado. Para más información, consulte la documentación de la herramienta que desee utilizar.

### 1.- Acceso a la consola

Para acceder a la consola de Panda Malware Radar visite la página <https://private.malwareradar.com/> e introduzca el nombre de usuario y la contraseña que le enviamos por correo electrónico tras realizar el registro. Tras aceptar el acuerdo de licencia, haga clic en **Acceder** para entrar en la consola.

**Nota:** La primera vez que acceda a la consola de Panda Malware Radar observará una alerta de seguridad solicitando la aprobación de un certificado de seguridad. Cuando aparezca este mensaje haga clic en Sí para aceptar dicho certificado.

### 2.- Generar una nueva auditoría

En la pestaña **Estado** de Panda Malware Radar podrá ver las auditorías disponibles. Siga estos pasos para comenzar el proceso:

The screenshot shows the Panda Malware Radar web console interface. The page title is "Automated malware audit". The navigation menu includes "Estado", "Auditorías", "Histórico", "Audit info", "FAQ", and "Tienda". The "Estado" tab is active. The main content area shows "Mi suscripción" with "Validez hasta: 02/04/2008" and "Licencias contratadas: 25", and a "Generar nueva auditoría" button. Below is "Mis alertas" with a message "No se han producido alertas hasta el momento". At the bottom is "Mi estado" with a list of audit entries and links for "Comenzar auditoría", "Monitorizar desinfección", and "Comenzar limpieza". The footer contains "Guía de uso", "© Panda Software 2007", and "Acuerdo de licencia".



1. Si ha contratado una auditoría única haga clic en **Comenzar auditoría**.
2. Indique el nombre con el que desee identificar la auditoría.
3. Haga clic en **Comenzar ahora**.

### 3.- Configuración y descarga de la Herramienta de Distribución

Antes de distribuir el programa de análisis de Panda Malware Radar con la herramienta mencionada, es posible configurar algunos aspectos. Siga estos pasos para hacerlo:

- Si es la primera vez que se dispone a configurar Panda Malware radar, o desea establecer una nueva configuración, haga clic en **Nueva configuración**. En el campo **Nombre de configuración** indique el nombre que desee para una fácil identificación posterior.
- Si desea utilizar alguna configuración establecida con anterioridad, selecciónela de la lista que aparece en el margen izquierdo.

**Nota:** Es imprescindible que el equipo en el que se utilice la herramienta de distribución disponga de conexión a Internet. Si desea realizar la distribución en una red en la que ningún puesto dispone de conexión a Internet, deberá realizar un **despliegue manual**.

Puede configurar los siguientes aspectos:

- **Ficha General:** Panda Malware Radar necesita conectarse a Internet para enviar los informes de las auditorías a la aplicación. Si utiliza un servidor proxy para acceder a Internet, indique los datos requeridos: la dirección IP del servidor y el puerto. Si además el servidor requiere autenticación, deberá indicar también el nombre de usuario y contraseña con la que se identifica en el servidor proxy.



Si por el contrario, los equipos a auditar no disponen de conexión a Internet, indique un recurso compartido de dicha red en el que desee que se guarde el informe. Por ejemplo, \\xxx\informes (donde XXX es el nombre del equipo en el que se guardará el informe en cuestión).

Si va a realizar el despliegue en equipos con Windows 9x o Windows NT 4, active la casilla que permite la compatibilidad con dichos sistemas operativos.

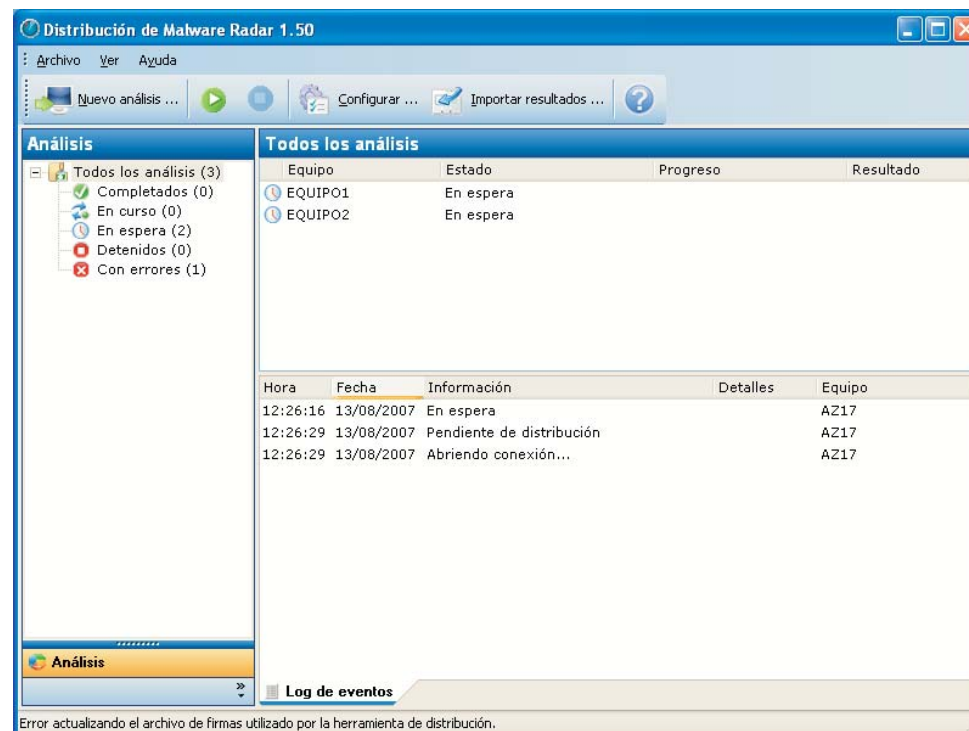
- **Ficha Análisis:** Indique cómo desean que sea el análisis a realizar. Entre otras posibilidades, le permite indicar el tipo de análisis que desea realizar (rápido o completo).
- **Ficha Exclusiones:** En el caso de haber seleccionado un análisis completo, podrá indicar si desea excluir del análisis algún directorio. Si se trata de una limpieza, y no desea eliminar algún tipo concreto de malware, podrá indicarlo activando la casilla que corresponda.

Una vez establecida la configuración deseada, haga clic en **Guardar cambios** y a continuación en **Comenzar descarga**.

## 4.- Despliegue con la herramienta de distribución automática

Al ejecutar el archivo que ha descargado se abrirá la herramienta de distribución automática. Esta herramienta le permite seleccionar los equipos de su red en los que desee realizar la auditoría. Puede hacerlo de dos maneras:

- Seleccionando los dominios o los equipos concretos que desee en el árbol que muestra la estructura de su red.
- Indicando el nombre o la dirección IP de los equipos en los que desee lanzar la auditoría.



### Despliegue por dominios

- Haga clic en **Nuevo análisis**.
- Seleccione **Por dominios**.
- Seleccione los dominios de la red que desee analizar. Puede optar por analizar todos los equipos del dominio, o seleccionar equipos concretos marcando las casillas que desee.
- Opcionalmente, puede indicar un nombre de usuario y una contraseña con privilegios de administrador en los equipos analizar. Si opta por no indicar estos datos ahora, la aplicación los solicitará cuando lo necesite más adelante. Es aconsejable utilizar una contraseña de administrador de dominio. De este modo, no tendrá que



indicar el nombre de usuario y la contraseña de cada equipo.

- Haga clic en **Aceptar**.

## Despliegue por IP o nombre de equipo

- Haga clic en **Por IP o nombre de equipo**.
- Indique los equipos que desee analizar. Puede indicar los nombres de los equipos, sus direcciones IP o rangos de IP, separando estos datos con comas. Por ejemplo: 127.0.0.1, EQUIPO01, 192.0.17.1-192.0.17.128.
- Una vez indicados los datos que desee haga clic en **Añadir**.
- Opcionalmente, puede indicar un nombre de usuario y contraseña con privilegios de administrador en los equipos a analizar. Si opta por no indicar estos datos ahora, la aplicación los solicitará cuando los necesite más adelante. Es aconsejable utilizar una contraseña de administrador de dominio. De este modo, no tendrá que indicar el nombre de usuario y la contraseña de cada equipo.
- Haga clic en **Aceptar**.

Panda Malware Radar necesita conocer el nombre de usuario y la contraseña de administrador de los equipos en los que desea distribuir el programa de análisis. Si desea utilizar unas credenciales por defecto para todos los equipos (por ejemplo, una contraseña de dominio), puede indicar estos datos en la configuración de la herramienta de distribución antes de lanzar el análisis.

**Nota:** Si no indica estos datos antes de lanzar el análisis, Panda Malware Radar se los pedirá cuando los necesite.

Una vez seleccionados los equipos, haga clic en **Lanzar análisis**.

## 5.- Despliegue manual

Panda Malware Radar le permite realizar auditorías en equipos que carecen de conexión a Internet y que no se encuentran conectados en red, o en redes locales en las que ninguno de los equipos dispone de conexión a Internet. Si desea utilizar otras herramientas de distribución (SMS, Tivoli, etc.), deberá seguir también las instrucciones especificadas abajo.

**Notas:**

La herramienta de distribución de Panda Malware Radar sólo puede utilizarse en un equipo con conexión a Internet, independientemente de que el resto de equipos de la red dispongan de dicha conexión.

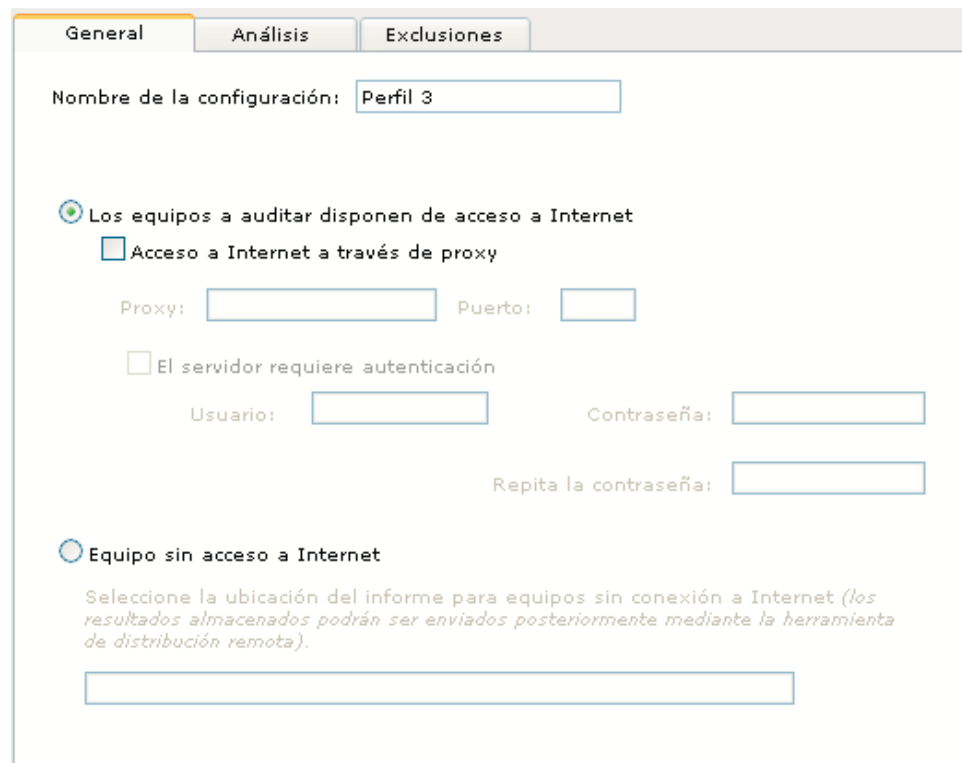
Para más información sobre la distribución utilizando otras herramientas, consulte la documentación de la herramienta que desee utilizar.

Siga estos pasos:

1. En la ficha **Estado** o **Auditorías**, haga clic en **Comenzar auditoría** (si no existe una auditoría creada previamente haga clic en **Crear nueva auditoría**).
2. Haga clic en **Desplegar manualmente o utilizar otras herramientas** para descargar el programa de análisis.
3. Haga clic en **Nueva configuración** y seleccione la opción **Equipos sin acceso a Internet**. Indique la ruta donde desee que se guarde el informe de la auditoría. Existen dos posibilidades:
  - Puede indicar una ruta local donde desea que se guarde el informe de auditoría del equipo. Por ejemplo, C:\Informes.
  - Si se trata de una red local en la que ninguno de los equipos tiene conexión a Internet, indique un recurso compartido de dicha red local sin conexión a Internet, en el que desee que se genere el informe. Por ejemplo, \\xxx\informes (donde XXX es el nombre del equipo en el que se guardará el informe en cuestión).

4. Haga clic en **Guardar cambios**.

5. Haga clic en **Comenzar descarga**.



General | **Análisis** | Exclusiones

Nombre de la configuración: Perfil 3

Los equipos a auditar disponen de acceso a Internet

Acceso a Internet a través de proxy

Proxy:  Puerto:

El servidor requiere autenticación

Usuario:  Contraseña:

Repita la contraseña:

Equipo sin acceso a Internet

Seleccione la ubicación del informe para equipos sin conexión a Internet (los resultados almacenados podrán ser enviados posteriormente mediante la herramienta de distribución remota).

Una vez descargado el programa de análisis, ejecútelo en cada uno de los equipos a auditar. Para ver los resultados una vez concluido el proceso, es necesario copiar el archivo .DAT y la carpeta que se habrá generado con el mismo nombre que este fichero de cada máquina auditada a un ordenador con conexión a Internet y enviarlo a los servidores de Panda Malware Radar **utilizando la herramienta de distribución**.

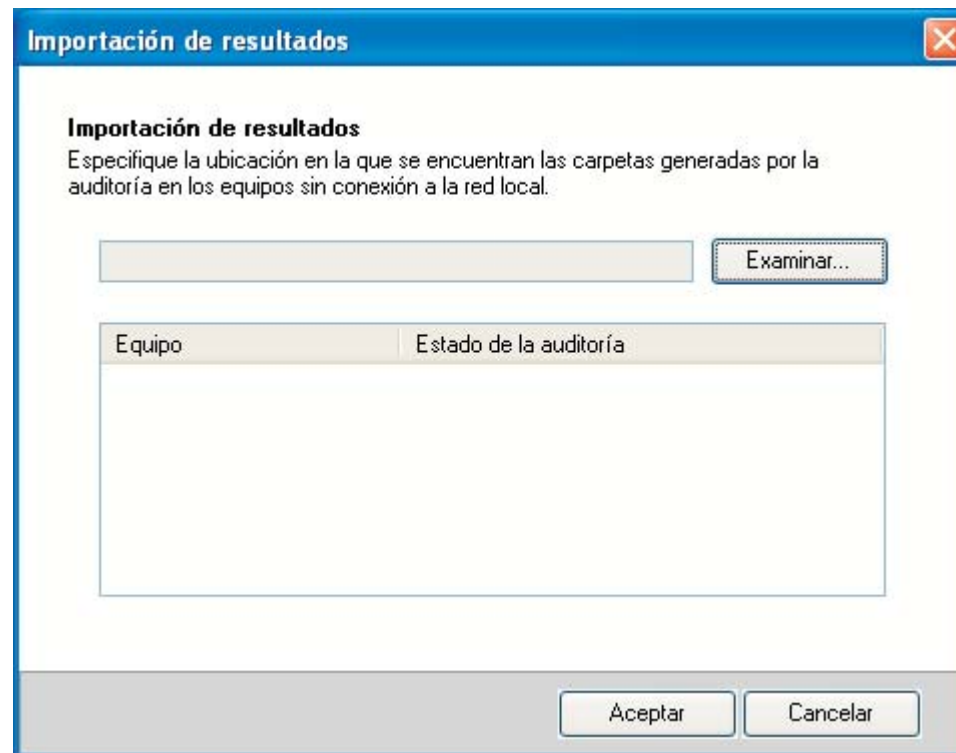


Puede descargar la herramienta de distribución siguiendo estos pasos:

1. En la ficha **Auditorías** haga clic en **Comenzar auditoría**.
2. Haga clic en **Utilizar herramienta de distribución automática**.
3. Seleccione una de las configuraciones que pueda haber establecido anteriormente, o cree una nueva.
4. Asegúrese de que se encuentra marcada la opción **Los equipos a auditar disponen de conexión a Internet**. Si la conexión se realiza a través de un servidor proxy deberá indicar también su dirección IP, puerto y contraseña (si es necesario).
5. Guarde los cambios y haga clic en **Comenzar descarga**.

A continuación, debe importar el informe siguiendo estos pasos:

1. Ejecute la herramienta de distribución automática y haga clic en **Importar resultados**.
2. Haga clic en **Examinar** y localice el directorio que contiene el archivo .DAT y la carpeta que se habrá generado con el mismo nombre que este fichero.
3. Haga clic en Aceptar para realizar el envío.



Una vez finalizada la recogida de datos, para ver el informe, acceda a la ficha **Monitorización** de la consola y haga clic en **Ver informes de Auditoría**. También puede hacerlo directamente mediante la opción **Informes** de la consola.

## 6.- Monitorización de análisis y desinfección

La segunda fase de las auditorías consiste en la monitorización. La monitorización ofrece información sobre el estado de los análisis, y se divide en varios apartados:



[Desconectar](#) [Español](#) | [English](#)  
 Usuario: MR

[Estado](#) **Auditorías** [Histórico](#) [Audit info](#) [FAQ](#) [Tienda](#)

[1 Despliegue](#) **2 Monitorización** [3 Informes](#) [4 Limpieza](#)

**Auditoría {1D631D11-3444-44B2-9825-5B59CF482819}**  
 Fecha inicio: 02/05/2007 10:52  
 Fecha cierre: --/--/-- --:--:--  
[Cancelar auditoría](#)

**1 Análisis**

**Equipos distribuidos:** [1](#)  
**Análisis finalizados:** [1](#)  
 Con éxito [1](#)  
 Con alertas [0](#)  
**Análisis en curso:** [0](#)

**2 Estudio de laboratorio**

**Pendiente**  
**Archivos sospechosos:** [0](#)  
 Pendientes [0](#)  
 Analizados [0](#)  
**PCs afectados:** [0](#)

**3 Resultados**

**Pendiente**  
 Debe finalizarse la adquisición de datos y análisis de los equipos, así como el estudio de laboratorio para disponer de resultados de la auditoría.  
[+ info](#)  
[Ver informes de Auditoría](#)

**Etapa de análisis**  
 Datos obtenidos el 02/05/2007 a las 10:56 [Actualizar datos](#)

- No se ha encontrado código malicioso en su parque.
- El 0% de su parque tiene código malicioso activo.
- No se ha podido encontrar una protección óptima en el 100% de su parque.

Cuando considere que el volumen de datos recogidos es suficientemente representativo del estado de su organización o no desee continuar con el proceso de adquisición de datos, **finalice manualmente la etapa de análisis**.

[Finalizar recogida de datos](#)

**Códigos maliciosos encontrados:**

Tipo	Activas	Latentes	PCs afectados
Virus, gusanos y troyanos	0	0	0
Spyware	0	0	0
Adware	0	0	0
Otros	0	0	0
Total	0	0	0

**Nivel de protección de su parque:**

Protección	PCs	Detecciones	
		Activas	Latentes
Óptima	0 (0%)	0	0
Óptima no detectada	<a href="#">1</a> (100%)	0	0

**Vulnerabilidades críticas:**

Vulnerabilidades	PCs	Detecciones	
		Activas	Latentes
<a href="#">39</a>	<a href="#">1</a> (100%)	0	0

[Guía de uso](#) © Panda Software 2007 | [Acuerdo de licencia](#)

- Etapa de análisis:** Muestra información pormenorizada sobre el estado de su parque informático: amenazas encontradas (activas y latentes), número de equipos afectados, nivel protección de su parque, vulnerabilidades encontradas, etc.

Una vez concluido el análisis en todos los equipos de la red, haga clic en **Finalizar etapa de análisis**.

**Nota importante:** Antes de finalizar la recogida de datos, es importante que no queden archivos sospechosos pendientes del análisis por parte de PandaLabs. De lo contrario, en caso de ser malware, estos archivos no se desinfectarán en la fase de limpieza.

- Análisis:** Le permite saber en qué equipos se han distribuido los programas de análisis, así como el número de análisis realizados. Si desea conocer el nombre de los equipos analizados y el dominio de red en el que se encuentran, haga clic en la cifras que aparecen a la derecha.
- Estudio del laboratorio:** PandaLabs, el laboratorio de virus de Panda, interviene en el proceso de análisis de procesos y archivos sospechosos. En esta sección puede conocer el número de archivos sospechosos que ha procesado el laboratorio, cuántos están pendientes de análisis, y los PC en los que hay archivos sospechosos.
- Resultados:** Es la fase de recogida de datos procedentes de los análisis. Si dispone de una versión de suscripción o de una auditoría única, puede consultar diferentes tipos de informes para conocer el estado de su organización. Haga clic en **Ver informes de auditoría (Ver informes de desinfección, si se trata de una limpieza)** para ver los resultados.



## 7.- Informes

Es muy importante conocer e interpretar correctamente los resultados para corregir cualquier situación de riesgo en la red y para planificar de forma acertada las estrategias de protección.

### Consulta de los resultados

Si dispone de una versión de suscripción o auditoría única puede consultar los resultados detallados de la auditoría a través de los diferentes tipos de informes:

- **Informe ejecutivo:** Muestra el informe de la situación general: número de amenazas activas y latentes detectadas, estadísticas, recomendaciones, etc.
- **Informe técnico:** Muestra el informe completo con todos los datos del análisis realizado en cada uno de los equipos auditados.
- **Informe técnico de desinfección:** Muestra el resultado de la limpieza de su parque informático, y detalla el número de amenazas activas y latentes que han sido detectadas y eliminadas, así como su nivel peligrosidad, su ubicación, etc.

Una vez finalizada la auditoría puede enviarla al histórico donde podrá volver a consultar los informes cuando desee. En el histórico también podrá generar informes consolidados con los datos de esta auditoría y los de otras que ya pudieran encontrarse en el histórico.

### Descarga de los resultados

Además de observar los informes en pantalla, puede descargarlos en formato PDF o XML.

#### Descargar informe ejecutivo y datos de la auditoría

Puede generar un informe ejecutivo en PDF y descargar los datos de la auditoría en XML. Para ello haga clic en la opción **Generar informe** correspondiente al informe que desea descargar y espere unos segundos a que aparezca el enlace de descarga.

#### Descargar informe técnico o informe de desinfección

Si desea descargar un informe técnico o un informe de desinfección en PDF podrá seleccionar los equipos sobre los que desee que se genere el informe. De este modo, puede evitar informes excesivamente extensos, obteniendo exclusivamente los datos que le interesan. Puede hacerlo siguiendo estos pasos:



1. Haga clic en la opción **Generar informe** que aparece a la derecha de **Informe técnico** o **Informe de desinfección**.
2. Seleccione en la lista desplegable los equipos sobre los que desee generar un informe. Puede seleccionar todos los equipos, o únicamente aquellos en los que se haya detectado malware (con diferentes niveles de peligrosidad), vulnerabilidades, etc.
3. Haga clic en **Buscar** y marque las casillas que correspondan con los equipos sobre los que desee ver el informe.
4. Haga clic en **Generar informe**, y aguarde unos segundos hasta que se genere el informe de descarga.

## 7.- Limpieza con la herramienta de distribución

Una vez realizado el análisis y revisados los informes, es el momento de proceder a la limpieza de su parque informático. Para ello es necesario distribuir un programa de desinfección en su red, siguiendo unos pasos similares a los realizados para distribuir el programa de análisis:

1. Acceda a la consola de Panda Malware Radar.
2. En la ventana **Estado** (o en la sección **Auditorías**) haga clic en **Comenzar limpieza**.
3. Indique cómo desea distribuir el programa de desinfección: utilizando la herramienta de distribución automática (recomendado en redes con al menos un equipo con conexión a Internet), de forma manual, o usando otras herramientas.

La **fase final** de las auditorías consiste en la limpieza de los equipos en los que se haya detectado algún tipo de código malicioso, ya sea conocido o desconocido. Para ello es necesario el **despliegue del programa de desinfección** en los equipos auditados. Dispone de varias posibilidades de despliegue:

**Utilizar Herramienta de distribución automática (Recomendado)**  
Distribuya automáticamente el programa de desinfección a aquellos equipos auditados descargando la **herramienta de distribución automática**. No es necesario que todos los equipos tengan conexión a Internet, basta con que uno de ellos pueda descargar el conjunto de herramientas y se comuniquen con el resto.

**Desplegar manualmente o utilizar otras herramientas**  
Descargue el **programa de desinfección** para realizar manualmente o con otras herramientas el proceso de despliegue en los equipos auditados. Utilice este tipo de despliegue en los equipos situados fuera de la red de área local.

[Ver monitorización](#)

4. Establezca la configuración que desee. Para más información consulte el apartado **Configuración**.
5. Haga clic en **Guardar cambios** y a continuación en **Comenzar descarga**.
6. Al ejecutar el archivo descargado se abre la herramienta de distribución.
7. Haga clic en **Nueva desinfección** y seleccione los equipos que desee desinfectar (sólo se mostrarán los equipos en los que se haya realizado un análisis).



8. Opcionalmente, puede introducir un nombre de usuario y una contraseña con privilegios de administrador en los equipos que desea desinfectar. Esto es aconsejable si conoce la contraseña de administrador de dominio, ya que de este modo no tendrá que indicar las credenciales de cada uno de los equipos a desinfectar. Si no indica estos datos ahora, Panda Malware Radar se los solicitará cuando los necesite más adelante.

9. Haga clic en **Desinfectar**.

Para ver los resultados de la desinfección, regrese a la consola siguiendo estos pasos:

1. En la pestaña **Estado** (o **Auditorías**) haga clic en **Monitorizar desinfección**. Esto mostrará el resultado de la limpieza.

2. Una vez desinfectados todos los equipos, haga clic en **Finalizar etapa de desinfección**.

**Nota importante:** Antes de finalizar la etapa de desinfección, es importante que no queden equipos pendientes de análisis. Una vez finalizada esta etapa no se podrá volver a realizar la limpieza.

3. Haga clic en **Ver informes de desinfección**. Consulte el apartado Informes para obtener más información.

Si lo desea, también puede archivar la auditoría en el histórico haciendo clic en el botón correspondiente. Consulte el apartado **Histórico** para obtener más información.

The screenshot shows the Panda Malware Radar interface for an automated malware audit. The main content area is titled 'Etapa de desinfección' (Disinfection Stage) and shows the following information:

- Auditoría {1D631D11-3444-44B2-9825-5B59CF482819}**
- Fecha inicio: 02/05/2007 10:52
- Fecha cierre: --/-- --:--

Progress indicators show:

- 1 Desinfección:** Equipos distribuidos: 1, Desinfecciones finalizadas: 1 (Con éxito), 0 (Con alertas), Desinfecciones en curso: 0.
- 2 Resultados:** Pendiente. Debe finalizarse la etapa de desinfección de los equipos para disponer de los resultados. A button 'Ver informes de desinfección' is visible.

Summary information:

- Datos obtenidos el 02/05/2007 a las 12:13
- Ningún equipo finalizó la desinfección con alertas.
- Finalizar etapa de desinfección button.

Summary tables:

**Códigos maliciosos activos desinfectados:**

Peligrosidad	Con éxito	Con alertas	PCs afectados
Muy alta	0	0	0
Alta	0	0	0
Moderada	0	0	0
Baja	0	0	0

**Códigos maliciosos latentes desinfectados:**

Peligrosidad	Con éxito	Con alertas	PCs afectados
Muy alta	0	0	0
Alta	0	0	0
Moderada	0	0	0
Baja	0	0	0

Footer: Guía de uso | © Panda Software 2007 | Acuerdo de licencia



## 8.- Limpieza manual

Para realizar la limpieza en redes sin conexión a Internet es necesario descargar el **programa de desinfección** y ejecutarlo en cada uno de los equipos que desee limpiar. Para ello siga estos pasos:

1. Acceda a la consola de Panda Malware Radar.
2. En la ventana **Estado** (o en la sección Auditorías) haga clic en **Comenzar limpieza**.
3. Haga clic en **Desplegar manualmente o utilizar otras herramientas**.
4. Indique la ruta donde desee que se guarde el informe de la limpieza. Existen dos posibilidades:
  - Puede indicar una ruta local donde desea que se guarde el informe de auditoría del equipo. Por ejemplo, C:\Informes.
  - Si se trata de una red local sin conexión a Internet en la que ninguno de los equipos tiene conexión a Internet, indique un recurso compartido de dicha red en el que desee que se genere el informe. Por ejemplo, \\xxx\informes (donde XXX es el nombre del equipo en el que se guardará el informe en cuestión).

### Equipo sin acceso a Internet

Seleccione la ubicación del informe para equipos sin conexión a Internet (los resultados almacenados podrán ser enviados posteriormente mediante la herramienta de distribución remota).

5. Establezca la configuración que desee. Para más información consulte el apartado **Configuración**.

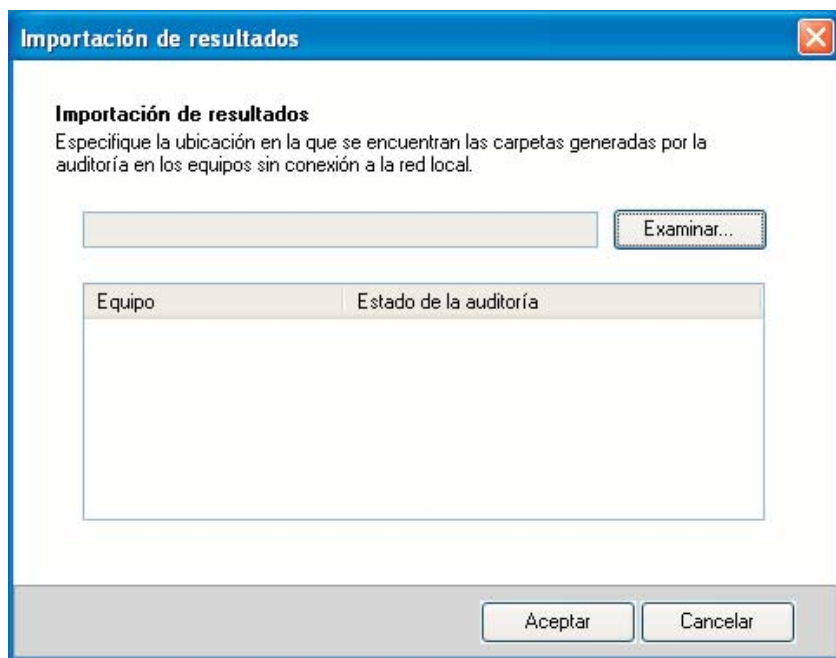
6. Haga clic en **Guardar cambios**.

7. Haga clic en **Comenzar descarga**.

Una vez descargado el programa de desinfección, ejecútelo en cada uno de los equipos a desinfectar. Para ver los resultados una vez concluido el proceso, es necesario copiar el archivo .DAT y la carpeta que se habrá generado con el mismo nombre que este fichero de cada máquina auditada a un ordenador con conexión a Internet. De este modo podrá enviarlo a los servidores de Panda Malware Radar **utilizando la herramienta de distribución**.

Puede descargar la herramienta de distribución siguiendo estos pasos:

1. Acceda a la ficha **Auditorías** y haga clic en **Comenzar limpieza**.
2. Haga clic en **Utilizar herramienta de distribución automática**.
3. Seleccione una de las configuraciones que pueda haber establecido anteriormente, o cree una nueva.
4. Asegúrese de que se encuentra marcada la opción **Los equipos a auditar disponen de conexión a Internet**. Si la conexión se realiza a través de un servidor proxy deberá indicar también su dirección IP, puerto y contraseña (si es necesario).
5. Guarde los cambios y haga clic en **Comenzar descarga**.



A continuación, debe importar el informe siguiendo estos pasos:

1. Ejecute la herramienta de distribución automática y haga clic en **Importar resultados**.
2. Haga clic en **Examinar** y localice el directorio que contiene el archivo .DAT y la carpeta que se habrá generado con el mismo nombre que este fichero.
3. Haga clic en **Aceptar** para realizar el envío.

Para ver los resultados de la desinfección, regrese a la consola siguiendo estos pasos:

1. En la pestaña **Estado** (o **Auditorías**) haga clic en **Monitorizar desinfección**. Esto mostrará el resultado de la limpieza.
2. Una vez concluido el proceso de desinfección en todos los equipos haga clic en **Finalizar etapa de desinfección**.
3. Haga clic en **Ver informes de desinfección**. Consulte el apartado Informes para obtener más información.

Si lo desea, también puede archivar la auditoría en el histórico haciendo clic en el botón correspondiente.



## Histórico

Las auditorías que ya han finalizado pueden ser almacenadas en un archivo histórico para su posterior consulta. Si ya dispone de auditorías almacenadas en modo histórico, haga clic en el enlace **Ver** de la columna **Resultados** para conocer la información detallada.

Si lo desea, puede crear un informe combinado de todas las auditorías realizadas. Este informe recibe el nombre de **Informe consolidado**.

Siga estos pasos para crear un informe consolidado:

1. En la tabla de auditorías históricas, active las casillas situadas al comienzo de las líneas que recogen la información de las auditorías que desee y haga clic en **Generar informe consolidado**.
2. El informe consolidado tardará cierto tiempo en generarse, dependiendo del número de equipos que se han auditado. Haga clic en **Actualizar estado** cada cierto tiempo, hasta que compruebe que el botón **Descargar informe consolidado** se ha activado.
3. Haga clic en **Descargar informe consolidado**.

## Más información

Si desea obtener más información sobre Panda Malware Radar, puede consultar:

- [El área de preguntas frecuentes \(Para acceder a esta sección deberá identificarse previamente con su nombre de usuario y contraseña.\)](#)
- [La ayuda del programa](#)
- [Otros recursos](#)

## Soporte técnico

Todas las versiones de Panda Malware Radar disponen de soporte técnico telefónico y soporte por correo electrónico. Puede obtener la información de contacto de la delegación de Panda Security más próxima en la siguiente dirección:

<http://www.pandasecurity.com/spain/about/contact>