INFORME ASSESSMENT PLATAFORMA DE ANTIVIRUS CLOUD – TRELLIX EPO MVISION

Preparado para:

AERONÁUTICA CIVIL
Unidad Administrativa Especial

BOGOTÁ
2022

RENOVACIÓN DE LICENCIA

Producto adquirido: MVISION Protect Standard

Cantidad de licencias: 3000

Número de concesión: 17728123-NAI

Fecha de inicio: 20/09/2022

Fecha de finalización: 19/09/2023

Servicio	Utilizadas
MVISION Endpoint	0
Device Control	0
Threat Prevention	2928
Firewall	11
Web Control	2926
ATP	2927

MVISION Protect Standard	3000

CONSUMO DE RECURSOS

Se debe tener claro que el antivirus se encarga de analizar la información que se cree, modifique, descargue, elimine y demás acciones con ayuda del módulo ATP (Adaptative Threat Prevention).

El antivirus usualmente puede consumir en equipos que dispongan de una memoria RAM de 4GB, 8GB y 16 GB un total de 300 o 350 MB físicas.

Por otro lado, si se comienza un proceso de traslado de información en un servidor, es necesario que se notifique al administrador de la consola para aplicar las exclusiones necesarias y no afectar el performance del equipo.

Es de aclarar que el antivirus de igual forma se encarga de monitorear incluso la navegación web de los usuarios, aquí entra a cumplir un rol importante el módulo de web control ya que este puede indicar cuales sitios son de confianza para que el usuario pueda acceder sin que esto represente un peligro con su información.

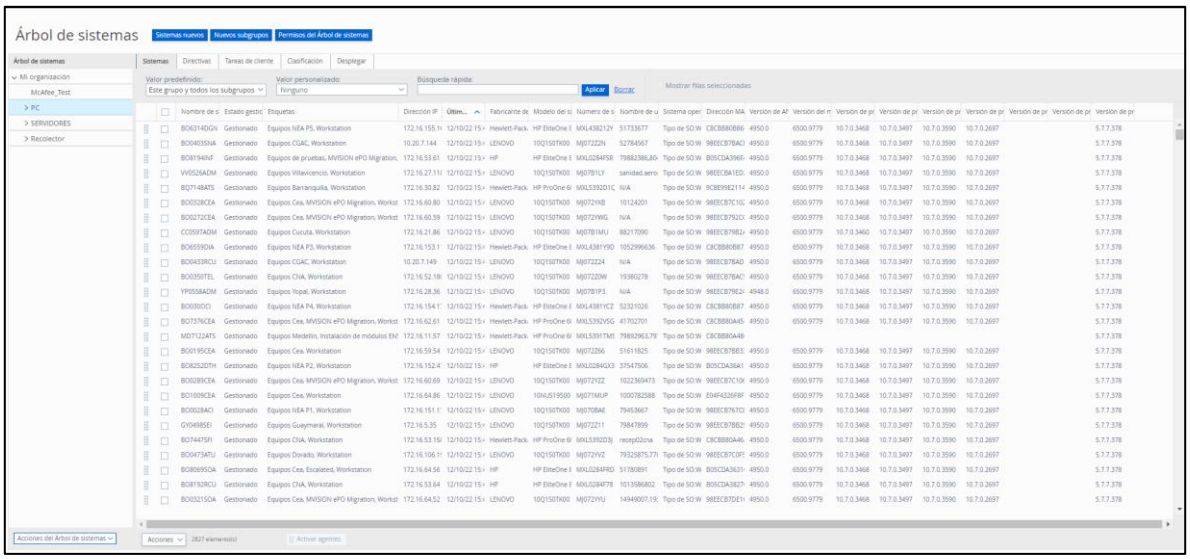
Desde el módulo TP (Threat Prevention) podemos validar bajo las directivas de análisis en tiempo real y análisis bajo demanda, las configuraciones correspondientes a solucionar problemas de perfomance en un equipo bien sea una estación de trabajo o servidor de la entidad.

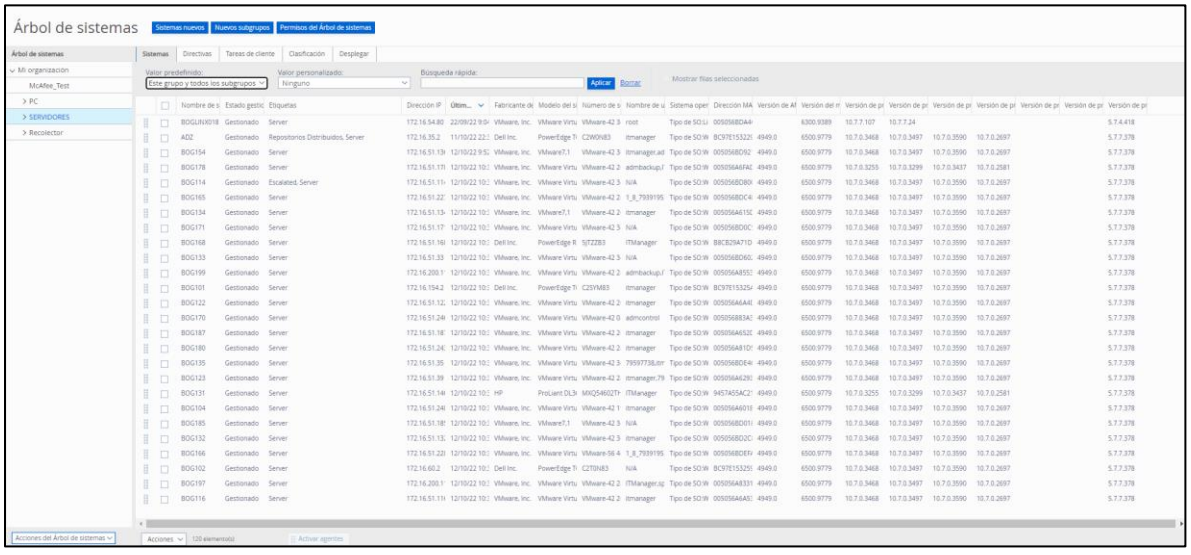
Si el consumo del servicio ***Trellix Agent Service*** sobrepasa el umbral de 300 MB en memoria, es necesaria la intervención del administrador de consola para analizar en tiempo real que puede estar ocurriendo con el sistema.

SUPERFICIE PROTEGIDA

Actualmente el antivirus mantiene un alcance a nivel de Endpoints de 2938 equipos. Estos se encuentran categorizados por regionales que a diario se están actualizando con el renombramiento de equipos o la integración de nuevos equipos a la entidad.

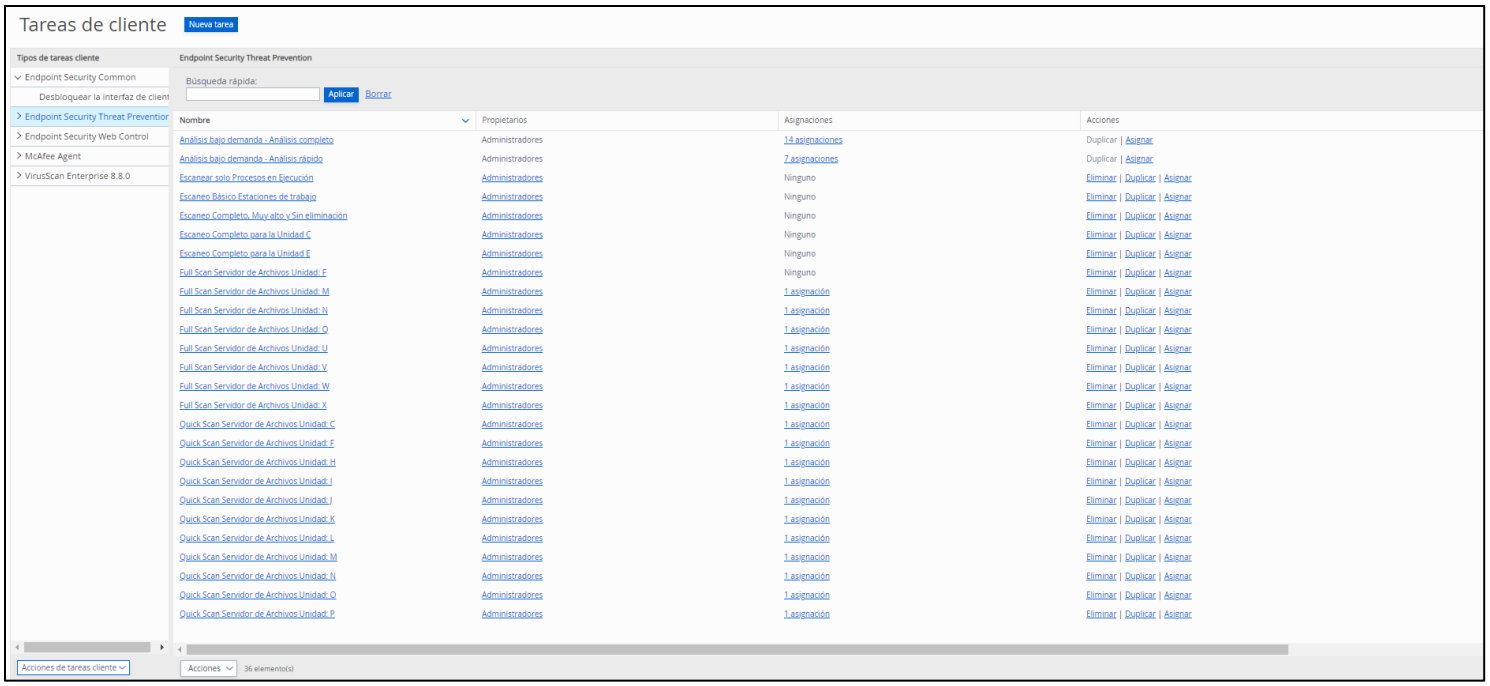
- Estaciones de trabajo: 2818 equipos
- Servidores: 120 equipos (servidor Linux BOGLINX018)

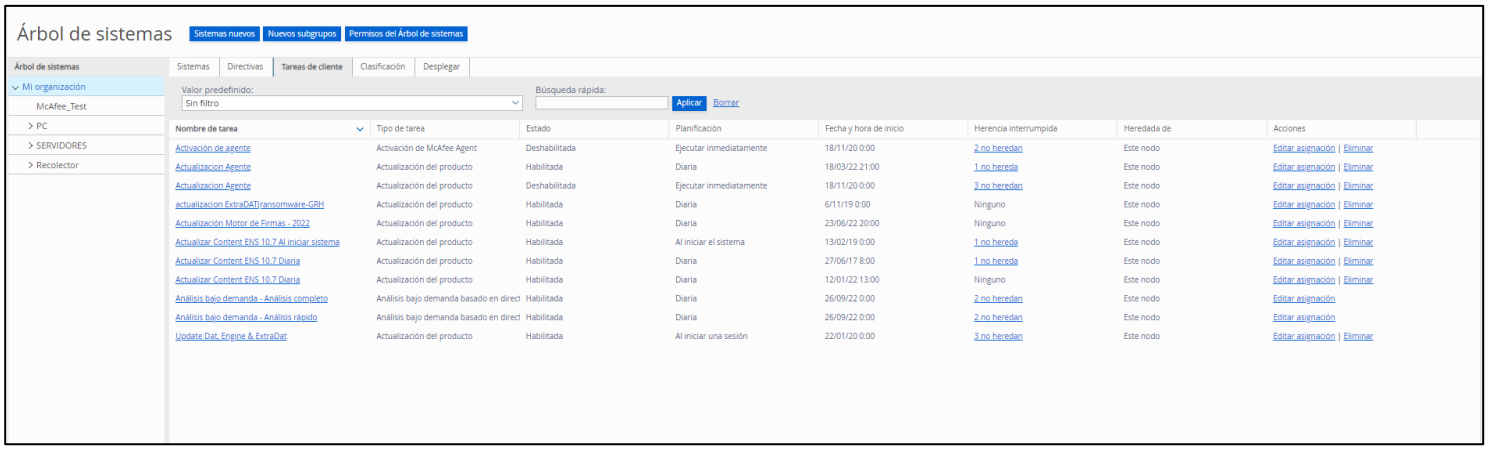




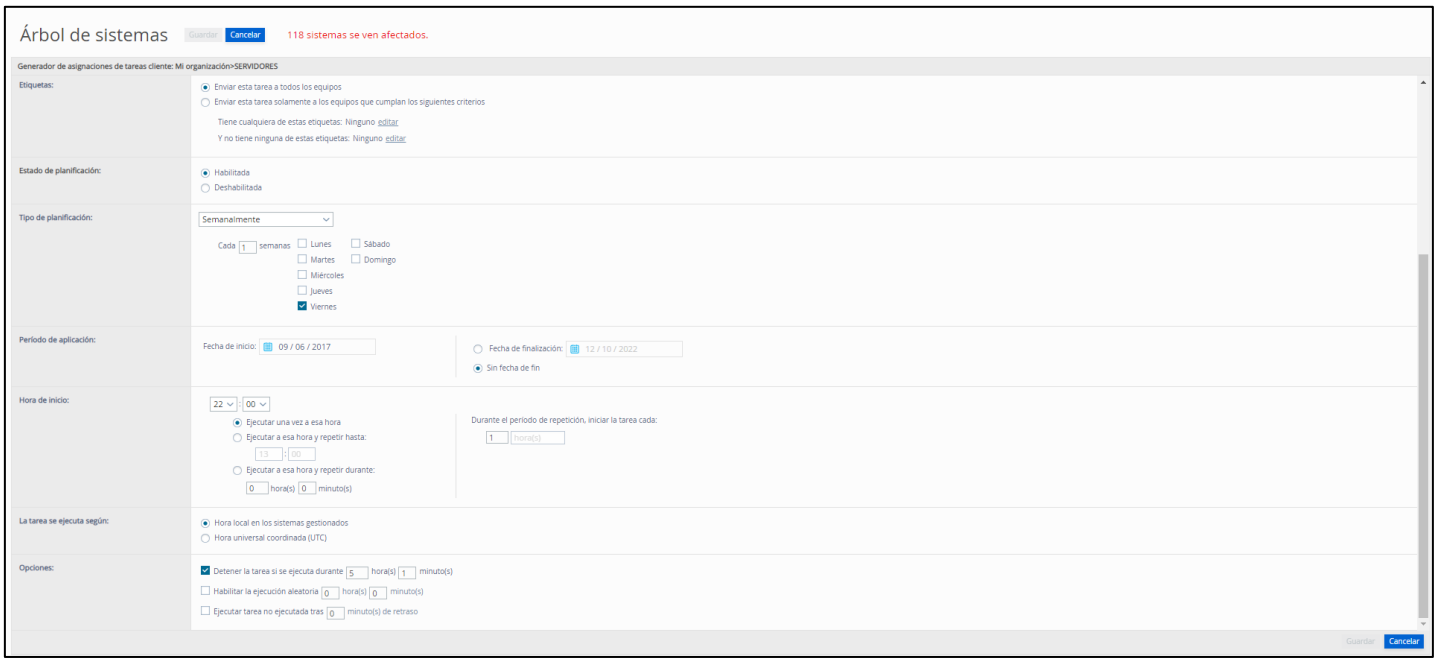
TAREAS CLIENTE

Actualmente se tienen configuradas una serie de tareas cliente que comprenden desde la directiva Threat Prevention los tipos de análisis y escaneos, basados según las necesidades de la entidad.

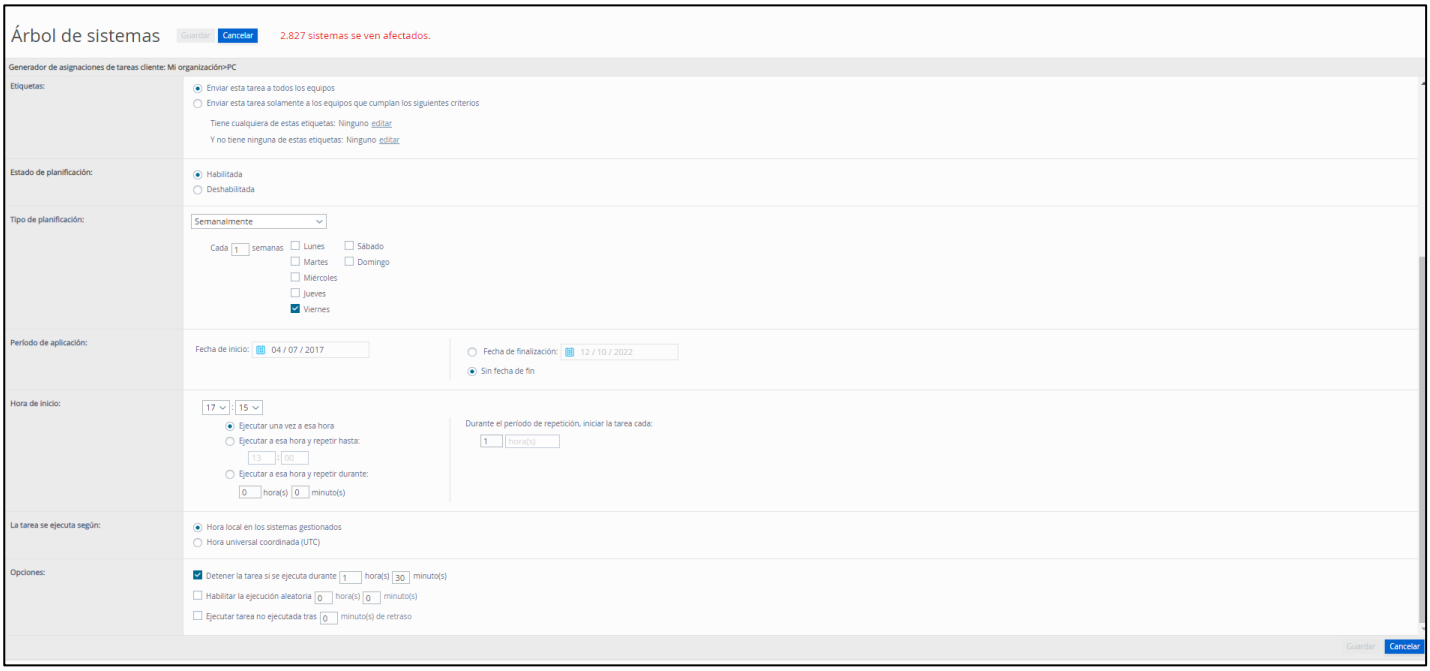




Para los análisis completos en los servidores, se ha dejado una configuración semanal para que esta tarea se ejecute solamente el viernes a las 10:00 p.m. Se tiene una contramedida que indica que si la ejecución del análisis dura mas de 5 horas se detenga para evitar problemas a nivel de performance.



El análisis completo en las estaciones de trabajo de igual forma que en los servidores, está propuesto para que se ejecute el viernes después de las 5:15 p.m. Si el análisis tiene una duración superior a 1 hora y media este se detendrá automáticamente.



TAREAS SERVIDOR

Se tienen actualmente 3 tareas implementadas en la consola **ePO MVISION**. Las tres tares configuradas se encargan de:

- Activar los agentes diariamente. Este proceso está configurado para que se realice cada 15 minutos.

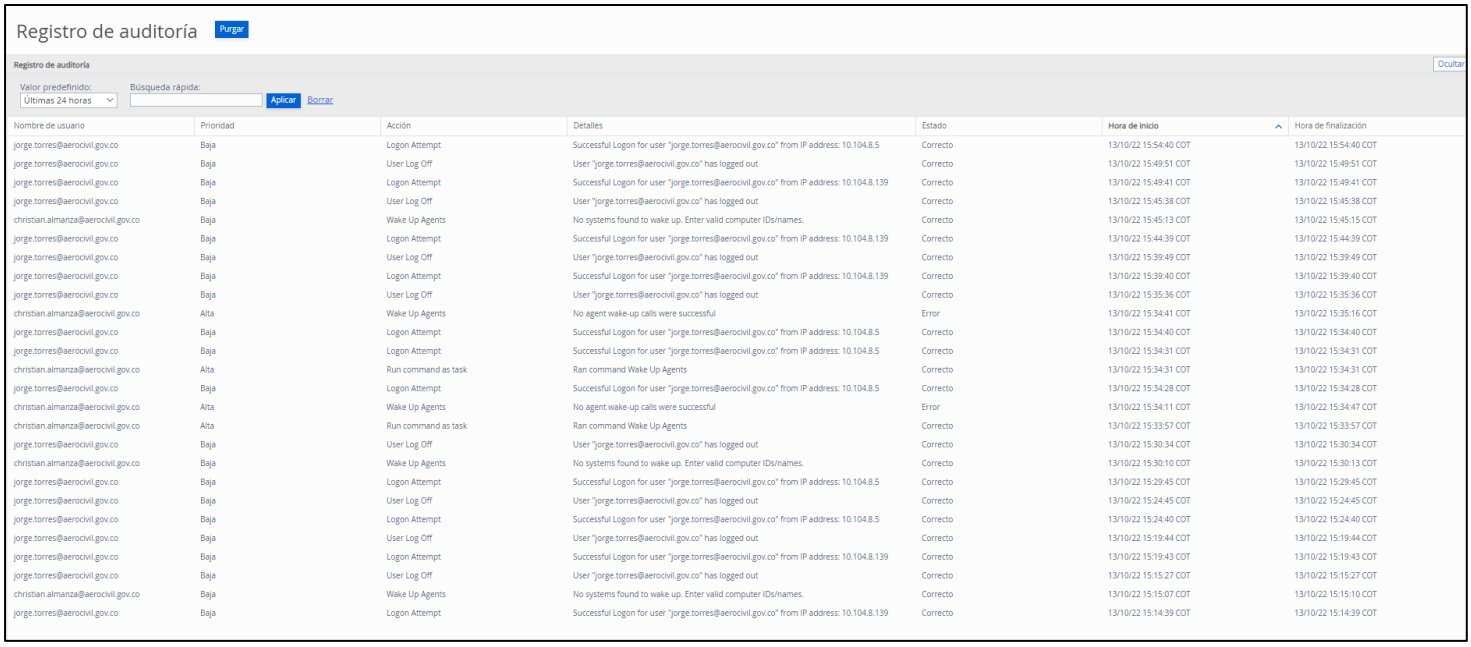
- Se ha configurado una consulta que nos comparte al momento de ejecutarla, los equipos que se encuentran actualmente con nombre duplicado. Su ejecución se realiza diariamente a las 7:00 p.m.

- La tercera y última tarea servidor se envía semanalmente a los administradores de plataformas de la entidad. Este es un informe de conformidad que permite revisar a detalle el versionamiento de los agentes y módulos de ENS en los servidores de la entidad. Además de la última comunicación agente – consola.



REGISTRO DE AUDITORIA

Desde el registro de auditoría, se pueden monitorear las actividades que los administradores de la consola realizan a diario. Desde una eliminación o movimiento de equipo desde el árbol de sistemas, hasta la creación y ejecución de una tarea cliente o servidor a un grupo en particular.



Registro de auditoría Purgar

Registro de auditoría Ocultar

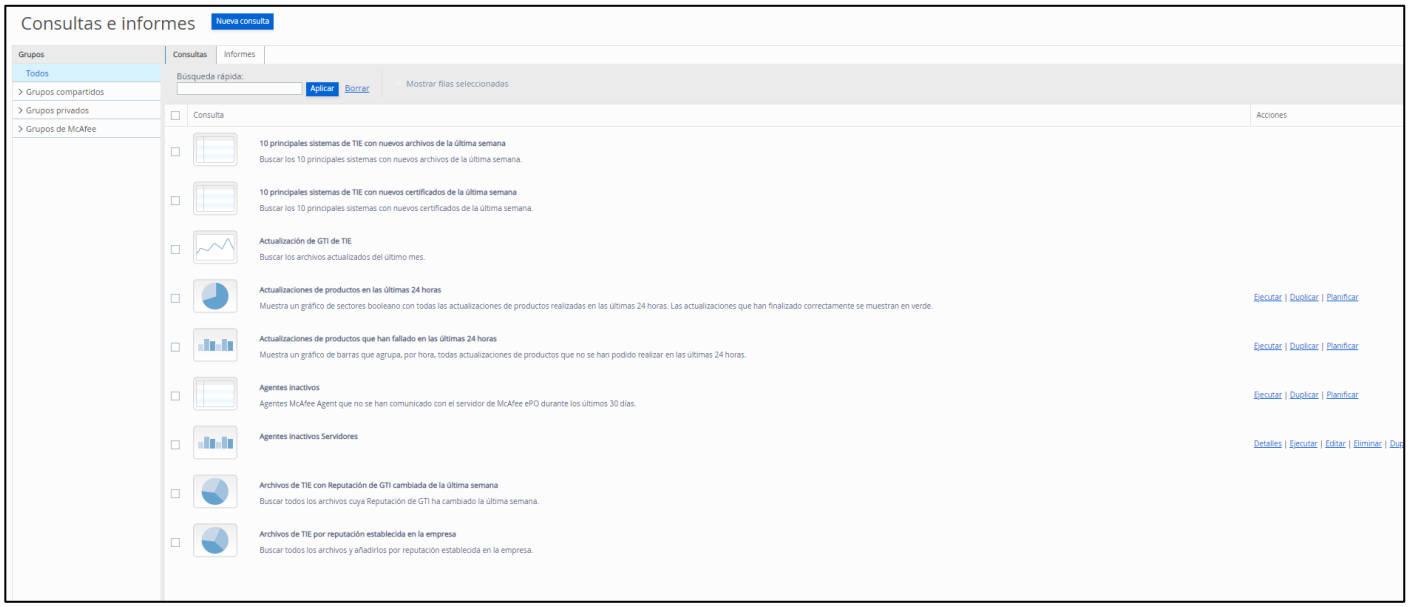
Valor predefinido: Últimas 24 horas | Búsqueda rápida: | Aplicar | Borrar

Nombre de usuario	Prioridad	Acción	Detalles	Estado	Hora de inicio	Hora de finalización
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.5	Correcto	13/10/22 15:54:40 COT	13/10/22 15:54:40 COT
jorge.torres@aerocivil.gov.co	Baja	User Log Off	User "jorge.torres@aerocivil.gov.co" has logged out	Correcto	13/10/22 15:49:51 COT	13/10/22 15:49:51 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.139	Correcto	13/10/22 15:49:41 COT	13/10/22 15:49:41 COT
jorge.torres@aerocivil.gov.co	Baja	User Log Off	User "jorge.torres@aerocivil.gov.co" has logged out	Correcto	13/10/22 15:45:38 COT	13/10/22 15:45:38 COT
christian.almanza@aerocivil.gov.co	Baja	Wake Up Agents	No systems found to wake up. Enter valid computer IDs/names.	Correcto	13/10/22 15:45:13 COT	13/10/22 15:45:15 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.139	Correcto	13/10/22 15:44:39 COT	13/10/22 15:44:39 COT
jorge.torres@aerocivil.gov.co	Baja	User Log Off	User "jorge.torres@aerocivil.gov.co" has logged out	Correcto	13/10/22 15:39:49 COT	13/10/22 15:39:49 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.139	Correcto	13/10/22 15:39:40 COT	13/10/22 15:39:40 COT
jorge.torres@aerocivil.gov.co	Baja	User Log Off	User "jorge.torres@aerocivil.gov.co" has logged out	Correcto	13/10/22 15:35:36 COT	13/10/22 15:35:36 COT
christian.almanza@aerocivil.gov.co	Alta	Wake Up Agents	No agent wake-up calls were successful	Error	13/10/22 15:34:41 COT	13/10/22 15:35:16 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.5	Correcto	13/10/22 15:34:40 COT	13/10/22 15:34:40 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.5	Correcto	13/10/22 15:34:31 COT	13/10/22 15:34:31 COT
christian.almanza@aerocivil.gov.co	Alta	Run command as task	Ran command Wake Up Agents	Correcto	13/10/22 15:34:31 COT	13/10/22 15:34:31 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.5	Correcto	13/10/22 15:34:28 COT	13/10/22 15:34:28 COT
christian.almanza@aerocivil.gov.co	Alta	Wake Up Agents	No agent wake-up calls were successful	Error	13/10/22 15:34:11 COT	13/10/22 15:34:47 COT
christian.almanza@aerocivil.gov.co	Alta	Run command as task	Ran command Wake Up Agents	Correcto	13/10/22 15:33:57 COT	13/10/22 15:33:57 COT
jorge.torres@aerocivil.gov.co	Baja	User Log Off	User "jorge.torres@aerocivil.gov.co" has logged out	Correcto	13/10/22 15:30:34 COT	13/10/22 15:30:34 COT
christian.almanza@aerocivil.gov.co	Baja	Wake Up Agents	No systems found to wake up. Enter valid computer IDs/names.	Correcto	13/10/22 15:30:10 COT	13/10/22 15:30:13 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.5	Correcto	13/10/22 15:29:45 COT	13/10/22 15:29:45 COT
jorge.torres@aerocivil.gov.co	Baja	User Log Off	User "jorge.torres@aerocivil.gov.co" has logged out	Correcto	13/10/22 15:24:45 COT	13/10/22 15:24:45 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.5	Correcto	13/10/22 15:24:40 COT	13/10/22 15:24:40 COT
jorge.torres@aerocivil.gov.co	Baja	User Log Off	User "jorge.torres@aerocivil.gov.co" has logged out	Correcto	13/10/22 15:19:44 COT	13/10/22 15:19:44 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.139	Correcto	13/10/22 15:19:43 COT	13/10/22 15:19:43 COT
jorge.torres@aerocivil.gov.co	Baja	User Log Off	User "jorge.torres@aerocivil.gov.co" has logged out	Correcto	13/10/22 15:15:27 COT	13/10/22 15:15:27 COT
christian.almanza@aerocivil.gov.co	Baja	Wake Up Agents	No systems found to wake up. Enter valid computer IDs/names.	Correcto	13/10/22 15:15:07 COT	13/10/22 15:15:10 COT
jorge.torres@aerocivil.gov.co	Baja	Logon Attempt	Successful Logon for user "jorge.torres@aerocivil.gov.co" from IP address: 10.104.8.139	Correcto	13/10/22 15:14:39 COT	13/10/22 15:14:39 COT

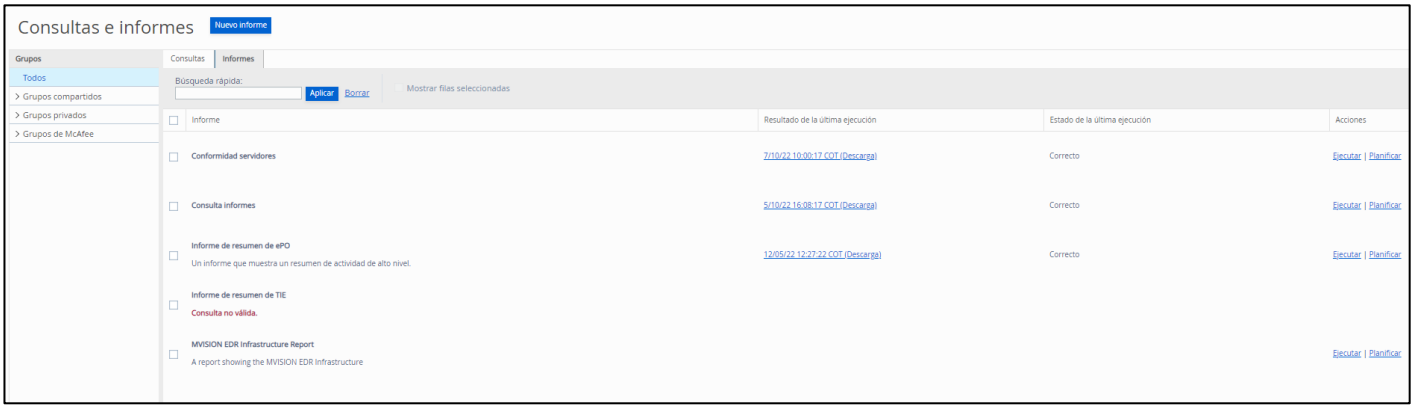
CONSULTA E INFORMES

Desde este apartado, podemos visualizar las consultas que ofrecen en primera instancia la información en tiempo real que va ligada con los eventos de amenazas, actualizaciones, desinstalaciones, despliegues de productos, acciones realizadas entre otras.

Adicionalmente, en las consultas se pueden aplicar las siguientes acciones: ejecutar, planificar, duplicar o editar los detalles. La información se comparte por lo general por medio de gráficos estadísticos que permiten detallar mucho más la información que se desea consultar.

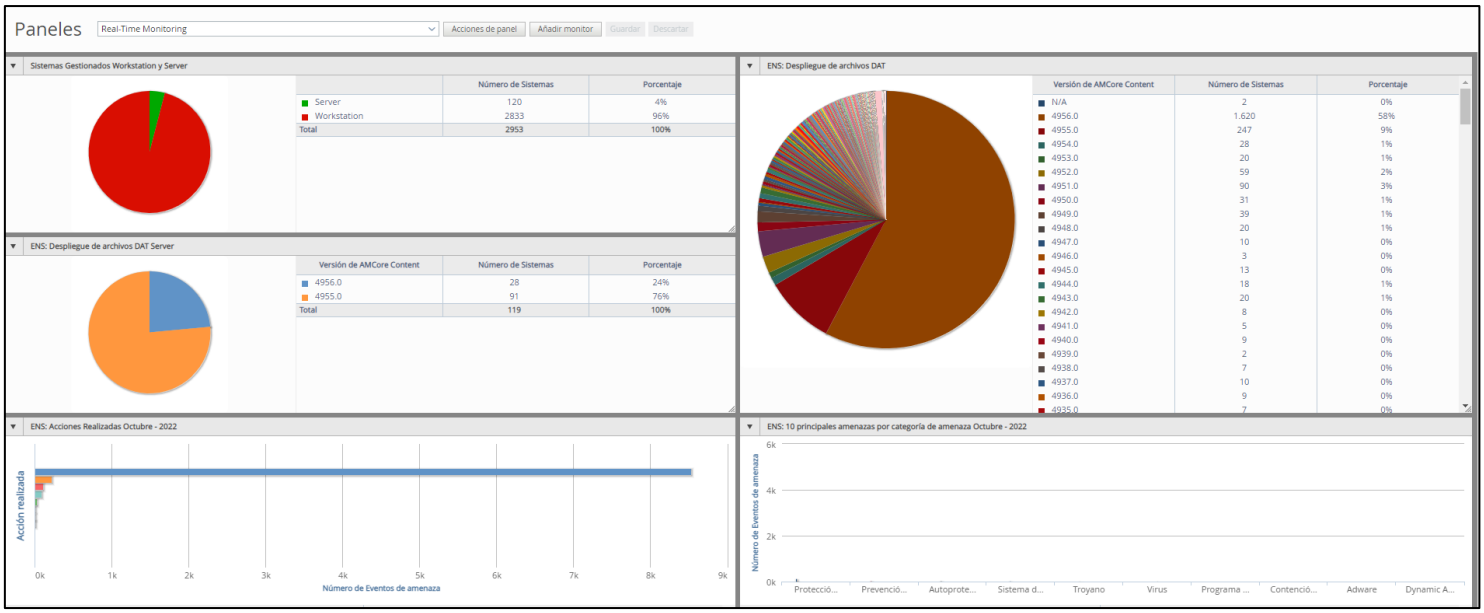


Desde la opción informes, se puede visualizar el informe de conformidad de servidores que semanalmente se ha estado enviando a los administradores de las plataformas como son AD y VMware. De igual forma, se permite la consulta del estado del análisis en tiempo real, protección de acceso y prevención de exploits.

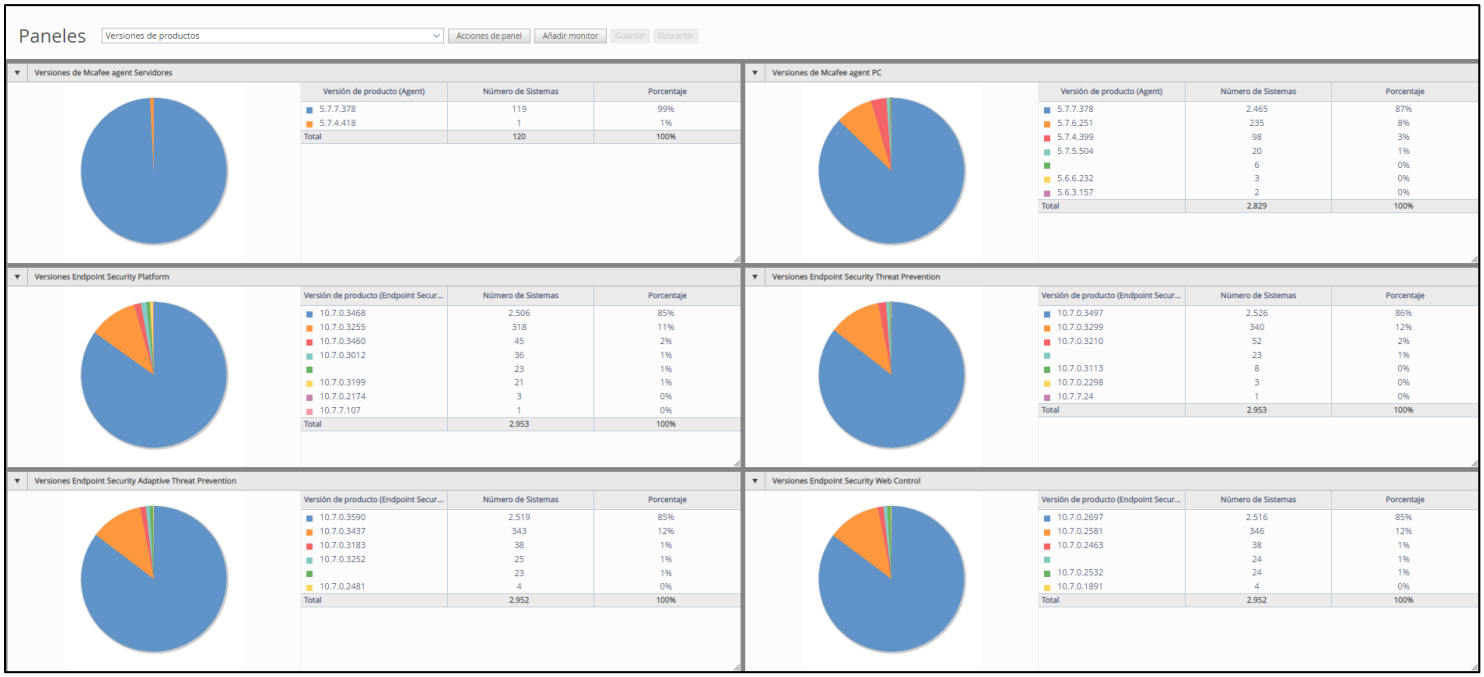


PANELES

Monitoreo en tiempo real

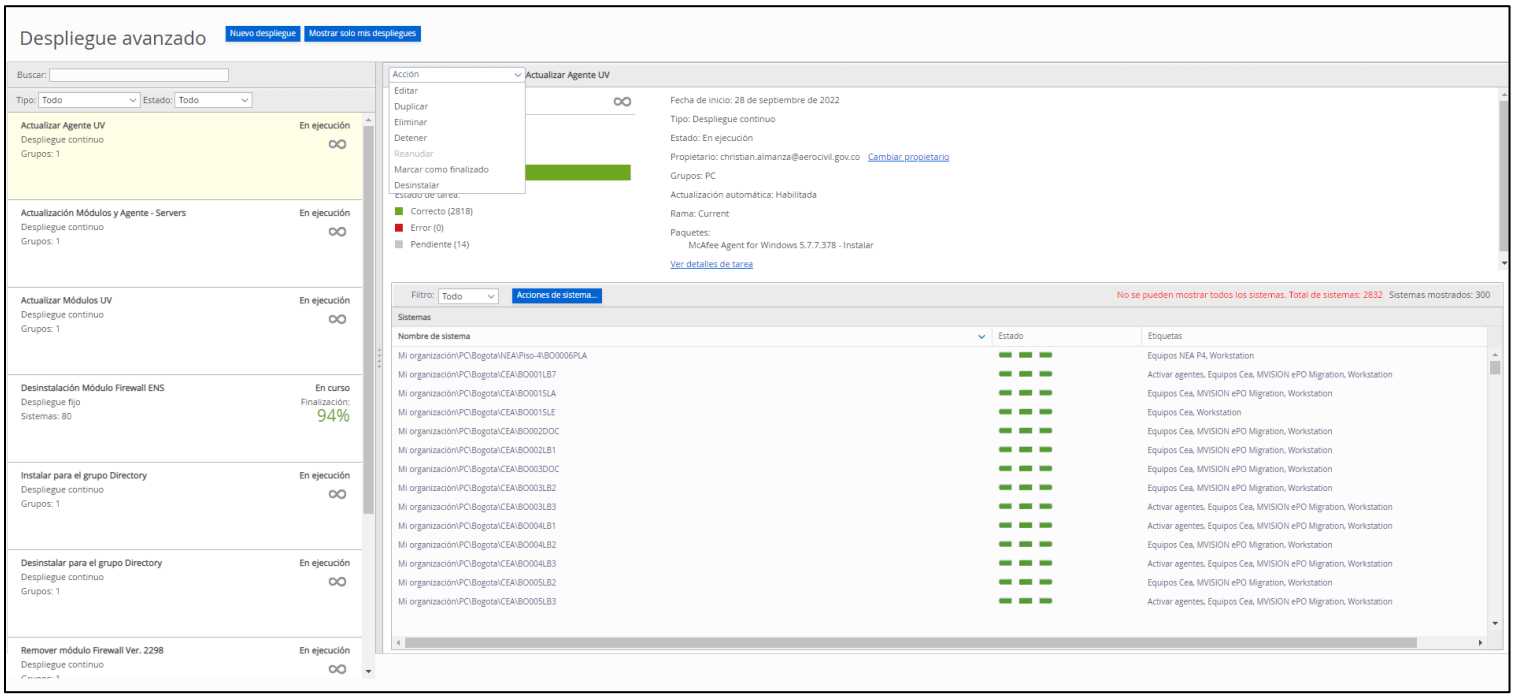


Versiones de productos



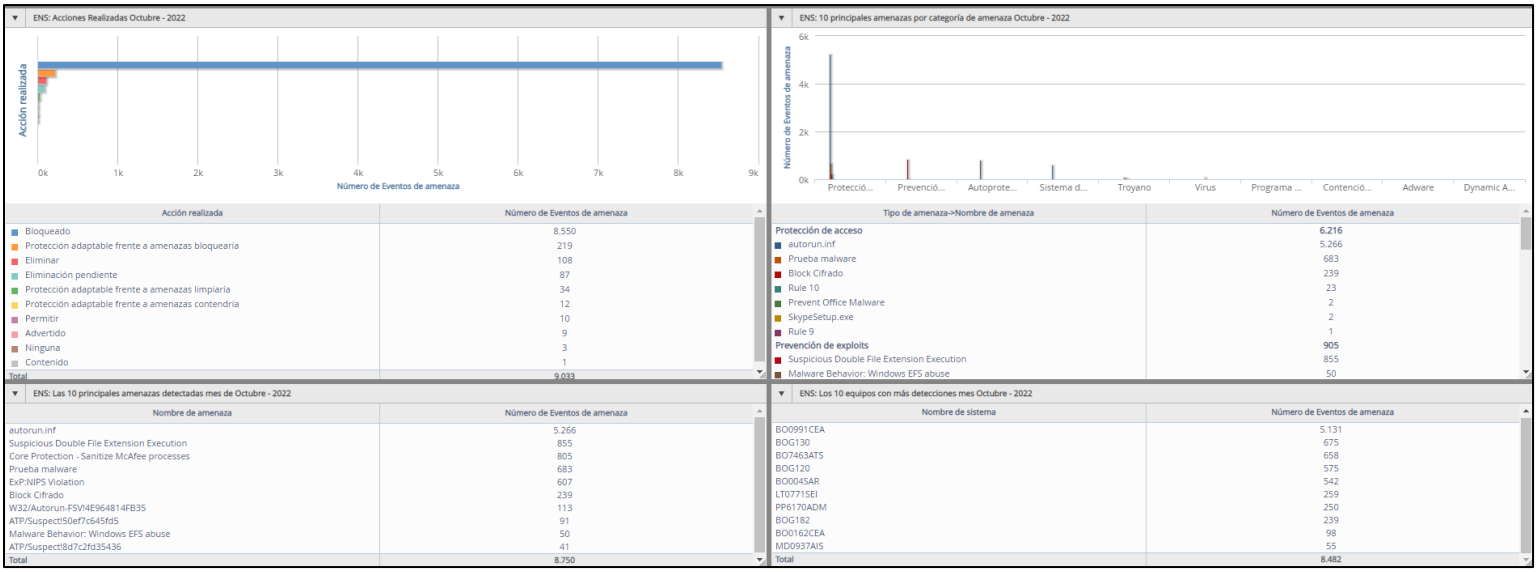
DESPLIEGUE AVANZADO DE PRODUCTO

Desde este apartado se pueden realizar en lote las actualizaciones correspondientes al nuevo versionamiento de los equipos a nivel de agente y módulos de ENS. Adicionalmente, se pueden configurar desinstalaciones a uno o varios equipos según sea el requerimiento.



ALARMAMIENTO DESDE CONSOLA

Principalmente desde consola **ePO MVISION** más que un sistema de alarma, como administradores de consola podemos ver el estado de los equipos desde los monitores que hacen parte del panel **monitoreo en tiempo real** y desde allí tomar las medidas necesarias para entrar a bloquear o eliminar las amenazas de acuerdo con su nivel de criticidad y previo análisis.



CATALOGO DE DIRECTIVAS

Desde este apartado tenemos los productos que en su mayoría se están utilizando actualmente. Es el caso de los **módulos del ENS** que aquí se detallan y nos permiten hacer configuraciones a nivel de análisis, prevención y protección. Desde acá podemos realizar exclusiones y agregar IoC conforme a una amenaza que se haya identificado y bajo una regla de parametrización.

