ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad en Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE CONSOLA CENTRALIZADA MCAFEE EPOLICY ORCHESTATOR (EPO) EN UNA INSTITUCIÓN PÚBLICA"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SISTEMAS DE SEGURIDAD INFORMÁTICA APLICADA

XAVIER MIGUEL CARVAJAL GALECIO

GUAYAQUIL-ECUADOR

AÑO: 2015

AGRADECIMIENTO

A DIOS sobre todas las cosas, a MIS PADRES por darme la vida y por siempre estar conmigo, su apoyo ha sido fundamental para la realización de todas mis metas y mi éxito alcanzado.

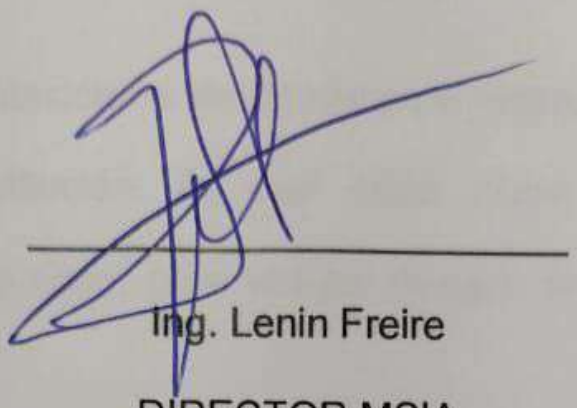
A mi compañera de vida, gracias por tu amor, apoyo y paciencia durante todo este tiempo.

A mi director de Maestría, Ing. Lenin Freire y a todos los profesores que nos impartieron conocimientos invaluables y que serán aplicados en mi vida profesional.

DEDICATORIA

A mis PADRES quienes a lo largo de mi vida profesional han sido el pilar de apoyo y empuje para la culminación de todas mis metas, de manera especial, les dedico este trabajo.

TRIBUNAL DE SUSTENTACIÓN



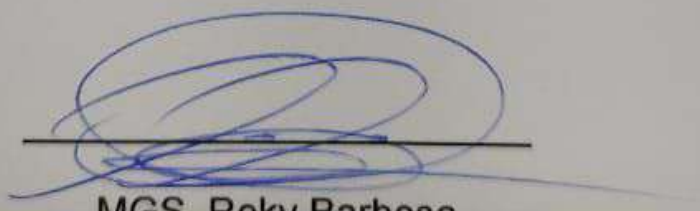
Ing. Lenin Freire

DIRECTOR MSIA

por: MSc. Cruz María Falcones

MGS. Gonzalo Luzardo

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA



MGS. Roky Barbosa

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

RESUMEN

La presente implementación es destinada para mejorar la administración de seguridad de la institución, la cual tiene como objetivo mejorar su infraestructura de seguridad, para mitigar riesgos de ataques y amenazas internas y externas.

La institución necesita actualmente una mejora en su infraestructura de seguridad, debido a que destina muchos recursos para administrar la seguridad, esto sin contar el alto costo que significa dar el soporte debido a que se tiene oficinas externas y se realiza una logística para movilizar al personal a estas.

Se requiere una solución centralizada donde se pueda monitorear y administrar la seguridad sin destinar recursos innecesarios a las oficinas externas, y mejorar la seguridad interna y externa de la institución.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÌA

ePo: ePolicy orchestator

Tics: Tecnología de la Información y Comunicación.

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La implementación de la consola centralizada McAfee ePolicy Orchestator (ePO) significo una gran mejora para la administración de la seguridad dentro de la infraestructura de la institución.

Con la implementación de todas las características dentro de su versión básica, se plantearon ciertas configuraciones, en las cuales se buscó mejorar la detección de amenazas, mantener actualizada cada uno de los equipos dentro del bosque y mantener informado al administrador de la infraestructura sobre el estado de la misma en cuanto a seguridad, para mejorar la toma de decisiones y ayudar a administrar mejor los recursos tecnológicos y de personal de soporte, para así constituir un área de TI que utilice mejores prácticas y estar acorde a estándares internacionales.

CAPÍTULO 1.

GENERALIDADES

1.1. Descripción del problema

Esta institución contaba con antivirus McAfee local por cada máquina, lo cual no estaba centralizado, y la administración del antivirus era in situ, debido a este esquema con el cual se trabajaba se derivaron varios problemas, los cuales van a ser detallados a continuación:

a. Las políticas para el antivirus se tenían que configurar localmente en cada máquina de la institución, lo cual presentaba un problema

por la asignación de recurso para realizar esta tarea, además que por más que se haya desarrollado un procedimiento para realizar esta tarea se estaba a expensas de lo que los técnicos realicen, es decir si cumplieran el procedimiento de configuración de las políticas, y esto supone un riesgo debido a que si no se configuraba correctamente no tendríamos manera de darnos cuenta hasta que la maquina sea infectada o falle de alguna forma.

b. El licenciamiento también nos perjudicaba debido a que era por máquina y no por lote, lo cual representa una gran diferencia en términos económicos para la institución.

c. Debido a que se tenía el antivirus local por máquina, se tenía previsto siempre realizar varias tareas para poder realizar el mantenimiento necesario para minimizar riesgos, esto demandaba en alta proporción de recursos.

d. La consola antivirus de McAfee servía para sus tareas más básicas que era la detección y manejo de virus, pero no tenía integración con otras aplicaciones para poder tener controlado todos los

frentes de ataques ante las amenazas, por ejemplo no podía filtrar correos desde Outlook, herramienta importante y más comúnmente usada en la institución, lo cual significaba un gran riesgo para la institución.

e. Las alertas que proporcionaba el antivirus no se podían evidenciar remotamente, había que revisar localmente en cada máquina cual era el inconveniente, debido a esto se produjeron algunas infecciones, porque no se pudo actuar a tiempo.

f. Las actualizaciones se debían hacer por máquina, lo cual significaba una gran demanda de ancho de banda para la institución, además de que se necesitaba enviar recursos a cada máquina para supervisar que este proceso se realice de manera correcta.

g. Los reportes se los debía llevar prácticamente a mano, porque obviamente no había un sistema que me permita obtener el estado actual de los antivirus de las máquinas de la institución.

1.2. Solución propuesta

Debido a que esta institución estaba atravesando un déficit con respecto a la administración de la seguridad del antivirus, y no se pueda controlar y gestionar la seguridad en el bosque de equipos, para mitigar los posibles riesgos que se puedan presentar debido a las crecientes amenazas que existen a nivel mundial.

Conforme la problemática de la institución se planteó obtener una consola de administración de seguridad para el antivirus McAfee, la cual se ajusta a las necesidades que tiene la institución, con esta consola se podrá optimizar recursos, minimizar los riesgos y amenazas, centralizar las actualizaciones, mejorar los tiempos de respuesta. La herramienta es la consola centralizada McAfee Policy Orchestator (ePO), la cual tiene todos los requisitos necesarios para cumplir con las expectativas de la institución. Con esta solución vamos a mejorar la seguridad tanto en las maquinas finales (endpoints), garantizar la protección de redes, con capacidad de integrar servicios de navegación web y de correo electrónico.

Dentro de las cualidades principales que ofrece esta consola encontramos los siguientes:

- Visibilidad integral: consigna una visión unificada de su nivel de seguridad. Los paneles que permiten visualizar información detallada y que se pueden arrastrar proporcionan información de todos los endpoints, datos, dispositivos móviles y redes para obtener una visión inmediata y reducir los tiempos de respuesta [1].

- Operaciones de seguridad simplificadas: racionalice los flujos de trabajo para conseguir una mayor eficacia demostrada. Según han demostrado estudios independientes, el software McAfee ePO ayuda a todas las organizaciones, sea cual sea su tamaño, a simplificar las tareas administrativas, reducir la carga de las auditorías y limitar considerablemente los costes en hardware relacionado con la administración de la seguridad [1].

- Arquitectura abierta y ampliable: aproveche su actual infraestructura de TI. El software McAfee ePO conecta la gestión de las soluciones de seguridad, tanto de McAfee como de terceros,

a su LDAP, operaciones de TI y herramientas de administración de configuración [1].

CAPÍTULO 2.

2. METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. Administración de seguridad de un Antivirus

La administración de seguridad de un antivirus se basa prácticamente en controlar todas las bondades y al mismo tiempo explotarlas, en beneficio de los objetivos de negocio de la empresa, sin embargo en la mayoría de los casos no se da una correcta administración del mismo, provocando que no se aprovechen estas ventajas.

Para mejorar esta situación que estaba convirtiéndose en un problema para la institución, se decidió implementar una plataforma que permita

administrar la solución antivirus y poder explotar todas las bondades, la cual tenía que ser compatible con la solución antivirus actual, ajustarse a la factibilidad económica y estar acorde con los objetivos de negocio.

Se decidió por consola centralizada McAfee ePolicy Orchestator (ePO), debido a que cumplía con los requisitos principales de la empresa, puesto que como antecedente la institución tiene instalado una solución antivirus McAfee[7].

2.2. Despliegue de la solución en toda la institución

La institución cuenta actualmente con 100 ordenadores a nivel de todos los usuarios, en los cuales se instaló el agente McAfee, por otro lado para implementar el ePO, se tuvieron que realizar los siguientes pasos:

a. Servidor de la solución

El servidor de la solución cuenta con las siguientes características:

- Virtualizado
- CPU: 2.4 GHZ

- Memoria: 2 GB
- Disco: 80 GB
- Windows Server 2003 Enterprise Edition SP2

Figura 2.1 Detalles del Servidor

Se utilizó bases datos SQL Server 2005

b. La base de datos se instaló en una unidad separada a la de la solución.

c. La instalación y sus componentes se hicieron en discos separados por mejores prácticas.

d. Una vez instalada la solución, se procede a descargar las características que fueron adquiridas de acuerdo a la versión del producto, en este caso la versión es la Básica.

- Una de las características que voy a describir es el Virus Scan 8.5

e. Instalación del McAfee Agent en los ordenadores

- El agente McAfee sirve para que el cliente se comunique de manera segura con el McAfee ePolicy Orchestator y también con los productos gestionados por el mismo.

- Este agente se ejecuta en segundo plano de manera silenciosa

- Solo podrán ser gestionados los equipos que tengan instalado el agente.

- El agente podrá actualizar contenido de seguridad, como los archivos DAT que son asociados con VirusScan Enterprise, además implementa directivas y planifica tareas en los sistemas gestionados.

- Reporta eventos e información de los sistemas gestionados y los envía al servidor ePO [6].

2.3. Configuraciones generales

Una vez instalada la aplicación y descargada todas las características adquiridas con el producto se procedió a realizar las configuraciones necesarias para nuestras necesidades dentro de la empresa, los cuales se van a detallar a continuación:

Se procede a configurar las tareas del servidor ePO:

- Las tareas generales se establecen por Default
- Además se añaden nuevas tareas:

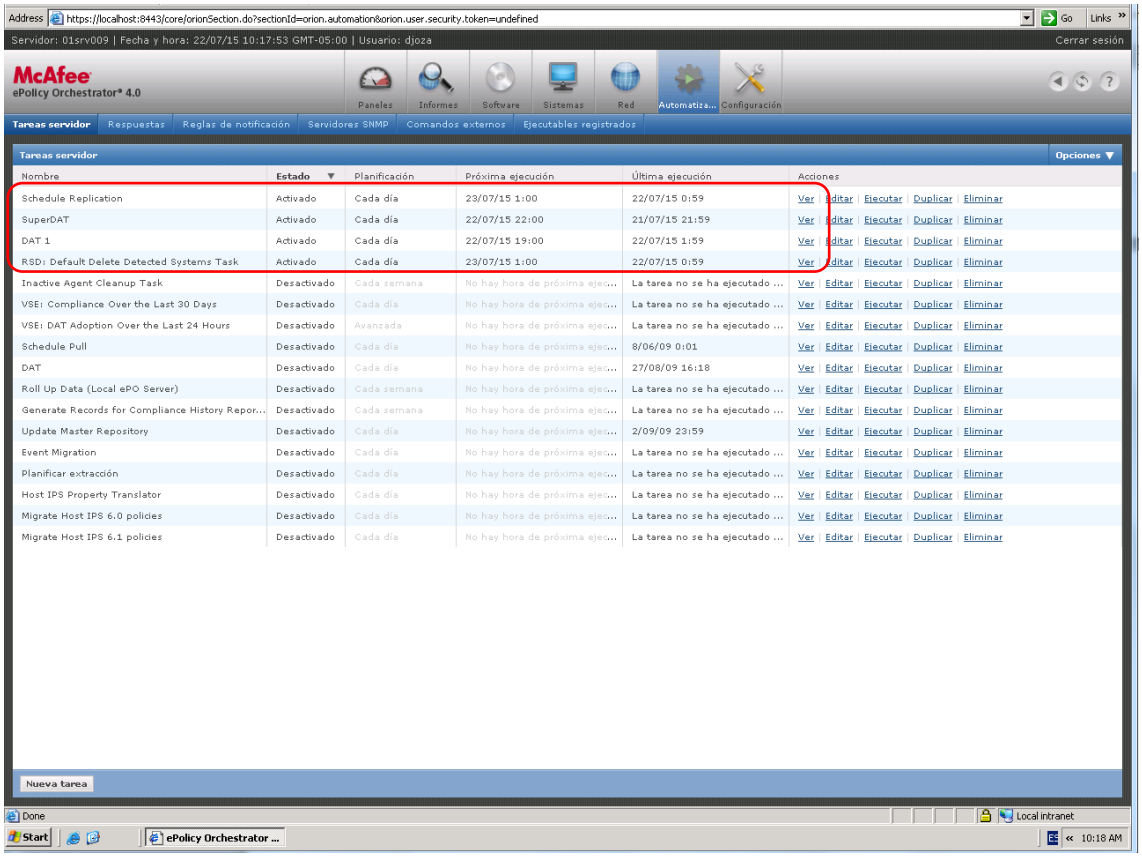


Figura 2.2.Tareas Nuevas

- Default Delete Detected Systems: Esta tarea realiza la depuración de los sistemas no detectados por un periodo de 2 meses, a esto me refiero a que si existieron equipos que tenían instalado el agente, no se comunicaron con el servidor ePO en ese tiempo, esta tarea los elimina y envía un reporte que se guarda en el log de eventos.

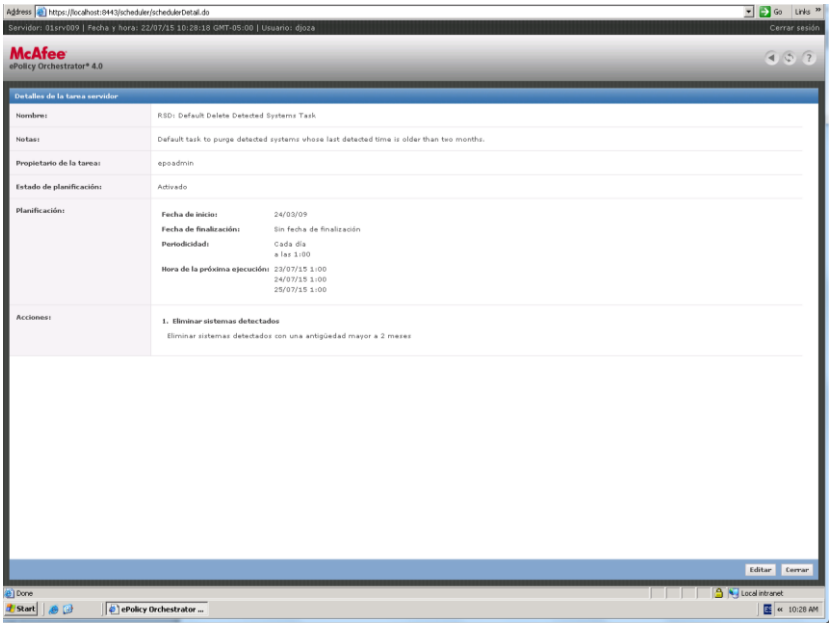


Figura 2.3.Configuración Default Delete Detected Systems

- SuperDAT: Esta tarea actualiza la base de datos de la consola VirusScan, es decir actualiza las definiciones de antivirus, la cual en es transmitida posteriormente mediante los agentes a cada uno de los equipos gestionados, para así mantenerlos actualizados.

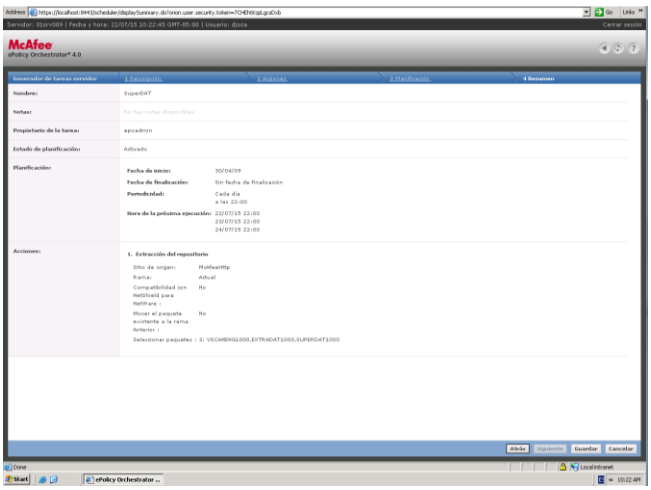


Figura 2.4 Configuración SuperDAT

- Schedule Replication: Debido a la infraestructura de la institución, en la cual se tiene contemplados agencias externas, las cuales se las debe mantener actualizadas, esta tarea realiza la replicación a repositorios que son utilizados por estas agencias, para no tener la necesidad de llegar al servidor ePO o repositorio principal y evitar que estos ordenadores queden sin la gestión y actualización de las firmas de virus.

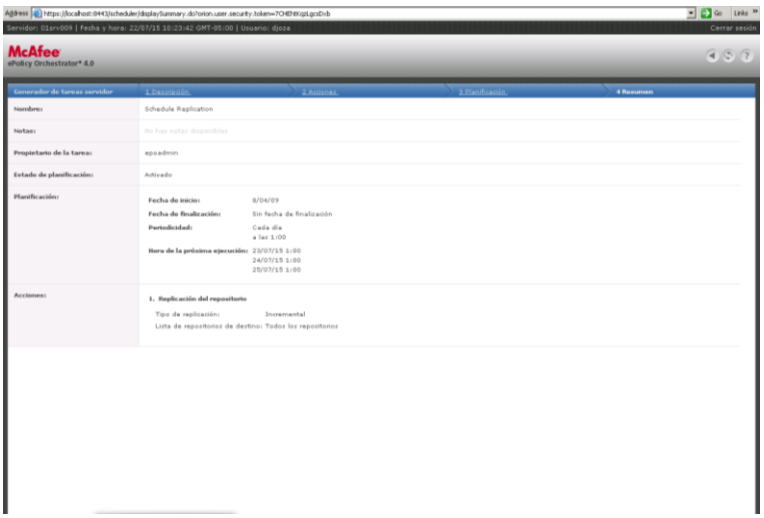


Figura 2.5 Configuración Schedule Replication

- Se establecen directivas del VirusScan McAfee para la consola ePO y las estaciones de trabajo.
    - La directiva que se configuró fue Directivas de protección de acceso.

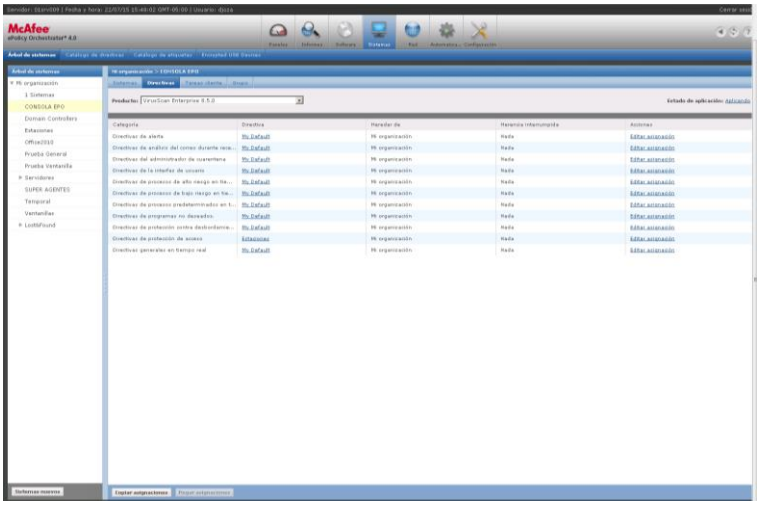


Figura 2.6 Directivas Generales

- Dentro de la directiva se configuran ciertos parámetros, de los cuales voy a describir a continuación:

  - Protección estándar de antivirus

    Se define por default, personalizando ciertos parámetros que no afecten el funcionamiento normal de Windows: Ej. No se bloquean falsificación de procesos de Windows, debido a que puede entrar en conflicto con procesos ejecutados desde el servidor de dominio o el System Center.

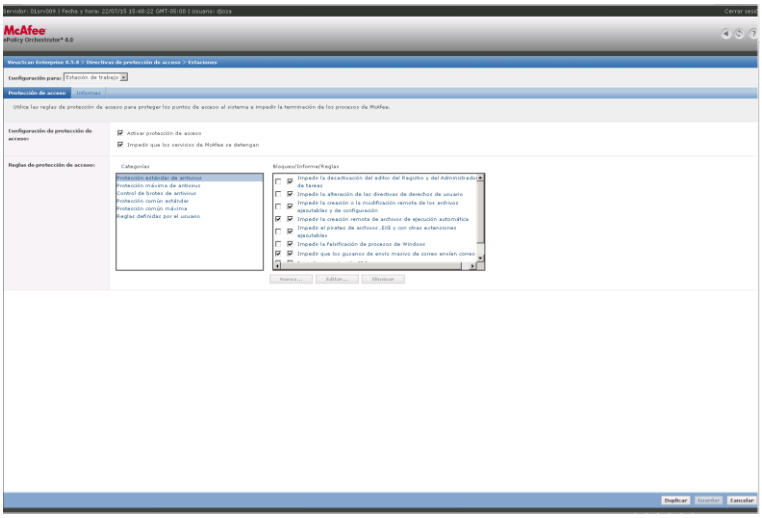


Figura 2.7 Protección estándar de virus

- Protección máxima de antivirus

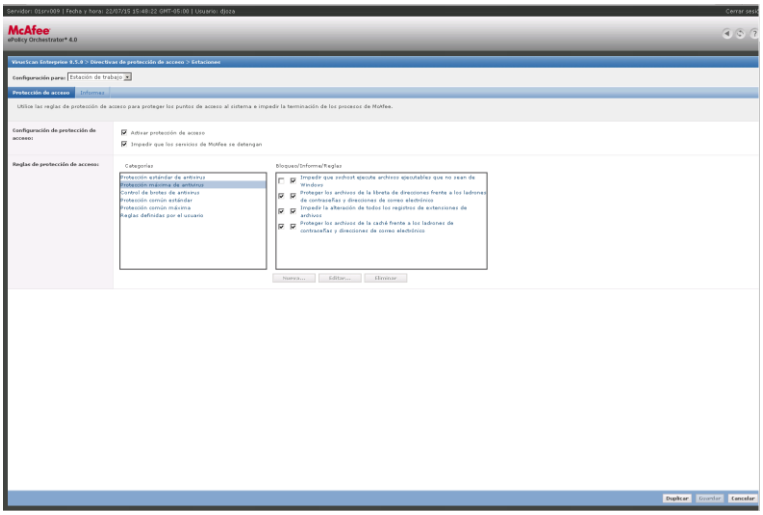


Figura 2.8 Protección máxima de antivirus

- Control de brotes de antivirus

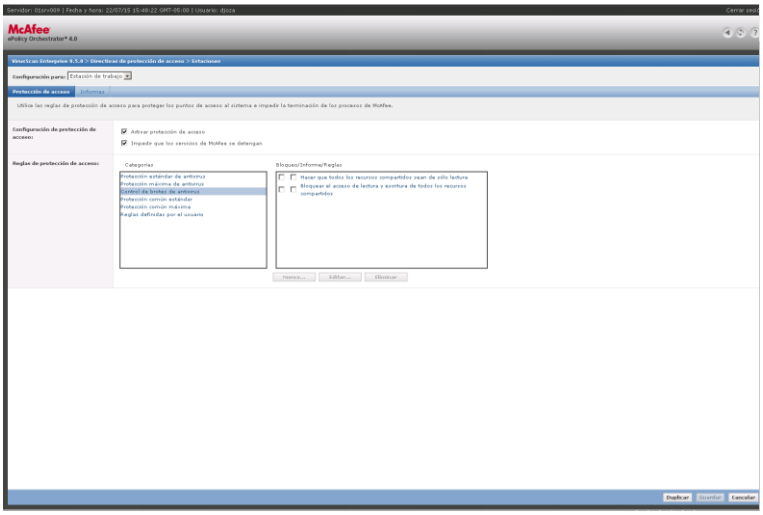


Figura 2.9 Control de brotes de antivirus

- Protección común estándar

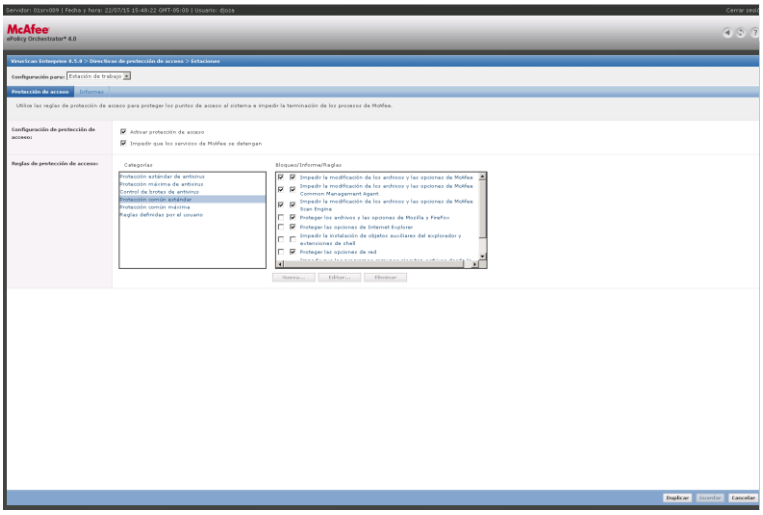


Figura 2.10 Protección común estándar

- Protección común máxima

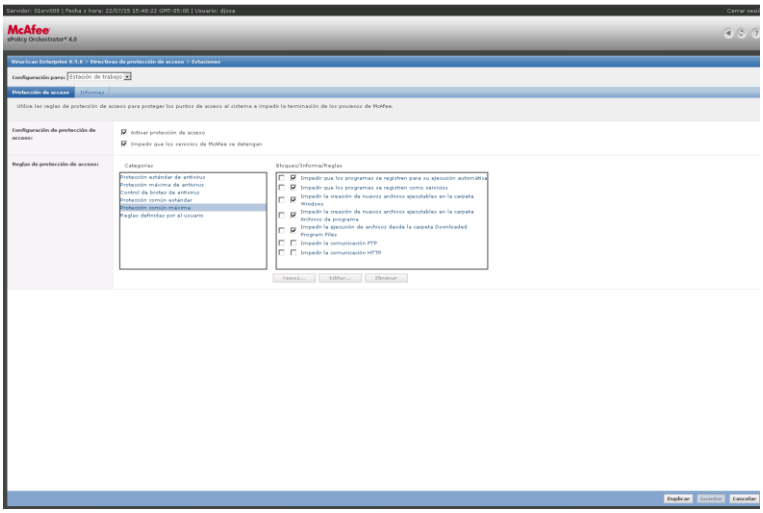


Figura 2.11 Protección común máxima

- Se definieron exclusiones e inclusiones del análisis
    - Inclusiones:
        - Spyware
        - Adware
        - Herramientas de administración remota
        - Programas de marcación
        - Falsificadores de contraseña
        - Bromas

        - Registradores de pulsaciones de teclado
        - Otros programas no deseados
    - Exclusiones
        - Pidclient.exe

    La única exclusión que se detalla se define debido a que ese programa se lo utiliza para levantar el sistema CORE del negocio.

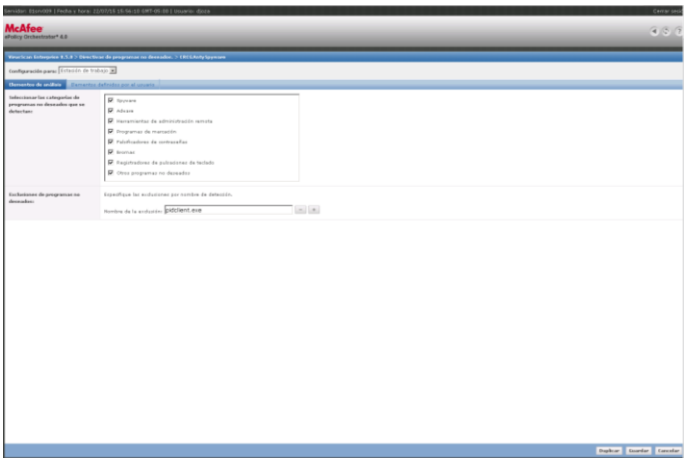


Figura 2.12 Inclusiones y exclusiones

- Los informes de los eventos de esta directiva se registran en un archivo que es respaldado periódicamente

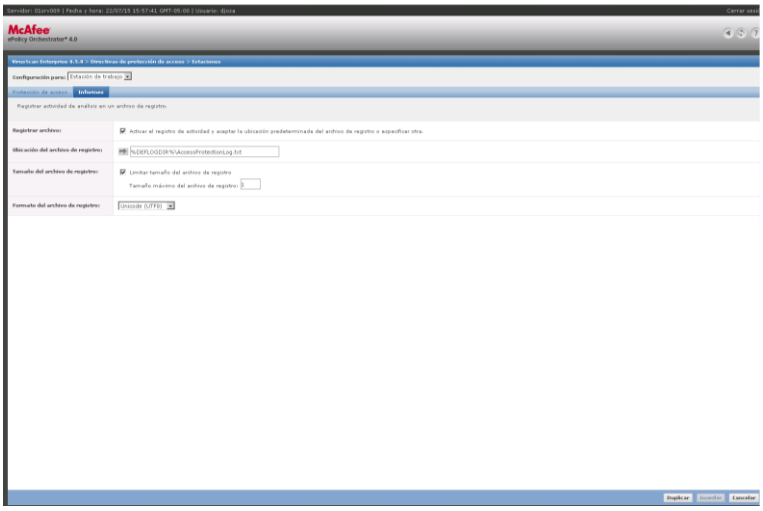


Figura 2.13 Configuración de archivo de respaldo

- Se generan reportes personalizados
    - El reporte se configuró con el nombre de “pc_gestionadas” como se muestra en la siguiente figura:

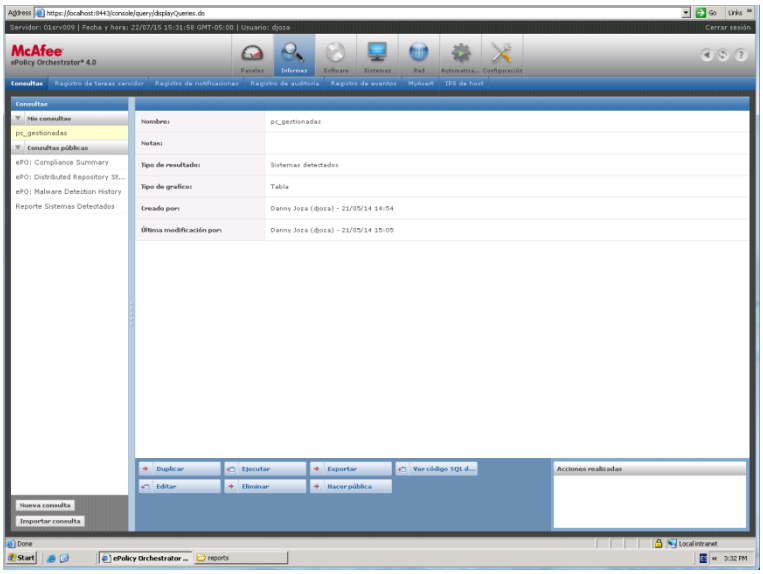


Figura 2.14 Configuración de reportes

- La autenticación de la consola es mediante Windows, ésta plataforma se complementa con el Active Directory.

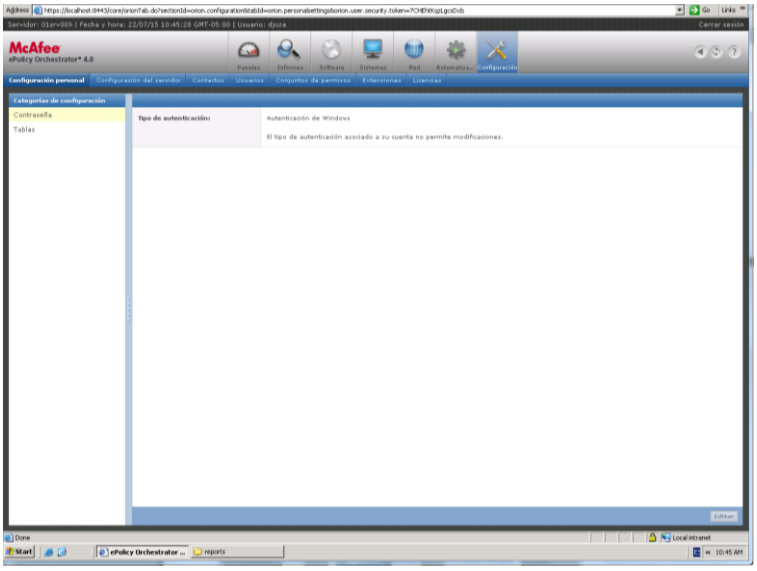


Figura 2.15 Configuración de autenticación

-

- Se parametriza el envío de correos desde el servidor, medida que solo está activada para eventos por necesidad.

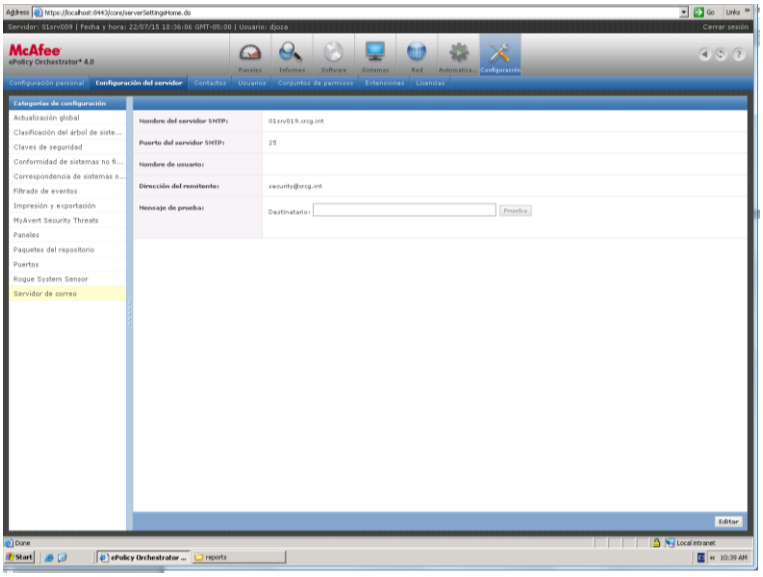


Figura 2.16 Configuración de envío de correos

- Los puertos por los cuales va a trabajar el sistema, son los que vienen por default, en caso de que se necesite cambiar los puertos, se lo hará bajo demanda.

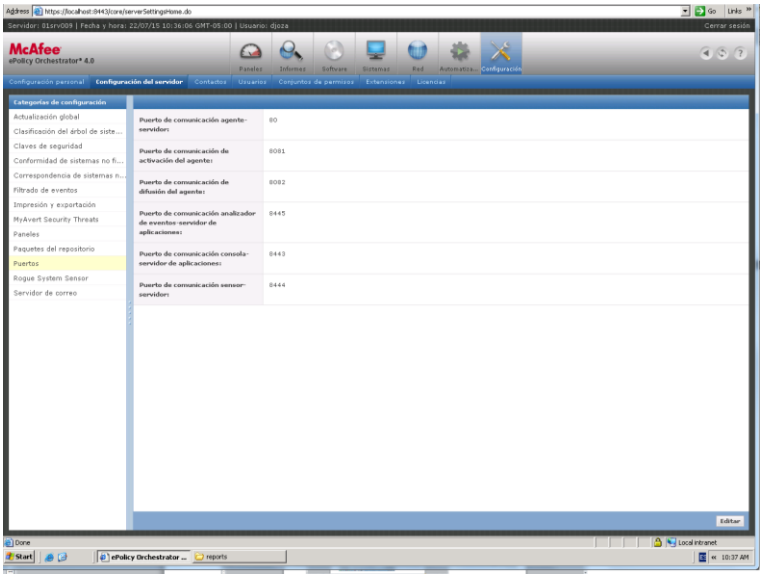


Figura 2.17 Configuración de puertos

- Se configura el Rogue System Sensor, el cual es el que permite gestionar la conexión del agente con el servidor ePO, para lograr realizar las diferentes tareas en todos los equipos gestionados.

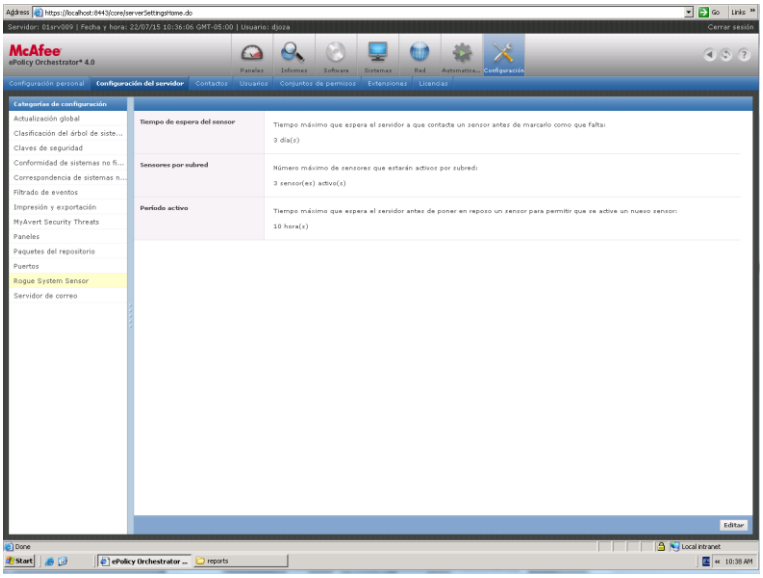


Figura 2.18 Configuración de Rogue System

- Se establece la página por omisión que se muestra cuando se inicia el servidor ePO

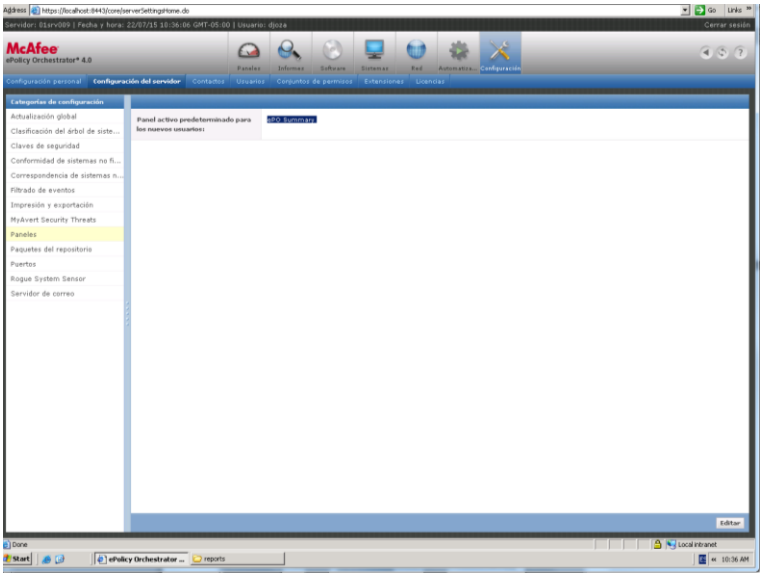


Figura 2.19 Configuración de página de inicio

- Se establece que se mantenga actualizado el módulo de amenaza de seguridad cada 15 minutos como buena práctica.

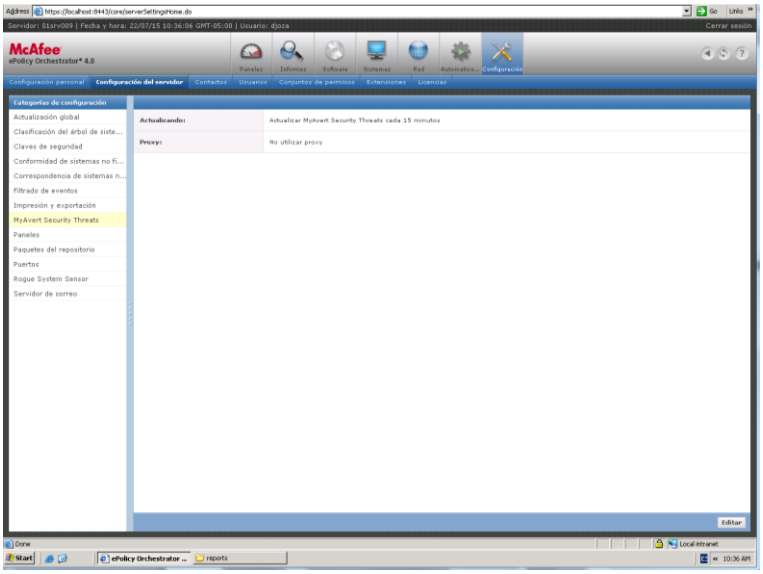


Figura 2.20 Configuración de actualización

- Las actualizaciones se las configura para que siempre utilicen la rama Actual, con esto se previene que alguna firma no se actualice

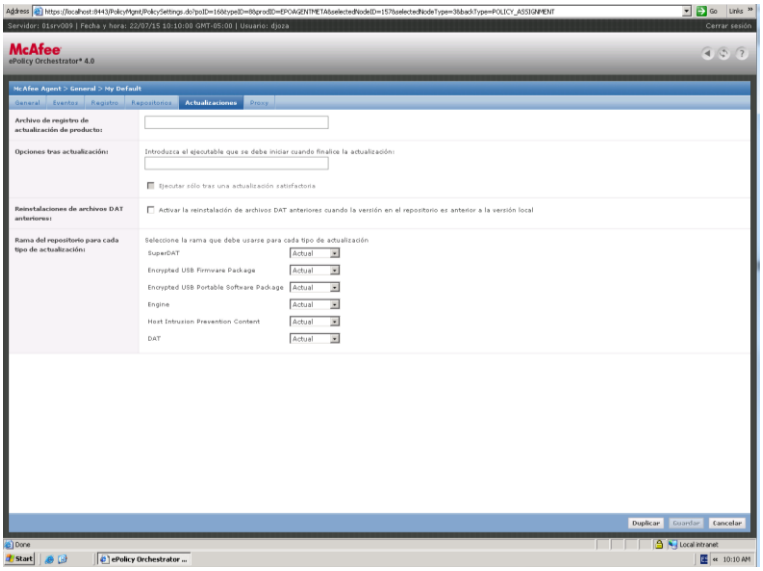


Figura 2.21 Configuración de ramas de actualización

- Se configuraron diferentes repositorios, los cuales se utilizaron para mantener actualizado la base de firmas de virus en las agencias externas.

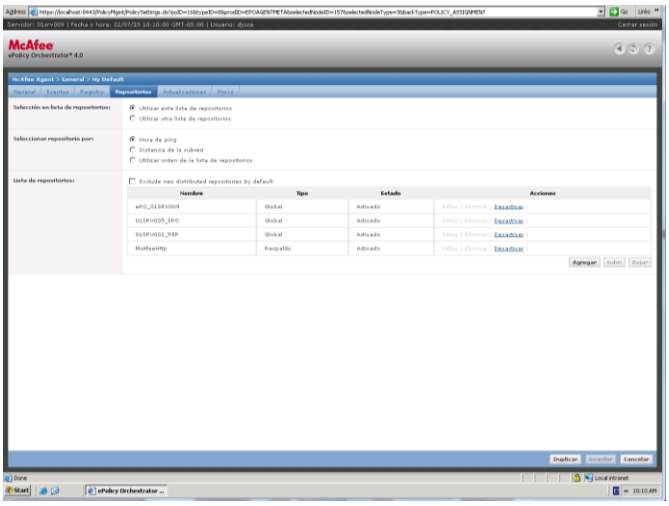


Figura 2.22 Configuración de repositorios

- Se configura globalmente para que se registre la actividad del agente en cada equipo gestionado.

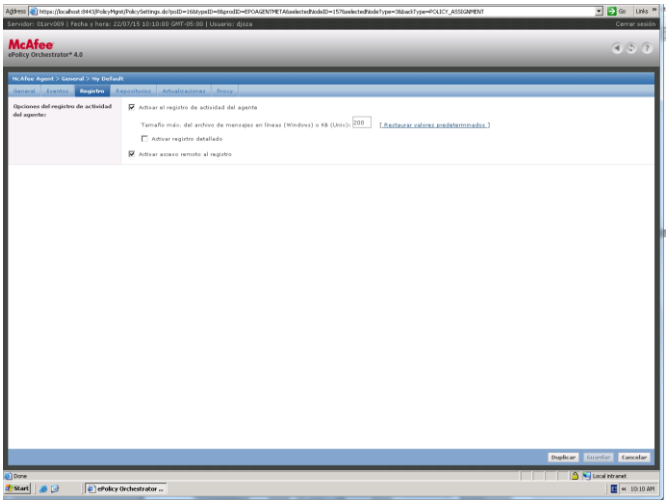


Figura 2.23 Configuración de actividad del agente

- La pantalla principal del sistema muestra el resumen de toda la actividad del mismo [2] [3] [4].

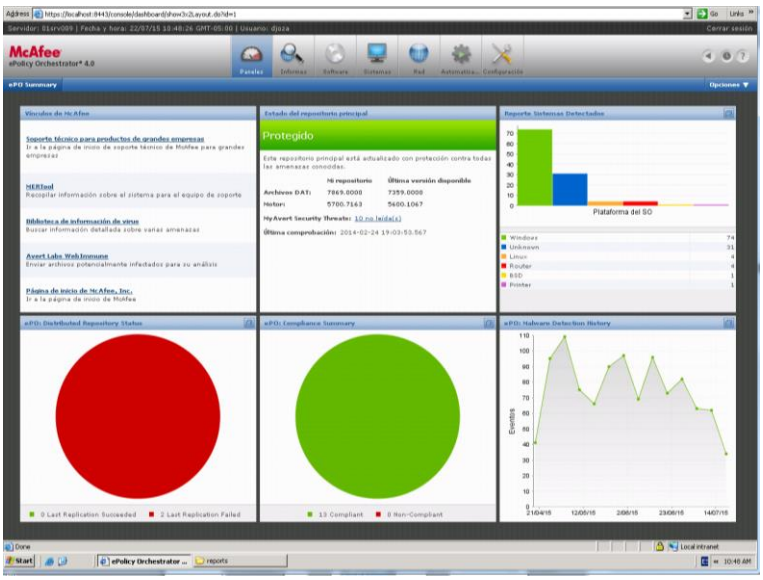


Figura 2.24 Vista de resumen de la consola

2.4. Factibilidad económica

Anteriormente se tenían licencias McAfee Virus Scan individuales por cada equipo, debido a que no se realizaba la gestión de administración y de seguridad, y esto representaba un alto costo por licencia, lo cual no era beneficioso para la institución, ya que cada año se tenía que renovar las mismas y los costos no disminuían, adicionalmente, que no se administraba desde una consola central, y se destinaban recursos para poder administrar todos los equipos, ésto también incurría en costos de operación, puesto que para las oficinas externas había que montar una logística para dar el debido soporte.

Con la adquisición de este sistema para gestionar la seguridad McAfee ePO, se generó un ahorro del 25% sobre lo que ya estaba implementado, debido a que las licencias por cada equipo con esta plataforma se las debía adquirir por grupo de máquinas a ser gestionadas, esto favoreció la adquisición de la solución, y el soporte con el que ya contábamos de McAfee, los cuales fueron factores decisivos para la adquisición.

Por consiguiente, desde que se implementó la solución, no se tenía que destinar ningún recurso para dar el soporte, ya que todo estaba administrado centralmente desde la consola.

CAPÍTULO 3.

3. ANÁLISIS DE RESULTADOS

3.1. Evaluación de rendimiento de detección de Malware

La implementación de esta solución nos permitió saber cómo se estaba comportando el Virus Scan frente a malwares, spywares y demás amenazas dentro de la institución, antes de esta plataforma no teníamos una estadística detallada de cuanto o a que escala estábamos siendo atacados por estas amenazas.

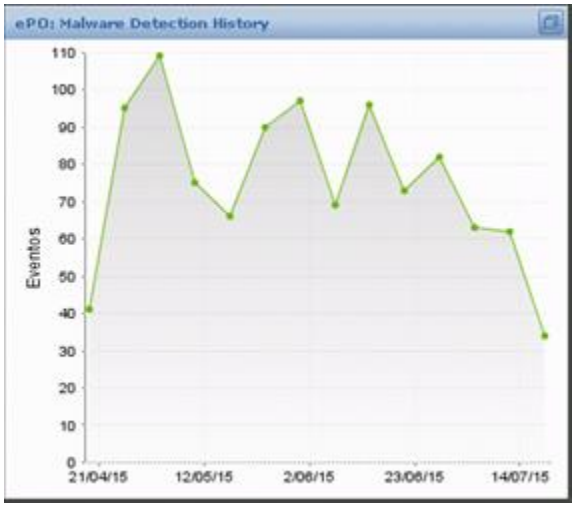


Figura 3.25 Reporte de detección de malware

Debido a esta ventaja hemos podido actuar con anticipación ante las amenazas, alcanzando un mejor rendimiento en mitigar ataques de este tipo, incrementando la seguridad de todo el parque informático.

A esto también atribuyo que gracias al agente los equipos permanecen gestionados y actualizados con las últimas firmas de virus, lo cual fortalece aún más la plataforma para hacer frente a estos ataques y disminuir el riesgo de sufrir una intromisión.

3.2. Análisis de gestión de la consola centralizada ePO

Debido a la capacidad avanzada de gestión de la consola ePO, y sus características con las cuales fue adquirida, se mejoraron los siguientes aspectos a nivel de toda la infraestructura:

- Mejoró la administración de los equipos que tenían el producto Virus Scan instalados, puesto que con el Agente McAfee se pueden realizar diferentes actividades y tareas remotamente y de manera automática en todo el parque informático:

- El agente McAfee sirve para actualizar y administrar de manera centralizada desde McAfee ePO con la aplicación e implementación de directivas y tareas planificadas. en los registros se recogen los eventos y las acciones que se producen en los equipos gestionados

- Gracias a las directivas que se implementaron, el agente logró mantener actualizado todo el parque informático, así como

también mantiene al servidor ePO informado sobre todo los que sucede con los equipos gestionados.

- Mediante los repositorios que se configuraron se mejoró el aspecto de actualización para las oficinas de afuera puesto que como estos repositorios son réplicas del original, estas oficinas no necesariamente necesitaban llegar al repositorio general, sino solo a los que se configuró para que se conecten con las réplicas, ésto mejoró el tráfico de datos obteniendo un equilibrio de carga y mejores velocidades de actualización.

- Se mejoró el control de los equipos en los cuales tenemos el producto Virus Scan, debido a que gracias al agente se logró tener una idea detallada de los equipos gestionados, así como también el estado en el cual se encontraban.

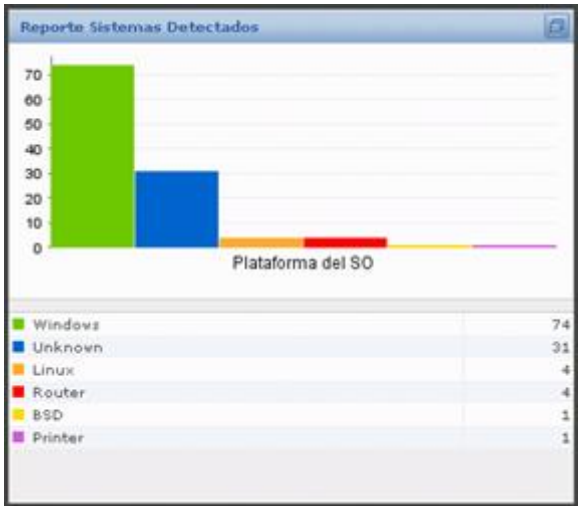


Figura 3.26 Reporte de sistemas detectados

- Facilitó la actualización de las políticas de seguridad y ayudó con los cambios de seguridad en curso.

- Se almacena los logs en los cuales se encuentran todos los eventos que ocurren en todo el parque informático sobre los sistemas gestionados.

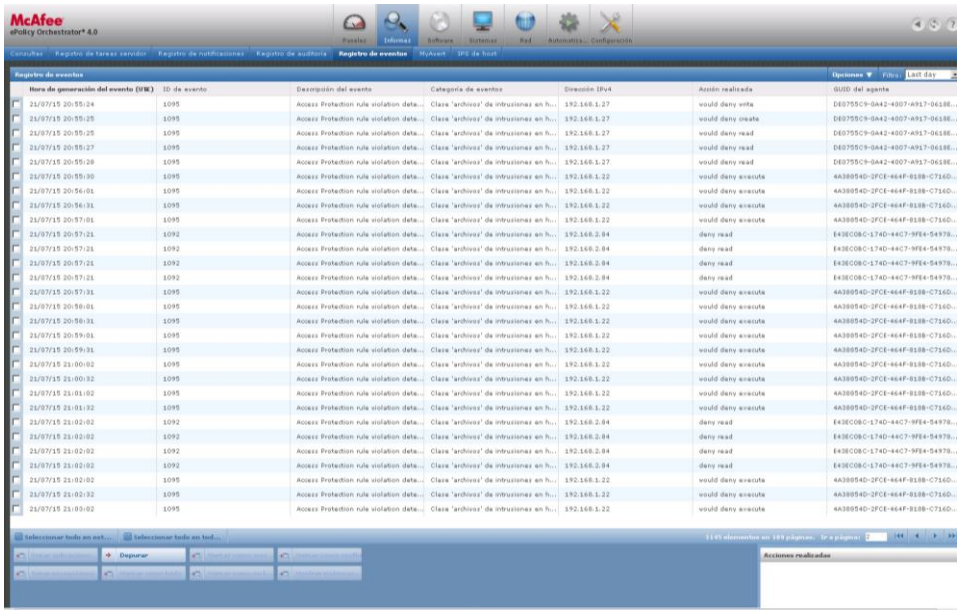


Figura 3.27 Reporte de actividades

- Debido a que se configuro el sistema para realizar un barrido cada día sobre los sistemas gestionados que existen en la red, podemos tener una idea clara de cómo se encuentra en cada momento nuestra infraestructura, y que equipos se encuentran gestionados y cuáles no, lo cual fomenta una mejor administración y respuestas rápidas ante las falencias que se puedan evidenciar con respecto a la gestión de los equipos. Con esta herramienta podemos mantener una mejor organización de nuestros recursos y disminuir el índice de asistencias no necesarias.

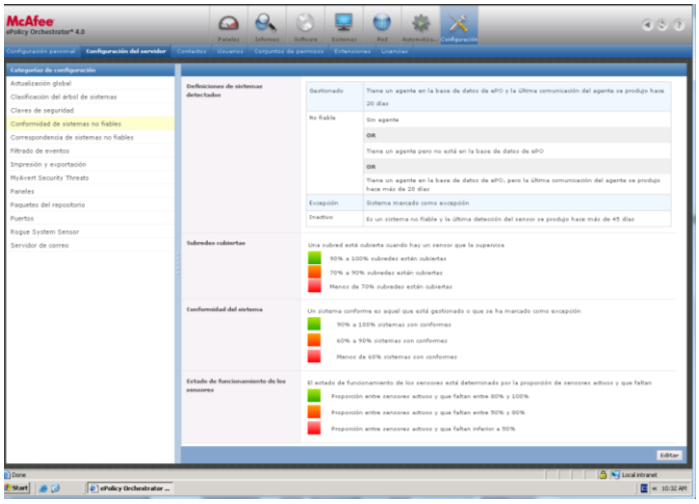


Figura 3.28 Reporte de detección de equipos en la red

3.3. Análisis de reportes generados

Los reportes generados por el ePO son detallados y personalizables, para nuestro caso configuramos el reporte para que nos muestre un detalle de todos los equipos gestionados en la red.

En la siguiente figura se muestran todos los equipos detallados:

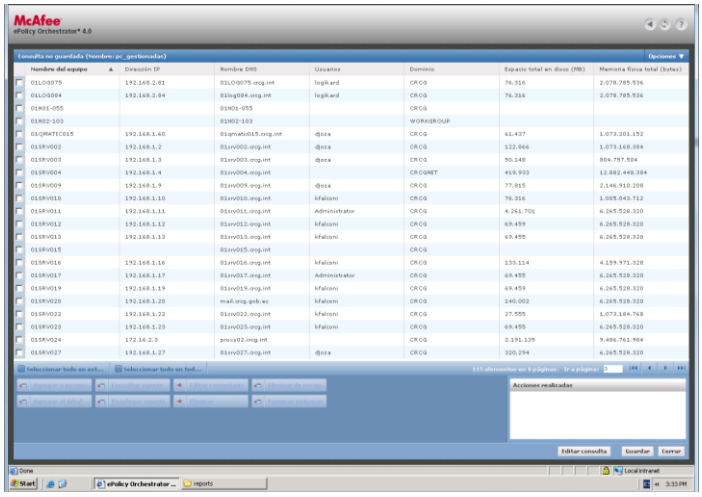


Figura 3.29 Reporte de PC gestionadas

También se configuro el registro de auditorías del sistema, lo cual nos va a servir para investigación en caso de que exista algún inconveniente con el sistema o la solución en sí, a continuación se muestra la gráfica donde están alguna auditorias que se han realizado:

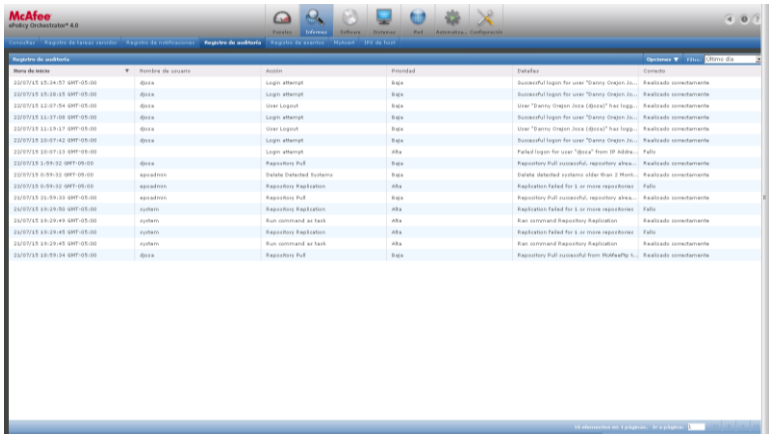


Figura 3.30 Reporte de auditorías del sistema

El almacenamiento de los reportes detallados y de los logs de eventos se guarda en una ubicación dedicada para los mismos en un disco aparte, esto se resolvió como mejores prácticas para llevar un control del consumo de espacio y no interfiera con el funcionamiento del sistema. La ubicación es F:/reports

A continuación se muestra como está configurado donde se guardan los logs:

Figura 3.31 Repositorio donde se almacena los logs

3.4. Evaluación de costos de la implementación frente a la infraestructura antigua

La adquisición de este sistema para gestionar la seguridad McAfee ePO, supuso un ahorro del 25% sobre lo que ya estaba implementado, este sistema permitió disminuir los costes en los siguientes puntos:

- Licencias por equipo

Las licencias que se tenían en la plataforma anterior eran individuales, por consiguiente el costo de licencia es superior o el más alto debido a que las empresas distribuidoras de estas soluciones de seguridad tiene como fin vender por paquetes empresariales más económicos, por consiguiente al momento de adquirir este sistema, nos vimos en la necesidad de adquirir un paquete empresarial de licencias, lo cual significo una reducción en los costos sumamente significativo.

- Soporte McAfee

Debido a que ya contábamos con productos McAfee en la infraestructura, favoreció la adquisición de esta solución, puesto que nos realizaron una rebaja por el soporte debido a la fidelidad que tenemos con el distribuidor, esto beneficio a la institución manteniendo un estándar en términos de solución y se ahorró dinero en la implementación.

- Recursos mejor administrados

A consecuencia de la implementación de esta solución, se logró mejorar la gestión de recursos, debido a que ya no se necesitaba enviar a cada ordenador para verificar que el antivirus funcionaba correctamente, lo cual beneficio al departamento de IT, reduciendo

costos dentro de sus filas, y mejorando la gestión y llevándola a un nivel más alto.

CONCLUSIONES Y RECOMENDACIONES

1. El sistema de administración de seguridad McAfee ePO, ha mejorado la falta de gestión de recursos tecnológicos para mantener la infraestructura segura de la institución, con las características que se han implementado se han optimizado los tiempos de respuestas así como la efectividad al momento de escanear amenazas así como al momento de tratar las mismas, es decir se han reducido los equipos infectados o propensos a infectarse.

2. La administración de los recursos destinados a dar soporte, se han disminuido, esto beneficia directamente al área de TICS, puesto que van a contar con ese personal para otros proyectos, esto se suma a la

mejor distribución de esfuerzo dentro del equipo de trabajo, menos trabajo de hormiga y más trabajo especializado.

3. Mediante los reportes que son generados por el sistema, podemos analizar mejor la situación en la que se encuentra toda la infraestructura con respecto a seguridad, incrementando el acierto al momento de la toma de decisiones, esto favorece implícitamente al administrador de infraestructura, para poder saber con anticipación que debe mejorar en un futuro, y así realizar una planificación más acertada sobre lo que se debe invertir.

4. Indudablemente esta implementación significó un ahorro de un 25% con respecto a la infraestructura que se tenía, esto fue un gran beneficio para la institución, agregando el soporte otorgado por la empresa distribuidora seguía siendo barato debido a que nos decidimos por la misma línea McAfee, asegurando la continuidad del negocio debido a la fidelidad de la marca, incrementado los ventajas frente a otras propuestas.

RECOMENDACIONES

1. Se recomienda mantener un seguimiento continuo de esta plataforma y asegurar cada año la renovación en la misma línea, para no perder los beneficios que nos han otorgado en cuanto a soporte y fiabilidad del sistema.

2. Mantener al personal que administra esta plataforma con capacitación constante para aprovechar todos los beneficios de la misma y estar al día con las últimas actualizaciones.

BIBLIOGRAFÍA

[1]Mcafee, EPolicy-Orchestrator, http://www.mcafee.com/es/products/epolicy-orchestrator.aspx#vt=vtab-Overview,k, fecha de consulta Julio 2015

[2]Epomcafee, Fallo de Seguridad EPo Mcafee http://epomcafee.blogspot.com/ fecha de consulta Julio 2015

[3]Microsa, Mcafee Agent 4.8.0, http://www.microsa.es/biblioteca/McAfee/agent/MA_480_ProductGuide_es-es.pdf, fecha de consulta Julio 2015

[4]Mcafee, Cofiguraciones, http://ordenador.wingwit.com/software/antivirus-software/103082.html#.VbmbVPl_NBc

[5]EHowenespanol, http://www.ehowenespanol.com/agente-mcafee-epo-sobre_91450/, fecha de consulta Julio 2015

[6]Mcafee, Productos, http://www.mcafee.com/us/downloads/endpoint-protection/products/epo-mcafee-agent-deployment.aspx, fecha de consulta Julio 2015

[7]Mcafee,https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25187/es_ES/ma_500_pg_es-es.pdf, fecha de consulta Julio 2015