Universidad Nacional Autónoma de Nicaragua

UNAN-León

Facultad de Ciencias y Tecnología

Ingeniería en Telemática

Propuesta de solución para la monitorización de los laboratorios del Departamento de Computación de la Facultad de Ciencias y Tecnología de la UNAN-León utilizando las herramientas Pandora FMS 6.0 e Integria IMS 5.0 en el período de septiembre a noviembre de 2017

Tesis para optar al título de Ingeniero en Telemática

Autor(es): **Br. Josué Ramón Gutiérrez Canales**
Br. Norlyht Josué Gómez Ortiz
Br. José Jerónimo Méndez García

Tutor: **Ing. Denis Espinoza, M.Sc.**

León, Nicaragua

Agradecimiento

Primero que nada, a Dios por darme la oportunidad de seguir adelante en cualquier situación y permitirme llegar hasta esta etapa final de mi formación profesional.

A mi madre, abuela y tía, por el gran esfuerzo que hacen a diario por darme lo necesario y poder llegar hasta estas instancias de mi vida.

Quiero agradecer sinceramente a aquellas personas que compartieron sus conocimientos para hacer posible la conclusión de esta tesis. Especialmente agradezco a nuestro tutor el MSc. Denis Espinoza por su asesoría siempre dispuesta.

(José Méndez)

Le agradezco a DIOS por haberme acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y brindarme una vida llena de aprendizajes y experiencias.

A mis padres Norberto Gómez y Merarly Ortíz por su apoyo y consejos durante el tiempo que llevo de vida y a los cuales con amor y orgullo les dedico esta tesis profesional que simboliza la culminación de mis estudios universitarios. También agradezco la confianza, Esfuerzo y dedicación a mis profesores: Julio, Santiago, Aldo, Wilmer, Álvaro, Miguel, profesoras: Valeria, Karina, Ana María, Claudia, Davinia, y en especial Gracias al Ingeniero Denis Espinoza por confiar en nosotros y brindarnos la oportunidad de desarrollar nuestra tesis profesional, por su dedicación sin más que agregar solo puedo decir Gracias por todo.

(Norlyht Gómez)

En primer lugar, doy gracias a Dios por haberme dado el tiempo necesario para realizar este trabajo, por haberme permitido conocer a muchas personas que colaboraron conmigo para hacer de uno de mis sueños una realidad y porque en todo momento, aunque no siempre lo percibí, él estuvo conmigo.

También la dedico a mi familia quienes me han apoyado para poder llegar a esta instancia de mis estudios, ya que ellos siempre han estado presentes brindándome consejos, compresión, amor, ayuda en los momentos difíciles y con los recursos necesarios para estudiar. Me han enseñado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia y coraje para conseguir mis objetivos.

Gracias a mis compañeros que sin ustedes no existiría hoy esta tesis, por sus valiosas aportaciones que hicieron posible este proyecto y por la gran calidad humana que me han demostrado con su amistad.

Finalmente agradezco M.sc Denis Espinoza por su valiosa guía y asesoramiento para la realización de la misma.

(Josué Gutiérrez)

INDICE

1 Introducción

La monitorización de redes es de suma importancia para cualquier organización, ya que de esto depende el poder conocer el comportamiento general de la infraestructura de comunicaciones y garantizar una alta disponibilidad y eficiente en la red.

Actualmente el Departamento de Computación de la Facultad de Ciencias y Tecnología de la UNAN-León no cuenta con una solución para el monitoreo de los laboratorios que permita una mejor gestión y administración de los mismos; por lo cual en el presente trabajo se propone la implementación de un sistema de monitoreo de red y un gestor de incidencias sencillo utilizando las herramientas Pandora FMS e Integria IMS.

La herramienta Pandora FMS proporciona una solución completa para monitorizar el rendimiento y disponibilidad de las máquinas de los laboratorios a fin de garantizar que todas estas están funcionando bajo los criterios de operación establecidos. Por otro lado, Integria IMS permite la gestión de tickets para llevar el control de incidencias, además de un completo sistema de inventario y capacidad interna de auditoria. Integria es un derivado parcial de Pandora FMS.

El trabajo presentado en este documento contiene la información sobre el diseño e implementación de un sistema de monitoreo de las máquinas de los laboratorios del Departamento de Computación empleando los protocolos SNMP e ICMP. De igual manera se implementa un sistema de gestión de incidencias e inventario.

1.1 Antecedentes

Son muchas las implementaciones que hoy en día existen de sistemas de monitorización desplegados como parte de proyectos estudiantiles. Entre estas podemos mencionar:

- IMPLEMENTACIÓN DE ZABBIX COMO HERRAMIENTA DE MONITORIZACIÓN DE INFRAESTRUTURA INFORMÁTICA DE LA COMPAÑÍA SANTINI SYSTEM GROUP LTDA.

  Esta práctica se llevó acabo por Santiago Martínez Clavijo Gabriel Narváez Salazar en la Universidad de Santo Tomas Bogotá D.C, consistía en la implementación de ZABBIX (una herramienta Open Source de Libre distribución) para la monitorización de la infraestructura informática de la compañía SANTINI SYSTEM GROUP LTDA en el año 2010. Esta herramienta brinda al administrador una serie de facilidades para llevar a cabo tareas de diagnóstico, prevención y control de los diferentes equipos de red, mejorando los tiempos de respuesta y garantizando mayor efectividad.

- IMPLANTACIÓN DE LA HERRAMIENTA OSSIM PARA EL MONITOREO Y GESTIÓN DE LA SEGURIDAD DE LA RED Y PLATAFORMAS WINDOWS Y LINUX APLICADO A EMPRESAS MEDIANAS

  Este proyecto fue realizado por los estudiantes: Ángel Heraldo Bravo y Álvaro Luis Villafuerte Quiroz de la Universidad Escuela Superior Politécnica del Litoral (ESPOL) y la ejecución de la práctica se llevó acabo el Campus Gustavo Galindo, Km 30.5 vía Perimetral Apartado 09-01-5863 Guayaquil-Ecuador. En éste se implementa OSSIM (herramienta Open Source) la cual aparte de una herramienta de monitoreo logs es un SIEM (Security Information and Event Management) que incorpora diversas formas de gestionar la seguridad en la red, bases de datos, análisis de virus y malware en plataformas Windows. OSSIM está orientado a los Administradores de red de empresas medianas que necesitan tener un monitoreo general de su infraestructura, obtener reportes en tiempo real de lo que está sucediendo para analizar las anomalías y tomar decisiones y correcciones oportunas.

1.2 Planteamiento de la Problemática

El Departamento de Computación de la UNAN-León posee 7 laboratorios de cómputo al servicio de los estudiantes de Ingeniería en Sistemas de Información e Ingeniería en Telemática. Cada laboratorio cuenta aproximadamente 30 computadoras siendo solamente 6 de éstos los que cuentan con conexión a la red de la Universidad y acceso a Internet. A estos laboratorios se les da mantenimiento 1 vez a la semana.

Tabla 1 Laboratorios del Departamento de Computación. Fuente: Entrevista M. Somarriba

Laboratorio	Ubicación	Capacidad
Hardware	Edificio CIDS	13
Alcalá 1	Edificio CIDS	32
Alcalá 2	Edificio ATM	29
Laboratorio 1	Edificio del Básico segundo piso	29
Laboratorio 2	Edificio CIDS (Sin acceso a internet)	25
Cisco	Edificio del Básico primer piso	26
ACAI-LA	Edificio Mariano Fiallos (Anexo al Básico)	24

Entre el nodo central de la UNAN-León y los administradores de los laboratorios, se monitorizan amenazas tanto físicas como lógicas de los mismos, siendo los problemas más comunes:

- Los bucles en la red y abusos de ancho de banda con contenido no educativo monitorizados desde el nodo central (J. Treminio, comunicación personal, 5 de julio de 2017)
- Mal funcionamiento hardware o software de las computadoras y perdidas de mouse u otra pieza de la computadora monitorizado por los administradores de los laboratorios (M. Somarriba, comunicación personal, 7 de julio de 2017)

Al centrarnos en las problemáticas observadas por los administradores de los laboratorios, el Ing. Somarriba explicó que existen diversos elementos que se deben implementar para mejorar la gestión actual de los mismos, entre los cuales destacaron:

- Conocer de forma remota el estado de los laboratorios. Ya que si no es de forma presencial no hay manera de obtener ninguna información de los equipos.

- Falta de un historial de las incidencias reportadas y resueltas. Pues actualmente las incidencias son reportadas verbalmente (en su gran mayoría) o por correo no permitiendo tener un reporte general de todo lo resuelto.
- Falta de un inventario actualizado, así como el registro de préstamo de equipos. Aunque en la Universidad se cuenta con un inventario este no se actualiza de manera frecuente (1 vez al año) por ende si durante ese lapso ocurre algún movimiento de los equipos este no se verá reflejado hasta el inventario del año siguiente.

Tomando los elementos anteriormente citados se planten la siguiente pregunta general y preguntas específicas:

Pregunta general:

¿De qué manera se puede mejorar el sistema de monitoreo de los laboratorios del Departamento de Computación?

Preguntas específicas:

- ¿Cómo saber el estado actual de los equipos de manera remota?

- ¿Cómo mantener un inventario actualizado de los equipos y mobiliario de los laboratorios del Departamento de Computación?

- ¿Cómo mejorar el tiempo de respuesta ante fallos y perdidas que se presentan en los laboratorios?

1.3 Justificación

En base a los problemas antes planteados se hace necesario utilizar programas de monitoreo de redes y reportes de incidencias que ayuden a llevar un mejor control de los laboratorios del Departamento de Computación de la UNAN-León.

1.3.1 Originalidad

Se desarrolló esta propuesta con el fin de ser los primeros en proponer un sistema de monitorización y gestión de inventario e incidencias para mejorar el sistema actual.

1.3.2 Alcance

La solución propuesta permitirá la monitorización del estado actual de los laboratorios, la creación y actualización del inventario de los equipos y la gestión de incidencias.

1.3.3 Producto

Se entregará un equipo configurado con el sistema de monitorización de los laboratorios (Pandora FMS) con los componentes estándar para monitorear máquinas Linux y Windows; y el sistema para la gestión de inventario e incidencias (Integria IMS).

1.3.4 Impacto

Una mejora significativa en la administración de los laboratorios del Departamento de Computación de la UNAN-León, mejorando el tiempo de respuesta en caso de fallos en un determinado equipo logrando así una mayor disponibilidad de los laboratorios.

1.4 Objetivos

1.4.1 Objetivo General

Proponer una solución para la monitorización de los laboratorios del Departamento de Computación de la Facultad de Ciencias y Tecnología de la UNAN-León utilizando las herramientas Pandora FMS 6.0 e Integria IMS 5.0 en el período de septiembre a noviembre de 2017

1.4.2 Objetivos Específicos

- Monitorizar el estado de los recursos de los equipos en los laboratorios del Departamento de Computación de la UNAN-León mediante la herramienta Pandora FMS utilizando los protocolos SNMP e ICMP.

- Mantener un inventario actualizado de los laboratorios del Departamento de Computación de la UNAN-León mediante la herramienta Integria IMS.

- Gestionar las incidencias de los laboratorios del Departamento de Computación utilizando el sistema de tickets proporcionado por la herramienta Integria IMS.

2 Marco Teórico

2.1 Conceptos generales

2.1.1 Sistemas de monitorización de red

El término Monitoreo de red (Monitorización de red) describe el uso de un sistema que constantemente monitoriza una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico u otras alarmas. Es un subconjunto de funciones de la administración de redes.

2.1.2 Sistemas de control de incidencias

Un sistema de seguimiento o control de incidentes (denominado en inglés como issue tracking system, trouble ticket system o incident ticket system) es un paquete de software que administra y mantiene listas de incidentes, conforme son requeridos por una institución. Los sistemas de este tipo son comúnmente usados en la central de llamadas de servicio al cliente de una organización para crear, actualizar y resolver incidentes reportados por usuarios, o inclusive incidentes reportados por otros empleados de la organización. Un sistema de seguimiento o control de incidencias también contiene una base de conocimiento que contiene información de cada cliente, soluciones a problemas comunes y otros datos relacionados. Un sistema de reportes de incidencias es similar a un Sistema de seguimiento de errores (bugtracker) y, en algunas ocasiones, una compañía de software puede tener ambos, y algunos bugtrackers pueden ser usados como un sistema de seguimiento de incidentes, y viceversa.

2.1.3 Sistemas de gestión de inventario

Un sistema de inventarios es un conjunto de normas, métodos y procedimientos aplicado de manera sistemática para planificar y controlar los materiales y productos que se emplean en una organización. Este sistema puede ser manual o automatizado. Para el control de los costos, elemento clave de la administración de cualquier organización, existen sistemas que permiten estimar los costos de las mercancías que son adquiridas y luego procesadas o vendidas.

2.1.3.1 Tipos de sistemas de inventario

- **Sistema de Inventario Perpetuo:** el negocio mantiene un registro continuo para cada artículo del inventario. Los registros muestran por lo tanto el inventario disponible todo el tiempo. Los registros perpetuos son útiles para preparar los estados financieros mensuales, trimestral o provisionalmente.

- **Sistema de Inventario Periódico:** En el sistema de inventario periódico el negocio no mantiene un registro continuo del inventario disponible, más bien, al fin del periodo, el negocio hace un conteo físico del inventario disponible y aplica los costos unitarios para determinar el costo del inventario final. Ésta es la cifra de inventario que aparece en el Balance General. Se utiliza también para calcular el costo de las mercancías vendidas. El sistema periódico es conocido también como sistema físico, porque se apoya en el conteo físico real del inventario. El sistema periódico es generalmente utilizado para contabilizar los artículos del inventario que tienen un costo unitario bajo.

2.2 Pandora FMS

Pandora FMS es un software de monitorización para gestión de infraestructura TI. Esto incluye equipamiento de red, servidores Windows y Unix, infraestructura virtualizada y todo tipo de aplicaciones. Pandora FMS tiene multitud de funcionalidades, lo cual lo convierte en un software de nueva generación que cubre todos los aspectos de monitorización necesarios para su organización.

2.2.1 Componentes

Pandora FMS está formado por tres componentes: servidor, consola y agente (uno o más de cada uno, dependiendo de la extensión y cantidad de elementos a monitorizar).

- ***Servidor:*** El servidor de Pandora FMS es quien procesa los datos recolectados de diferentes maneras; también son los que ejecutan alertas y guardan la información en la base de datos.

- ***Consola:*** Es la interfaz web con la interfaz al usuario para administrar los servidores, catalogar la información, crear alertas, crear incidentes, cambiar contraseñas de acceso y en general permiten toda la configuración del sistema de manera horizontal. Aquí se realiza la conversión de lenguaje de bajo nivel al lenguaje de alto nivel.

- ***Agente:*** Los agentes de Pandora FMS son entidades organizativas, generalmente un ordenador. Los agentes tienen la información, y pertenecen a un solo grupo. Un agente puede ser diferente de un computador, por ejemplo, un vehículo, una edificación o cualquier otro objeto que contiene información. El agente resguarda información en diferentes módulos y bien puede estar relacionado con otros agentes, mediante una o varias relaciones de parentesco. Los agentes son, por tanto, unidades organizativas dentro de Pandora FMS, un concepto donde se deposita información de otras unidades de información llamadas módulos.

2.2.2 Módulos

- ***Remotos:*** Los módulos remotos se comunican mediante protocolos o tecnologías bien conocidas o en su defecto con complementos plugin especialmente creados a tal efecto:
    - **Módulos de red:** ICMP, TCP, SNMP, WMI y muchos más.
    - **Complementos o plugin:** para MySQL, PostgreSQL, entre otros.

- ***Locales:*** Son módulos que se ejecutan en el mismo ordenador que supervisan, en realidad son guiones o scripts escritos en diferentes lenguajes como Bash, Perl, Python e inclusive programas específicos que, desde luego, deben estar previamente instalados para que puedan ser indagados, capturada su respuesta y enviarlos al servidor correspondiente que esté ejecutando Pandora FMS.

2.2.3 Monitorización de rendimiento y disponibilidad

Pandora FMS proporciona una solución completa para monitorizar rendimiento y disponibilidad, monitorizando los recursos claves a través de la infraestructura, para asegurarse de que todos los dispositivos están funcionando bajo los criterios de operación establecidos. Es posible ejecutar las pruebas de monitorización de forma remota, o hacerlos mediante un agente que recoge información local de la máquina donde está instalado.

Tabla 2 Rendimiento y disponibilidad

Ejemplo de monitores con agentes	**Ejemplos de test de rendimiento de red**
Tiempo de latencia de red	Respuesta ICMP (Ping)
Uso de CPU, Disco, Memoria, etc.	Respuesta SNMP (v1, v2c, v3)
Operaciones IO en un disco.	Servicios estándar (HTTP, SMTP, etc.)
Número de usuarios conectados a un servidor	Puertos específicos TCP/IP con expresiones regulares
Temperatura de un sistema	Disponibilidad de una web
Disponibilidad de servicio o procesos en ejecución	Disponibilidad de proceso Linux/Unix (vía SNMP)
Estado de una base de datos Oracle, sus tablespaces y otros valores	Soporte Nagios Plugin (disponibilidad y funcionamiento)

2.2.4 Comparativa funcionalidades Pandora FMS

La siguiente tabla es una comparativa d entre las versiones Community y Enterprise de Pandora FMS

Tabla 3 Comparativa entre versiones Community y Enterprise de Pandora FMS

Funcionalidades	Community	Enterprise
Monitorización de rendimiento y disponibilidad	✓	✓
Gestión de eventos	✓	✓
Sistema de correlación de eventos		✓
Recolección de logs		✓
Gestión centralizada empleando políticas de monitorización		✓
Actualizaciones de seguridad certificadas		✓

Geolocalización	✓	✓
Administración por línea de comando	✓	✓
Autenticación LDAP/AD		✓
Virtualización y cloud computing		✓
Alta disponibilidad	✓	✓
Escabilidad horizontal (Metaconsola)		✓
Monitorización de servicios (BAM)		✓
Consola visual personalizable	✓	✓
Módulos sintéticos (creación de datos dinámicamente sobre datos existentes)		✓
Base de datos de histórico para almacenar datos a largo plazo		✓
Distribución centralizada de plugins		✓
Capacidad recomendada por servidor	1000 agentes	Sin límite
Monitorización z/OS		✓*
Monitorización SAP R3		✓*
Monitorización Transaccional WEB		✓
Netflow	✓	✓
Consola SSH/Telnet	✓	✓

Agentes multiplataforma para Windows, HP-UX, Solaris, BSD, AIX y Linux	✓	✓
Gestión remota de configuración de agentes software (con políticas y de forma manual)		✓
Agentes para Android y sistemas empotrados	✓	✓
Inventario remoto o mediante agente		✓
Monitorización de Virtualización centralizada: Vmware, RHEV, XenServer, HyperV		✓
Monitorización Oracle, Informix, SyBase, DB2, Weblogic, Jboss, Exchange, Citrix, WebSphere (y otros).		✓
Sistema de skins para la personalización completa de la interfaz, por usuario		✓

Niveles de control de acceso basados en roles	✓	✓
Sistema ACL de grano fino. Multicliente 100% listo para explotar como servicio		✓
Informes avanzados de SLA		✓
Cuadro de mandos (Dashboard)		✓
Detección de topología de red y autodescubrimiento		✓
Monitorización SNMP v3	✓	✓
Soporte IPv6	✓	✓
Monitorización sin agentes descentralizada, gestionable remotamente de alta capacidad		✓
Monitorización SNMP y WMI descentralizada	✓	✓
Monitorización de traps SNMP	✓	✓
Mapas navegables dinámicos de red modificables por el usuario en un entorno gráfico (Network console)		✓
Exploración ICMP y SNMP de alta velocidad		✓

2.2.5 SLA e Informes

Pandora FMS puede crear informes HTML, PDF y XML para cualquier elemento monitorizado. A estos informes se pueden añadir datos como: gráficas, SLAs, métricas, sumatorios, tablas, eventos, etc.

2.2.6 Características de Pandora

a. Consola visual personalizable

Pandora FMS permite a cada usuario definir su vista de monitorización personalizada. Esta es una vista gráfica personalizada, basada en una representación en el espacio, con ítems seleccionados, estatus representado, datos, gráficas u otros estatus de la consola visual, escalando siempre el evento crítico. Esta funcionalidad, es una monitorización flexible de grupos de elementos, basado en márgenes definidos por el usuario. Esto difiere de la monitorización “específica” de elementos individuales, ya que permite gestionar “grupos” en su totalidad, con cierto margen de error, basado en la acumulación sucesiva de fallos hasta llegar a un umbral.

b. Gestión de errores y eventos

El sistema de eventos de Pandora FMS mantiene un log de todo lo que ha sucedido: cuando un servicio o un host se cae o cuando se recupera, cuando se dispara una alerta, cuando se descubren nuevos hosts en la red, etc.

c. Alta disponibilidad

Pandora FMS tiene una estructura basada en servidores múltiples (Data Server, Plugin Server, Network Server, etc.), una consola Web y una Base de Datos. Tiene redundancia sobre todos sus sistemas. Se puede crear cualquier cantidad de servidores o consolas, así como un clúster MySQL para la Base de Datos. Esto, está incluido en las características de la versión Open Source. Los agentes también disponen de mecanismos para poder enviar a varios servidores, por si falla uno de ellos.

d. Capacidad recomendada por servidor

Pandora FMS está diseñado para trabajar en entornos empresariales, esto significa, conjuntos de sistemas que puedan crecer, y crecer hasta el infinito. Nuestros ingenieros han estimado una media de 2.000 agentes por servidor (en el caso de la versión Open Source estimamos 1.000 agentes por servidor), con 25 módulos cada uno, ejecutando pruebas cada cinco minutos, generando eventos e histórico de datos pormenorizado de cada dato recogido.

e. Gestión centralizada con políticas de monitorización

Esta funcionalidad está dirigida principalmente a empresas que tienen una gran cantidad de agentes. El sistema de políticas permite al usuario distribuir módulos y alertas a grupos de agentes de forma homogénea y masiva. Esto, se complementa con la metaconsola, permitiendo operar de forma rápida y eficiente sobre miles de agentes de forma simultánea.

f. Monitorización SNMP

Soporta todas las versiones de SNMP y disponemos de nuestro propio gestor de MIBS, incluido un navegador online. Podrá obtener cualquier parámetro y usar wizards de recolección comunes para interfaces y recursos hardware. Podrá utilizar plantillas SNMP y desplegar la monitorización de forma descentralizada usando nodos de pandora o el satélite.

g. Detección de topología de red y autodescubrimiento

Pandora FMS es capaz de reconocer y detectar periódicamente nuevos sistemas no monitorizados, detectando su sistema operativo y su relación con otros nodos de la red, bien a nivel de red o a nivel de enlace (mediante exploración de tablas ARP vía SNMP). Esto significa que Pandora FMS puede explorar una red de 1,000 nodos y dibujar su red conectando las interfaces de sus routers con las de sus switches, en menos de una hora.

h. Monitorización de Traps SNMP

Pandora FMS tiene una consola Trap que muestra los eventos SNMP que han sido recibidos por el servidor de Pandora FMS, mostrando diversa información acerca del evento: su estatus, la fuente OID y el agente asociado, la fecha, si tiene alguna alerta asociada, etc. Se pueden configurar alertas sobre cada Trap, simples o incluyendo expresiones regulares sobre el Trap recibido.

i. Agentes multiplataforma

Existen Agentes software para Windows, Linux, AIX, HP-UX, Solaris, BSD y Mac: agentes de pequeño tamaño que proporcionan información acerca del sistema donde están instalados (CPU, uso de la memoria, uso de disco, la salida de cualquier comando de consola, etc.). También existen agentes hardware (sensores) para monitorizar la temperatura, humedad, humo, gas, inundaciones y cualquier dispositivo que envíe contacto seco.

2.3 Integria IMS

2.3.1 Características Generales

Integria IMS es una herramienta que nos permite hacer una gestión integral para empresas, organizaciones y equipos de trabajo. IMS son las siglas de “ITIL Management System”, lo que implica que Integria sirve para gestionar una organización desde el punto de vista ITIL.

A un nivel más funcional, podemos definir Integria como una herramienta para la gestión de tickets, proyectos, recursos humanos, imputación de horas/time tracking, combinado con un completo sistema de inventario, y un sistema de CRM (gestión de clientes), un Wiki, gestión de asignación de tareas, una Base de conocimiento, un sistema de distribución de ficheros y algunas otras funcionalidades más. Todo ello vía WEB, multiusuario/multi-perfil.

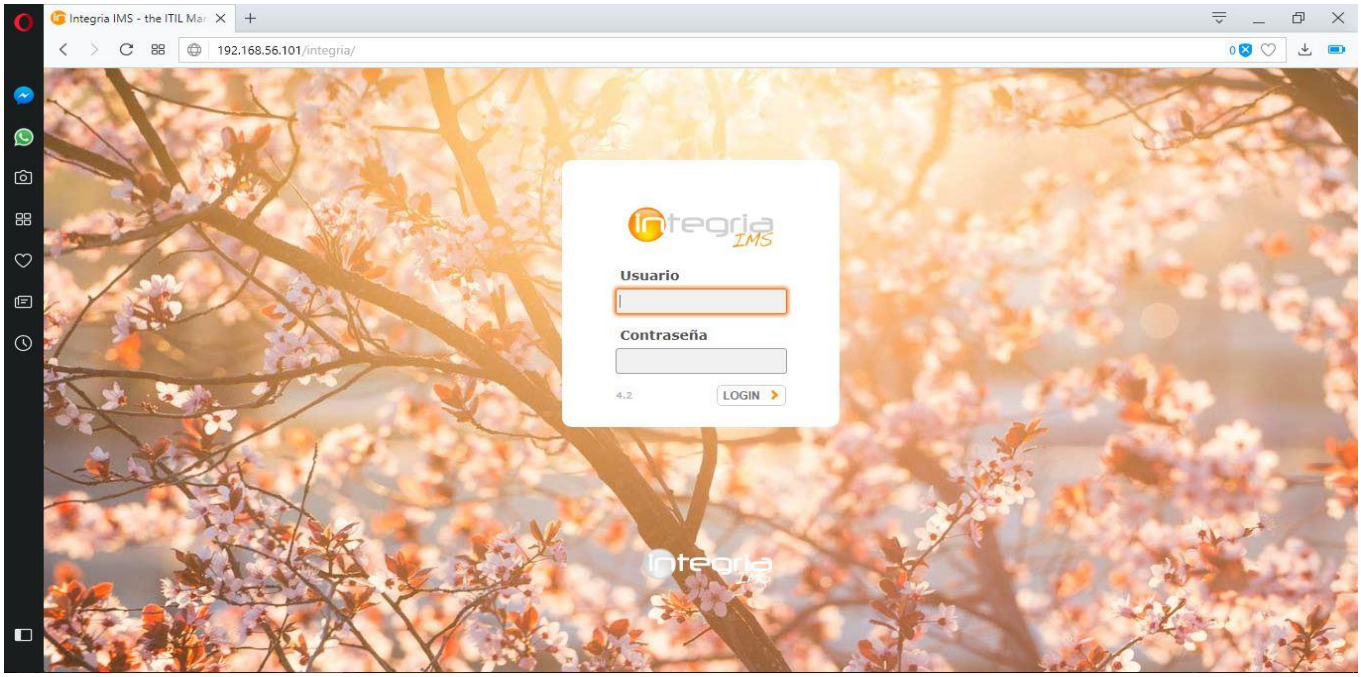


Figura 1 presentacion de integria en el navegador

2.3.2 Elementos característicos de Integria

Gestión de tickets (ticketing). Gestión de proyectos. Gestión del tiempo (time tracking). Gestión del conocimiento (knowledge base). Sistema de inventario (cmdb). Agenda. Wiki. Gestión de leads, empresas, contratos, contactos y facturas (CRM). Entorno centralizado de descargas de software. Control de personal.

2.3.3 Sistema de gestión de clientes (CRM)

Constituye por sí mismo un CRM completamente funcional. Incluye gestión de newsletters. Se utiliza para gestionar cuentas de clientes, contactos, contratos, leads, y tiene una gestión de facturas emitidas integrado en el sistema.

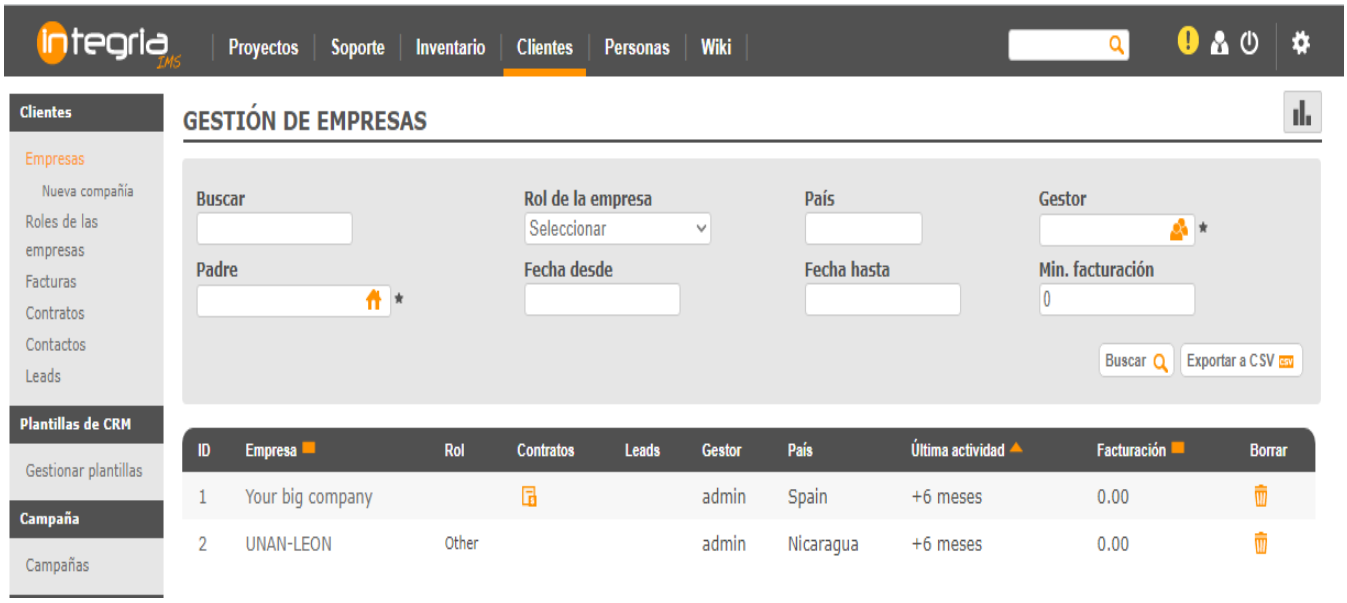


Figura 2 Gestión de clientes o proveedores

2.3.4 Inventario (CMDB)

Integria integra un sistema de inventario flexible, donde los tipos de objetos, los campos y las relaciones entre ellos son definidos por el administrador. Esto permite desde gestionar un stock de dispositivos de forma sencilla, hasta implementar una CMDB con datos que ya existan en su organización. El sistema de inventario está vinculado (opcionalmente) al CRM y al sistema de Ticketing.

2.3.5 Gestión de usuarios, roles, grupos, perfiles

Una de las características más importantes de Integria IMS es la posibilidad de trabajar con diferentes grupos de usuarios con accesos y visualización de elementos independientes, de modo que cada grupo sólo visualizará su información y elementos, siendo invisible el contenido de los otros grupos. Estos grupos de usuarios pueden ser departamentos, clientes o empresas diferentes. A esta característica generalmente se la conoce como entorno Multitenant.

2.3.6 La estructura de permisos se basa en tres conceptos:

- ***Grupo*****:** Conjunto de usuarios con visibilidad entre ellos, un grupo puede ser traducido por "departamento", "cliente" o "empresa", según sea el contexto del uso de Integria y la forma de trabajar deseada.

- ***Perfil*****:** Nivel de permisos. Define una serie de privilegios, por ejemplo: acceso a la agenda, tener acceso para crear tickets, o ser gestor de proyecto.

- ***Usuario*****:** Identificador para acceder a la herramienta. Los usuarios tendrán asociados una o varias combinaciones de perfil+grupo, definiendo el nivel de privilegios que tendrán y para qué grupo, pudiendo ser, por ejemplo, gestor de proyectos en un grupo y operador de tickets en otro.

- ***Usuarios*****:** Los usuarios de Integria IMS pueden tener diferentes perfiles para diferentes grupos (gestor de los tickets para una empresa, participante en un proyecto, etc.), definiendo el nivel de privilegios que tendrán sobre las diferentes secciones y funcionalidades de Integria. Mediante este flexible sistema los usuarios pueden pertenecer a diferentes grupos y tener diferentes roles en cada uno de ellos.

2.3.7 Gestión de Tickets

Integria IMS propone una visión de la gestión de tickets adaptable a diferentes necesidades: se puede entender un ticket como un problema técnico, el resultado de una intervención planificada, un bug de software o una hoja de trabajo sobre un problema más complejo.

Los tickets tienen una serie de características básicas, que responden a las necesidades de entornos de trabajo con tickets habituales, tales como la gestión mediante grupos de trabajo, usuarios creadores y propietarios, comentarios y seguimiento, asociación a objetos de inventario, SLA, etc.

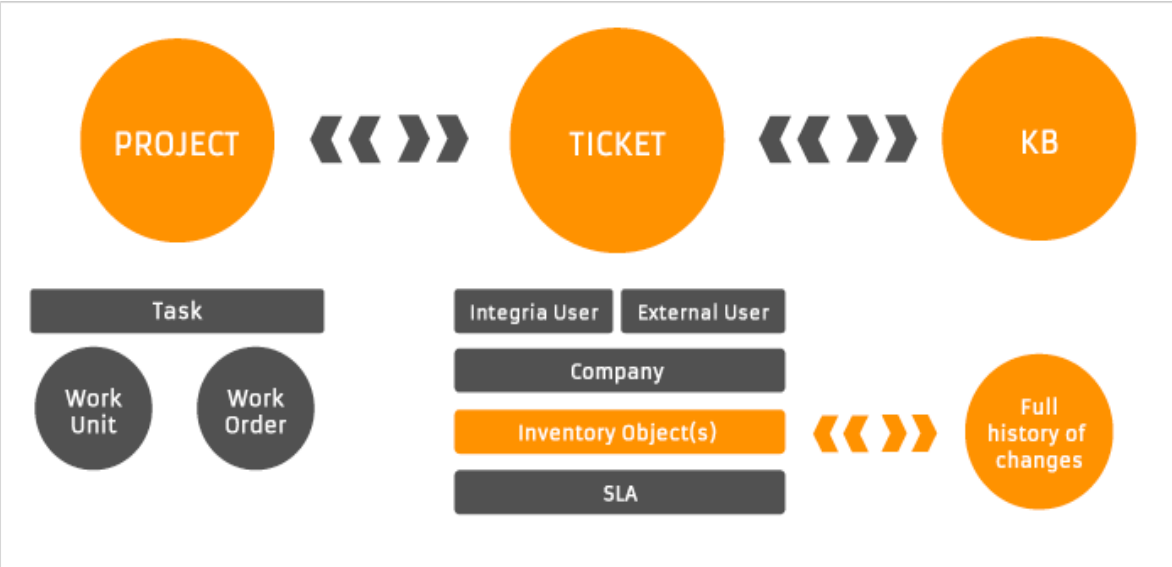


Figura 3 Flujo de ticket

Estados de un ticket

Uno de los campos más importantes de los tickets es el estado. Mediante este campo podremos hacer un seguimiento preciso del momento de su vida en que se encuentra el ticket, bien si es algo reciente, si está se encuentra a la espera de agentes externos, pendiente de cierre o cerrado. Este ciclo está abierto al usuario y se puede pasar de uno a otro sin restricción por defecto.

Es posible definir un flujo controlado para restringir el orden de los estados por los que un ticket puede pasar mediante la característica del Mapeo de estados. Haciendo uso del mapeo de estados podemos definir si un ticket debe pasar por diferentes fases antes de ser cerrado.

Figura 4 Estados de ticket

Usuarios en un ticket:

a. **Creador del ticket:** Es el autor original del ticket. Es quien establece el responsable de ese ticket (a no ser que esto se haga automáticamente, como veremos más adelante), el grupo al que pertenece el ticket (ídem) y otros parámetros como su criticidad, descripción, elementos de inventario a los que está vinculado, etc.

b. **Propietario del ticket:** Usuario asignado al ticket. Habitualmente en la definición de grupos se asigna un usuario predeterminado, que será el usuario al cual se le asignará el ticket por defecto, en función del grupo seleccionado por el usuario creador del ticket. Los privilegios que tendrá dependerán de su nivel de perfil para el grupo del ticket, puede ser simple lectura (usuario genérico) o permisos de gestión.

c. **Usuario con acceso de escritura al ticket**: El ticket siempre pertenece a un grupo. Todos los usuarios con el flag de acceso "IW" pueden escribir UT (Unidades de Trabajo o Workunit en inglés) sobre un ticket. Estas UT son comentarios que quedan reflejados en el ticket a modo de seguimiento personal, indicando acciones realizadas o facilitando datos. Este tipo de usuario no puede modificar ningún otro detalle del ticket, tal como estado o criticidad, ni alterar la descripción principal del ticket

d. **Usuario con acceso de lectura al ticket:** Cualquier usuario que pertenezca al grupo de trabajo de un ticket y tenga el flag de acceso “IR” podrá leer los detalles del ticket, aunque no podrá modificar nada, ni agregar comentarios o fichero.

e. **Usuario con acceso de gestión al ticket**: Un usuario con el bit de acceso IM sobre el grupo al que pertenece un ticket puede operar con el como si fuera el propietario del mismo. Esto implica que puede «escalar» el ticket apropiándoselo o traspasar la responsabilidad del mismo a otro usuario. Por supuesto puede agregar UT o ficheros e incluso cerrar el ticket.

f. **Usuario que cierra el ticket:** Puede ser cualquier usuario con permisos de gestión sobre el ticket. A la hora de cerrar un ticket aparece un nuevo campo “Cerrado por”, pudiendo elegir cualquier usuario del grupo; naturalmente por defecto será el usuario que lleve a cabo la acción de cerrar el ticket.

g. **Usuario suscrito a un ticket**: Cualquier persona que haya participado en algún momento durante la vida del ticket, realizando modificaciones o añadiendo comentarios. También recibirá notificaciones con las actualizaciones que se produzcan en el ticket. En la solapa “Contactos” podemos ver la lista completa de las personas que participan en un ticket.

2.3.8 Gestión de SLA

El SLA es la forma de “comprobar” que la gestión de tickets funciona bajo unos criterios. Integria cuenta con funcionalidades de gestión automática de SLA.

El SLA se procesa conforme unos parámetros:

- **Nombre:** Conjunto de reglas que definen un tipo de SLA en particular.
- **Enforced:** Hace que el SLA dispare los emails cuando se incumpla (enforced) o que solo avise con un indicador luminoso.
- **SLA Base:** Indica relación con otro SLA a nivel informativo.

2.3.8.1 Tipo SLA

- **SLA Normal:** Se tendrán en cuenta, a la hora de hacer el cálculo, los tickets que no se encuentren en estado Cerrado o Pendiente de terceros.
- **SLA de terceros:** Se tendrán en cuenta los tickets que estén en estado Pendiente de terceros.
- **Ambos**: Se tendrán en cuenta los tickets que estén en cualquier estado que no sea Cerrado.

2.3.8.2 Max. Tiempo de respuesta

En horas, tiempo máximo que puede transcurrir entre una workunit del creador del ticket y otra respuesta. Por ejemplo, si este tiempo son 4 horas, y un ticket nuevo tiene 4.1 horas de vida, se disparará el SLA. Si un ticket ya tiene varios días de vida y la última unidad de trabajo o workunit es del creador del ticket, tras 4 horas sin respuesta también se disparará el SLA.

- **Max. Tiempo de resolución:** en horas, el máximo tiempo de vida de un ticket. Si un ticket tiene más de ese tiempo y no está cerrado o resulto, saltará el SLA.
- **N.º Máx. de tickets abiertos al mismo tiempo:** si se supera, saltará el SLA.
- **Max. tiempo inactividad:** Tiempo en el que el ticket no tiene ningún cambio.
- **Hora de comienzo para activar el SLA:** hora del día a partir de la cual el SLA se empieza a calcular (p.e: 9 de la mañana).
- **Hora de fin para una SLA:** hora del día a partir de la cual el SLA ya no se calcula (p.e: 18h).
- **Deshabilitar SLA en fines de semana:** los fines de semana no se incluirían en los cálculos de SLA.
- **Deshabilitar SLA en vacaciones:** los días definidos de vacaciones no se incluirán en los cálculos de SLA.
- **Descripción:** informativo.

2.3.8.3 ¿Qué significa "saltará el SLA"?

Significa que el sistema enviará una notificación por email al propietario del ticket, advirtiendo que el ticket no cumple los parámetros establecidos en el conjunto de reglas de SLA asociada al ticket. Esto dependerá del grupo al que está asociado el ticket, ya que es en la configuración de grupo donde especificamos qué SLA se aplicará a los tickets de grupo:

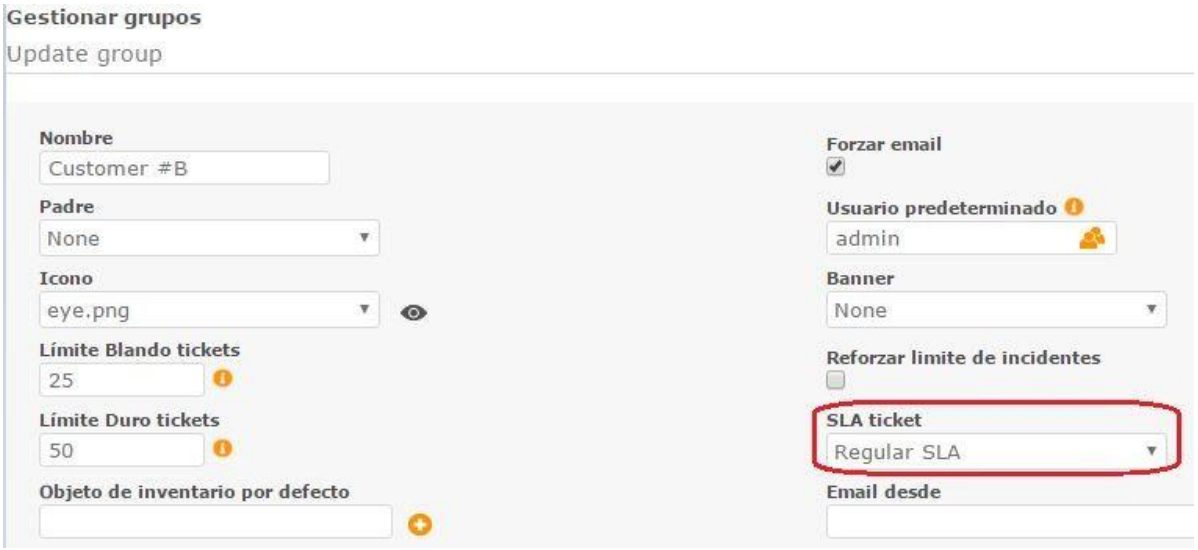


Figura 5 Aplicación de SLA a los Grupos

2.3.8.4 Ejemplo de definición de SLA:

Figura 6 Configuración de SLA y ticket

Los SLA están vinculados al estado de los tickets. De forma que si el tipo de SLA elegido es *Normal* no se aplicará el SLA para los tickets que están en estados Cerrado y Pendiente de terceras personas.

Si el tipo elegido es *SLA de terceros* sólo se aplicará el SLA para los tickets que estén en estado Pendiente de terceras personas. Si se eligen *Ambas* se aplicará el SLA para todos los tickets excepto los que estén en estado Cerrado.

2.3.9 Versiones disponibles para el uso de Integria IMS

Figura 7 Versiones de Integria IMS

3 Diseño Metodológico

3.1 Etapa I. Etapa de Exploración

En esta etapa se realizaron entrevistas e inspeccionaron a fondo los laboratorios con la finalidad de determinar los problemas que los afectan, para esto decidimos dividir la etapa en dos sub-etapas.

1) **Investigación:** En esta sub-etapa se recopiló la Información acerca del tema, haciendo búsquedas en libros, sitios web, etc. Se realizaron entrevistas al Ingeniero Marvin Somarriba (Administrador del Laboratorio Hardware del Departamento de Computación) y al Ingeniero Jorge Treminio (Responsable de la Unidad de Redes de la UNAN-León) También se inspeccionaron los laboratorios con el objetivo de conocer mejor las diversas problemáticas y el estado actual de los mismos.

2) **Identificación:** En esta sub-etapa se delimita el problema haciendo uso de la información recopilada en la sub-etapa anterior.

3.2 Etapa II. Selección de las herramientas

Luego de identificar y delimitar el problema, en esta etapa se ideó una estrategia para darle solución para lo cual se probaron diversas herramientas en un entorno controlado. Esto se hizo a través de la creación de una pequeña red de 5 máquinas donde se evaluaron y se seleccionaron las herramientas que a nuestro criterio eran las que mejor se adaptaban a las necesidades de los laboratorios.

3.3 Etapa III. Implementación de la solución

Aquí se procedió a implementar las herramientas previamente evaluadas mediante varias sub-etapas.

1) **Establecimiento de un lugar de administración centralizado**: Se designó el laboratorio de hardware como centro de control y administración de los demás laboratorios.

2) **Instalación y configuración del servidor:** Establecimos una computadora proporcionada por el Departamento de Computación como servidor desde donde se monitorizan los demás laboratorios y se gestionan los reportes de incidencias e inventario. En este equipo se instalaron las herramientas seleccionadas. Además, con el apoyo de la división de informática se proporcionó al equipo una IP fija accesible desde los laboratorios a monitorizar.

3) **Instalación de los agentes en los laboratorios**: Aquí se procedió a instalar el agente de monitorización en cada uno de los equipos de cada laboratorio en equipos con sistemas Windows y Linux.

3.4 Etapa IV. Prueba en el entorno físico de los laboratorios:

En esta etapa procedimos a realizar pruebas del funcionamiento del servidor y de las herramientas al momento de monitorizar los equipos de los laboratorios por un período de dos semanas, con el fin de garantizar la resolución de los problemas antes planteados y el buen funcionamiento del sistema.

3.5 Etapa V. Conclusiones y redacción del informe final

En esta última etapa se redacta las conclusiones y el informe final.

4 Resultados

4.1 Selección de las herramientas

Lo primero a abordar en el acápite de resultados es la selección de las herramientas. Se realizaron diversas pruebas para poder determinar cuál era la que mejor se adaptaba a los requerimientos de la solución que deseábamos proponer. Entre las herramientas evaluadas se encontraron: Cacti, OTRS, Request Tracker, etc. siendo Pandora FMS e Integria IMS las que finalmente fueron seleccionadas por las siguientes razones:

- Pandora FMS monitoriza y muestra el estado actual de los equipos, visualiza un mapa de red de los mismos y permite automatizar la creación inmediata de un ticket ante un determinado fallo el cual es enviado a Integra IMS.
- Integria IMS permite llevar un control de las incidencias y la creación de un inventario en un mismo sistema con lo cual es fácil indicar sobre que elemento del inventario es que se crea la incidencia. Además tiene una fácil integración con Pandora FMS.
- Ambas herramientas son de OpenSource y tienen una versión que gratuita que responden a las necesidades de los laboratorios.
- Ambas herramientas poseen interfaces web intuitivas que permiten un rápido aprendizaje por parte de los usuarios además de poder coexistir sin ningún problema en el mismo servidor.

4.2 Equipo de monitorización

Para la instalación y puesta en marcha de la solución, se solicitó un equipo al Departamento de Computación un equipo que es el que funcionaría como servidor. Dicho equipo es un computador HP con un procesador Intel Celeron, 1 GB de memoria RAM y 40 GB de disco duro. En él se instaló CentOS 6 como sistema operativo y las herramientas Pandora FMS 6 e Integria IMS. Finalmente se asignó al servidor una dirección IP fija proporcionada por la División de Informática de la UNAN-León la cual es accesible desde todos los laboratorios.

Como medida de seguridad para el servidor, se bloquearon los puertos USB, se configuró el modo servidor para los casos en que haya corte de energía y se alojó en laboratorio de Hardware en un espacio aparte de las máquinas de uso frecuente y sin monitor, teclado y mouse.

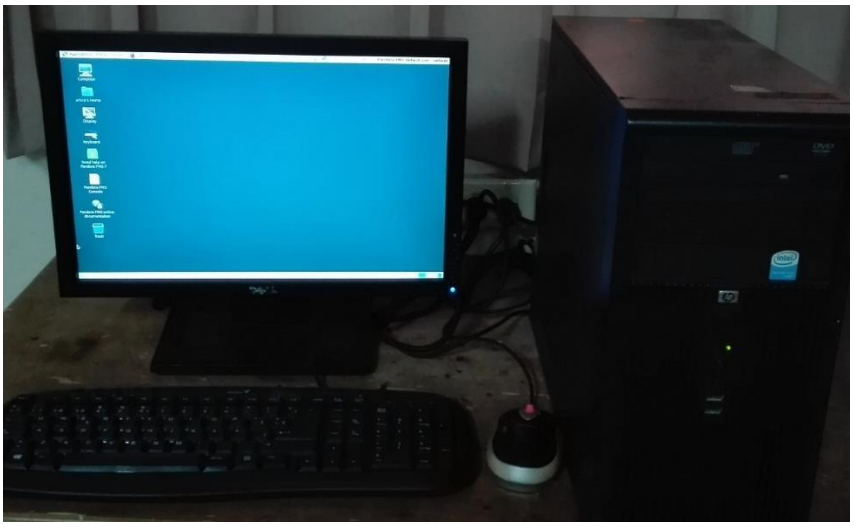


Figura 8 Servidor proporcionado por el Departamento

4.3 Monitorización de los laboratorios

Se instaló el agente Pandora FMS y se habilitó el protocolo SNMP en máquinas de los laboratorios Cisco, Alcalá 1, Alcalá 2 y Laboratorio 1, tomando como muestra 7 equipos con sistemas operativos Linux y Windows en cada uno ellos. Los equipos en los que se instaló el agente Pandora FMS fueron agregados manualmente al servidor con el fin de controlar que equipos son monitorizados. Por cada equipo se agrega el nombre de la computadora y dirección IP y de forma automática Pandora FMS detecta el resto de la información del equipo y activa los módulos básicos a monitorizar.

Para garantizar la comunicación entre el servidor y las máquinas de los laboratorios se habilitaron algunos puertos garantizando así que la información llegara sin problemas. El periodo de prueba de la monitorización fue de 2 semanas durante las vacaciones de los estudiantes. Durante este período se garantizó que los mensajes SNMP e ICMP llegaran de las máquinas de todos los laboratorios y que el estado de los recursos a monitorizados variará en función del estado de la máquina.

Tabla 4 Lista de criterios

Módulos	**Descripción**
Volumen de disco	Espacio libre en disco
Carga de CPU	Porcentaje de carga de CPU
DHCP	Chequea si el servicio DHCP si está disponible (modulo habilitado únicamente en S.O Windows)
Memoria RAM	Muestra el porcentaje de uso de la memoria RAM
Numero de proceso	Total, de procesos ejecutados
LastLogin	Muestra el ultimo ingreso de usuarios (modulo disponible únicamente en S.O Linux)
Memoria Swap	Porcentaje en memoria Swap (modulo disponible en S.O Linux)
Uso de la red	Total, de bytes transferido en el sistema (modulo disponible en S.O Linux)

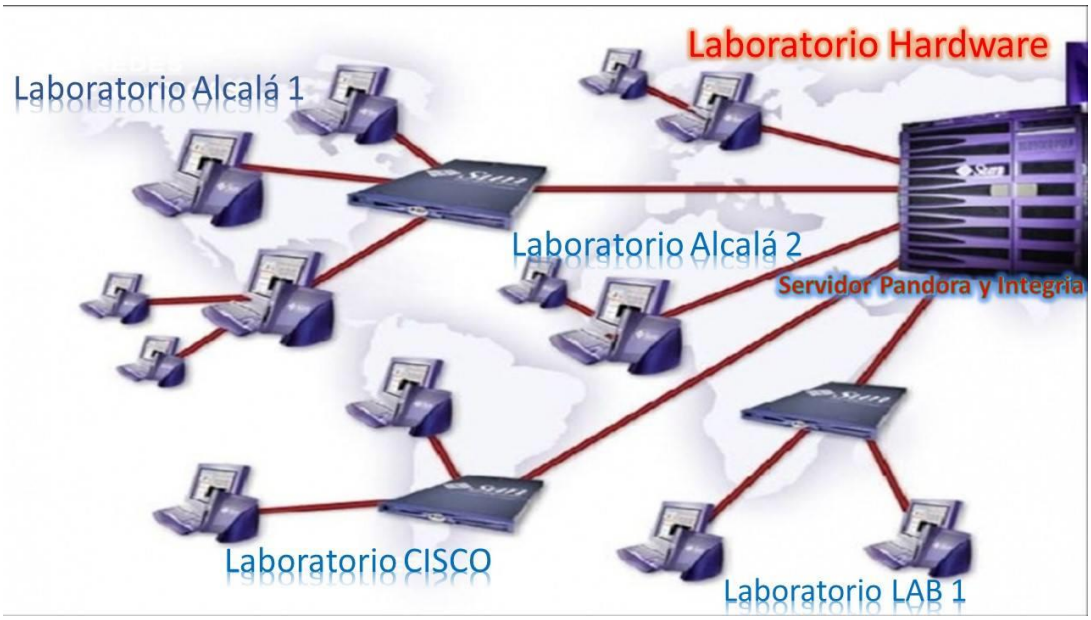
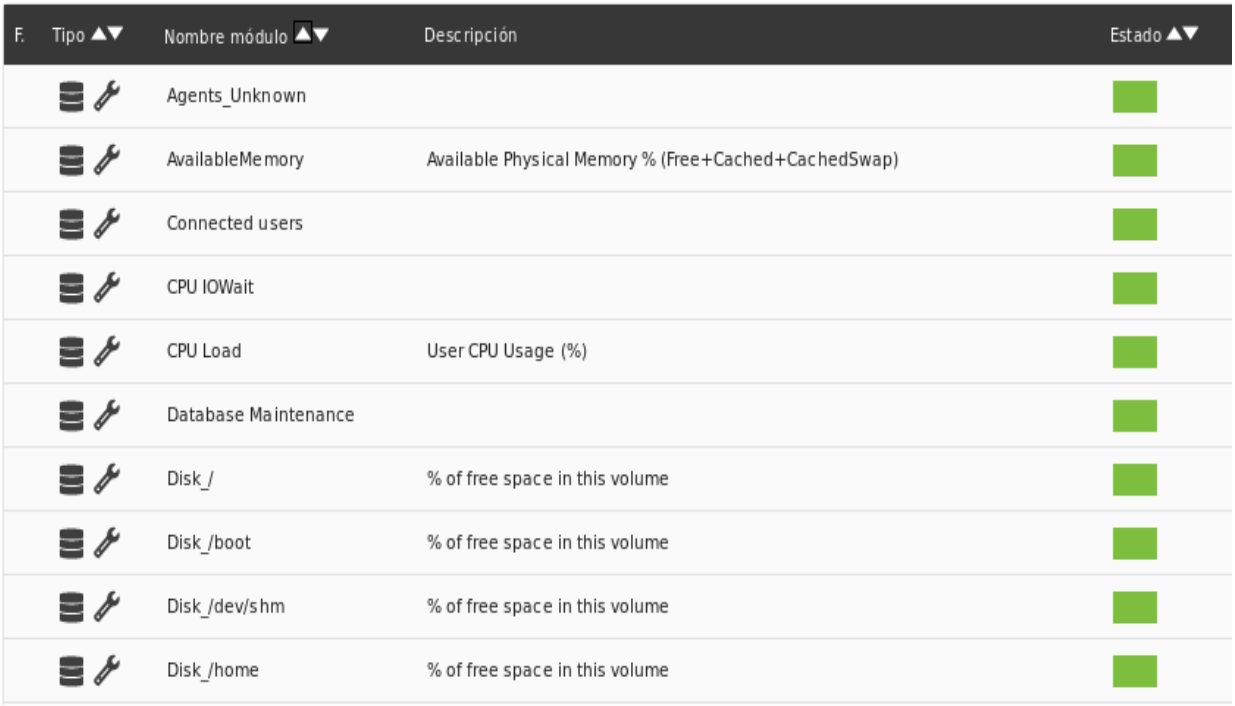


Figura 9 Mapa lógico de red



F.	Tipo	Nombre módulo	Descripción	Estado
		Agents_Unknown		
		AvailableMemory	Available Physical Memory % (Free+Cached+CachedSwap)	
		Connected users		
		CPU IOWait		
		CPU Load	User CPU Usage (%)	
		Database Maintenance		
		Disk_/	% of free space in this volume	
		Disk_/boot	% of free space in this volume	
		Disk_/dev/shm	% of free space in this volume	
		Disk_/home	% of free space in this volume	

Figura 10 Lista de módulos

Se creo un Shell Script con la función de depuración de la base de datos de Pandora FMS cada que se ejecutase cada 24 horas a fin de mantener el funcionamiento del servidor en óptimas condiciones.

```
#!/bin/bash
/usr/share/pandora_server/util/pandora_db.pl /etc/pandora/pandora_server.conf
```

Figura 11 Shell Script

4.4 Gestión de incidencias

Se configuro Integria IMS en el mismo servidor que Pandora FMS ya que ambas herramientas se vinculan para la generación de los tickets. Pandora detecta las incidencias y por medio de ese vínculo genera ticket a Integria IMS. Los administradores podrán ver no sólo las incidencias que reporta Pandora FMS sino también las incidencias que generen los usuarios.

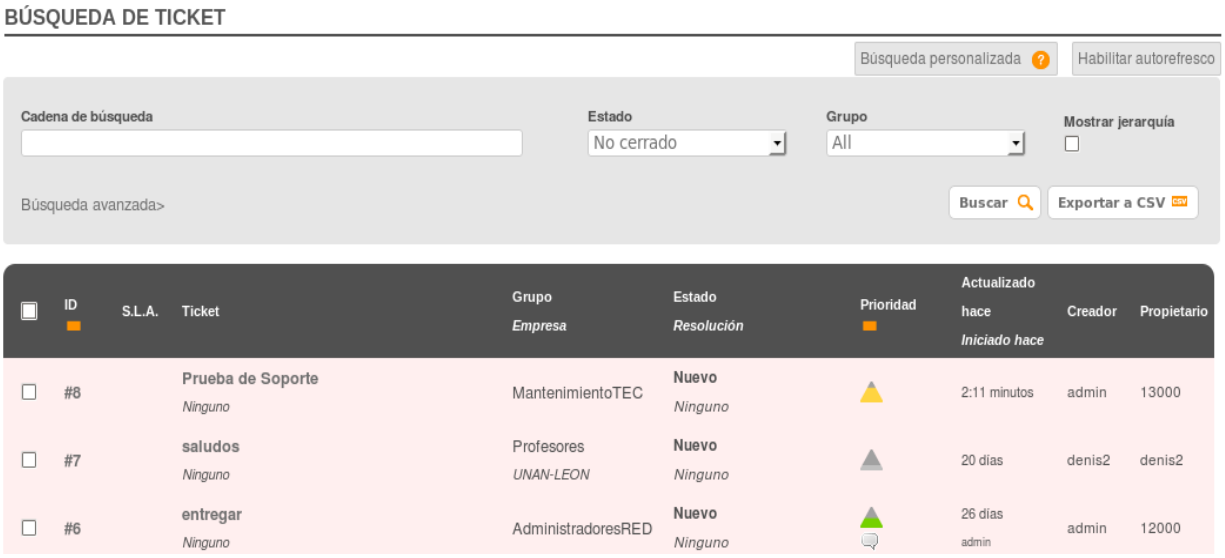


Figura 12 vista de ticket

Integria IMS cuenta con un manejador de usuarios el cual nos permite llevar un control del personal que tenga acceso al servidor también cuenta con la opción de poder organizar los usuarios en grupos y asignarle a cada usuario una tarea determinada.

Esto permite agilizar comunicación entre todos los grupos encargados de monitorización y supervisión de los laboratorios de manera que las incidencias que se detecten podrán ser tratadas de inmediato por el usuario o personal encargado.

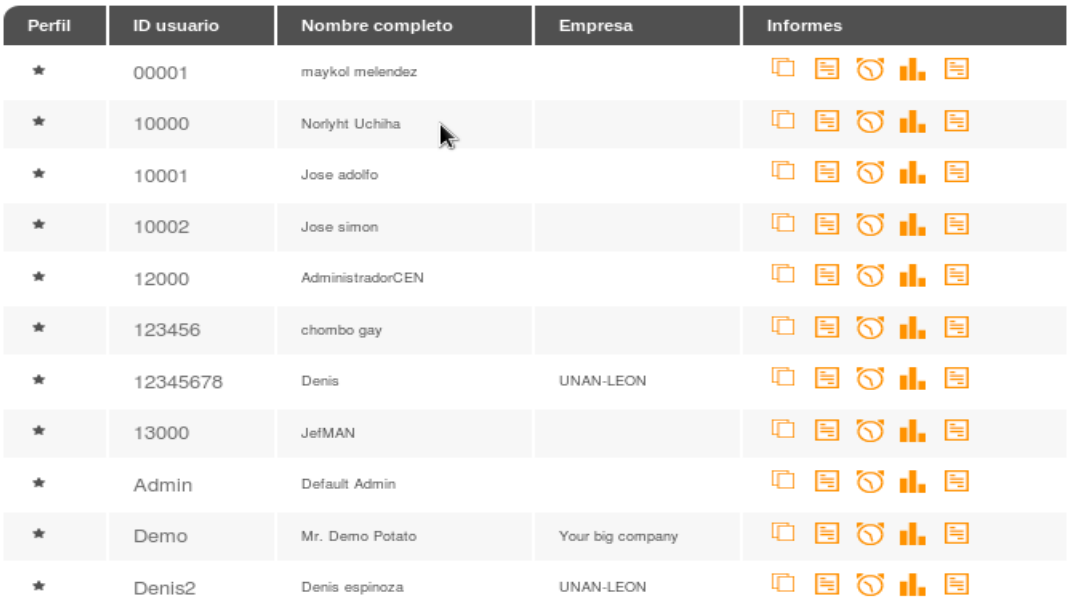


Figura 13 Vista general de la pestaña persona

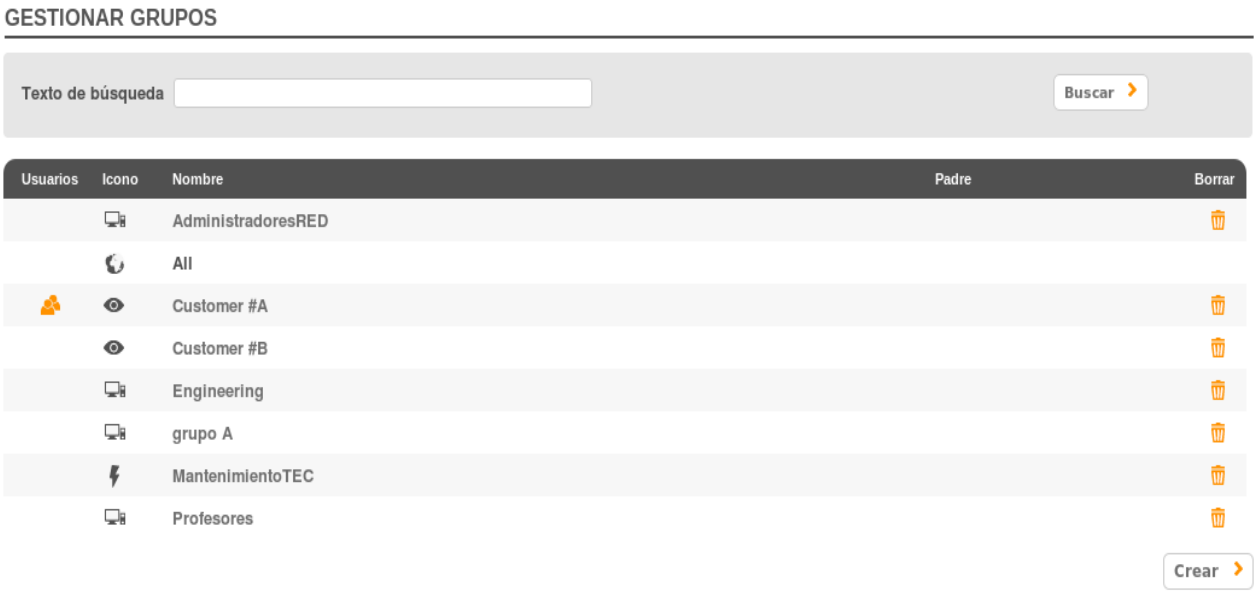


Figura 14 vista de gestión de Grupos

En caso de que la propuesta de Integria IMS para la gestión de incidencia se ha adoptada por el Departamento de Computación se capacitará a un Administrador de los laboratorios para el manejo y administración del sistema de ticket, también se dejara en el documento una explicación de los pasos a seguir para reportar una incidencia de forma que el personal docente y administrativo puedan utilizar el sistema.

A continuación se muestra un diagrama de flujo de la puesta en marcha de Integria IMS:

Figura 15 Diagrama de flujo de ticket

4.5 Realización del inventario

Para la creación del inventario de los laboratorios no se utilizó el existente en la Universidad por no encontrarse actualizado, por el contrario, se decidió recopilar la información personalmente creando un registro por cada objeto incluyendo las características que consideramos más apropiadas como código de registro, tipo de objeto, una breve descripción y algún otro campo dependiendo del tipo de objeto a inventariar.

Se creó un código de registro personalizado que permite brindar más detalles acerca del objeto como por ejemplo donde está ubicado, su tipo y el estado en que se encuentra. A continuación, se presenta la forma la estructura de este código:

Estructura del código de registro: FAC-DEP-LAB-CODIGONUMERICO-3DGITOS

Por ejemplo, para una silla del laboratorio Cisco el código sería: CT-CMP-LC011-001 sería leído de la siguiente manera

Facultad: Ciencias y Tecnología (CT)

Departamento: Computación (CMP)

Laboratorio: Laboratorio Cisco (LC)

Tipo de objeto: El primer y segundo dígito indican el tipo de objeto y el tercer dígito indica el estado en el que se encuentra el objeto:

Tabla 5 Tipos de objetos inventariados

Objeto	Número
Silla	01
Mesa	02
Computador	03
CPU	04
Estabilizador	05
Monitor	06
Mouse	07
Teclado	08
HD	09
Kit Arduino	10
Kit robótico	11
Soplete	12
Switch	13
Kit-herramientas de reparación	14
Impresoras	15
Router	16
Cámara	17
Data show	18
Repuesto	19

Tabla 6 estado de objetos inventariados

Estado	Número
Nuevo	1
En uso	2
Dañada	3
En reparación	4

Y los últimos 3 dígitos se usarán para diferenciar el objeto del mismo tipo ejemplo si hay varias sillas serian silla1 (001) y la silla2 (002).

Una vez definida el código de registro personalizado procedimos a inventariar los objetos de los siguientes laboratorios: Hardware, Cisco, Alcalá 1, Alcalá 2, Laboratorio 1 y Laboratorio 2. No se inventario el laboratorio ACAI-LA debido a que no se obtuvo permiso para acceder. Toda esta información se recopiló en un periodo de 2 semanas en octubre del 2017.

814	Codigo-Inventario	CodigoREG	Num-Sensores	num-Piezas	Descripcion
815	25655	CT-CMP-LH-102-001	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
816	25645	CT-CMP-LH-102-002	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
817	25651	CT-CMP-LH-102-003	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
818	25659	CT-CMP-LH-102-004	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
819	25643	CT-CMP-LH-102-005	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
820	25647	CT-CMP-LH-102-006	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
821	25644	CT-CMP-LH-102-007	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
822	25653	CT-CMP-LH-102-008	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
823	25642	CT-CMP-LH-102-009	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
824	25648	CT-CMP-LH-102-010	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
825	25640	CT-CMP-LH-102-011	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
826	25658	CT-CMP-LH-102-012	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador
827	25650	CT-CMP-LH-102-013	3 SENSORES	10 PIEZAS	Arduino robot explorador y rastreador

Figura 16 Recopilación de inventario Excel

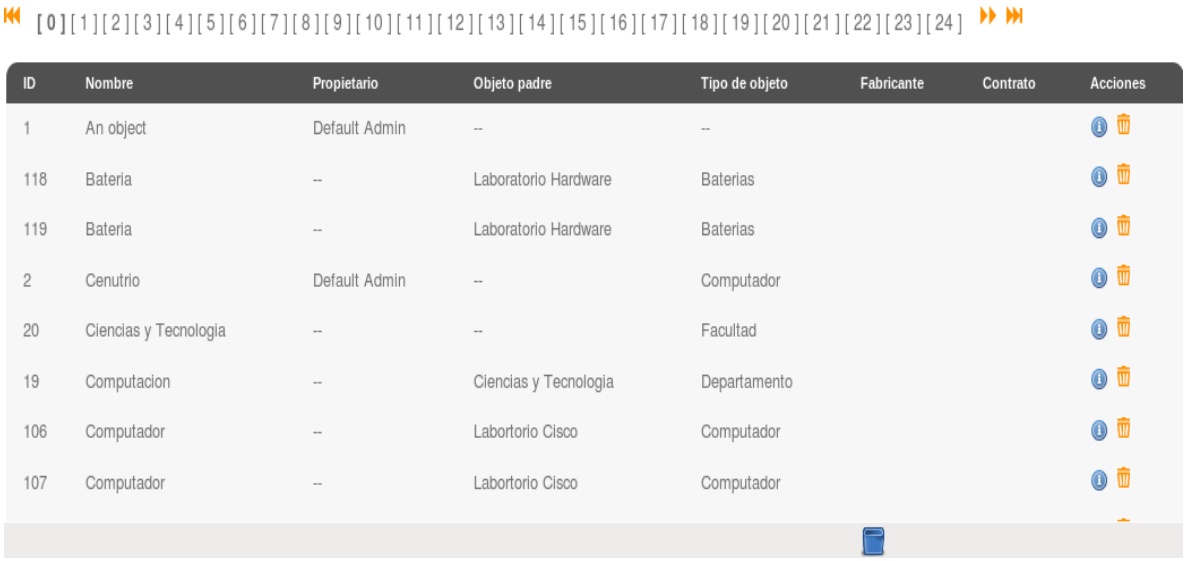


Figura 17 Vista general de inventario

Durante este proceso se observó que muchos de los objetos no tenían la etiqueta inventario de la Universidad, así como el evidente deterioro en el que se encontraban muchos de estos. Una vez recopilada la información se procedió a ingresar los datos en un archivo de Excel para su organización y posteriormente se ingresaron a la base de datos de inventario de Integria IMS. Los objetos en Integria IMS fueron organizados siguiendo una estructura jerárquica.

Figura 18 Vista de árbol de inventario

4.6 Valoraciones

De los resultados obtenidos y las pruebas realizadas consideramos oportuno realizar las siguientes valoraciones:

1. La implementación de la monitorización con la herramienta Pandora FMS permite tener un mejor control del estado de los equipos en los laboratorios. Si bien es cierto, no es un mecanismo suficiente, es un complemento valioso al chequeo frecuente que realizan los administradores de los laboratorios. Así mismo, la información que aporta la monitorización es de vital importancia para la toma de decisiones acerca de que instalar en lo equipos o incluso del uso que se da a los mismos.
2. La utilización del gestor de incidencias de Integria IMS, permitiría mantener un mejor registro de las diferentes incidencias que se suscitan en los laboratorios. También ayudaría a generar estadísticas que identifiquen los principales focos así como distribuir y organizar mejor los esfuerzos por mantener a punto los laboratorios.
3. Por último, el proceso de actualización, organización e ingreso del inventario de los laboratorios a Integria IMS, ayudaría a que cada administrador de laboratorio, tenga una visión más clara de los elementos que tiene a su cargo, realizar asignaciones o préstamos de equipos de forma fácil y generar informes de forma rápida.

5 Aspectos finales

5.1 Conclusión

Al finalizar nuestro trabajo monográfico podemos concluir que hemos desarrollado una propuesta de una solución para el monitoreo de los laboratorios del Departamento de Computación de la UNAN-León mediante la implementación de las herramientas Pandora FMS para el monitoreo mediante el protocolo SNMP e Integria IMS para el mantenimiento de un inventario actualizado de los laboratorios además de una gestión de ticket que permitirá llevar un mejor control de las incidencias.

5.2 Recomendaciones

A nivel general las recomendaciones sobre este proyecto tienen como objetivo contribuir con la mejora continua del funcionamiento de los laboratorios del Departamento de Computación de la Facultad de Ciencias y Tecnología UNAN-León. Por tanto se recomienda:

- ✓ Instalar el agente Pandora FMS en la mayor cantidad de dispositivo que conforman la red. De esta manera se podrá realizar un mejor proceso de gestión de recursos.

- ✓ Actualizar ambas aplicaciones a media que el fabricante lance versiones nuevas, debido a que generalmente solucionan inconvenientes que se presentan con las versiones actuales e ingresan nuevas funciones para mejorar la calidad de experiencia percibida por el usuario final.

- ✓ Instar a todo el personal docente que haga uso de los laboratorios a reportar cualquier incidencia en Integria IMS para que el personal técnico encargado de solución al instante.

- ✓ Que los Administradores de los laboratorios puedan profundizar en el conocimiento de las herramientas Pandora FMS e Integria IMS para obtener un mayor manejo de ellas.

Anexos

Anexo 1: Entrevistas

Ing. Jorge Treminio

1. ¿Qué programas se utilizan para monitorizar La red de la Universidad?
   R: Nagios.

2. ¿Se monitorizan los laboratorios del Departamento de Computación? ¿por qué?
   R: Si, para tener la disponibilidad en la red.

3. ¿Que se monitoriza en la red de la UNAN?
   R: Que este activo los enlaces de cada edificio y amenazas lógicas y físicas.

Ing. Marvin Somarriba

1. ¿Cuantos laboratorios posee el Departamento de computación?

   R: Posee 7 laboratorios disponibles para los estudiantes desde el día lunes a sábado.

2. ¿Cada cuánto tiempo se les da mantenimiento a los laboratorios?
   R: Debido a su constante uso a los laboratorios se les da mantenimiento una vez por semana.

3. ¿Quiénes son los encargados de los laboratorios del Departamento de Computación?
   R:
   Denis Berrios:
   - Acai-la
   - Cisco
   - Laboratorio 2
   - Alcalá 2 o ATM

   Lester Chavarría:
   - Alcalá 1
   - Laboratorio 1

   Marvin Somarriba:
   - Hardware

4. ¿Qué problemas se presentan con frecuencia en los laboratorios del Departamento de Computación?
   R:
   - Los bucles en la red
   - Mal funcionamiento de las computadoras en el hardware o software
   - Perdidas de mouse o de otra pieza de la computadora

Anexo 2: Instalación de servidor Pandora FMS

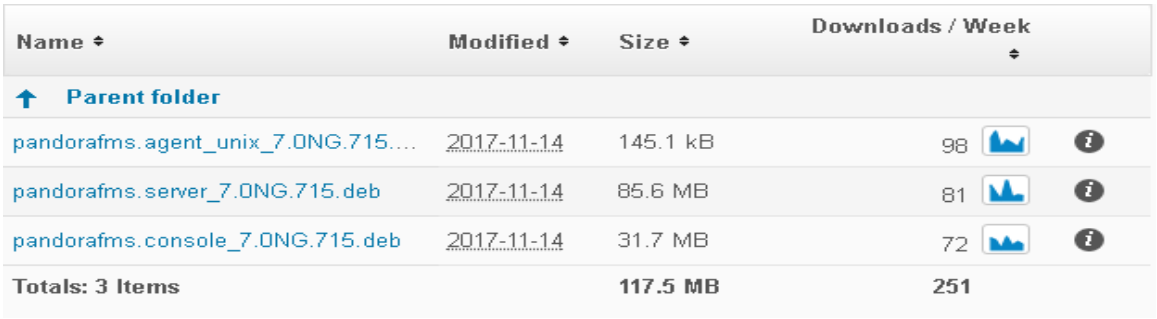
Para instalar el servidor de pandora solo se descarga la ISO basada en CentOS desde la siguiente página web seleccionamos Appliance CD basado en CentOS.

https://pandorafms.org/es/producto/descargar-gratis-software-de-monitorizacion/

Figura 19 Descarga de CD basado en CentOS

Anexo 3: Instalación de agente Pandora FMS Linux

La manera de instalar el agente Pandora es muy sencilla solo se descarga el paquete que dice Debian/Ubuntu es un paquete deb que encontraremos en la siguiente url: https://sourceforge.net/projects/pandora/files/Pandora%20FMS%207.0NG/715/Debian_Ubuntu/



Name	Modified	Size	Downloads / Week
Parent folder			
pandorafms.agent_unix_7.0NG.715....	2017-11-14	145.1 kB	98
pandorafms.server_7.0NG.715.deb	2017-11-14	85.6 MB	81
pandorafms.console_7.0NG.715.deb	2017-11-14	31.7 MB	72
Totals: 3 Items		117.5 MB	251

Figura 20 Descarga de agente Pandora FMS

Para instalar el paquete deb descargado ejecutaremos el comando:

```
dpkg -i nombre_del_agente_pandora.deb
```

Una vez instalado procedemos a configurarlo abriendo la terminal de comandos Linux y editamos el fichero /etc/pandora/pandora_agent_daemon.conf ubicando la siguiente línea “server_ip localhost” borramos “localhost” y asignamos la IP del servidor pandora, procedemos a ubicar la siguiente línea que sería “Remote_config 0” reemplazamos el cero por 1 para habilitar la configuración de monitorización remota y para finalizar iniciamos el servicio de agente pandora ejecutando el comando

```
/etc/init.d/pandora_agent_daemon start.
```

Anexo 4: Instalar agente de software Pandora FMS en Windows

Accederemos a la web oficial de Pandora FMS, en la sección "Descargas", descargaremos el agente para Windows, de 34 ó de 64 bits, Ejecutaremos el fichero descargado "Pandora FMS Windows Agente" si es en sistemas operativos Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 lo ejecutaremos como administrador, pulsando con el botón derecho del ratón sobre el fichero y seleccionando "Ejecutar como administrador":

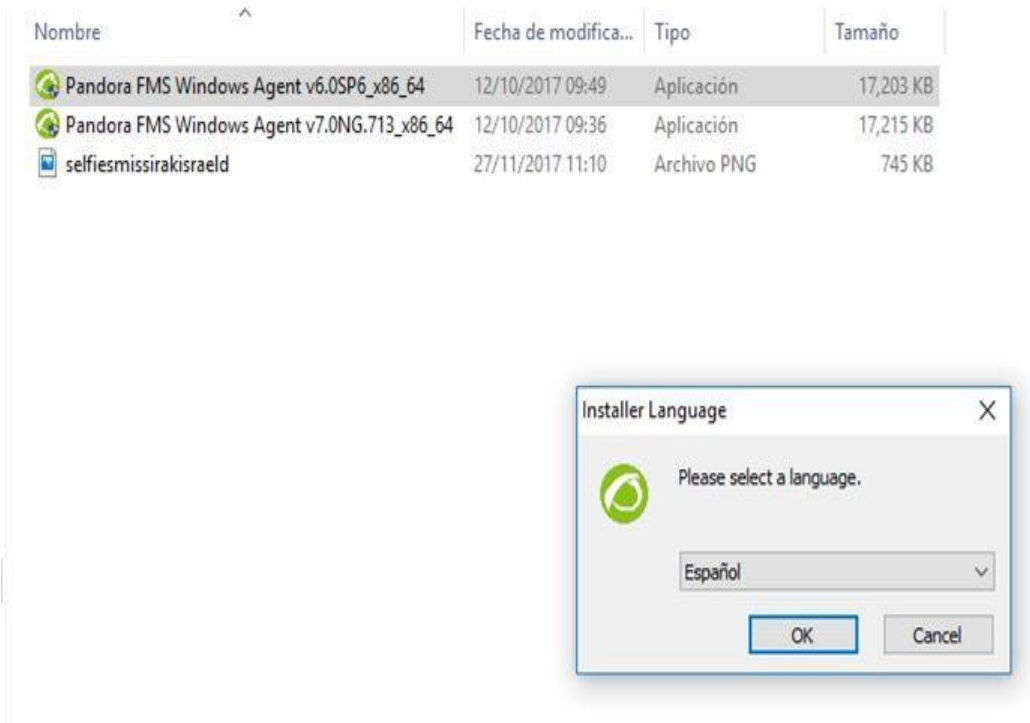


Figura 21 paso 1 instalación de agente Pandora FMS

Pulsaremos "Siguiente" para instalar Pandora FMS Agente 6.0 (la versión del momento de este tutorial):

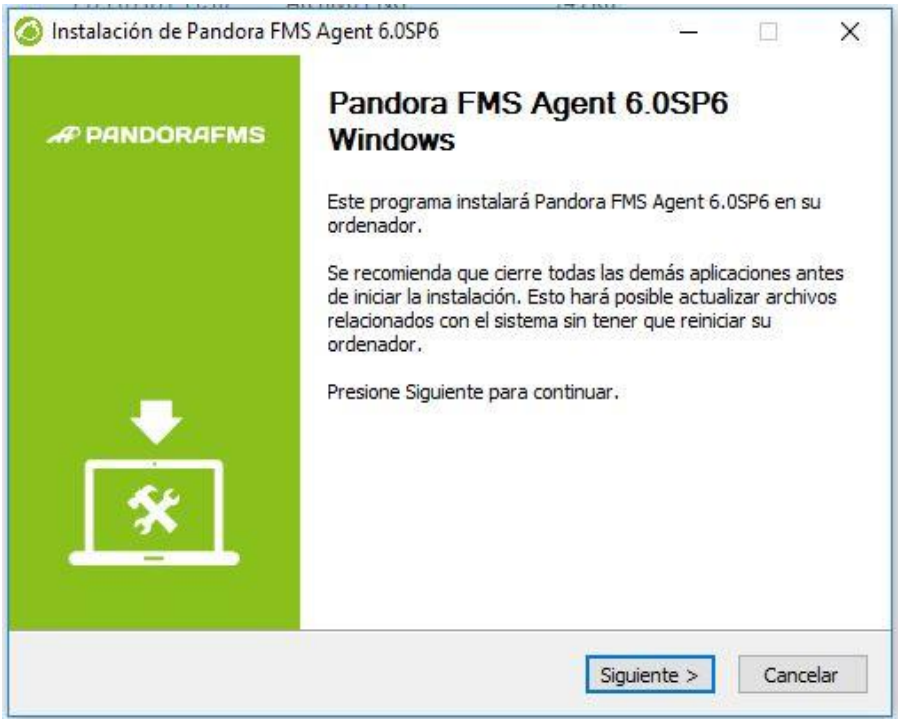


Figura 22 Paso 2 instalación de agente Pandora FMS

Leeremos los términos de licencia de Pandora FMS, si estamos de acuerdo pulsaremos "Siguiente" para continuar:

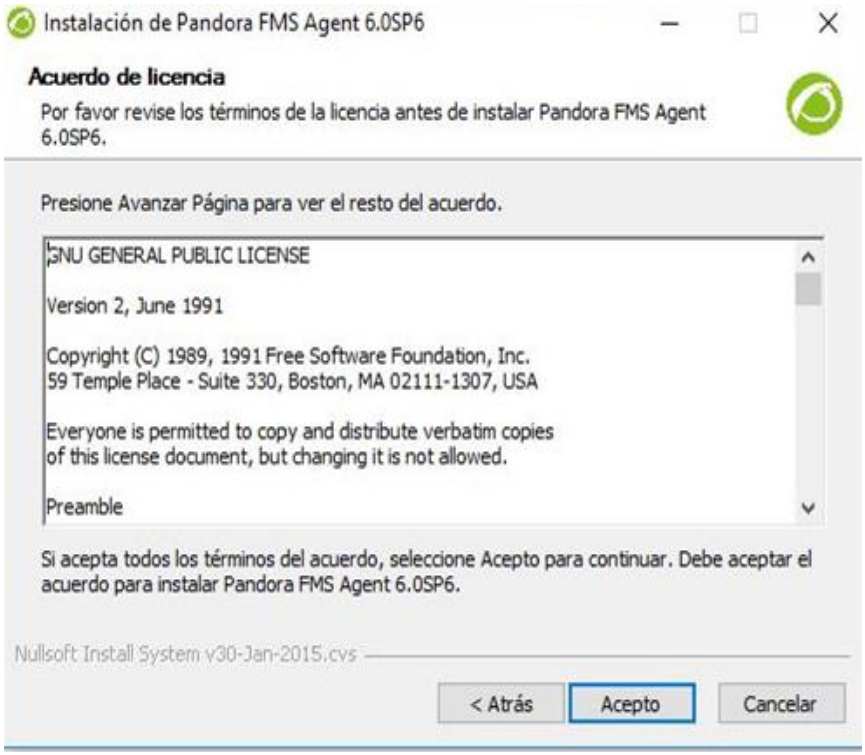


Figura 23 Paso 3 instalación de agente Pandora FMS

Elegiremos la carpeta de instalación de Pandora FMS Agente, por defecto en sistemas Windows: *C:/Program FIles (x86)/pandora_agent*

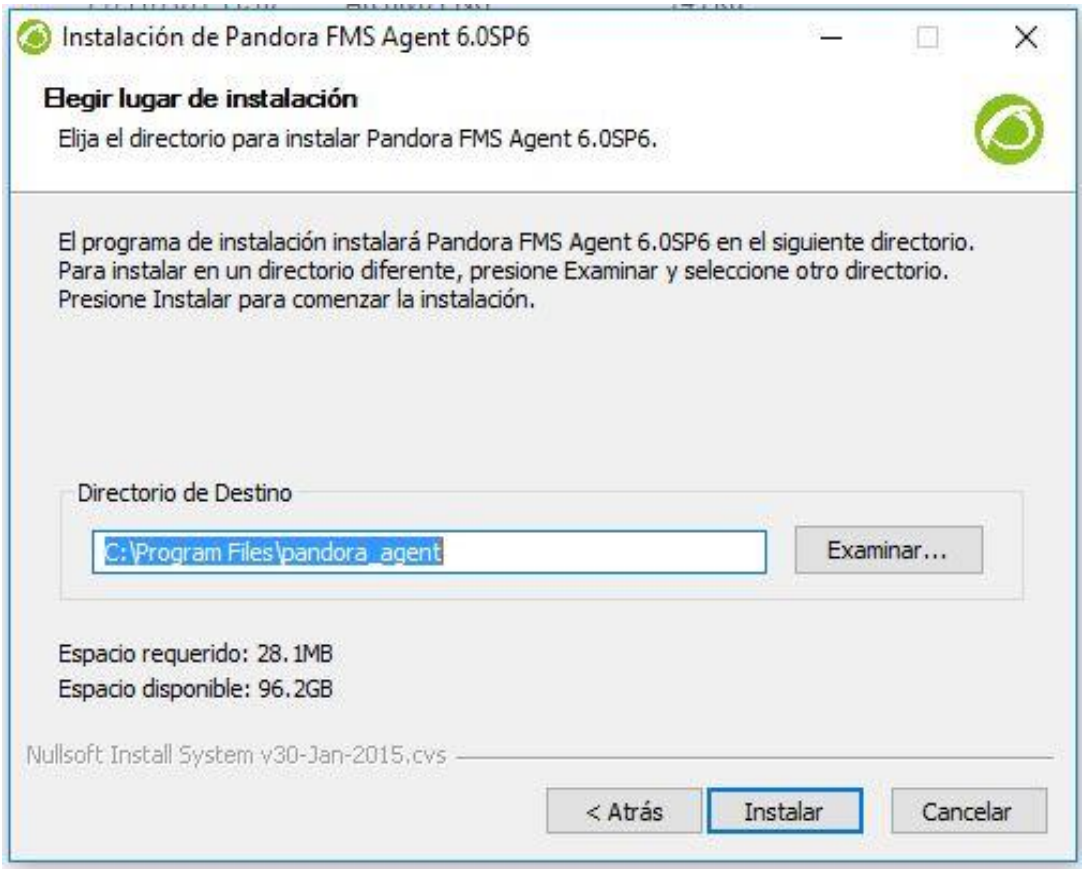


Figura 24 Paso 4 instalación de agente Pandora FMS

Especificaremos la IP o nombre DNS (si está disponible) del servidor de monitorización Pandora FMS en "IP Servidor Pandora FMS" y si queremos agregar este agente a un grupo concreto podremos especificarlo en "Grupo del agente". Estos datos pueden ser configurados posteriormente. Pulsaremos "Siguiente":

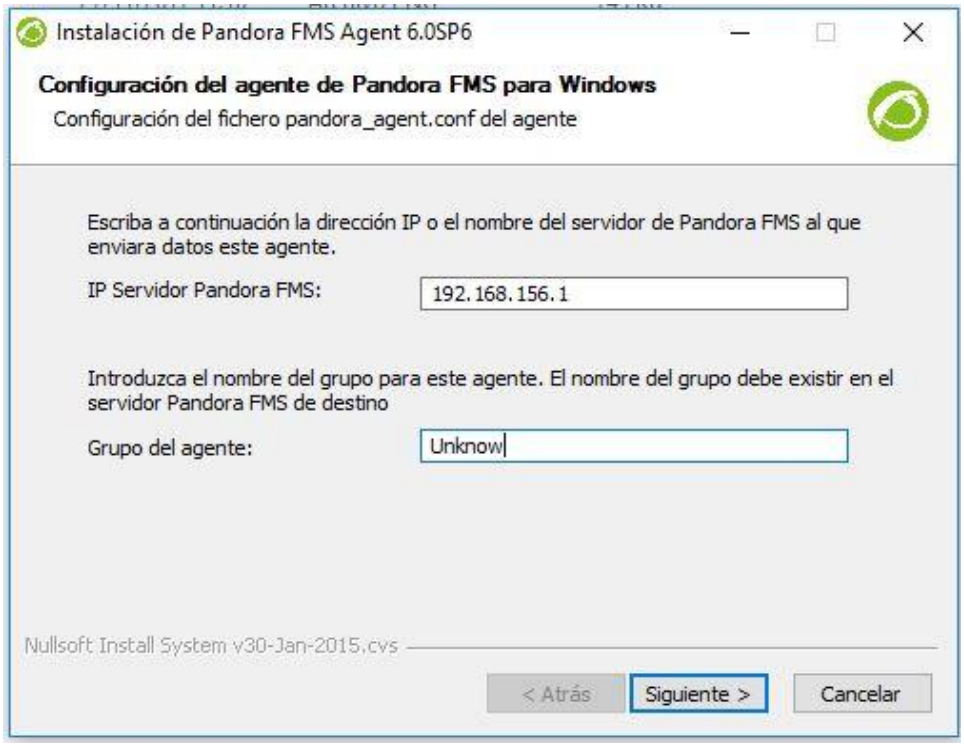


Figura 25 Paso 5 instalación de agente Pandora FMS

Dejaremos habilitada la configuración remota y le damos Siguiente:

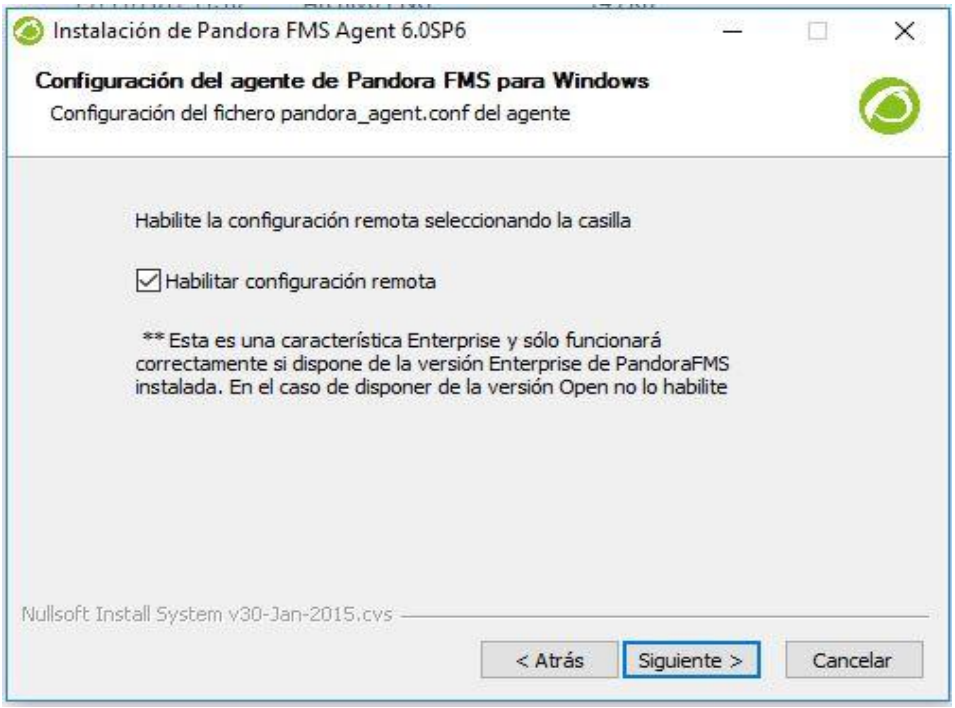


Figura 26 Paso 5 instalación de agente Pandora FMS

El asistente de instalación de Pandora FMS Agent nos iniciará que ha finalizado, pulsaremos "Terminar":

Figura 27 Paso 6 instalación de agente Pandora FMS

Para configurar el agente de pandora accederemos a la carpeta de instalación y editaremos el fichero "pandora_agent.conf":

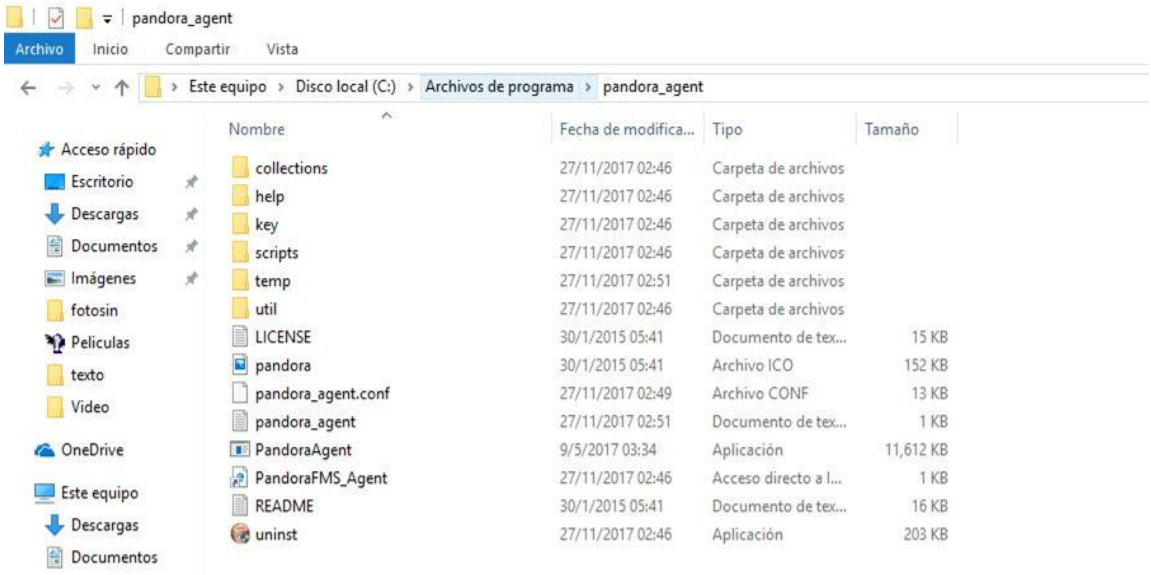


Figura 28 Paso 7 instalación de agente Pandora FMS

Desde este fichero podremos configurar todos los parámetros del agente, desde la IP del servidor de Pandora FMS al que se conectará como los módulos que monitorizará. El parámetro para especificar la IP del servidor de Pandora FMS será "server_ip":

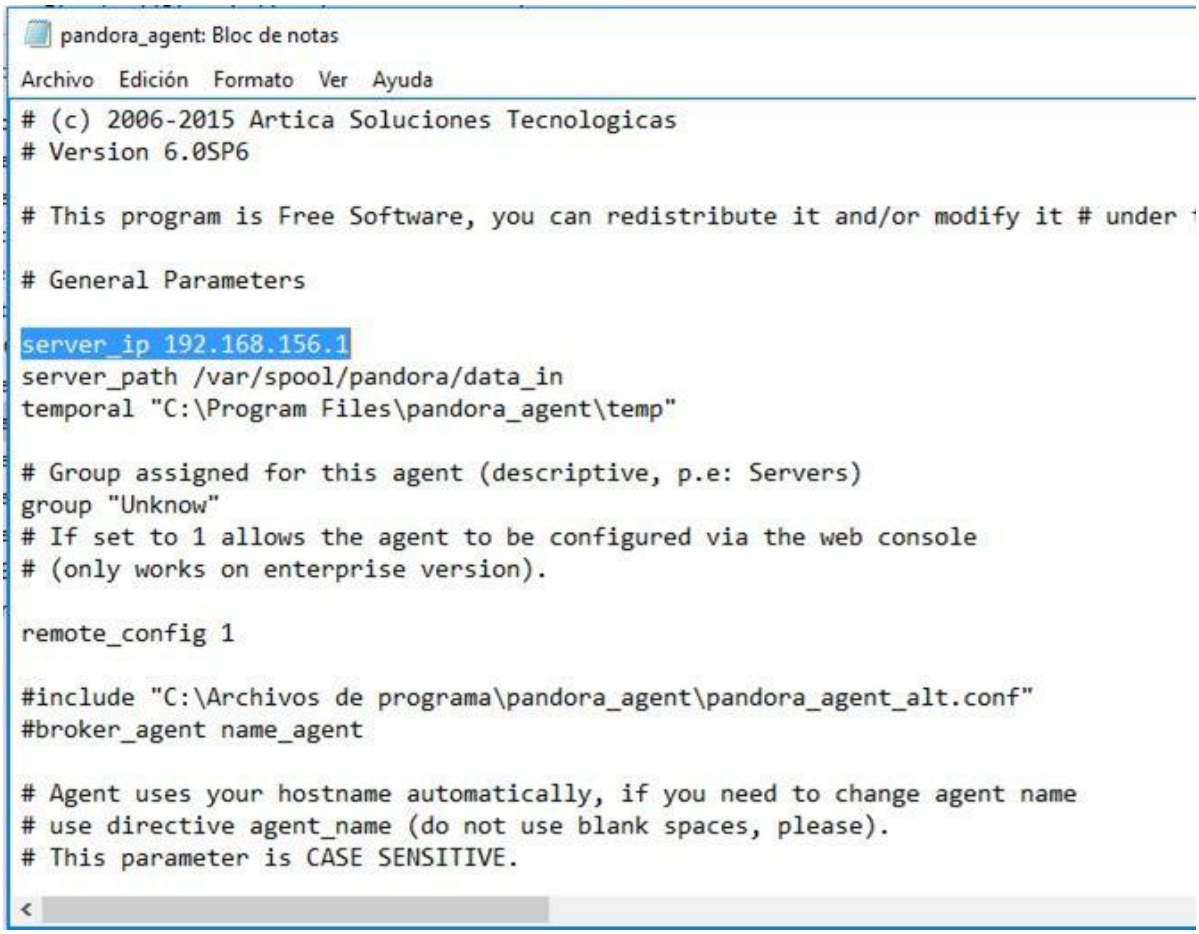


Figura 29 Modificación de IP

Otro parámetro interesante, si disponemos de la versión Enterprise de Pandora FMS, es "remote_config". Con este parámetro podremos indicar a Pandora FMS que administre y configure el agente de forma remota desde el servidor de Pandora FMS, de forma que cualquier configuración que queramos aplicar al agente podremos hacerla de forma centralizada desde la consola web de Pandora FMS. Para activar esta opción añadiremos la línea:

remote_config 1

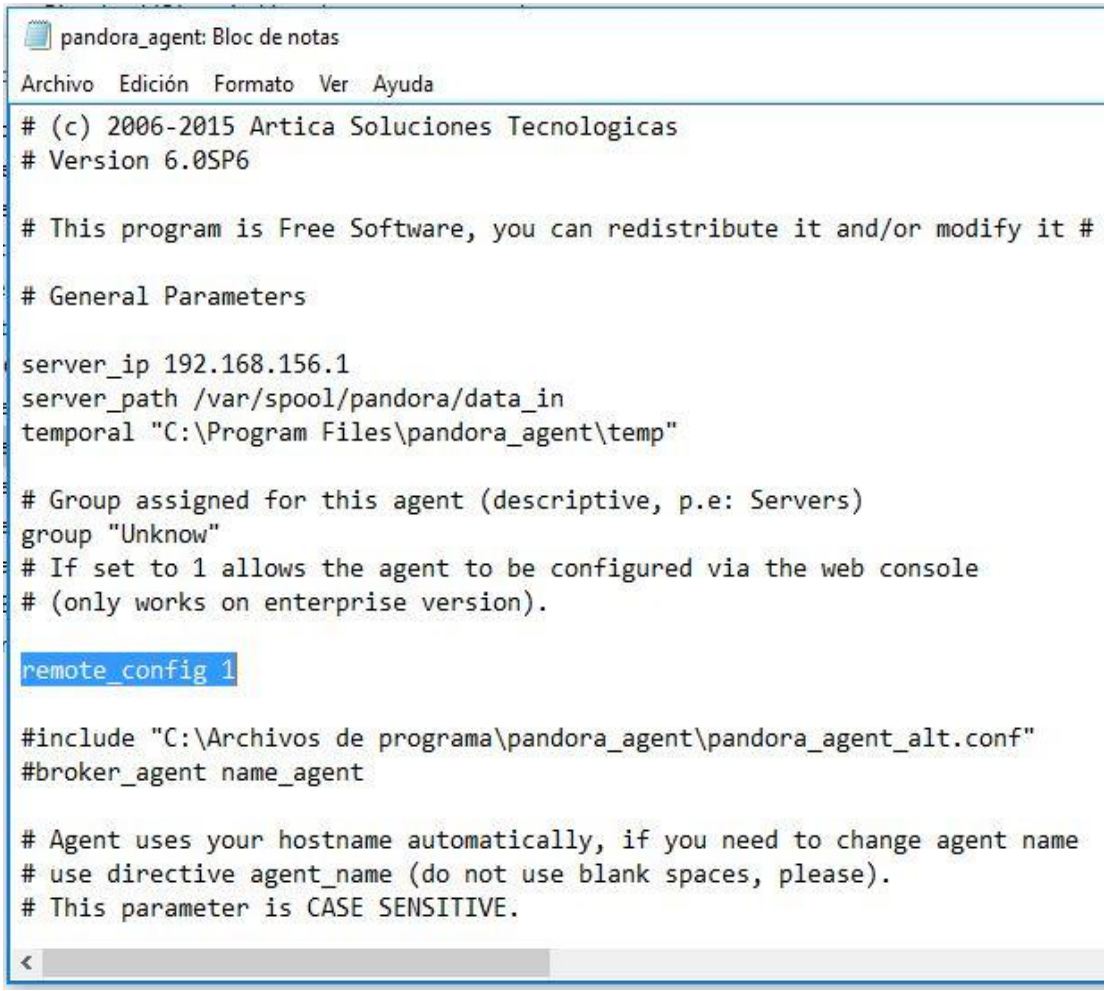


Figura 30 Habilitar configuración Remota

Si queremos aplicar directamente los cambios establecidos en el fichero de configuración de Pandora FMS Agent deberemos reiniciar el servicio, para ello desde "Inicio" - "Ejecutar" escribiremos "services.msc":

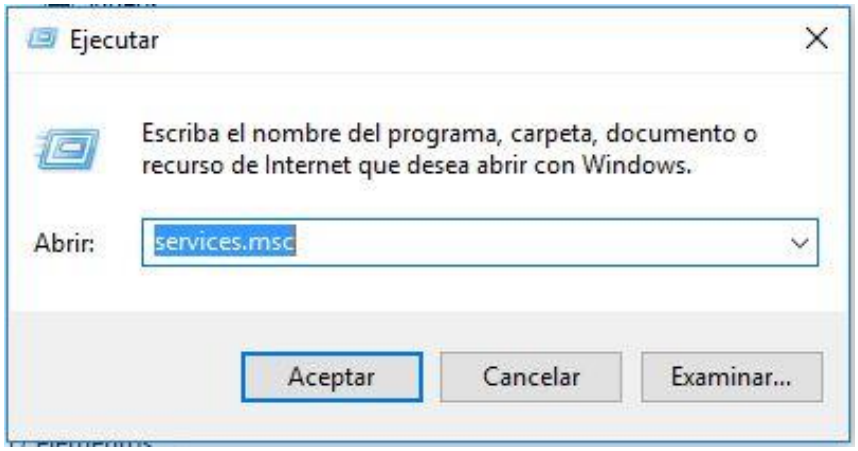


Figura 31 Reinicio del servicio

Buscaremos el servicio de Pandora FMS agent y pulsaremos con el botón derecho del ratón sobre él, seleccionaremos "Reiniciar" en el menú emergente:

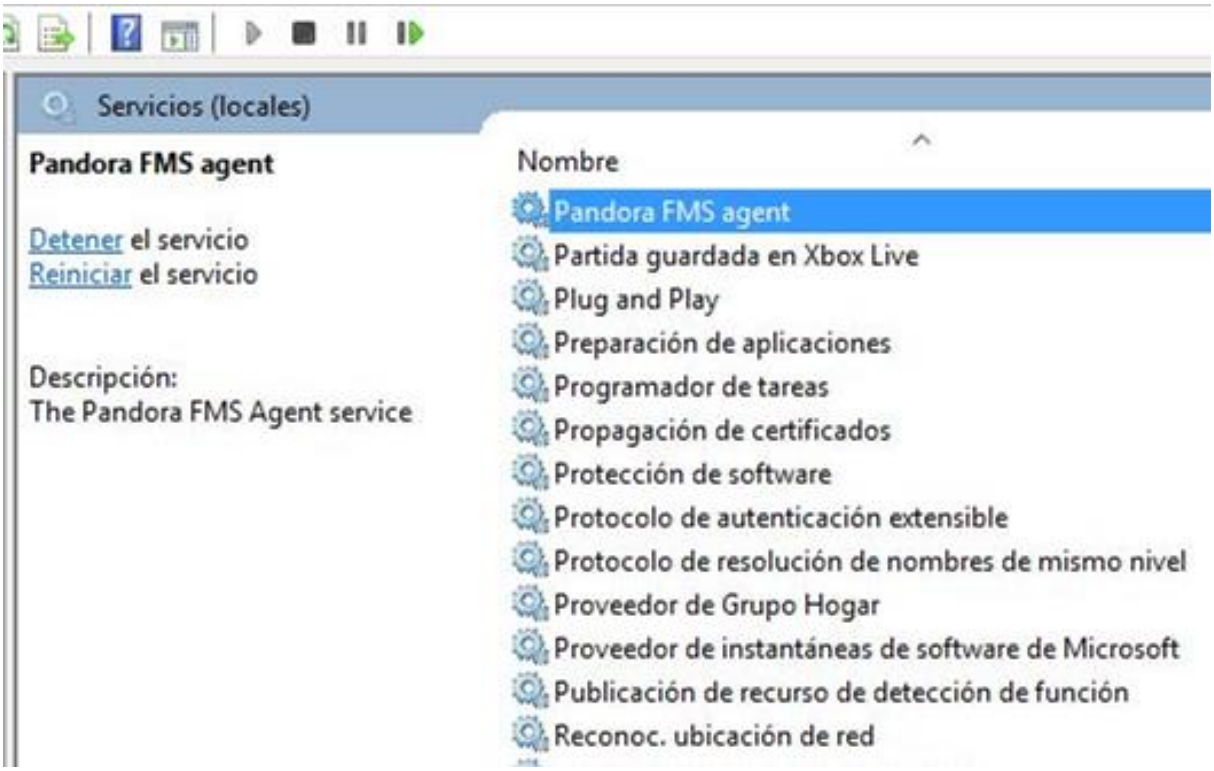


Figura 32 Servicio Pandora FMS

Es importante mencionar que Pandora FMS Agent comunica con el servidor de Pandora FMS mediante el puerto 41121, por lo que este puerto debe estar abierto (al menos de salida) en el cortafuegos de Windows (si lo tenemos activado) o en otro firewall que usemos. Para abrir este puerto en el firewall de Windows Server 2012, accederemos al menú de Inicio buscamos en el Panel de control sistema y seguridad:

Figura 33 Configuración de Firewall

Buscamos firewall de Windows y pulsamos configuración avanzada, con el botón derecho del ratón sobre "Reglas de salida" y elegiremos "Nueva regla":

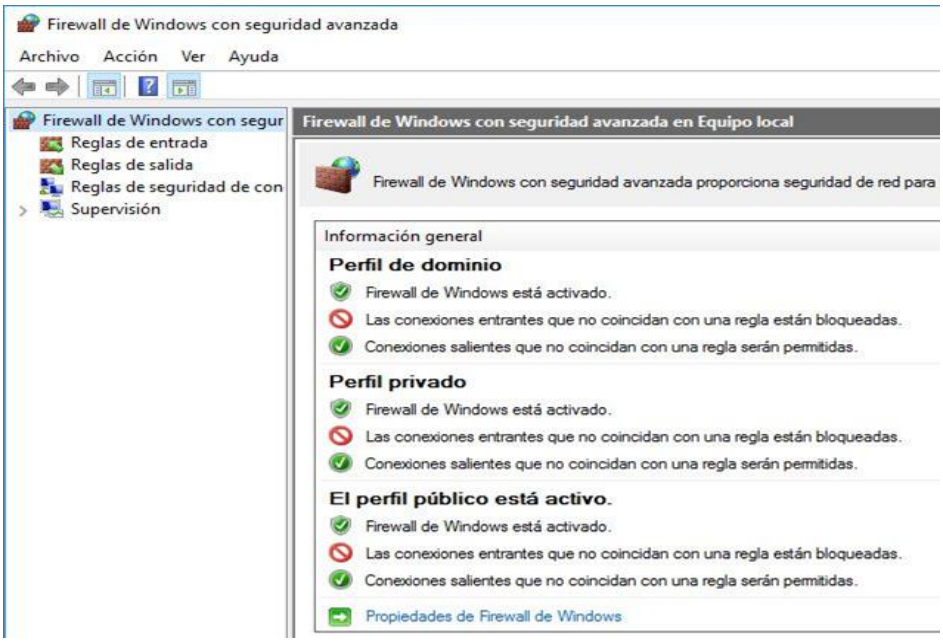


Figura 34 Configuración avanzada de firewall

Marcaremos "Puerto" y pulsaremos "Siguiente":

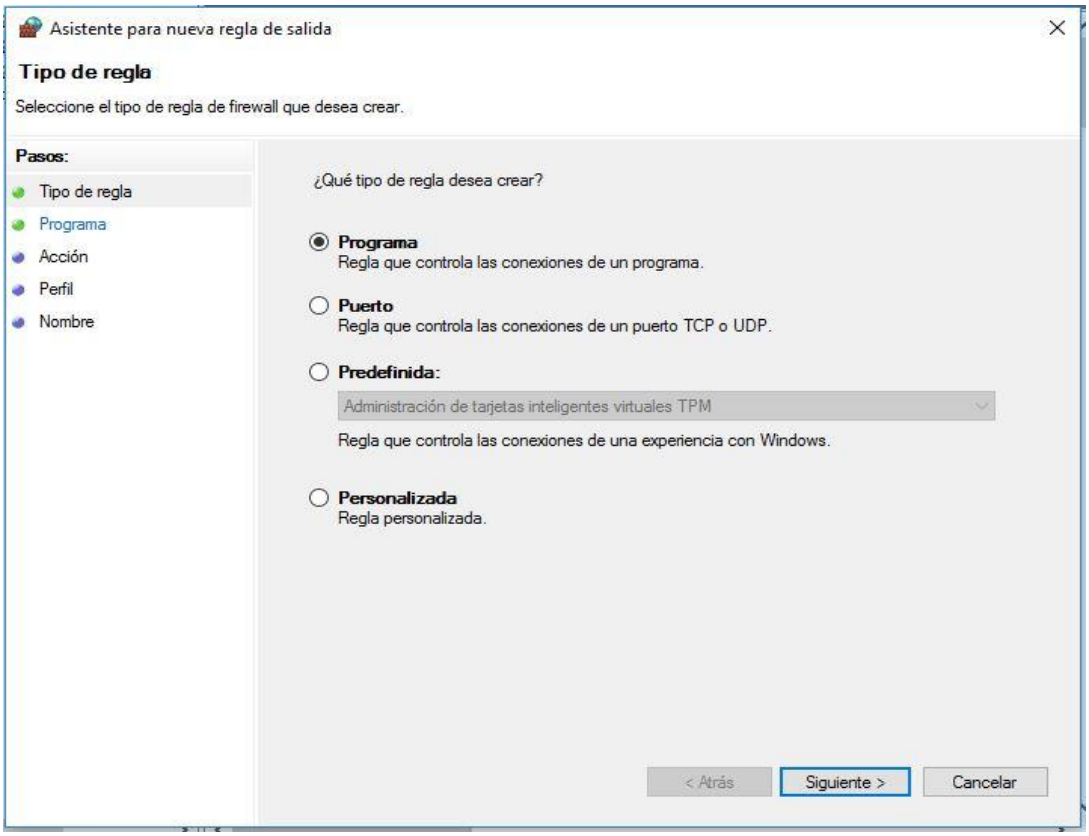


Figura 35 Crear Nueva Regla de Salida

Marcaremos "Puerto" y escribiremos el 41121 y pulsaremos "Siguiente":

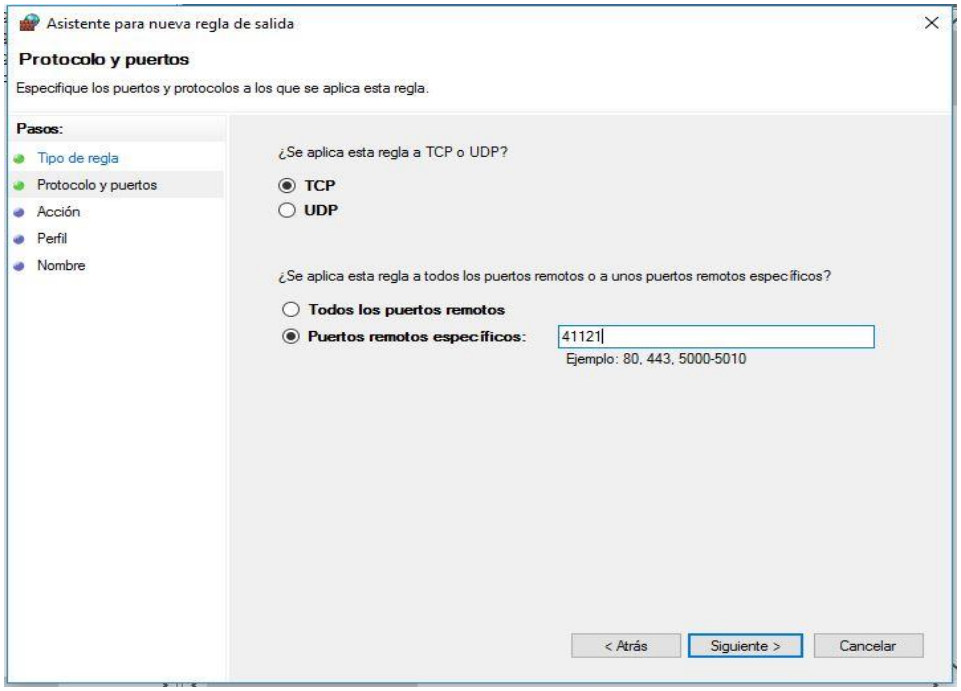


Figura 36 Asignación de Puerto para regla de salida

Marcaremos "Permitir la conexión":

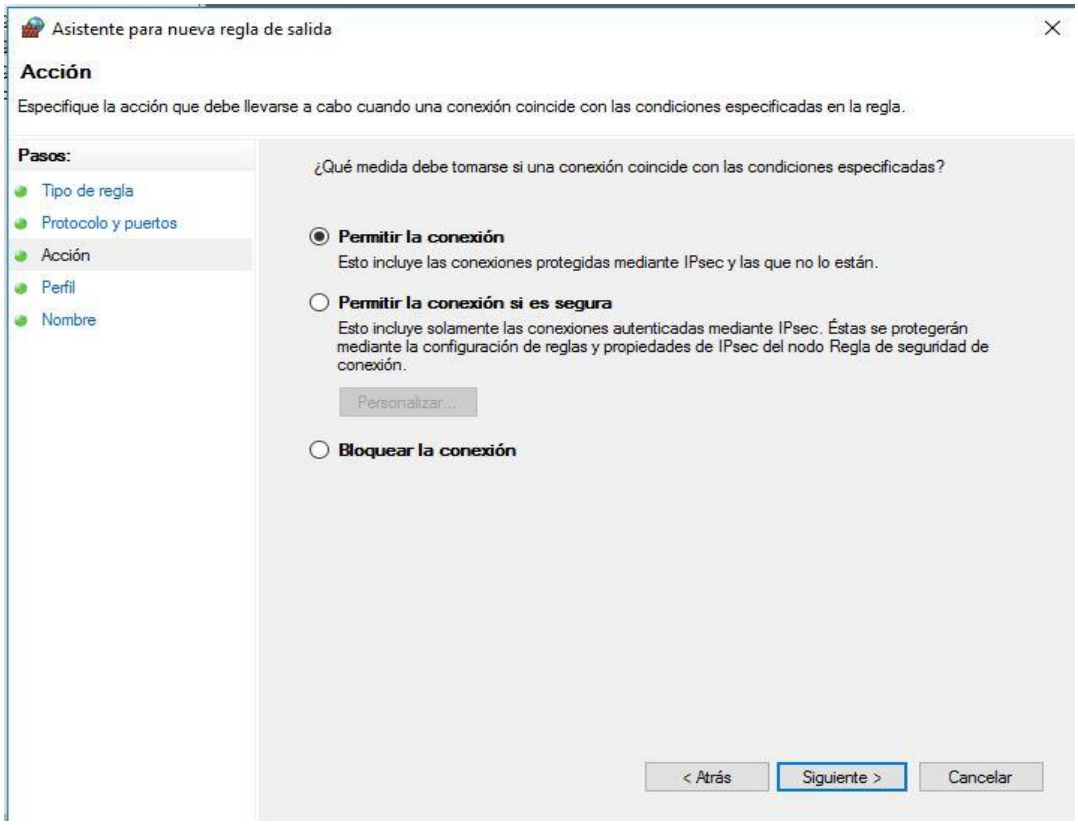


Figura 37 Asignar acción para Regla de salida

Desmarcaremos "Público" y marcaremos "Dominio" y "Privado":

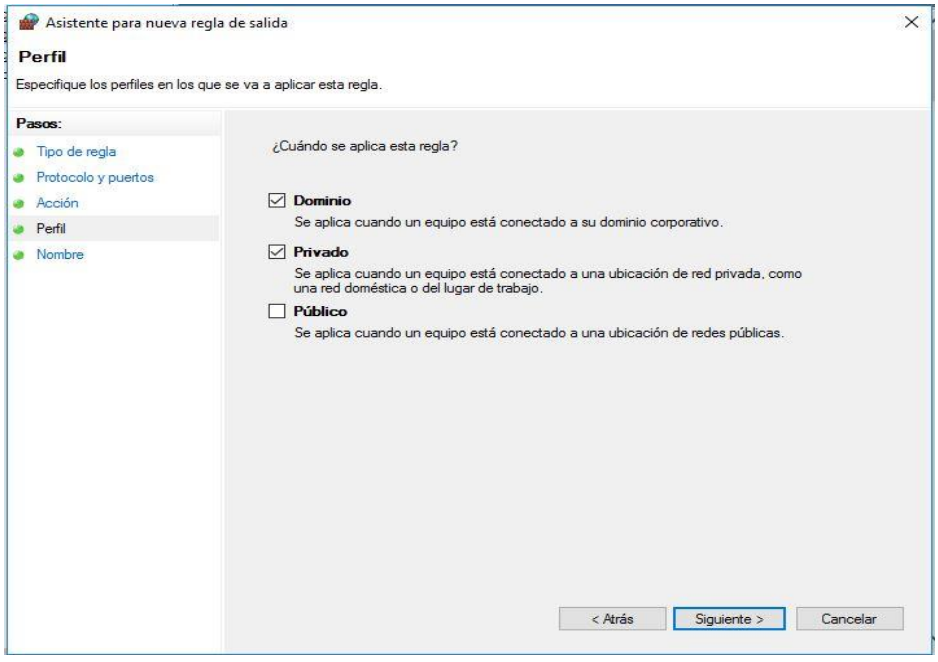


Figura 38 Asignar el perfil para la Regla de Salida

Introduciremos un nombre para la regla del cortafuegos, por ejemplo "Pandora FMS" y pulsaremos "Finalizar":

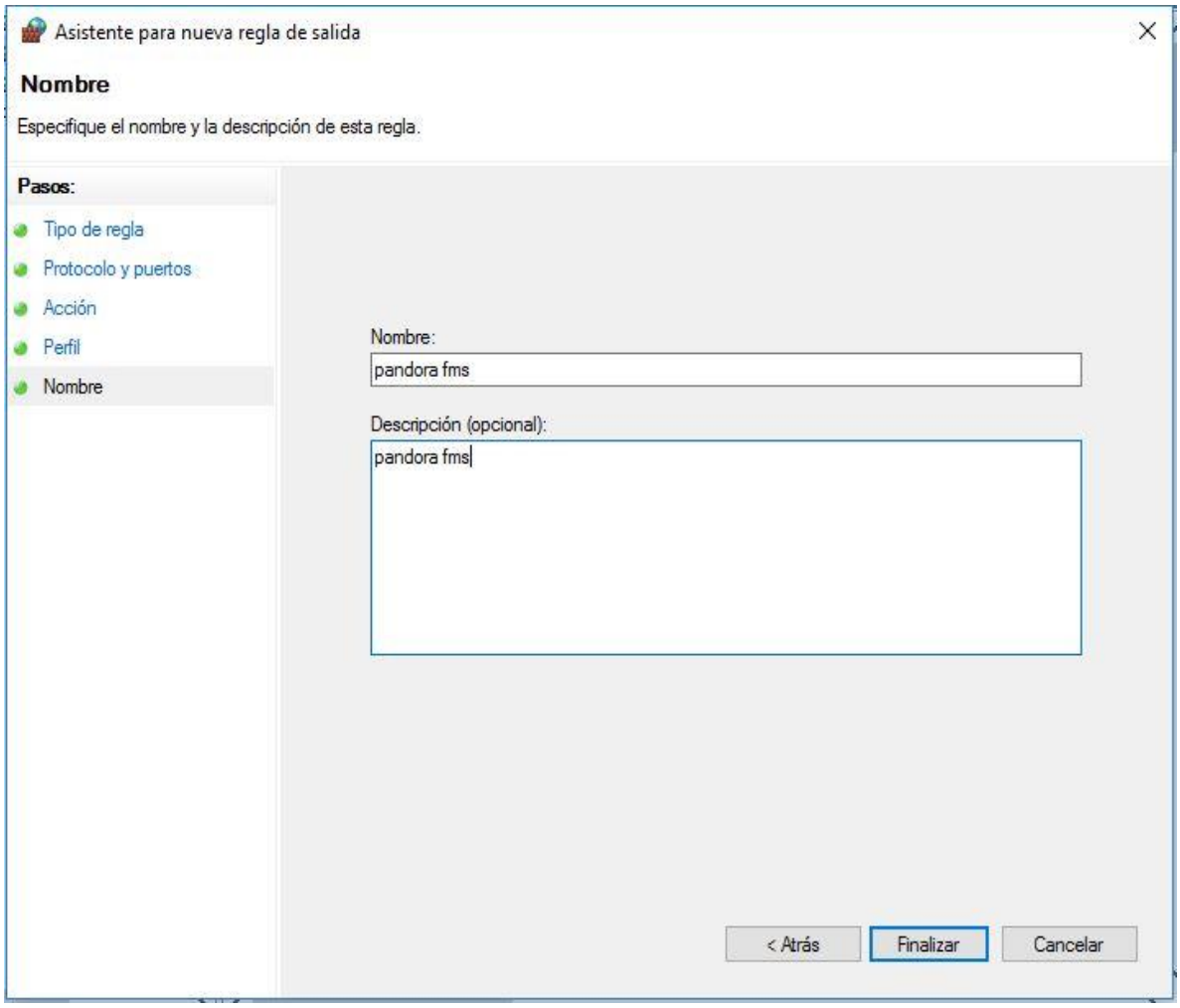


Figura 39 Asignar nombre para la nueva regla

Ahora entramos a panel de control para habilitar el servicio de snmp de Windows y seleccionamos programas.

Figura 40 Panel de control

En programas bajo programas y características de Windows seleccionamos activar o desactivar características de Windows

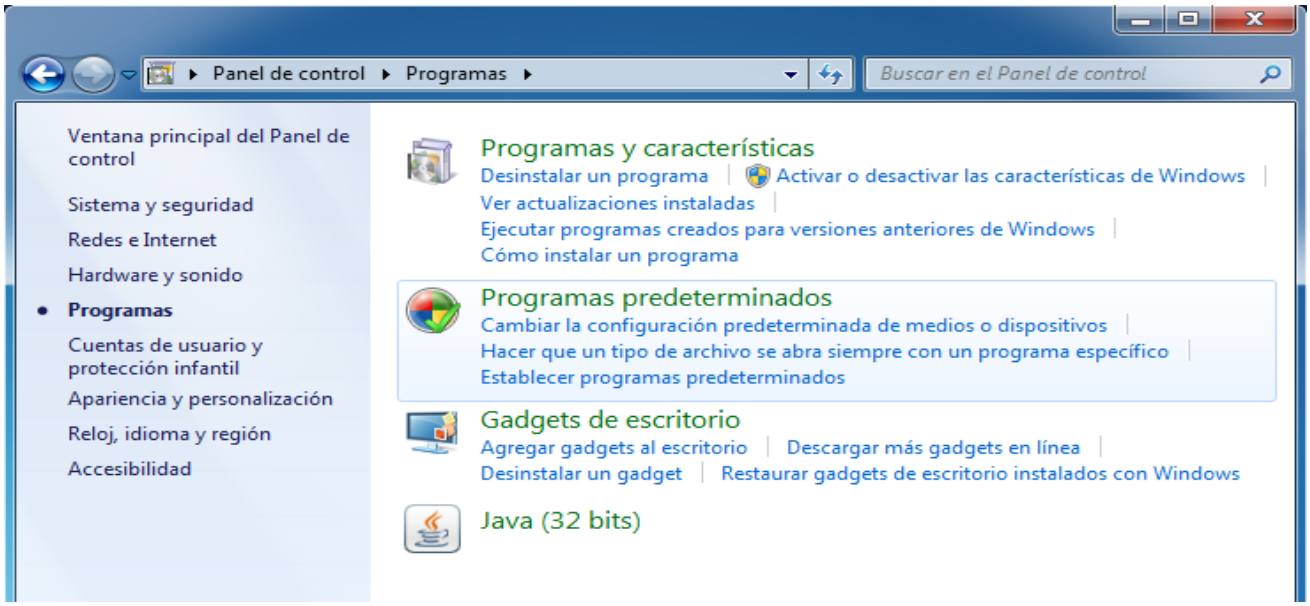


Figura 41 Habilitar SNMP paso 1

Se abrirá una nueva ventana donde habilitaremos el protocolo msnm y le damos aceptar.

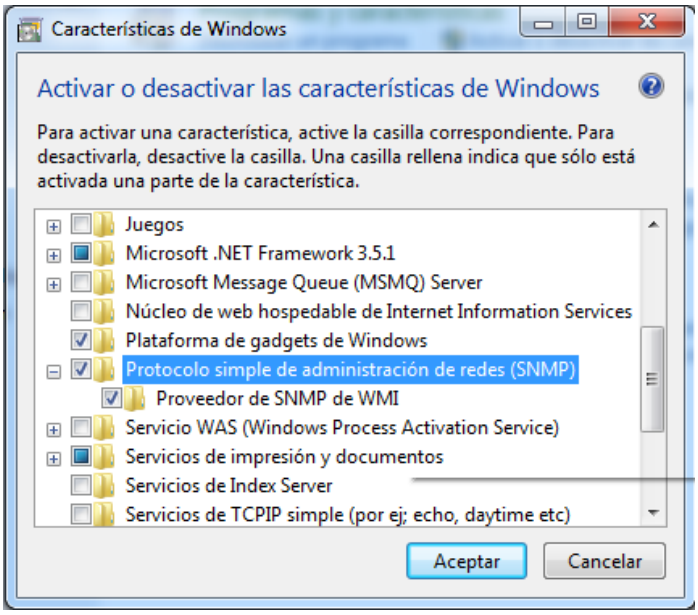


Figura 42 Habilitar SNMP paso 2

Ahora nuevamente nos vamos a servicios y buscaremos el servicio de capturas snmp le damos clic derecho y seleccionamos propiedades nos aparecerá un cuadro de dialogo se debe cambiar el tipo de inicio de snmp de manual a automático para que cada vez que se encienda o reinicie siempre inicie el servicio automáticamente y antes de darle aceptar le damos en el botón iniciar.

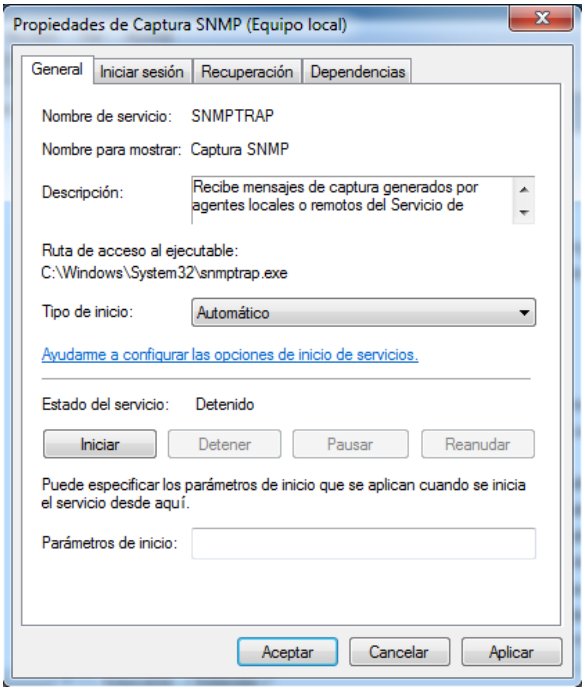


Figura 43 Habilitar SNMP paso 3

En la misma pestaña de servicios buscamos servicio SNMP le damos clic derecho y seleccionamos propiedades y en la pestaña de seguridad agregamos una comunidad public le damos aplicar y aceptar.

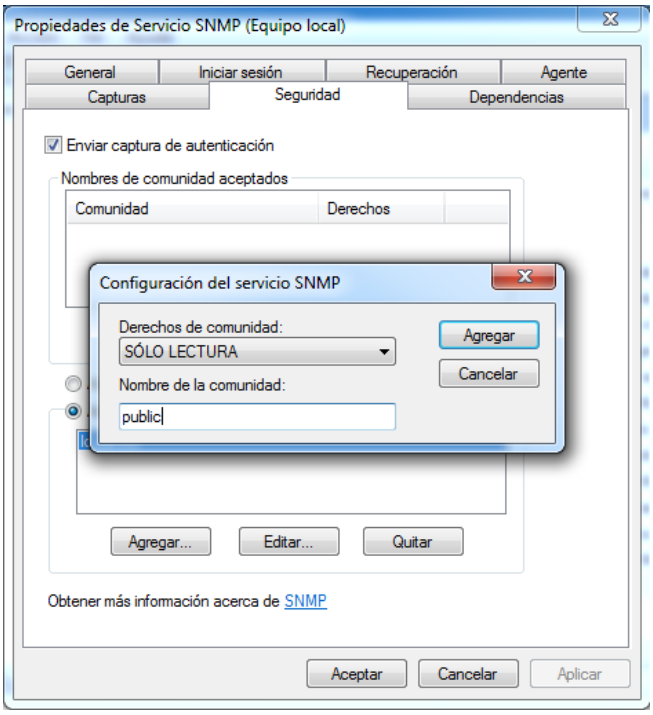


Figura 44 Habilitar SNMP paso 4

Anexo 5: Instalación de Integria IMS

Para comenzar con la instalación de IMS y tener un correcto funcionamiento necesitamos instalar las dependencias las cuales son:

php php-cli php-gd php-intl curl php-ldap php-imap php-mysql php-mbstring php

Una vez hechos los cambios es necesario reiniciar el servidor de apache

```
service httpd restart
```

Descargamos desde la fuente para ello necesitaremos tener instalado el paquete de subversión mediante el comando “yum install subversión” desde la terminal de comandos y a continuación nos ubicamos en la dirección /var/www/html y ejecutamos el siguiente comando para descargar Integria ya que se descargará la versión descomprimida en dicha carpeta.

```
svn co https://integria.svn.sourceforge.net/svnroot/integria/trunk integria
```

Ahora procederemos a cambiar permisos para qué el directorio sea propiedad del usuario del servidor web en este caso sería:

```
chown -R apache:apache  /var/www/html/Integria
```

Ahora debemos acceder vía web a la dirección ip del servidor para proseguir con la instalación de Integria IMS. Esta parte de la instalación sirve para crear la base de datos de Integria y configurar las credenciales de acceso como usuario, password y nombre de la base de datos.

http://ip_servidor/integria/trunk/install.php

Anexo 6: Configuración para envió de correo

Edite el archivo de configuración /etc/postfix/main.cf y agregue las siguientes líneas al final del archivo:

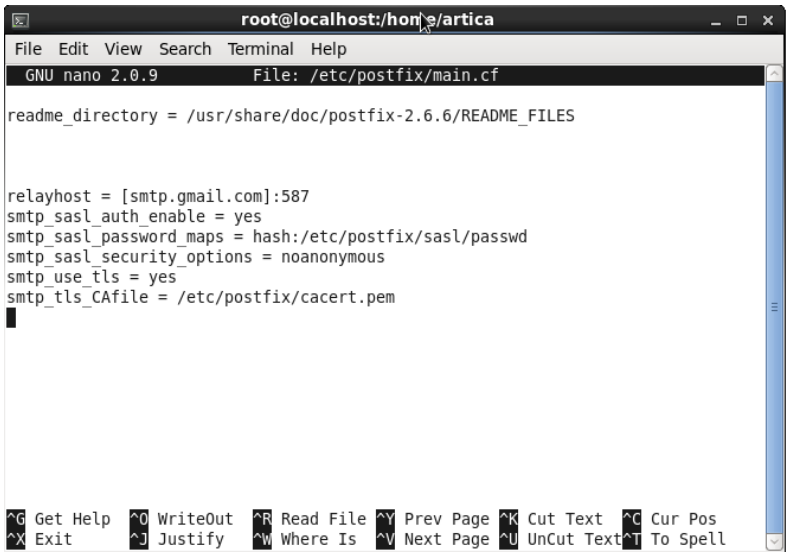


Figura 45 Configuración de postfix paso 1

Cree el archivo / etc / postfix / sasl / passwd con su dirección y contraseña de gmail (debe crear el directorio "sasl" y luego crear el archivo passwd allí).

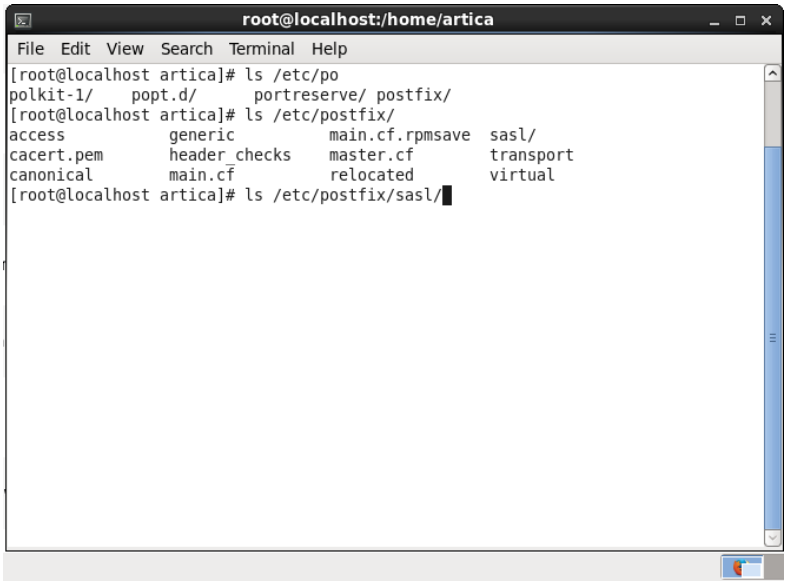


Figura 46 Configuración de postfix paso 2

Entramos al directorio nano /etc/postfix/sasl/passwd y copiamos la siguiente línea con la cuenta de correo que se va a utilizar:

[smtp.gmail.com]:587 ACCOUNT@gmail.com:PASSWORD

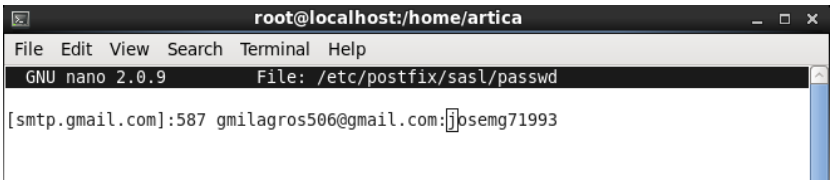


Figura 47 Configuración de postfix paso 3

Proteja el archivo de contraseña en consecuencia:

```
chmod 600 /etc/postfix/sasl/passwd
```

Transforme /etc/postfix/sasl/passwd en un archivo indexado tipo hash. Esto creará una tabla de búsqueda a través de postmap:

```
postmap /etc/postfix/sasl/passwd
```

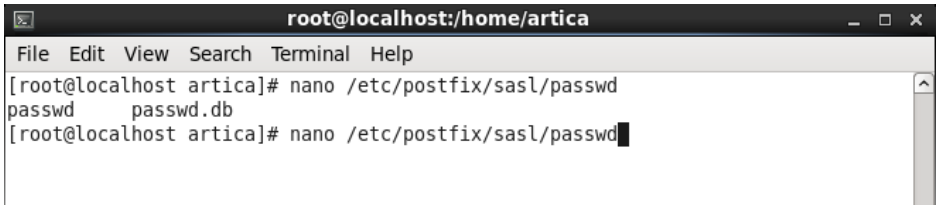


Figura 48 Configuración de postfix paso 4

Ahora para instalar los certificados de Gmail y Equifax. La imagen preconstruida de Pandora FMS ISO y VMware virtual no tiene estos certificados por defecto. Si tiene los certificados instalados, puede omitir esta parte nos movemos a la carpeta /etc/pki/tls/ y ejecutamos el siguiente comando:

```
sudo wget -O Equifax_Secure_Certificate_Authority.pem
https://www.geotrust.com/resources/root_certificates/certificates/Equifax_Secure_Certificate_Authority.cer
```

Luego necesitamos adquirir el certificado para GMail. Entonces usa openssl para hacer esto:

```
openssl s_client -connect pop.gmail.com:995 -showcerts
```

La salida debe contener las líneas requeridas para el certificado y debemos copiarlas al archivo /etc/pki/tls/gmail.pem. Para esto, crea el archivo:

```
nano /etc/pki/tls/gmail.pem
```

Pegue estas líneas en el archivo gmail.pem:

Figura 49 Configuración de postfix paso 5

Finalmente, podemos probarlo con:

```
openssl s_client -connect pop.gmail.com:995 -CApath /etc/pki/tls
```

El punto importante es Verificar el código de retorno: 0 (ok), y el OK Gpop final listo. Si los obtiene, puede conectarse a Gmail. Guardar y Salir. Para agregar la autoridad de certificación de Equifax (que certifica los correos electrónicos de Gmail) en el archivo de certificado que usa postfix, ejecute el siguiente comando en una consola raíz:

```
cat /etc/ssl/certs/Equifax_Secure_CA.pem > /etc/postfix/cacert.pem
```

Finalmente, reinicie postfix para aplicar los cambios:

```
/etc/init.d/postfix restart
```