



**UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL**

CARRERA: INGENIERÍA DE SISTEMAS

**Proyecto Técnico previo a la obtención del título de: INGENIERO DE
SISTEMAS**

TEMA:

**IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE REDES
UTILIZANDO HERRAMIENTAS OPEN SOURCE Y PROVEER SERVICIOS DE
DIRECTORIO A TRAVÉS DE ACTIVE DIRECTORY EN LA FACULTAD DE
FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN DE LA UNIVERSIDAD
DE GUAYAQUIL**

AUTORES:

**CARLOS ANGEL VELASCO BRIONES
GIANELLA STEPHANIA CAGUA ORDOÑEZ**

DIRECTOR:

ING. DANNY BARONA VALENCIA MBA.

Guayaquil, enero de 2017

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Nosotros Carlos Angel Velasco Briones y Gianella Stephania Cagua Ordoñez autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además, declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Carlos Angel Velasco Briones
C.C: 092828777-0

Gianella Stephania Cagua Ordoñez
C.C: 093076093-9

CESIÓN DE DERECHOS DE AUTOR

Nosotros Carlos Angel Velasco Briones, con documento de identificación N° 092828777-0 y Gianella Stephania Cagua Ordoñez con documento de identificación N° 093076093-9, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de grado intitulado: “IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO DE REDES UTILIZANDO HERRAMIENTAS OPEN SOURCE Y PROVEER SERVICIOS DE DIRECTORIO A TRAVÉS DE ACTIVE DIRECTORY EN LA FACULTAD DE FILOSOFÍA, LETRAS Y CIENCIAS DE LA EDUCACIÓN DE LA UNIVERSIDAD DE GUAYAQUIL”, mismo que ha sido desarrollado para optar por el título de: Ingeniero en Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....
Carlos Angel Velasco Briones
C.C: 092828777-0

.....
Gianella Stephania Cagua Ordoñez
C.C: 093076093-9

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Ingeniero Danny Barona, tengo a bien certificar que los estudiantes Carlos Angel Velasco Briones y Gianella Stephania Cagua Ordoñez, han realizado el presente Proyecto de Titulación bajo mi supervisión; y, por lo tanto, se encuentran aptos para su correspondiente presentación.

Guayaquil, diciembre del 2016

Ing. Danny Barona Valencia. MBA

DEDICATORIA

Dedico este proyecto principalmente a Dios por darme las fuerzas para alcanzar esta meta.

Una dedicatoria especial a mi madre por su amor, entrega y que por sobre todas las cosas me enseñó a ser la persona que soy en estos tiempos.

A mi padre por su enseñanza por sus consejos, su apoyo y por brindarme los recursos necesarios.

A mi abuela por su constante apoyo, enseñanzas, dedicación y empuje para cumplir mis objetivos.

A Gianella Cagua por su amor, apoyo y ayuda para culminar esta meta.

Carlos Velasco Briones

DEDICATORIA

Una dedicación muy especial a Dios, que por las fuerzas que él me brinda día a día es que logre terminar una de mis tantas metas. Dedico a mis padres por ser los guías de mi vida y los instrumentos que Dios usa constantemente.

A mis hermanos, cuñadas y especialmente a mi sobrina, este trabajo también va para ustedes.

A Carlos Velasco por ser mi amigo incondicional, mi profesor en algunas materias y su paciencia y amor constante. Te dije que lo lograríamos.

Gianella Cagua Ordoñez

AGRADECIMIENTO

Agradecemos a Dios y a nuestros padres por su amor, enseñanza y disciplina; valores que nos ayudaron a cumplir cada una de las metas trazadas, y forjarnos como personas de bien, a ellos sea la honra, consideración y estima.

Agradecemos a nuestras familias por sus palabras de aliento.

Agradecemos a nuestro tutor por su constante apoyo e interés en nuestro proyecto.

Carlos Angel Velasco Briones

Gianella Stephania Cagua Ordoñez

RESUMEN

En la actualidad las empresas cuentan con servidores para base de datos, aplicaciones web, aplicaciones internas, servicios de correo, entre otros; que son indispensables para proveer servicios a los usuarios internos y externos. Por ello la relevancia del uso de una herramienta para el monitoreo, la prevención temprana de problemas y el conocimiento del estado de todos aquellos servidores desde cualquier lugar o dispositivo. Toda empresa provee de PC o laptops para que los empleados accedan a la información y a los recursos compartidos, pero es necesario que se autentifiquen en estos dispositivos para mantener la confidencialidad y la integridad de dicha información.

En la Facultad de Filosofía, Letras y Ciencias de la Educación de la Universidad de Guayaquil, se desconoce el estado de los servidores, el estado de los servicios que se provee, el consumo del ancho de banda, el estado del enlace de comunicaciones entre las ciudades del norte - centro que pertenecen a la Facultad, virus por el uso de USB personales por parte del personal administrativo y alteraciones en las configuraciones de las máquinas provistas a los usuarios.

Por ello la Facultad necesita una herramienta para el monitoreo constante de los servidores, los enlaces de comunicaciones, información del estado del ancho de banda que provee la Unidad de Computo de la Universidad de Guayaquil; también se requiere una herramienta para la administración de todas las computadoras y que aporte seguridad a los recursos compartidos en la red.

Después de las reuniones establecidas con el Director del Departamento de Sistemas, se planteó la utilización de Nagios como herramienta de monitoreo de redes y para la administración de los diferentes equipos, considerando que el departamento ya contaba con un servidor con sistema operativo Windows Server 2012 R2, se optó por la herramienta Active Directory.

Después de la implementación de cada software se mostraron cambios positivos en la administración y tiempo de respuesta a problemas por parte del personal de Sistemas. Como resultado del uso de la herramienta de monitoreo se obtiene información por medio de datos estadísticos del estado de los servidores, alertas vía correo, identificar problemas

en los servidores y el consumo del ancho de banda. Usando directorio activo para la administración de los equipos se reducen los incidentes o percances ocasionado por los usuarios, permite establecer políticas internas en los dispositivos conectados y almacena información en una base de datos central de todo objeto y usuario que pertenezca al dominio.

SUMMARY

Currently, companies have database servers, web applications, internal applications, mail services, among others; which are indispensable to provide services to internal and external users. Therefore, the relevance of the use of a tool for monitoring, early prevention of problems and knowledge of the status of all those servers from any place or device. Every company provides PCs or laptops for users to access information and shared resources, but they need to be authenticated on these devices to maintain the confidentiality and integrity of such information.

In the Faculty of Philosophy, Literature and Education Sciences of the University of Guayaquil, the status of the servers, the state of the services provided, the consumption of the bandwidth, the state of the communications link between the North - center citadels that belong to the Faculty, virus by the use of personal USB by the administrative staff and alterations in the configurations of the machines provided to the users.

Therefore, the Faculty needs a tool for the constant monitoring of the servers, the communications links, information of the state of the bandwidth provided by the Computation Unit of the University of Guayaquil; It also requires a tool for the administration of all the computers and that provides security to the shared resources in the network.

After the meetings established with the Director of the Systems Department, the use of Nagios was considered as a network monitoring tool and for the administration of the different computers, considering that the department already had a server with Windows Server 2012 R2 operating system, we opted for the Active Directory tool.

After the implementation of each software, there were positive changes in the administration and response time to problems by the System personnel. As a result of the use of the monitoring tool, information is obtained by statistical data of the state of the

servers, alerts by mail, identify problems in the servers, consumption of the bandwidth. Using Active Directory for the administration of the equipment reduces the incidents or mishaps caused by the users, allow establishing internal policies in the connected devices and stores information in a central database of every object and user that belongs to the domain.

Índice

| | |
|----------------------------------------------------------------------------------|------|
| DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO | II |
| CESIÓN DE DERECHOS DE AUTOR | III |
| CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN..... | IV |
| DEDICATORIA | V |
| DEDICATORIA | VI |
| AGRADECIMIENTO | VII |
| RESUMEN | VIII |
| SUMMARY | X |
| 1. Introducción..... | 1 |
| 2. Problema..... | 2 |
| 2.1. Antecedentes | 2 |
| 2.2. Importancia y alcances | 3 |
| 2.3. Delimitación | 6 |
| 2.4. Presupuesto..... | 7 |
| 3. Objetivo General y Específicos | 8 |
| 4. Fundamentos Teóricos..... | 8 |
| 4.1. Open Source | 8 |
| 4.2. Redes de comunicaciones..... | 9 |
| 4.3. Infraestructura de red | 12 |
| 4.4. Monitoreo de redes..... | 19 |
| 4.5. Directorio Activo..... | 26 |
| 4.6. Metodología PPDIIO | 29 |
| 5. Marco Metodológico | 30 |
| 5.1. FASE I: Preparar | 31 |
| 5.2. FASE II: Planificar..... | 32 |
| 5.3. FASE III: Diseñar..... | 44 |
| 5.4. FASE IV: Implementar | 49 |
| 5.5. FASE V: Operar | 56 |
| 6. Resultados..... | 57 |
| 6.1. Pruebas y Métricas | 57 |
| 7. Conclusiones..... | 80 |
| 8. Recomendaciones | 81 |

| | |
|--------------------------------------------------------------|-----|
| 9. Referencias Bibliográficas..... | 82 |
| 10.1. Anexo A | 84 |
| 10.1.1. Manual de instalación de Nagios..... | 84 |
| 10.2. Anexo B..... | 87 |
| 10.2.1. Manual de configuración de Nagios | 87 |
| 10.3. Anexo C..... | 89 |
| 10.3.1. Instalación de clientes para monitoreo | 89 |
| 10.4. Anexo D | 96 |
| 10.4.1. Instalación de PNP4 Nagios | 96 |
| 10.5. Anexo E..... | 103 |
| 10.5.1. Instalación y configuración de Active Directory..... | 103 |
| 10.6. Anexo F..... | 112 |
| 10.6.1. Creación de unidades organizativas | 112 |
| 10.6.2. Creación de usuarios..... | 115 |
| 10.6.3. Creación de Grupo..... | 118 |
| 10.7. Anexo G | 122 |
| 10.7.1. Capacitación de Nagios y Directorio Activo..... | 122 |
| 10.8. Anexo H..... | 126 |
| 10.8.1. Oficio No. 113-UGFF-DSIST-JR-16 | 126 |
| 10.9. Anexo I..... | 128 |
| Comunicado al Ingeniero Carlos Ruiz. | 128 |
| 10.10. Anexo J..... | 129 |
| 10.10.1. Creación de políticas de red..... | 129 |
| 10.11. Anexo K | 144 |
| 10.11.1. Asignación de usuarios a las computadoras | 144 |
| 10.12. Anexo L..... | 148 |

Índice de Ilustraciones

| | |
|------------------------------------------------------------------------------------|----|
| Figura 1: Red de la Facultad de Filosofía, Letras y Ciencias de la Educación. | 4 |
| Figura 2: Ubicación geográfica Facultad de Filosofía..... | 6 |
| Figura 3: Ubicación satelital de la Facultad de Filosofía. | 7 |
| Figura 4: Capas del modelo OSI..... | 11 |
| Figura 5: Topología bus..... | 14 |
| Figura 6 : Topología estrella..... | 15 |
| Figura 7: Topología anillo. | 16 |
| Figura 8: Redes PAN..... | 17 |
| Figura 9: Redes LAN..... | 17 |
| Figura 10: Redes CAN. | 18 |
| Figura 11: Redes WAN. | 19 |
| Figura 12: Comparativa entre grupo de trabajo y active directory | 27 |
| Figura 13: Objetos y atributos del directorio activo | 28 |
| Figura 14: Esquema directorio activo..... | 29 |
| Figura 15: Diseño de dominio filosofia.ug.edu.ec. | 46 |
| Figura 16: Diseño de diagrama de nagios. | 48 |
| Figura 17: Árbol directorio activo. | 52 |
| Figura 18: Árbol directorio activo. | 53 |
| Figura 19: Políticas directores. | 54 |
| Figura 20: Políticas directores. | 54 |
| Figura 21: Políticas secretarias. | 55 |
| Figura 22: Políticas secretarias. | 55 |
| Figura 23: Políticas secretarias. | 56 |
| Figura 24: Monitoreo en host del proxy norte..... | 57 |
| Figura 25: Monitoreo disco duro | 57 |
| Figura 26: Monitoreo ping..... | 58 |
| Figura 27: Monitoreo ping..... | 59 |
| Figura 28: Monitoreo carga de cpu..... | 60 |
| Figura 29: Monitoreo carga de cpu..... | 60 |
| Figura 30: Monitoreo servicio ssh..... | 61 |
| Figura 31: Cantidad usuarios conectados al servidor. | 62 |
| Figura 32: Monitoreo del consumo del ancho de banda..... | 63 |

| | |
|-----------------------------------------------------------------------------|-----|
| Figura 33 : Detalle de estado de los host | 64 |
| Figura 34: Mapa de monitoreo de nagios | 65 |
| Figura 35: Paso 1 de reporte | 66 |
| Figura 36: Paso 2 de reporte | 66 |
| Figura 37: Paso 3 de reporte | 67 |
| Figura 38: Generación de reporte | 67 |
| Figura 39: Generación de reporte por porcentaje de estado de los host | 68 |
| Figura 40: Generación de reporte | 69 |
| Figura 41: Reporte de los host por servicio | 70 |
| Figura 42: Reporte de los host por servicio | 70 |
| Figura 43: Recepción de correos y alertas..... | 71 |
| Figura 44: Bloqueo panel de control. | 76 |
| Figura 45: Bloqueo aplicaciones. | 77 |
| Figura 46: Bloqueo aplicaciones. | 77 |
| Figura 47: Aplicación papel tapiz..... | 78 |
| Figura 48: Bloqueo usb. | 78 |
| Figura 49: Bloque a recursos de red. | 79 |
| Figura 50: Bloqueo inicio de sesión. | 79 |
| Figura 51: Portal web nagios. | 86 |
| Figura 52: Servidores creados. | 87 |
| Figura 53: Servicios agregados en nagios. | 88 |
| Figura 54: Descarga NSClient++. | 89 |
| Figura 55: Configuración NSClient..... | 90 |
| Figura 56: Configuración NSClient..... | 90 |
| Figura 57: Configuración NSClient..... | 91 |
| Figura 58: Configuración NSClient..... | 91 |
| Figura 59: Configuración NSClient..... | 92 |
| Figura 60: Configuración NSClient..... | 92 |
| Figura 61: Configuración NSClient..... | 93 |
| Figura 62: Monitoreo de NSClient. | 95 |
| Figura 63: Descarga pnp4nagios. | 97 |
| Figura 64: Ingreso de host-pnp y servicios srv-pnp. | 100 |
| Figura 65: Generar gráficos con pnp4nagios..... | 101 |
| Figura 66: Generar gráficos con pnp4nagios..... | 101 |

| | |
|-------------------------------------------------------------------------|-----|
| Figura 67: Grafica en intervalo de tiempo..... | 102 |
| Figura 68: Agregar roles y características. | 103 |
| Figura 69: Selección servidor para agregar roles y características..... | 104 |
| Figura 70: Selección servicios de dominio..... | 104 |
| Figura 71: Agregar características al servidor..... | 105 |
| Figura 72: Agregar roles y características. | 105 |
| Figura 73: Agregar roles y características. | 106 |
| Figura 74: Configuración directorio activo. | 106 |
| Figura 75: Configuración directorio activo. | 107 |
| Figura 76: Configuración directorio activo. | 108 |
| Figura 77: Configuración directorio activo. | 109 |
| Figura 78: Configuración directorio activo. | 109 |
| Figura 79: Configuración directorio activo. | 110 |
| Figura 80: Configuración directorio activo. | 110 |
| Figura 81: Configuración directorio activo. | 110 |
| Figura 82: Agregar unidad organizativa..... | 112 |
| Figura 83: Agregar unidad organizativa..... | 113 |
| Figura 84: Agregar unidad organizativa..... | 114 |
| Figura 85: Creación de usuarios..... | 115 |
| Figura 86: Creación de usuarios..... | 116 |
| Figura 87: Creación de usuarios..... | 116 |
| Figura 88: Creación de usuarios..... | 117 |
| Figura 89: Creación de grupos en directorio activo. | 118 |
| Figura 90: Creación de grupos en directorio activo. | 119 |
| Figura 91: Creación de grupos en directorio activo. | 120 |
| Figura 92: Creación de grupos en directorio activo. | 121 |
| Figura 93: Capacitación al Departamento de Sistemas. | 124 |
| Figura 94: Capacitación al Departamento de Sistemas. | 124 |
| Figura 95: Capacitación al Departamento de Sistemas. | 125 |
| Figura 96: Acceso a la opción ad ds..... | 129 |
| Figura 97: Opción herramientas administrativas:..... | 130 |
| Figura 98: Crear gpo..... | 131 |
| Figura 99: Crear gpo..... | 131 |
| Figura 100: Crear gpo..... | 132 |

| | |
|----------------------------------------------------|-----|
| Figura 101: Opción plantillas administrativas..... | 132 |
| Figura 102: Bloqueo panel de control. | 133 |
| Figura 103: Bloqueo panel de control. | 133 |
| Figura 104: Bloqueo panel de control. | 134 |
| Figura 105: Bloqueo panel de control. | 134 |
| Figura 106: Bloqueo discos extraíbles. | 135 |
| Figura 107: Bloqueo discos extraíbles. | 135 |
| Figura 108: Política fondo de pantalla..... | 136 |
| Figura 109: Política fondo de pantalla..... | 136 |
| Figura 110: Política fondo de pantalla..... | 137 |
| Figura 111: Política fondo de pantalla..... | 137 |
| Figura 112: Política fondo de pantalla..... | 138 |
| Figura 113: Política propiedades de la red. | 138 |
| Figura 114: Política propiedades de la red. | 139 |
| Figura 115: Política propiedades de la red. | 140 |
| Figura 116: Política restricción de software. | 141 |
| Figura 117: Política restricción de software. | 141 |
| Figura 118: Política restricción de software. | 142 |
| Figura 119: Política restricción de software. | 142 |
| Figura 120: Política restricción de software. | 143 |
| Figura 121: Política restricción de software. | 143 |
| Figura 122: Asignación de usuarios. | 144 |
| Figura 123: Asignación de usuarios. | 145 |
| Figura 124: Asignación de usuarios. | 146 |
| Figura 125: Asignación de usuarios. | 147 |

Índice de Tablas

| | |
|---------------------------------------------------------------------------|----|
| Tabla 1: Total de Máquinas de la Facultad de Filosofía. Sede Central..... | 5 |
| tabla 2: Presupuesto..... | 7 |
| tabla 3: Estado de los host de servicios. | 23 |
| tabla 4: Comparación software de monitoreo de redes. | 25 |
| tabla 5: Cronograma actividades del proyecto. | 34 |
| tabla 6: Listado de usuarios de la Facultad..... | 38 |
| tabla 7: Listado de Directores..... | 41 |
| tabla 8: Requisitos de hardware recomendado para Nagios..... | 44 |
| tabla 9: Requisitos de hardware recomendado para Active Directory. | 45 |
| tabla 10: Cronograma de ingreso de las máquinas al dominio. | 50 |
| tabla 11: Total de máquinas en el dominio..... | 72 |
| tabla 12: Cuadro estadístico de las máquinas ingresadas al dominio. | 75 |

1. Introducción

El presente trabajo abarca los temas de monitoreo de redes y el uso del directorio activo, como soluciones a la creciente demanda en el área de redes de una empresa. Una red debe tener entre sus características la escalabilidad, pero esto implica un mayor trabajo en mantenimiento, soluciones rápidas y el conocimiento del estado actual de la red. Por estas necesidades es que se requiere de un software que ayude a gestionar y mantener una red, ayudando a simplificar las funciones de un administrador y prestando la información necesaria para la solución de problemas o prevención de estos.

El software para monitoreo que se puso en funcionamiento en la Facultad de Filosofía es Nagios, esta herramienta se eligió después de un análisis de la situación de la Facultad. Entre las características que ofrece un software para monitoreo de redes es hallar el punto o el problema dentro de la red de manera más rápida, recolección y análisis de datos para la posterior visualización en gráficos estadísticos.

El directorio activo permitirá tener una gran base de datos con la información de todo equipo conectado a la red para su fácil administración e inventario, ayuda en la seguridad y confiabilidad de los dispositivos. Y permite a un administrador gestionar la red desde un solo servidor, establecer y aplicar políticas.

Después de un análisis de diferentes herramientas planteadas para la solución, se recomendó el uso de Nagios por sus características, alertas y mensajes. La herramienta recomendada ofrece licencia de código abierto con diferentes funcionalidades y es más reconocida entre los administradores de red.

Para el uso del directorio activo la versión de Windows server elegida será Windows Server 2012 R2, puesto que es la versión ya implementada anteriormente en el Departamento de Sistemas de la Facultad y esta versión provee servicios actualizados para el uso del dominio en una empresa.

2. Problema

2.1. Antecedentes

Una de las funciones del área de sistemas de una empresa es el garantizar el correcto funcionamiento de software y hardware de los equipos asignados a los empleados de esta. El Ing. Carlos Ruiz, encargado del Departamento de Sistemas juntamente con los empleados del área ya mencionada, determinaron que, debido al incumplimiento por parte de los usuarios a las políticas internas de la Facultad de Filosofía de la Universidad de Guayaquil y el uso indebido de los computadores asignados, se ven reflejados problemas tales como:

- Virus en máquinas por USB personales, aun cuando el uso de estos está prohibido en la institución por los contratos de confidencialidad, que estipulan que toda información creada dentro de la Facultad le pertenece a esta.
- Instalación de programas (juegos) en las computadoras por parte de los funcionarios administrativos.
- Necesidad de monitorear cuantas veces cae el servicio que provee el Carrier de telecomunicaciones.
- Necesidad de monitorear el ancho de banda de la facultad debido al acceso inadecuado de los usuarios a páginas que hacen gran consumo de este.
- No existen nombres de usuarios asignados por la Facultad de Filosofía para las máquinas de cada empleado.

Con las dificultades que se presentan en la red es que se requiere un software que ayude al monitoreo y a una fácil administración. Las máquinas de la facultad constantemente presentan problemas y en su mayoría por virus encontrados en estas. Los usuarios tienen la facilidad de instalar programas y esto provoca que no se haga un buen manejo o se presenten configuraciones que alteren a la funcionalidad de los equipos.

Los usuarios también tenían acceso a las configuraciones de internet provocando en la red falencias y conflictos de IP, por ejemplo, se presentaban duplicados de IP o cambios en la configuración de DNS o proxy en las máquinas.

Al tener acceso a cualquier configuración de la máquina se dieron casos de carpetas compartidas con información vulnerable e importante y se requiere un control sobre los documentos de cada usuario.

2.2. Importancia y alcances

Cuando suceden percances en una red, es necesario poder tener una herramienta que ayude a identificar de manera rápida donde ocurrió el fallo. Existe software que permite el monitoreo de la red, el cual se puede obtener por medio de licencia pagada o licencia de código abierto.

También es necesario instalar un servidor de directorio activo para la aplicación de políticas internas que ayuden a la administración de las máquinas. Con el software para monitoreo y un directorio activo se darán las facilidades al administrador de red para que dé soluciones óptimas si llega a ocurrir un problema.

Aunque cabe destacar que con un directorio activo los problemas se reducirán, ya que se pretende limitar los accesos de los usuarios a configuraciones de las máquinas y de la red. Con un software de monitoreo encontraremos los fallos que se presentan de manera más eficaz y con las configuraciones adecuadas se permitirá conocer el estado del problema en el mismo momento en que se presenta, puede ser por medio de alertas a correo o gráficos por medio de un portal web. Como se conoce que existen problemas con la administración del ancho de banda con las soluciones presentadas se podrá tener alertas si el servicio cae o se colapsa.

Cada software se pondrá en funcionamiento en la Facultad de Filosofía, Letras y Ciencias de la Educación. Todos los departamentos, secretarías y directores que pertenecen a la Facultad y que han sido agregados anteriormente a la red, pertenecerán al servidor de dominio y los servidores ubicados en el Departamento de Sistemas serán monitoreados por el software que se elegirá como el óptimo para dar las soluciones a los problemas planteados.

El personal de Sistemas será capacitado para el uso de las herramientas propuestas que serán instaladas en la red de la Facultad que se muestra a continuación:

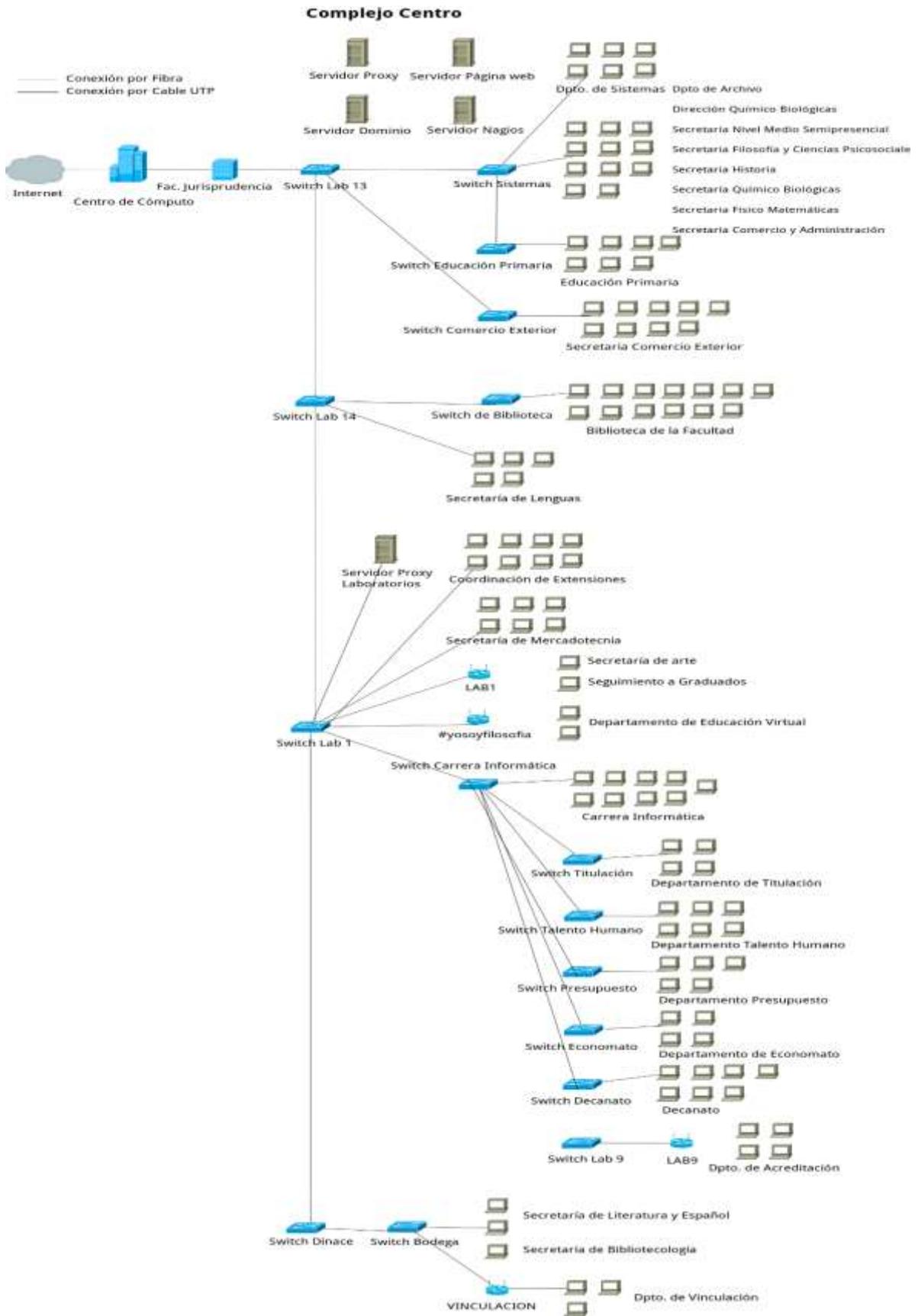


Figura 1: Red de la Facultad de Filosofía, Letras y Ciencias de la Educación.

Elaborado por: Los Autores

La Facultad está conformada por 34 departamentos ubicados en 4 edificios de la ciudadela universitaria. Se hace mención solo de los departamentos de la ciudadela central que serán ingresados al servidor de dominio, detallados a continuación:

Tabla 1: Total de Máquinas de la Facultad de Filosofía. Sede Central.

| Campus | Edificio | Planta | Departamento | No. Pc |
|---------------|-------------------|---------------|------------------------------------|---------------|
| Centro | Dinace | P1 | Prácticas Docentes | 4 |
| Centro | Dinace | PB | Vinculación | 3 |
| Centro | Dinace | PB | Literatura | 1 |
| Centro | Dinace | PB | Bibliotecología | 1 |
| Centro | Dinace | PB | Bienestar Estudiantil | 2 |
| Centro | Comercio Exterior | P1 | Archivo | 2 |
| Centro | Comercio Exterior | PB | Secretaría Comercio Exterior | 3 |
| Centro | Comercio Exterior | PB | Dirección Comercio Exterior | 3 |
| Centro | Comercio Exterior | PB | Sala Docentes Comercio Exterior | 6 |
| Centro | Comercio Exterior | PB | Nivel Medio Semipresencial | 2 |
| Centro | Comercio Exterior | PB | Filosofía y Ciencias Psicosociales | 2 |
| Centro | Comercio Exterior | PB | Historia | 1 |
| Centro | Comercio Exterior | PB | Secretaría Químico Biológicas | 1 |
| Centro | Comercio Exterior | PB | Dirección Químico Biológicas | 1 |
| Centro | Comercio Exterior | PB | Físico Matemáticas | 1 |
| Centro | Comercio Exterior | PB | Comercio y Administración | 2 |
| Centro | Comercio Exterior | PB | Educación Primaria | 7 |
| Centro | Lenguas | PB | Secretaría Lenguas | 4 |
| Centro | Lenguas | P1 | Secretaría Biblioteca | 6 |
| Centro | Principal | PB | Seguimiento a Graduados | 2 |
| Centro | Principal | PB | Carrera de Arte | 1 |
| Centro | Principal | PB | Investigaciones | 5 |
| Centro | Principal | PB | Mercadotecnia y Publicidad | 7 |
| Centro | Principal | PB | Extensiones | 8 |
| Centro | Principal | PB | Aula Virtual | 2 |
| Centro | Principal | P1 | Titulación | 4 |
| Centro | Principal | P1 | Informática y Multimedia | 10 |
| Centro | Principal | P1 | Economato | 4 |
| Centro | Principal | P1 | Presupuesto | 6 |
| Centro | Principal | P1 | Talento Humano | 6 |
| Centro | Principal | P1 | Coordinación Académica | 3 |
| Centro | Principal | P1 | Coordinación General | 2 |
| Centro | Principal | P2 | Evaluación y Acreditación | 7 |
| TOTAL | | | | 119 |

Fuente: Departamento de Sistemas.

Elaborado por: Los Autores.

2.3. Delimitación

El Sistema de Monitoreo de Redes y el Directorio Activo serán implementados en la Facultad de Filosofía, Letras y Ciencias de la Educación perteneciente a la Universidad de Guayaquil.

Ubicación Geográfica

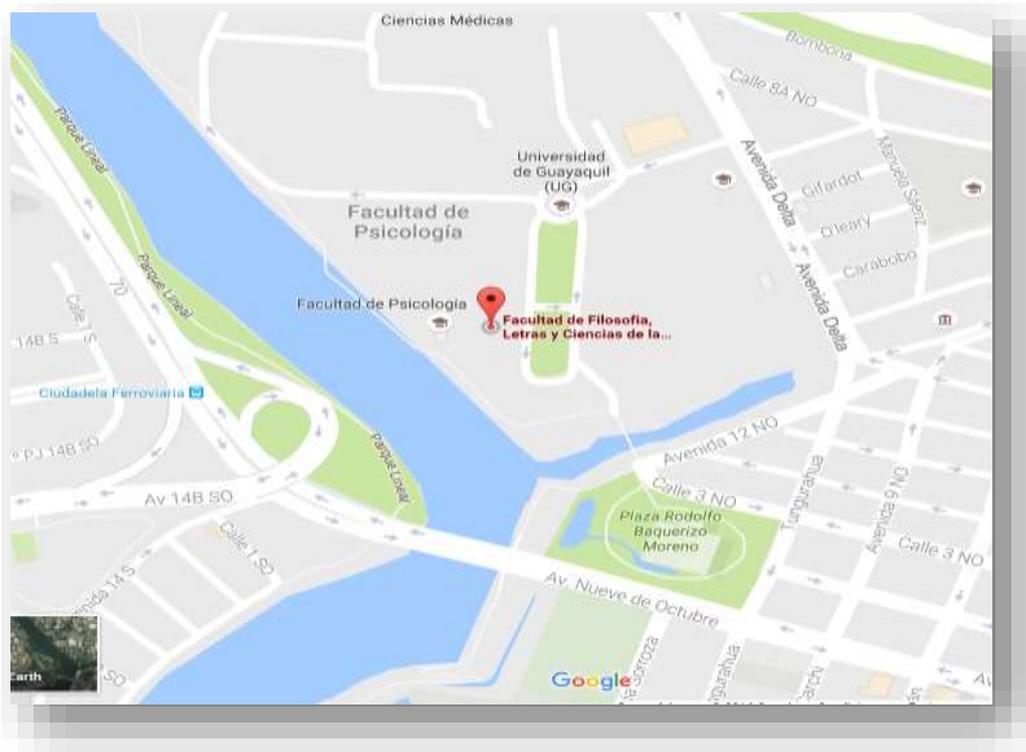


Figura 2: Ubicación geográfica Facultad de Filosofía, Letras y Ciencias de la Educación.

Fuente: <https://www.google.com.ec/maps/>

Ubicación Satelital

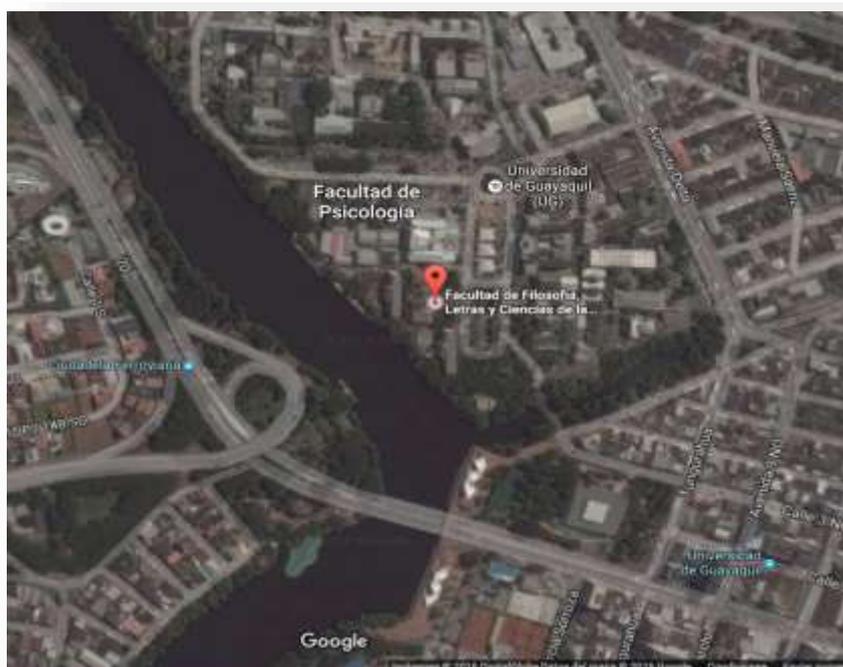


Figura 3: Ubicación satelital de la Facultad de Filosofía.

Fuente: <https://www.google.com.ec/maps/>

2.4. Presupuesto

Tabla 2: Presupuesto.

| Descripción | Cantidad | Precio | Subtotal |
|---------------------------------|----------|--------------|------------------|
| Servidor | 2 | \$1985.20 | \$3970.40 |
| Licencia Nagios | 1 | \$0.00 | \$0.00 |
| Licencia Windows Server 2012 R2 | 1 | \$100.00 | \$100.00 |
| Días de implementación | 81 | \$17.70 | \$1433.70 |
| Horas de Capacitación | 4 | \$30 | \$120.00 |
| | | TOTAL | \$5624.10 |

Fuente: Los Autores:

Elaborado por: Los Autores.

3. Objetivo General y Específicos

3.1. Objetivo General

Implementar sistemas para el monitoreo de redes y directorio activo en la Facultad de Filosofía, Letras y Ciencias de la Educación.

3.2. Objetivos Específicos

- Controlar el acceso de los usuarios a los equipos de la facultad mediante el directorio activo.
- Monitorear los servidores y enlaces de la Facultad de Filosofía por medio de Nagios.
- Establecer políticas por medio del directorio activo para el cumplimiento de las normas establecidas en la Facultad.

4. Fundamentos Teóricos

4.1. Open Source

4.1.1. Definición

Open Source o Código Abierto es el software que es distribuido y desarrollado de manera libre. Su punto de vista se orienta en compartir el código, para que el software resultante sea de calidad superior al del propietario. Es importante diferenciar el Código Abierto, que presenta su código fuente, con el Código Libre, que se distribuye libremente, pero existen programas que no presentan su código fuente (por lo tanto, no es Código Abierto). “Una licencia oficial de Código Abierto para un producto debe proporcionar al programador el código fuente legible para los humanos. No puede restringir las modificaciones hechas al software, ni la capacidad de venderlas o regalarlas.” (Wayner, 2001)

4.1.2. Tipos de software

Hay diferentes tipos de Software Open Source:

- Sistemas Operativos
- Antivirus
- Herramientas Ofimáticas
- Lenguajes de Programación
- Navegadores Web
- Clientes de Correo Electrónico
- Sistema de Monitoreo de Redes

4.2. Redes de comunicaciones

Una red de comunicaciones es aquella que tiene como finalidad intercambiar información entre dos o más entidades. Toda información que viaje como paquete de datos va a ser una secuencia de ceros y unos. Para que se logre una comunicación entre las entidades se debe considerar el medio que se va a utilizar, protocolo para comunicaciones, entre otros.

4.2.1. Modelo OSI

El modelo OSI (interconexión de sistemas abiertos) fue diseñado por la ISO, para permitir dividir las funciones de la comunicación en siete capas y así cada capa se comunicará con la anterior y la siguiente. “La torre OSI pretendía ser un modelo básico de referencia, un marco para el desarrollo de estándares que permitieran la interoperabilidad completa” (Griera, 2008)

En la década de 1980 hubo un enorme crecimiento del tamaño y cantidad de las redes en las cuales surgieron problemas de incompatibilidad. Para dar solución a este problema, la Organización Internacional de Normalización (ISO) desarrolló un modelo de red que ayuda a las diferentes empresas a crear redes compatibles con otras.

El Modelo de referencia OSI fue lanzado en 1984, el cual proporcionó a las diferentes empresas estándares para mayor compatibilidad entre las distintas tecnologías de red.

Este modelo permite dividir las funciones de la comunicación en siete capas de tal manera que una capa se comuniquen con su anterior y la siguiente.

Cada capa tiene una función que será detallada brevemente a continuación:

- Capa física: “El nivel físico se encarga de las tareas de transmisión física de las señales eléctricas entre los diferentes sistemas” (Griera, 2008). Cada equipo que interviene en la comunicación contiene especificaciones eléctricas, mecánicas y funcionales. Esta información se define en la capa física.
- Capa de enlace a datos: “Proporciona un servicio similar al nivel físico, mejorando las características de fiabilidad de la transmisión” (Griera, 2008). Esta capa se encargará de la respectiva transferencia de datos entre una entidad y la siguiente, de la detección y corrección de errores en el proceso.
- Capa de red: se encarga de direccionar las cadenas de datos entre las diferentes entidades de la red o de una red distinta y de asignar una IP.
- Capa de transporte: Segmenta las cadenas de datos a transmitir y las transporta de una entidad a otra.
- Capa de Sesión: “El encargado de gestionar las conexiones de larga duración, la recuperación de caídas de red de manera transparente y los protocolos de sincronía entre aplicaciones” (Griera, 2008). Controla el enlace que se estableció en la capa anterior, el mantenimiento y restablecer el enlace si se llega a interrumpir.
- Capa de presentación: representación de la información que se transmitió. “Se encarga de conseguir que las diferentes plataformas se puedan entender al conectarse por medio de una misma red” (Griera, 2008).
- Capa de aplicación: Proporciona el acceso a los servicios de las capas anteriores y establece los protocolos para el intercambio de la información.



Figura 4: Capas del modelo OSI.

Elaborado por: Los Autores.

4.2.2. Protocolos de comunicación

Los protocolos son un conjunto de normas que al aplicarse a un proceso de comunicación permiten a entidades intercambiar información. “Con los protocolos se pretende la intercomunicación de entidades situadas en diferentes maquinas” (Griera, 2008). Existen una gama de protocolos, pero en esta sección se hará referencia a los protocolos usados en el modelo OSI.

- Protocolos de capa física o capa 1: Se hace referencia al tipo de medio que se establecerá para la conexión, sea esta inalámbrica o por medio de cableado. “Especifica las características del hardware que se utilizará para la red”. (Oracle, 2010)
- Protocolos de capa de enlace o capa 2: se hace mención a los protocolos de la interfaz que se utiliza para conectar la entidad a la red de comunicaciones. “La capa de vínculo de datos proporciona también control de errores y estructuras” (Oracle, 2010).

- Protocolos de capa de red o capa 3: el protocolo característico es el protocolo IP, con este protocolo se permite que la información viaje desde su origen hasta su destino por medio de la mejor ruta seleccionada.
- Protocolos de capa de transporte o capa 4: “garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos” (Oracle, 2010). Tenemos a los protocolos como UDP y TCP. El protocolo UDP se caracteriza por enviar paquetes al destino sin necesidad de una conexión previamente establecida. Por el contrario, el protocolo TCP establece la conexión entre las entidades emisoras y receptoras previamente para garantizar que el envío de los paquetes es confiable e íntegro.
- Protocolo de capa de sesión o capa 5: Para el modelo OSI haremos referencia a dos protocolos; el primero la unión de los protocolos SSL y TLS conjunto con el segundo protocolo RPC. SSL y TLS son protocolos que ayudan a la encriptación de la información que se transmite entre emisor y receptor de tal manera que solo el receptor pueda comprender o des encriptar el mensaje. Mientras que el RPC se usa para establecer conexiones remotas, siendo un protocolo muy usado para las comunicaciones cliente – servidor; en el cual es el cliente que hace la solicitud para que el servidor ejecute cierto proceso y este conteste con los resultados de la operación.
- La capa 6 o capa de representación de datos es la encargada de que la información se reconozca en cualquier equipo indiferente de la representación que use la máquina en sí. En esta capa se puede usar la Notación Sintáctica Abstracta o ANSI.1 que cumple con el objetivo de representar datos independientemente de la forma de representación interna de la máquina.
- Protocolos de capa 7: Es la capa para interactuar con el usuario por eso se puede usar variedad de protocolos. Podemos usar los más conocidos como HTTP que se encarga de la representación y publicación de las páginas web, SMTP es el protocolo usado para los envíos de correo electrónico, FTP es el protocolo que se encarga de la transferencia de archivos, entre otros.

4.3. Infraestructura de red

Como se distribuyen las entidades que van a intercambiar información en una red se le denomina infraestructura de red. Dependiendo de la forma que tome la red cuando se la diseña es lo que se define como topología de red, esta puede ser física o lógica. “Lo primero que caracteriza una red local es la manera en que se conectan las estaciones; es decir, la forma que adopta el medio compartido entre las mismas” (Griera, 2008).

4.3.1. Topologías físicas

La topología física hace referencia a la distribución física de los elementos de red que se van a implementar y de los medios que los interconectaran.

- **Topología en Bus**

“Todos los ordenadores están pendientes de si hay actividad en el cable. En el momento en que un ordenador pone una trama, todos los ordenadores la cogen y miran si son el destinatario de la misma. Si es así, se la quedan, en caso contrario, la descartan” (Griera, 2008) . Considerada la topología más básica y fácil de implementar. Contiene un solo canal de comunicaciones para todos los dispositivos de red, este canal recibe el nombre de bus o backbone. En los extremos del cable, que permite la comunicación y es único, contiene una resistencia de acople denominada terminador; este acople nos indica que no hay más equipos en los extremos y el cierre del bus por medio del acople de impedancias.

Aunque su simplicidad cuente como una de sus ventajas este tipo de topología cuenta con un límite en la cantidad de equipos conectados, es de complicada reconfiguración, colisión de mensajes, perdidas en la transmisión y la degradación de la señal.

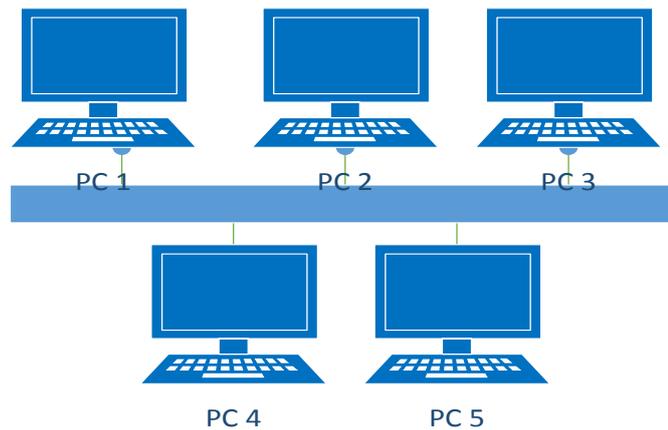


Figura 5: Topología Bus.

Elaborado por: Los Autores

- Topología en estrella

“La topología en estrella consiste en conectar cada ordenador a un punto central, que puede ser tan sencillo como una simple unión física de los cables.” (Griera, 2008). Es una de las topologías más usadas. La topología en estrella tiene un punto central al cual todos los dispositivos están conectados, al ser de esta manera la conexión toda comunicación, distribución, conmutación y control deberá pasar por este nodo central. Podemos encontrar topologías en estrellas con nodos activos que previenen el eco y lo solucionan y otras que carecen de esta función.

Entre sus ventajas está que si uno de los terminales falla no afecta al resto y la fácil escalabilidad de la red; pero si un nodo es el que falla la red se desconecta.

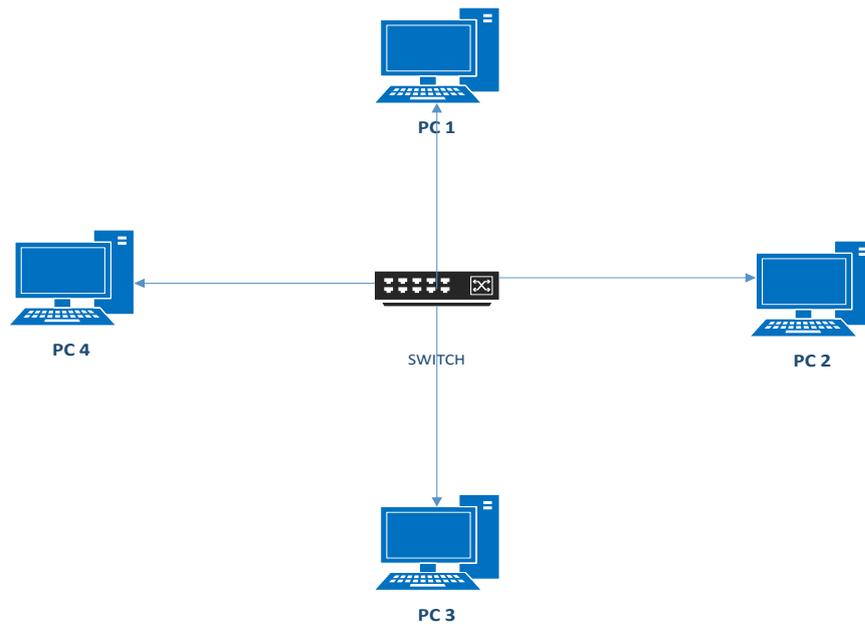


Figura 6 : Topología Estrella

Fuente: Los autores

- Topología en Anillo

Se caracteriza por tener una estación conectada a la siguiente y así hasta que la última estación se conecta con la primera dando forma de un círculo.” Cuando un ordenador quiere enviar una trama a otro, ésta debe pasar por todos los ordenadores que haya entre ellos” (Griera, 2008). Para poder repetir la señal cada nodo tiene un transmisor y un receptor. Entre sus ventajas tenemos que es la que menos colisiones presenta entre las topologías por usar el algoritmo token ring y si se desea que la comunicación sea bidireccional creando una topología de doble anillo y con una gran tolerancia a fallos.

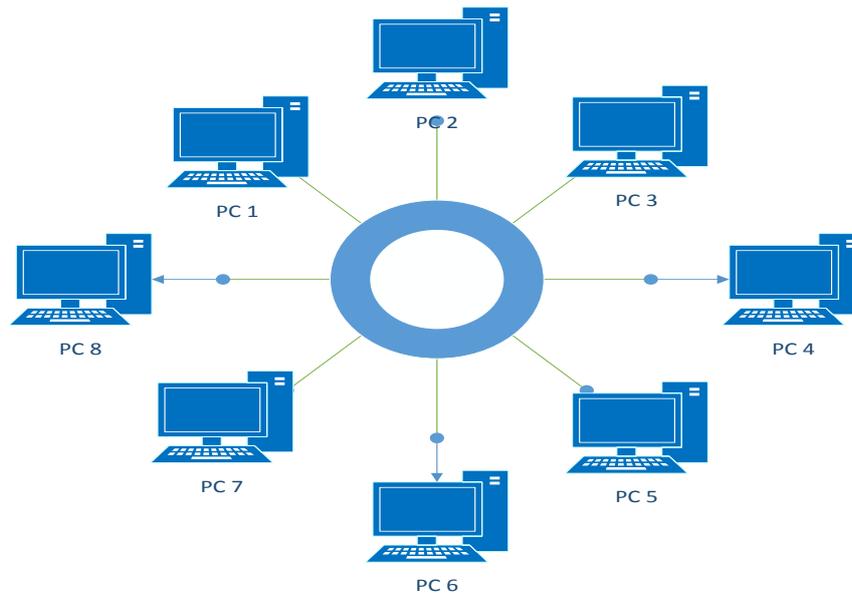


Figura 7: Topología Anillo.

Elaborado por: Los Autores

4.3.2. Topologías lógicas

La topología lógica abarca las configuraciones de red de las entidades que intervienen en la comunicación.

- Según su tamaño:
 - Redes de Área Personal “PAN”: son aquellas redes que su área de acción comprende solo el entorno del usuario con aquellos dispositivos que interactúe. Entre las tecnologías que se pueden implementar tenemos Wifi o bluetooth.

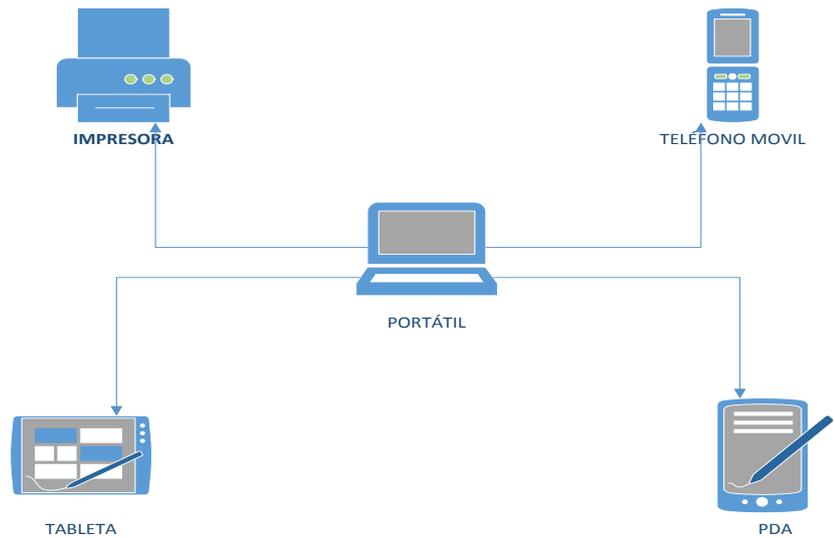


Figura 8: Redes Pan.

Elaborado por: Los autores

- Redes de Área Local “LAN”: “Son redes de propiedad privada que se encuentran en un solo edificio o en campos de pocos kilómetros de longitud” (Tanenbaum, 2003). Redes que su alcance llega hasta unos cuantos kilómetros de cobertura, se las considera redes privadas por lo que su estructura suele ser una empresa, una casa, etc. Operan entre los 10 y 100 Mbps de velocidad.

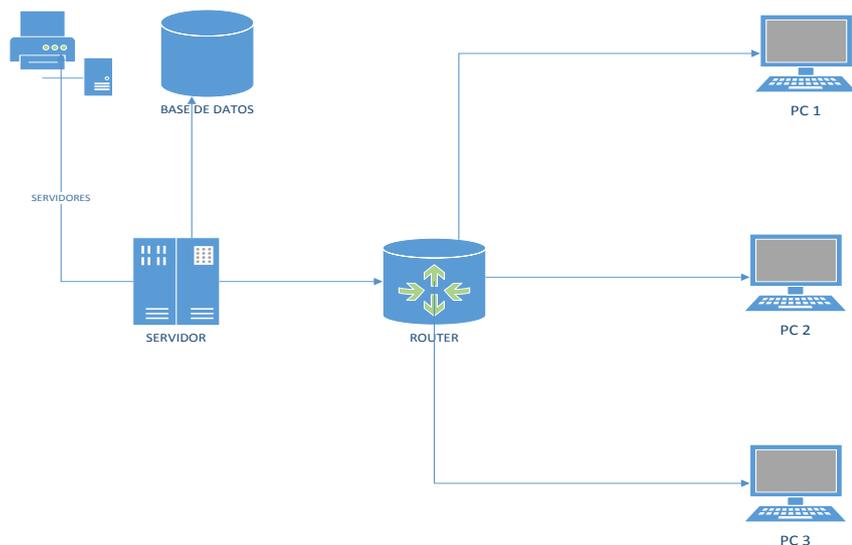


Figura 9: Redes LAN.

Elaborado por: Los Autores

- Redes de Área de Campus “CAN”: es una extensión de la red LAN, cuando se interconectan diferentes edificios con cierta proximidad entre sí. Tienen un área geográfica limitada, a veces se las puede considerar redes de área metropolitana pero que su uso se limita a áreas como campus universitarios.

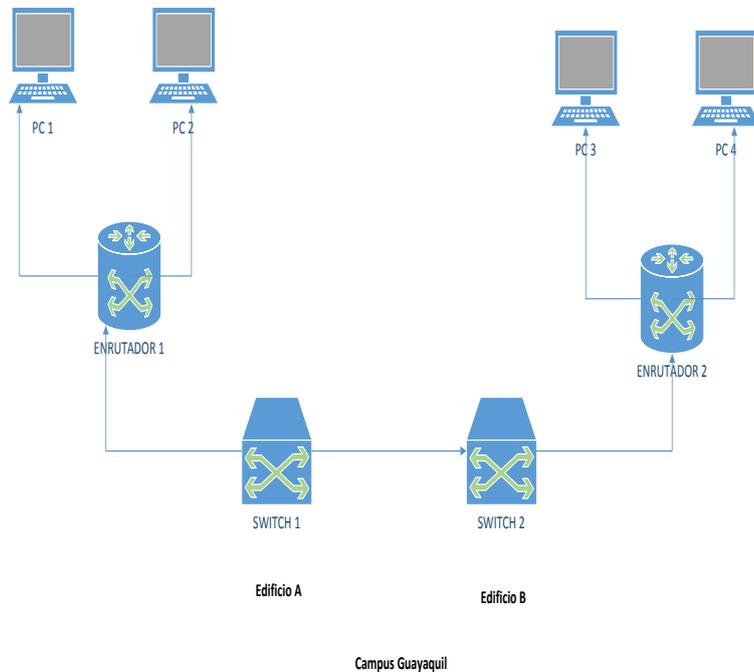


Figura 10: Redes Can.

Elaborado por: Los Autores

- Redes de Área Metropolitana “MAN”: aunque en la actualidad no son muy usadas, son aquellas redes LAN que están interconectadas en la misma ciudad o ciudades próximas. “El ejemplo más conocido de una MAN es la red de televisión por cable disponible en muchas ciudades” (Tanenbaum, 2003).
- Redes de Área extensa “WAN”: cuando unimos varias redes LAN que están separadas por miles de kilómetros reciben el nombre de WAN. “Abarca una gran área geográfica, con frecuencia un país o un continente” (Tanenbaum, 2003).

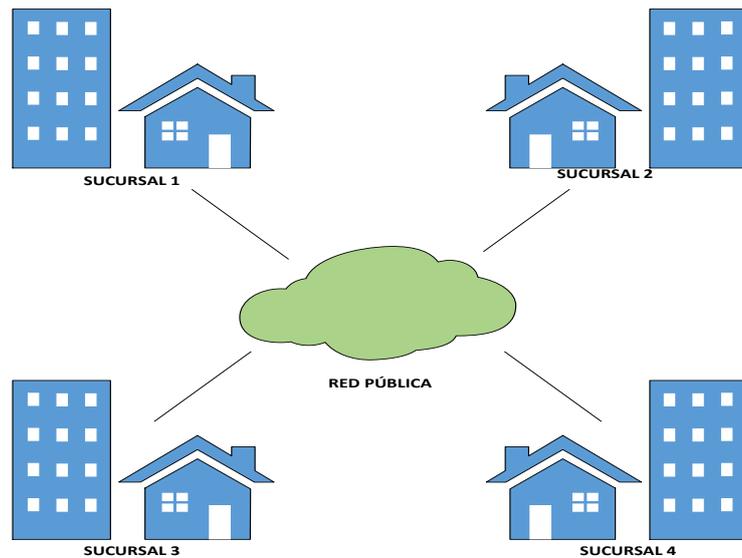


Figura 11: Redes WAN.

Fuente: Visio Profesional

- Según su carácter:
 - Redes privadas: aquellas redes que son propiedad de una empresa, adecuada según las necesidades de esta.
 - Redes públicas: Se las utiliza para la unión de redes pequeñas, caracterizadas por su precio económico.
 - Redes mixtas: redes privadas que hacen uso de una red pública.
- Según la tecnología que usan para la transmisión:
 - Redes punto a punto: redes cuya comunicación está dada de equipo a equipo (origen y destino).
 - Redes broadcast: cuando todos los equipos de la red comparten un canal de comunicación se le denomina broadcast.

4.4. Monitoreo de redes

4.4.1. Definición de monitoreo

Es el uso de un Sistema que monitorea constantemente los servicios en una red de equipos en busca de fallas, para notificar a los administradores de red ya sea vía correo, mensaje de texto u otras alarmas.

4.4.2. Herramientas para el monitoreo de redes

4.4.2.1. Zabbix



“Este sistema viene con una interfaz web que nos permitirá ver la monitorización, representación de los datos, configuraciones de monitores, alertas y la administración de los usuarios.” (Zabbix, 2016).

Zabbix es un sistema completo para la monitorización de cualquier dispositivo que se encuentre conectado en nuestra red. Zabbix tiene entre sus funciones el obtener datos desde sus monitores que ya vienen predefinidos o la creación de alguno que cumpla con nuestras necesidades. Realiza la monitorización usando SNMP en sus dos formas polling o trapping. Para la monitorización en servidores se hace uso de agentes instalados previamente.

Este sistema viene con una interfaz web que nos permitirá ver la monitorización, representación de los datos, configuraciones de monitores, alertas y la administración de los usuarios. Zabbix permite definir la gravedad de una incidencia y en base a esta configuración se tomará acciones. Se puede definir plantillas sobre las cuales se determinará el monitor y el disparador de alerta correspondiente. Zabbix nos provee plantillas genéricas para servidores Linux, web, correo, switch, etc.

Zabbix almacena los valores que se obtuvieron de las monitorizaciones en una base de datos MySQL y a partir de estas elabora las gráficas.

4.4.2.2. SolarWinds



“SolarWinds Network Configuration Manager proporciona administración de configuración accesible y fácil de usar que se usa en forma independiente o se integra perfectamente con SolarWinds NPM.” (SolarWinds, 2010).

Es una herramienta que permite la administración de archivos de la configuración de nuestra red por medio de una interfaz web. SolarWinds nos permite acceder a la configuración de los dispositivos y da alertas sobre cualquier cambio que se efectuó.

No es necesario un inicio de sesión por telnet o SSH con el dispositivo para cambiar algún parámetro de configuración. Todo esto lo hace en tiempo real y da notificaciones de forma instantánea, dando como resultado una visibilidad instantánea y la mejora de seguridad en la red.

4.4.2.3. Cacti



“Una herramienta para monitorizar, archivar y presentar estadísticas de redes y servidores” (Center, 2012).

Esta herramienta está basada en RRDTOol dando cierto énfasis en la interfaz gráfica. También toda información del monitoreo se guarda en una base de datos MySql y su interfaz está basada en el lenguaje de programación PHP.

Entre las funciones de monitoreo que tiene esta el medir la carga de un CPU y su capacidad. Emite alarmas basándose en umbrales. Organiza la información en estructuras jerárquicas. Usa SNMP para capturar datos o también por medio de scripts. Permite la creación de plantillas para reutilizar las definiciones de gráficos.

4.4.2.4. Nagios



“Es muy usada por los administradores de sistemas y red para comprobar la conectividad entre los hosts y garantizar que los servicios de la red están funcionando como se esperaba” (Barth, 2008) .

Nagios es una herramienta orientada a la supervisión de los recursos de la red, enviando notificaciones por vía correo electrónico, mensajes de texto, pop-ups, etc.

Una de sus principales funciones es el observar y verificar los comportamientos de los servicios de la red tales como http, SQL, SSH, etc o al del host como router, switch, impresoras entre otros.

Entre sus funciones esta:

- Monitoreo de recursos de red.
- Monitoreo de los servicios de la red.
- Capacidad para identificación de nodos padres o hijos para detección de problemas.
- Log de eventos.

- Administración vía web para supervisar los estados de los servicios.

“Nagios Core proporciona un marco de seguimiento riguroso y configurable para realizar controles de una manera consistente y para alertar a las personas apropiadas y sistemas de cualquier problema que detecte.” (Barth, 2008).

Al ser un software open source nagios da muchas facilidades para realizar configuraciones según la necesidad del administrador permitiéndole modificar las alertas o desde que vía desea recibirlas.

Nagios al monitorear recursos de red da el alcance de tener vigilado los recursos de sistemas de hardware como el uso de discos, la memoria, los puertos USB y sus estados independientes del sistema operativo.

Estados de los hosts y servicios:

Nagios para hacer la evaluación de los puertos y servicios usa cuatro valores diferentes detallados a continuación:

Tabla 3: Estado de los Host de Servicios.

| Estado | Nombre | Descripción |
|---------------|---------------|--------------------------------------------------------------------------------------|
| 0 | OK | Todo está en orden |
| 1 | Warning | Se ha superado el límite de advertencia, pero el límite crítico no se ha alcanzado |
| 2 | Critical | Límite crítico excedido o el plugin se averió después del tiempo de espera de prueba |
| 3 | Unknown | Ocurrió un error dentro del plugin |

Fuente:(Barth, 2008)

Elaborado por: Los Autores

Los estados de los servicios tendrán los valores detallados en la tabla mientras que para los hosts tienen un ligero cambio:

- Up: el host es alcanzable o si se puede detectar.
- Down: el equipo está inactivo
- Unreachable: el host es inalcanzable o no es detectado por el nagios.

4.4.3. Comparación software de monitoreo

Tabla 4: Comparación Software de Monitoreo de redes.

| Nombre | Graficas | Informes | Grupos Lógicos | Estadísticas | Agentes | SNMP | Complementos | Alertas | Aplicación Web |
|------------|----------|----------|----------------|--------------|---------|------|--------------|---------|----------------|
| Zabbix | X | X | -- | X | X | X | X | X | X |
| SolarWinds | X | -- | -- | X | X | X | X | X | X |
| Cacti | X | X | X | X | X | X | X | X | X |
| Nagios | X | X | X | X | X | X | X | X | X |

Elaborado por: Los Autores.

4.5. Directorio Activo

4.5.1. Definición

“Las cuestiones básicas relacionadas con un centro de servicios de directorio giran alrededor de la información que se puede almacenar en la base de datos, cómo se almacena, cómo se puede consultar información específica y qué se puede hacer con los resultados.” (Microsoft, 2000) .

Un directorio Activo en sí, es un almacén de datos que permite almacenar información de los objetos de la red y usuarios. Los objetos pueden ser: servidores, impresoras, cuentas de equipo y cuentas de usuario de red.

Si no poseemos un directorio activo lo que vamos a obtener es un gran conjunto de equipos que administrar, para lo cual nos vamos a tener que desplazar por equipo para hacer las respectivas configuraciones y restricciones.

Al ser una gran base de datos vamos a obtener una estructura jerárquica con la información de todos los objetos existentes permitiendo al administrador tener a su disposición todos los datos del directorio y usuarios. “Los usuarios pueden buscar y usar recursos en la red sin conocer el nombre o la ubicación exactos del recurso.” (Microsoft, 2000).

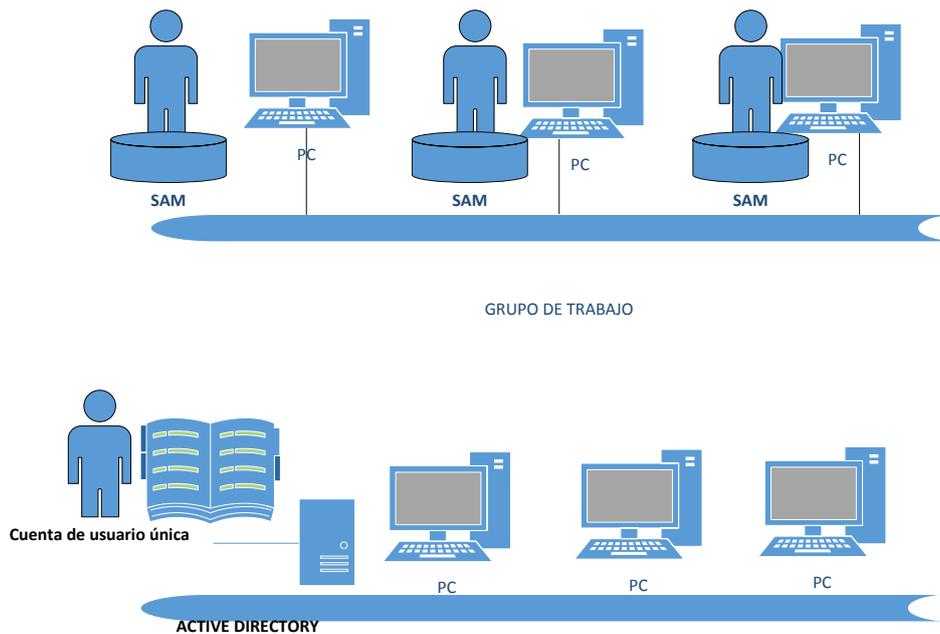


Figura 12: Comparativa entre grupo de trabajo y Active Directory

Fuente: (Molina Caballero & Baena Espejo).

Elaborado por: Los Autores

Para el usuario será indiferente la localización del objeto y únicamente podrá acceder a este por medio de la autenticación de inicio de sesión desde cualquier parte de la red. No todo usuario podrá acceder a todos los servicios, esto será delimitado por el control de acceso que maneja el administrador.

Un directorio activo facilita las tareas asignadas al administrador de red, permitiéndole obtener un catálogo con todos los objetos del directorio, crear reglas de control de acceso a los objetos y la distribución de todos los datos del directorio por la red.

4.5.2. Objetos de directorio activo

A todo elemento que compone la red y está dentro de la base de datos del directorio, se le define como objeto. Cada objeto tiene sus propias características denominados atributos. Como ya se especificó vamos a obtener por medio del directorio activo una estructura jerárquica para la fácil administración, esta

estructura determinara o dará una estructura lógica separada de la estructura física que mantenga, es decir indiferente la ubicación física los equipos.

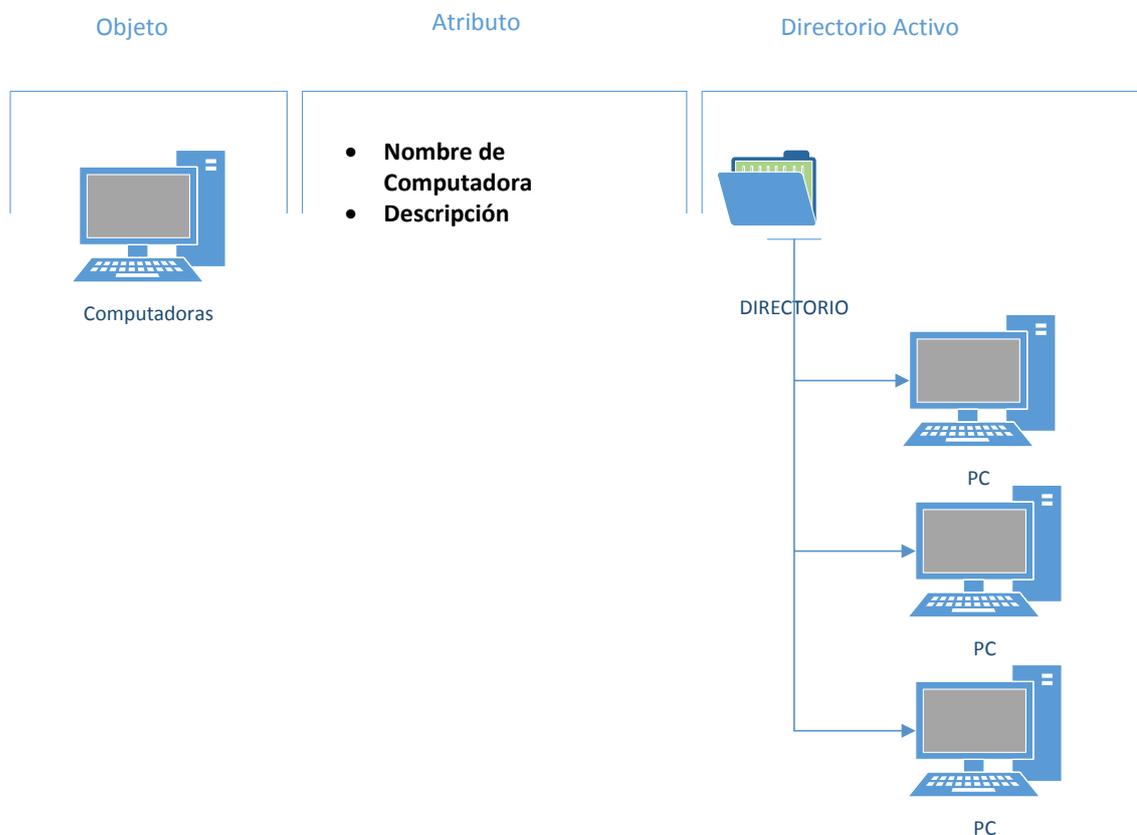


Figura 13: Objetos y Atributos del Directorio Activo

Elaborado por: Los Autores

4.5.3. Formas de Organización en Directorio Activo

- Dominios: Es la unidad base de la estructura lógica del directorio activo. “En Active Directory, un dominio es una colección de equipos, usuarios, impresoras, etc.” (Budris, 2011).
- Bosque: Dominios que comparten una configuración en común.
- Árbol: Dominios que comparten un DNS (espacio de nombre) contiguo.
- Unidades Organizativas: Son contenedores donde se pueden colocar otros objetos. En estas unidades se pueden configurar las directivas de grupo y se utilizan para establecer una estructura jerárquica.

- Grupos: Conjunto de objetos que se lo puede tratar como a uno solo al ser del mismo tipo. Se utiliza para asignar derechos a recursos y así poder simplificar tareas.
- Usuarios: Son los que poseen cuentas para la identificación en el sistema y poder acceder por medio de esta a los recursos de la red.
- Equipos: Cada ordenador que está dentro de la red y puede ser parte del dominio se lo denomina equipo.
- Espacios de nombres: “Un espacio de nombres es un área designada que tiene límites específicos donde se puede resolver un nombre lógico asignado a un equipo” (Barth, 2008), permitiéndole tanto al administrador como a un usuario localizar un objeto de la red conociendo sus características o buscar información de un servicio o recurso.

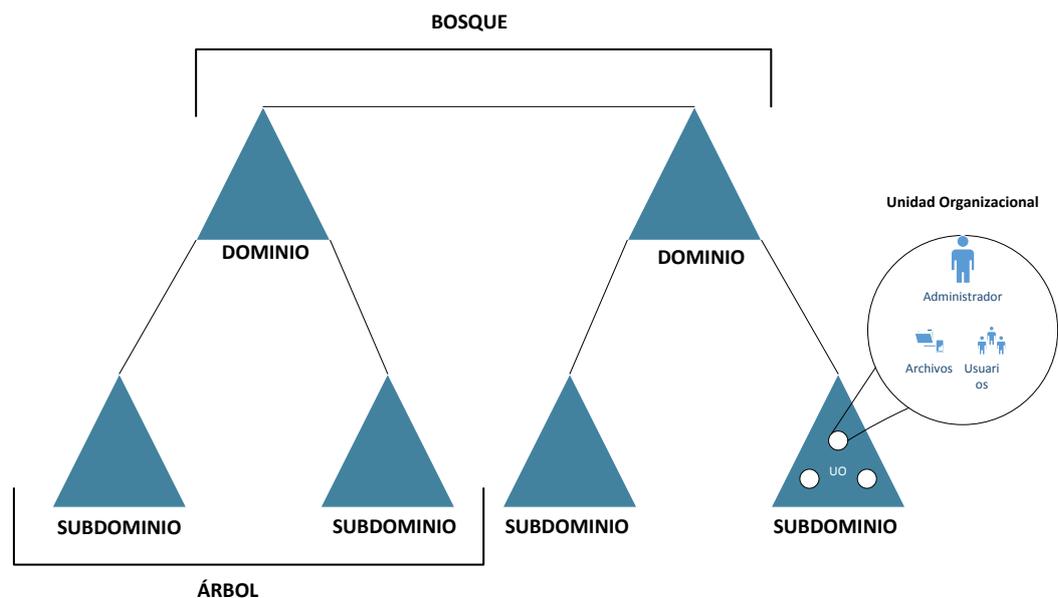


Figura 14: Esquema Directorio Activo.

Elaborado por: Los Autores.

4.6. Metodología PPDIOO

“El proceso PPDIOO es el camino crítico para lanzar y completar un despliegue exitoso del cliente, desde la propuesta de solicitud de información hasta la capacitación exitosa del personal de operaciones.” (Cisco, 2008). Esta metodología

fue desarrollado por la compañía de Cisco para definir actividades mínimas que se requieran para la instalación y operación de tecnologías. Esta definida por la siguientes fases:

- Preparar y Planear: “Utilizando herramientas de evaluación y planificación, los ingenieros de sistemas ayudan a los socios y clientes a encontrar la mejor solución para sus necesidades empresariales.” (Cisco, 2008). En estas fases se visualiza el proyecto, se levanta información y se evalúa con que herramientas se cuenta para lograr los objetivos del proyecto.
- Diseñar: “Utilizando los requisitos verificados del cliente, el equipo de diseño crea el diseño detallado, que incluye la lista de equipos, diagramas de red y flujos de tráfico.” (Cisco, 2008). En esta fase todo diseño de red se basará sobre los requerimientos de negocio y técnicos, que ha sido obtenidos de las dos fases anteriores.
- Implementar: “El equipo de implementación utiliza el diseño detallado para instalar y configurar el equipo, luego desarrolla e implementa un plan de pruebas detallado para determinar que la red está lista para su uso.” (Cisco, 2008). Se comienza la configuración e integración de los equipos basado en el diseño de la fase anterior, todo esto sin afectar a la disponibilidad de la red.
- Operación: “Las operaciones en curso incluyen la administración y supervisión de componentes, la realización de mantenimiento rutinario, la administración de actualizaciones y la administración de contratos de rendimiento y de nivel de servicio”. (Cisco, 2008).
- Optimizar: En esta fase se maneja y mejora la red. Se realiza cualquier optimización sin afectar o interrumpir el rendimiento de la red.

5. Marco Metodológico

La metodología escogida para realizar este proyecto y su aplicación sobre la implementación está basada en la metodología PPDIIO (Preparar, Planificar, Diseñar, Implementar y Operar), la cual provee los siguientes beneficios:

- Disminuye el TCO (Costo Total de Propiedad) de un proyecto de red validando los requisitos previos para el diseño e implementación del mismo y planeando el requerimiento de recursos, cambios de infraestructura a lo largo del proyecto.

- Incrementa la disponibilidad de la red creando diseños sólidos y validando la operación de la red final.
- Mejora la agilidad de la institución uniendo las necesidades con la estrategia tecnológica del mismo.
- Incrementa los tiempos de acceso a las aplicaciones y servicios.

La implementación de esta metodología ayudará a realizar los siguientes análisis de la factibilidad del proyecto monitoreo de redes y directorio activo:

- Factibilidad Técnica: se encuentran disponibles todas las herramientas a usarse para la implementación en un servidor.
- Factibilidad Legal: no registra ningún impedimento de tipo legal, de acuerdo a las leyes de Ecuador, ya que se está usando software propietario correctamente licenciado y todas las ideas y aplicaciones que se realizarán en el proyecto son basadas en software libre, que nos permite realizar modificaciones a las herramientas utilizadas con la licencia GPL.
- Factibilidad Económica: no reviste gastos en el mismo durante el curso, ya que se usarán herramientas libres para la implementación. En caso de implementar el proyecto para el acceso general en una institución académica, se usará el presupuesto referencial para la implementación de los equipos necesarios para soportar el proyecto.

El desarrollo del presente proyecto se llevará a cabo en 5 fases ejecutadas secuencialmente, para aquello se hará uso de la metodología PPDIIO (Preparar, Planificar, Diseñar Implementar y Operar), con la finalidad de obtener la información necesaria y seguir un adecuado orden durante el proceso de ejecución del presente proyecto.

5.1. FASE I: Preparar

Toda implementación, inversión o propuesta de solución en el área de redes, dará como resultado una mejora u optimización en las funciones del personal a cargo del área técnica, causando efectos positivos en la institución. Para el presente proyecto no habrá inversión económica directamente, ya que se dará uso de los equipos que

posee la Facultad de Filosofía, proveyendo de beneficios tanto para la institución como para los autores del proyecto. Es necesario definir los aspectos relacionados al problema que éste proyecto resolverá:

- La necesidad de monitorear el ancho de banda de la facultad.
- El acceso inadecuado de los usuarios a páginas que hacen gran consumo del ancho de banda.
- No existen nombres de usuarios asignados por la Facultad de Filosofía para las máquinas de cada empleado.
- Restringir el uso de USB y acceso a la información sensible.

Esta etapa permite definir las características que comprenden a los usuarios, las aplicaciones, servicios y los equipos. Esta información ha sido obtenida a través de la documentación de red y la realización de las entrevistas al personal de la institución.

- Los usuarios internos son 119, con equipos asignados por la Facultad, y se encuentran laborando dentro de los diferentes departamentos ubicados en los diferentes edificios de la Facultad de Filosofía.
- Los usuarios externos son generalmente estudiantes que utilizan los servicios ofrecidos por la organización.
- Aplicaciones y Servicios que ofrece son utilizados por usuarios internos y externos. Las aplicaciones son de tipo web y se encuentran alojadas en los servicios de mayor uso que son: Sistema Académico, Correo Empresarial, Internet, Cámaras, Control de Acceso, Biométricos.
- Equipos y dispositivos de red. Para ofrecer los servicios y aplicaciones en la red se tienen desplegados los siguientes equipos y dispositivos de red:
 - Ciento diecinueve computadores.
 - Dos servidores.
 - Dos proxy - firewalls.

5.2. FASE II: Planificar

Durante este proceso se podrán identificar los requerimientos técnicos, y los alcances que proporcionará la herramienta de monitoreo Nagios y el directorio activo. Este

proceso se llevará a cabo mediante la recolección de información. En este se describe el análisis de la situación actual considerando la red física, la seguridad de la red y las aplicaciones y servicios. Una herramienta de monitoreo en la actualidad dará facilidades y ventajas a la Facultad, como que es en tiempo real y que permite la alarma en su interfaz cuando el enlace de una de las sedes se ve afectado. Para fines analíticos, es bueno considerar que la herramienta muestra un histórico de alarmas y estados acerca de los equipos.

5.2.1. Cronograma de Actividades del proyecto

Para cada fase se estableció un cronograma:

Tabla 5: Cronograma Actividades del Proyecto.

| Fase | Actividad | Departamentos | Fecha inicio | Fecha fin | Responsable |
|-------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------|---------------------|------------------|----------------------------------|
| Preparar | Aprobación Anteproyecto en Facultad de Filosofía | Facultad de Filosofía – Sede Central | 02/12/2015 | 02/12/2015 | Carlos Velasco |
| Preparar | Aprobación Anteproyecto Universidad Politécnica Salesiana | Universidad Politécnica Salesiana | 30/03/2016 | 30/03/2016 | Carlos Velasco Gianella Cagua |
| Planificar | Entrevista detallada al Ing. Carlos Ruiz Berna, Director del Departamento de Sistemas de la Facultad de Filosofía | Dpto. de Sistemas Facultad Filosofía | 02/05/2016 | 02/05/2016 | Carlos Velasco Gianella Cagua |
| Planificar | Revisar la documentación de la configuración de los equipos que están conectados en la red | Dpto. de Sistemas Facultad Filosofía | 09/05/2016 | 11/05/2016 | Carlos Velasco Gianella Cagua |
| Planificar | Revisar la documentación de la organización del personal administrativo de la Facultad ya antes mencionada | Dpto. de Sistemas Facultad Filosofía | 12/05/2016 | 13/05/2016 | Carlos Velasco Gianella Cagua |
| Diseño | Diseño del dominio | Dpto. de Sistemas Facultad Filosofía | 16/05/2016 | 17/05/2016 | Carlos Velasco Gianella Cagua |
| Diseño | Diseño de topología en Nagios | Dpto. de Sistemas Facultad Filosofía | 18/05/2016 | 19/05/2016 | Carlos Velasco Gianella Cagua |

| | | | | | |
|-------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------|------------|------------|----------------------------------|
| Implementar | Instalación y configuración del directorio activo 2012r2 | Dpto. de Sistemas Facultad Filosofía | 23/05/2016 | 25/05/2016 | Gianella Cagua |
| Implementar | Instalación y configuración de Nagios | Dpto. de Sistemas Facultad Filosofía | 26/05/2016 | 27/05/2016 | Carlos Velasco |
| Implementar | Pruebas de funcionamiento de los servidores de directorio activo y Nagios | Dpto. de Sistemas Facultad Filosofía | 30/05/2016 | 31/05/2016 | Carlos Velasco Gianella Cagua |
| Implementar | Creación de usuarios y grupos en el directorio activo | Dpto. de Sistemas Facultad Filosofía | 30/05/2016 | 31/05/2016 | Carlos Velasco Gianella Cagua |
| Implementar | Creación de políticas de red | Dpto. de Sistemas Facultad Filosofía | 01/06/2016 | 01/06/2016 | Carlos Velasco Gianella Cagua |
| Implementar | Instalación de programa agente para monitoreo de red en los equipos (computadoras y servidores) de la Facultad | Dpto. de Sistemas Facultad Filosofía | 15/06/2016 | 15/09/2016 | Carlos Velasco |
| Implementar | Ingreso de máquinas al servidor de dominio | Sede central Facultad Filosofía | 03/06/2016 | 16/09/2016 | Carlos Velasco Gianella Cagua |
| Operar | Pruebas de funcionamiento agentes de monitoreo y usuarios de directorio activo | Dpto. de Sistemas Facultad Filosofía | 19/09/2016 | 30/09/2016 | Carlos Velasco Gianella Cagua |
| Operar | Capacitación al personal de sistemas de la Facultad de Filosofía | Dpto. de Sistemas Facultad Filosofía | 21/10/2016 | 24/10/2016 | Carlos Velasco Gianella Cagua |

Fuente: Los Autores.

La recolección de datos se obtiene mediante entrevista realizada al Ing. Carlos Ruiz Berna, Director del Departamento de Sistemas de la Facultad de Filosofía, sobre los objetivos de la organización y los aspectos técnicos, como la funcionalidad y la seguridad que se espera que cumpla la red. Para obtener y documentar la información se ha realizado un cuestionario a utilizar en la entrevista, quien determinará las necesidades del mismo y que pueden ser cubiertas por la herramienta que se presenta en el proyecto. Esta información se encuentra detallada en el Anexo L del documento. Se debe identificar la infraestructura que la empresa posee, y con toda esta información mostrar un análisis de esta fase.

5.2.2. Diseño de la entrevista

El diseño de la entrevista tiene como finalidad obtener y documentar la información necesaria para definir los requerimientos de la red de datos. La entrevista está compuesta por un conjunto de preguntas que nos ayudan a identificar:

- Las aplicaciones y servicios de red.
- Los objetivos y las restricciones organizacionales.
- Los objetivos y las restricciones técnicas.

La información obtenida será analizada y se obtendrán los requerimientos.

5.2.3. Análisis de la entrevista

Una vez realizada la entrevista se han documentado y analizado los resultados, obteniendo la siguiente información:

- Las aplicaciones de mayor importancia para la organización son: Sistema Académico, Correo Empresarial e Internet. Estas aplicaciones se encuentran dentro de los servicios públicos que ofrece la organización a los usuarios externos.
- Las aplicaciones descritas en el punto “a” manejan información personal de los usuarios. La propuesta de un directorio activo debe permitir que estas aplicaciones se ejecuten en un entorno seguro.

- Al momento no se tiene definido que aplicaciones o servicios que se podrían agregar a los ya existentes. Es común que las autoridades en cualquier momento, soliciten que se implementen nuevas aplicaciones sin la realización de una planificación adecuada.
- Los servicios que actualmente brinda la red de datos son: Internet, Correo, Recursos Compartidos. La propuesta debe mantener la capacidad de soportar la ejecución de todos estos servicios.
- Los switches desplegados en la arquitectura de red son dispositivos de la marca Cisco. Estos dispositivos presentan configuraciones de tecnologías y protocolos desarrollados por la misma compañía. Por este motivo, la propuesta en lo posible debe mantener la misma línea tecnológica.
- El personal de la organización considera que un problema que enfrentan es que no se está realizando una administración centralizada, haciendo de este un proceso desorganizado por lo que la propuesta de nuevo diseño debe considerar la implementación de esta característica.
- Por último, tenemos que el principal reto de la organización es mantener siempre la disponibilidad de sus aplicaciones y servicios, para satisfacer las necesidades de los usuarios. Esta característica está enfocada principalmente hacia los usuarios externos. La disponibilidad requerida para los usuarios que acceden desde el Internet es del 99.6%. La disponibilidad requerida para los usuarios de la red Interna y de las sucursales es del 98%.

Además, se revisa la documentación de la configuración de los equipos que están conectados a la red. El administrador de red provee un listado de todo equipo conectado a la red y el nombre del usuario asignado, anexo a continuación:

Tabla 6: Listado de usuarios de la Facultad.

| Departamento | Usuario |
|-----------------------------------------|----------------------------|
| Sistemas | Firewall – Proxy |
| Sistemas | Carlos Velasco |
| Sistemas | Ing. Carlos Ruiz |
| Sistemas | Johanna Robalino |
| Sistemas | Pilar Espinoza |
| Sistemas | Maq. Virtual – Angélica |
| Sistemas | Maq. Virtual – Carlos |
| Sistemas | Angélica Tomalá |
| Sistemas | Maq. Estudiantes |
| Sistemas | Router Mikrotik |
| Secretaría – Historia | Miguel Lecaro |
| Dirección – Educ. Primaria | Ingrid Pineda |
| Dirección – Educ. Primaria | Mariana Guerra |
| Dirección – Educ. Primaria | Mercy Rodriguez |
| Dirección – Quibio | MSc. Azucena Rivera |
| Dirección – Filosofía y CP | MSc. Carlos Idrovo Copiano |
| Dirección – Filosofía y CP | Lcdo. Omar Valle |
| Secretaría – Filosofía y CP | Miguel Lecaro |
| Secretaría – Filosofía y CP | MSc. Alava Mieles |
| Secretaría – Nivel Medio | Ronny Sarmiento |
| Secretaría – Nivel Medio | MSc. Sarmiento |
| Secretaría – Nivel Medio | Leticia Mata |
| Secretaría – Quibio, Fima | Mireya Hernandez |
| Secretaría – Quibio, Fima | Rosaura Mayea |
| Secretaría – Quibio, Fima | Isabel Mancheno |
| Secretaría – Adm. Educativa | Danny Mendez |
| Secretaría – Adm. Educativa | Aracely Gonzalez |
| Secretaría – Párvulos Semipresencial | Johanna Moreta |
| Secretaría – Párvulos Semipresencial | Magno Nicola |
| Secretaría – Párvulos Semipresencial | Todos |
| Secretaría – Párvulos Semipresencial | Router (S.E.S.S.) |
| Secretaría – Primaria | Lina Monroy |
| Secretaría – Primaria | Carlos Loor |
| Secretaría – Primaria | Lina Monroy |
| Secretaría – Primaria | Xavier Villacres |
| Secretaría – Primaria | Jeovanny Villacis |
| Secretaría – Comercio Exterior | Katherine Morán |
| Secretaría – Comercio Exterior | Isis Valverde |
| Secretaría – Comercio Exterior | Docentes |
| Secretaría – Comercio Exterior | Diana Sanchez |
| Secretaría – Comercio Exterior | Docente - Sandra Avilés |
| Dirección – Comercio Exterior | Router (Direccion) |

| Departamento | Usuario |
|-------------------------------|--------------------------|
| Dirección – Comercio Exterior | Elina Ullauri |
| Dirección – Comercio Exterior | MSc. Xavier Vivar |
| Dirección – Comercio Exterior | Docentes |
| Dirección – Comercio Exterior | Router (Sala_Docentes) |
| Archivo | Lcda. Concepcion Moreno |
| Archivo | Vilma Jordán |
| Secretaría – Lenguas | Olinda Triviño |
| Secretaría – Lenguas | Alexandra Delgado |
| Secretaría – Lenguas | Directora Pract. Docente |
| Secretaría – Lenguas | Router (Lenguas) |
| Secretaría – Lenguas | MSc. Larry Torres |
| Secretaría – Lenguas | Fabricio Conforme |
| Biblioteca | Directora Maria Jurado |
| Biblioteca | Todos |
| Biblioteca | Sara Zevallos |
| Biblioteca | Verónica Yagual |
| Biblioteca | Norma Calle |
| Biblioteca | Ana Ramia |
| Secretaría – Informática | Karina Orrala |
| Secretaría – Informática | Verónica Macias |
| Secretaría – Informática | Juan Carlos Calderón |
| Secretaría – Informática | Olver Jama |
| Secretaría – Informática | Carlos Pesantez |
| Secretaría – Informática | Secretarios Centros |
| Secretaría – Informática | Vannesa Cantos |
| Secretaría – Multimedia | Luis Reyes |
| Secretaría – Informática | Jessica Siguenca |
| Secretaría – Multimedia | Daniel Choez |
| Secretaría – Multimedia | Marlon Sotomayor |
| Secretaría – Multimedia | Jorge Baque |
| Secretaría – Multimedia | Nataly Ortega |
| Secretaría – Multimedia | Router (SALAMULTIMEDIA) |
| Director – Multimedia | MSc. Leopoldo Muñoz |
| Unidad Títulos | Donnys Alvarado |
| Unidad Títulos | Isaac Ruiz |
| Unidad Títulos | Todos |
| Unidad Títulos | Director UT |
| Presupuesto | Geovanny Lucio |
| Presupuesto | Emma Garcés |
| Presupuesto | Jessenia León |
| Presupuesto | Boris Bone |
| Presupuesto | Cristian Rodriguez |
| Presupuesto | Todos |
| Presupuesto | Tania Palma |
| Presupuesto | Ec. Jorge Rebolledo |
| Presupuesto | Liliana Suarez |
| Coord. General | Lcda. Elena Díaz |

| Departamento | Usuario |
|-----------------------------------|------------------------------|
| Coord. General | Aurelio Martinez |
| Coord. Académica | Norma Romero |
| Coord. Académica | MSc. Yanchapaxi |
| Coord. Académica | MSc. Amable Salazar |
| Economato | Diocelina Cedeño |
| Economato | Félix Lopez |
| Economato | Antonio Calderón |
| Economato | Eddy Merchán |
| Economato | Patricio Pancho |
| Talento Humano | Maria Tumbaco |
| Talento Humano | Tatiana Bohorquez |
| Talento Humano | Silvia Castillo |
| Talento Humano | Gina Bustamante |
| Talento Humano | Jorge Baque |
| Acreditación | Margarita Naranjo |
| Acreditación | Catalina Rodriguez |
| Acreditación | MSc. Fernando Silva |
| Acreditación | MSc. Lilian Reza |
| Acreditación | Miguel Chila |
| Acreditación | Guiliana Román |
| Acreditación | MSc. Pedro Rizzo |
| Secretaría – Bibliotecología | Dpl. Shirley Bueno |
| Secretaría – Literatura y Español | Johanna Choez |
| Seguimiento a Graduados | Norma Castelo |
| Desarrollo Comunitario | Karen Rizzo |
| Seguimiento a Graduados | Aida Torres |
| Devoluciones | Javier Matute |
| Secretaría – Mercadotecnia | Alba Macias |
| Secretaría – Mercadotecnia | Elizabeth Avilés |
| Secretaría – Mercadotecnia | Johanna Guerra |
| Sala Docentes - Comercio Exterior | Router (Sala_Comercio) |
| Vinculación | Router (Vinculación) |
| Senescyt | Router |
| Talento Humano | Directora |
| Talento Humano | Router |
| Economato | Eduardo Zúñiga |
| Coordinación Académico | MSc. Jackelyn Astudillo |
| Laboratorio # 2 | Matriculas |
| Laboratorio # 2 | Matriculas |
| Coordinación de extensiones | Msc. Maria del Carmen Rivera |
| Coordinación de extensiones | Ingrid Pineda |
| Coordinación de extensiones | Mercy Rodriguez |
| Coordinación de extensiones | Carlos Pesantez |
| Coordinación de extensiones | MSc. Denia Ochoa |
| Coordinación de extensiones | MSc. Denia Ochoa |

| Departamento | Usuario |
|-----------------------------------|--------------------------|
| Coordinación de extensiones | Kelly Hernandez |
| Practicas Docentes | MSc. Geoconda Castro |
| Practicas Docentes | Jessica Siguienza |
| Sala docente - Comercio Exterior | Docente |
| Sala docente - Comercio Exterior | Docente |
| Sala docente - Comercio Exterior | Docente |
| Sala docente - Comercio Exterior | Docente |
| Sala docente - Comercio Exterior | Docente |
| Virtual | Router (#yosoyfilosofia) |
| Secretaría – Literatura y Español | Router (Literatura) |
| Bibliotecología | Sala Profesores |
| Bibliotecología | Sala de Talleres |

Fuente: Departamento de sistemas.

Elaborado por: Los Autores.

La Facultad de Filosofía en su sede central cuenta con diferentes departamentos administrativos, cada departamento con el respectivo jefe de área. Los directores y subdirectores, por las funciones que realizan y por dirección del Director del departamento de sistemas, pertenecerán a una unidad organizativa diferente a las de secretarías. La lista de los directores y subdirectores se anexa a continuación:

Tabla 7: Listado de Directores.

| Docentes de la Facultad | Cargo | Departamentos/ carreras presencial y semipresencial |
|--------------------------------|--------------------|------------------------------------------------------------|
| Msc. Silvia Moy-Sang Castro | Decana | Decanato |
| Msc. José Zambrano García | Vice decano | Vice-decanato |
| Ab. Sebastián Cadena Alvarado | Secretario General | Secretaría General |
| Msc. Amable Salazar Sánchez | Director | Coordinación académica |
| Msc. Nelly Yanchapanxi Sánchez | Sub-Directora | Coordinación académica |
| Ing. Hugo Alcívar Dominguez | Director | Unidad de presupuesto |

| Docentes de la Facultad | Cargo | Departamentos/ carreras presencial y semipresencial |
|--------------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C.p.a. Liliana Suárez Menéndez | Subdirectora | Unidad de presupuesto |
| Ab. Alexy Meza Solís | Jefa | Unidad de talento humano |
| Msc. William Chenche García | | Fiscal de la Facultad |
| Ab. Vicente Villón Barros | | Fiscal Suplente de la Facultad |
| Msc. Walter Menéndez Chávez | Director | Dpto. de Planificación |
| Msc. Wilson Romero Dávila | Director | Unidad de Post-grado |
| Msc. Jhon Granados Romero. | Director | Acreditación y Evaluación |
| Lcdo. Patricio Pancho Orellana | Director | Administración de la Facultad |
| Sr. Jorge Ruiz Aguilera | | Ayudante del Administrador en el Complejo de la Facultad |
| Ing. Carlos Villegas Barros | | Administrador en el Complejo de la Facultad |
| Lcda. María Jurado de Zevallos | Directora | Biblioteca de la Facultad |
| Dra. Yoconda Castro Tehanga | Directora | Prácticas Docentes |
| Msc. Domingo Tapia Avilés | Director | Vinculación con la Comunidad |
| MSc. Sofía | Subdirector | Educadores de Párvulos (Semipresencial) Educación Primaria (Subcoordinador de Extensiones) Prácticas Preprofesionales (Semipresencial) excepto Comercio Exterior, Lenguas y Mercadotecnia |
| Msc. Carlos Barros Bastidas | Gestor-director | Investigación |
| Msc. Carlos Aveiga Paini | Director | Informática – Sistema Multimedia (Presencial – Semipresencial) |
| Msc. Erika Llerena Choez | Subdirectora | Informática – Sistema Multimedia (Presencial – Semipresencial) |
| Msc. Luis Benavides | Director | Aulas virtuales |
| Ph.d. Pedro Alcoser Aparicio | Director | Arte |
| Msc. Matilde Barros Morales | Director | Educación Básica |

| Docentes de la Facultad | Cargo | Departamentos/ carreras presencial y semipresencial |
|-----------------------------------|-------------------------------|------------------------------------------------------------|
| Msc. Carlos Echeverría | Subdirector | Educación Básica |
| Msc. Ruth Carvajal Martínez | Directora | Escuela de Bibliotecología y Archivología |
| Dra. Blanca Bermeo de Rivas, MSc. | Directora | Educadores de Párvulos |
| Msc. Jacqueline Aviles Salazar | Subdirectora | Educadores de Párvulos |
| Msc. Jacinto Calderón Vallejo | Director | Escuela de Lenguas y Lingüística |
| Msc. Alfonso Sánchez Avila | Subdirector | Escuela de Lenguas y Lingüística |
| Msc. Larry Torres Vivar | Subdirector | Escuela de lenguas y lingüística (semipresencial) |
| Msc. Pilar Huayamave Navarrete | Directora | Mercadotecnia y Publicidad |
| Msc. Olga Bravo Santos | Subdirectora (Semipresencial) | Mercadotecnia y Publicidad (Presencial y Semipresencial) |
| Msc. Xavier Vivar Vélez | Director | Comercio Exterior (Presencial – Semipresencial) |
| Msc. Karina Moeses | Subdirectora | Comercio Exterior (Presencial – Semipresencial) |
| Dr. Rubén Sarmiento Chuqui | Subdirector | Comercio y Administración (Presencial – Semipresencial) |
| Msc. Jessica Guevara | Directora | Química Biológicas – Desarrollo Comunitario Ambiental |
| Msc. Jorge Encalada Noboa | Director | Fima (Presencial – Semipresencial) |
| | | |
| Msc. Oswaldo Pacheco Gil | Director | Literatura y Español (Presencial – Semipresencial) |
| Dr. Rubén Holguín Arias | Director | Historia y Geografía (Presencial – Semipresencial) |
| Msc. Wilson Flores Rodríguez | Subdirector | Historia y Geografía |
| Msc. Carlos Idrovo Coppiano | Director | Filosofía y Ciencias Psicosociales |

| Docentes de la Facultad | Cargo | Departamentos/ carreras presencial y semipresencial |
|--------------------------------|----------------------|------------------------------------------------------------|
| Lic. Elena Díaz Maridueña | Coordinadora General | Semipresencial |
| MSc. Manuel Alencastro Oviedo | Director | Bienestar Estudiantil Facultad Filosofía |
| Msc. Luis Sanchez Robalino | Director | Nivelación y Admisión |
| Msc. Karina Córdova Tamayo | Directora | Unidad Educativa Minerva |
| Ing. Carlos Ruiz Berna | Director | Dpto. De Sistemas Facultad Filosofía |
| Lic. Julia Mejía Alvarado | Directora | Seguimiento a Graduados |
| Msc. Jorge Arango González | Director | Unidad de Titulación |

Fuente: Departamento de Sistemas.

Elaborado por: Los Autores.

5.3. FASE III: Diseñar

La etapa de diseño se realiza con base en los requerimientos ya planteados por el personal de sistemas, buscando llegar a satisfacer las necesidades o problemas encontrados. Basado en la fase de planeación, se determina las características que se requieren de los servidores a implementar tanto de hardware y software para nuestro servidor Nagios y el directorio activo:

Requisitos de Hardware recomendados para Nagios

Tabla 8: Requisitos de Hardware recomendado para Nagios.

| Nodos Monitoreados / Hosts | Servicios Monitoreados | Espacio de Disco Duro | CPU Cores | RAM |
|-----------------------------------|-------------------------------|------------------------------|------------------|------------|
| 50 | 250 | 40 GB | 1 - 2 | 1 – 4 GB |
| 100 | 500 | 80 GB | 2 – 4 | 4 – 8 GB |
| > 500 | > 2500 | 120 GB | > 4 | > 8 GB |

Fuente: (Nagios, 2014)

Requisitos de Hardware recomendados para Active Directory

Tabla 9: Requisitos de Hardware recomendado para Active Directory.

| Requisito de hardware | Requisito mínimo | Requisito recomendado |
|-----------------------|---------------------------------|-----------------------|
| Velocidad de CPU | Procesador de 64 bits a 1,4 GHz | Cuatro núcleos, 2 GHz |
| RAM | 512 MB | 4 GB |
| Espacio en disco | 32 GB | 100 GB |

Fuente: (Microsoft, 2000)

Requisitos de software para Nagios

- Apache
- PHP
- Librería GD de Thomas Boutell

Para realizar una correcta estructura del Directorio activo y Nagios se estableció realizar los diseños basados en el diagrama de red. Además de los siguientes puntos:

- Diseño del dominio y bosque en el Active Directory 2012 R2.
- Diseño de topología en Nagios.

El nombre del dominio que se designó es: Filosofia.ug.edu.ec, este cuenta con 3 unidades organizativas: Secretarías, Directores y Sistemas que se podrán visualizar en el diseño. La unidad organizativa de secretarías comprende los usuarios de cada departamento con la función administrativa de secretaria/o. Se cuenta con 26 secretarías en la sede central. Otra unidad es el grupo de directores de cada departamento y para finalizar se cuenta con el departamento de sistemas.

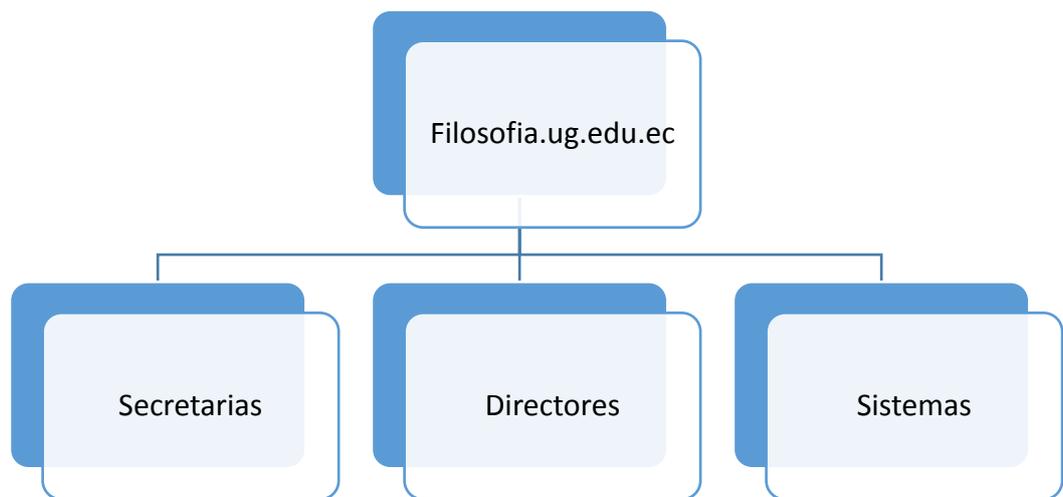


Figura 15: Diseño de Dominio filosofia.ug.edu.ec.

Fuente: Departamento de Sistemas.

Elaborado por: Los Autores.

Con lo planteado de las 3 unidades organizativas se realizó un listado de las políticas a implementar.

Para la unidad organizativa “directores” se aplicaría lo siguiente:

- Política de papel tapiz
- Política de eliminar el historial de exploración
 - Impedir que se elimine el historial de descarga
 - Impedir que se eliminen cookies
 - Impedir que se eliminen los datos de formularios
 - Impedir que se eliminen los sitios web que el usuario visito
- Política Panel de control
 - Prohibir el acceso a Configuración de PC y a Panel de control
- Política de Red/Conexiones de red
 - Capacidad para habilitar o deshabilitar una conexión LAN
 - Prohibir el acceso a las propiedades de componentes de una conexión LAN
 - Prohibir el acceso a las propiedades de una conexión LAN

- Prohibir el acceso al elemento Configuración avanzada en el menú “Opciones avanzadas”
- Prohibir la configuración TCP/IP avanzada

Para la unidad organizativa “Secretarías” se aplicaría las siguientes políticas:

- Política de papel tapiz
- Política de eliminar el historial de exploración
 - Impedir que se elimine el historial de descarga
 - Impedir que se eliminen cookies
 - Impedir que se eliminen los datos de formularios
 - Impedir que se eliminen los sitios web que el usuario visito
- Política Panel de control
 - Prohibir el acceso a Configuración de PC y a Panel de control
 - Ocultar la página “Programas y características”
- Política de Red/Conexiones de red
 - Capacidad para habilitar o deshabilitar una conexión LAN
 - Prohibir el acceso a las propiedades de componentes de una conexión LAN
 - Prohibir el acceso a las propiedades de una conexión LAN
 - Prohibir el acceso al elemento Configuración avanzada en el menú “Opciones avanzadas”
 - Prohibir la configuración TCP/IP avanzada
- Política de Acceso de almacenamiento extraíble
 - Discos extraíbles: denegar acceso de escritura
 - Discos extraíbles: denegar acceso de lectura
- Directivas de restricción de software/ Reglas adicionales
 - Reglas de hash para programas: psiphon-95 y u1304

Para la unidad organizativa “Sistemas” según lo acordado con el Ing. Carlos Ruiz, se optó por no aplicar reglas al departamento.

Al realizar el diseño de la topología de Nagios se incluye a los servidores que serán monitoreados, estos servidores son los que constan en el departamento de sistemas y

de los cuales se requiere un informe del estado de los servicios y del consumo del ancho de banda.

La Facultad de Filosofía está conectada directamente al centro de cómputo de la Universidad, la mayoría de los sistemas usados por los usuarios necesitan comunicarse con los servidores de centro de cómputo y a la vez este provee también de internet a la Facultad, por eso se hace necesario el conocer el estado del enlace con dicha área.

Los servidores mencionados serán detallados en el siguiente diagrama:

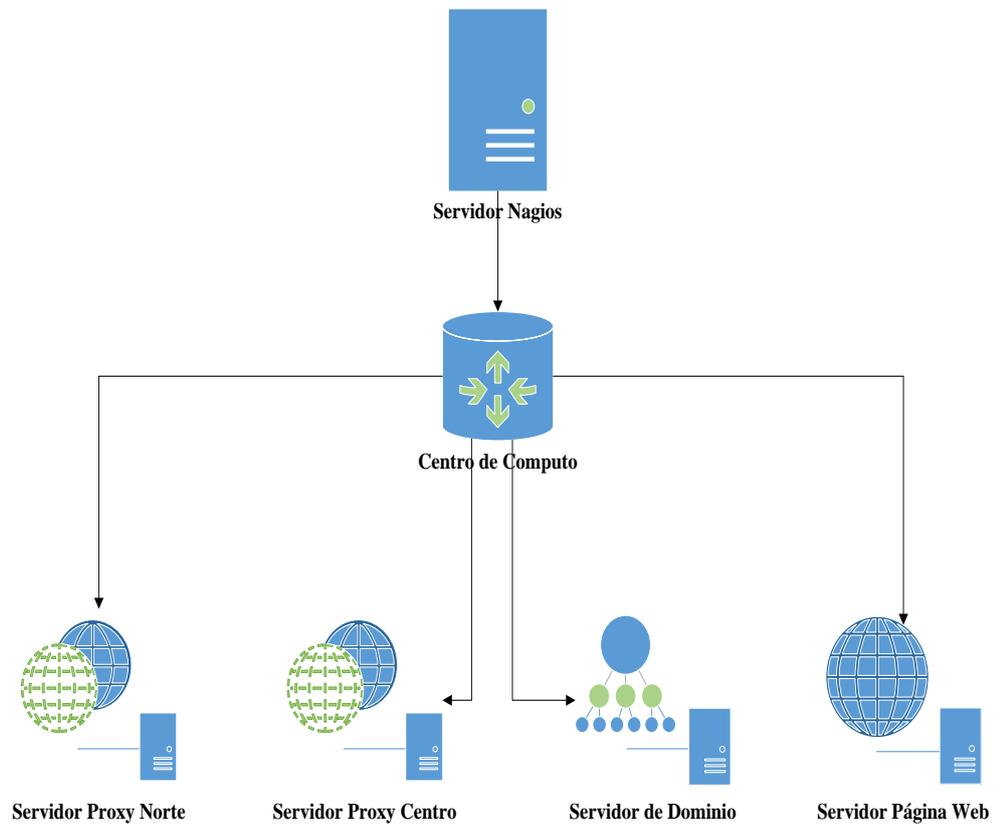


Figura 16: Diseño de diagrama de Nagios.

Fuente: Departamento de Sistemas.

Elaborado por: Los Autores.

5.4. FASE IV: Implementar

Se procede a realizar la integración del diseño propuesto, lo primero es la instalación de Nagios y del Directorio activo, posterior la configuración de cada servidor, y por último el ingreso de la información correspondiente a los enlaces de clientes y servidores a monitorear para Nagios, y para directorio activo el ingreso de los objetos de red, en este caso las máquinas de la Facultad, y los usuarios que pertenecen al dominio.

Al conocer la organización del personal se decidió realizar tres unidades organizativas: Directores, secretarias y departamento de sistemas. Cada unidad contara con políticas diferentes que se detallaron en la fase de diseño.

- Instalación y configuración del Active Directory 2012 R2.
Se encuentra detallado en el Anexo D: Instalación y configuración de Active Directory.
- Instalación y configuración de Nagios.
La instalación de Nagios Core se encuentra detallado en el Anexo A Instalación de Nagios Core y la configuración de Nagios se encuentra en el Anexo B Manual de configuración de Nagios.
- Pruebas de funcionamiento del Active Directory y Nagios.
Las pruebas del funcionamiento de los servidores corriendo eficazmente se muestran en el capítulo 6.
- Creación de Usuarios y grupos en el Active Directory.
Detallado en Anexo E.
- Creación de políticas de red.
Detallado en Anexo E en el ítem Creación de políticas de red
- Instalación de programa agente para monitoreo de red en los equipos (computadoras y servidores) de la facultad.
Detallado en Anexo G: Instalación de clientes para monitoreo
- Configuración de las computadoras para que puedan conectarse al controlador de dominio de Active Directory.

En la fase de implementación para la actividad de la configuración de las computadoras, las fechas a seguir fueron las siguientes:

Tabla 10: Cronograma de ingreso de las máquinas al dominio.

| Departamentos/ carreras presencial y semipresencial | Fecha | Actividad |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------------------------------------------|
| Química biológica – desarrollo comunitario ambiental | 03/06/2016 | Ingreso de máquinas al servidor de dominio |
| Historia y Geografía (presencial – semipresencial) | 03/06/2016 | Ingreso de máquinas al servidor de dominio |
| Filosofía y Ciencias Psicosociales | 03/06/2016 | Ingreso de máquinas al servidor de dominio |
| Historia y Geografía | 03/06/2016 | Ingreso de máquinas al servidor de dominio |
| Fima (presencial – semipresencial) | 03/06/2016 | Ingreso de máquinas al servidor de dominio |
| Literatura y Español (presencial – semipresencial) | 06/06/2016 | Ingreso de máquinas al servidor de dominio |
| Comercio y Administración (presencial – semipresencial) | 06/06/2016 | Ingreso de máquinas al servidor de dominio |
| Educadores de párvulos (semipresencial) | 07/06/2016 | Ingreso de máquinas al servidor de dominio |
| Educación Primaria (Subcoordinador de extensiones) prácticas pre profesionales (semipresencial) excepto Comercio Exterior, Lenguas y Mercadotecnia | - 10/06/2016 | |
| Comercio Exterior (presencial – semipresencial) | 13/06/2016 - | Ingreso de máquinas al servidor de dominio |
| Archivo | 14/06/2016 | |
| Archivo | 15/06/2016 | Ingreso de máquinas al servidor de dominio |
| Escuela de Lenguas y Lingüística | 15/06/2016 | Ingreso de máquinas al servidor de dominio |
| Escuela de Lenguas y Lingüística (semipresencial) | 16/06/2016 | Ingreso de máquinas al servidor de dominio |
| Biblioteca de la Facultad | 16/06/2016 - | Ingreso de máquinas al servidor de dominio |
| | 17/06/2016 | |
| Vinculación con la Comunidad | 20/06/2016 | Ingreso de máquinas al servidor de dominio |
| Prácticas docentes | 21/06/2016 | Ingreso de máquinas al servidor de dominio |

| Departamentos/ carreras presencial y semipresencial | Fecha | Actividad |
|----------------------------------------------------------------------|-------------------------------|--------------------------------------------|
| Bienestar estudiantil Facultad Filosofía | 21/06/2016 | Ingreso de máquinas al servidor de dominio |
| Escuela de Bibliotecología y Archivología | 21/06/2016 | Ingreso de máquinas al servidor de dominio |
| Arte | 22/06/2016 | Ingreso de máquinas al servidor de dominio |
| Aulas virtuales | 22/06/2016 | Ingreso de máquinas al servidor de dominio |
| Mercadotecnia y Publicidad (presencial y semipresencial) | 23/06/2016 - 24/06/2016 | Ingreso de máquinas al servidor de dominio |
| Investigación | 27/06/2016 - 29/06/2016 | Ingreso de máquinas al servidor de dominio |
| Unidad de Talento Humano | 04/07/2016 - 06/07/2016 | Ingreso de máquinas al servidor de dominio |
| Unidad de Presupuesto | 14/07/2016 | Ingreso de máquinas al servidor de dominio |
| Unidad de Titulación | 15/07/2016 - 20/07/2016 | Ingreso de máquinas al servidor de dominio |
| Seguimiento a graduados | 21/07/2016 | Ingreso de máquinas al servidor de dominio |
| Economato | 22/07/2016 - 25/07/2016 | Ingreso de máquinas al servidor de dominio |
| Coordinación Académica | 26/07/2016 – 29/07/16 | Ingreso de máquinas al servidor de dominio |
| Coordinación General | 1/08/2016 – 15/08/2016 | Ingreso de máquinas al servidor de dominio |
| Informática – Sistema Multimedia (presencial – semipresencial) | 16/08/2016 - 31/08/2016 | Ingreso de máquinas al servidor de dominio |
| Acreditación y evaluación | 5/09/2016 – 16/09/2016 | Ingreso de máquinas al servidor de dominio |

Elaborado por: Los Autores.

Para las configuraciones de los agentes de monitoreo de redes en los servidores se procedió a realizar las actividades desde el 15 de junio del 2016 hasta el 15 de septiembre del 2016.

Los servidores a monitorear:

- Servidor de dominio.
- Servidor de la Página web de la Facultad.
- Servidor Proxy Ciudadela Norte.
- Servidor Proxy Ciudadela Central.

Una vez configurado el servidor de dominio y aplicado las políticas a las dos unidades organizativas Directores y secretarías se obtiene lo siguiente desde el administrador de directivas de grupo:

Árbol de filosofía.ug.edu.ec:

- Directores:

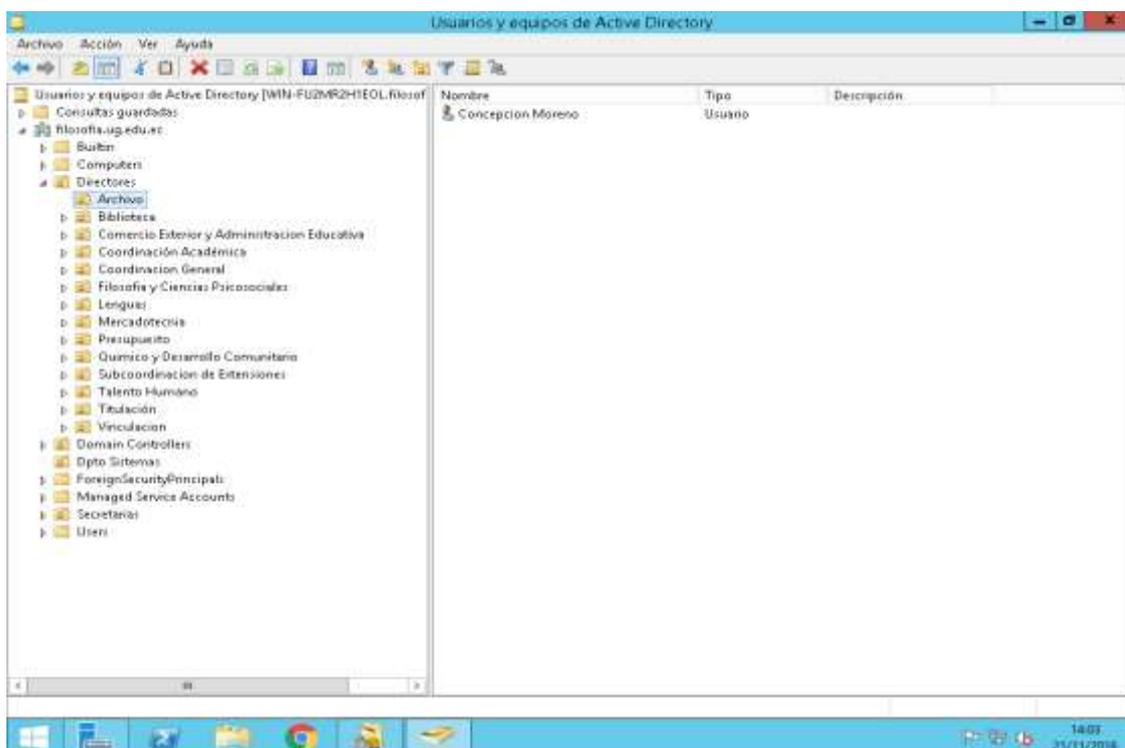


Figura 17: Árbol Directorio Activo.

Fuente: Directorio Activo.

- Secretarias

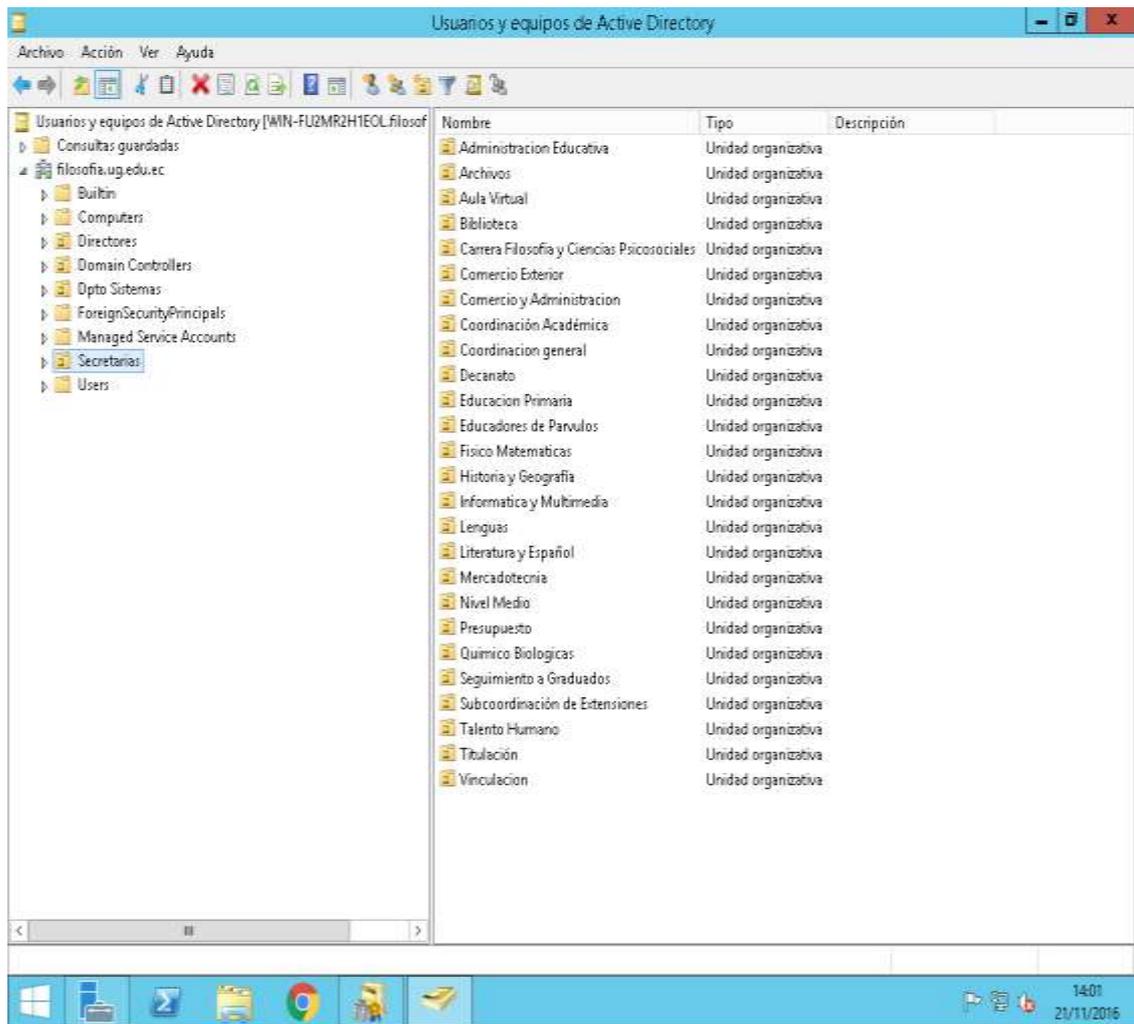


Figura 18: Árbol Directorio Activo.

Fuente: Directorio Activo

Políticas establecidas para la unidad de Directores:

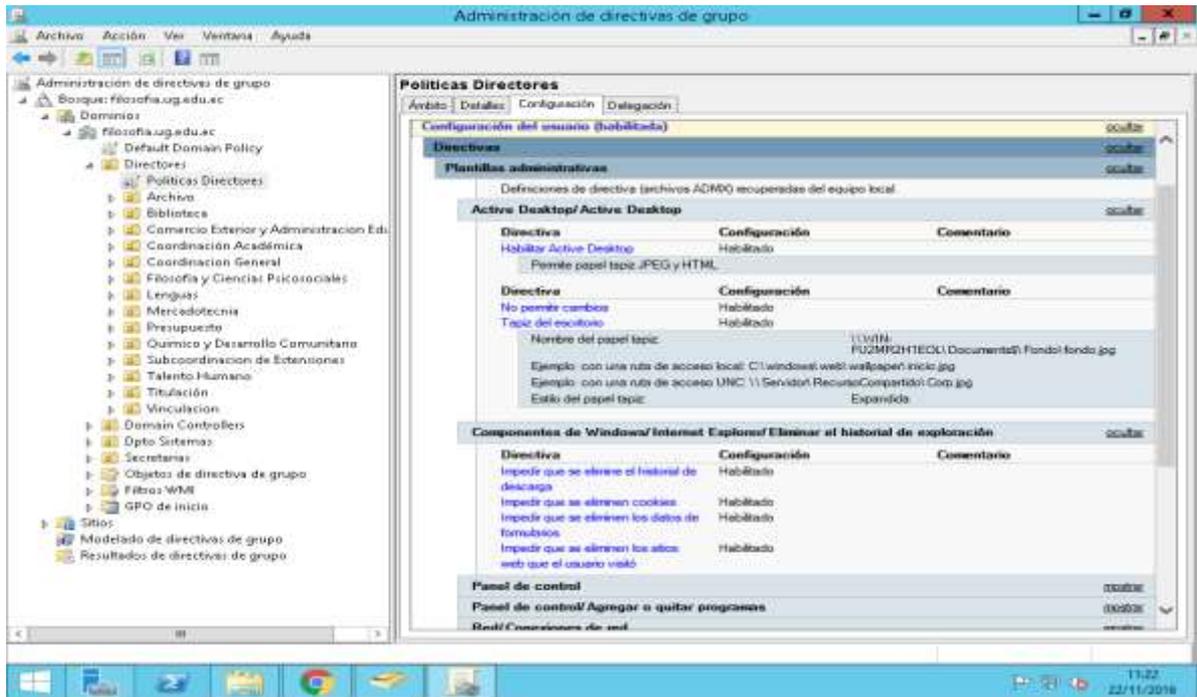


Figura 19: Políticas Directores.

Fuente: Directorio Activo

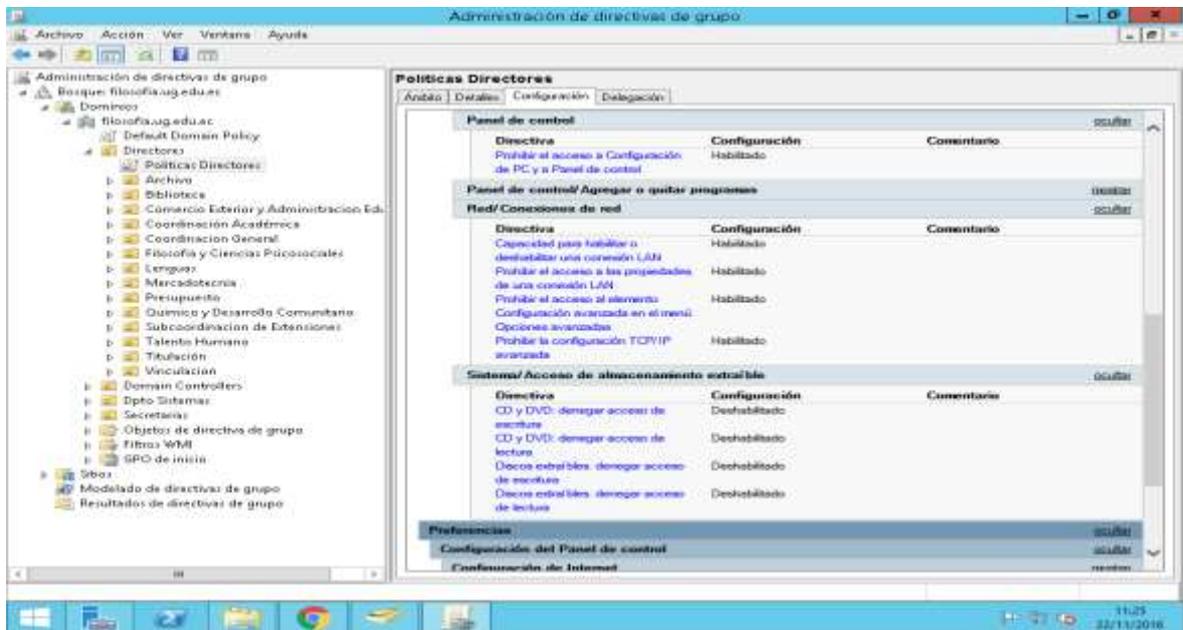


Figura 20: Políticas Directores.

Fuente: Directorio Activo

Para la unidad de Secretarías:

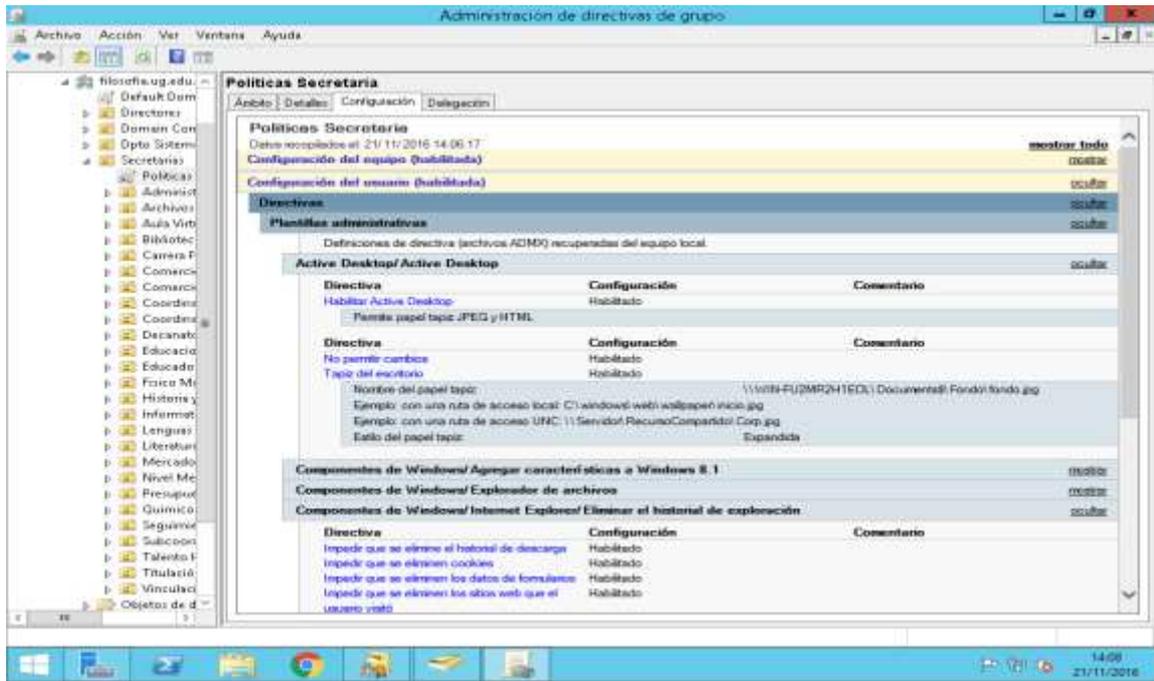


Figura 21: Políticas Secretarías.

Fuente: Directorio Activo

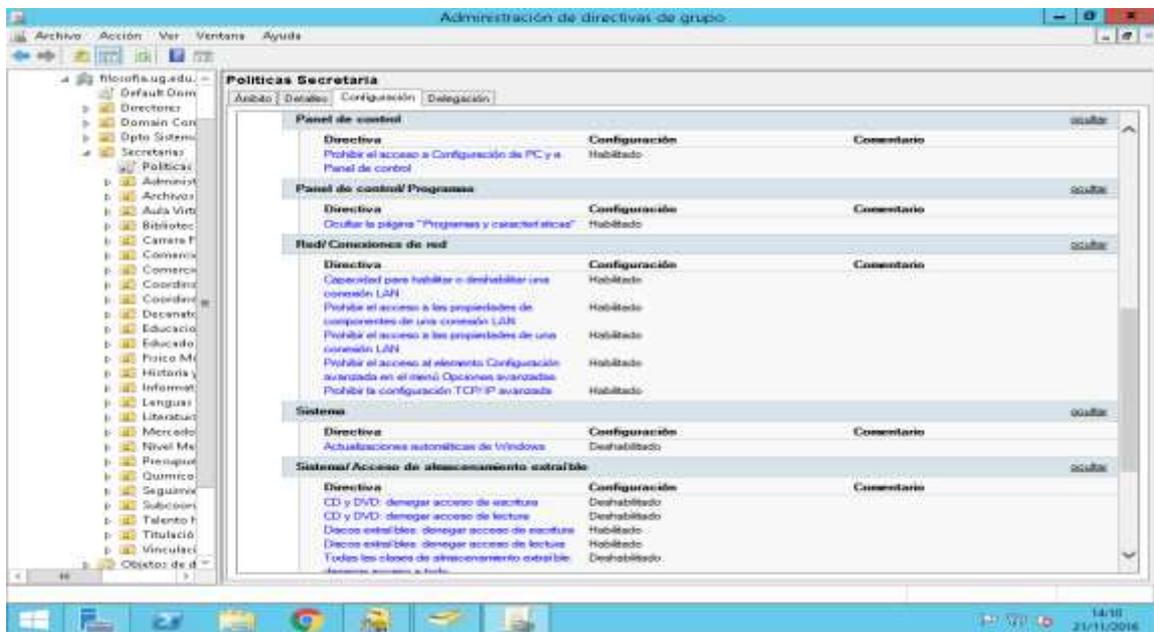


Figura 22: Políticas Secretarías.

Fuente: Directorio Activo.

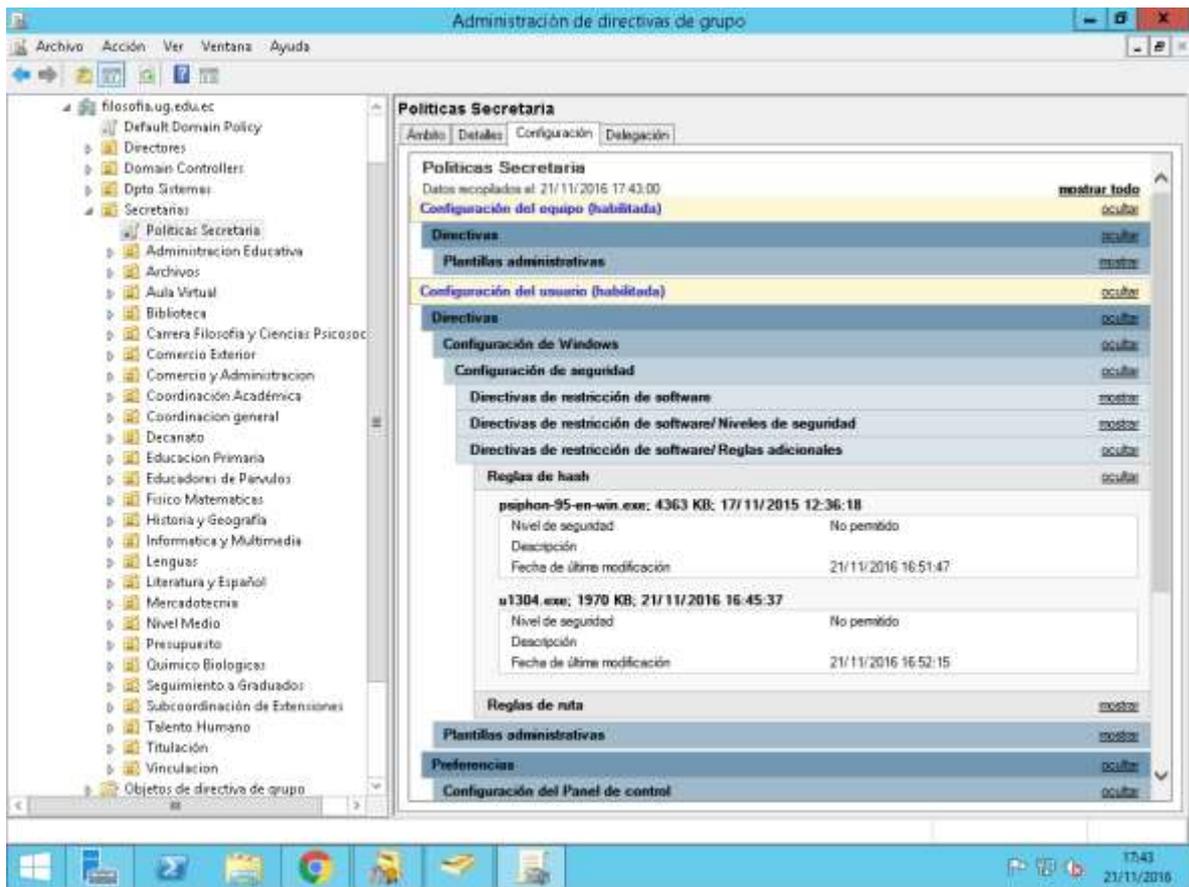


Figura 23: Políticas Secretarias.

Fuente: Directorio Activo.

5.5. FASE V: Operar

La fase de operación iniciará una vez se dé por concluida la implementación, durante esta fase todo agente de monitoreo realizará las alertas y cuadros estadísticos para conocer del funcionamiento. La función principal de este proyecto, es cumplir con cada una de las necesidades por el cual fue concebido, pero se obtendrá la capacidad de desarrollar las características que poseen las herramientas planteadas. Por parte de Nagios obtendremos un monitoreo constante y alarmas para cualquier percance y el directorio activo brindará las seguridades y confiabilidad a la red. En esta fase veremos puestos en acción a cada software, los agentes de monitoreo instalados corriendo normalmente y el uso de los usuarios designados a cada máquina y empleado de la Facultad.

6. Resultados

Como validación de la propuesta se utilizará un plan de pruebas para el correcto funcionamiento del sistema de monitoreo Nagios y del directorio activo, así como los procesos que se han determinado para una correcta puesta en marcha de las herramientas planteadas como solución. A continuación, se detallan las pruebas.

6.1. Pruebas y Métricas

6.1.1. Pruebas en Host Proxy Norte

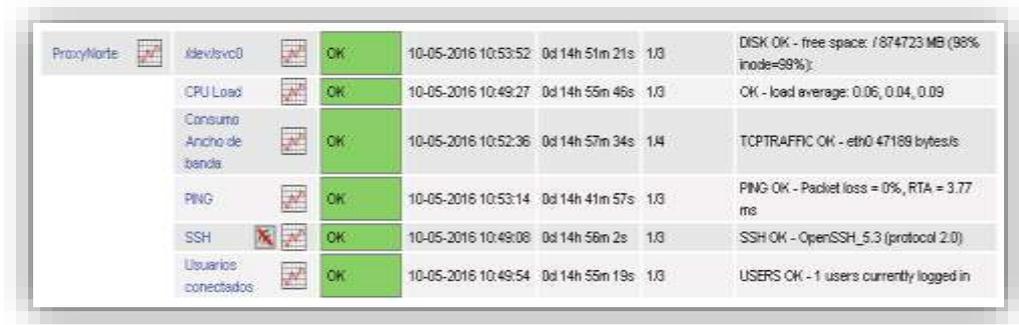


Figura 24: Monitoreo en Host del Proxy Norte

Fuente: Nagios

6.1.2. Monitoreo Disco Duro



Figura 25: Monitoreo Disco Duro

Fuente: Nagios

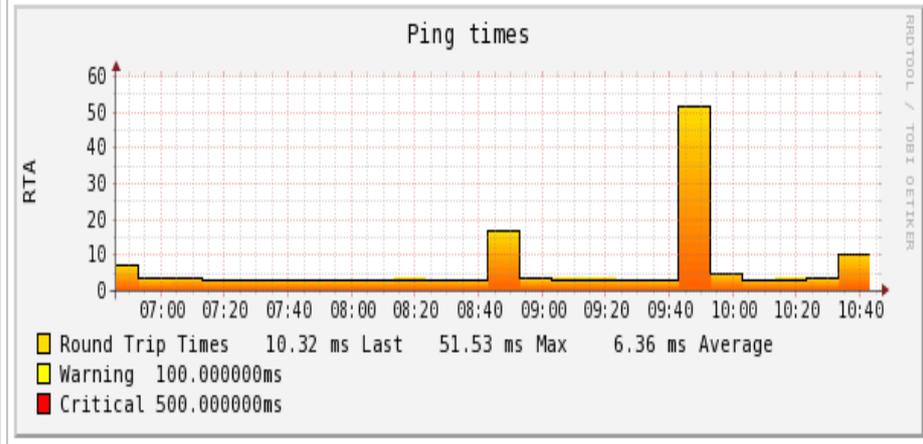
6.1.3. Monitoreo de Ping

Service details ProxyNorte -> PING

Host: ProxyNorte Service: PING

4 Hours 05.10.16 6:45 - 05.10.16 10:45

Datasource: Round Trip Times



Datasource: Packets Lost

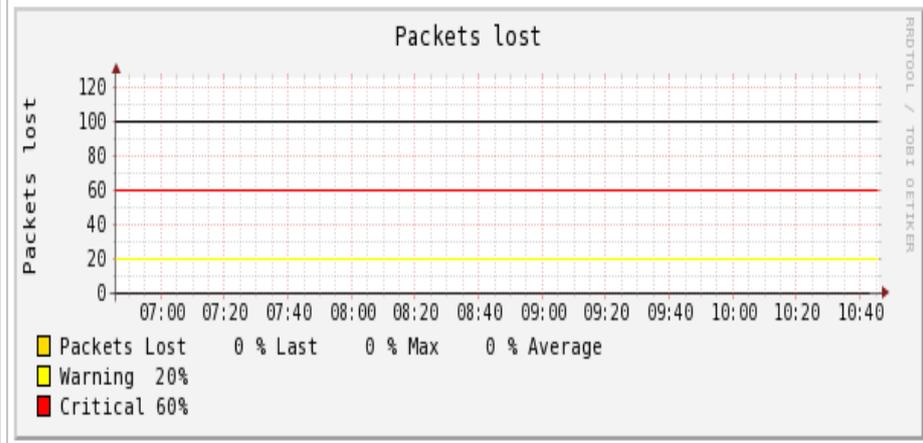


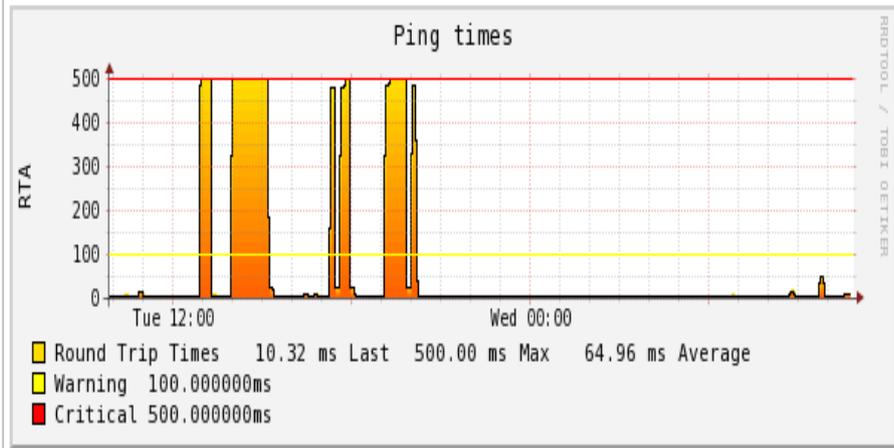
Figura 26: Monitoreo Ping

Fuente: Nagios

Host: ProxyNorte Service: PING

25 Hours 04.10.16 9:48 - 05.10.16 10:48

Datasource: Round Trip Times



Datasource: Packets Lost

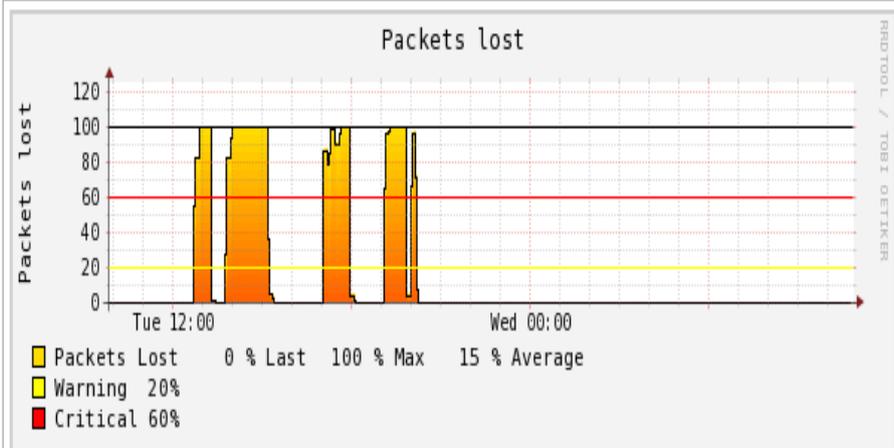


Figura 27: Monitoreo Ping

Fuente: Nagios

6.1.4. Monitoreo de carga del CPU

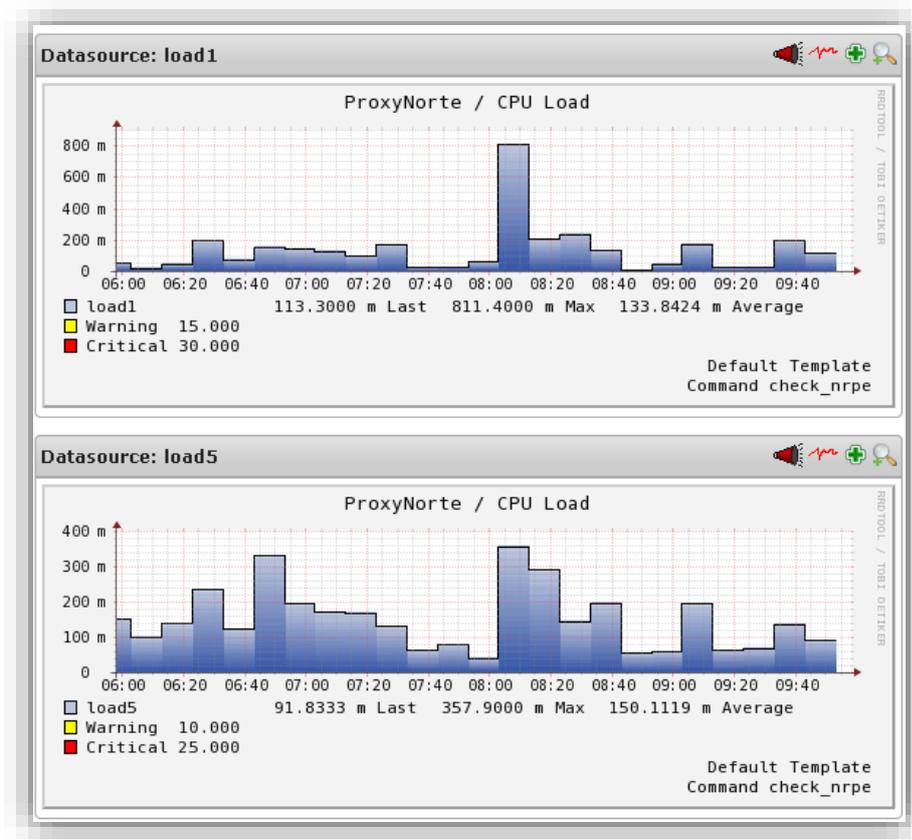


Figura 28: Monitoreo Carga de CPU.

Fuente: Nagios

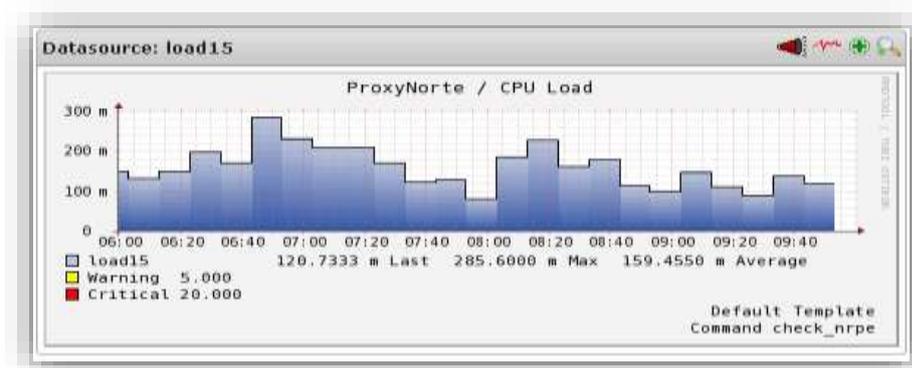


Figura 29: Monitoreo Carga de CPU.

Fuente: Nagios.

6.1.5. Monitoreo del servicio de SSH

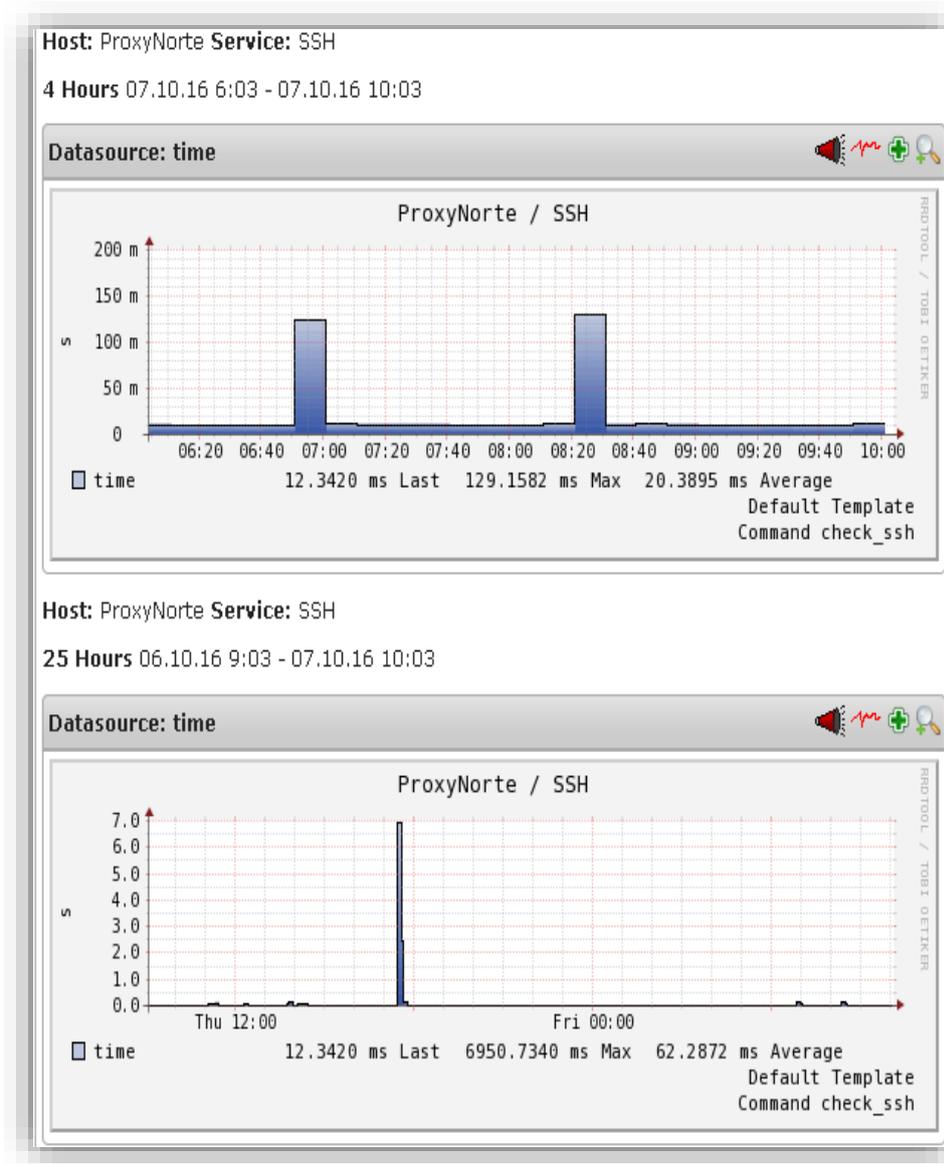


Figura 30: Monitoreo Servicio SSH.

Fuente: Nagios.

6.1.6. Monitoreo de usuarios conectados

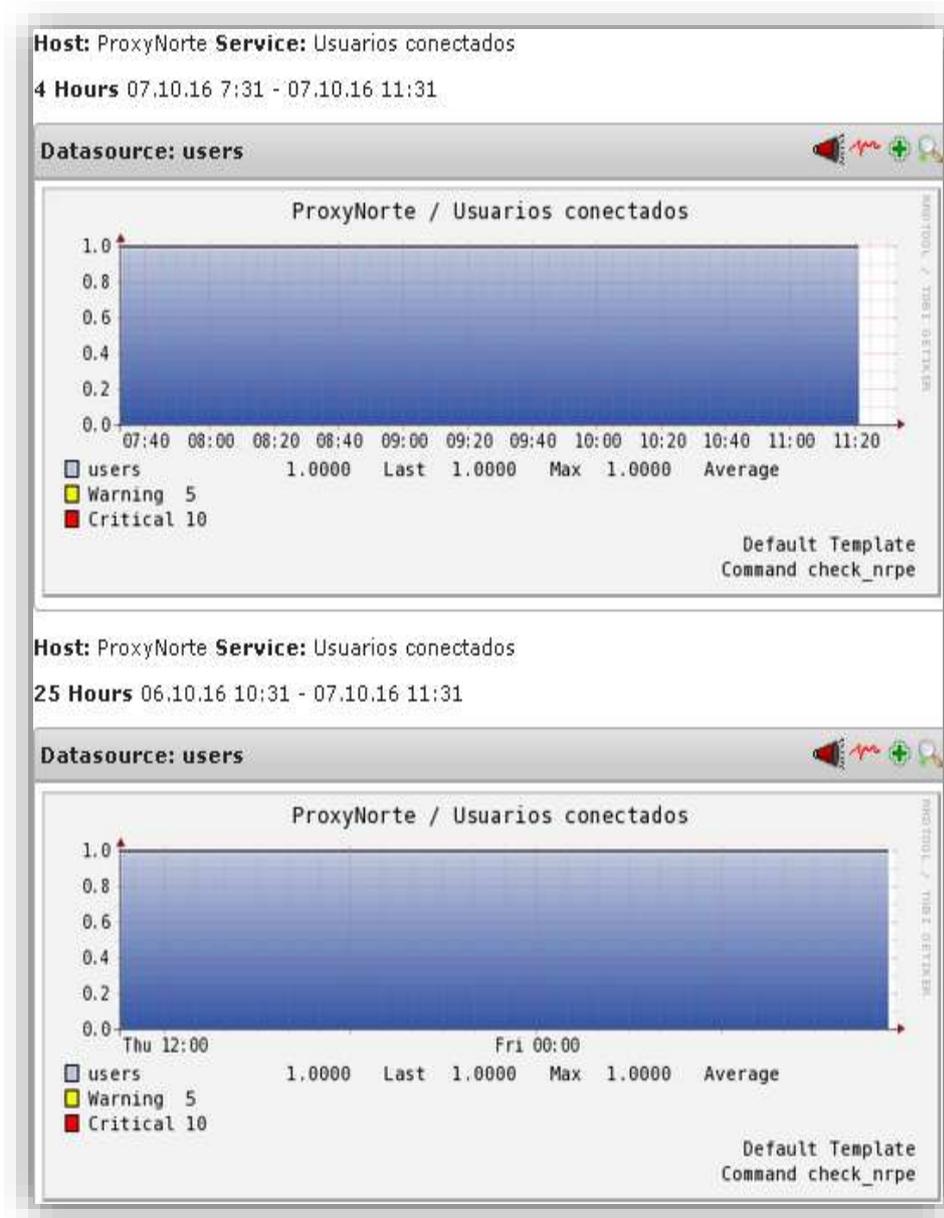


Figura 31: Cantidad Usuarios Conectados al Servidor.

Fuente: Nagios

6.1.7. Monitoreo de consumo de ancho de banda

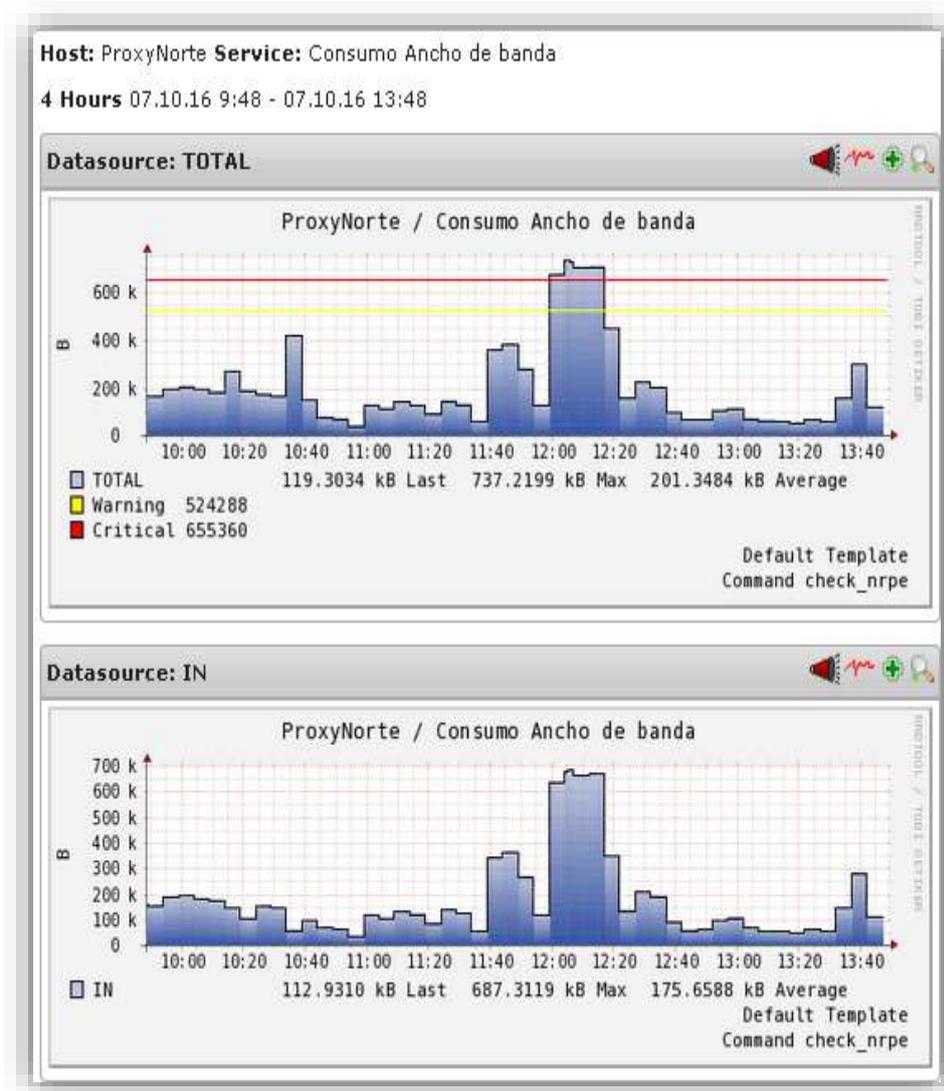


Figura 32: Monitoreo del Consumo del Ancho de Banda.

Fuente: Nagios

6.1.8. Cantidad de Host ingresados

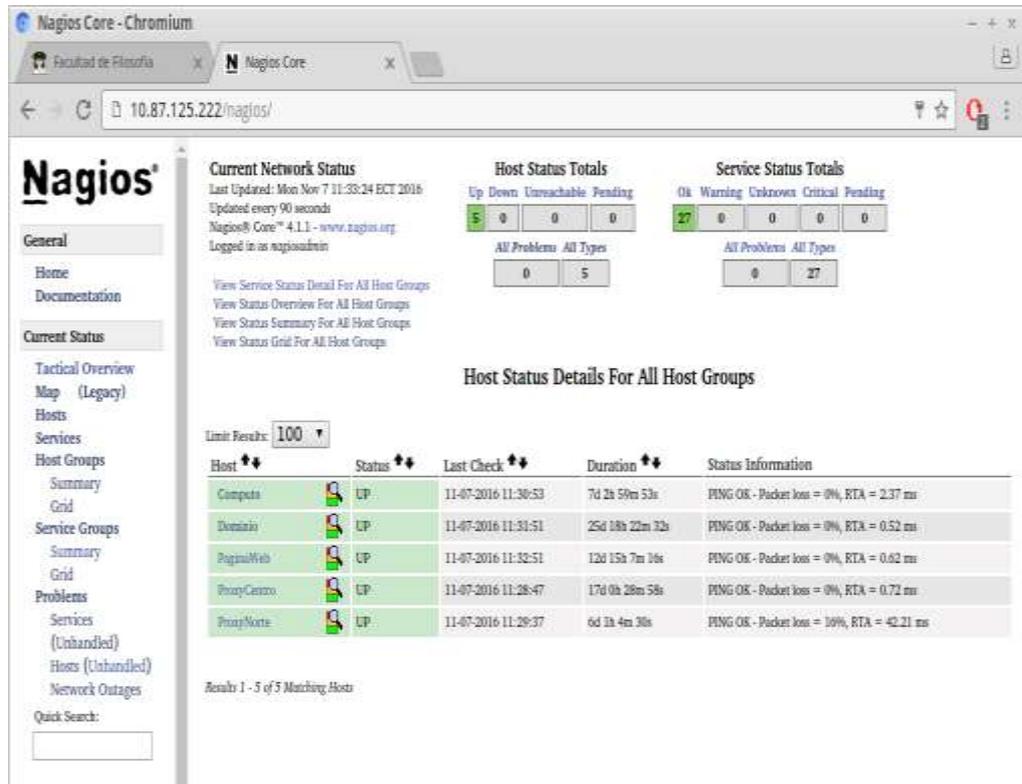


Figura 33 : Detalle de Estado de los Host

Fuente: Nagios

6.1.9. Mapa de Nagios

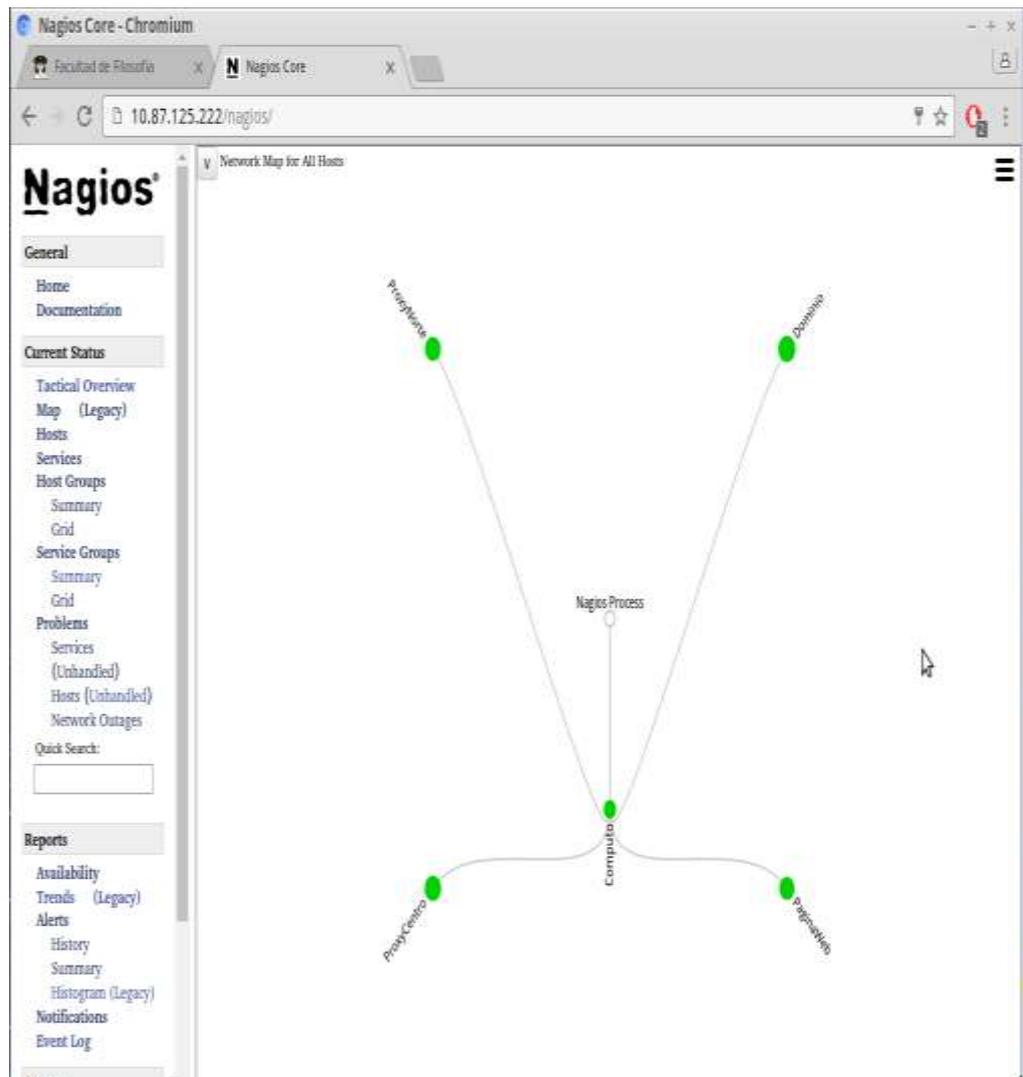


Figura 34: Mapa de Monitoreo de Nagios

Fuente: Nagios

6.1.10. Reporte de Nagios del Estado de todos los Host

Paso 1: Se escoge el tipo de reporte que se desea

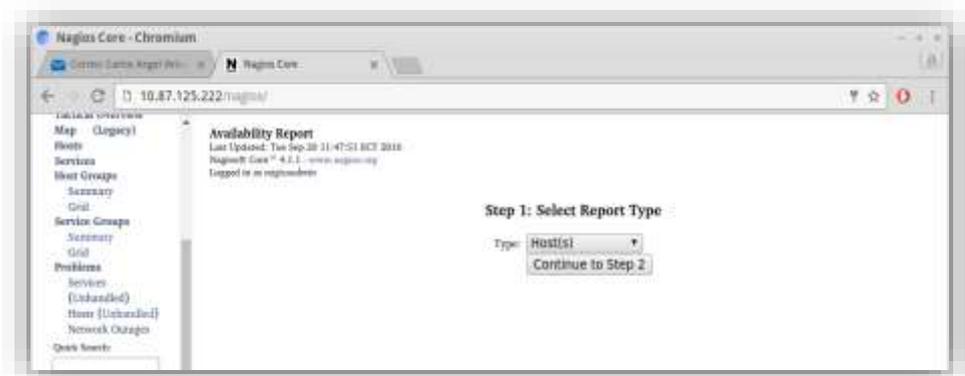


Figura 35: Paso 1 de Reporte

Fuente: Nagios

Paso 2: Se selecciona el Host del cual se desea el reporte



Figura 36: Paso 2 de Reporte

Fuente: Nagios

Paso 3: Se modifica según los requerimientos del reporte

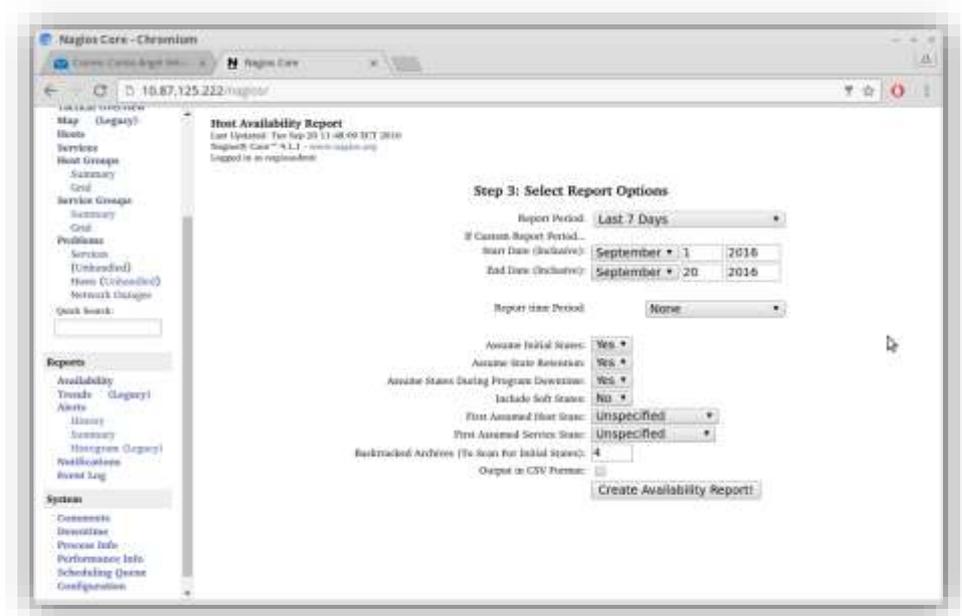


Figura 37: Paso 3 de Reporte

Fuente: Nagios

Paso 4: Se genera el reporte en el portal web

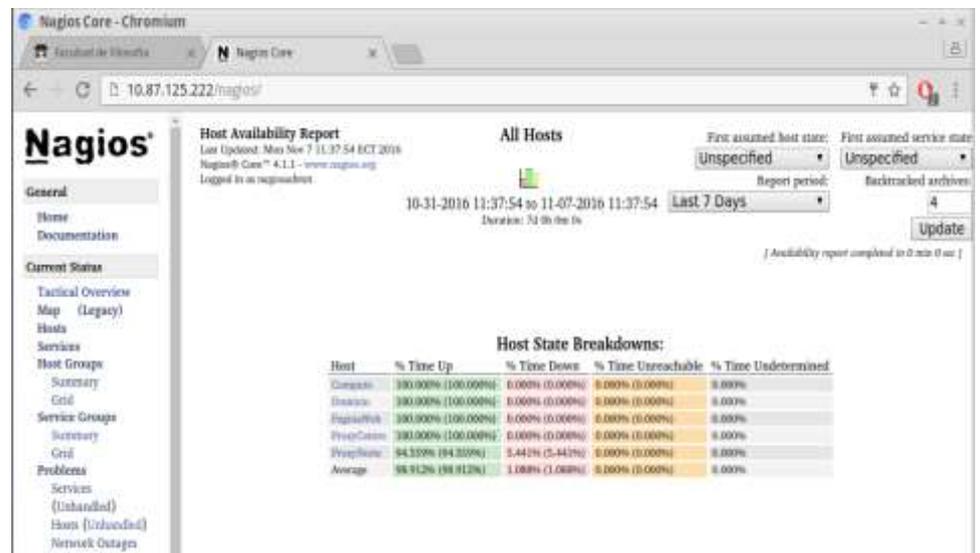


Figura 38: Generación de reporte

Fuente: Nagios

6.1.11. Reporte por porcentaje de Estado de los Host

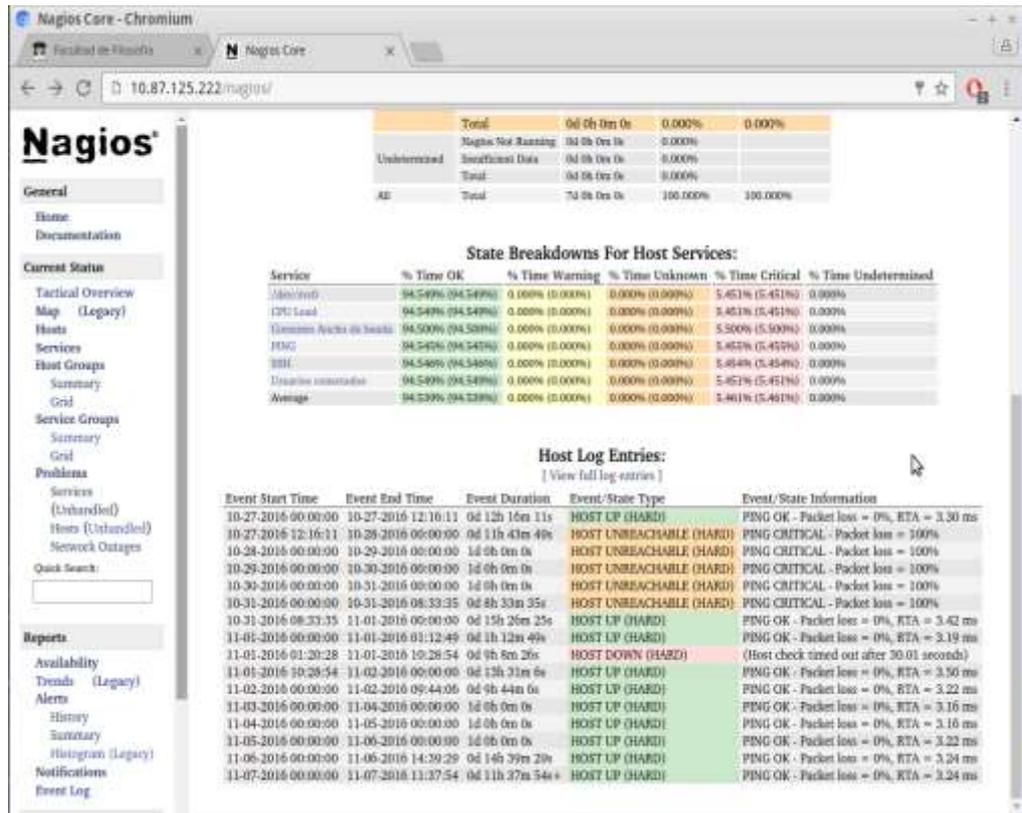


Figura 39: Generación de reporte por porcentaje de Estado de los Host

Fuente: Nagios

6.1.12. Reporte global de Estado del host.

The screenshot shows the Nagios Core web interface in a Chromium browser. The main content area displays a table of host events. The left sidebar contains navigation menus for 'Local Overview', 'Reports', and 'System'. The table columns are: Event Start Time, Event End Time, Event Duration, Event/State Type, and Event/State Information. The events are sorted chronologically from 09-09-2016 to 09-20-2016.

| Event Start Time | Event End Time | Event Duration | Event/State Type | Event/State Information |
|---------------------|---------------------|----------------|------------------|---------------------------------------------------|
| 09-09-2016 00:00:00 | 09-10-2016 00:00:00 | 1d 0h 0m 0s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.39 ms |
| 09-10-2016 00:00:00 | 09-11-2016 00:00:00 | 1d 0h 0m 0s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 4.20 ms |
| 09-11-2016 00:00:00 | 09-12-2016 00:00:00 | 1d 0h 0m 0s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.21 ms |
| 09-12-2016 00:00:00 | 09-12-2016 15:33:55 | 0d 15h 33m 55s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.41 ms |
| 09-12-2016 15:33:55 | 09-12-2016 15:49:51 | 0d 0h 15m 56s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-12-2016 15:49:51 | 09-12-2016 16:17:31 | 0d 0h 27m 40s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 14.28 ms |
| 09-12-2016 16:17:31 | 09-12-2016 16:59:25 | 0d 0h 41m 54s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-12-2016 16:59:25 | 09-12-2016 17:13:54 | 0d 0h 14m 29s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 42.81 ms |
| 09-12-2016 17:13:54 | 09-12-2016 17:43:32 | 0d 0h 29m 38s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-12-2016 17:43:32 | 09-13-2016 00:00:00 | 0d 0h 16m 28s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.01 ms |
| 09-13-2016 00:00:00 | 09-13-2016 12:27:31 | 0d 12h 27m 31s | HOST UP (HARD) | PING WARNING - Packet loss = 0%, RTA = 3509.48 ms |
| 09-13-2016 12:27:31 | 09-13-2016 12:53:15 | 0d 0h 25m 44s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-13-2016 12:53:15 | 09-13-2016 14:02:01 | 0d 1h 8m 46s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.14 ms |
| 09-13-2016 14:02:01 | 09-13-2016 14:53:25 | 0d 0h 51m 24s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-13-2016 14:53:25 | 09-13-2016 14:59:32 | 0d 0h 6m 7s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.25 ms |
| 09-13-2016 14:59:32 | 09-13-2016 15:16:30 | 0d 0h 16m 58s | HOST DOWN (HARD) | CRITICAL - Host Unreachable (10.87.127.1) |
| 09-13-2016 15:16:30 | 09-13-2016 16:01:24 | 0d 0h 44m 54s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 14.32 ms |
| 09-14-2016 00:00:00 | 09-14-2016 03:13:47 | 0d 3h 13m 47s | HOST UP (HARD) | PING OK - Packet loss = 72%, RTA = 3.22 ms |
| 09-14-2016 03:13:47 | 09-14-2016 03:22:27 | 0d 0h 8m 40s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-14-2016 03:22:27 | 09-14-2016 08:41:52 | 0d 5h 19m 25s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 2.96 ms |
| 09-14-2016 08:41:52 | 09-14-2016 09:03:55 | 0d 0h 22m 3s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-14-2016 09:03:55 | 09-14-2016 11:37:46 | 0d 2h 33m 51s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 185.73 ms |
| 09-14-2016 11:37:46 | 09-14-2016 12:33:32 | 0d 0h 55m 46s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-14-2016 12:33:32 | 09-14-2016 12:46:58 | 0d 0h 13m 26s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 992.07 ms |
| 09-14-2016 12:46:58 | 09-14-2016 14:49:43 | 0d 2h 2m 45s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-14-2016 14:49:43 | 09-14-2016 15:11:28 | 0d 0h 21m 45s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.25 ms |
| 09-14-2016 15:11:28 | 09-14-2016 15:39:22 | 0d 0h 27m 54s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-14-2016 15:39:22 | 09-14-2016 15:49:16 | 0d 0h 9m 54s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.37 ms |
| 09-14-2016 15:49:16 | 09-14-2016 15:51:52 | 0d 0h 2m 36s | HOST DOWN (HARD) | PING CRITICAL - Packet loss = 100% |
| 09-14-2016 15:51:52 | 09-15-2016 00:00:00 | 0d 8h 8m 8s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 32.83 ms |
| 09-15-2016 00:00:00 | 09-15-2016 09:09:12 | 0d 9h 9m 12s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.32 ms |
| 09-16-2016 00:00:00 | 09-17-2016 00:00:00 | 1d 0h 0m 0s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.35 ms |
| 09-17-2016 00:00:00 | 09-18-2016 00:00:00 | 1d 0h 0m 0s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.26 ms |
| 09-18-2016 00:00:00 | 09-19-2016 00:00:00 | 1d 0h 0m 0s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.19 ms |
| 09-19-2016 00:00:00 | 09-20-2016 00:00:00 | 1d 0h 0m 0s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.27 ms |
| 09-20-2016 00:00:00 | 09-20-2016 07:07:01 | 0d 7h 7m 1s | HOST UP (HARD) | PING OK - Packet loss = 0%, RTA = 3.14 ms |

Figura 40: Generación de reporte

Fuente: Nagios

6.1.14. Recepción de correos y alertas

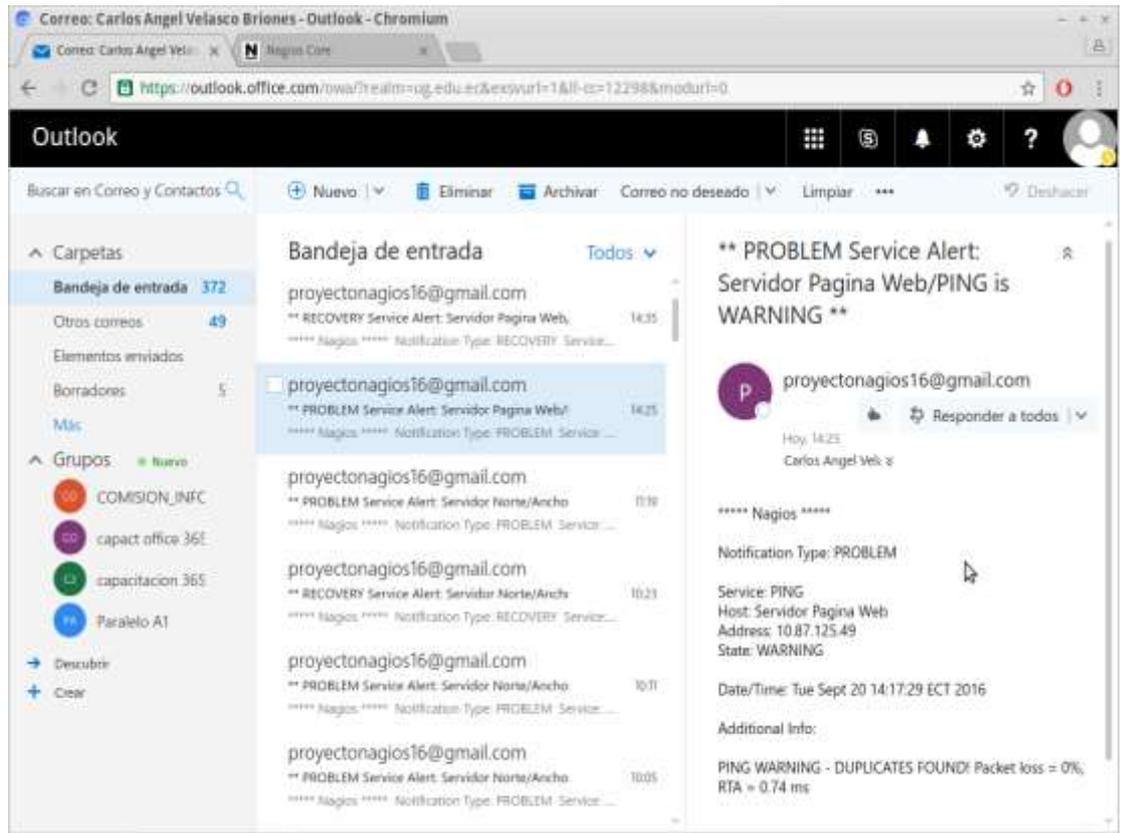


Figura 43: Recepción de correos y alertas.

Fuente: Nagios.

6.1.15. Máquinas ingresadas al dominio

Tabla 11: Total de Máquinas en el dominio.

| Campus | Edificio | Planta | Departamento | No. Pc | Dominio | Home | Sin Conexión | Usuarios mostraron impedimentos |
|--------|-------------------|--------|------------------------------------|--------|---------|------|--------------|---------------------------------|
| Centro | Dinace | PB | Vinculación | 3 | 2 | 1 | 0 | 0 |
| Centro | Dinace | PB | Literatura | 1 | 1 | 0 | 0 | 0 |
| Centro | Dinace | PB | Bibliotecología | 1 | 1 | 0 | 0 | 0 |
| Centro | Dinace | PB | Bienestar Estudiantil | 2 | 0 | 0 | 2 | 0 |
| Centro | Comercio Exterior | p1 | Archivo | 2 | 2 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Secretaria Comercio Exterior | 3 | 3 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Dirección Comercio Exterior | 3 | 3 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Sala Docentes Comercio Exterior | 6 | 6 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Nivel Medio Semipresencial | 2 | 2 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Filosofía y Ciencias Psicosociales | 2 | 1 | 0 | 0 | 1 |

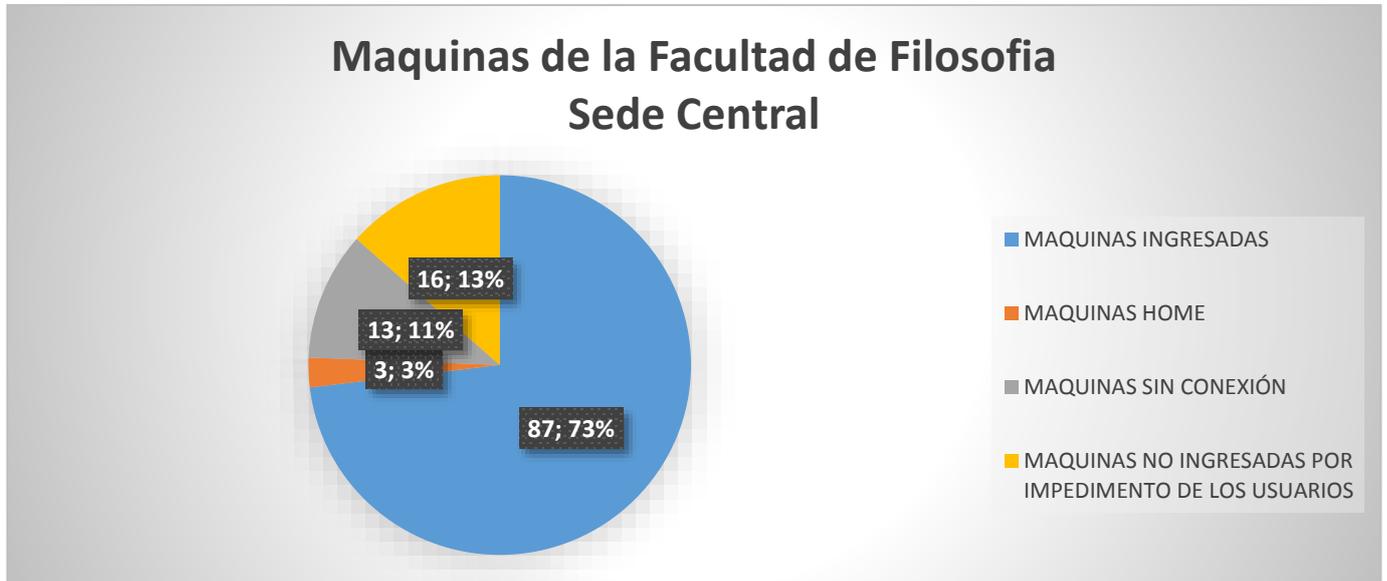
| Campus | Edificio | Planta | Departamento | No. Pc | Dominio | Home | Sin Conexión | Usuarios mostraron impedimentos |
|---------------|-------------------|---------------|-------------------------------|---------------|----------------|-------------|---------------------|----------------------------------------|
| Centro | Comercio Exterior | PB | Historia | 1 | 1 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Secretaría Químico Biológicas | 1 | 1 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Dirección Químico Biológicas | 1 | 0 | 0 | 1 | 0 |
| Centro | Comercio Exterior | PB | Físico Matemáticas | 1 | 1 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Comercio y Administración | 2 | 2 | 0 | 0 | 0 |
| Centro | Comercio Exterior | PB | Educación Primaria | 7 | 7 | 0 | 0 | 0 |
| Centro | Lenguas | PB | Secretaría Lenguas | 4 | 4 | 0 | 0 | 0 |
| Centro | Lenguas | p1 | Secretaría Biblioteca | 6 | 6 | 0 | 0 | 0 |
| Centro | Principal | PB | Seguimiento a Graduados | 2 | 2 | 0 | 0 | 0 |
| Centro | Principal | PB | Carrera de Arte | 1 | 0 | 0 | 1 | 0 |
| Centro | Principal | PB | Investigaciones | 5 | 0 | 0 | 5 | 0 |

| Campus | Edificio | Planta | Departamento | No. Pc | Dominio | Home | Sin Conexión | Usuarios mostraron impedimentos |
|---------------|-----------------|---------------|----------------------------|---------------|----------------|-------------|---------------------|----------------------------------------|
| Centro | Principal | PB | Mercadotecnia y Publicidad | 7 | 6 | 0 | 1 | 0 |
| Centro | Principal | PB | Extensiones | 8 | 6 | 0 | 2 | 0 |
| Centro | Principal | PB | Aula Virtual | 2 | 2 | 0 | 0 | 0 |
| Centro | Principal | p1 | Titulación | 4 | 0 | 0 | 0 | 4 |
| Centro | Principal | p1 | Informática y Multimedia | 10 | 10 | 0 | 0 | 0 |
| Centro | Principal | p1 | Economato | 4 | 0 | 0 | 0 | 4 |
| Centro | Principal | p1 | Presupuesto | 6 | 6 | 0 | 0 | 0 |
| Centro | Principal | p1 | Talento Humano | 6 | 6 | 0 | 0 | 0 |
| Centro | Principal | p1 | Coordinación Académica | 3 | 2 | 1 | 0 | 0 |
| Centro | Principal | p1 | Coordinación General | 2 | 2 | 0 | 0 | 0 |
| Centro | Principal | p2 | Evaluación y Acreditación | 7 | 0 | 0 | 0 | 7 |
| Centro | Dinace | p1 | Prácticas Docentes | 4 | 2 | 1 | 1 | 0 |
| TOTAL | | | | 119 | 87 | 3 | 13 | 16 |

Fuente: Los Autores.

Elaborado por: Los Autores.

Tabla 12: Cuadro Estadístico de las Máquinas ingresadas al dominio.



Fuente: Los Autores.

Elaborado por: Los Autores.

6.1.16. Aplicación de políticas a las unidades organizativas

Bloqueo Panel de control:



Figura 44: Bloqueo Panel de control.

Fuente: Los autores.

Bloqueo de aplicaciones:



Figura 45: Bloqueo Aplicaciones.

Fuente: Los autores.

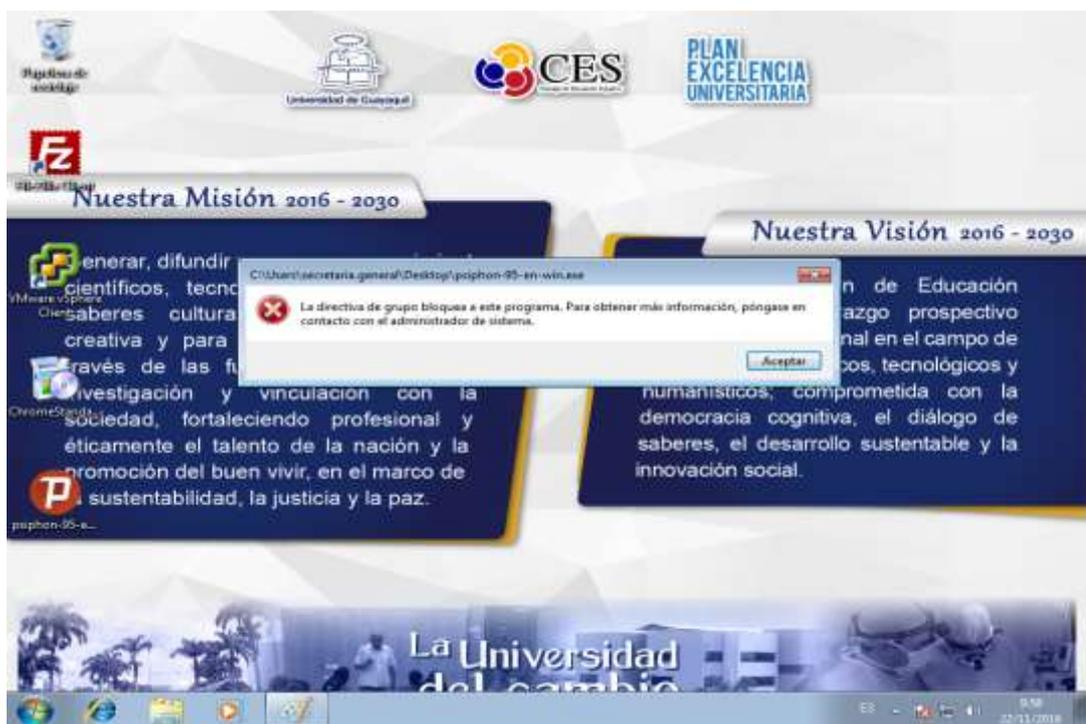


Figura 46: Bloqueo Aplicaciones.

Fuente: Los autores.

Aplicación Papel Tapiz:



Figura 47: Aplicación Papel Tapiz.

Fuente: Los Autores.

Bloqueo USB:

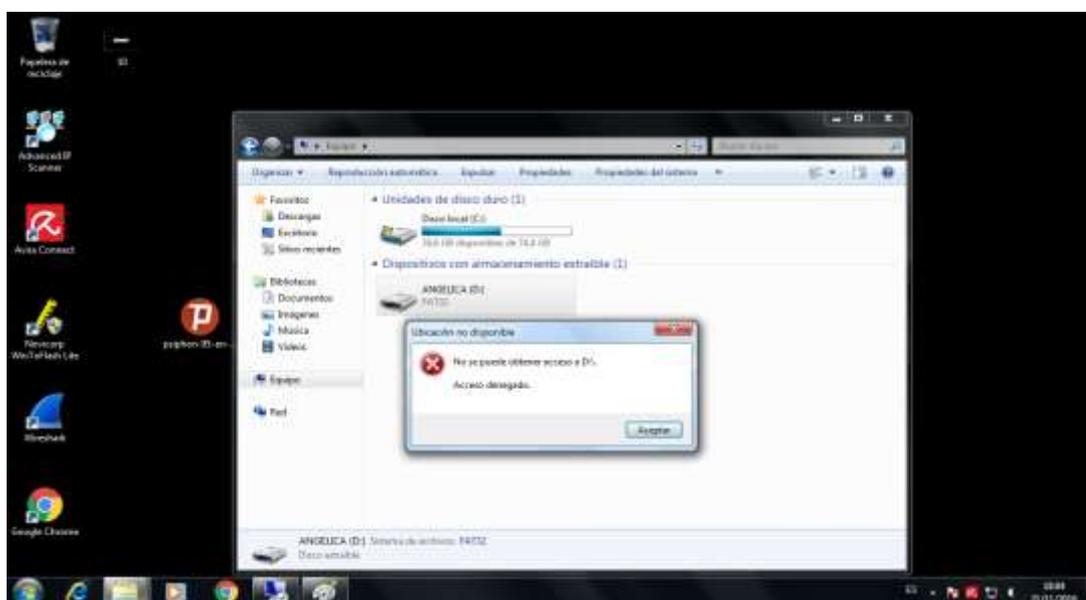


Figura 48: Bloqueo USB.

Fuente: Los Autores.

Bloqueo a recursos de red:

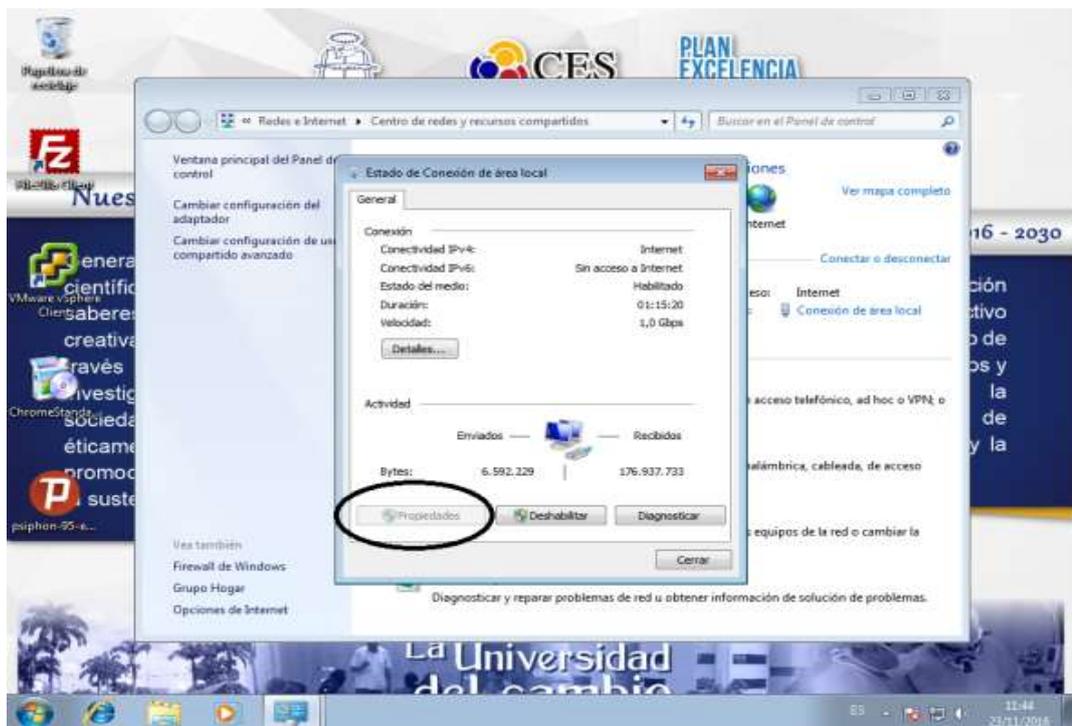


Figura 49: Bloqueo a recursos de red.

Fuente: Los Autores.

Inicio de Sesión solo en máquinas asignadas:



Figura 50: Bloqueo Inicio de Sesión.

Fuente: Los Autores.

7. Conclusiones

Con la implementación del directorio activo y de Nagios en la Facultad de Filosofía, Letras y Ciencias de la Educación se logró una mejor administración de los recursos de la red.

La instalación de Nagios permitirá monitorear los servidores, donde se obtendrán gráficas en intervalos de tiempo dando información del estado actual de cada servicio monitoreado (CPU, memoria, ping, procesador, usuarios conectados, ancho de banda).

La instalación de directorio activo permitirá tener un catálogo con todos los equipos, usuarios y dispositivos para la localización de estos y obtener información de cualquier dispositivo del dominio por medio de búsquedas rápidas.

Con la herramienta de monitoreo de redes, Nagios, se podrá identificar y prevenir errores mediante alarmas o gráficos por medio del portal web y optimizar recursos para dar soluciones rápidas a cualquier problema que se presente.

8. Recomendaciones

La Facultad de Filosofía, Letras y Ciencias de la Educación con la ayuda de la tecnología pone en ejecución un sistema de monitoreo de redes y la herramienta de directorio activo. Ya el personal encargado cuenta con la información y capacitación para la administración de las herramientas, pero esto no excluye de recomendaciones para el correcto uso, y aprovechar al máximo las características que poseen.

Dentro del servidor Nagios toda configuración se realiza por medio de archivos de texto, por lo que es recomendable que se realicen copias de seguridad de estos archivos. Los respaldos y los intervalos de tiempo con el cual se los haga, queda a consideración del administrador de red de la Facultad.

El administrador de red de la Facultad debe hacer revisiones constantes del estado de la memoria y almacenamiento de los servidores que contienen las herramientas de Nagios y directorio activo, de esta manera se podrá seguir añadiendo más host para monitoreo y si se requiere se realizarán las actualizaciones del software implementado.

En cuanto a la administración de la herramienta Nagios y el directorio activo, se recomienda la creación de usuarios para el acceso a la información que contienen los servidores.

9. Referencias Bibliográficas

- Barth, W. (2008). *Nagios, 2nd Edition: System and Network Monitoring*. Obtenido de https://books.google.com.ec/books?id=xFArj2MDYGwC&printsec=frontcover&source=gbbs_ge_summary_r&cad=0#v=onepage&q&f=false
- Budris, P. (2011). *Administrador de Redes Windows*. Buenos Aires: Fox Andina.
- Center, N. S. (2012). *Es la Red*. Obtenido de <http://www.eslared.org.ve/walc2012/material/track3/cacti-desde-paquetes.pdf>
- Cisco. (2008). *Cisco*. Obtenido de <http://www.cisco.com/cisco/web/docs/iam/unified/ipcc611/pdfs/01home.pdf>
- Griera, J. I. (2008). *Estructura de redes de computadores*. Barcelona: Editorial UOC.
- Microsoft. (18 de 10 de 2000). *Microsoft Windows 2000 Server*. Obtenido de <https://support.microsoft.com/es-ec/kb/196464>
- Molina Caballero, J., & Baena Espejo, L. M. (s.f.). *Sistemas Operativos en Entornos monousuario y multiusuario. Windows 2003 Server y Linux*. Madrid (España): Vision Net.
- Nagios. (Marzo de 2014). *nagios.com*. Obtenido de <https://assets.nagios.com/downloads/nagiosxi/docs/Nagios-XI-Hardware-Requirements.pdf>
- Oracle. (2010). *Oracle Corporation*. Obtenido de <https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r0r9/index.html>
- SolarWinds. (2010). *SolarWinds Network Configuration Manager*.
- Tanenbaum, A. (2003). *Redes de computadoras*. México: Perason Educación de México.
- Wayner, P. (2001). *La ofensiva del software libre*. Barcelona: Ediciones Granica.
- Zabbix. (2016). *Zabbix*. Obtenido de <http://www.zabbix.com/>

Anexos

10. Anexos

10.1. Anexo A

10.1.1. Manual de instalación de Nagios

Instalación de Nagios Core

Paso 1: Instalar Pre requisitos

Se debe instalar los programas que el Core necesita para funcionar

```
#yum install httpd php php-cli gcc glibc glibc-common gd  
gd-devel net-snmp openssl-devel wget unzip -y
```

Paso 2: Se crea el usuario y el grupo para usar en Nagios

```
#useradd nagios  
#groupadd nagcmd  
#usermod -a -G nagcmd nagios  
#usermod -a -G nagcmd apache
```

Paso 3: Descargar e instalar Nagios

```
#cd /tmp  
#wget  
https://assets.nagios.com/downloads/nagioscore/releases/n  
agios-4.1.1.tar.gz  
#wget http://www.nagios-plugins.org/download/nagios-  
plugins-2.1.1.tar.gz  
#tar xzf nagios-4.1.1.tar.gz  
#tar xzf nagios-plugins-2.1.1.tar.gz  
#cd nagios-4.1.1
```

Paso 4: Se deben extraer los archivos y compilar Nagios

```
#./configure --with-command-group=nagcmd
#make all
#make install
#make install-init
#make install-config
```

Paso 5: Crear una contraseña para nagiosadmin

```
#htpasswd -c /usr/local/nagios/etc/htpasswd.users
nagiosadmin
```

Paso 6: Instalar Plugins de Nagios

```
#cd /tmp/nagios-plugins-2.1.1
#./configure --with-nagios-user=nagios --with-nagios-
group=nagios --with-openssl
#make all
#make install
```

Paso 7: Levantar el servicio de Nagios

Levantar los servicios de Nagios y httpd; solo si todo funciona correctamente

```
#service httpd start
#service nagios start
```

Paso 8: Ingresamos a Nagios desde la interfaz web

Accedemos a la siguiente dirección <http://nagiosip/nagios> con el usuario nagiosadmin y su contraseña. Si esta todo correcto aparecerá la siguiente pantalla.



Figura 51: Portal Web Nagios.

Fuente: Nagios

10.2. Anexo B

10.2.1. Manual de configuración de Nagios

Configuración de Nagios

Paso 1: Ingreso de hosts a Nagios

Lo primero será crear una carpeta.

```
# mkdir /usr/local/nagios/etc/servers
```

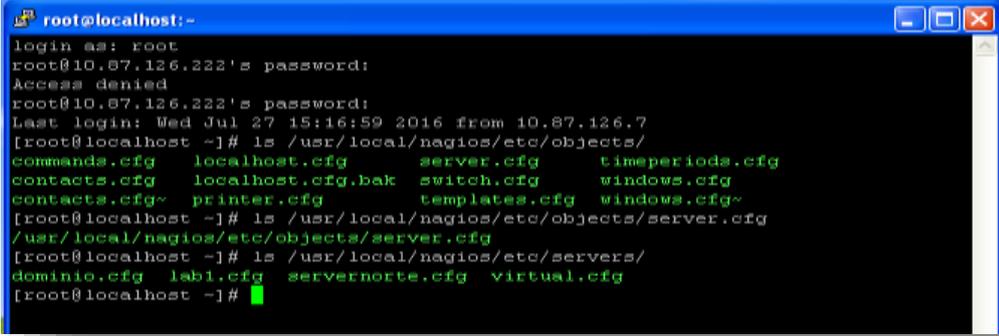
Ingresamos la carpeta al archivo de configuración.

```
/usr/local/nagios/etc/nagios.cfg  
cfg_dir=/usr/local/nagios/etc/servers
```

Accedemos a la carpeta creada e ingresamos los hosts que vamos a monitorear de la siguiente manera.

```
# cd /usr/local/nagios/etc/servers  
# touch servernorte.cfg
```

Servidores creados



```
root@localhost:~  
login as: root  
root@10.87.126.222's password:  
Access denied  
root@10.87.126.222's password:  
Last login: Wed Jul 27 15:16:59 2016 from 10.87.126.7  
[root@localhost ~]# ls /usr/local/nagios/etc/objects/  
commands.cfg  localhost.cfg  server.cfg  timeperiods.cfg  
contacts.cfg  localhost.cfg.bak  switch.cfg  windows.cfg  
contacts.cfg~  printer.cfg  templates.cfg  windows.cfg~  
[root@localhost ~]# ls /usr/local/nagios/etc/objects/server.cfg  
/usr/local/nagios/etc/objects/server.cfg  
[root@localhost ~]# ls /usr/local/nagios/etc/servers/  
dominio.cfg  lab1.cfg  servernorte.cfg  virtual.cfg  
[root@localhost ~]#
```

Figura 52: Servidores creados.

Fuente: Nagios

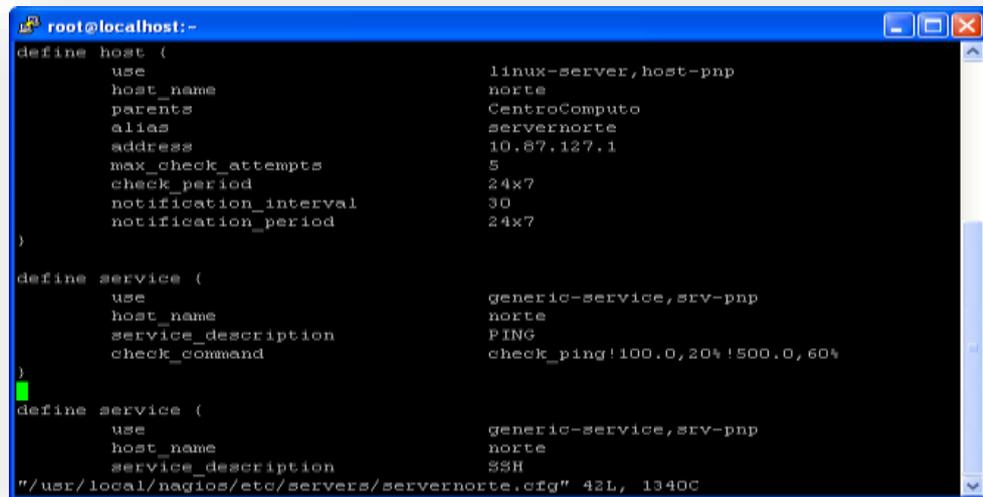
Paso 2: Escribimos la configuración del servidor

```
define host{
    use                linux-server
    host_name          norte
    alias              servernorte
    address            10.87.127.1
}
```

Paso 3: Añadimos sus servicios

```
define service{
    use                generic-service
    host_name          norte
    service_description PING

    check_command      check_ping!100.0,20%!500
                      .0,60%
}
```



The screenshot shows a terminal window titled "root@localhost:-" with a black background and white text. It displays the following Nagios configuration:

```
root@localhost:-
define host (
    use                linux-server,host-pnp
    host_name          norte
    parents            CentroComputo
    alias              servernorte
    address            10.87.127.1
    max_check_attempts 5
    check_period       24x7
    notification_interval 30
    notification_period 24x7
)

define service (
    use                generic-service,svr-pnp
    host_name          norte
    service_description PING
    check_command      check_ping!100.0,20%!500.0,60%
)

define service (
    use                generic-service,svr-pnp
    host_name          norte
    service_description SSH
)
"/usr/local/nagios/etc/servers/servernorte.cfg" 42L, 1340C
```

Figura 53: Servicios Agregados en Nagios.

Fuente: Nagios

10.3. Anexo C

10.3.1. Instalación de clientes para monitoreo

Para agregar los clientes al servidor existen 2 agentes para nagios: NSClient++ y el NRPE. El NSClient++ es para clientes con Sistema Operativo Windows y el NRPE para Sistemas Operativos Linux.

Instalación del NSClient++

Paso 1: Se descarga el cliente desde su página oficial, escogiendo la arquitectura de su servidor (32 o 64 bits).



Figura 54: Descarga NSClient++.

Fuente: Nagios

Paso 2: Descargado proseguimos con la instalación.



Figura 55: Configuración NSClient.

Fuente: Nagios

Paso 3: Damos siguiente y luego clic en aceptar los términos de la licencia.

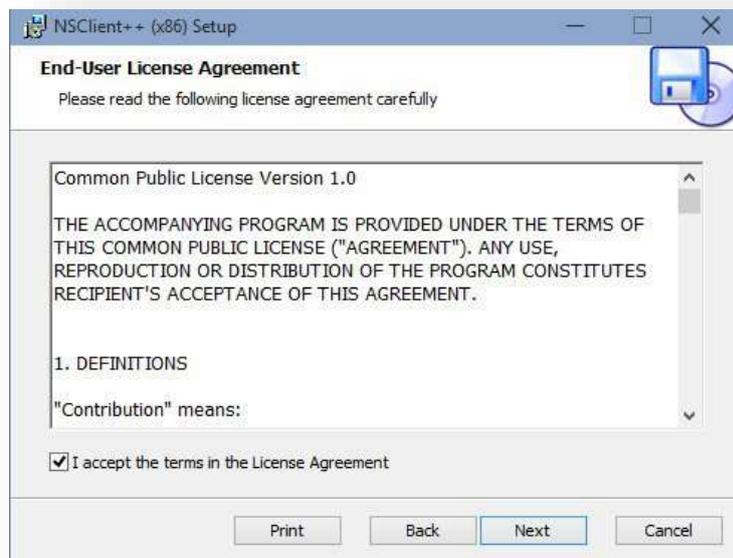


Figura 56: Configuración NSClient.

Fuente: Nagios.

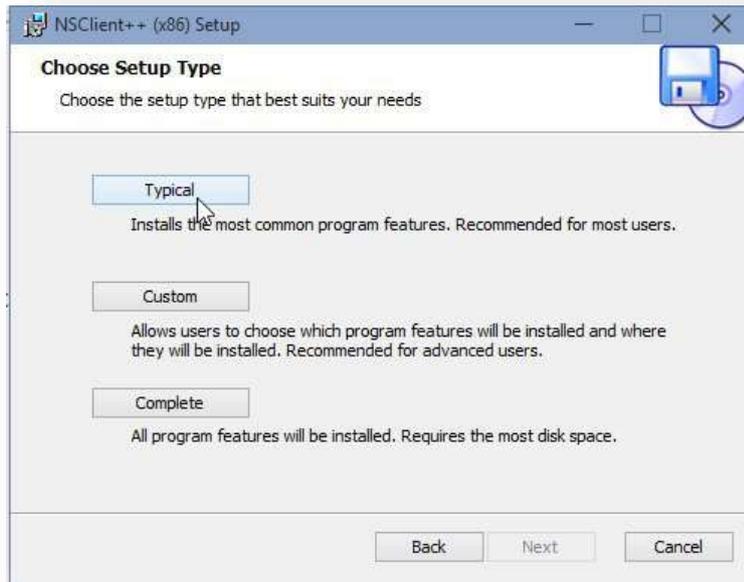


Figura 57: Configuración NSClient.

Fuente: Nagios.

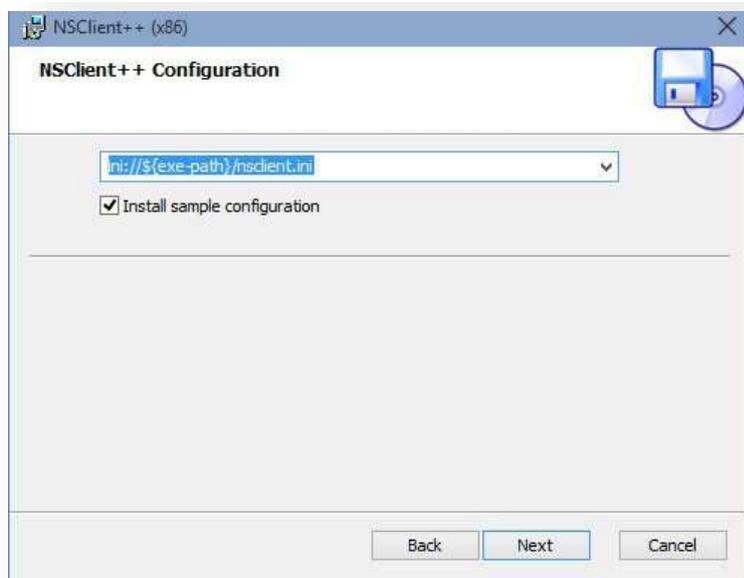


Figura 58: Configuración NSClient.

Fuente: Nagios.

Paso 4: Escogemos Typical y damos siguiente.

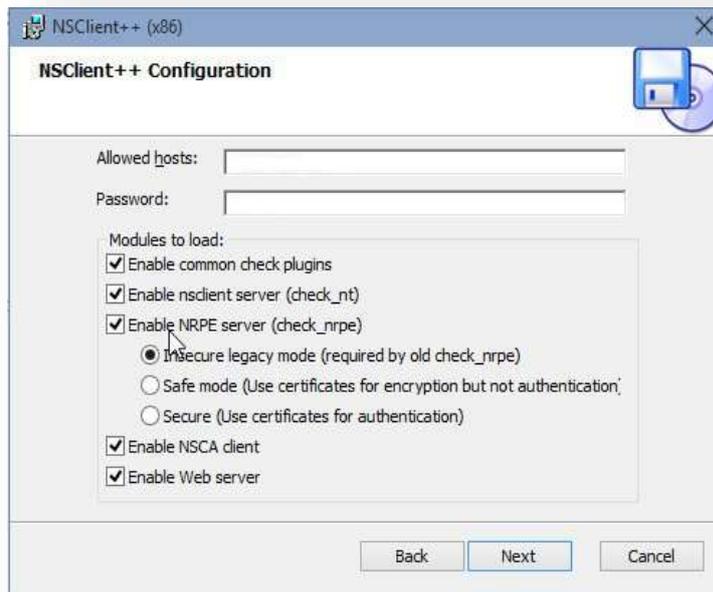


Figura 59: Configuración NSClient.

Fuente: Nagios.

Paso 5: En Allowed hosts se escribe la ip de nuestro servidor donde tenemos instalado Nagios y sin poner contraseña.

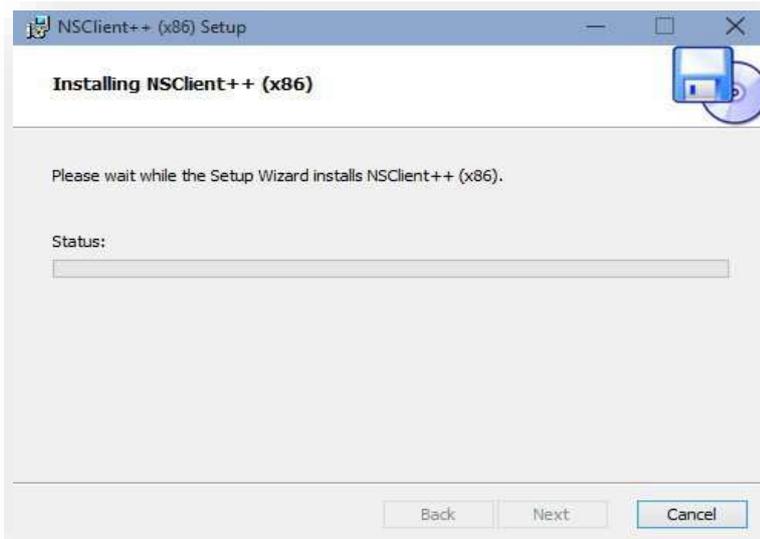


Figura 60: Configuración NSClient.

Fuente: Nagios.

Paso 6: Y se procede a instalar

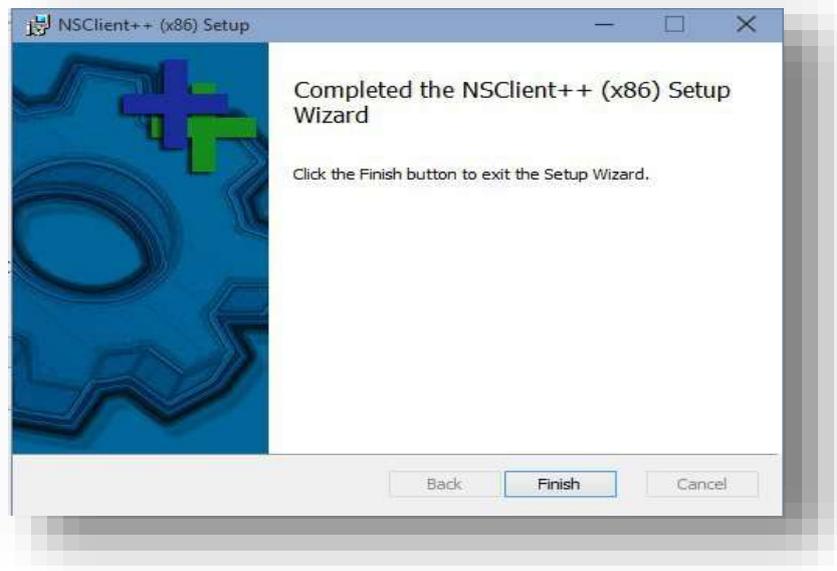


Figura 61: Configuración NSClient.

Fuente: Nagios.

Paso 7: Configuramos nuestro servidor en Nagios

Editamos el archivo en:

```
/user/local/nagios/etc/objects/windows.cfg
```

Nombre de host:

```
define host{
  use           windows-server
  host_name     FirewallProxy
  alias         Firewall
  address       192.168.0.103
}
```

NSClient++ instalado:

```
define service{
    use                generic-service
    host_name          FirewallProxy
    service_description NSClient++ Version
    check_command      check_nt!CLIENTVERSION
}
```

Uptime del servidor:

```
define service{
    use                generic-service
    host_name          FirewallProxy
    service_description Uptime
    check_command      check_nt!UPTIME
}
```

Memoria usada:

```
define service{
    use                generic-service
    host_name          FirewallProxy
    service_description Memory Usage
    check_command      check_nt!MEMUSE!-w 80 -c 90
}
```

Espacio en Disco duro:

```
define service{
    use                generic-service
    host_name          FirewallProxy
    service_description C:\ Local Disk
    check_command      check_nt!USEDISKSPACE!-l c -w 80
    -c 90
}
```

Paso 8: Se edita el archivo nagios.cfg ubicado en:

```
/usr/local/nagios/etc/
```

Des comentamos la línea:

```
cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

Paso 9: Reiniciamos el servicio de Nagios:

```
# service nagios restart
```

Paso 10: Entramos a la página de Nagios y comprobamos que nuestro servidor ya se está monitoreando:



| | | | | | | |
|---------------|--------------------|----|---------------------|----------------|-----|------------------------------------------------------------------------------------|
| FirewallProxy | C:\ Drive Space | OK | 07-28-2016 15:28:44 | 7d 12h 7m 24s | 1/3 | c: - total 90.00 Gb - used: 71.52 Gb (79%) - free 18.48 Gb (21%) |
| | CPU Load | OK | 07-28-2016 15:24:25 | 7d 12h 5m 9s | 1/3 | CPU Load 6% (5 min average) |
| | Memory Usage | OK | 07-28-2016 15:28:40 | 7d 12h 12m 56s | 1/3 | Memory usage: total 16504.38 Mb - used: 4847.44 Mb (29%) - free: 11656.94 Mb (71%) |
| | NSClient++ Version | OK | 07-28-2016 15:30:44 | 7d 12h 10m 46s | 1/3 | NSClient++ 0.4.2.88 2014-03-16 |
| | Uptime | OK | 07-28-2016 15:29:05 | 7d 12h 7m 4s | 1/3 | System Uptime - 7 day(s) 12 hour(s) 21 minute(s) |

Figura 62: Monitoreo de Servidor.

Fuente: Nagios.

10.4. Anexo D

10.4.1. Instalación de PNP4 Nagios

Para poder visualizar los servicios por medio de graficas es necesario instalar PNP4Nagios, cuyas características son:

- Visualizar graficas por intervalo de tiempo
- Visualizar las distintas graficas por servicios de Host
- Búsqueda de Hosts
- Exportar graficas por PDF
- Acceso directo desde un icono al lado de los servicios

Paso 1: Descargar los siguientes paquetes

```
#yum install rrdtool perl-Time-HiRes rrdtool-perl php-gd
```

Paso 2: Se descarga PNP4Nagios y se procede a compilar e instalar

```
#tar zxfv pnp4nagios-0.6.XX.tar.gz  
#cd pnp4nagios-0.6.XX  
#./configure  
#make all  
#make fullinstall
```

Paso 3: Para comprobar que no hay errores se ingresa a la siguiente dirección <http://ipnagios/pnp4nagios/> y debe de aparecer todo en verde

PNP4Nagios Environment Tests

The following options are determined by "configure". If any of the tests have failed, consult the [documentation](#) for more information on how to correct the problem.

| | |
|--------------------------|------------------------------------------------|
| PNP4Nagios Version | pnpnagios-0.6.24 |
| Prefix | /usr/local/pnp4nagios |
| Configure Arguments | /configure |
| RRD Storage | /usr/local/pnp4nagios/var/perfdata is readable |
| RRDtool Binary | /usr/bin/rrdtool is executable by PHP |
| PHP GD extension | Pass |
| PHP function proc_open() | Pass |
| PHP zlib extension | Pass |
| PHP session extension | Pass |
| PHP JSON extension | Pass |
| PHP magic_quotes_gpc | Off |
| PHP socket extension | Pass |
| Apache Rewrite Module | Pass |

Kohana Environment Tests

The following tests have been run to determine if Kohana will work in your environment. If any of the tests have failed, consult the [documentation](#) for more information on how to correct the problem.

| | |
|------------------------|------------------------------------------|
| PHP Version | 5.4.11 |
| System Directory | /usr/local/pnp4nagios/lib/kohana/system/ |
| Application Directory | /usr/local/pnp4nagios/share/application/ |
| Reflection Enabled | Pass |
| Iconv Extension Loaded | Pass |
| URI Determination | Pass |

Your environment passed all requirements. Remove or rename the `/usr/local/pnp4nagios/share/INSTALL.php` file.

Figura 63: Descarga PNP4Nagios.

Fuente: Nagios

Paso 4: Se procede a eliminar o cambiar de nombre al siguiente archivo

```
/usr/local/pnp4nagios/share/install.php
```

Integración con Nagios

```
/usr/local/pnp4nagios/etc/nagios.cfg-sample
```

Paso 5: Copiar solo el texto del archivo

Al archivo

```
/usr/local/nagios/etc/nagios.cfg
```

```

#
# Bulk / NPCD mode
#
process_performance_data=1
# *** the template definition differs from the one in the
original nagios.cfg
#
service_perfd_data_file=/usr/local/pnp4nagios/var/service-
perfd_data
service_perfd_data_file_template=DATATYPE::SERVICEPERFDATA\
tTIMET::$TIMET$\tHOSTNAME::$HOSTNAME$\tSERVICEDESC::$SERV
ICEDESC$\tSERVICEPERFDATA::$SERVICEPERFDATA$\tSERVICECHECK
COMMAND::$SERVICECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATE$\t
HOSTSTATETYPE::$HOSTSTATETYPE$\tSERVICESTATE::$SERVICESTA
TE$\tSERVICESTATETYPE::$SERVICESTATETYPE$
service_perfd_data_file_mode=a
service_perfd_data_file_processing_interval=15
service_perfd_data_file_processing_command=process-service-
perfd_data-file
# *** the template definition differs from the one in the
original nagios.cfg
#
host_perfd_data_file=/usr/local/pnp4nagios/var/host-
perfd_data
host_perfd_data_file_template=DATATYPE::HOSTPERFDATA\tTIMET
::$TIMET$\tHOSTNAME::$HOSTNAME$\tHOSTPERFDATA::$HOSTPERFD
ATA$\tHOSTCHECKCOMMAND::$HOSTCHECKCOMMAND$\tHOSTSTATE::$H
OSTSTATE$\tHOSTSTATETYPE::$HOSTSTATETYPE$
host_perfd_data_file_mode=a
host_perfd_data_file_processing_interval=15
host_perfd_data_file_processing_command=process-host-
perfd_data-file

```

Paso 6: Se copia también de `/usr/local/pnp4nagios/etc/misccommands.cfg-sample` al archivo `/usr/local/nagios/etc/objects/commands.cfg`

```
#
# Bulk with NPCD mode
#
define command {
command_name process-service-perfdata-file
command_line /bin/mv /usr/local/pnp4nagios/var/service-
perfdata /usr/local/pnp4nagios/var/spool/service-
perfdata.$TIMET$
}
define command {
command_name process-host-perfdata-file
command_line /bin/mv /usr/local/pnp4nagios/var/host-
perfdata /usr/local/pnp4nagios/var/spool/host-
perfdata.$TIMET$
}
```

Paso 7: Se procede a reiniciar Nagios y pnp4nagios

```
service npcd restart && service nagios restart
```

Paso 8: Se agrega el siguiente texto al archivo

```
/usr/local/nagios/etc/objects/templates.cfg
```

```

define host {
name host-pnp
action_url
/pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=_HOST_
' class='tips'
rel='/pnp4nagios/index.php/popup?host=$HOSTNAME$&srv=_
HOST_
register 0
}
define service {
name srv-pnp
action_url
/pnp4nagios/index.php/graph?host=$HOSTNAME$&srv=$SERVI
CEDESC$' class='tips'
rel='/pnp4nagios/index.php/popup?host=$HOSTNAME$&srv=$
SERVICEDESC$
register 0
}

```

Para que aparezcan las gráficas en los hosts se agrega host-pnp y en los servicios srv-pnp.

```

root@localhost:~
define host {
    use                linux-server,host-pnp
    host_name          norte
    parents             CentroComputo
    alias              servernorte
    address            10.87.127.1
    max_check_attempts 5
    check_period       24x7
    notification_interval 30
    notification_period 24x7
}

define service {
    use                generic-service,srv-pnp
    host_name          norte
    service_description PING
    check_command      check_ping!100.0,20%!500.0,60%
}

define service {
    use                generic-service,srv-pnp
    host_name          norte
    service_description SSH
}
"/usr/local/nagios/etc/servers/servernorte.cfg" 42L, 1340C

```

Figura 64: Ingreso de host-pnp y servicios srv-pnp.

Fuente: Nagios

Paso 9: Se ingresa a la página web de Nagios y se puede observar un icono de grafica al lado de los hosts y así mismo al lado de los servicios.

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---------------|---------------------|--------|---------------------|-----------------|---------|-------------------------------------------------------------------------------------|
| AulaVirtual | PING | OK | 07-28-2016 15:28:05 | 0d 1h 17m 57s | 1/0 | PING OK - Packet loss = 0%, RTA = 0.45 ms |
| | SSH | OK | 07-28-2016 15:28:00 | 27d 23h 15m 45s | 1/0 | SSH OK - OpenSSH_6.4 (CentOS 3.0) |
| CentroComputo | PING | OK | 07-28-2016 15:27:59 | 0d 0h 32m 3s | 1/0 | PING OK - Packet loss = 0%, RTA = 3.47 ms |
| Dominio | C:\ Drive Space | OK | 07-28-2016 15:32:05 | 0d 3h 54m 55s | 1/0 | C: - total: 253.97 Gb - used: 46.53 Gb (18%) - free: 207.45 Gb (82%) |
| | CPU Load | OK | 07-28-2016 15:28:06 | 0d 22h 55m 52s | 1/0 | CPU Load 8% (5 min average) |
| | Memory Usage | OK | 07-28-2016 15:28:20 | 0d 3h 55m 8s | 1/0 | Memory usage: total:65532 (63 Mb) - used: 2497.79 Mb (4%) - free: 63034.22 Mb (96%) |
| | NSIClient - Version | OK | 07-28-2016 15:30:23 | 0d 3h 56m 54s | 1/0 | NSIClient++ (0.4.1.105 2014-04-20) |
| | Uptime | OK | 07-28-2016 15:32:53 | 0d 3h 54m 36s | 1/0 | System Uptime - 0 day(s) 22 hour(s) 57 min(s) 6s |
| FirewallProxy | C:\ Drive Space | OK | 07-28-2016 15:28:44 | 7d 12h 7m 24s | 1/0 | C: - total: 80.20 Gb - used: 71.52 Gb (79%) - free: 18.68 Gb (21%) |
| | CPU Load | OK | 07-28-2016 15:24:25 | 7d 12h 5m 5s | 1/0 | CPU Load 8% (5 min average) |
| | Memory Usage | OK | 07-28-2016 15:28:40 | 7d 12h 12m 55s | 1/0 | Memory usage: total:10524.28 Mb - used: 4017.44 Mb (38%) - free: 11898.94 Mb (71%) |
| | NSIClient - Version | OK | 07-28-2016 15:30:44 | 7d 12h 10m 46s | 1/0 | NSIClient++ (0.4.2.08 2014-03-18) |
| | Uptime | OK | 07-28-2016 15:29:05 | 7d 12h 7m 4s | 1/0 | System Uptime - 7 day(s) 12 hour(s) 21 min(s) 4s |
| Nagios | Current Load | OK | 07-28-2016 15:32:51 | 36d 0h 33m 26s | 1/4 | OK - load average: 0.00, 0.00, 0.00 |
| | Current Users | OK | 07-28-2016 15:32:51 | 36d 0h 01m 28s | 1/4 | USERS OK - 1 users currently logged in |
| | HTTP | OK | 07-28-2016 15:28:06 | 27d 1h 55m 21s | 1/4 | HTTP OK: HTTP/1.1 200 OK - 200 bytes in 0.001 second response |

Figura 65: Generar gráficos con PNP4Nagios.

Fuente: Nagios.

| Host | Status | Last Check | Duration | Status Information |
|---------------|--------|---------------------|----------------|-------------------------------------------|
| AulaVirtual | UP | 07-28-2016 15:35:46 | 37d 23h 40m 5s | PING OK - Packet loss = 0%, RTA = 0.43 ms |
| CentroComputo | UP | 07-28-2016 15:32:27 | 0d 0h 34m 47s | PING OK - Packet loss = 0%, RTA = 4.11 ms |
| Dominio | UP | 07-28-2016 15:35:46 | 0d 23h 0m 24s | PING OK - Packet loss = 0%, RTA = 0.64 ms |
| FirewallProxy | UP | 07-28-2016 15:35:46 | 7d 12h 15m 44s | PING OK - Packet loss = 0%, RTA = 0.73 ms |
| Nagios | UP | 07-28-2016 15:32:53 | 36d 0h 36m 42s | PING OK - Packet loss = 0%, RTA = 0.03 ms |
| lab1 | UP | 07-28-2016 15:35:46 | 0d 3h 42m 46s | PING OK - Packet loss = 0%, RTA = 0.76 ms |
| norfe | UP | 07-28-2016 15:35:06 | 0d 0h 39m 14s | PING OK - Packet loss = 0%, RTA = 4.50 ms |

Results 1 - 7 of 7 Matching Hosts

Figura 66: Generar gráficos con PNP4Nagios.

Fuente: Nagios

Paso 10: Al dar clic sobre ellos se generan las gráficas en intervalo de tiempo

10.5. Anexo E

10.5.1. Instalación y configuración de Active Directory

Para instalar el servicio de directorio activo se requiere:

Paso 1: Iniciar una sesión en el Servidor como Administrador.

Paso 2: Abrir el Administrador del servidor y dar clic en Agregar roles y características.

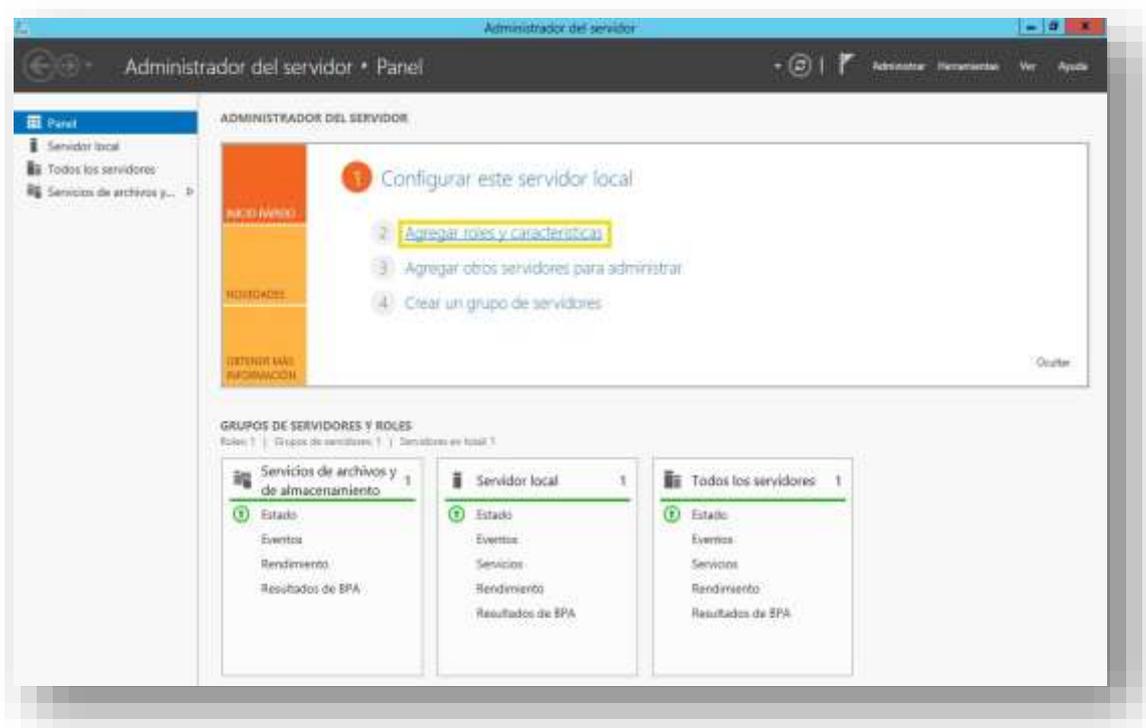


Figura 68: Agregar Roles y características.

Fuente: Windows Server 2012.

Paso 3: Dar clic en Siguiente en la página del asistente.

Paso 4: Seleccionar el tipo de instalación: Instalación basada en características o en roles.

Paso 5: Seleccionar el servidor correspondiente.

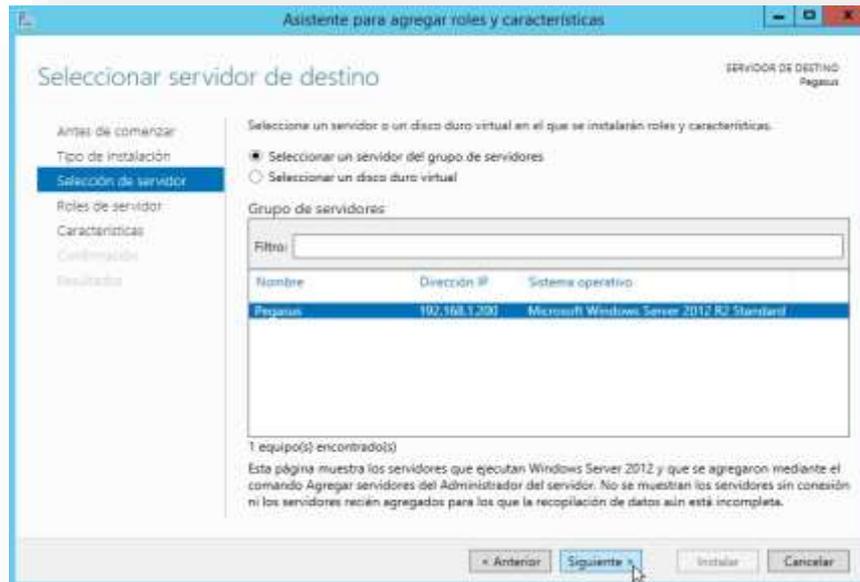


Figura 69: Selección servidor para agregar roles y características.

Fuente: Windows Server 2012.

Paso 6: Seleccionar la casilla Servicios de dominio de Active Directory.

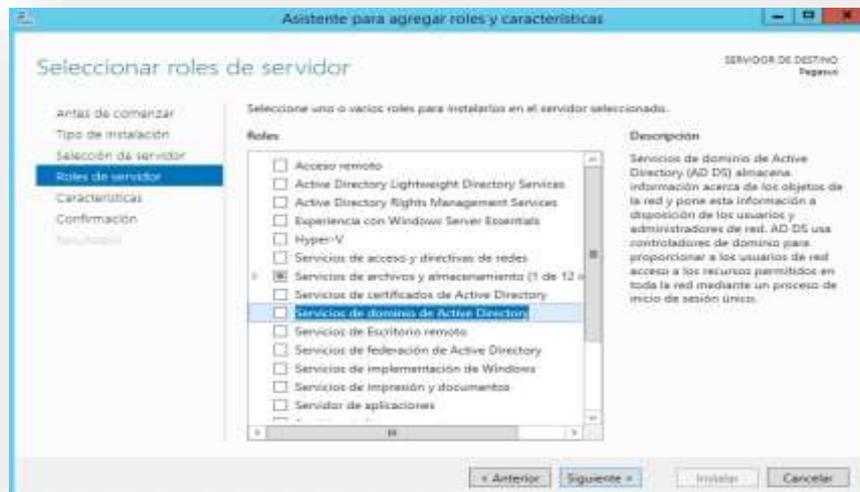


Figura 70: Selección servicios de dominio.

Fuente: Windows Server 2012.

Paso7: En el asistente para agregar roles y características dar clic sobre

Agregar características y después en Siguiente.

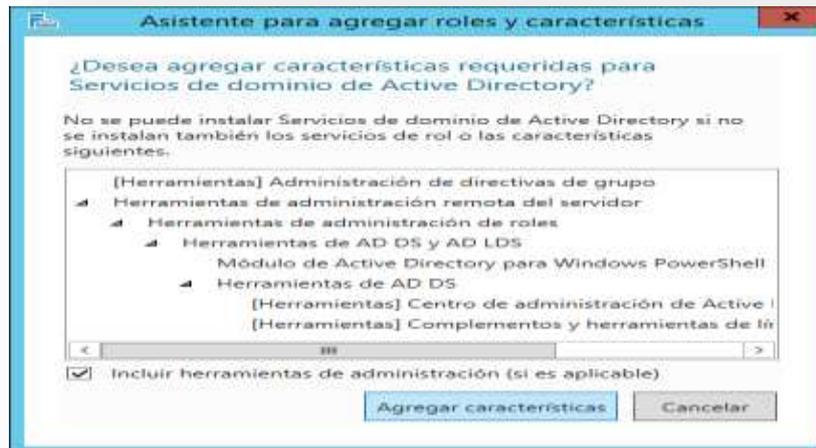


Figura 71: Agregar características al servidor.

Fuente: Windows Server 2012.

Paso 8: Se escoge las características necesarias para la instalación de Active Directory. A continuación, se da clic en Siguiente.

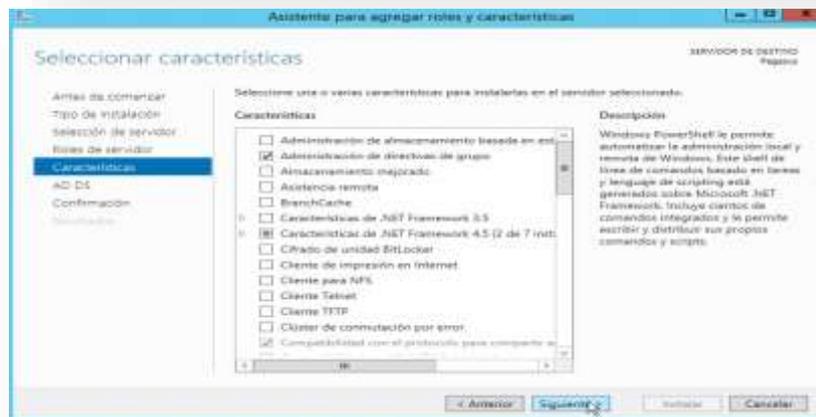


Figura 72: Agregar roles y características.

Fuente: Windows Server 2012.

Paso 9: Se da clic en Siguiente y a continuación Instalar.

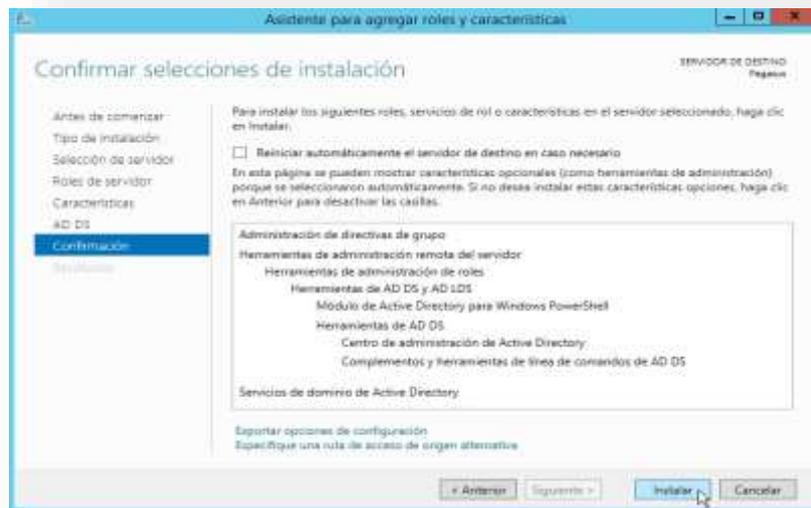


Figura 73: Agregar roles y características.

Fuente: Windows Server 2012.

Paso 10: Se procede a crear el dominio. En la ventana de Resultados de la instalación de Active Directory se da clic en Promover este servidor a controlador de dominio.



Figura 74: Configuración directorio activo.

Fuente: Windows Server 2012.

Si se da el caso de haber cerrado la pestaña anterior se puede acceder a ella pulsando en el icono de advertencia de la barra de herramientas del Administrador del servidor.

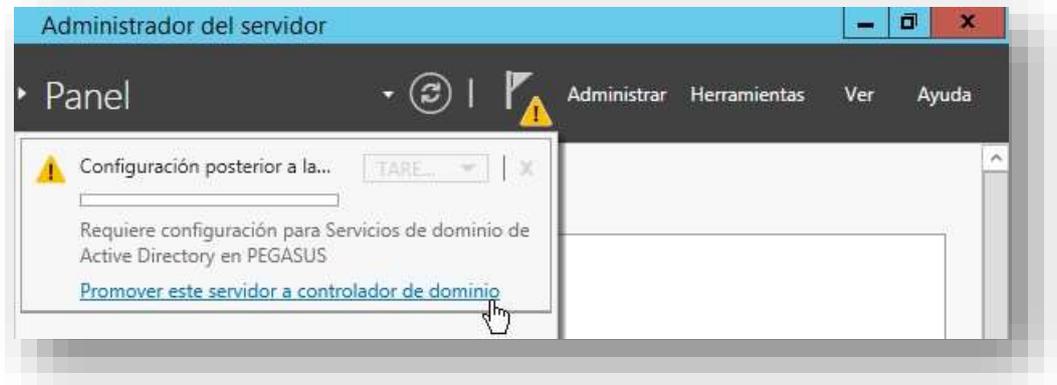


Figura 75: Configuración directorio activo.

Fuente: Windows Server 2012.

Paso 11: Se debe crear un nuevo bosque para formar el dominio filosofía.ug.edu.ec y así poder asociar el servidor de directorio activo al dominio. Para esto se prosigue al asistente para configuración de servicios de dominio de Active Directory, en la opción agregar un nuevo bosque y se escribe el nombre del dominio. A continuación de esto se da clic en Siguiente.

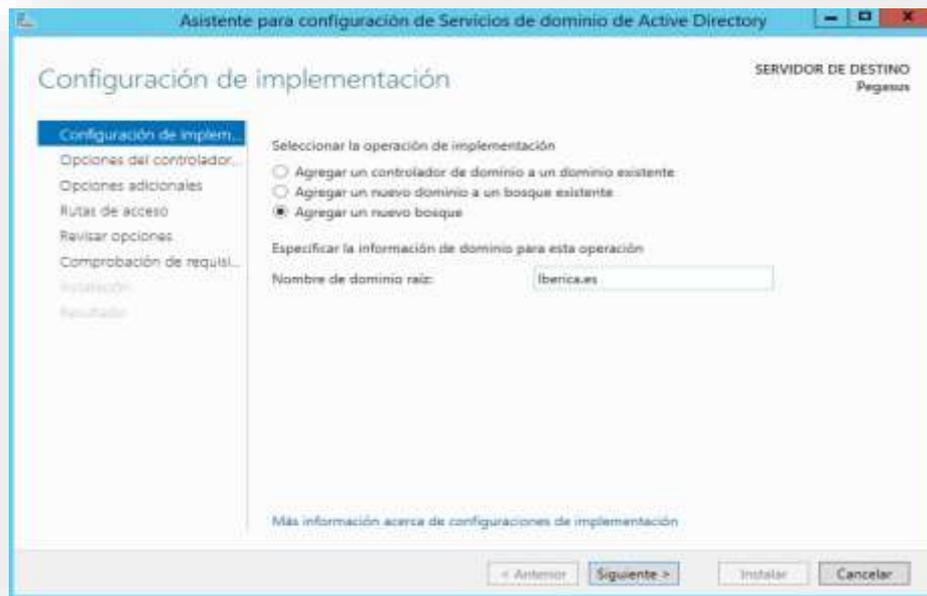


Figura 76: Configuración directorio activo.

Fuente: Windows Server 2012.

Paso 12: en opciones del controlador tanto para nivel de funcionalidad del bosque como para el dominio debe estar seleccionado Windows server 2012R y deben estar seleccionadas las casillas de Servidor de Sistema de nombre de dominio y el catalogo global. Después de seleccionar se da clic en siguiente.

Paso 13: En opciones adicionales se puede escribir el nombre del NetBIOS en nuestro caso “Filosofía”.

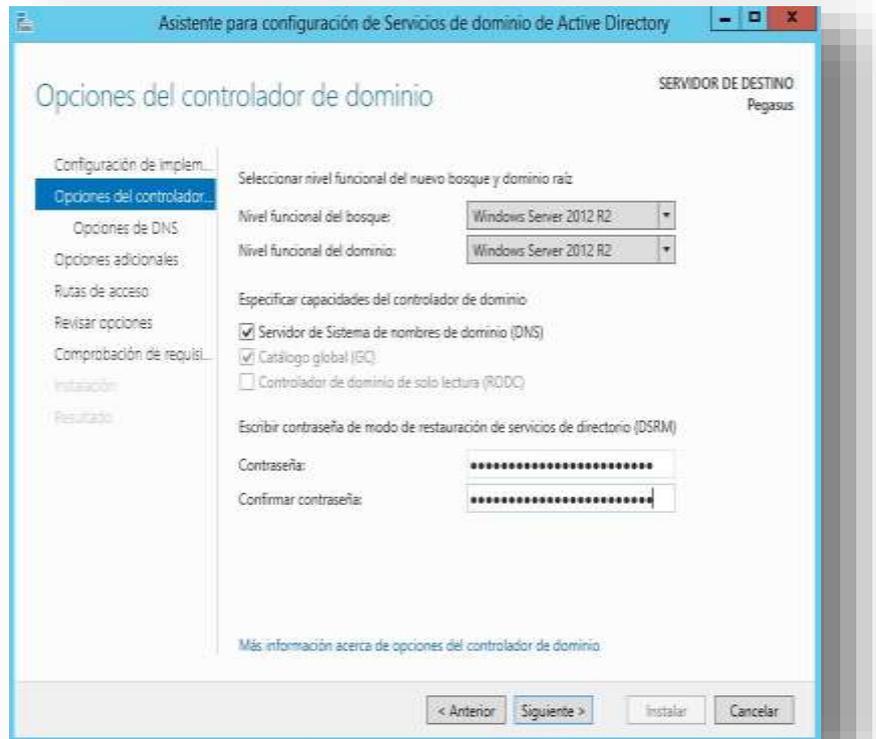


Figura 77: Configuración directorio activo.

Fuente: Windows Server 2012.

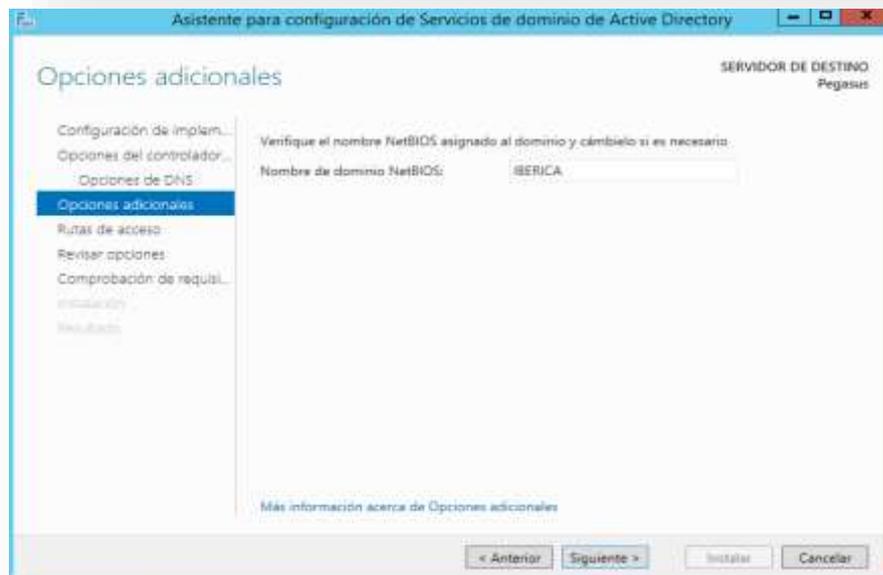
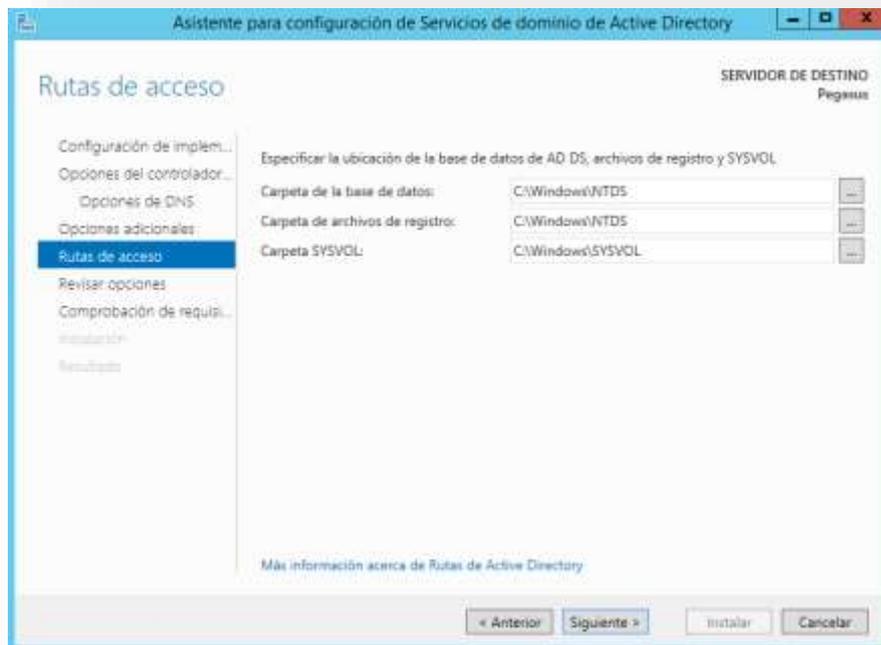


Figura 78: Configuración directorio activo.

Fuente: Windows Server 2012.

Paso 14: Especificar la ubicación de la base de datos del directorio Activo y archivos de registros.



Paso 15: Se revisa las selecciones hechas y se da clic en siguiente.

Paso 16: Clic en instalar.

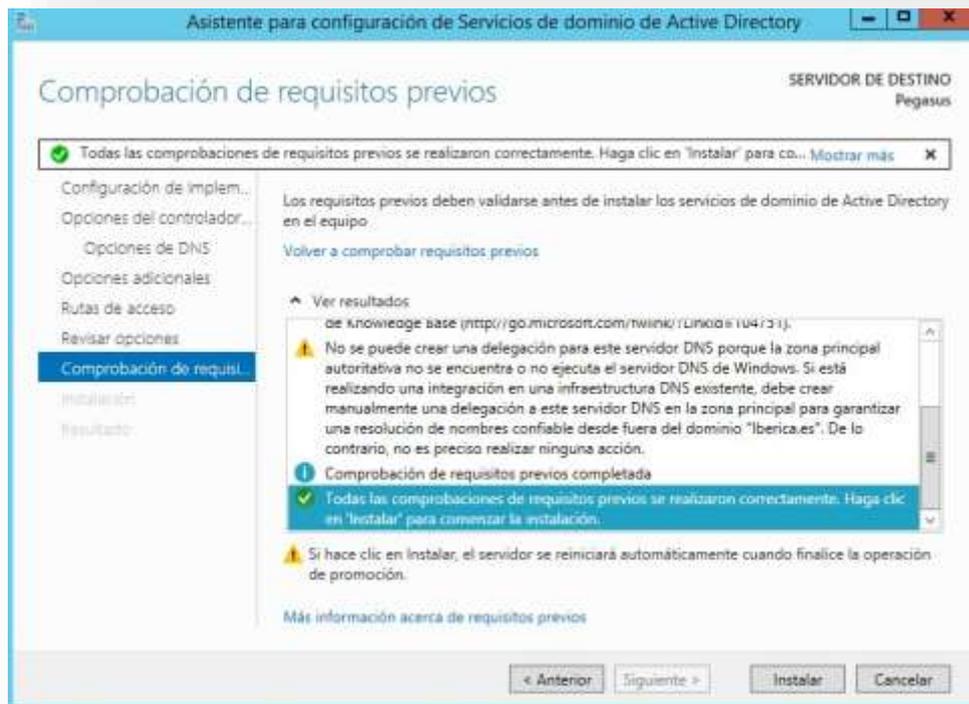


Figura 79: Configuración directorio activo.

Fuente: Windows Server 2012.

Figura 81: Configuración directorio activo.

Fuente: Windows Server 2012.



10.6. Anexo F

10.6.1. Creación de unidades organizativas

Paso 1: Abrir Usuarios y equipos de Active Directory desde herramientas administrativas

Paso 2: En el árbol de la consola hacer clic con el botón derecho del ratón sobre el dominio Filosofia.ug.edu.ec.

Paso 3: Seleccionar nuevo y hacer clic en Unidad Organizativa.

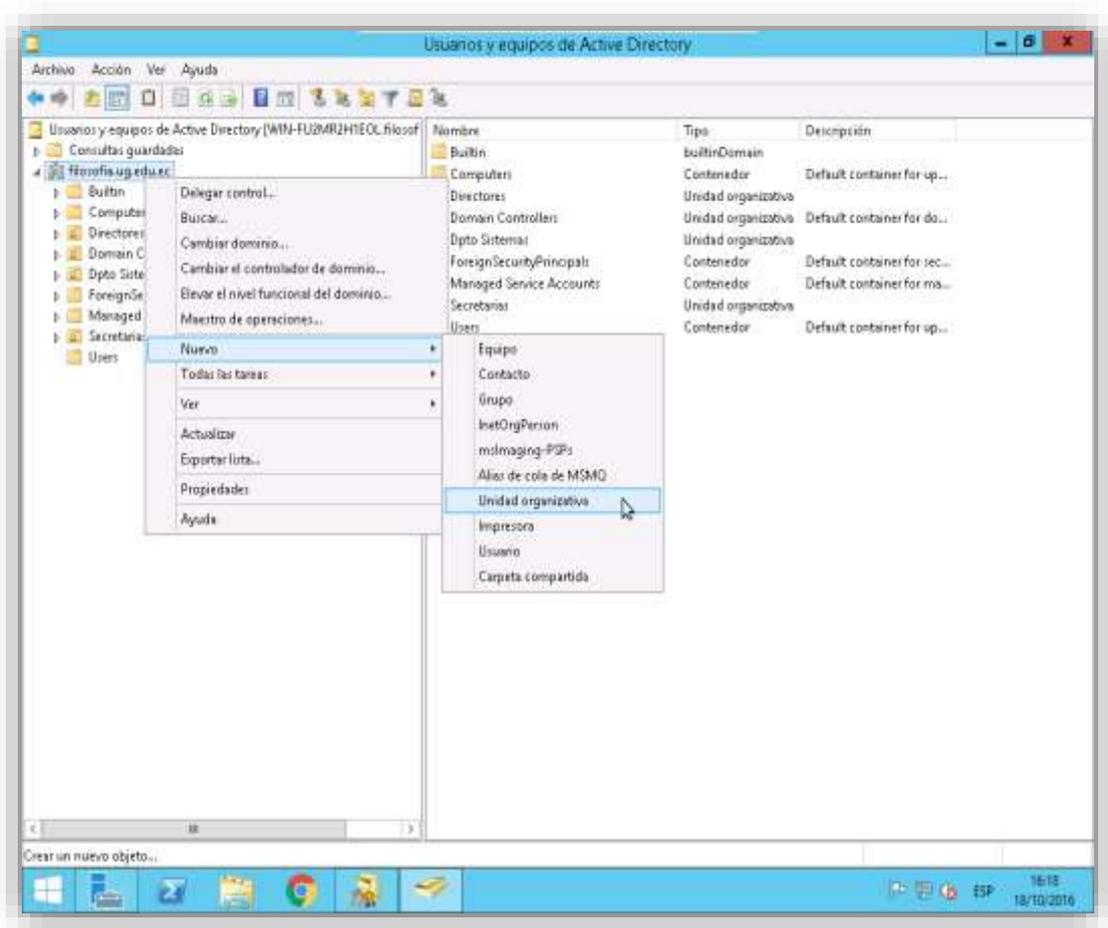


Figura 82: Agregar Unidad organizativa.

Fuente: Windows Server 2012.

Paso 4: Aparecerá el cuadro de dialogo Nuevo objeto – Unidad Organizativa.

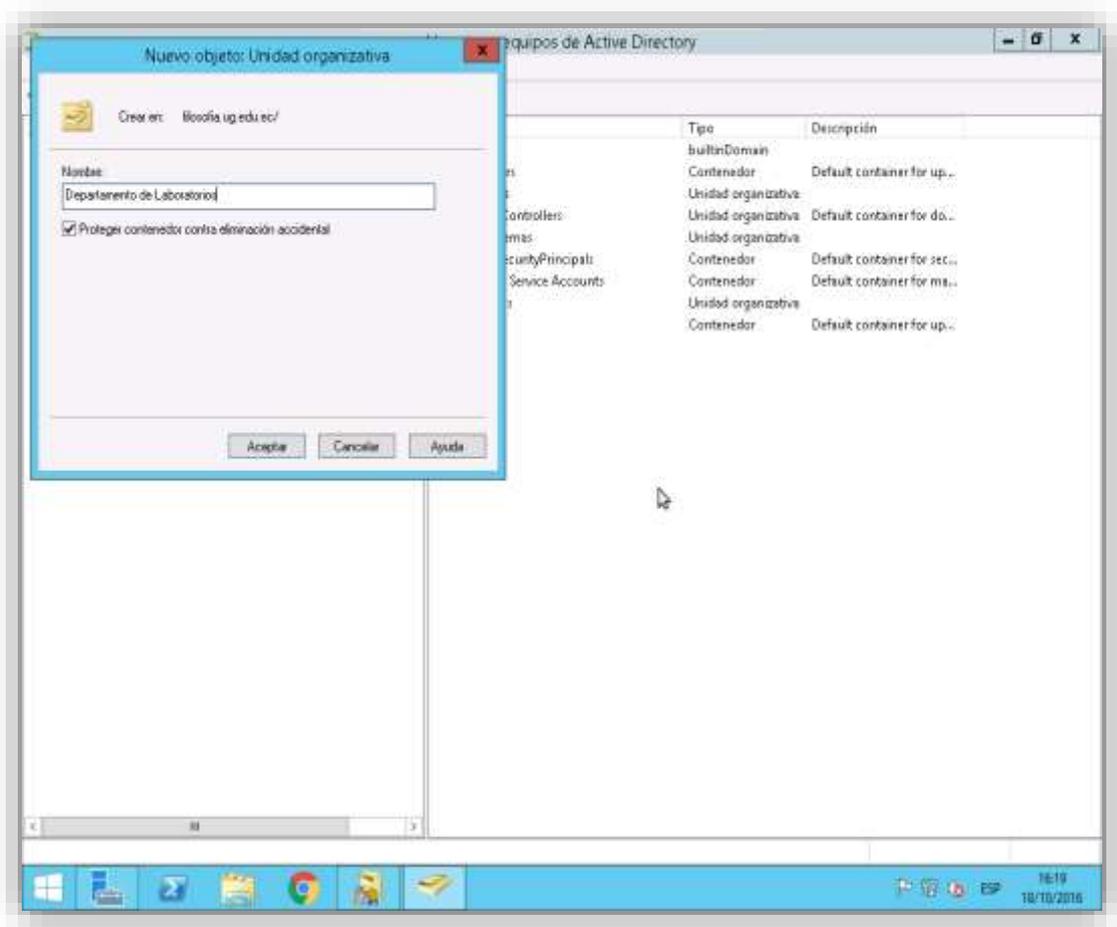


Figura 83: Agregar Unidad organizativa.

Fuente: Windows Server 2012.

Paso 5: En el cuadro de dialogo escribir el nombre de la nueva Unidad Organizativa.

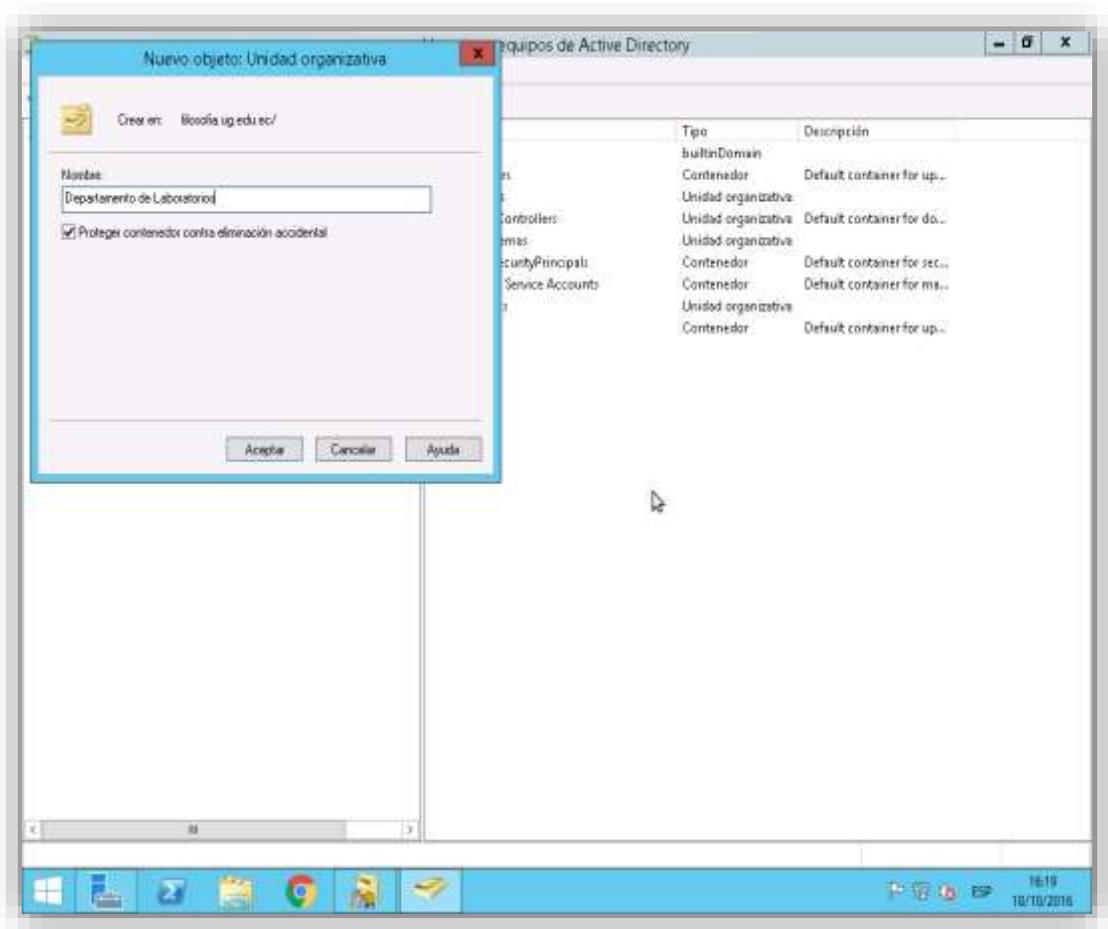


Figura 84: Agregar Unidad organizativa.

Fuente: Windows Server 2012.

Paso 6: Dentro de la unidad organizativa nueva se puede crear el resto de unidades organizativas.

10.6.2. Creación de usuarios

Paso 1: Desde usuarios y equipos de Active Directory, dar clic derecho sobre una unidad organizativa. Seleccionar nuevo y hacer clic en Usuario.

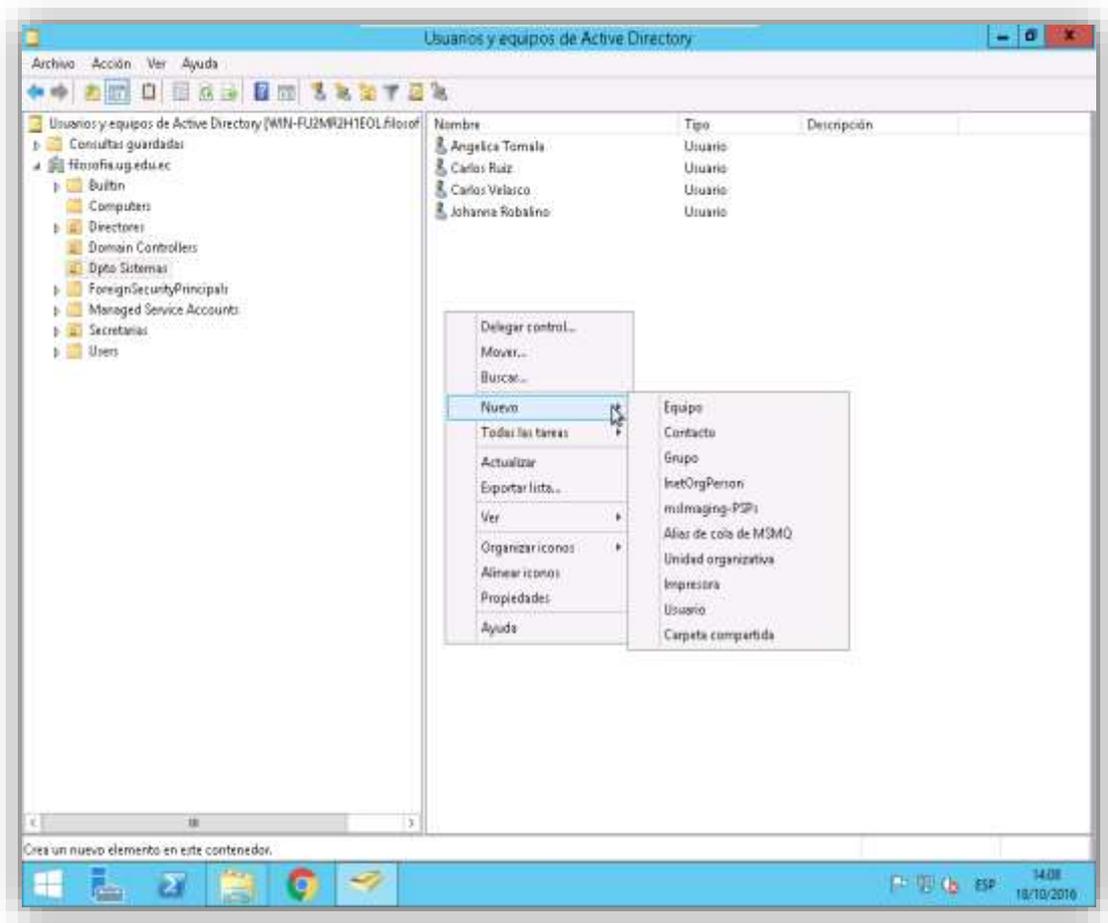


Figura 85: Creación de usuarios.

Fuente: Windows Server 2012.

Paso 2: Llenar los campos con los datos respectivos.

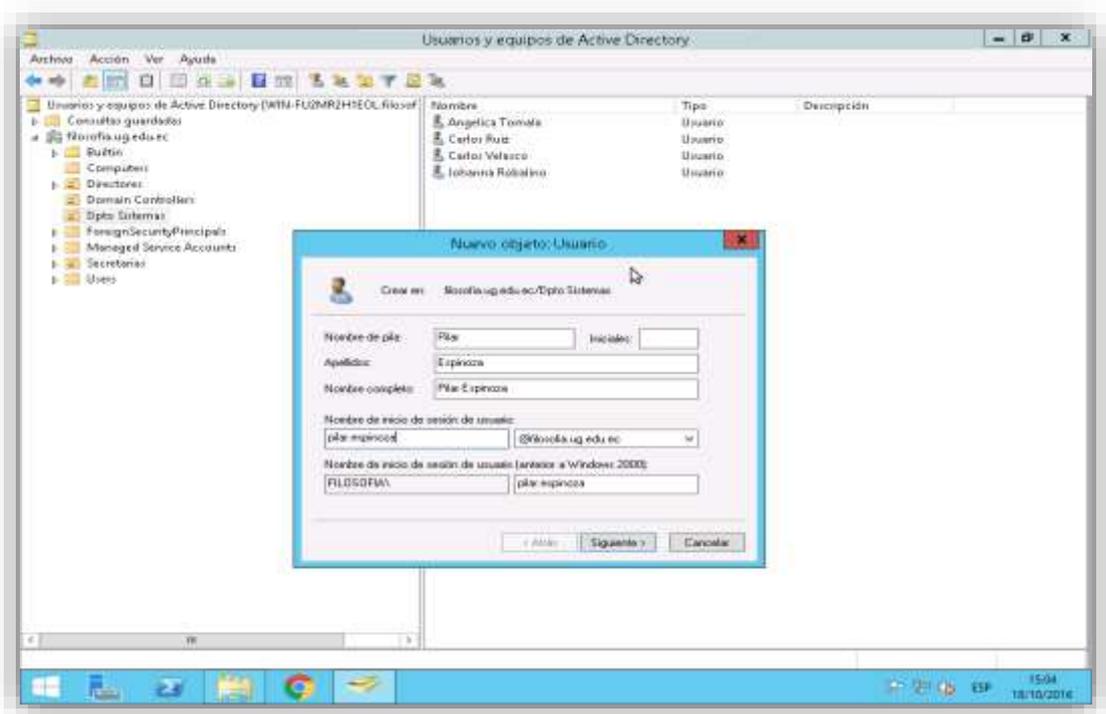


Figura 86: Creación de usuarios.

Fuente: Windows Server 2012.

Paso 3: Escribir si es el caso la contraseña temporal y marcar la opción que corresponda.

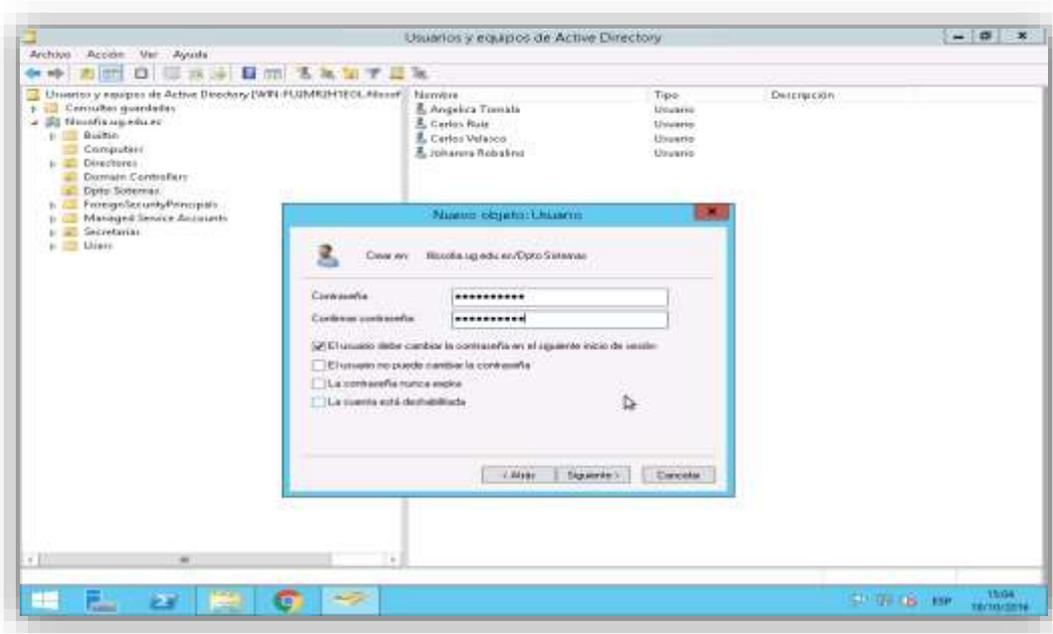


Figura 87: Creación de usuarios.

Fuente: Windows Server 2012.

Paso 4: Finalizar

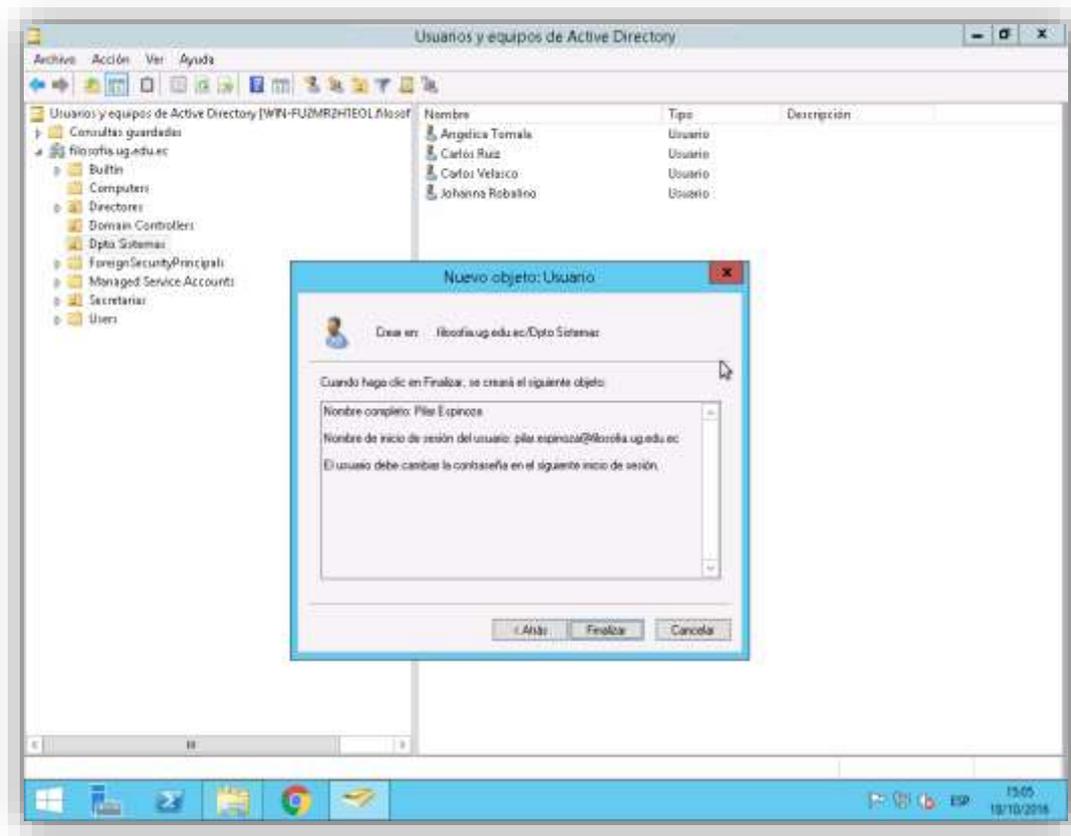


Figura 88: Creación de usuarios.

Fuente: Windows Server 2012.

10.6.3. Creación de Grupo

Paso 1: Desde usuarios y equipos de Active Directory dar clic derecho y escoger Grupo – Nuevo Grupo.

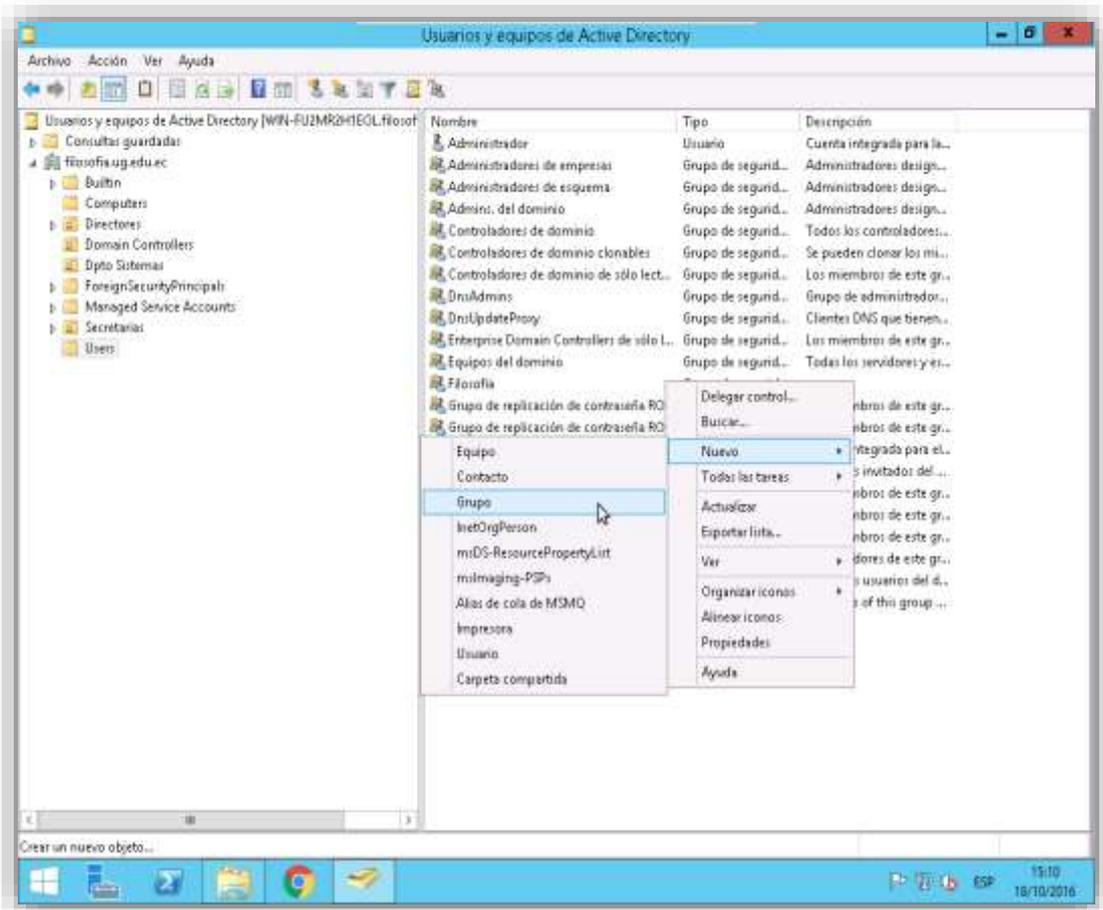


Figura 89: Creación de grupos en Directorio Activo.

Fuente: Windows Server 2012.

Paso 2: Llenar los campos con los datos respectivos.

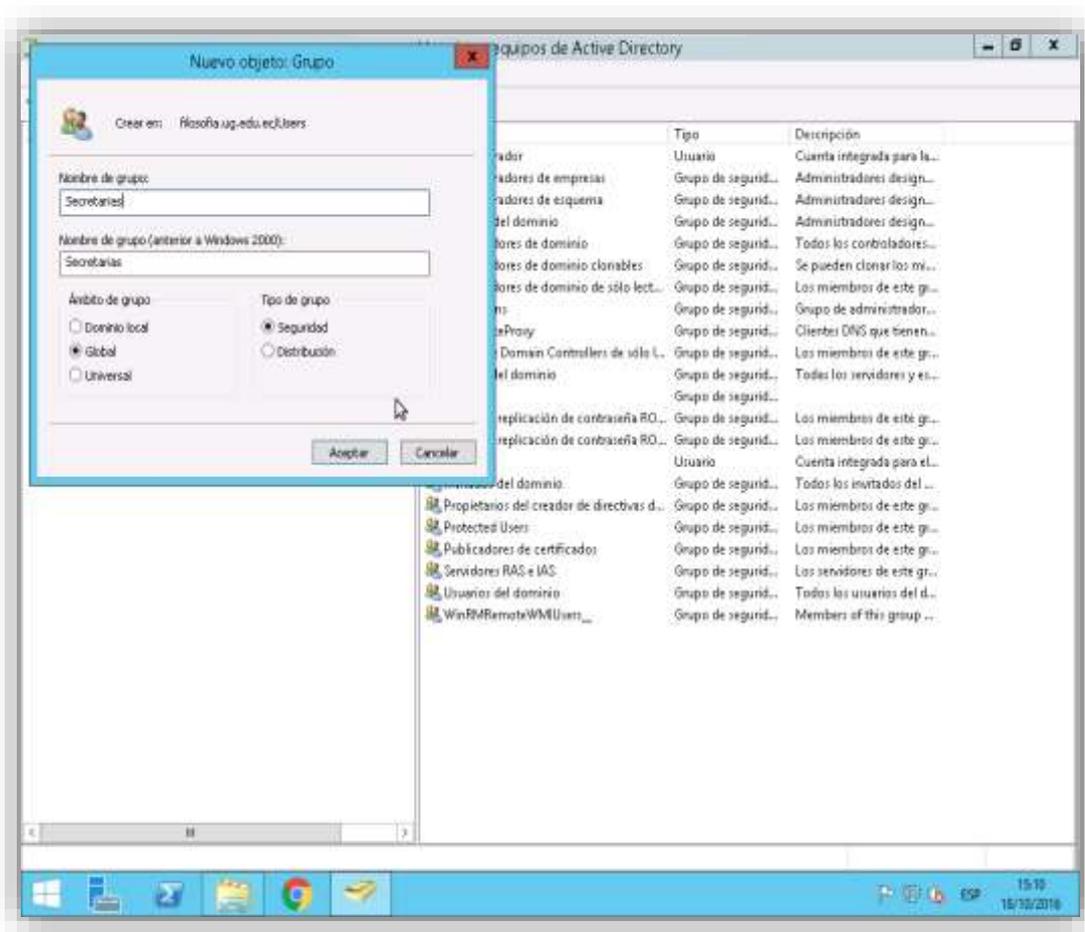


Figura 90: Creación de grupos en Directorio Activo.

Fuente: Windows Server 2012.

Paso 3: Una vez creado el grupo se puede añadir miembros en Propiedades – Miembros.

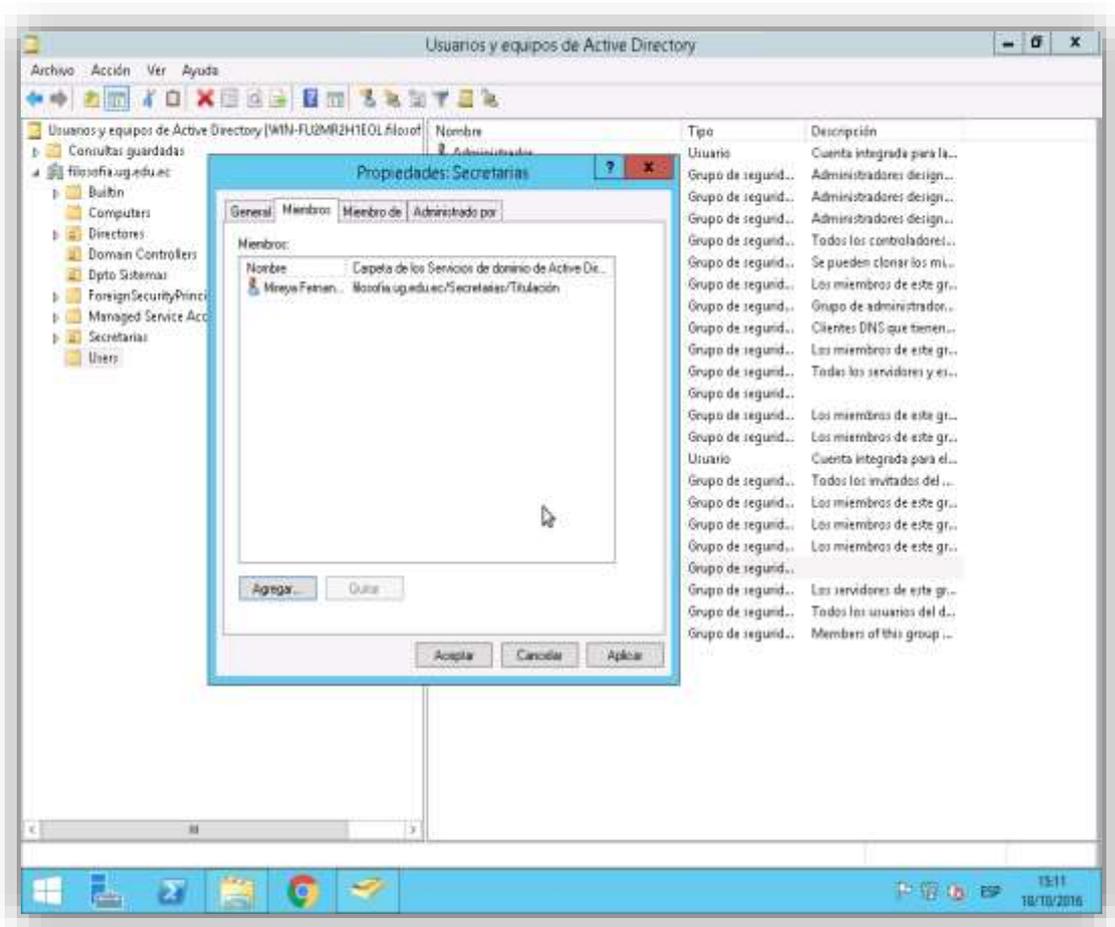


Figura 91: Creación de grupos en Directorio Activo.

Fuente: Windows Server 2012.

Paso 4: Al dar clic en Agregar aparecerá un cuadro de dialogo que permitirá agregar objetos al grupo.

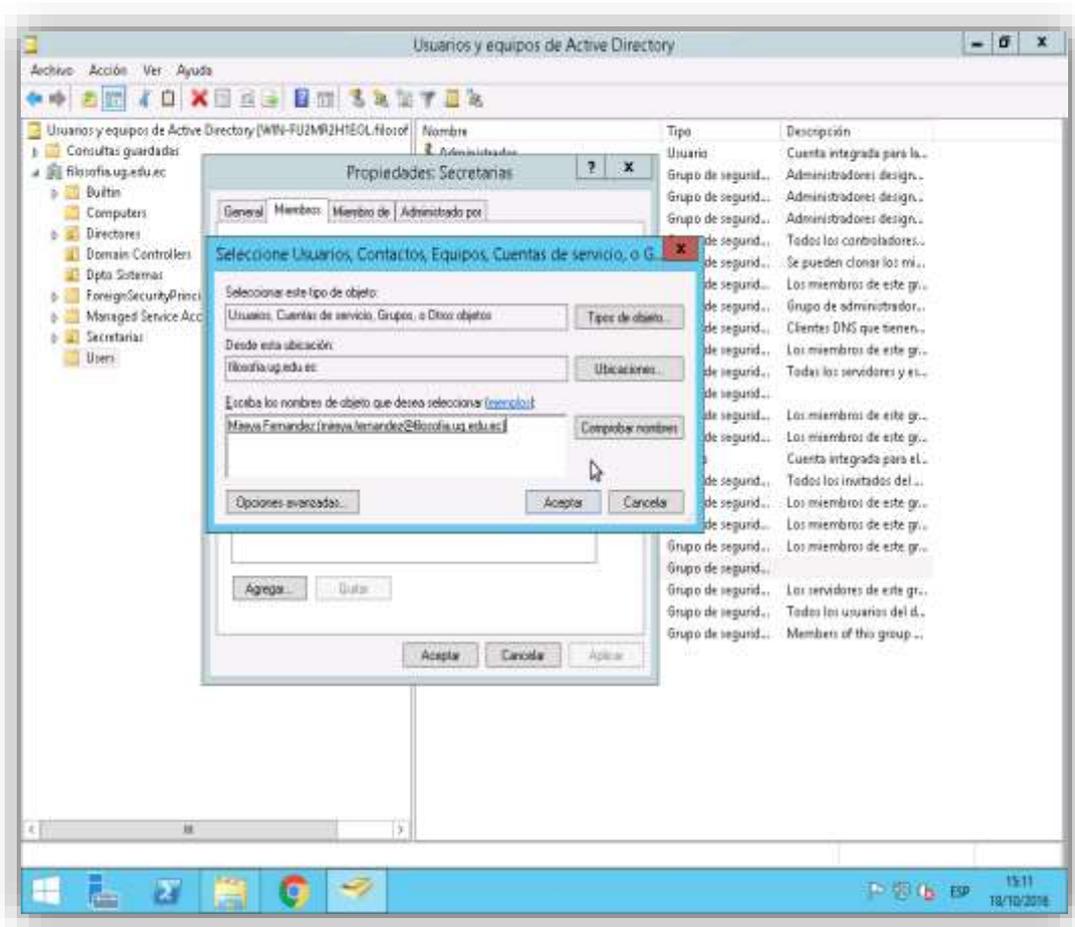


Figura 92: Creación de grupos en Directorio Activo.

Fuente: Windows Server 2012.

10.7. Anexo G

10.7.1. Capacitación de Nagios y Directorio Activo

Una vez instalados y configurados las dos herramientas planteadas en el proyecto, se procedió a impartir las capacitaciones respectivas al departamento de sistemas de la Facultad.

El día 21 de octubre del 2016 desde las 14:30 hasta las 17:30 en el departamento de sistemas se impartieron los siguientes temas:

- Definición de Directorio Activo.
- Pasos para la configuración de Directorio Activo.
- Creación de roles, usuarios y grupos en el directorio.
- Ingreso de máquinas al servidor de dominio.

El lunes 24 de octubre del 2016 desde las 10:30 hasta las 12:00 se capacitó al personal con los siguientes temas:

- Nagios y sus beneficios.
- Instalación de Nagios.
- Alertas y mensajes del software de monitoreo.

Para la respectiva constancia se anexa la hoja en formato digital con las firmas de los integrantes del departamento de sistemas que recibieron las capacitaciones.

Capacitación sobre el Servidor de Dominio y Nagios

Expositores:

- Sr. Carlos Velasco
- Srta. Gianella cagua

| N° | Nombre y Apellidos | Cédula | Firma |
|----|------------------------------------|------------|-----------------------------------------------------------------------------------|
| 1 | MSc. Carlos Ruiz Berna | 0910662386 |  |
| 2 | Lcda. Johanna Robalino Salvatierra | 0914896949 |  |
| 3 | Lcda. Pilar Espinoza Arias | 0917954794 |  |
| 4 | Lcda. Angélica Tomalá | 0918788761 | VACACIONES |

A continuación, se anexa fotos de los días de la capacitación impartidos.

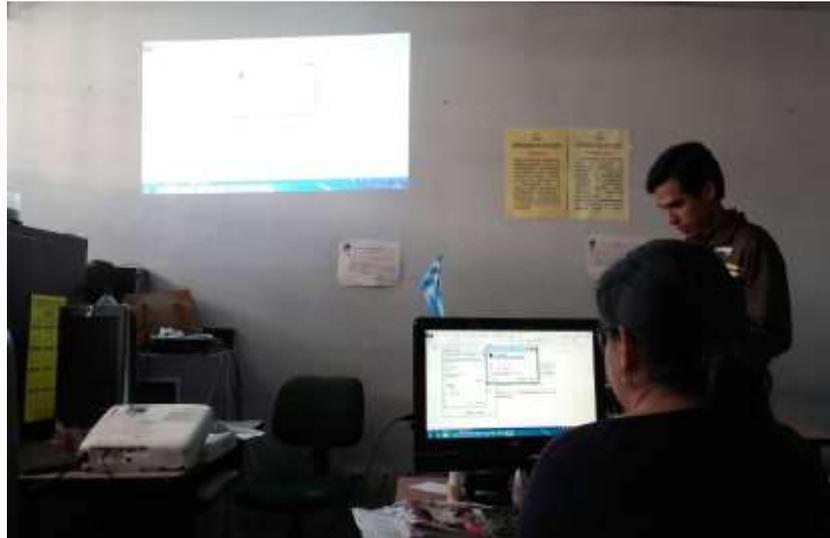


Figura 93: Capacitación al departamento de sistemas.
Fuente: Los Autores

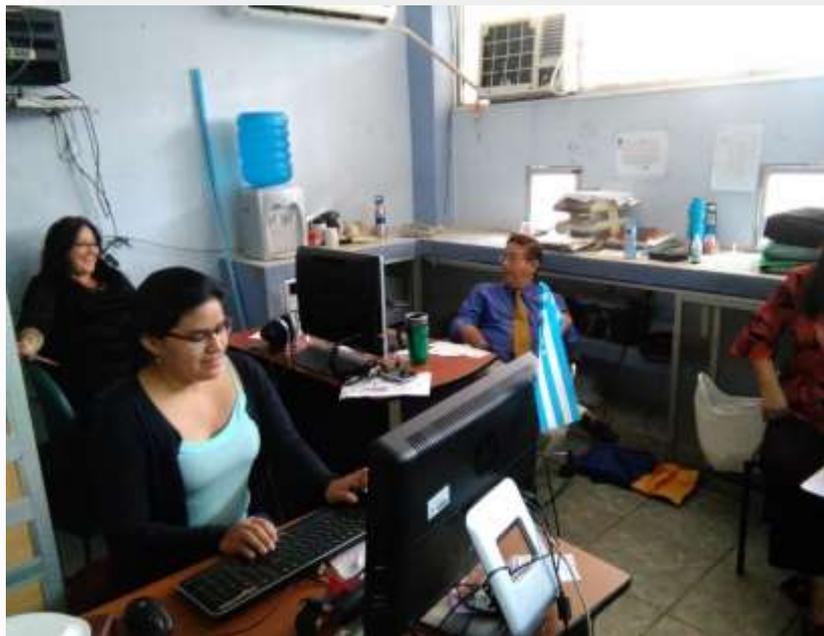


Figura 94: Capacitación al departamento de sistemas.
Fuente: Los Autores.



Figura 95: Capacitación al departamento de sistemas.

Fuente: Los Autores.

10.8. Anexo H

10.8.1. Oficio No. 113-UGFF-DSIST-JR-16

 **UG**
Universidad
de Guayaquil

 Facultad de Filosofía
Letras y Ciencias de la
Educación

 **sistemas**

FF.DPTO.SISTEMAS@ug.edu.ec
Teléfono: 2-296630

Oficio No.113-UGFF-DSIST-JR-16

12 de octubre de 2016

Arquitecta
Silvia Moy – Sang Castro, Msc.
Decana
En su despacho

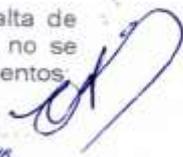
De mi consideración:

Hago llegar un saludo cordial, a la vez que, por medio de la presente y siendo el antecedente Oficio No.215-UGFF-DSIST-JR-15, con fecha 2 de diciembre de 2015, en el que avalado con respectiva autorización suya, este departamento procedió a ingresar las computadoras, en el servidor de dominio de la facultad, informo a usted lo siguiente:

Se han ingresado al servidor de dominio, los departamentos y carreras detallados a continuación:

Coordinación Académica Presencial, Unidad Técnica de Proforma Presupuestaria, Unidad Administrativa de Talento Humano, Biblioteca Dr. Humberto Salvador Guerra, Vinculación con la colectividad, Aulas Virtuales, Filosprint, Coordinación Académica Semi Presencial, Seguimiento a Graduados, Departamento de Archivo Semi Presencial, Informática Educativa, Escuela de Lenguas, Mercadotecnia y Publicidad, Comercio Exterior, Administración y Supervisión Educativa, Comercio y Administración, Físico Matemáticas, Historia y Geografía, Desarrollo Comunitario y Ambiental, Químico Biológicas, Filosofía y Ciencias Psicosociales, Educación Primaria.

A su vez, debido al poco interés, desconocimiento, falta de cooperación y desacato a la autorización que usted emitió, no se han ingresado al servidor de dominio, los siguientes departamentos:



FACULTAD DE FILOSOFÍA
LETRAS Y CIENCIAS DE LA EDUCACIÓN
RECEPCIÓN DE OFICINA

Fecha: 13-10-2016
No. 17400
Firma: *[Handwritten]*



Economato
Unidad Ejecutora de Títulos
Evaluación y Acreditación

Por lo expuesto y en conversación sostenida con Ing. Inelda Martillo, Jefa División Centro de Cómputo, quien indicó haber aclarado a Lic. Diocelina Cedeño, que el servidor de dominio, exclusivamente sirve para tener un respaldo de información, irremplazable desde todo punto y de valor académico únicamente, para la Facultad y la Universidad, haciendo hincapié, en que las órdenes dictaminadas, por toda autoridad (en este caso decanato) deben ser simplemente **acatadas**, sin formular comentarios inexactos, propiciando desasosiego y vacilación; por lo cual, Ing. Martillo concluyó que la autorización sea actualizada y ejecutada.

Para finalizar, se resalta el hecho de que, los datos de los equipos ingresados, se encuentran respaldados a través de este servidor de dominio, lo cual brinda además de la funcionalidad (suprime la movilización a cada departamento para realizar un respaldo), ofrece la seguridad de conservar (evitando que servidor alguno extraiga información) y rescatar (en caso de daño de los computadores), para lo cual se recomienda dar el respectivo mantenimiento, así como aumentar la capacidad de almacenamiento a 10 TB, para lo cual se deberán comprar los respectivos discos duros.

Agradeciendo su digna atención a la presente.

Atentamente

Ing. Carlos A. Ruiz Berna, Msc.
Director

| Elaborado por | FUNCIONARIO RESPONSABLE | CARGO | FECHA |
|--------------------------|---------------------------------|----------|-------|
| Revisado y Aprobado por: | Ing. Carlos A. Ruiz Berna, Msc. | Director | |

10.9. Anexo I

Comunicado al Ingeniero Carlos Ruiz.

En el presente comunicado se establece los motivos por los cuales se hace inviable la instalación del servidor de dominio en el complejo norte de la Facultad.



10.10. Anexo J

10.10.1. Creación de políticas de red

Paso 1: Acceder a administrador del servidor en la opción AD DS

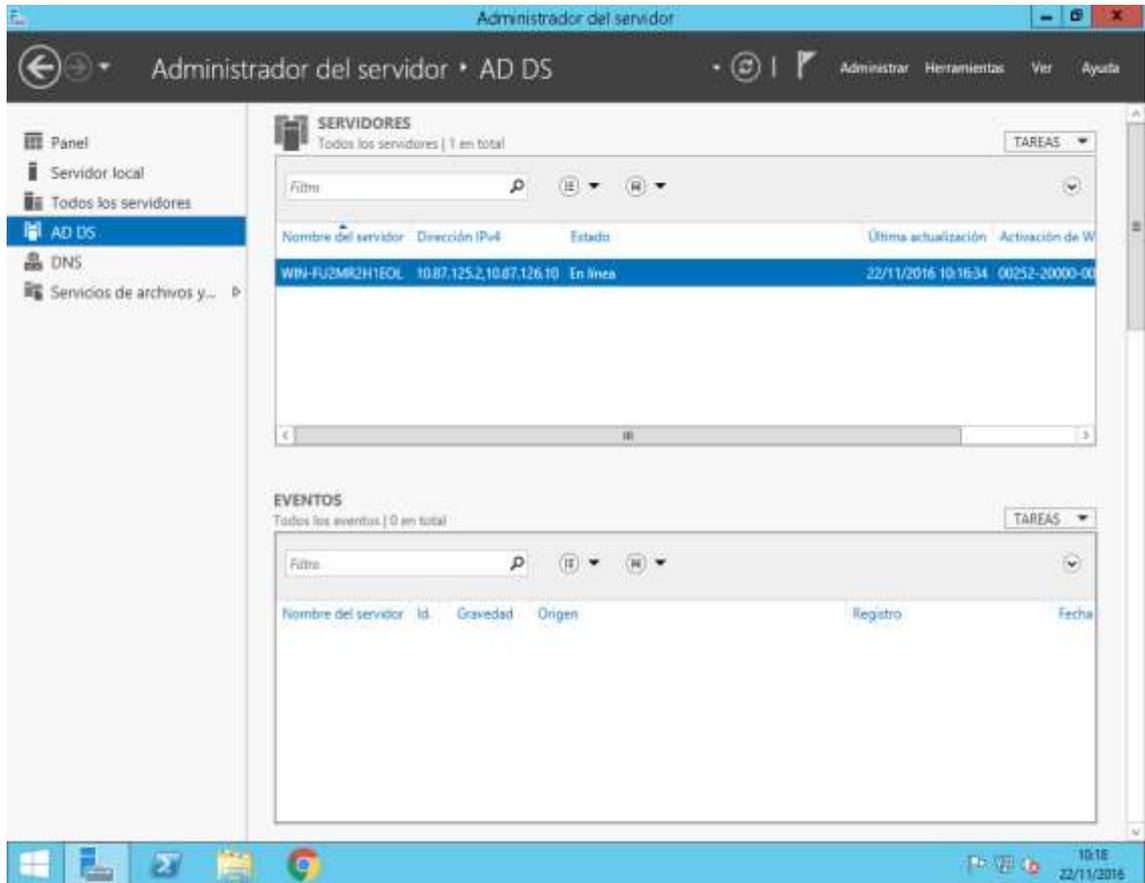


Figura 96: Acceso a la opción AD DS.

Fuente: Directorio Activo.

Paso 2: Clic en la opción Herramientas – Administración de directivas de grupo.

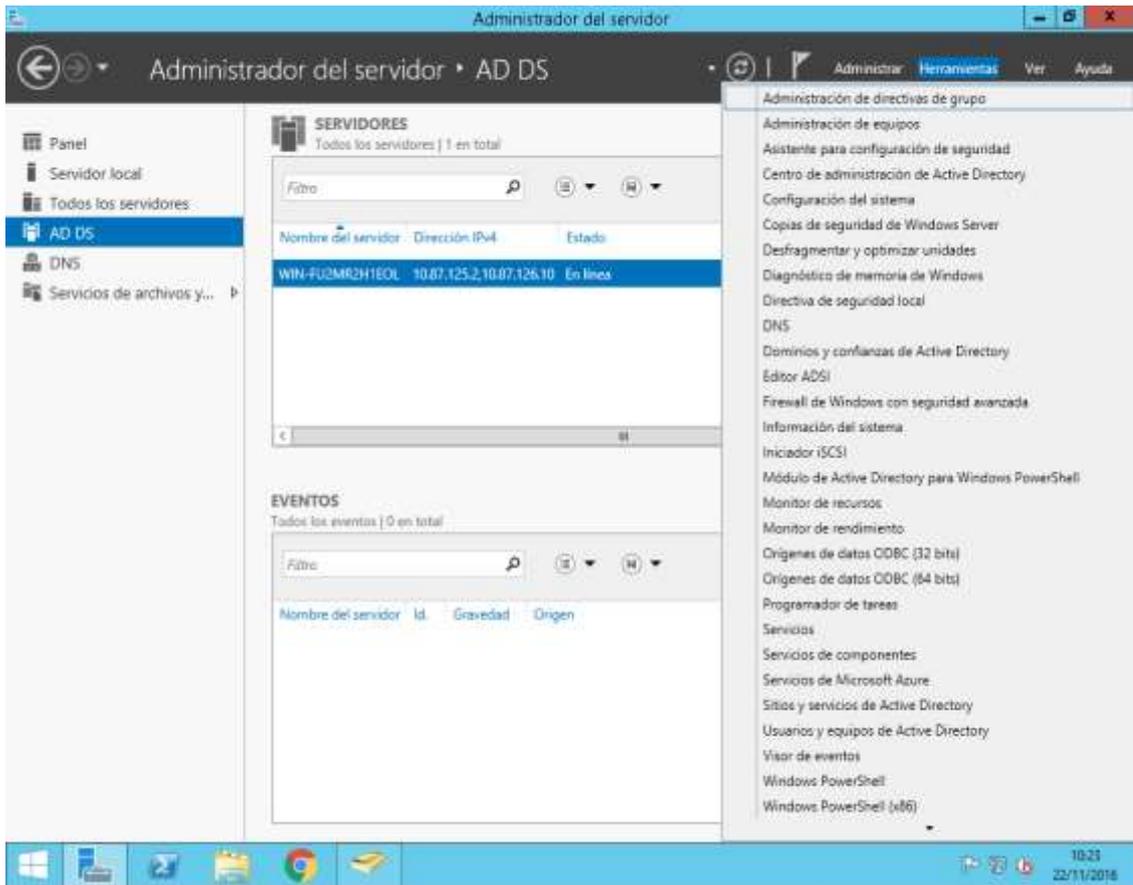


Figura 97: Opción Herramientas Administrativas:

Fuente: Directorio Activo.

Paso 3: Seleccione la unidad organizativa y creamos un Grupo de Políticas de Objeto (GPO).

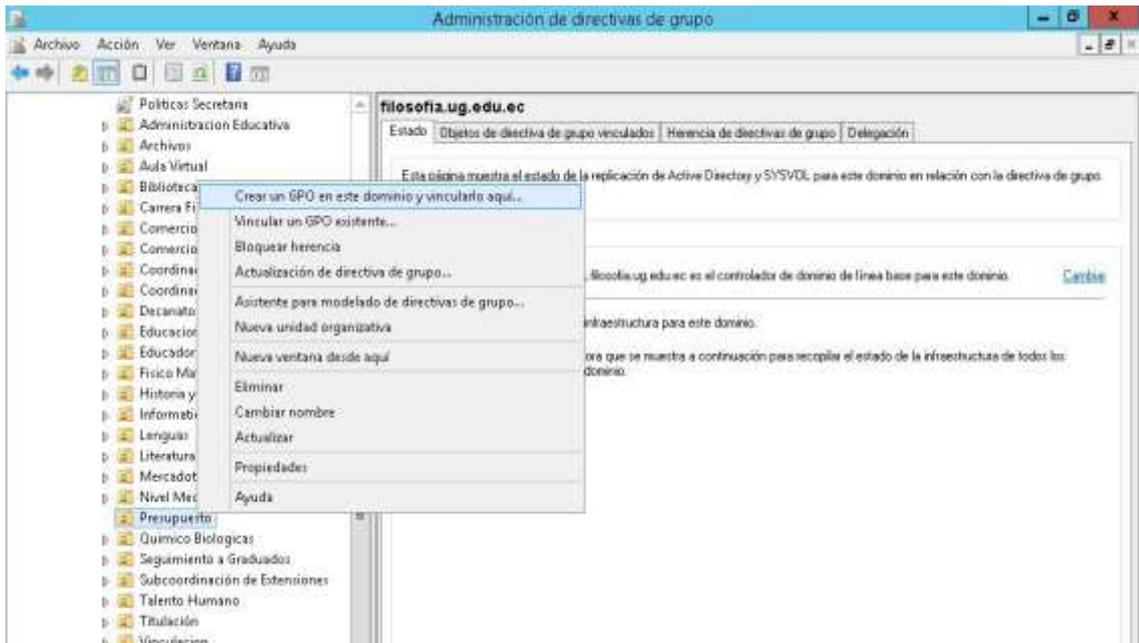


Figura 98: Crear GPO.
Fuente: Directorio Activo.

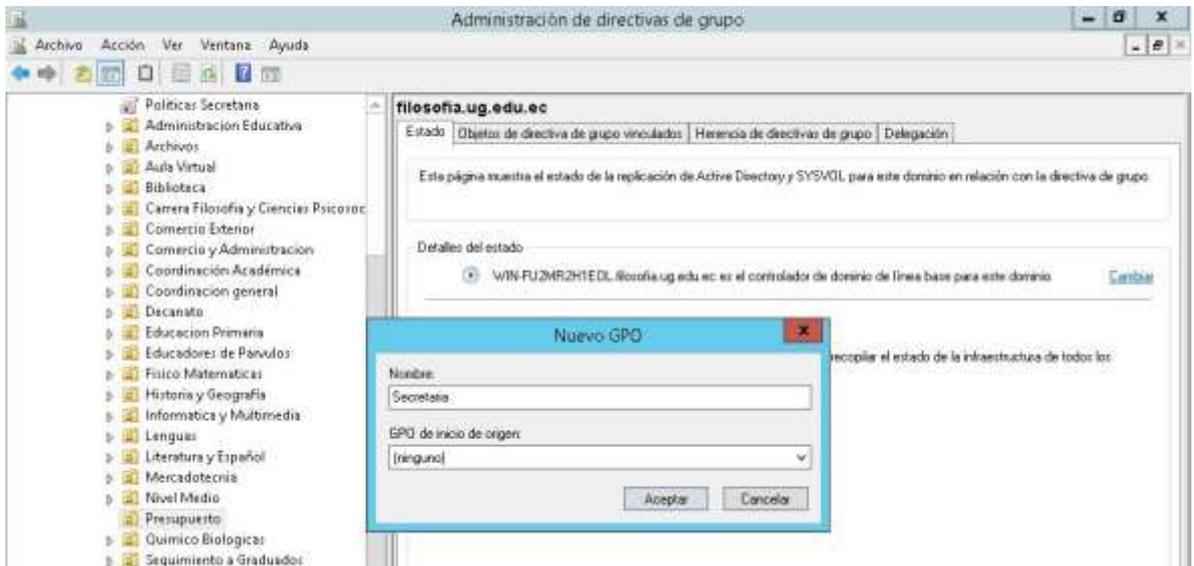


Figura 99: Crear GPO.
Fuente: Directorio Activo.

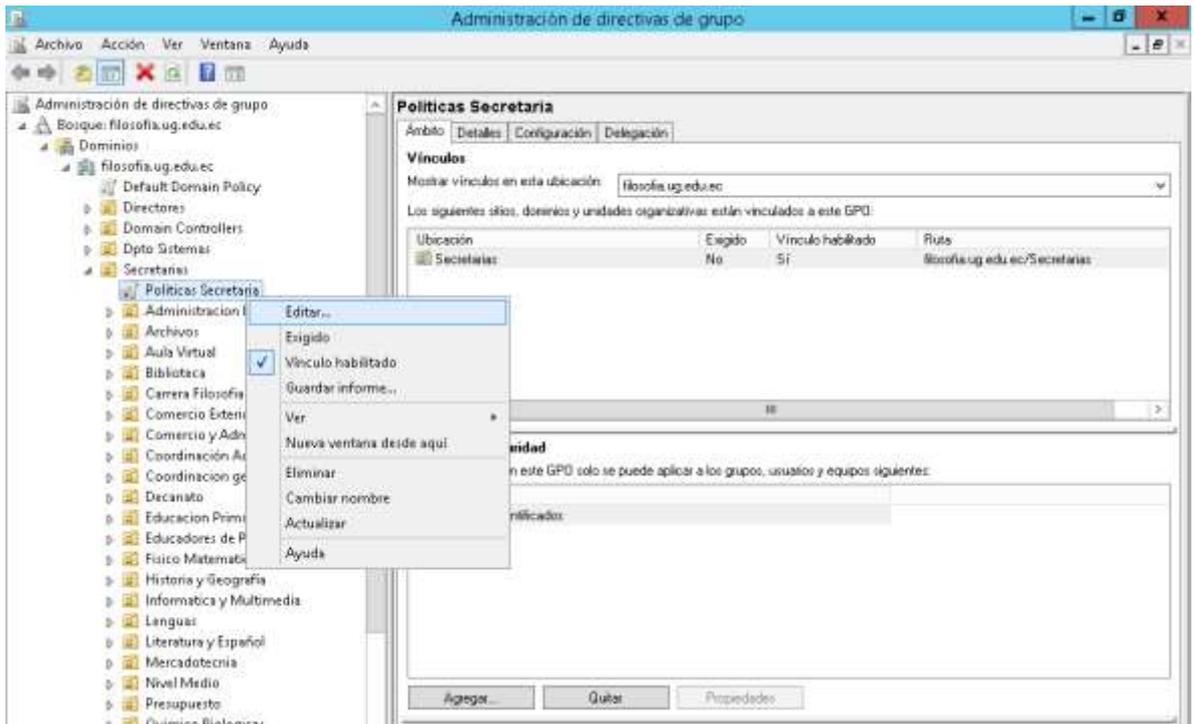


Figura 100: Crear GPO.

Fuente: Directorio Activo.

Paso 4: Seleccione dentro de Configuración de usuario – Directivas – Plantillas administrativas.

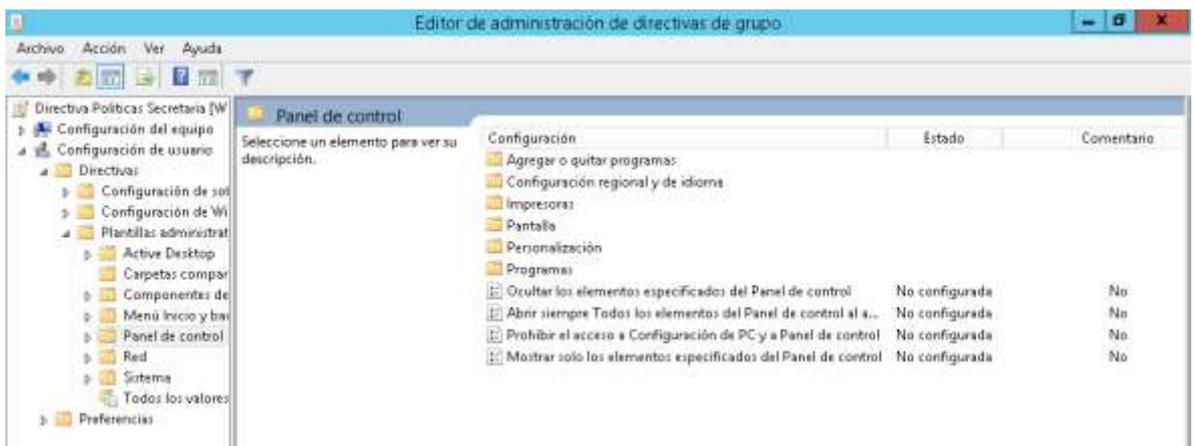


Figura 101: Opción plantillas administrativas.

Fuente: Directorio Activo.

Paso 5: Desde este punto se puede escoger entre las diferentes opciones que da la administración de directivas y establecer las políticas dependiendo de la unidad organizativa.

Para el caso de bloqueo de panel de control se da clic en Plantillas Administrativas – Panel de Control. Se encontrará las opciones que se puede habilitar/deshabilitar.

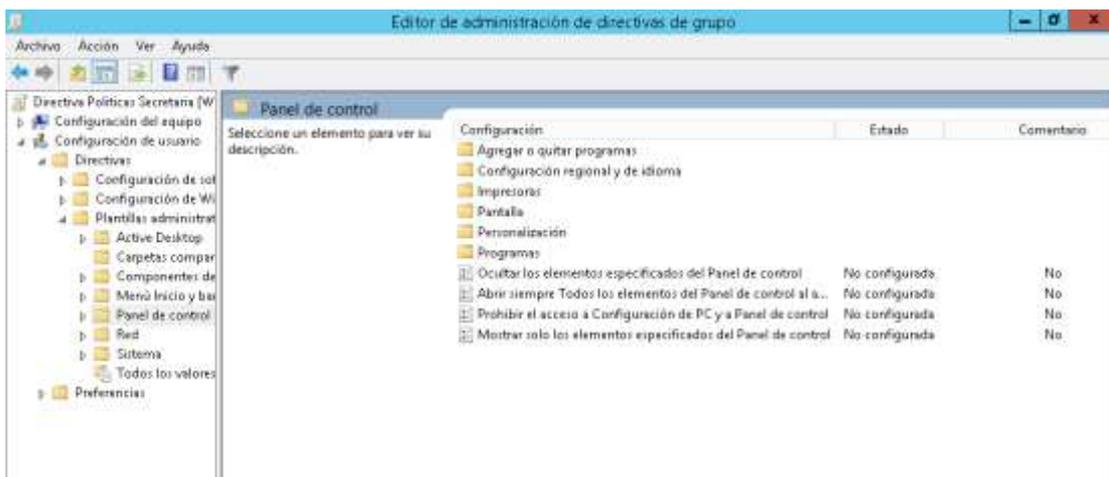


Figura 102: Bloqueo Panel de Control.

Fuente: Directorio Activo.

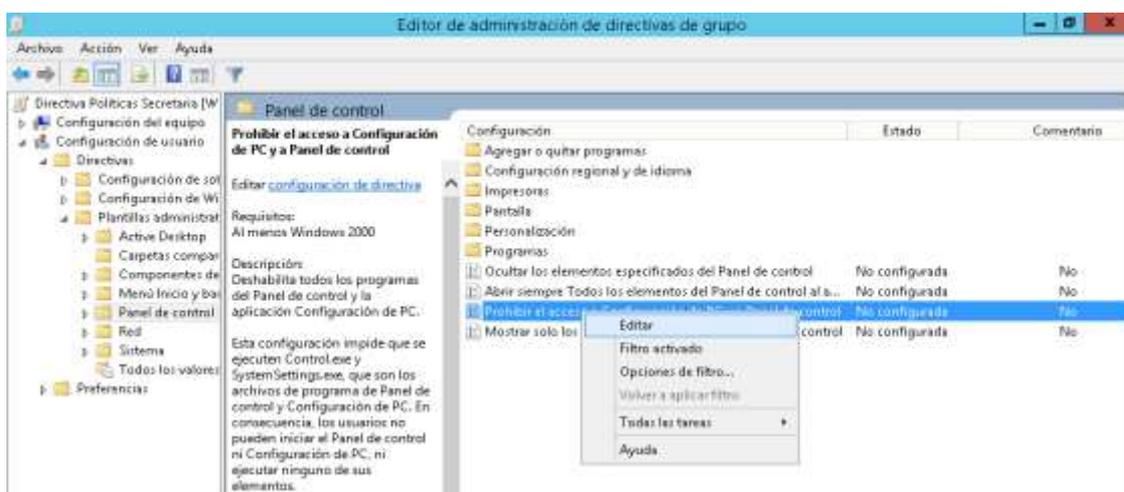


Figura 103: Bloqueo Panel de Control.

Fuente: Directorio Activo.

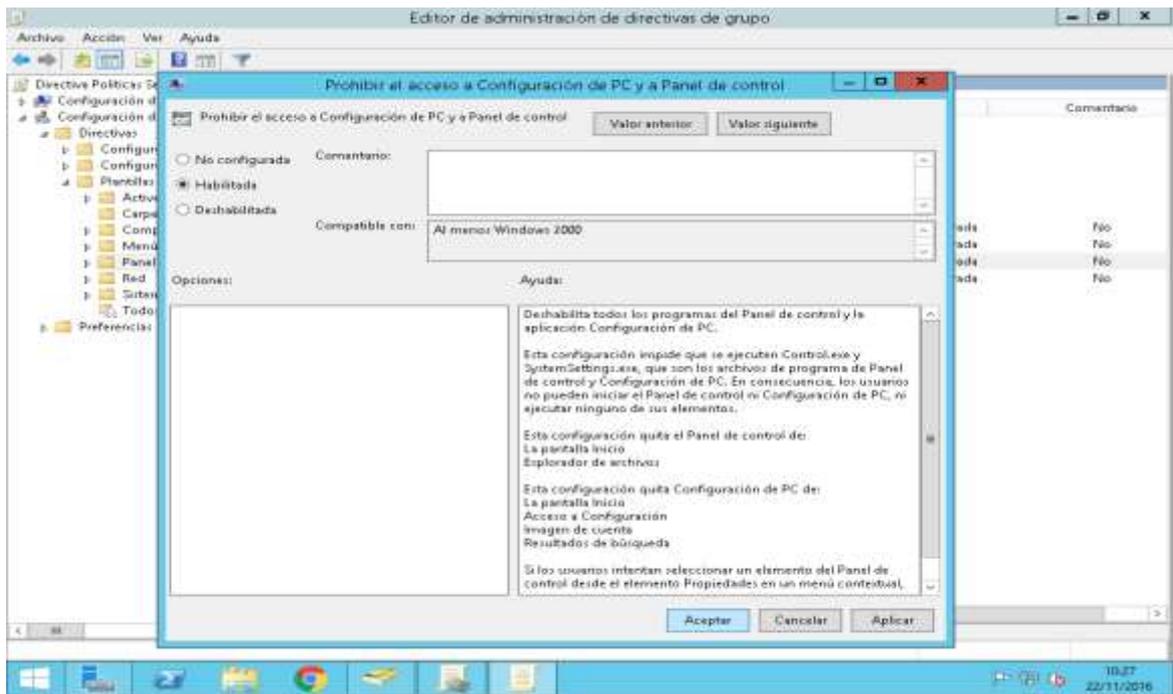


Figura 104: Bloqueo Panel de Control.

Fuente: Directorio Activo.

Prueba en una de las máquinas:



Figura 105: Bloqueo Panel de Control.

Fuente: Directorio Activo.

Para inhabilitar el acceso a Pendrive se da clic en Sistema - Acceso de almacenamiento – Discos extraíbles. Se da clic en editar. Se habilita la opción y Aceptar.



Figura 106: Bloqueo Discos extraíbles.

Fuente: Directorio Activo

Prueba del bloqueo en una máquina.

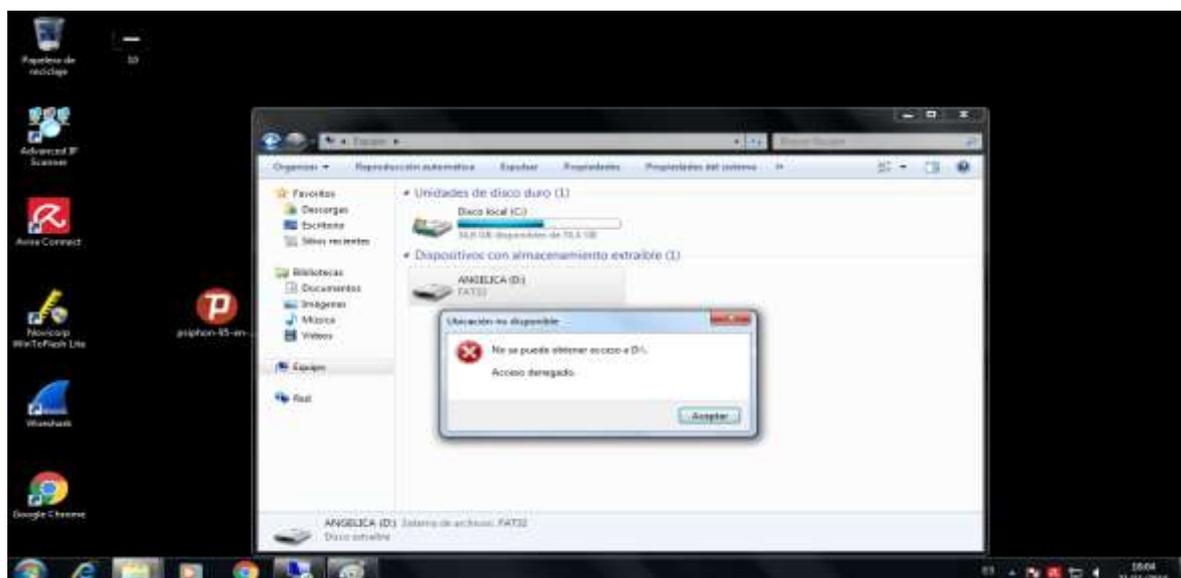


Figura 107: Bloqueo Discos extraíbles.

Fuente: Directorio Activo.

Para la política de fondo de pantalla se da clic en Active Desktop – Habilitar Active Desktop. Clic derecho y escoger editar.

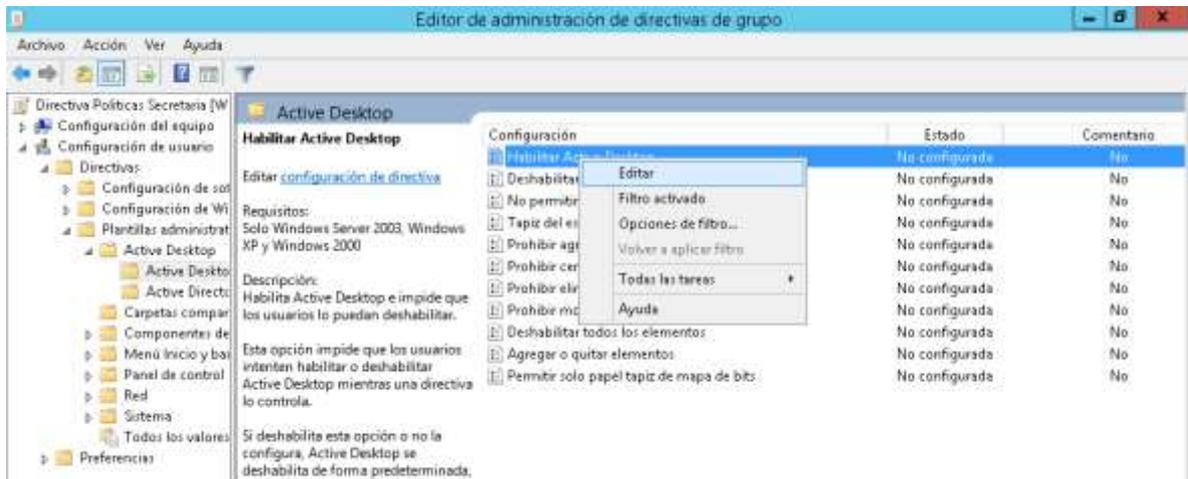


Figura 108: Política Fondo de pantalla.

Fuente: Directorio Activo.

Se habilita la opción y clic en aceptar.

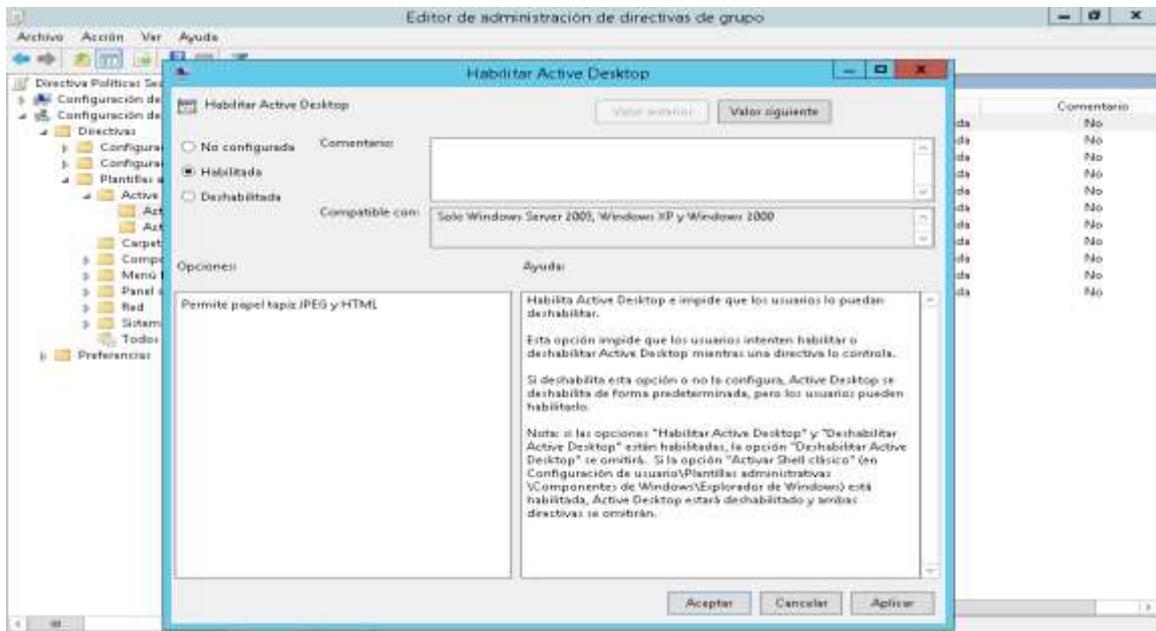


Figura 109: Política Fondo de pantalla.

Fuente: Directorio Activo.

Después se selecciona Tapiz del escritorio - clic derecho – Editar.

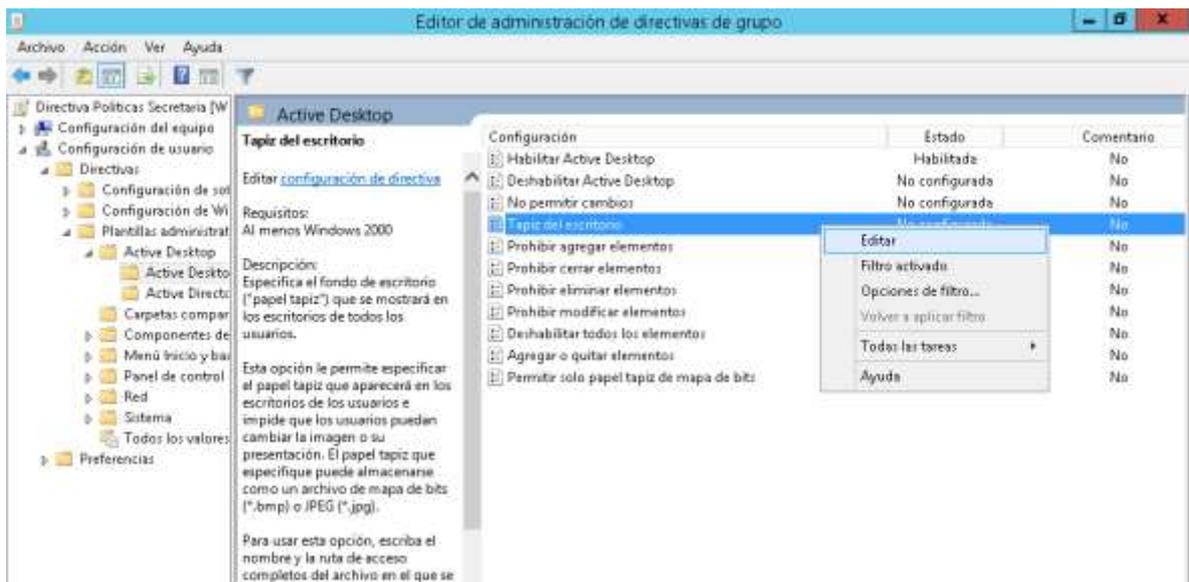


Figura 110: Política Fondo de pantalla.

Fuente: Directorio Activo.

Se habilita la política y en el recuadro de opciones en Nombre del papel tapiz se pega la ruta de la imagen seleccionada como fondo. Clic en aceptar.



Figura 111: Política Fondo de pantalla.

Fuente: Directorio Activo.

Pruebas del fondo establecido.

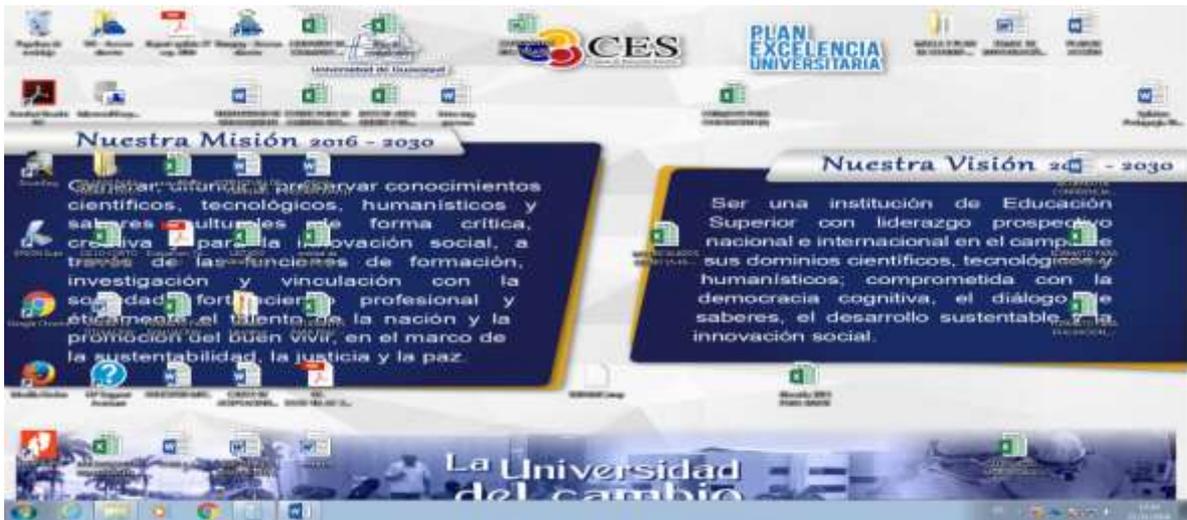


Figura 112: Política Fondo de pantalla.

Fuente: Directorio Activo.

Para bloquear el acceso a las propiedades de la red se da clic en Directivas – Plantillas administrativas – Red – Conexiones de red – Prohibir el acceso a las propiedades de una conexión LAN, se escoge editar.

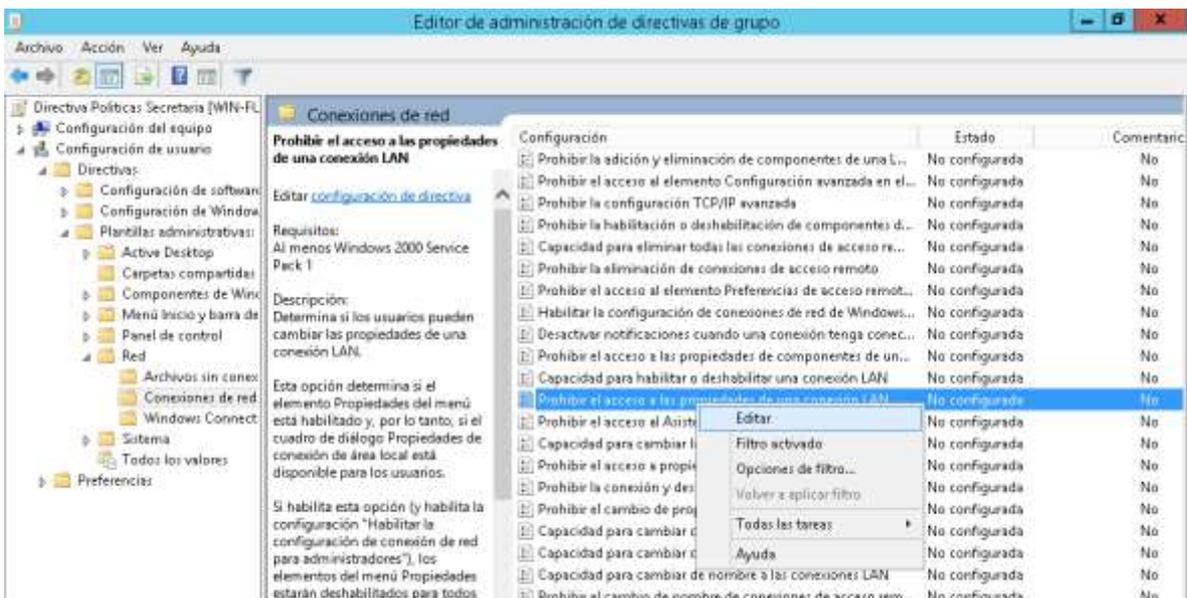


Figura 113: Política Propiedades de la red.

Fuente: Directorio Activo.

Se lo habilita y de da clic en aceptar

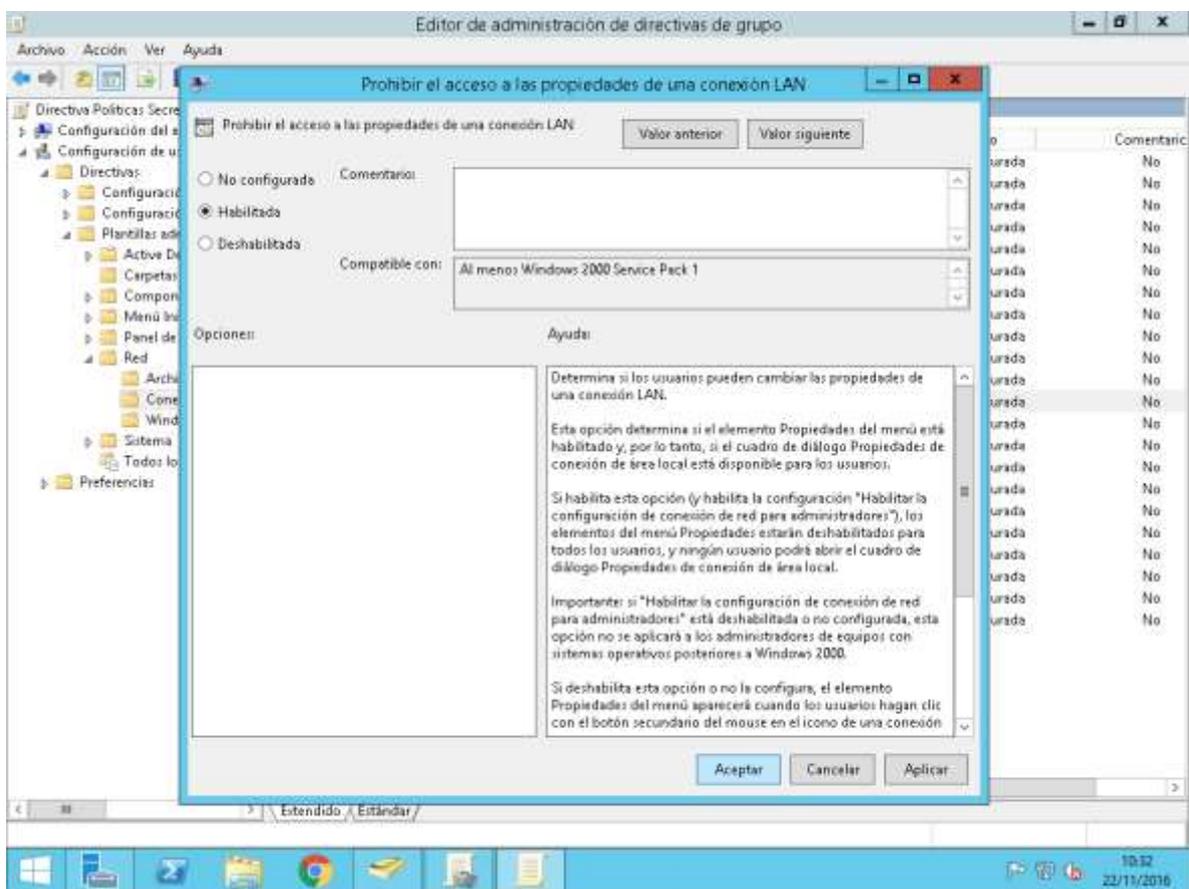


Figura 114: Política Propiedades de la red.

Fuente: Directorio Activo.

Prueba de que se bloquea las propiedades de red

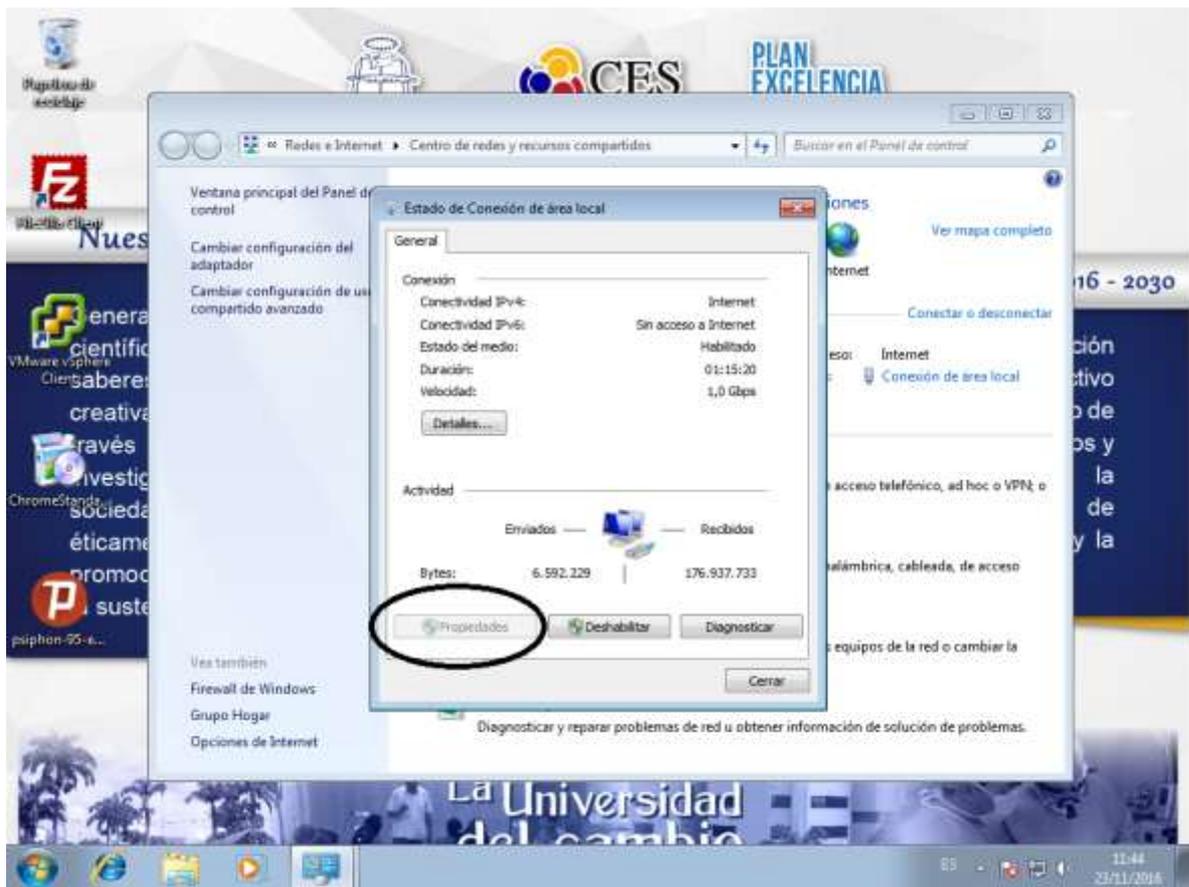


Figura 115: Política Propiedades de la red.

Fuente: Directorio Activo.

Para bloquear aplicaciones que son prohibidas en la institución, se da clic derecho en Directivas – Configuración de Windows – Directivas de restricción de software, y se elige Nuevas directivas de restricción de software

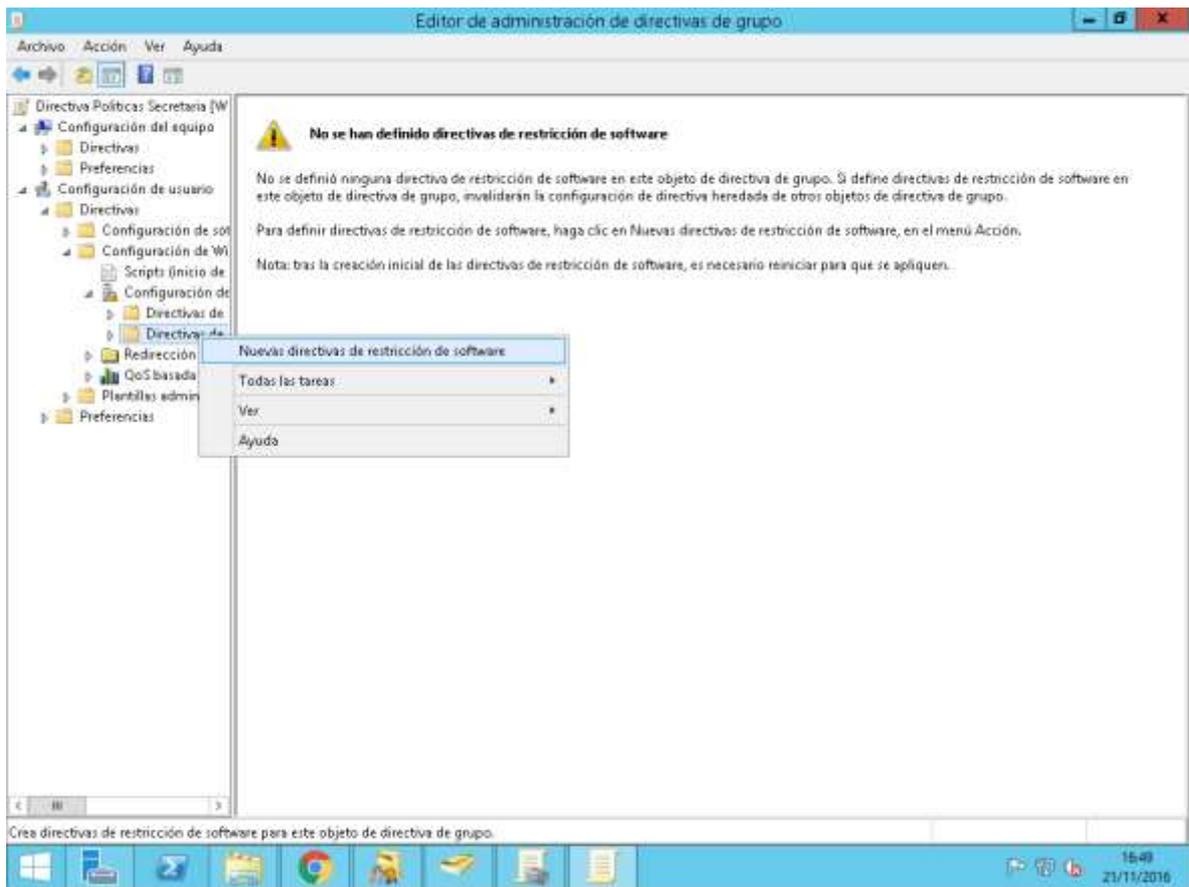


Figura 116: Política Restricción de software.

Fuente: Directorio Activo.

Clic en Regla de nuevo hash

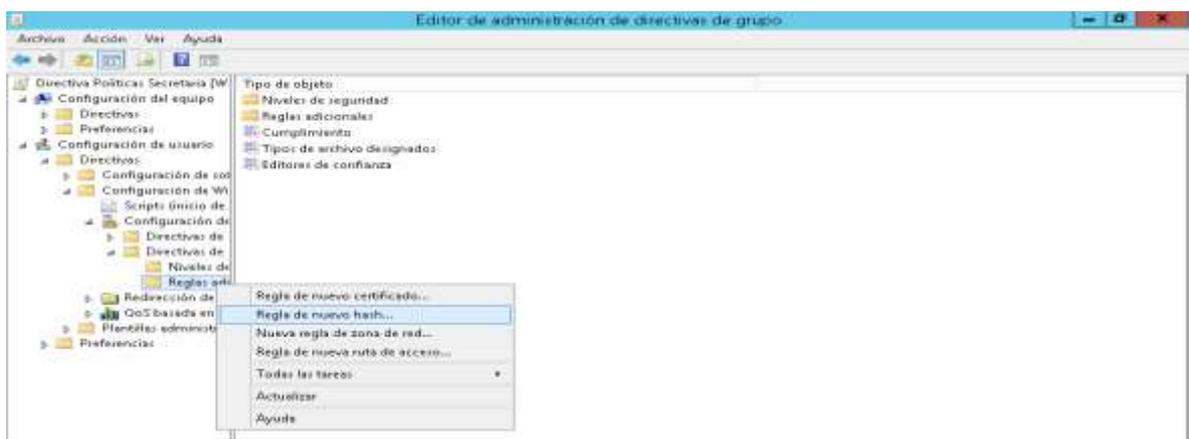


Figura 117: Política Restricción de software.

Fuente: Directorio Activo.

Se procede a elegir la aplicación que se desea bloquea y se da clic en aceptar.

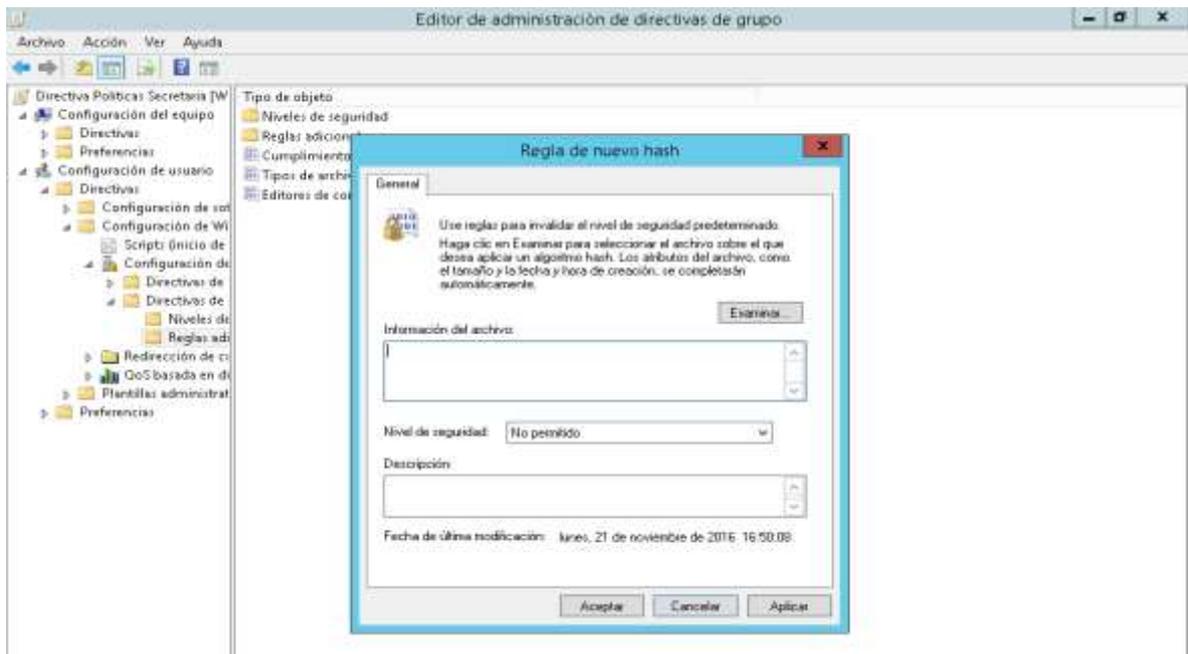


Figura 118: Política Restricción de software.

Fuente: Directorio Activo.

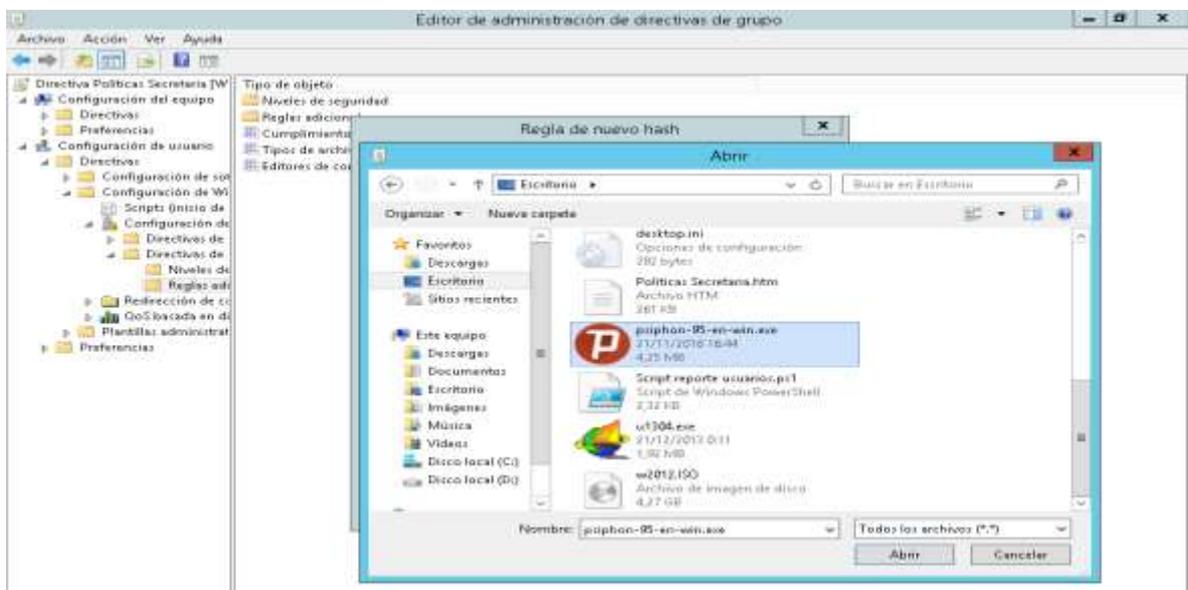


Figura 119: Política Restricción de software.

Fuente: Directorio Activo.

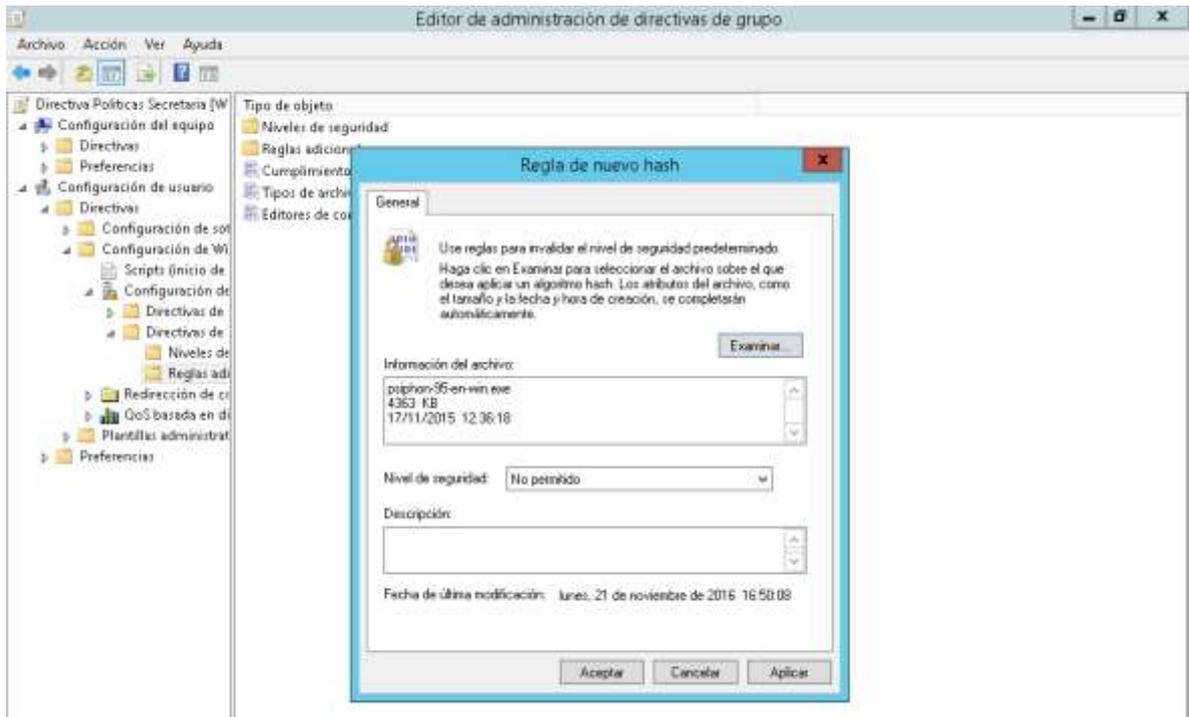


Figura 120: Política Restricción de software.

Fuente: Directorio Activo.

Pruebas del bloqueo

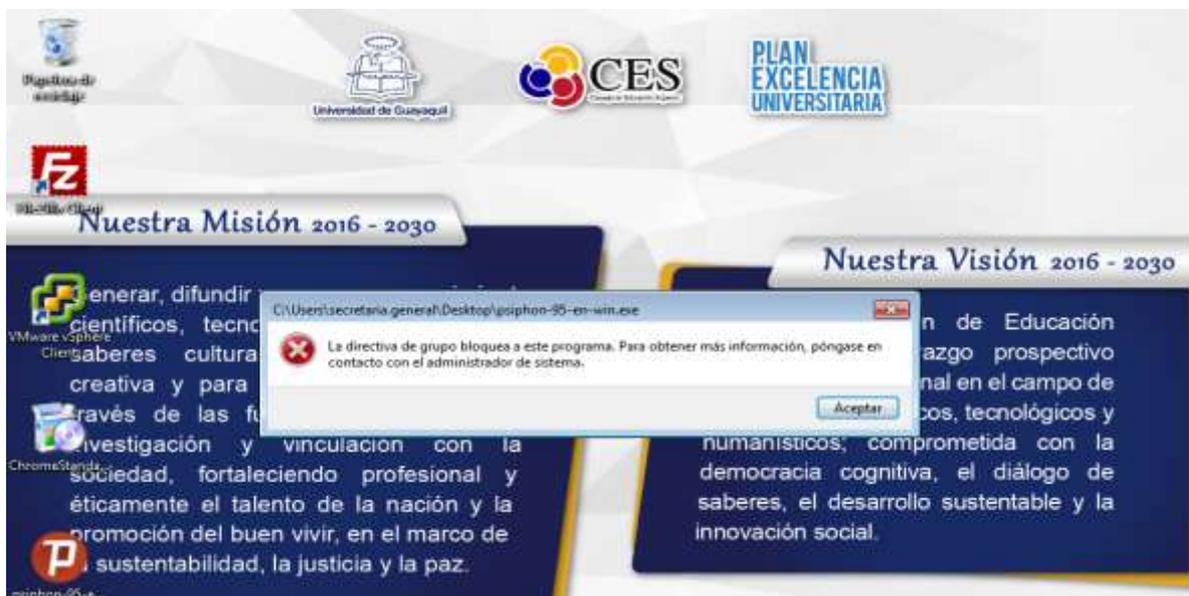


Figura 121: Política Restricción de software.

Fuente: Directorio Activo.

10.11. Anexo K

10.11.1. Asignación de usuarios a las computadoras

Paso 1: Se ingresa al Active Directory, se elige el usuario, se da clic sobre el mismo y se elige Propiedades

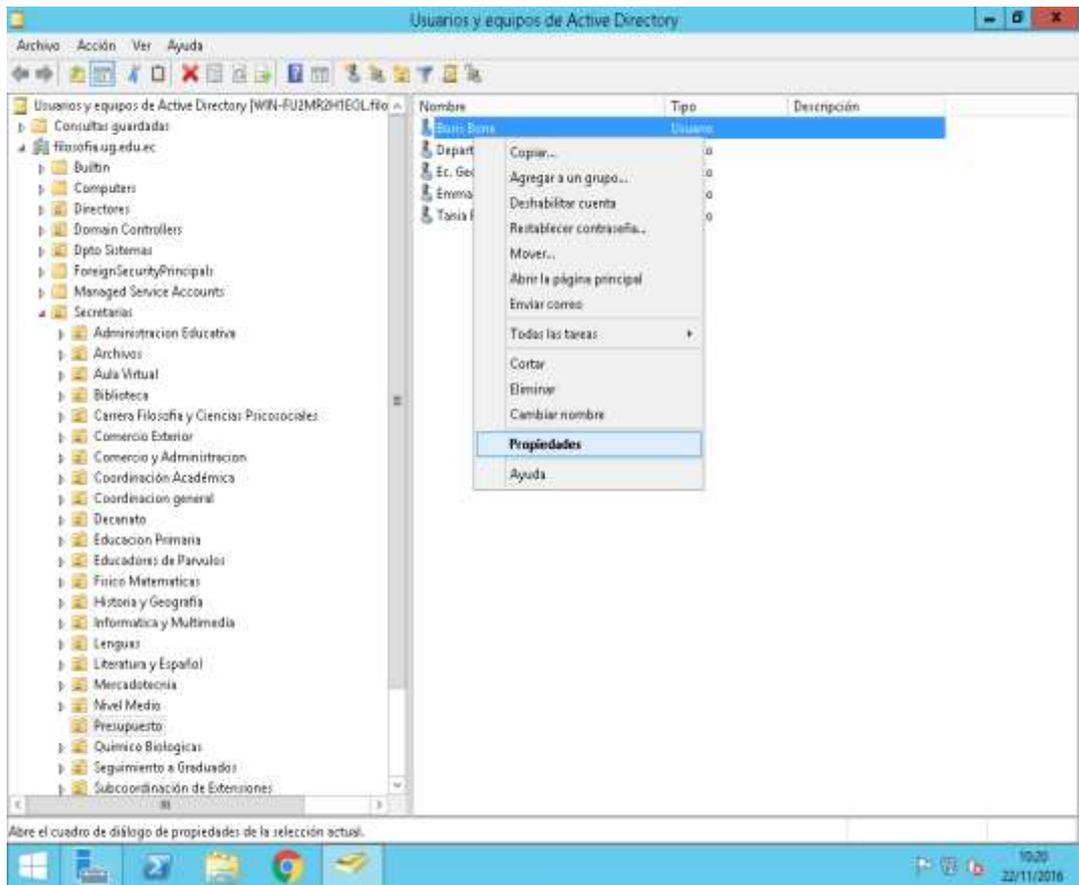


Figura 122: Asignación de usuarios.

Fuente: Directorio Activo.

Paso 2: Se escoge la pestaña Cuenta y se da clic sobre **Iniciar sesión en..**

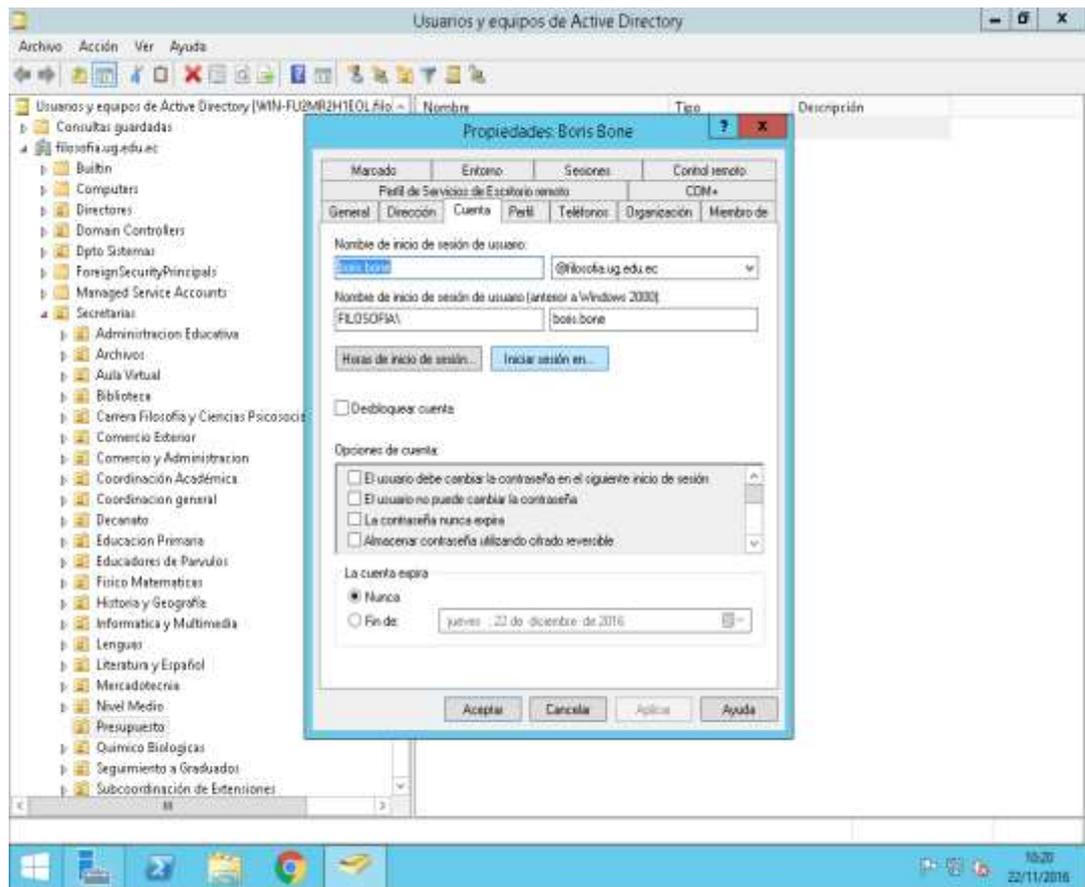


Figura 123: Asignación de usuarios.

Fuente: Directorio Activo.

Paso 3: Se elige la opción **Los siguientes equipos**, se escribe el nombre del equipo y se da clic en agregar – aceptar.

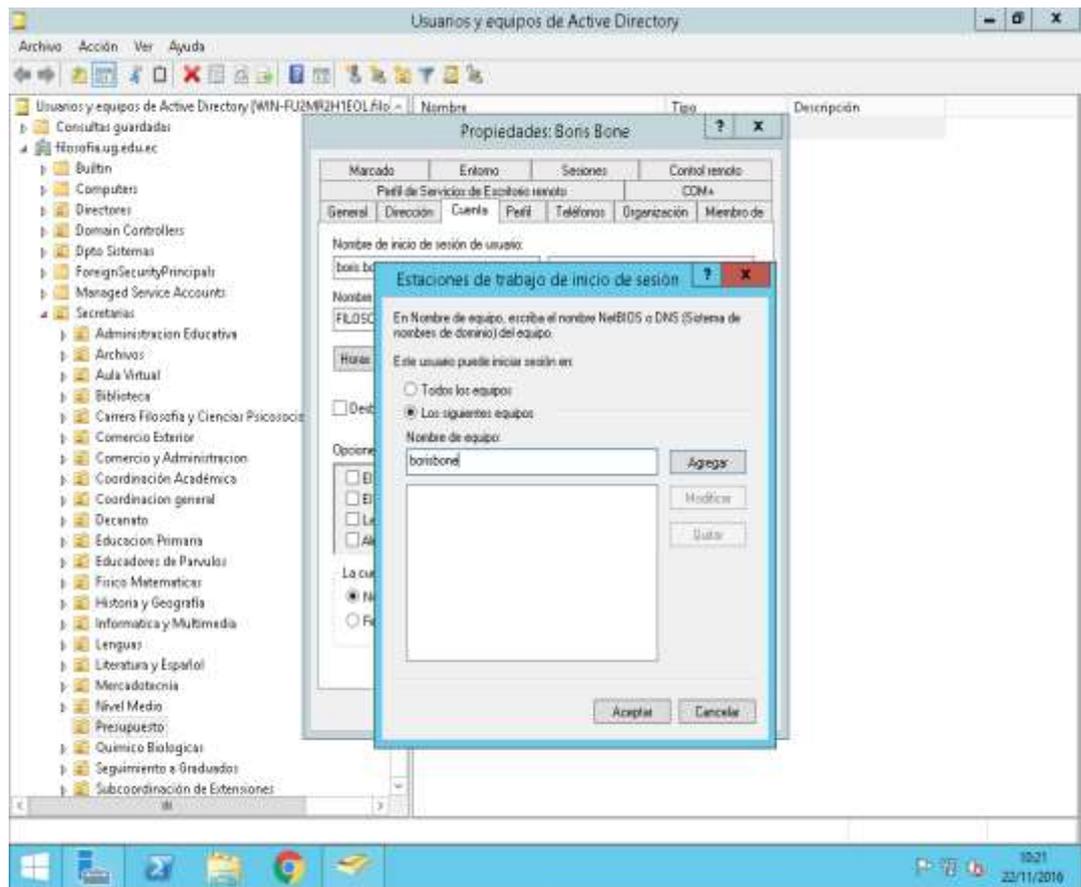


Figura 124: Asignación de usuarios.

Fuente: Directorio Activo.

Paso 4: Se hace la prueba iniciando sesión en otro equipo



Figura 125: Asignación de usuarios.

Fuente: Directorio Activo.

Se observa que no permite iniciar sesión en otro equipo del dominio.

10.12. Anexo L

Entrevista detallada al Ing. Carlos Ruiz Berna

Conforme a lo detallado en la fase de planeación del proyecto, se llevó a cabo una reunión con el Director del departamento de sistemas de la Facultad de Filosofía. En esta reunión se toparon los puntos que se mencionan a continuación:

- Problemas encontrados en la red de la Facultad.
- Necesidades del departamento de sistemas.
- Políticas establecidas por la Facultad a sus empleados.
- Alcances del proyecto.

Por medio de las siguientes preguntas se reconocieron los problemas, el personal encargado para la administración de la red y los alcances del proyecto en la Facultad:

- ¿Cuáles son las funciones encargadas al departamento de Sistemas en la actualidad?
- ¿Cómo está estructurada la red de la Facultad de Filosofía?
- ¿Cuántas sedes posee la Facultad de Filosofía?
- ¿Con que herramientas cuenta para la administración de la red?
- ¿Quién es el personal encargado del área de redes y el área técnica?
- ¿Qué servicios provee actualmente?
- ¿Qué problemas se han encontrado en la administración de los equipos provistos a los usuarios?
- ¿Qué y cuantos dispositivos de red posee la Facultad?
- ¿Cuáles son las políticas aplicadas a la Facultad a nivel interno de la red?
- ¿Qué políticas se desea aplicar y el motivo?
- ¿Cuáles son las limitantes encontradas para el correcto cumplimiento de las funciones del departamento de sistemas?
- ¿Qué necesidades se va a cubrir con el proyecto?
- ¿Cuáles son los alcances del proyecto?
- ¿Qué seguridades se le provee a la red de la Facultad actualmente?