

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

Disertación teórica aplicada

Propuesta para la Detección de Problemas de Seguridad en Redes LAN y WLAN para el LTIC con Herramientas de Administración WEB

Saúl Lozada Enríquez

Directora de Tema de Tesis

Ing. Suyana Arcos

Revisores

Ing. Beatriz Campos

Ing. Javier Cóndor

2014

Agradecimientos

A Dios, mis padres, y mis hermanos, pues han sido el soporte de cada momento de mi vida y han estado a mi lado de manera incondicional.

A la Pontificia Universidad Católica del Ecuador, su personal administrativo, profesores y alumnos por haberme brindado la oportunidad de compartir su tiempo, conocimientos y amistad.

A la Ing. Suyana Arcos por haberme brindado su tiempo y experiencia para guiar mi trabajo de tesis, ya que todo el tiempo ha sabido ser más que maestra en todo mi carrera una amiga.

A mis maestros, grandes personas y sobre todos amigos, Ing. Beatriz Campos y el Ing. Xavier Cóndor.

A todos mis compañeros con quienes hemos compartido aula y amistad por brindarme su apoyo y compañerismo dentro y fuera de la Universidad.

Tabla de contenido

Declaración 2

Agradecimiento 3

Tabla de Contenidos 4

Índice de Ilustraciones 9

Índice de Tablas 11

Introducción 12

CAPITULO I **13**

1. Problema de investigación 13

1.1. Planteamiento del Problema 13

1.1.1. Sujeto del Problema 14

1.1.2. El objeto de la Investigación 14

1.1.3. Delimitación de Teoría 14

1.1.4. Delimitación de Tiempo 14

1.1.5. Delimitación de Espacio 14

1.2. Objetivos 14

1.2.1. Objetivo General 14

1.2.2. Objetivos Específicos 15

1.3. Justificación 15

1.4. Alcance 15

1.5. Marco Teórico y Marco Conceptual 16

1.6. Sustento Teórico 16

1.6.1. Que es la Seguridad Informática 16

1.6.2. La Seguridad Lógica y la Seguridad Física 17

1.6.2.1. Seguridad Lógica 17

1.6.2.2. Seguridad Física 18

1.6.2.2.1. Incendios 19

1.6.2.2.2. Seguridad del Equipamiento 19

1.6.2.2.3. Inundaciones 20

1.6.2.2.4. Instalaciones Eléctricas 20

1.6.2.2.5. Picos y Ruidos Electromagnéticos 20

1.6.2.2.6. Cableado 20

1.6.2.2.7. Cableado de Alto Nivel de Seguridad 21

1.6.2.2.8. Pisos y Placas Extraíbles 21

1.6.2.2.9. Sistema de Aire Acondicionado 21
1.6.2.2.10. Emisiones Electromagnéticas 21
1.6.2.2.11. Robo 21
1.6.2.2.12. Fraude 22
1.6.2.2.13. Sabotaje 22
1.6.2.2.14. Control de Acceso 22
1.7. Políticas de Seguridad dentro de un Laboratorio Informático 23
1.8. Protocolos de Red 26
1.8.1. Definición 26
1.8.2. Modelo OSI 26
1.8.3. Pila de Protocolos 26
1.8.4. El Modelo OSI y sus Capas 26
1.8.4.1. Como Trabaja el Modelo de capas OSI 27
1.8.5. Capa Física 28
1.8.6. Capa de enlace de Datos 28
1.8.7. Capa de Red 29
1.8.8. Capa de Transporte 30
1.8.9. Capa de Sesión 30
1.8.10. Capa de Presentación 31
1.8.11. Capa de Aplicación 32
1.8.11.1. Aplicaciones reconocidas por la Red 33
1.8.11.2. Servicios de la Capa de Aplicación 33
1.9. Estructura y Topología de Red 37
1.9.1. Arquitectura Cliente/Servidor 37
1.9.2. Características de la arquitectura Cliente/Servidor 39
1.10. Que es una Topología de Red 40
1.10.1. Topología de Malla 40
1.10.2. Topología de Estrella 41
1.10.3. Topología de Árbol 42
1.10.4. Topología de Bus 42
1.10.5. Topología de Anillo 43
1.10.6. Topología Mixta 44
2. Herramientas de Seguridad Informática 45
2.1. Herramientas de Seguridad para realizar un Scanner en la seguridad de la Red 45

3. Delitos Informáticos 46
3.1. Que es un Delito Informático 46
3.2. Sujeto Activo 46
3.3. Sujeto Pasivo 47
3.4. Tipos de Delito Informático 47
3.4.1. Fraude Informático 47
3.4.1.1. Datos Falsos o Engañosos (Data Diggling) 47
3.4.1.2. Manipulación de programas o “Caballos de Troya” 47
3.4.1.3. Técnica del Salami 47
3.4.1.4. Falsificaciones Informáticas 48
3.4.1.5. Manipulación de los Datos de Salida 48
3.4.1.6. Phising 48
3.4.2. Sabotaje Informático 48
3.4.2.1. Bombas Lógicas (Logic Bomb) 48
3.4.2.2. Gusanos 48
3.4.2.3. Virus Informático y Malware 48
3.4.2.4. Ciberterrorismo 48
3.4.2.5. Ataque denegación de Servicios 49
3.4.3. Espionaje Informático, el robo o hurto de software 49
3.4.3.1. Fuga de Datos (Data Leakage) 49
3.4.3.2. Reproducción no Autorizada de programas informáticos de protección legal 49
3.4.4. Robo de Servicios 49
3.4.4.1. Hurto del tiempos del Computador 49
3.4.4.2. Apropiación de Informaciones Residuales 49
3.4.4.3. Parasito Informático (Piggybacking) y Suplantación de Personalidad (Impersonation) 49
3.4.5. Acceso no Autorizado a Servicios Informáticos 50
3.4.5.1. Puertas Falsas (Trap Doors) 50
3.4.5.2. Llave Maestra (SuperZapping) 50
3.4.5.3. Pinchado en Línea (Wiretapping) 50
3.4.5.4. Piratas Informáticos Hackers y Crackers 50
4. Delitos dentro de un laboratorio Informático 50
5. Delitos Informáticos en el Ecuador 51
6. Normativas que se deben tomar ante la amenaza de un delito informático o violación de Seguridad Informática 53

7. Deficiencias y problemas en la Red LTIC 54
7.1 Visión Global e Histórica del LTIC 54
7.2 Visión del LTIC proyectada a los próximos 2 años 59
CAPITULO II **60**
8. Herramientas de Monitoreo y control para la seguridad de la red del LTIC 60
8.1. Parallels 60
8.1.1. Requerimientos 60
8.1.2. Compatibilidad 61
8.1.3. Sistema operativo 32 bits 61
8.1.4. Sistema operativo 64 bits 62
8.1.5. Características de la Aplicación 62
8.1.6. Plataformas en las que se puede Utilizar 63
8.1.7. Funcionamiento y Pruebas de la Aplicación Parallels 63
8.1.7.1. Instalación de la Aplicación Parallels 63
8.1.7.2. Cláusulas de la instalación y Términos de Licencia 63
8.1.7.3. Aplicación en Sistema Operativo Mac 65
8.1.7.4. Aplicación en Sistemas Operativo Windows 69
8.1.7.5. Aplicación Parallels Mobile 71
8.2. PRTG 75
8.2.1. Requerimientos 75
8.2.2. Compatibilidad 75
8.2.3. Características de la Aplicación 75
8.2.4. Plataformas en las que se puede Utilizar 76
8.2.5. Funcionamiento Y Pruebas de la Aplicación PRTG 76
8.2.5.1. Instalación de la Aplicación PRTG 76
8.3. SpiceWorks 85
8.3.1. Requerimientos 85
8.3.2. Requerimientos de Explorador WEB 86
8.3.3. Compatibilidad 86
8.3.4. Características de la Aplicación 86
8.3.5. Plataformas en las que se puede Utilizar 86
8.3.6. Funcionamiento Y Pruebas de la Aplicación SpiceWorks 86
8.3.6.1. Instalación de la Aplicación SpiceWorks 86

CAPITULO III **96**

9. Obtención de Resultados 96

10. Obtención de Resultados con la Herramienta SpiceWorks 96

10.1. Análisis y Pruebas con la Herramienta SpiceWorks 96

10.2. Scan e Identificación de equipos 97

10.3. Identificación de Problemas 98

10.4. Identificación de Software 99

10.5. Monitoreo de Dispositivos Externos 99

10.6. HelpDesk 100

10.6.1. Equipos y Usuarios que están dentro de nuestra Red 100

10.7. Reportes SpiceWorks 101

10.8. Grupos 102

11. Obtención de Resultados con la Herramienta PRTG 103

11.1. Análisis y Pruebas con la Herramienta PRTG 103

11.2. Análisis de pruebas Aula 203 – semana del 11 al 19 de abril 103

11.3. Análisis de pruebas Aula 203 – semana del 19 al 26 de abril 107

CAPITULO IV **108**

12. Síntesis de resultados obtenidos con la Propuesta para la detección de problemas de seguridad en la red del LTIC 108

CAPITULO V **108**

13. Conclusiones y recomendaciones 113

13.1. Conclusiones 113

13.2. Recomendaciones 114

14. Bibliografía 116

Índice de ilustraciones

ILUSTRACIÓN 1: MODELO OSI. REFERENCIA: HTTP://WWW.TEXTOSCIENTIFICOS.COM/REDES/TCP-IP/COMPARACION-MODELO-OSI 27

ILUSTRACIÓN 2: GRAFICO 2 ENTORNO FÍSICO DE RED. REFERENCIA: HTTP://WWW.TEXTOSCIENTIFICOS.COM/REDES/TCP-IP/ENTORNO -DE-RED/MODELO-OSI 27

ILUSTRACIÓN 3: TRAMA ETHERNET. REFERENCIA: HTTP://INTERNETT.GALEON.COM/REDES.HTM 29

ILUSTRACIÓN 4: COMUNICACIÓN CAPA DE SESIÓN: REFERENCIA: HTTP://TELEMATICA-JOCASOFT.BLOGSPOT.COM/2010/05/CAPA-DE-SESION.HTML 31

ILUSTRACIÓN 5: CAPA DE APLICACIÓN – SERVIDORES. REFERENCIA: EXPLORATION CCNA1 33

ILUSTRACIÓN 6: PROCESO DE SOFTWARE – CAPA DE APLICACIÓN. REFERENCIA: EXPLORATION CCNA1 34

ILUSTRACIÓN 7: SERVICIOS – CAPA DE APLICACIÓN. REFERENCIA: EXPLORATION CCNA1 34

Ilustración 8: Operaciones de sistema – Capa de Aplicación. Referencia: Exploration CCNA1 35
Ilustración 9: Programa – Capa de Aplicación. Referencia: Exploration CCNA1. 35
Ilustración 10: Conexión de interfaz entre redes humanas y de datos. Referencia: Exploration CCNA1 36
Ilustración 11: Protocolos en la capa de Aplicación. Referencia: Exploration CCNA1.. 37
Ilustración 12: Modelo Cliente-Servidor/ Proceso de descarga. Referencia: Exploration CCNA1 ... 38
Ilustración 13: Modelo Cliente-Servidor/ Proceso de carga. Referencia: Exploration CCNA1 39
Ilustración 14: Topología de Malla. Referencia: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red. 40
Ilustración 15: Topología de estrella. Referencia: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red 41
Ilustración 16: Topología de Árbol. Referencia: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red 42
Ilustración 17: Topología de Bus. Referencia: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red. 43
Ilustración 18: Topología de Anillo. Referencia: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red 43
Ilustración 19: Topología Mixta. Referencia: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red 44
Ilustración 20: Ventana Instalación Parallels referencia: proceso de instalación Parallels. Autor: Saúl lozada. 59
Ilustración 21: Ventana contenido instalación Parallels Lozada referencia proceso de instalación Parallels. Autor: Saúl lozada. 59
Ilustración 22: Licencia Parallels. Autor: Saúl lozada 60
Ilustración 23: Términos de aceptación Licencia Parallels. Autor: Saúl lozada. 60
Ilustración 24: Icono de la Aplicación Parallels. Autor: Saúl lozada. 61
Ilustración 25: Ventana de activación del producto. Autor: Saúl lozada. 61
Ilustración 26: Venta de asistente de creación de máquina virtual. Autor: Saúl lozada.. 62
Ilustración 27: Creación de máquina virtual Window 7. Autor: Saúl lozada..... 62
Ilustración 28: Creación de máquina virtual Window 7. Autor: Saúl lozada..... 62
Ilustración 29: Ventana de máquinas virtuales existentes. Autor: Saúl lozada..... 63
Ilustración 30: Sistemas Operativos máquina virtual Parallels. Autor: Saúl lozada.. 63
Ilustración 31: Procesos de Virtualización con Parallels. Autor: Saúl lozada. 64
Ilustración 32: Ventana de instalación Paralles Windows. Autor: Saúl lozada. 65
Ilustración 33: Ventana de activación Parallels. Autor: Saúl lozada 65
Ilustración 34: Ventanas de instalación Creación de máquina virtual. Autor: Saúl lozada 66
Ilustración 35: Botones control máquina virtual Parallels. Autor: Saúl lozada..... 66
Ilustración 36: Ventana de virtualización. Autor: Saúl lozada 67
Ilustración 37: Aplicación Parallels en Mobile. Autor: Saúl lozada 68
Ilustración 38: Ventana de ingreso aplicación Parallels Mobile Autor: Saúl lozada 68
Ilustración 39: Máquinas virtuales aplicación Mobile. Autor: Saúl lozada. 69
Ilustración 40: Mandos de control aplicación Mobile. Autor: Saúl lozada. 69
Ilustración 41: Virtualización en Mobile. Autor: Saúl lozada. 70
Ilustración 42: Instalación de PRTG. Autor: Saúl lozada.. 72
Ilustración 43: Proceso de instalación PRTG. Autor: Saúl lozada. 73

Ilustración 44: Proceso de instalación y aceptación Licencia PRTG. Autor: Saúl lozada.. 73
Ilustración 45: Proceso de instalación PRTG. Autor: Saúl lozada. 74
Ilustración 46: Proceso de instalación PRTG. Autor: Saúl lozada.. 74
Ilustración 47: Configuración PRTG. Autor: Saúl lozada. 75
Ilustración 48: Procesos de instalación PRTG. Autor: Saúl lozada. 76
Ilustración 49: Procesos de instalación PRTG. Autor: Saúl lozada 76
Ilustración 50: Icono de control de PRTG en Windows. Autor: Saúl lozada 77
Ilustración 51: Ventana PRTG. Autor: Saúl lozada 77
Ilustración 52: Mensaje de control no autorizado en PRTG, error de conexión. Autor: Saúl lozada 77
Ilustración 53: Opciones de configuración conexión con PRTG. Autor: Saúl lozada 78
Ilustración 54: configuración de IP, puerto nombre de registro contraseña id raíz para conexión PRTG. Autor: Saúl lozada 78
Ilustración 55: Ventana de conexión PRTG configurada. Autor: Saúl lozada 78
Ilustración 56: Ventana de acceso web PRTG. Autor: Saúl lozada 79
Ilustración 57: Vista monitoreo y grafico de tráfico de la Red. Autor: Saúl lozada 80
Ilustración 58: Ventana de control PRTG. Autor: Saúl lozada 81
Ilustración 59: Ventana de instalación Spiceworks. Autor: Saúl lozada 83
Ilustración 60: Ventana de instalación Spiceworks, aceptación de términos. Autor: Saúl lozada.... 83
Ilustración 61: Proceso de instalación Spiceworks. Autor: Saúl lozada. 84
Ilustración 62: Proceso de arranque de la plataforma Spiceworks. Autor: Saúl lozada 85
Ilustración 63: Plataforma Web Spiceworks. Autor: Saúl lozada.. 86
Ilustración 64: Plataforma Web Spiceworks, configuración de cuenta. Autor: Saúl lozada. 86
Ilustración 65: Ventana de ingreso Spiceworks. Autor: Saúl lozada.. 87
Ilustración 66: Ventana de control interfaz Web Spiceworks. Autor: Saúl lozada. 87
Ilustración 67: Identificador de sistema Operativos y antivirus. Autor: Saúl lozada.. 88
Ilustración 68: Identificador de arquitecturas con la que contamos. Autor: Saúl lozada. 88
Ilustración 69: Identificador de errores y advertencias. Autor: Saúl lozada. 89
Ilustración 70: Identificador de dispositivos conectados a nuestra red. Autor: Saúl lozada 89
Ilustración 71: Información relevante de nuestro equipo mediante inventory – Spiceworks. Autor: Saúl lozada 90
Ilustración 72: Alertas y actualizaciones de nuestro equipo mediante inventory – Spiceworks. Autor: Saúl lozada 90
Ilustración 73: Reporte de software con el que contamos en nuestros equipos. Autor: Saúl lozada 91
Ilustración 74: Reporte de capacidad en disco con la que contamos. Autor: Saúl lozada 91
Ilustración 75: Pantalla Spiceworks información servidor. Autor: Saúl lozada 92
Ilustración 76: Pantalla Spiceworks información equipo por icono. Autor: Saúl lozada 92
Ilustración 77: Sumario de software Spiceworks. Autor: Saúl lozada 93
Ilustración 78: Dispositivo externo – monitoreo Spicework de Impresora. Autor: Saúl lozada 95
Ilustración 79: Pantalla de reportes Spiceworks. Autor: Saúl lozada..... 96
Ilustración 80: Archivo reporte PDF. Autor: Saúl lozada 97
Ilustración 81: Grupos en Spiceworks. Autor: Saúl lozada. 98
Ilustración 82: GRAFICOS DE OBTENCIÓN DE RESULTADOS HERRAMIENTA PRTG NETWORK MONITOR AULAS 203 y 204

. AUTOR: SAÚL LOZADA. ..... 103 AL 114

Índice de tablas

TABLA 1: CUADRO DE PROCEDIMIENTO PENAL CPP REFERENCIA: DELITOS PENALES E INFORMÁTICOS FISCALÍA GENERAL DEL ESTADO DEL ECUADOR AUTOR: SAÚL LOZADA 52
TABLA 2: DISTRIBUCION IP'S MAQUINAS AULA 203 AUTOR: SAÚL LOZADA 94
TABLA 3: DISTRIBUCION IP'S MAQUINAS. AULA 204 AULA 203. AUTOR: SAÚL LOZADA..... 94
TABLA 4 : TABLA COMPARATIVA HERRAMIENTAS WEB INVESTIGACIÓN. AUTOR: SAÚL LOZADA 99

Introducción.-

Hoy en día la mayoría de laboratorios de ingeniería constan con equipos, software y tecnología de última generación, con el objetivo de lograr cumplir las normas esénciales y poder dar un servicio óptimo para cada una de las tareas que se encuentra conformado en el campo de la informática.

Pero debido a la creciente índice de violaciones en la seguridad informática y a su vez el aumento de personas con más conocimientos informáticos y que hacen mal uso de estas facultades; se ha generado optar por otro tipo de medidas más profundas respeto al monitoreo de nuestra seguridad informática.

Tal como es nuestro caso de estudio, el LTIC, el mismo que presta un servicio de calidad a cada uno de los estudiantes de la facultad de Ingeniería en sistemas y a su vez a los estudiantes de Civil. El mismo que día a día ha mejorado sus equipos, sistemas operativos, software, conocimientos tecnología e información, pero aun no es suficiente.

Un estudio exhaustivo respecto a las deficiencias y necesidades del LTIC, en base a la detección de problemas de seguridad en su red LAN y WLAN es nuestro enfoque principal.

El LTIC en cada uno de sus semestres y años laborables ha sufrido algunos inconvenientes, podría decirse hasta ataques contra su red y a su vez contra las políticas de seguridad con las que esta se maneja.

Este tipo de situaciones han provocado que el servicio que presta se vea afectado y que en cierto momento se haya dado el reclamo por parte de los estudiantes así como de los maestros que hacen uso de las instalaciones.

Entre estos podemos referir: nombres y claves de usuarios afectadas o no existentes, problemas en el ingreso a sistema por parte de estudiantes y maestros, falta de privilegios para ciertas aplicaciones para maestros, inconvenientes con la conexión y la velocidad de nuestra red al momento de ingresar a la internet, cambios en las políticas de seguridad por personas no autorizadas al LTIC, no tener un respectivo mantenimiento y control en nuestros equipos y servidores.

El LTIC, sin embargo trata de solventar todas estas necesidades por el momento, ya que todo este conjunto de inconvenientes se dan todos los días de trabajo.

La presente investigación practica propone fortalecer todo el campo de seguridad de esta red, enfocando su estudio a los equipos con los que se trabaja, los sistemas operativos, programas, protocolos y políticas de seguridad y aplicar en base a las pruebas y monitoreo que vamos a realizar para crear la respectiva documentación en base a la propuesta que nos permitirá la detección y prevención de problemas de seguridad a corto y largo plazo en nuestro laboratorio.

Capítulo I

1. Problema de la Investigación.

1.1. Planteamiento del problema.

Hoy en día la mayoría de laboratorios de ingeniería constan con equipos, software y tecnología de última generación, con el objetivo de lograr cumplir las normas esénciales y poder dar un servicio óptimo para cada una de las tareas que se encuentra conformado en el campo de la informática.

Pero debido a la creciente índice de violaciones en la seguridad informática y a su vez el aumento de personas con más conocimientos informáticos y que hacen mal uso de estas facultades; se ha generado optar por otro tipo de medidas más profundas respeto al monitoreo de nuestra seguridad informática.

Tal como es nuestro caso de estudio, el LTIC, el mismo que presta un servicio de calidad a cada uno de los estudiantes de la facultad de Ingeniería en sistemas y a su vez a los estudiantes de Civil. El mismo que día a día ha mejorado sus equipos, sistemas operativos, software, conocimientos tecnología e información, pero aun no es suficiente.

Un estudio exhaustivo respecto a las deficiencias y necesidades del LTIC, en base a la detección de problemas de seguridad en su red LAN y WLAN es nuestro enfoque principal.

El LTIC en cada uno de sus semestres y años laborables ha sufrido algunos inconvenientes, podría decirse hasta ataques contra su red y a su vez contra las políticas de seguridad con las que esta se maneja.

Este tipo de situaciones han provocado que el servicio que presta se vea afectado y que en cierto momento se haya dado el reclamo por parte de los estudiantes así como de los maestros que hacen uso de las instalaciones.

Entre estos podemos referir: nombres y claves de usuarios afectadas o no existentes, problemas en el ingreso a sistema por parte de estudiantes y maestros, falta de privilegios para ciertas aplicaciones para maestros, inconvenientes con la conexión y la velocidad de nuestra red al momento de ingresar a la internet, cambios en las políticas de seguridad por personas no autorizadas al LTIC, no tener un respectivo mantenimiento y control en nuestros equipos y servidores.

El LTIC, sin embargo trata de solventar todas estas necesidades por el momento, ya que todo este conjunto de inconvenientes se dan todos los días de trabajo.

La presente investigación practica propone fortalecer todo el campo de seguridad de esta red, enfocando su estudio a los equipos con los que se trabaja, los sistemas operativos, programas, protocolos y políticas de seguridad y aplicar en base a las pruebas y monitoreo que vamos a realizar para crear la respectiva documentación en base a la propuesta que nos permitirá la detección y prevención de problemas de seguridad a corto y largo plazo en nuestro laboratorio.

1.1.1. Sujeto del Problema.-

El sujeto del problema es el LTIC y su personal, es aquí donde parte nuestro tema de estudio, hay que mirar más a fondo ya que no solo esta entidad trabaja autónomamente, si no que el personal con el que cuenta debe estar capacitado y tener todo el conocimiento necesario para que se preste un servicio de calidad.

1.1.2. El objeto de la investigación.-

Es la falta de seguridad en el LTIC que conllevan a no poder detectar y prevenir los problemas con la seguridad de la red.

1.1.3. Delimitaciones de Teoría.-

La información tiene que ser SELECTIVA, EXHAUSTIVA, y CRÍTICA.

Para el desarrollo del planteamiento del problema utilizaremos un conjunto de técnicas que nos faciliten su elaboración como son: entrevista a expertos, uso de herramientas específicas y que se enfoquen en el monitoreo y seguridad de una red informática, pruebas y recolección de datos, lecturas bibliografía, resúmenes, citas textuales y si es necesario una bitácora para llevar nuestra información diaria o semanal.

1.1.4. Delimitaciones de Tiempo.-

El tiempo en el que está estimado realizar y plantear la Propuesta para la detección de problemas de seguridad en redes LAN y WLAN para el LTIC con herramientas de Administración WEB son unos 3 meses.

1.1.5. Delimitaciones de espacio.-

El espacio en el que se va a desarrollar es en una red privada para hacer las pruebas iniciales, para la recolección de datos y su respectivo monitoreo y en el LTIC para su implantación.

1.2. Objetivos.

1.2.1. Objetivo General.-

- Desarrollar la Propuesta para la detección de problemas de la seguridad en redes LAN y WLAN para el LTIC, a través de la implementación y uso de herramientas de administración WEB multiplataforma.

1.2.2. Objetivos Específicos.-

1. Inspeccionar el área física de trabajo, para poder tener la respetiva información sobre las herramientas con las que contamos, tanto, equipos, plataformas y su respectiva compatibilidad.
2. Analizar la infraestructura de redes LAN y WLAN del LTIC, para visualizar las necesidades de seguridad y conectividad entre múltiples plataformas.
3. Gestionar y adquirir todos los conocimientos sobre los protocolos de seguridad y administración que se manejen en el LTIC.
4. Realizar el estudio y pruebas respectivas de las herramientas WEB con las que contaremos para el desarrollo de nuestra investigación.

5. Aplicar las respectivas y adecuadas técnicas de investigación para que a través de las pruebas y resultados de las herramientas WEB implementadas podamos desarrollar completa y correctamente la propuesta para la prevención de problemas de seguridad en la red LTIC.
6. Explorar nuevos mecanismos y herramientas multiplataforma para el desarrollo de la Propuesta que nos permita la detección de problemas en la red del LTIC.
7. Realizar la documentación en base a la propuesta para la prevención de problemas de seguridad en la red LTIC.

1.3. Justificación.

Actualmente con el avance tecnológico apresurado y los constantes cambios que conlleva la tecnología, vemos que la seguridad es un problema de hoy en día, para lo cual nosotros tenemos que estar presentes o no para dar soluciones eficaces.

En base a lo citado, podemos ver que gracias a esta propuesta se puede hacer frente a cada una de las problemáticas de la seguridad en redes LAN y WLAN que se den dentro del LTIC, sea aplicando herramientas multiplataforma, así como se puede gestionar herramientas basadas en la WEB, y gracias a esto tener un acceso total desde cualquier punto que se pueda conectar a nuestra red.

1.4. Alcance.

La presente disertación de grado culminará con la entrega del documento sobre la Propuesta para la detección de problemas de seguridad en redes LAN y WLAN para el LTIC, utilizando herramientas de Administración WEB. Además se documentaran las pruebas realizadas y resultados obtenidos.

1.5. Marco Teórico y Marco Conceptual.

a) Antecedentes o Marco referencial.

Podemos citar que durante años se ha intentado reforzar la seguridad informática en los diferentes lugares de trabajo tanto como empresas privadas y estatales, compañías y laboratorios.
De esta forma cada una de estas entidades ha trabajado, cuidando y respaldando su información, pero sin tener un control exacto ni un monitoreo de lo que pasa el día a día, podría decirse con sus respectivas redes informáticas y a su vez con sus equipos y software.

En lo que a nuestro tema nos concierne, el LTIC durante todos los años que tiene de funcionamiento no ha tenido un control exhaustivo respecto a un monitoreo y menos a la prevención o detección de problemas de seguridad en su red, ya que no se ha utilizado ningún sistema de monitoreo o control respetivo para sus equipos y su red.

Analizar las necesidades que el laboratorio conlleva, además de los respectivos problemas que ha tenido en consideración a que sus políticas de seguridad algún momento se vieron afectadas, se realizara la respectiva investigación con el fin de brindar un mejor servicio y tener un mayor control en la seguridad de su red.

b) Marco Teórico.

La seguridad dentro de un espacio de trabajo es primordial para que podamos brindar un servicio de calidad y sobre todo podamos estar al tanto en cada uno de los aspectos con los cuales contamos que pueden estar desde el nivel más bajo hasta el nivel más complejo.

Tratándose en nuestro campo de la seguridad informática debemos ver mucho más allá, para lo cual debemos además de tener equipos y tecnología que nos facilite nuestras tareas, contar con un conjunto de herramientas que nos permitan tener un control total y poder determinar cada uno de los posibles y latentes problemas dentro de nuestra red.

c) Marco Conceptual.

La seguridad informática dentro de nuestro lugar de trabajo, el laboratorio LTIC, durante años ha tenido que lidiar con problemas en la seguridad de su red, de la misma forma que no se ha podido determinar de una manera más exacta y completa, en que le afecta ya que no se ha contado con herramientas para el monitoreo y control de su seguridad y más aún que puedan utilizarse vía WEB para su facilidad. Además de darle la respectiva solución.

1.6 Sustento Teórico.

1.6.1. Qué es la Seguridad Informática.

La Seguridad Informática conlleva un sin número de técnicas, aplicaciones y dispositivos que nos permiten garantizar que los recursos informáticos dentro de una institución o compañía estén disponibles para cumplir con sus propósitos, así como la información tenga su integridad y privacidad ante factores externos que pueden alterar su esencia o que pueden dañarla.

En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

Es muy importante citar que la seguridad informática es parte tanto de las empresas, instituciones o compañías así también como de sus miembros o usuarios, para lo cual si se habla de seguridad informática, se debe tener responsabilidad y dar el conocimiento oportuno respecto de todas las normas y políticas de seguridad, como grupo.

Dentro de una empresa o institución, citando el caso de la seguridad dentro del laboratorio de informática LTIC, se pude decir que es imposible lograr un sistema que sea ciento por ciento seguro, pero mediante las políticas de seguridad que se establezcan dentro de nuestro laboratorio, las herramientas de software como firewall, antivirus etc., y en el caso de estudio, la propuesta de aplicar herramientas de administración WEB para el monitoreo de cada uno de los equipos con los que contamos podremos evitar daños y problemas que puedan ocasionar posibles intrusos.

En nuestro laboratorio la información es primordial, ya que se trabaja y se presta un servicio día a día, por lo que nuestra información es el elemento principal a proteger, resguardar y recuperar dentro de nuestra red LTIC.

Respecto al estudio de la Seguridad Informática podemos clasificarla respecto a la naturaleza de la amenaza en dos tipos:

1.6.2 La Seguridad lógica y la Seguridad Física.

1.6.2.1 Seguridad Lógica.

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Esto se puede dar con el uso de aplicaciones para la seguridad, herramientas de software, antivirus, firewall, etc., con el objetivo de resguardar y proteger nuestra información.

Todo lo que no está permitido debe estar prohibido y esto es lo que debe asegurar la Seguridad Lógica.

Para la Seguridad Lógica se plantean y se deben respetar estos puntos:

1. Restringir el acceso a los programas y archivos.

2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

3. Asegurar que se estén utilizados los datos, archivos y programas correctos y por el procedimiento correcto.

4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

5. Que la información recibida sea la misma que ha sido transmitida.

6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

7. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Además de estos puntos dentro de la Seguridad Lógico, debe existir un control de acceso para lo que respecta a nuestra red, y en el caso del laboratorio LTIC.

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario, constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de aplicación o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) además de resguardar la información confidencial de accesos no autorizados.

En el LTIC, tenemos un servidor de usuarios y un servidor de archivos respectivamente, los mismos que trabajan en conjunto con nuestro Dominio INGENIERIA.

Para nuestro control de acceso tenemos una clasificación en nuestros usuarios, los cuales son administradores, ayudantes y becarios, personal docente, y estudiantes (Sistemas y Civil).

Dentro nuestro Dominio INGENIERIA, los identificadores de acceso que utilizaremos para los usuarios son los siguientes:

Estudiantes (Sistemas y Civil): primera letra del primer nombre, primera letra de segundo nombre, primer apellido y primera letra del segundo apellido.

Por ejemplo: Olmedo Saúl Lozada Enríquez = oslozadae

Para la autentificación con una clave inicial, ingresando el número de cédula, que luego deberá cambiarse una clave personal por parte de cada uno de los alumnos.

Los únicos que tienen acceso total son los administradores del servidor.

El LTIC posee roles para cada uno de los usuarios, cada uno tendrá privilegios y restricciones dependiendo el tipo de usuario que sea.

Al igual que las transacciones, también pueden implementarse controles a través de las transacciones, por ejemplo, solicitando una clave al requerir el procesamiento de una transacción determinada.

Y las Limitaciones a los Servicios**,** estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

1.6.2.2. Seguridad Física.

Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos que contienen nuestra información confidencial.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

Entre las amenazas a un centro de cómputo más importantes tenemos las siguientes:

1.6.2.2.1. Incendios.

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es un enemigo de consideración para las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.

- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área de proceso.
- Deben usarse muebles incombustibles, cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

1.6.2.2.2. Seguridad del Equipamiento.

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

1.6.2.2.3. Inundaciones.

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

1.6.2.2.4. Instalaciones eléctricas.

Trabajar con computadoras implica trabajar con electricidad, por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

1.6.2.2.5. Picos y Ruidos Electromagnéticos.

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

1.6.2.2.6. Cableado.

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que sí sufren los cables metálicos.
- Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

- Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de accesos adecuados hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.
- Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

1.6.2.2.7. Cableado de Alto Nivel de Seguridad.

Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreo de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

1.6.2.2.8. Pisos de Placas Extraíbles.

Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser, en caso necesario, alojados en el espacio que, para tal fin se dispone en los pisos de placas extraíbles, debajo del mismo.

1.6.2.2.9. Sistema de Aire Acondicionado.

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

1.6.2.2.10. Emisiones Electromagnéticas.

Desde hace tiempo se sospecha que las emisiones, de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano.

Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas. Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

Dentro de la Seguridad Física hay un factor sumamente importante que son las acciones por parte de personal no autorizado o con mala intención sobre la información y a su vez sobre los equipos de un centro informático. Estas serán denominadas como acciones hostiles.

1.6.2.2.11. Robo.

Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero.

Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina.

La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora.

El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

1.6.2.2.12. Fraude.

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imágen, no se da ninguna publicidad a este tipo de situaciones.

1.6.2.2.13. Sabotaje.

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos.

Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

Al igual que la Seguridad Lógica la Seguridad Física también posee un punto llamado control de acceso.

La diferencia de este en relación al control de acceso Lógico que consta con nombres de usuario, contraseñas, privilegios y restricciones. Es que el control de acceso no sólo requiere la capacidad de identificación, sino también asociarse a la apertura o bloqueo de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa institución o centro informático.

1.6.2.2.14. Control de Acceso.

Como es el caso del LTIC, en el periodo en el que fui parte del personal de trabajo en el área de becaria, se implementó el sistema de control de acceso a las diferentes aulas, a través de tarjetas electrónicas y magnéticas, las mismas que son activadas por parte del personal autorizado del LTIC, y que es de uso individual y exclusivo para trabajar en los equipos del LTIC.

Este tipo de acceso es muy importante ya que gracias a este se ha controlado el buen uso de los equipos y de las instalaciones del LTIC, reduciendo en su totalidad riesgos del mal uso y daño de los equipos, y a su vez de robos.

Cada tarjeta al momento de su activación, se la identifica con el nombre del alumno que la solicite para su uso, indicando el tiempo de llegada y de salida, como a su vez el tiempo límite de uso de la tarjeta que es de 2 horas, caso contrario esta será inhabilitada y no se podrá abrir la puerta del aula a la cual fue asignada.

Gracias a este sistema de acceso podremos determinar si existió algún daño por parte de o los alumnos que hayan ingresado y hayan hecho uso de las instalaciones como de los equipos en la hora indicada. O a su vez determinar la pérdida o hurto de los mismos.

Además del control de acceso también contamos con un sistema de vigilancia con cámaras de seguridad, el mismo que está permanentemente gravando cada una de las actividades que se realizan en el LTIC.

1.7 Políticas de seguridad dentro de un laboratorio informático.

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización. Así también como cada organización debe generar sus propias políticas de seguridad.

Una política de seguridad es una manifestación clara y precisa de lo que está permitido y de lo que no está permitido realizar dentro de sistema informático, plasmado en un documento con un orden y una sistematización.

Dentro del LTIC, en base a las políticas de seguridad establecidas, contamos con las siguientes normas:

Dirigido a el/la Director/ra del LTIC que tenga acceso total a los privilegios de seguridad y manejo y cambio de las políticas de seguridad.

1. El/la Director/ra del LTIC tiene control total sobre los privilegios de seguridad y las políticas de seguridad establecidas.

2. Los equipo o partes de ellos no pueden salir de las instalaciones del LTIC salvo con excepción autorizada por el/la Directo/ra.
3. El/la Director/ra tiene acceso total mediante su tarjeta magnética, así también como a un punto del sistema de acceso de las puertas magnéticas.
4. El/la Director/ra del LTIC es responsable de calendarizar y aprobar los horarios para cada semestre académico para pregrado y postgrado.
5. Estos horarios y disponibilidad de las aulas del LTIC son comunicados oportunamente por medio de correo electrónico a los docentes y publicado para los alumnos en cartelera.
6. El/la Director/ra es la única persona que permite la autorización y de uso de las tarjetas de acceso, así mismo, será emitida exclusivamente por el/la Director/ra del LTIC.
7. Si se necesita realizar actividades académicas o administrativas por parte de los docentes o estudiantes, estas actividades deberán ser justificadas ante el Directo/ra del LTIC.
8. El/la Director/ra es la persona que se encuentra a cargo de la administración del módulo de seguridad del LTIC.
9. El/la Director/ra está a cargo de los registros de la información del módulo de visitas al LTIC
10. El/la Director/ra del LTIC es la única persona con acceso al Data Center, y la única que puede autorizar a otra persona su acceso.

Dirigido a los Becarios y Ayudantes del LTIC.

1. Es responsabilidad del personal autorizado del LTIC el cambio de equipos con desperfectos de hardware o software para su respectivo arreglo y corrección.
2. Es obligación del Personal del LTIC llevar un registro de todos los estudiantes que utilizan el Laboratorio así como de sus tiempos de uso.
3. Es responsabilidad del personal del LTIC velar por la integridad de los equipos.
4. La documentación del hardware del LTIC debe estar disponible en todo momento para dar soporte y mantenimiento según sea considerable.
5. Los becarios están a cargo de los registros de la información del módulo de visitas al LTIC.
6. La documentación del software utilizado en los equipos del LTIC debe estar disponible en todo momento para dar soporte y mantenimiento según sea considerable.
7. Cualquier daño, sea este deliberado o accidental a un activo del LTIC deberá ser registrado para posteriormente ser informado al Departamento de Sistemas.
8. Sin excepción, el software anti virus será instalado en todas los equipos del LTIC y actualizado diariamente.
9. Es responsabilidad del personal del LTIC un chequeo semanal de los equipos y software.
10. Es responsabilidad del personal del LTIC que los equipos como infocus, laptops, cables de red, protoboards, etc. No pueden ser sustraídos o prestados fuera de las instalaciones.
11. Los equipos pueden ser prestados dentro de las horas de clase o prácticas de laboratorio establecida en las instalaciones del LTIC, con previa autorización de el/la directora/ra.
12. Los horarios de atención del LTIC son desde las 07h00 a 13h00 y de 14h00 a 20h00 de lunes a viernes para las actividades de pregrado, a los cuales los ayudantes y becarios deben respetar sus horarios establecidos por parte del/la Directo/ra del LTIC. Los días sábados se permite el funcionamiento para las maestrías y actividades de postgrado que hayan solicitado la reserva de las aulas y equipos del LTIC.
13. Es responsabilidad llevar una bitácora de las actividades diarias realizadas en el LTIC.
14. Es responsabilidad llevar un control de asistencia por parte de los becarios y ayudantes del LTIC.

Dirigido a los estudiantes de Ingeniería de la Pontificia Universidad Católica del Ecuador, tanto para lo que es la Escuela de Sistemas, Civil y Maestrías.

1. Los estudiantes que reciban por primera vez la tarjeta de acceso, el estudiante usuario de la misma debe firmar el ACTA DE ENTREGA-RECEPCION de la tarjeta de acceso.
2. Los estudiantes solamente accederán al servicio del LTIC y a sus respectivas aulas a través de la presentación de su carnét de estudiante de la Universidad, que sea perteneciente a la Carrera de Ingeniería y que se encuentre matriculado en el respetivo semestre vigente, con la presentación de este documento se les facilitara una tarjeta magnética de acceso.
3. La tarjeta de acceso proporcionada a los estudiantes es de uso personal e intransferible.
4. En el caso de que el acceso a un aula sea por parte de dos personas que vayan a utilizar un mismo equipo, tendrán que obligatoriamente dejar las dos personas su carnet y retirar una sola tarjeta de acceso. Una de las dos personas será el único responsable de la tarjeta de acceso.
5. Los equipos del LTIC son únicamente para uso con fines académicos y el acceso a Internet sólo para fines investigativos y revisión de cuentas de correo.
6. La sustracción de equipos del LTIC o de sus partes es una acción prohibida y considerada como robo.
7. Respecto al uso en el LTIC, se prohíbe la desconexión y daño de: cables de red, eléctricos, mouse, teclados, fuente de poder, monitor o cualquier otro elemento que permita el normal funcionamiento del equipo.
8. Respecto a los equipos, no está permitido el acceso, con privilegios de usuario administrador, a los equipos del LTIC por parte de los estudiantes.
9. Para los perfiles de estudiantes no está permitido modificar las configuraciones de los equipos del LTIC y tampoco de los privilegios de seguridad establecidos.
10. Respecto a los equipos del LTIC, no está permitida la instalación de programas adicionales por parte de personas no autorizadas al LTIC, si el caso amerita por parte de los tutores o profesores, se puede realizar la instalación con previa autorización de el/la directora/ra.
11. Está totalmente prohíbo hacer uso de juegos en los computadores del LTIC, ya que son para uso académico.
12. Por el bien de los equipos, no está permitido el ingreso al LTIC con alimentos y bebidas, así como el fumar en él.
13. Es obligación de los usuarios reportar inmediatamente cualquier anomalía en el funcionamiento del equipo o programas a los encargados del LTIC.
14. Una vez asignado un equipo al usuario, este es responsable del equipo durante el tiempo (2 horas) que permanece en su poder.
15. El estudiante tiene la obligación de entregar la tarjeta de acceso, a la persona autorizada en la ventanilla al finalizar su uso.
16. En caso de pérdida o robo de la tarjeta es obligación del estudiante informar de forma inmediata a el/la Director/ra del LTIC para su respectiva anulación y evitar accesos indebidos.
17. En caso de pérdida o robo de la tarjeta de acceso el estudiante debe acercarse a tesorería de la Universidad para el pago respectivo de la misma, su valor es de $3,00 USD, previo el retiro de la autorización del pago en la dirección del LTIC. Luego del pago debe entregar una copia del comprobante de pago en la dirección del LTIC, hasta 15 días laborables a partir de la fecha de reporte de la perdida de la tarjeta.

Dirigido a los profesores de Ingeniería de la Pontificia Universidad Católica del Ecuador, tanto para lo que es la Escuela de Sistemas, Civil y Maestrías.

1. Cada inicio de semestre los profesores recibirán una tarjeta de acceso personal, para esto se debe firmar el ACTA DE ENTREGA-RECEPCION de la tarjeta de acceso.
2. Dependiendo de los Horarios asignados por el/la Director/ra del LTIC, se asignaran el acceso respetivo con la tarjeta magnética para cada profesor.
3. Cada profesor tendrá 15 minutos antes para el ingreso y 20 minutos para la salida de las aulas al culminar sus horas de clase.
4. Cada profesor es responsable de las aulas de clase en sus horas de clase.
5. Los profesores que estén asignados para laboratorio son los únicos responsables de los equipos que son facilitados bajo la autorización de el/la Director/ra del LTIC.
6. Si es necesario por parte de los profesores instalar software adicional al que se encuentra en los equipos del LTIC, tiene que ser pedido con 48 horas de anticipación a el/la Director/ra del LTIC.
7. Si los profesores necesitan reservar un aula tienen que pedirla y reservarla con anticipación a el/la Director/ra del LTIC, dependiendo la disponibilidad del laboratorio.
8. Para las clases de maestría que se dictan los fines de semana, se deben pedir las aulas con anterioridad, el/la Director/ra del LTIC, es la única encargada de autorizar los horarios y las aulas en las que se impartirán las clases.
9. Si son profesores tiempo completo, tendrán asignada una tarjeta de acceso para todo el periodo del semestre.
10. En caso de los profesores que no son tiempo completo, que son tiempo parcial, deberán pedir a el/la Director/ra del LTIC que se le asigne los accesos a las aula en sus horas clase, para el acceso los becarios serán los encargados de abrir las puertas de las aulas para dichos profesores.

1.8. Protocolos de red.

1.8.1. Definición.-

Un protocolo es una regla o estándar que controla o permite la comunicación de computadoras una entre otra en su forma más simple a través de una red, un protocolo puede ser definido como las reglas que dominan la sintaxis, semántica y sincronización de la comunicación. Los protocolos pueden ser implementados por hardware, software, o una combinación de ambos. A su más bajo nivel, un protocolo define el comportamiento de una conexión de hardware.

1.8.2. Modelo OSI.

A finales de la década de los setenta, la Organización Internacional para la Normalización (ISO) empezó a desarrollar un modelo conceptual para la conexión en la red ala que bautizo con el nombre de Open Systems Interconnection Reference Model o Modelo de Referencia de Interconexión de Sistemas Abiertos. En 1984, este modelo pasó a ser el estándar internacional para las comunicaciones en red al ofrecer un marco de trabajo conceptual que permitía explicar el modo en que los datos se desplazaban dentro de una red.

El modelo OSI divide en siete capas el proceso de transmisión de la información entre equipos informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global.

Este marco de trabajo estructurado en capas, aun siendo puramente conceptual, puede utilizarse para describir y explicar el conjunto de protocolos reales que se utilizan para la concesión de sistemas.

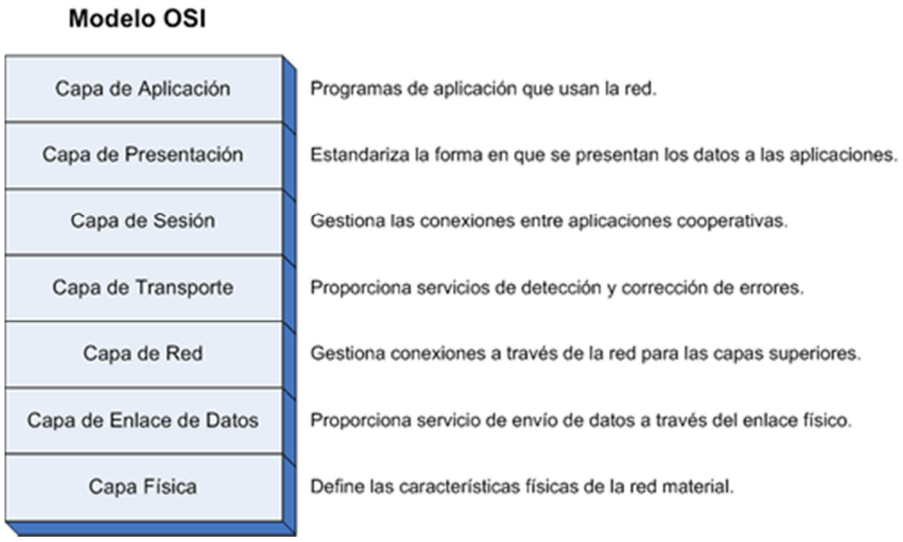
1.8.3. Pila de protocolos.

Se dicen pila de protocolos o capas, porque no son más que una jerarquía de pequeños protocolos que trabajan juntos para llevar a cabo la transmisión de datos de un nodo a otro de la red.

1.8.4. El modelo OSI y sus capas.

Las capas del modelo OSI describen el proceso de transmisión de los datos dentro de una red.

Gráfico 1: Modelo OSI*



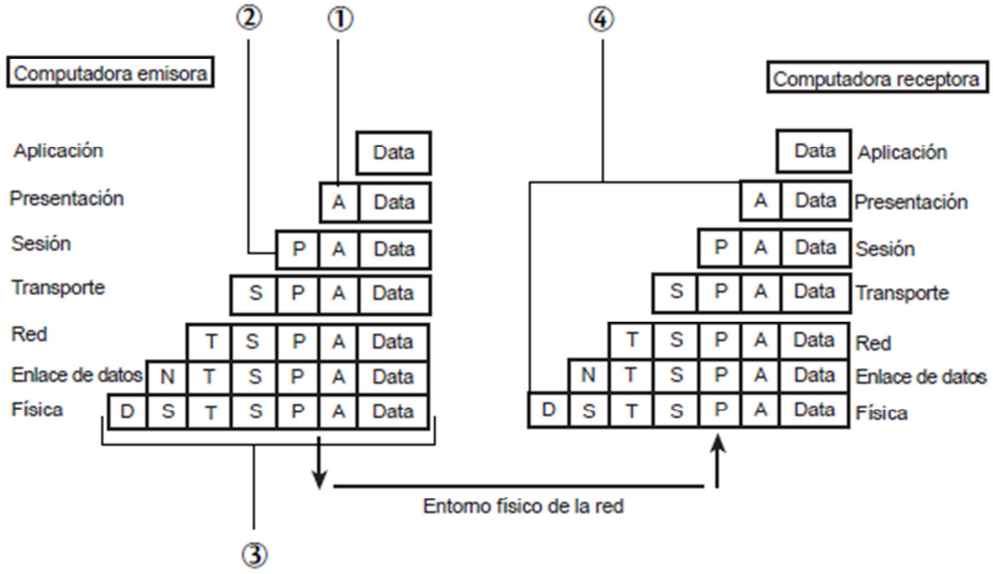
* Gráfico 1: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

Dentro del modelo OSI, las únicas capas que interactúan con el usuario son la capa Física y la capa de Aplicación.

1.8.4.1. Como trabaja el modelo de capas OSI.

El siguiente diagrama muestra como en el modelo OSI los datos bajan por cada una de las capas de una computadora emisora y suben por las mismas capas de otra computadora receptora.

Gráfico 2: Entorno físico de Red*



* Gráfico 2: http://www.textoscientificos.com/redes/tcp-ip/entorno -de-red/modelo-osi

El entorno físico de la Red trabaja sobre 4 puntos dentro del modelo OSI.:

1. Encabezado de la capa de Aplicación.
2. Encabezado de la capa de presentación.
3. Paquete con todos los encabezados de la capas OSI.
4. Los encabezados se van suprimiendo a medida que los datos suben por la capa OSI.

Desde el nivel más bajo al más alto detallaremos las 7 capas que forman parte del modelo OSI.

1.8.5. Capa Física.

Es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.

- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas del medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de dicha conexión).

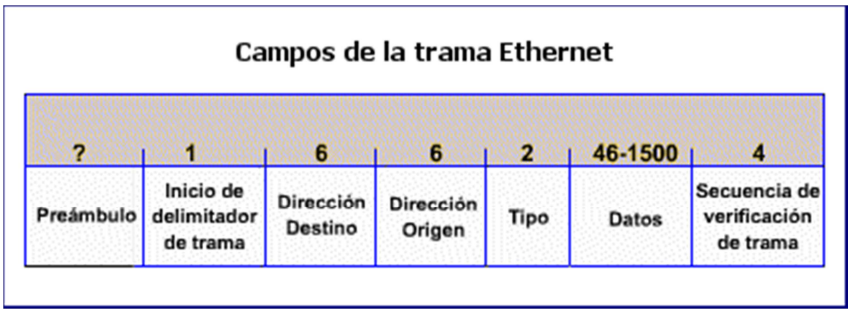
1.8.6. Capa de enlace de Datos.

Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo.

Cuando los paquetes de datos llegan a la capa de enlace de datos, estos pasan a ser tramas unidades de datos, que vienen definidas por la arquitectura de red que se está utilizando, como Ethernet, Token Ring, EEE 802.3, IEEE 802.11 o Wi-Fi, IEEE 802.16 o WiMAX, etc.

La capa del enlace de datos se encarga de desplazar los datos del enlace físico de comunicación hasta el nodo receptor e identificar cada computadora incluida en la red de acuerdo con su dirección de hardware, que viene codificada en la NIC.

Gráfico 3: Trama Ethernet*



* Gráfico 3: http://internett.galeon.com/REDES.htm

En la figura podemos ver la trama Ethernet que se crea en la capa de enlace de datos, donde:

Preámbulo: Los bits de alteración (1 y 0) que indican que se ha enviado una trama.
Destino: La dirección de destino
Fuente: La dirección de origen.
Longitud: especifica el número de bytes de datos incluidos en la trama.
DSAP: Destination Service Access Point o Punto de Acceso al Servicio de Destino, indica a la tarjeta de red de la computadora receptora donde tiene que ubicar la trama dentro de la memoria intermedia.
SSAP: Proporciona la información de Punto de Acceso al Servicio (Service Access Point) para la trama.
CTRL: Es un campo de control Lógico de Enlace.
Datos: Este segmento de la trama mantiene los datos que se han enviado.
FCS: El campo de secuencia de comprobación de la trama contiene el valor para la trama.

1.8.7. Capa de Red.

La capa de red es la encargada de encaminar los paquetes además de ocuparse de entregarlos. La determinación de la ruta que deben seguir los datos se producen en esta capa, lo mismo que el intercambio efectivo de los mismos dentro de dicha ruta.

En la capa de Red es donde las direcciones Lógicas, como las direcciones IP de una computadora paran a convertirse en direcciones Físicas, como son las direcciones de Hardware de la NIC, la tarjeta de Interfaz para Red, de cada computadora especifica.

Entre los protocolos de la capa de red tenemos los siguientes:
- IP (IPv4, IPv6, IPsec)
- OSPF
- IS-IS
- ARP, RARP
- RIP
- ICMP, ICMPv6
- IGMP
- DHCP

Los protocolos de red que común mente se utilizan en nuestro laboratorio son IP y DHCP.

Dentro de lo que es la capa de red tenemos el algoritmo de enrutamiento. Donde su función principal es enrutar paquetes de la maquina origen a la maquina destino.

El algoritmo de enrutamiento es aquella parte del software de la capa de red encargada de decidir la línea de salida por la que se transmitirá un paquete de entrada.

Hay ciertas propiedades que todo algoritmo de enrutamiento debe poseer: exactitud, sencillez, robustez, estabilidad, equidad y optimización.

Los algoritmos de enrutamiento pueden agruparse en dos clases principales:

Los no adaptivos o de enrutamiento estático.
- Ruta más corta, más rápida, más barata, etc.
- Enrutamiento por inundación.
- Enrutamiento basado en flujo.

Aditivos o de enrutamiento dinámico.
- Enrutamiento por vector de distancia.
- Enrutamiento por estado de enlace.

1.8.8. Capa de Transporte.

La capa de transporte se encarga de controlar el flujo de datos entre los nodos que establecen una comunicación. Los datos no sólo deben entregarse sin errores, sino además en la secuencia que procesa.

La capa de transporte se ocupa también de evaluar el tamaño de los paquetes con el fin de que estos tengan el tamaño requerido por las capas inferiores del conjunto de protocolos.

Esta comunicación se establece al mismo nivel tanto en la computadora emisora y receptora, la aceptación por parte del nodo receptor se recibe cuando el nodo emisor ha enviado el número acordado de paquetes.

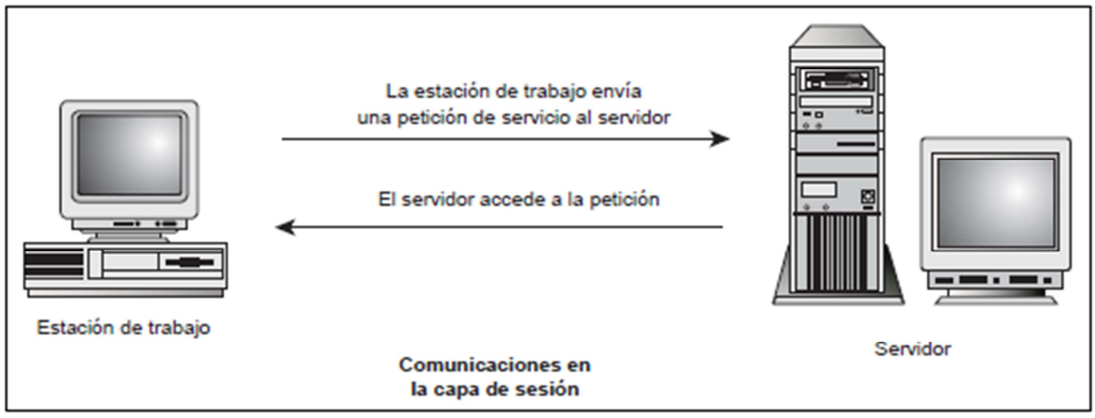
Esta comunicación en la capa de transporte resulta muy útil cuando la computadora emisora manda demasiados datos a la computadora receptora, en este caso, el nodo receptor tomara todos los datos que pueda aceptar de una sola vez y pasará a enviar una señal de ocupado si se envía más datos.

Una vez que la computadora receptora haya procesado los datos y esté lista para recibir más paquetes enviara a la computadora emisora un mensaje de luz verde para que envié los paquetes restantes.

1.8.9. Capa de Sesión.

La capa de sesión está encargada de establecer el enlace de comunicación o sesión entre los computadores emisora y receptora. Esta capa también gestiona la sesión que se establece entre ambos nodos.

Gráfico 4: Comunicación capa de sesión *



* Gráfico 4: *http://telematica-jocasoft.blogspot.com/2010/05/capa-de-sesion.html

La capa de sesión proporciona el enlace de comunicación entre dos computadores que se están comunicando.

Una vez establecida la sesión entre los nodos participantes, la capa de sesión pasa a encargarse de ubicar puntos de control en la secuencia de datos. De esta forma, se proporciona cierta tolerancia a fallos dentro de la sesión de comunicación. Si una sesión falla y se pierde la comunicación entre los nodos, cuando después se restablezca la sesión sólo tendrán que volver a enviarse los datos situados detrás del último punto de control recibido. Así se evita el tener que enviar de nuevo todos los paquetes que incluía la sesión.

Los protocolos que operan en la capa de sesión pueden proporcionar dos tipos distintos de enfoques para que los datos vayan de emisor al receptor: la comunicación orientada a la conexión y la comunicación sin conexión.

1.8.10. Capa de presentación.

La capa de presentación se puede considerar el traductor del modelo OSI.

Esta capa toma los paquetes de la capa de aplicación y los convierte a un formato genérico que pueden leer todas las computadoras.

La capa de presentación también se encarga de cifrar los datos (si así lo requiere la aplicación utilizada en la capa de aplicación) así como de comprimir para reducir su tamaño. El paquete que crea la capa de presentación contiene los datos prácticamente con el formato con el que viajaran por las restantes capas de la pila OSI (aunque las capas siguientes irán añadiendo elementos al paquete, lo cual puede dividir los datos en paquetes más pequeños).

La capa de presentación tiene tres funciones principales:

- Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen se puedan interpretar por la aplicación adecuada en el dispositivo de destino.
- Compresión de los datos de forma que los pueda descomprimir el dispositivo de destino.
- Encriptación de los datos para la transmisión y la encriptación de los mismos cuando lleguen a su destino.

1.8.11. Capa de Aplicación.

Es la capa superior de los modelos OSI y TCP/IP.

Es la capa que proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación y siempre se desarrollan protocolos nuevos.

La capa de aplicación prepara la comunicación entre las personas para la transmisión en la red de datos.

Aunque el grupo de protocolos TCP/IP se desarrolló antes de la definición del modelo OSI, la funcionalidad de los protocolos de la capa de aplicación de TCP/IP se adaptan aproximadamente a la estructura de las tres capas superiores del modelo OSI. Capas de aplicación, presentación y sesión.

La mayoría de los protocolos de la capa de aplicación de TCP/IP se desarrollaron antes de la aparición de computadoras personales, interfaces del usuario gráficas y objetos multimedia.

Los protocolos de capa de aplicación de TCP/IP más conocidos son aquéllos que proporcionan intercambio de la información del usuario. Estos protocolos especifican la información de control y formato necesaria para muchas de las funciones de comunicación de Internet más comunes. Algunos de los protocolos TCP/IP son:

- El Protocolo servicio de nombres de dominio (DNS, Domain Name Service) se utiliza para resolver nombres de Internet para direcciones IP.
- El Protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol) se utiliza para transferir archivos que forman las páginas Web de la World Wide Web.
- El Protocolo simple de transferencia de correo (SMTP) se utiliza para la transferencia de mensajes de correo y adjuntos.
- Telnet, un protocolo de emulación de terminal, se utiliza para proporcionar acceso remoto a servidores y a dispositivos de red.
- El Protocolo de transferencia de archivos (FTP) se utiliza para la transferencia de archivos interactiva entre sistemas.

Los protocolos en la suite de TCP/IP los definen generalmente las Solicitudes de comentarios (RFC). El Grupo de trabajo de ingeniería de Internet mantiene las RFC como los estándares para la suite de TCP/IP.

Gráfico 5: Capa de Aplicación – Servidores*

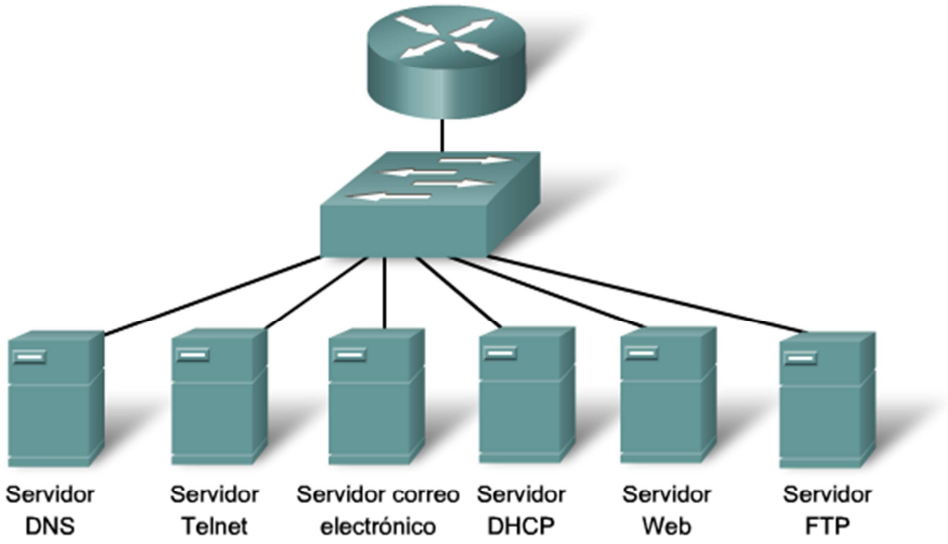


*Gráfico 5: Exploration CCNA1

Las funciones asociadas con los protocolos de la capa de aplicación permiten a la red humana comunicarse con la red de datos subyacente. Cuando abrimos un explorador Web o una ventana de mensajería instantánea se inicia una aplicación, y el programa se coloca en la memoria del dispositivo donde se ejecuta. Cada programa ejecutable cargado a un dispositivo se denomina proceso.

Dentro de la capa de aplicación, existen dos formas de procesos o programas de software que proporcionan acceso a la red: aplicaciones y servicios.

1.8.11.1. Aplicaciones reconocidas por la red.

Las aplicaciones son los programas de software que utiliza la gente para comunicarse a través de la red. Algunas aplicaciones de usuario final son reconocidas por la red, lo cual significa que implementan los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores del stack de protocolos. Los clientes de correo electrónico y los exploradores Web son ejemplos de este tipo de aplicaciones.

1.8.11.2. Servicios de la capa de aplicación.

Otros programas pueden necesitar la ayuda de los servicios de la capa de aplicación para utilizar los recursos de la red, como transferencia de archivos o cola de impresión en la red. Aunque son transparentes para el usuario, estos servicios son los programas que se comunican con la red y preparan los datos para la transferencia. Diferentes tipos de datos, ya sea texto, gráfico o video, requieren de diversos servicios de red para asegurarse de que estén bien preparados para procesar las funciones de las capas inferiores del modelo OSI.

Cada servicio de red o aplicación utiliza protocolos que definen los estándares y formatos de datos a utilizarse. Sin protocolos, la red de datos no tendría una manera común de formatear y direccionar los datos. Es necesario familiarizarse con los protocolos subyacentes que rigen la operación de los diferentes servicios de red para entender su función.

Gráfico 6: Proceso de Software – Capa de Aplicación. *

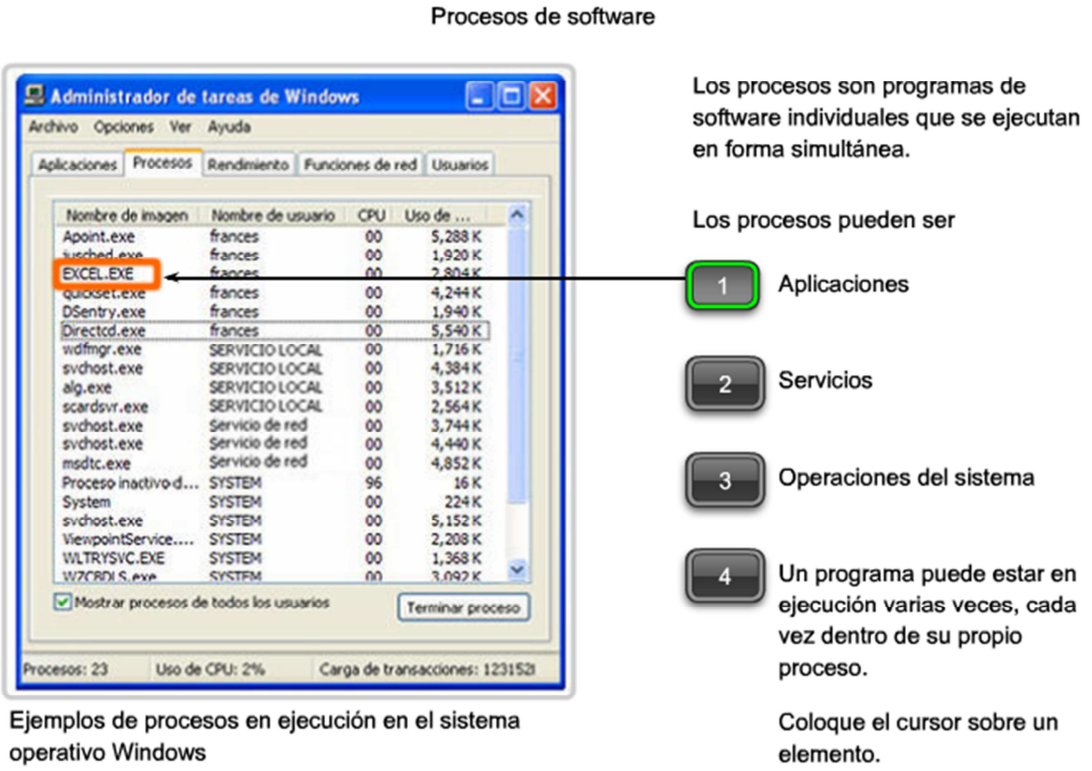


Gráfico 7: Servicios – Capa de Aplicación.*

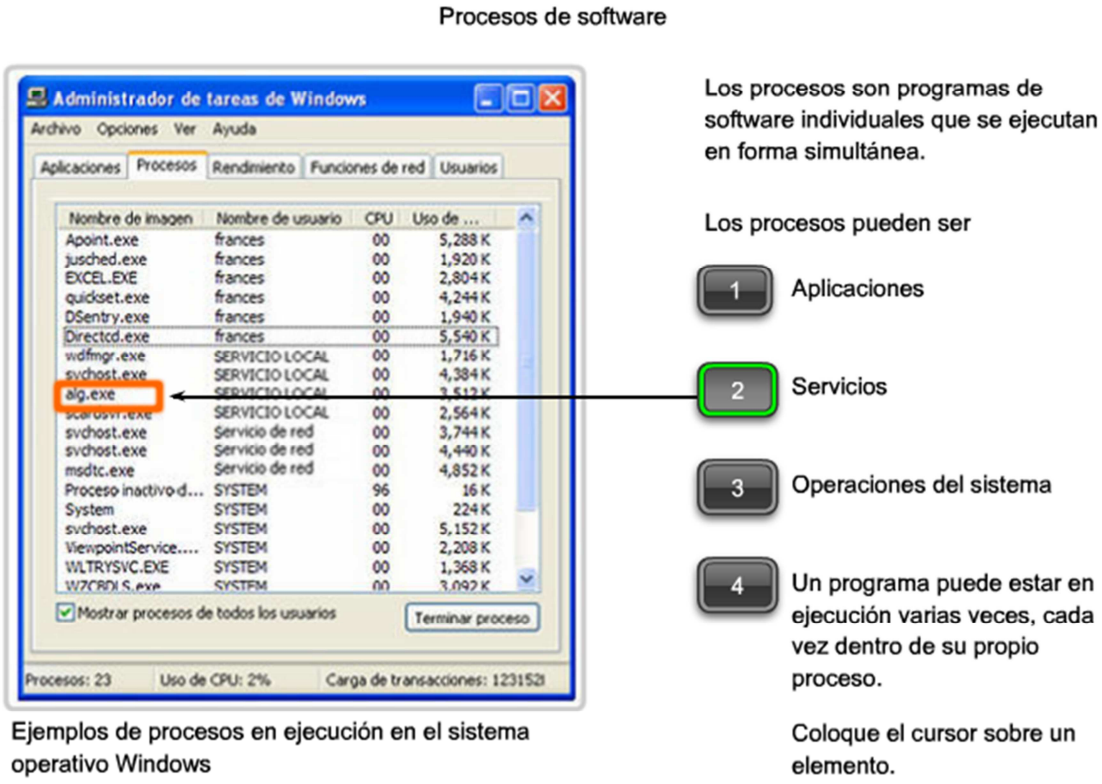


Gráfico 8: Operaciones de sistema – Capa de Aplicación.*

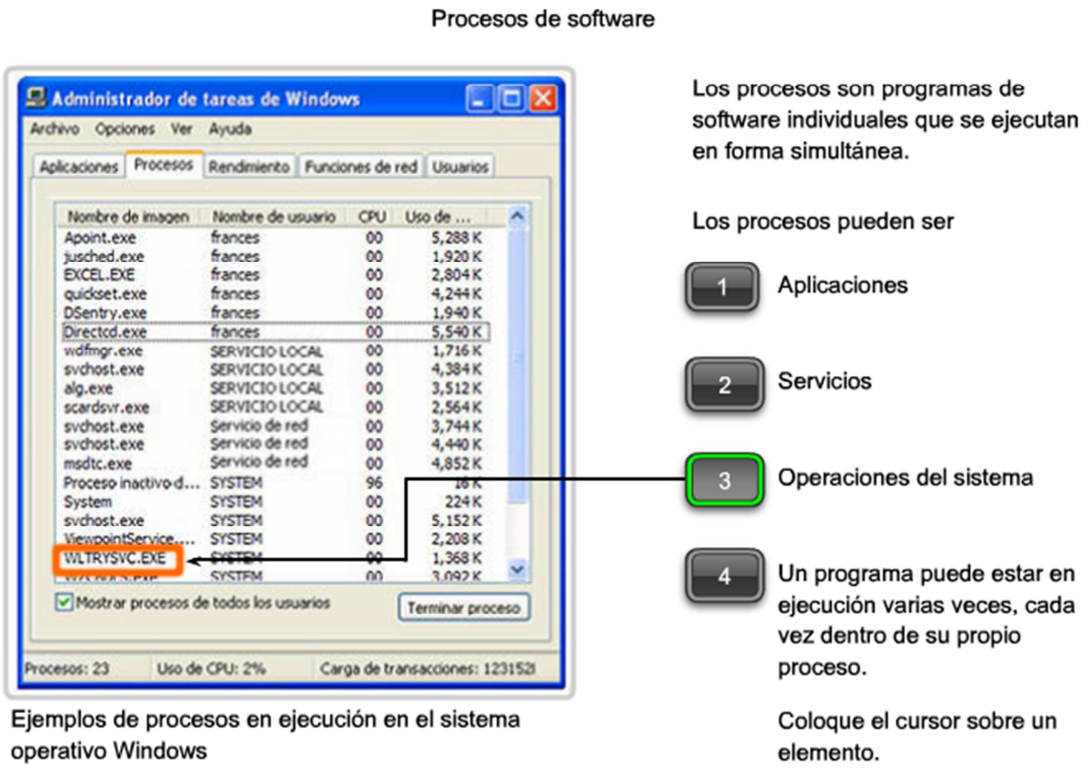
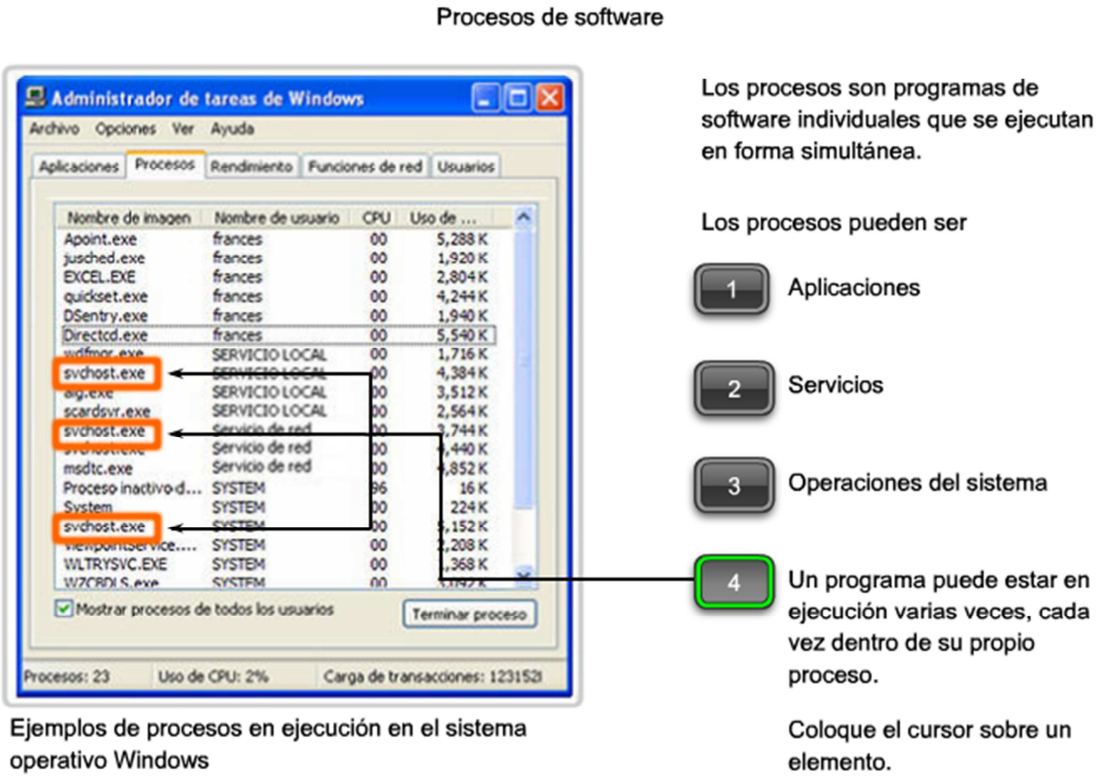


Gráfico 9: Programa – Capa de Aplicación.*

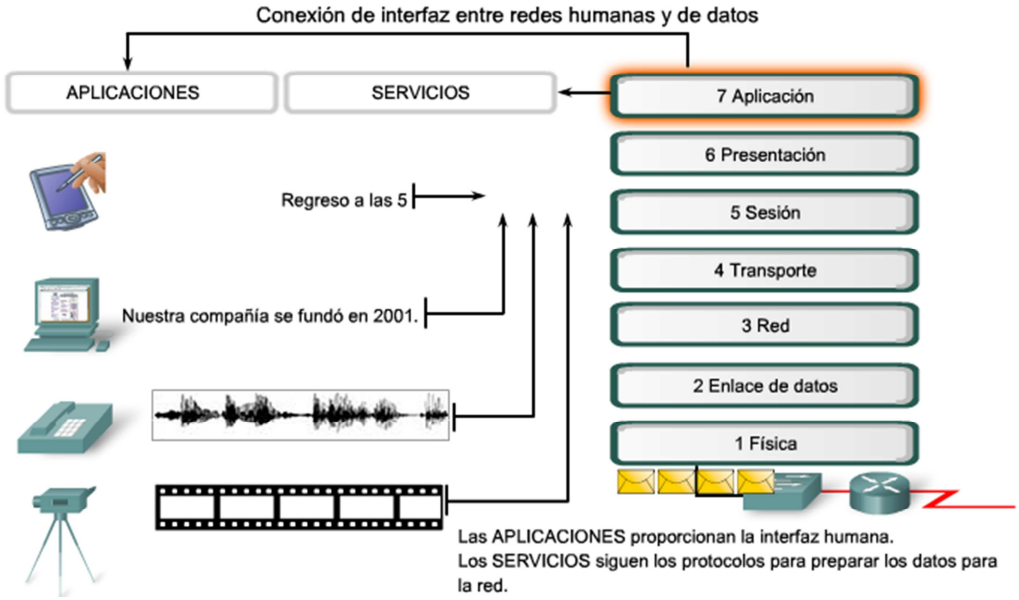


* Gráficos 6,7, 8, 9: Exploration CCNA1

Como se mencionó anteriormente, la capa de aplicación utiliza los protocolos implementados dentro de las aplicaciones y servicios. Mientras que las aplicaciones proporcionan a las personas una forma de crear mensajes y los servicios de la capa de aplicación establecen una interfaz con la red, los protocolos proporcionan las reglas y los formatos que regulan el trato de los datos. Un solo programa ejecutable debe utilizar los tres componentes e inclusive el mismo nombre. Por ejemplo, al hablar de "Telnet" podemos estar refiriéndonos a la aplicación, al servicio o al protocolo.

En el modelo OSI, las aplicaciones que interactúan directamente con la gente se considera que están en la parte superior del stack, como la misma gente. Al igual que todas las personas dentro del modelo OSI, la capa de aplicación se basa en la funciones de las capas inferiores para completar el proceso de comunicación. Dentro de la capa de aplicación, los protocolos especifican qué mensajes se intercambian entre los host de origen y de destino, la sintaxis de los comandos de control, el tipo y el formato de los datos que se transmiten y los métodos adecuados para notificación y recuperación de errores.

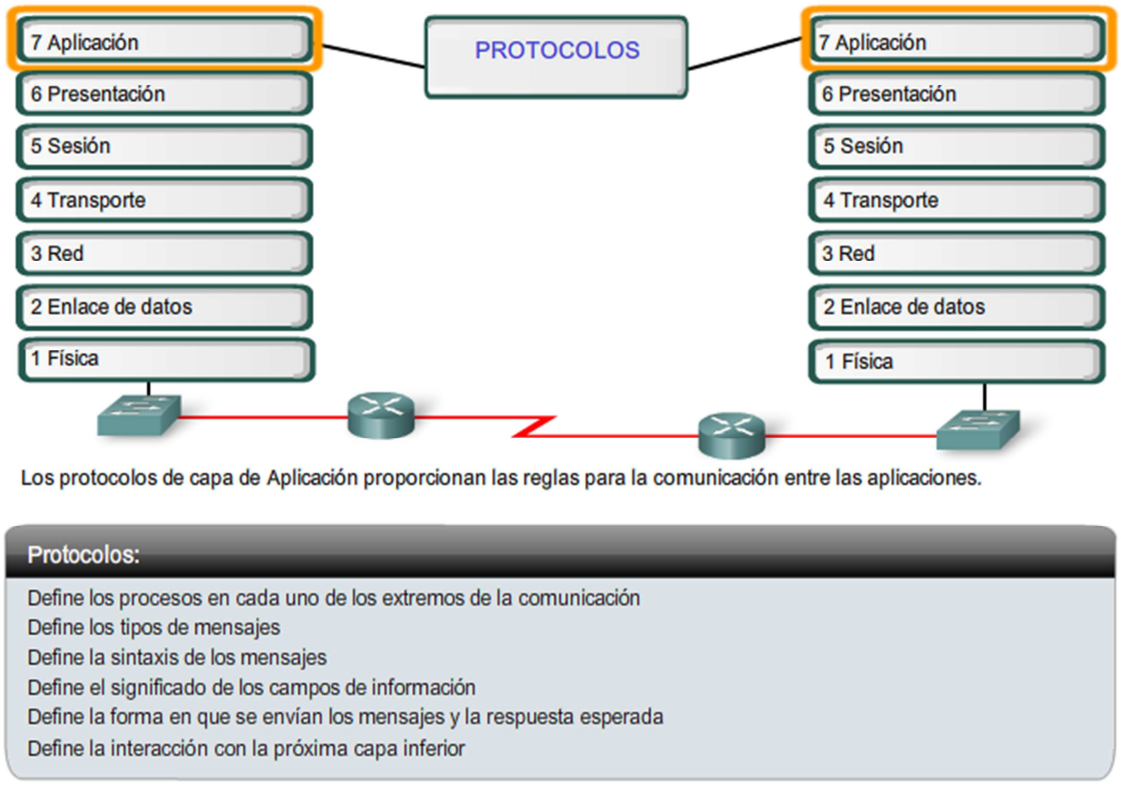
Gráfico 10: Conexión de interfaz entre redes humanas y de datos



* Gráfico10: Exploration CCNA1

Los protocolos de la capa de aplicación los utilizan tanto los dispositivos de origen como de destino durante una sesión de comunicación. Los protocolos de la capa de aplicación que se implementaron en los hosts de origen y destino deben coincidir para que las comunicaciones tengan éxito.

Gráfico 11: Protocolos en la capa de Aplicación.*



* Gráfico 11: Exploration CCNA1

1.9. Estructura y topología de la Red.

Dentro de lo que es la estructura de la Red debemos tener claro, que esta va estar conformada por un conjunto de equipos que interactúan entre sí para brindar un servicio y que a su vez se comunican todos entre sí.

Respecto a lo que es la estructura de una red, tenemos que tener claro que dentro de lo que es nuestro laboratorio de informática tenemos un tipo específico de Arquitectura, dentro de lo que es el laboratorio LTIC tenemos una arquitectura Cliente/Servidor.

1.9.1. Arquitectura Cliente/Servidor.

En el modelo cliente/servidor, el dispositivo que solicita información se denomina cliente y el dispositivo que responde a la solicitud se denomina servidor. Los procesos de cliente y servidor se consideran una parte de la capa de aplicación. El cliente comienza el intercambio solicitando los datos al servidor, quien responde enviando uno o más streams de datos al cliente. Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores. Además de la transferencia real de datos, este intercambio puede requerir de información adicional, como la autenticación del usuario y la identificación de un archivo de datos a transferir.

Gráfico 12: Modelo Cliente-Servidor/ Proceso de descarga.*

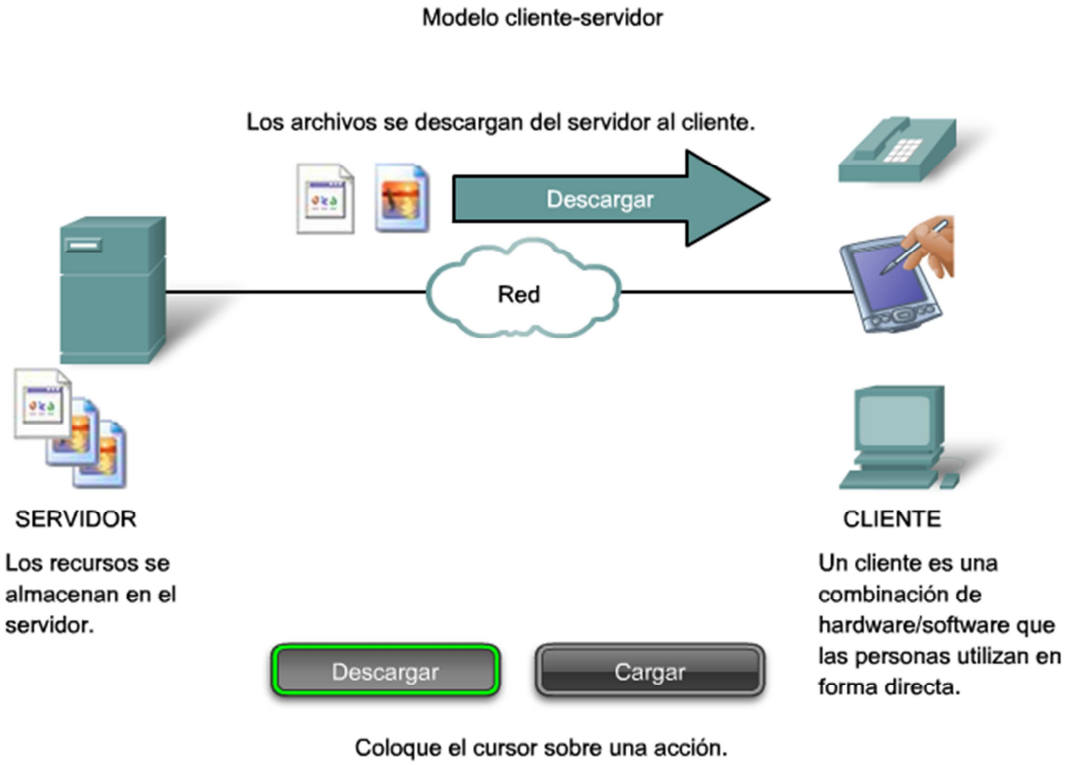
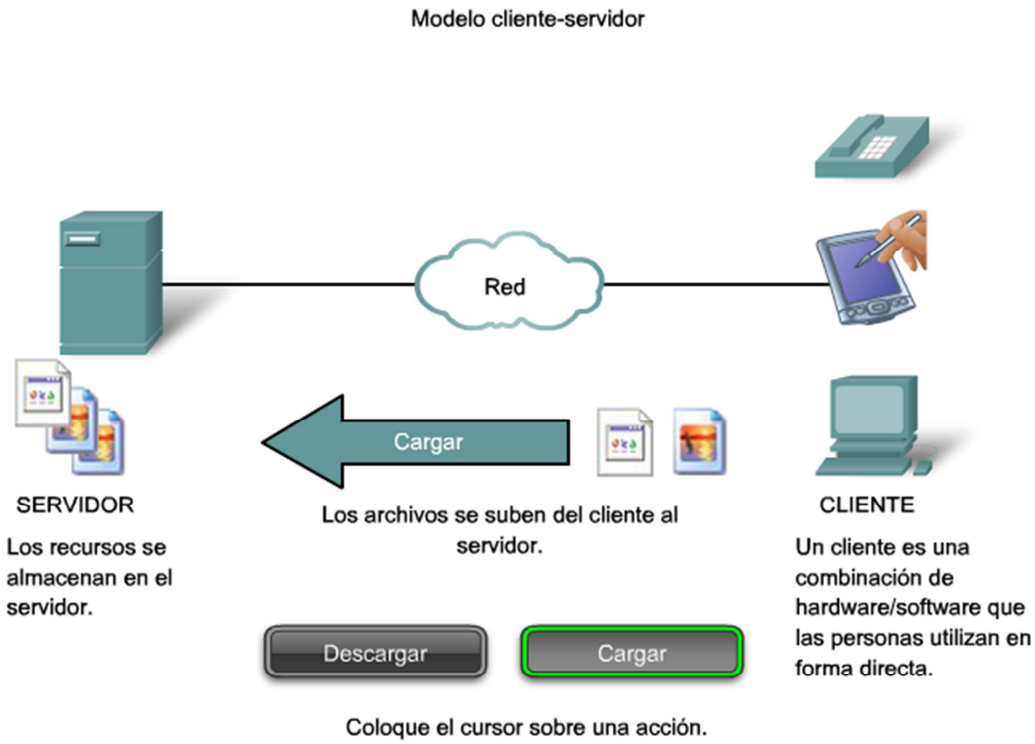


Gráfico 13: Modelo Cliente-Servidor/ Proceso de carga.*



* Gráfico 12 y 13: Exploration CCNA1

Un ejemplo de una red cliente-servidor es un entorno corporativo donde los empleados utilizan un servidor de correo electrónico de la empresa para enviar, recibir y almacenar correos electrónicos. El cliente de correo electrónico en la computadora de un empleado emite una solicitud al servidor de correo electrónico para un mensaje no leído. El servidor responde enviando al cliente el correo electrónico solicitado.

Aunque los datos se describen generalmente como el flujo del servidor al cliente, algunos datos fluyen siempre del cliente al servidor. El flujo de datos puede ser el mismo en ambas direcciones, o inclusive puede ser mayor en la dirección que va del cliente al servidor. Por ejemplo, un cliente puede transferir un archivo al servidor con fines de almacenamiento. La transferencia de datos de un cliente a un servidor se denomina cargar y de datos de un servidor a un cliente se conoce como descarga.

1.9.2. Características de la arquitectura Cliente/Servidor.

En la arquitectura Cliente/Servidor el remitente de una solicitud es conocido como cliente.

Sus características son:

- Es quien inicia solicitudes o peticiones, tienen por tanto un papel activo en la comunicación (dispositivo maestro o amo).
- Espera y recibe las respuestas del servidor.
- Por lo general, puede conectarse a varios servidores a la vez.

- Normalmente interactúa directamente con los usuarios finales mediante una interfaz gráfica de usuario.
- Al contratar un servicio de redes, se tiene que tener en la velocidad de conexión que le otorga al cliente y el tipo de cable que utiliza.

Al receptor de la solicitud enviada por el cliente se conoce como servidor. Sus características son:

- Al iniciarse esperan a que lleguen las solicitudes de los clientes, desempeñan entonces un papel pasivo en la comunicación (dispositivo esclavo).
- Tras la recepción de una solicitud, la procesan y luego envían la respuesta al cliente.
- Por lo general, aceptan conexiones desde un gran número de clientes (en ciertos casos el número máximo de peticiones puede estar limitado).
- No es frecuente que interactúen directamente con los usuarios finales.

1.10. Que es una Topología de Red.

La topología está definida como la forma en la que está diseñada la red, tanto en la parte física, donde se conforman las características de Hardware, y lógicamente respeto a lo que conforma las características de software.

Una topología básicamente es una cadena de comunicación en la que existe una relación entre todos los enlaces y los dispositivos que conforman la red. A todos estos enlaces entre casa una de los dispositivos que conforman nuestra red se los denomina Nodos.

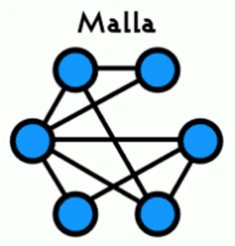
Dentro de la Topología de red existen cinco clasificaciones.

- Malla.
- Estrella.
- Árbol.
- Bus.
- Anillo.
-

1.10.1. Topología de Malla.

En la topología de malla la comunicación viene dada entre un enlace punto a punto en donde cada uno de los enlaces conducen el trafico únicamente entre los dos dispositivos que están conectados.

Grafico 1: Topología de Malla.*



* Gráfico 1: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

Una red en malla completamente conectada necesita n(n-1)/2 canales físicos para enlazar n dispositivos. Para acomodar tantos enlaces, cada dispositivo de la red debe tener sus puertos de entrada/salida (E/S)**.**

Entre las ventajas que posee la Topología de Malla están:

- El uso de los enlaces dedicados garantiza que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos.
- Es una topología robusta. Si un enlace falla, no inhabilita todo el sistema.
- Respecto a la privacidad y seguridad, cuando un mensaje es enviado, el único que puede ver el mensaje es el receptor adecuado.

Entre las desventajas que posee la Topología de Malla están:

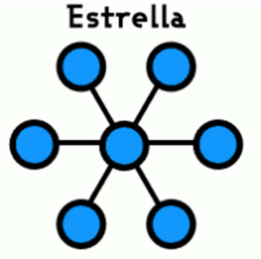
- Esta red es costosa de instalar ya que requiere de mucho cable.

1.10.2. Topología de Estrella.

Esta es una de las topologías más utilizadas ya que los datos viajan desde el concentrador o host hacia el destino.

El concentrador o Host de destino es quien se encarga del tráfico de datos y gestionando envió y recepción de la información.

Gráfico 2: Topología de estrella.*



* Gráfico 2: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

Entre las ventajas que posee la Topología de Estrella están:

- La topología en estrella no permite el tráfico directo de dispositivos, ya que El concentrador o Host actúa como un intercambiador, si un dispositivo quiere enviar datos a otro, envía los datos al concentrador, que los retransmite al dispositivo final
- Una topología en estrella es más barata.
- En la topología de estrella, cada dispositivo necesita solamente un enlace y un puerto de entrada/salida para conectarse a cualquier número de dispositivos.
- Para la instalación de una topología de estrella es necesario instalar menos cables, y la conexión, desconexión y traslado de dispositivos afecta solamente a una conexión, la que existe entre el dispositivo y el concentrador.

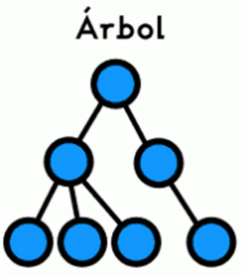
Entre las desventajas que posee la Topología de Estrella están:

- Si el nodo central falla, toda la red deja de transmitir.
- Es costosa, ya que requiere más cable que las topologías bus o anillo.
- El cable viaja por separado del hub a cada computadora.

1.10.3. Topología de Árbol.

La topología en árbol es una variante de la de estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se conectan directamente al concentrador central. La mayoría de los dispositivos se conectan a un concentrador secundario que, a su vez, se conecta al concentrador central.

Gráfico 3: Topología de Árbol.*



* Gráfico 3: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

Entre las ventajas que posee la Topología de Árbol están:

- Esta topología facilita el crecimiento de la red.
- El Hub central al retransmitir las señales amplifica la potencia e incrementa la distancia a la que puede viajar la señal.
- Se permite conectar más dispositivos gracias a la inclusión de concentradores secundarios.
- Permite priorizar y aislar las comunicaciones de distintas computadoras.
- Cableado punto a punto para segmentos individuales.

- Soportado por multitud de vendedores de software y de hardware

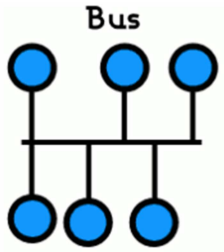
Entre las desventajas de la Topología de Árbol están:

- Se requiere mucho cable.
- La medida de cada segmento bien determinada por el tipo de cable utilizado.
- Si se viene abajo el segmento principal todo el segmento se viene abajo con él.
- Es más difícil su configuración.
- No tiene sentido único.

1.10.4. Topología de Bus.

Una topología de bus **es** multipunto. Un cable largo actúa como (troncal, bus backbone) que conecta todos los dispositivos en la misma red**.** De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

Gráfico 4: Topología de Bus.*



* Gráfico 4: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

Entre las ventajas que posee la Topología de Bus están:

- Esta topología es bien simple y fácil de arreglar.
- Es relativamente más económica ya que requiere menos cableado a diferencia de las otras topologías.
- Facilidad de implementación y crecimiento.
- Simplicidad en la arquitectura.

Entre las desventajas que posee la Topología de Bus están:

- Hay un límite de equipos dependiendo de la calidad de la señal.
- Puede producirse degradación de la señal.
- Complejidad de reconfiguración y aislamiento de fallos.
- Limitación de las longitudes físicas del canal.
- Un problema en el canal usualmente degrada toda la red.
- El desempeño se disminuye a medida que la red crece.
- El canal requiere ser correctamente cerrado (caminos cerrados).
- Altas pérdidas en la transmisión debido a colisiones entre mensajes.
- Es una red que ocupa mucho espacio.

1.10.5. Topología de Anillo.

En una topología en anillo cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino. Cada dispositivo del anillo incorpora un repetidor.

Gráfico 5: Topología de Anillo.*

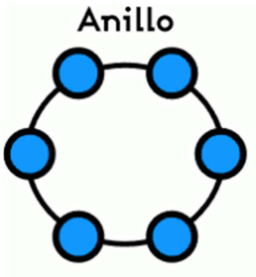


Gráfico 5:http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

Dentro de esta Topología existe una variante, la Topología en un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos).

Entre las ventajas que posee la Topología de Anillo están:

- La Topología de Anillo es relativamente fácil de instalar y reconfigurar.
- Para añadir o quitar dispositivos, solamente hay que mover dos conexiones.
- En la Topología de Anillo hay una señal en circulación continuamente.
- Simplicidad en la arquitectura y facilidad de fluidez

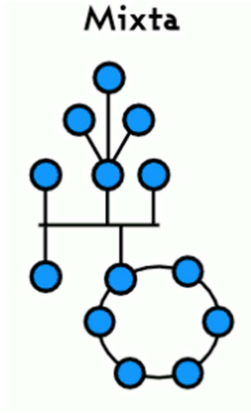
Entre las desventajas que posee la Topología de Anillo están:

- El canal usualmente se degradará a medida que la red crece.
- Máxima longitud del anillo y número de dispositivo
- Difícil de diagnosticar y reparar los problemas.

1.10.6. Topología Mixta.

Esta Topología no sigue un modelo determinado, abarca las anteriores topologías con el fin de asociar un mayor número de dispositivos entre distintas áreas de trabajo, al igual que reforzar la comunicación en el ambiente de red en el que está estructurada.

Gráfico 6: Topología Mixta.*



* Gráfico 6: http://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red

2. Herramientas de Seguridad Informática.

Dentro del área de la informática, se enfoca este tema de la protección de la información y la infraestructura computacional. Basándose y tomando como punto referencial los estándares, protocolos, métodos, reglamentos que respectan a la seguridad informática, Empresas, compañías y personas especializadas se encargan de a través de todos los conocimientos e información anterior mente mencionada, desarrollan herramientas que permiten que la información y la infraestructura de nuestras empresas compañías o laboratorios informáticos no corran posibles riesgos y se pueda evitar problemas de seguridad.

Dentro de lo que es la seguridad informática, se encuentran conformada por, software, bases de datos, metadatos, archivos y toda la información que en una organización sea esencial para su funcionamiento.

Ha este tipo de información dentro de una empresa se la conoce como información privilegiada o confidencial.

Muchas empresa como cabe el caso citar, Symantec, está encargada a través del desarrollo de sus herramientas Antivirus, cuidar y respaldar la información ante posibles amenazas como son los virus.

Symantec a través de sus productos como es el antivirus NORTON, brinda una herramienta que evita que nuestros equipos corran el riesgo de infectarse con virus y amenazas informáticas.

2.1. Existen herramientas de seguridad que realizan un scanner en la seguridad de la Red.

Un scanner de seguridad como herramienta, puede realizar una auditoria informática en busca de vulnerabilidades, realizando una completa exploración de todos los puertos y servicios. Presentándonos como resultado los puntos vulnerables que encuentra y sus posibles soluciones

Existen herramientas que nos permiten escuchar y analizar las conexiones de red a través de los protocolos de red con los que cuente nuestra empresa organización o laboratorio informático.

Dentro de lo que conlleva a la seguridad informática hay herramientas que nos permiten monitorizar todo el tráfico de una red, de esta forma nosotros como usuarios administradores de nuestra red, tenemos la posibilidad de recolectar todo la información posible y detectar las posibles amenazas y problemas que están dentro de nuestra red.

Dentro de nuestro sistema operativo, poseemos una herramienta que nos permite bloquear el acceso no autorizado a nuestro ordenador, para de este modo limitar cifrar, descifrar el tráfico que existe entre nuestro equipo y la red a la que se encuentre conectado, que puede ser tanto la Red Local como el Internet, esta herramienta de nuestro sistema operativo es el Firewall o contrafuego.

Además de éstas tenemos herramientas que nos permiten encriptar nuestra información privilegiada y confidencial. A su vez creando passwords o contraseñas seguras para nuestra información y a su vez que nuestra información se encuentre protegida ante la amenaza de personas no autorizadas y que quieran hacer eso de la misma.

Herramientas que pueden clasificar el nivel y el grado de los problemas y violación de la seguridad, son muy útiles dentro de los laboratorios de informática donde se trabaja y se trata con muchos usuarios diariamente. De esta forma el administrador de la red puede tener un informe de resultados de cada uno de los equipos y de las actividades que se realizaron en los mismos.

3. Delitos Informáticos.

3.1. Que es un delito Informático.

Un Delito informático es un acto que viola y va en contra de los principios de confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes de los datos y de la información privilegiada y confidencial que posee una entidad, empresa u organización.

La delincuencia informática es de difícil comprensión por que en el mayor de los casos se la considera parte de una conducta dentro del ámbito legal y/o jurídico.

Este abuso de los principios de confidencialidad abarca dos ámbitos de acción dentro de los que es la informática, el Hardware y el Software. Básicamente este tipo de delito está dirigido a las tecnologías de la computación y comunicación, el uso indebido de la tecnología para beneficios personales y la utilización incidental, maliciosa o intencional de computadoras con fines que son penados por la ley.

En la actualidad y con los avances tecnológicos, este es un tema que tiene un crecimiento diario, ya que el aspecto más importante y fundamental es la información, ya que esta se ha llegado a convertir en un valor económico dentro de cada una de las empresas entidades u organizaciones.

Dentro de los delitos informáticos existen dos tipos de sujetos, el Sujeto Activo y el Sujeto Pasivo.

3.2. Sujeto Activo.

Son las personas que cometen los Delitos informáticos, ya que tienen los conocimientos y las habilidades para el manejo de sistemas informáticos, además de esto dentro del campo en el que se desarrollan y su situación laboral se encuentran en lugares estratégicos donde manejan la información de carácter sensible.

El perfil de estas personas que son considerados delincuentes informáticos es que son personas decididas, listas, motivadas y dispuestas a aceptar un reto tecnológico, conjunto de aptitudes que le permiten violar y romper cualquier privilegio norma o políticas de seguridad, con el fin de conseguir lo que se propone.

Como Sujeto Activo podemos encontrar dos clasificaciones según el ambiente en el que operan.

Los Insiders (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros.

Los Outsiders (personas que atacan desde afuera de la ubicación física de la organización) ingresaban a la red simplemente averiguando una password válida.

Dentro de los estudios podemos saber que el porcentaje respeto a los Sujetos Activos y su clasificación es la siguiente.

- Insiders 90% dentro de los Delitos Informáticos.
- Los Outsiders 10% dentro de los Delitos Informáticos.

3.3. Sujeto Pasivo.

El sujeto pasivo es el dueño de un bien en este caso respecto a la tecnología informática, es el propietario de una computadora, o bien el administrador de una organización o laboratorio informático, el sujeto pasivo llega a ser la víctima del delito sobre el cual recae la acción o conducta realizada por el sujeto activo.

El Sujeto Pasivo es quien sufre el delito informático, donde la victima puede ser una persona, instituciones financieras como bancos, empresas, gobiernos, etc. Los cuales usan sistemas informáticos y posee sistemas de comunicación y redes.

3.4. Tipos de delito informáticos.

Existen muchos tipos de delitos informáticos pero entre los más importantes están 5 aspectos importantes.

a. El fraude
b. El Sabotaje Informático.
c. El Espionaje Informático, el robo o hurto de software.
d. El robo de servicios.
e. El acceso no autorizado a servicios informáticos.

3.4.1. Respeto a lo que es el fraude informático tenemos los siguientes delitos:

3.4.1.1. Los Datos falsos o engañosos (Data Diddling).

Es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa.

3.4.1.2. Manipulación de Programas o los “Caballos de Troya”.

Consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

3.4.1.3. La Técnica del Salami.

Consiste en introducir un programa dentro de una institución financiera o sea por un medio de comunicación con el que esta trabaje y a través de instrucciones para que remita a una determinada cuenta o cuentas y se vaya transfiriendo un determinado valor de dinero de muchas cuentas corrientes.

3.4.1.4. Falsificaciones informáticas.

Consiste en alteran datos de los documentos almacenados en forma computarizada, para lo cual se utiliza herramientas como fotocopiadoras computarizadas o scanners. De esta forma poder crear documentos falsos así no se requiera de los originales y producir documentos de tal calidad que sea difícil de diferenciarlos de uno que si este autorizado.

3.4.1.5. Manipulación de los datos de salida.

Consiste en el robo de la información electrónica que contiene las bandas magnéticas de las tarjetas bancarias y tarjetas de crédito, mediante equipos electrónicos y de computación.
El caso más común son los cajeros automáticos mediante la clonación de tarjetas y el robo de sus claves de acceso.

3.4.1.6. PISHING.

Consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Estos engaños pueden ser dados por mensajes masivos de páginas falsas o de origen desconocido que aparentan o anuncian mensajes provenientes de instituciones financieras o bancos, el que se solicitan datos personales y contraseñas.

3.4.2. Respeto a lo que es el Sabotaje Informático tenemos los siguientes delitos:

3.4.2.1. Bombas Lógicas (Logic Bombs).

Es un programa informático, el cual consiste en la destrucción o modificación de datos dado por un tiempo en el cual este programado. Estas pueden ser enviadas por mail o por la red propiamente dicha o también pueden ser instalados por medios magnéticos en la máquina que se desea que sufra el daño.

3.4.2.2. Gusanos.

Es un programa informático, el cual consiste en infiltrarse en los programas de procesamiento de datos con la finalidad de modificación o destrucción de datos pero con la diferencia de los virus de que este no se puede regenerar.

3.4.2.3. Virus Informáticos y Malware.

Es un programa informático al igual como el gusano ingresa en el sistema operativo y tiene a duplicarse y contagiar a todas las carpetas que contiene nuestro ordenador, se encuentra de forma encubierta y realiza funciones no autorizadas dentro de nuestro sistema operativo.

El Malware es otro tipo de ataque informático, que mediante el uso de las técnicas de los virus o los gusanos informáticos opera sobre las funciones del sistema operativo causando que este se propague para hacer daños en la información de nuestro computador.

3.4.2.4. Ciberterrorismo.

Este tipo de amenaza se caracteriza por ser un acto que deshabilitar los medios de comunicación o redes de un país o a su vez aplicar presión a un gobierno, utilizando métodos clasificados como sabotaje, limitando los accesos y la comunicación de las entidades gubernamentales de un país y ocasionar el caos y la confusión.

3.4.2.5. Ataques Denegación de Servicio.

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios.
Como ejemplo se puede citar deshabilitar el ingreso de usuarios dentro de un dominio de servidor, para lo cual la base de datos de los usuarios sea inhabilitada o borrada del servidor, y que ningún usuario pueda hacer uso de sus respectivas sesiones y no tenga acceso al sistema.

3.4.3. Respeto a lo que es el Espionaje Informático, el Robo o Hurto de software tenemos los siguientes delitos.

3.4.3.1. Fuga de Datos (Data Leakage).

Este tipo de delito informático se lo conoce también como la divulgación no autorizada de datos reservados, es una variedad de espionaje industrial. Consiste en la sustracción de información confidencial de una empresa u organización, por personas inescrupulosas que trabajan en cubierta dentro de la misma. La forma de proteger la información entro de nuestras empresas es a través de la criptografía.

3.4.3.2. Reproducción no autorizada de Programas Informáticos de protección legal.

Esto consiste en la reproducción no autorizada de un bien jurídicamente protegido en el caso de derechos de autor, propiedad intelectual y protección del software como Derecho Informático, con lo cual se ocasiona una pérdida económica a los propietarios legítimos. Esto es lo que común mente se conoce como la piratería informática y la cual si es penada por la ley.

3.4.4. Respeto a lo que es el Robo de servicios tenemos los siguientes delitos:

3.4.4.1. Hurto del Tiempo del Computador.

Este tipo de delito consiste en el robo del tiempo de uso de uno o más computadores, esto se lo puede explicar de mejor manera dando el caso del servicio de internet dentro de una empresa, a la cual se tiene una clave de acceso para conectarse a la red, esta clave o password es facilitada a otra persona o entidad por una persona no autorizada siendo de esta forma el vínculo, para que se haga uso no autorizado de este servicio, causando un perjuicio tanto a la empresa que paga por el servicio como a su proveedora.

3.4.4.2. Apropiación de Informaciones Residuales (Scavenging).

Consiste en recoger información residual de un trabajo previamente autorizado, esto se lo puede efectuar en archivos físicos como documentos, desecho de papeleras y archiveras o electrónicamente. A el termino Scavenging se lo como recoger basura.

3.4.4.3. Parasitismo Informático (Piggybacking) y Suplantación de Personalidad (Impersonation).

Consiste en la suplantación de personas para cometer el delito informático, tanto filtrándose o mediante la suplantación de identidad y el manejo de artimañas, de esta forma tener acceso a los sistemas o códigos privados de esta forma hurtar la información confidencial, rompiendo de esta forma los códigos de confianza con los que trabaja un empresa u organización.

3.4.5. Respeto a lo que es el Acceso no Autorizado a Servicios Informáticos tenemos los siguientes delitos:

3.4.5.1. Las Puertas Falsas (Trap Doors).

Consiste en alterar el código de programas y sus respectivos procesos, con el fin de introducir partes del código que sea medio para el control de tareas no autorizadas en áreas específicas a las cuales se desee atacar, sin que puedan ser detectadas porque serian parte ya del sistema.

3.4.5.2. La Llave Maestra (Superzapping).

Consiste en un programa informático que tiene la posibilidad de abrir cualquier archivo así este esté protegido, de esta forma poder alterar, borrar, copiar, insertar o utilizar a conveniencia la información o los datos que posea un computador, sin que queden rastros o constancia de dichos cambios.

3.4.5.3. Pinchado de Líneas (Wiretapping).

Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

3.4.5.4. Piratas Informáticos o Hackers y Cracker.

Son personas especializadas, amantes y apasionadas por la seguridad informática para quienes esto es un reto, quienes utilizan todos sus conocimientos y herramientas informáticas con el fin de eludir o desactivar todo lo que conlleve con la seguridad informática sea tanto dentro de un sistema operativo, software o sobre una red de comunicaciones.
La diferencia más importante entre un Hacker y un Craker es que, el Hacker viola las medidas de seguridad informática solo con fines de satisfacción y admiración personal a sí mismo y sobre salir intelectualmente ante las empresas que desarrollan software, y demostrarles que vulnerabilidades tienen sus sistemas.
Mientras que los Crakers utilizan los mismos conocimientos y herramientas especializadas para fines de lucro personal, como robo de dinero en cuentas de bancos, robo de información confidencial y que conlleva altos costos para empresas, y todo lo que conlleve su beneficio propio.

4. Delitos dentro de un laboratorio de Informática.

Dentro de un laboratorio informático, se puede decir que los delitos informáticos no son de mayor gravedad pero sí ocasionan problemas tanto en el servicio que se presta, a sus usuarios y a los privilegios con los que se trabaja.

Se pueden citar que dentro de los delitos informáticos que infringen con las políticas de seguridad, las siguientes:

- Personas con acceso a códigos de acceso y privilegios de administrador que facilitaban esto a amigos o personas conocidas.
- Instalación de programas y software no autorizado.
- El robo del ancho de banda.
- El mal uso de los equipos como Switchs o Routers, ya que se desconectaban los cables de comunicación de los equipos que eran de uso informático, para hacer uso de juegos u otras actividades.
- La sustracción de equipos informáticos y su información por parte de personas inescrupulosas.

5. Delitos informáticos en el Ecuador.

El Ecuador como otros países del resto del mundo ha sido también víctima de los delitos informáticos, el auge y el crecimiento de este tipo de delincuencia se ha ido incrementando cada año, y más aun con los avances tecnológicos acelerados y de los cuales personas inescrupulosas hacen su mal uso.

En el Ecuador se han escuchado varios casos de delincuencia informática, estos datos han sido proporcionados y se encuentran en el historial de la Fiscalía General del Ecuador, entre ellos están los siguientes:

- Robo y Fraude relacionado con elementos Físicos y Lógicos. Caso Laptops y Discos duros Raúl Reyes
- Reproducción no autorizada de Programas Informáticos de protección legal. Pornográfica infantil y trata de blancas, información digitalizada o vía web.
- Robo y peculado, Caso Peñaranda (información relevante Discos Duros de negocios ilícitos).
- Espionaje, Caso revisión Microfilm del Banco Central.
- Suplantación de identidad/Estafas, Caso clonación de páginas del Banco del Pichincha y Banco internacional con mensajes de premios falsos en los que se pide los números de cuanta y passwords de accesos para poder acreditar dichos valores, haciendo uso del nombre de estas entidades bancarios.
- Infracciones de propiedad intelectual, copias ilegales de software y sistemas operativos, así también como de películas o libros en archivo digital con protección de derechos de autor, dentro del país y de las distintas ciudades del Ecuador hay un sin número de locales dedicados a este tipo de negocio.
- Clonación de tarjetas de débito Bancario o tarjetas de crédito, alrededor de 988 estafas.

Dentro de los que son los delitos informáticos el Ecuador ante un caso Judicial se ampara en los siguientes aspectos.

- La instrucción Fiscal
- Dictamen acusatorio
- En el aspecto legal para lo que son los delitos informáticos, el Perito Informático.

Dentro de los aspectos que tenemos para un perito informático ante un caso judicial.

- Perito CPP (Código de Procedimiento Penal)
- Perito CPC (Código de Procedimiento Civil)
- Organismo de Acreditación de Peritos.
- Procedimiento de Acreditación.
- Pérdida de Acreditación.
- Implicaciones Legales.
- Peritaje.

Para un caso judicial acusatorio dentro de lo que es un delito informático existe el proceso de designación ante un delito informático, la posesión de culpa ante un delito, el proceso de ejecución ante el delito, y los resultados en obtención de los peritajes.

El Ecuador en la actualidad y con el incremento del índice delincuencial en el campo de los delitos informáticos, se encuentra ahora amparado contra los delitos informáticos según la legislación de la república, por las siguientes leyes.

- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos.
- Ley de Propiedad Intelectual.
- Ley Espacial de Telecomunicaciones.
- Ley de Control Constitucional (Habeas Data)

Según el Código de Procedimiento Penal CPP, los delitos informáticos son multados y penados con:

Cuadro de procedimiento Penal CPP

Infracción	Represión	Multas
Delitos de información protegida según el (CPP Art. 202)		
1.Violentando Claves o sistemas	6 meses a 1 año	$500 a $1000
2. Seguridad Nacional o secretos comerciales o industriales	3 años	$1000 a $1500
3. Divulgación o utilización fraudulenta	3 a 6 años	$2000 a $10000
4. Divulgación o utilización fraudulenta por custodios	9 años	$2000 a $10000
5. Obtención y uso no autorizado	2 meses a 2 años	$1000 a $2000
Destrucción maliciosa de documentos (CPP Art. 262)	6 años	
Falsificación electrónica (CPP Art. 353)	6 años	
Daños Informáticos (CPP Art. 553)		
1. Daño Dolosamente	6 meses a 3 años	$60 a $150
2. Servicio público o vinculado con la defensa	5 años	$200 a $600

nacional.		
3. No delito mayor	8 meses a 4 años	$200 a $600
Apropiación ilícita (CPP Art. 553)		
1. Uso Fraudulento	6 meses a 5 años	$500 a $1000
2. Uso de medios (Claves, tarjeas magnéticas, etc.)	5 años	$1000 a $2000
Estafa (CPP Art. 563)	5 años	$500 a $1000

* Fuente Manual de Delitos informáticos Fiscalía del Ecuador

6. Normativas que se deben tomar ante la amenaza de un delito informático o violación de la seguridad informática.

Ante la amenaza de un delito informático, muchos de nosotros no sabemos cómo reaccionar y menos aún en casos que se pueden dar el día a día y dentro de la comunidad.
Este tipo de fenómeno quizás no esté bien orientado e informado por parte del gobierno, las leyes y la prensa quienes tienen el deber de informar a la comunidad como ampararse o actuar frente a un delito informático.

Quizás dentro de los casos más comunes en el Ecuador frente a los delitos informáticos son el fraude y el fraude digital.
Se puede citar la clonación de tarjetas de crédito; este modus operandi se realiza a través de equipos y máquinas que retienen la información de las tarjetas de débito bancario y tarjetas de crédito, copiando toda la información de la banda magnética que éstas poseen, además de esto con pequeñas cámaras o celulares escondidos o ubicados en lugares específicos, los cuales capturan las claves de acceso cuando la víctima intenta hacer un retiro o transacción.

Ante este tipo de delito, los usuarios son los únicos responsables del uso de sus bienes y pertenencias, ser precavidos a la hora de hacer transacciones o retiros, mirar bien quien se encuentra en la fila, así también como si se observa objetos sospechosos en los cajas informar oportunamente a las autoridades pertinentes.

Dentro de otro caso común está el Pishing, este tipo de delito se ha incrementado los últimos años, y un sin número de entidades bancarias se han visto involucradas.
Ante este tipo de amenaza, como usuarios tenemos que tener las siguientes consideraciones.

- Si somos usuarios o estamos afiliados a una entidad bancaria y tenemos acceso a un portal Web como a claves de acceso que nos proporciona dicha entidad, esta información es personal e intransferible.
- Nunca debemos facilitar nuestra información.
- Existen mensajes con paginas clonadas de en el mayor de los casos las entidades bancarias con las que trabajamos, ya que los delincuentes se encargan de averiguar oportunamente esta información antes de enviarlas como mensaje.
- Ante un tipo de mensaje vía mail, en el cual se nos informe que hemos sido los ganadores de premios o sumas de valor altas, y que detalladamente se nos da un número de cuenta, se nos pide nuestro número de cuenta y password de ingreso, reportar inmediatamente a la entidad bancaria sobre este tipo de información.
- Ninguna entidad bancaria regala montos de dinero y menos premios vía mail o mensajes.
- Es responsabilidad nuestra como usuarios, velar por la información, los medios de comunicación así también como el tráfico que existe en la red, y aportar para que gracias a nosotros, las entidades bancarias, organismos pertinentes y las leyes que amparan en la república del Ecuador, eliminar este tipo de delitos informáticos.

Otro tipo de delito es la suplantación de identidad, este delito común mente se da en las entidades bancarias así como empresas u organismos que poseen información muy valiosa.

Es un poco difícil identificar este tipo de delito, ya que las personas o las bandas que operan dentro de este campo son muy especializadas. Ya que operan con currículos falsos o en el mayor de los casos son tan difíciles de identificar, que simplemente empresas u organizaciones caen como víctimas.

Quizás la mejor forma de evitar este tipo de delito dentro de una empresa es llevar un control y seguimiento del personal.
Un estudio individual de cada una de la persona con las que trabajamos que puede ser semanal o mensual, con esto identificar algún tipo de irregularidad, índices de mala conducta o intenciones de atentar contra los intereses de nuestra empresa u organización.

Cada empresa u organización debe tener dentro de sus políticas cláusula de seguridad ente este tipo de delitos y que servirán oportunamente para optar por las medidas pertinentes si se amerita el caso.

7. Deficiencias y problemas en la red del LTIC.

En los últimos años, el laboratorio LTIC ha realizado algunos cambios respecto a lo que son sus equipos, medios de comunicación e infraestructura.

El LTIC adquirió nuevos equipos de comunicación, equipos de escritorio para las aulas, como también computadores portátiles, dos nuevos servidores, pero esto no basta para satisfacer y brindar un servició óptimo.

Quizás el principal problema por el cual pasa el laboratorio LTIC, son los estándares con los que se trabaja a nivel de toda la Universidad.

El LTIC como parte de la Pontificia Universidad Católica del Ecuador, debe atenerse a los estándares con los que se trabaja respectivamente, dados por la Dirección de informática de la PUCE.

En el último periodo del año 2013, se ha logrado actualizar los equipos de comunicación que posee el laboratorio LTIC, ahora este cuenta con equipos de comunicación CISCO.

El problema más común que maneja el LTIC conlleva es la comunicación y dentro de esta están varios aspectos, los cuales citaremos a continuación:

- Inicialmente en la construcción del nuevo edificio de Ingeniería, carreras de Sistema y Civil, donde se encuentra las instalación del LTIC (2 nivel), se planifico que el medio de comunicación y la red sea inalámbrica y no se contó con un sistema de cableado o red LAN.
- Una red LAN proporciona a los usuarios seguridad y la capacidad de mover muchos datos de manera rápida y efectiva.
- Según el monitoreo realizado, se pudo identificar que además de los equipos con los que cuenta el LTIC, existe alrededor de unos 180 a 190 equipos que son parte de los estudiantes de Ingeniería y que hacen uso de la red, dentro de estos contamos con laptops, celulares, pads etc.

- El ancho de banda con el que cuenta el LTIC en estos momentos es de 3MEGAS, los cuales no cubren las necesidades de comunicación y hay sectores en donde la señal inalámbrica no está presente.
- Se ha identificado el uso inadecuado de la red del LTIC, ya que en algunos casos se utiliza para fines no académicos, si no que esta se utiliza como medio de comunicación para juegos u otras actividades no educativas, lo cual ocasiona que la velocidad disminuya significativamente.

7.1 Visión Global e Histórica del LTIC

Durante el periodo de inicio de actividades del LTIC del 2005 al último periodo al 2014, han existido muchos avances y mejoras tanto tecnológicas, de seguridad y servicios.

Detalladamente la evolución histórica del LTIC se ha visto reflejada por cada uno de los directores que han tomado el cargo durante todos estos años.

Periodo correspondiente al Ing. Xavier Condor Director 2005 al 2008

Software y Hardware:
Se han adquirido los siguientes equipos:
- Dos servidores HP Proliant ML350 con procesador Xeon de 3.2 GHz y 70 GB de disco duro.
- Conexión autónoma con Internet.
- 5 PCs HP de última generación.
- 6 Cámaras de seguridad.
- 2 Switchs 3COM de 100 MBPS.
- 1 UPS.
- Un disco duro USB portátil de 250 GB.
- 15 licencias de Mathlab 7.0.
- Todo el software que el Campus Agreement com Microsoft lo permite.
- 2 multímetros y 3 ponchadoras.
- 1 Access Point Wireless.

Donaciones:
- Se han donado los siguientes equipos:
- Un acces point Wireless, donado por el Ingeniero Roberth Henríquez

Proyectos realizados:
- Se han concretado los siguientes proyectos:
- Normativa Interna del Laboratorio de Computación.
- Intranet de la Facultada (A cargo de la Ing. Beatriz Campos)
- Acceso autónomo al Internet a los Profesores y Estudiantes que utilizan el Laboratorio de Computación.
- Acceso al Internet por medio de Wireless, usando el access point.
- Generación de cuentas de usuario propias para Profesores y Alumnos a través de uno de los nuevos servidores.
- Asignación de espacio personal para Profesores y Alumnos en la Red del Laboratorio.
- Cambio de la Red interna del Laboratorio de 10 MBPS a 100 MBPS utilizando los 2 switches.
- Montaje de la Red para el Aula 3 del Laboratorio.
- Atención continua e ininterrumpida de Lunes a Viernes de 7h00 a 20h00

Periodo correspondiente al Ing. Francisco Rodríguez Director 2008 – 2009 (1 semestre)

Proyectos realizados:
- Se habilito el servidor Proxi
- Se habilito el servidor de Seguridad
- Se habilito la plataforma Moodle, esto se dio para uso educativo y dictar clases a los docentes
- Se habilito la plataforma Simbra
- Se habilito plataforma de video BigBlueButton para uso educativo entre los estudiantes
- Implementación de solución del sistema de ventilación para el cuarto de servidores.
- Cursos de TI para docentes de la Pontifica Universidad Católica del Ecuador a través de la dirección académica.
- Se habilito video conferencias con el equipo Policom, conferencias con las universidades de Tokio y Houston
- Implementación de Ips públicas a través de los servidores Linux, creación de subdominios.
- Actualización y migración de IP4 a IP4 clase c y b, adicional implementación de subnetix
- Configuración y logística respecto al cableado estructurado y conexión con servidores LTIC
- Implementación de la plataforma Untangle en el servidor, implementación de políticas de seguridad y accesos, implementación de antivirus para IPs publicas.

Donaciones y convenio.
- Optimización de convenios con las casas comerciales Oracle y Microsoft
- Donación de software Microsoft y paquetes Adobe

Periodo correspondiente al Ing. Susana Masapanta Director 2009 – primer semestre del 2013.

Software y Hardware:
- Renovación de las computadoras de escritorio en las aulas 201, 204, 214 y 215.
- Cableado en las aulas 201, 204 y 215 con 16 puntos, 20 puntos y 20 puntos de red respectivamente.
- Renovación y aumento de cámaras de seguridad en cuatro puntos: entrada, sala de becarios, aula 203 y aula 214.
- Compra de un servidor para la administración de las cámaras.
- Instalación de los sensores de acceso con tarjetas magnéticas y los diferentes controles dentro del LTIC.
- Compra de nuevo servidor marca HP para el servidor Web.
- Servidor de impresión con una impresora en red, escáner y plotter

Proyectos Realizados.
- Instalación, configuración, pruebas y puesta en vivo del sistema de acceso con tarjeta magnética a las aulas y zona administrativa.
- Configuración de las tarjetas de acceso para los docentes, administrativos del LTIC y para los estudiantes que solicitan una computadora.
- Configuración en el servidor de Aplicaciones:
- Creación del nuevo portal de ingeniería.
- Puesta vivo de diferentes aplicaciones Web dentro del portal.
- Configuraciones de servicios de seguridad en el Proxy y en el servidor de aplicaciones.
- Configuración en el servidor de Dominio:
- Políticas de acceso para los usuarios del dominio.
- Configuración del servidor KMS para la activación de las licencias de Office.
- Políticas para la creación de usuarios y renovación de contraseña.
- Virtualización del servidor de Dominio como medida de respaldo en caso de daño físico o lógico.
- Cambio de los equipos de red en el core principal para el cableado interno.

Periodo correspondiente al Ing. Alberto Pazmiño Director 2013 Agosto a Febrero 2014

Software y Hardware:
Se encuentra ya aprobado por todas las instancias y en proceso de compra lo siguiente:
- SPSS
- MathLab
- Unity Pro
- Power Designer
- Antivirus
- Ipad AirGalaxy Note
- Teléfonos celulares Android , IOS y tablets para prácticas de Sistemas Operativos
- Implementos varios para la asignatura de Electrología y Circuitos Lógicos.
- En el aula 214 se instalaron 6 computadoras más, con lo cual se amplía a 18.

Donaciones y convenio.
- Productos como los de Oracle y Microsoft los hemos obtenido gracias a sendos convenio específicos para el LTIC alcanzados con estos dos fabricantes.
- Mediante el convenio DreamSpark con Microsoft, administrado directamente por el LTIC, hemos dotado de productos tales como Visual Studio, así como del sistema operativo Windows 8.1. Este convenio cubre una variedad de licencias excepto la suite de oficina.
Los señores profesores y los estudiantes pueden reportar sus requerimientos al LTIC para suministrarle el producto o abrirle una cuenta para que ellos mismos o sus alumnos bajen lo que necesiten.
- Con IBM está en proceso el convenio Academic Iniciative, este si es por medio de la DI, ya que esta firma lo ofertó como valor agregado en un concurso, pero esperamos poder administrarlo directamente en el LTIC para la obtención de productos de este fabricante, lo que eventualmente podría incluir hardware.

Proyectos
- Ancho de banda de la red wifi de sistemas
Hemos ampliado nuestro ancho de banda del LTIC de 3.6 a 60.0 Mbps, en el marco del convenio con CEDIA.
- Como recursos humanos, se integró como asistente del LTIC al Mtr. Damián Nicolalde, quien ya está colaborando de una manera muy eficiente en nuestro laboratorio.
- En cuanto a los becarios, esta figura desapareció como tal y se dio paso a la figura de estudiantes para proyectos formativos 1 y 2. Mediante esta figura disponemos de la colaboración de3 estudiantes.
- Mediante la figura de ayudantes tenemos la colaboración de estudiantes adicionales con cuya colaboración hemos realizado las actividades operativas detalladas abajo.
- Se van a cablear las aulas 214 y 215 para mejor servicio.
- Se van a ampliar a 20 los computadores en todas las aulas.
- Todo lo anterior se va iniciar una vez determinemos la disponibilidad de presupuesto que quede luego de las adquisiciones detalladas arriba.

Facilidad de acceso a las aulas
- Actualmente los señores profesores deben acudir al borrador a al basurero para impedir que la puerta del aula se cierre y puedan circular de mejor manera los estudiantes. Esto desvirtúa por completo el esquema de seguridad, por lo que hemos analizado alternativas con el proveedor del sistema de control de accesos llegando a la definición de que al entrar el profesor se desbloquea la puerta hasta tanto él decida bloquearla. Esto permitirá que cada profesor, de acuerdo con sus políticas, defina durante cuánto tiempo de su clase pueden entrar estudiantes o en qué momento bloquea el acceso. Oportunamente se darán las respectivas instrucciones previas a la entrada en vigor de esta modalidad.

Actividades operativas
Desde el mes de agosto del 2013 hasta la fecha se han realizado las siguientes actividades:

- Se habitó el aula 215, verificando computadora por computadora las máquinas virtuales
- Se lo dedico a revisar la documentación existente del laboratorio, la parte del manejo de las tarjetas, se desarrolló las plantillas de ayudantes con su horario, también se hizo una convocatoria a las personas interesadas.
- Se citó a los ayudantes para capacitarles tanto en el uso de las tarjetas como en el mantenimiento de las máquinas virtuales, se conversó con Javier Cóndor para arreglar detalles para la utilizar las aulas.
- Se capacitó a los otros estudiantes para el uso de dominios, también se hizo que ciertas máquinas las metieran en el dominio creado con el nuevo servidor.
- Se incluyó en el dominio creado a todas las computadoras de las aulas del laboratorio, se rehabilitó el escáner, se vio el estado de la impresora de red.
- Se verificó el funcionamiento de las máquinas virtuales en las aulas 201, 203, se reparó las máquinas virtuales defectuosas, también se tuvo una reunión con Andrés Jiménez para coordinar horarios adicionales en las aulas del laboratorio, conjuntamente con él se verificó el estado de las aulas, en las cuales Andrés trabaja.
- Se comenzó a realizar el inventario de los gabinetes del área de la Oficina de la Becaria
- Se revisó exhaustivamente el software de recepción.
- Se verificó el funcionamiento de las máquinas virtuales en las aulas restantes, también se organizó el aula solicitada por Javier Cóndor para que se cuente con 30 estudiantes
- Se finalizó el inventario de los gabinetes del área de la Oficina de la Becaria
- Se capacitó a los ayudantes para la realización de tareas.
- Se formateo una computadora nueva, para la instalación de programas básicos.
- Se formateo 5 computadoras nuevas, para la instalación de programas básicos, esto en sí fue una capacitación para los estudiantes que no saben estos procesos de instalación, los usuarios puestos son: USUARIO: becario, CONTRASEÑA: LTIC.2013
-Se conversó con Javier Cóndor, y nos pidió que le ayudemos con un cable HDMI de 5 ó 10 metros para la conexión.
-Se realizó una reunión con 3 estudiantes de 6to nivel, las cuales están interesadas en la ayudantía, para lo cual se les incluyó en la franja de ayudantes para proyectos y tareas especializadas (redes, programación extrema).
- Se revisó las instalaciones de la red de cableado, logrando reparar los lugares en donde había errores de comunicación, también se detectó que el cable UTP de la antena inalámbrica de red del aula 203, debe ser cambiado.
-Se revisó el funcionamiento de cada una de las computadoras de las aulas del laboratorio.
- Se asesoró a las ayudantes encargadas de Proyectos de Modelado en 3D
- Se verificó el estado de las 14 portátiles, que se encuentran en su oficina, adicionalmente se realizó la limpieza en servidores.
- Se asesoró a las ayudantes encargadas de Proyectos de Modelado en 3D

Revisión de Informes de Ayudantía
- Asignación Aula 201 para Nuevas Técnicas de Programación
- Instalación de Windows 7 en computadores nuevos
- Rehabilitación computadoras MAC
- Revisión de Informes de Ayudantía
- Instalación de Windows 7 en computadores nuevos
- Rehabilitación computadoras MAC
- Revisión de actividades semestrales para LTIC
- Coordinación Cursos y Capacitaciones LTIC
- Instalación de Windows 7 en computadores nuevos
- Rehabilitación computadoras MAC
- Revisión de actividades semestrales para LTIC
- Coordinación Cursos y Capacitaciones LTIC

- Asignación Temporal Aula 214 para Andrés Jiménez
- Revisión Aula 204
- Rehabilitación computadoras MAC
- Revisión de actividades semestrales para LTIC
- Coordinación Cursos y Capacitaciones LTIC
- Revisión de Informes de Ayudantía
- Rehabilitación computadoras MAC
- Revisión de actividades semestrales para LTIC
- Coordinación Cursos y Capacitaciones LTIC
- Instalación Máquina Virtual Matlab Aula 201
- Se realizó la lista definitiva de las personas que van a estar en la Ayudantía, también se verificó el estado de una computadora en el aula 201, en la que Rafael Melgarejo mencionaba que existía problemas.
- También se instaló un software para Lenguajes de Programación.
- Cabe mencionar que existieron problemas, ya que algunos de los ayudantes de la franja de las 11 a 13, no asistieron.
- Se incluyó en la lista de ayudante a Mariela Monge.
-Se conversó con Andrés Jiménez, para darle las facilidades en las aulas 205 y 201.
- Se le asignó a Patricio Córdova una tarjeta, para el acceso como profesor
- Se Instaló Visual Studio 2012
-Se asesoró a las ayudantes encargadas de Proyectos de Modelado en 3D
- Se asignó el aula 204 a Gestión Hotelera
- Se creó la tarjeta para el profesor
- Se instaló Racket en las portátiles
- Se asesoró a las ayudantes encargadas de Proyectos de Modelado en 3D
- Se instaló la máquina virtual GIS en el aula 204, asignada para Gestión Hotelera.
- Se habilitó el plotter.
-Se incluyó una computadora adicional en el aula 201, según el pedido de Rafael Melgarejo.
- Coordinación del Curso de Android con el Experto.
- Coordinación de Proyecto de reconocimiento de Patrones Corporales en blender con Kinect
- Adecuación del Aula 204 para Jorge Alarcón.
- Asignación del Aula 201 para PHD. Danilo Chávez
- Readecuación y mantenimiento de Computadoras MAC
- Readecuación y mantenimiento de Computadoras MAC
- Asignación de tareas específicas para ayudantes de LTIC
- Aula 204, computadora de la puerta, instalación visual studio, máquinas virtuales
- Inventario Área de Mantenimiento
- Instalación de Octave en el Aula 201
- Aula 204, Verificación Estado máquinas virtuales (java, .net y gis)
- Instalación Unity Aula 215 y en Portátiles.

7.2 Visión del LTIC proyectada a los 2 próximos años.

Con los avances tecnológicos, culturales, sociales y académicos, el laboratorio LTIC ha tomado diferente actividades durante los últimos años a partir de su iniciación.

Como visión futura lo que se espera es una mejora respecto a la plataforma de comunicación de RED que se está utilizando actualmente, CISCO.

Se planifica utilizar una sola plataforma, y los equipos con los que se trabaja actualizarlos a esa única plataforma.

Mejorar todos los servicios e implementar otros según las necesidades de los docentes y estudiantes.

Estar en un correcto proceso de actualización y mejora continua.

Finalizar los proyectos que se planten para cada periodo semestral.

Capitulo II

8. Herramientas de monitoreo y control para la seguridad en la red del LTIC.

Para la propuesta en detección de problemas de seguridad en redes LAN y WLAN para el LTIC se va a utilizar las siguientes herramientas:

- Parallels.
- PRTG.
- Spiceworks.

Y como una variante adicional del software Parallels, VMWARE.

8.1. Parallels.

Parallels es una herramienta para soluciones de virtualización a alto nivel para cualquier campo tanto de trabajo investigación o desarrollo. Con el cual se puede consolidad cargas de trabajo múltiples en una sola estación de trabajo a alto rendimiento, sin sacrificar el rendimiento de aquellas aplicaciones de elevado consumo gráfico.

Parallels permite Ejecutar cargas de trabajo de elevado consumo gráfico en distintas máquinas dedicadas en una única Workstation.

Parallels permite no tener que reiniciar entre entornos de SO para acceder a distintas cargas de trabajo.

8.1.1. Requerimientos.

Parallels soporta los siguientes dos modos operativos:

1. Modo de conexión de red y gráficos emulados.

2. Modo de conexión de red y asignación directa de gráficos.

Requisitos de software.

Parallels es una herramienta multiplataforma que trabaja con los siguientes sistemas operativos.

Distribución Windows

- Windows Vista SP1
- Windows XP SP2 o SP3
- Windows 7
- Windows Server 2008 R2, SP2, SP1, SP0
- Windows Server 2003 R2, SP2, SP1, SP0
- Windows 9X,NT

Distribución Linux

- Debian 5.0
- Fedora 11
- Mandriva 2009
- OpenSUSE 11.1
- RHEL 5.3
- SLES 11
- Ubuntu 9.04

Distribución Mac

- Mac OS X Snow Leopard 10.6.3 o posterior
- Mac OS X Leopard v10.5.8 o posterior

8.1.2. Compatibilidad.

Compatibilidad software Parallels para computadores de escritorio.

- Procesador x64 o x86 a 700 (o superior) MHz (Intel o AMD).
- 256 MB o más de RAM.
- 50 MB de espacio en disco duro para la instalación de Parallels Transporter Agent.
- Adaptador de red WiFi o Ethernet para la migración sobre red.
- Puerto USB para la migración utilizando el cable USB de Parallels.
- Versiones soportadas de Windows y Linux: Windows 7, Windows Vista, Windows XP, Windows Server 2003, Windows 2000, Red Hat Enterprise Linux 5, Ubuntu Linux 8.04.

Compatibilidad software Parallels para Servidores.

- Procesador: 1 o 2 CPUs con procesadores Intel Xeon de la serie 5500 o 5600
- Memoria: Se recomienda un mínimo de 8 GB de RAM
- Disco duro: 0 GB de espacio en disco por máquina virtual. El tamaño requerido de espacio en disco duro dependerá del SO, aplicaciones y datos de la máquina virtual.
- Adaptador de red WiFi o Ethernet para la migración sobre red.
- Puerto USB para la migración utilizando el cable USB de Parallels.

Sistemas Operativos huéspedes suportados

8.1.3. Sistemas operativos de 32 bits.

- Windows 7
- Windows Vista SP 0, SP 1, SP 2
- Windows Server 2008 R2, SP2, SP1, SP0
- Windows Server 2003 R2, SP2, SP1, SP0
- Windows XP Professional SP3, SP2, SP1, SP0
- Windows XP Home SP3, SP2, SP1, SP0
- Windows 2000 Professional SP4
- Windows 2000 Server SP4
- Windows NT 4.0 Server SP6
- Windows NT 4.0 Workstation SP6
- Windows ME
- Windows 98 SE

- Windows 95
- Windows 3.11
- MS-DOS 6.22
- Red Hat Enterprise 5.x, 4.x
- Fedora 14, 13, 12
- Ubuntu 10.10, 10.04, 9.10, 9.04, 8.10
- CentOS 5.x, 4.x
- Debian 5.0
- Suse Linux Enterprise Server 11, 10 SP2
- Suse Linux Enterprise Desktop 11
- OpenSUSE Linux 11.x
- Mandriva 2010, 2009
- Solaris 10
- Open Solaris 2009.06
- FreeBSD 8.x, 7.x
- OS/2 Warp 4.5, 4
- eComStation 1.2
- Mac OS X Leopard Server 10.5.x
- Mac OS X Snow Leopard Server 10.6.x

8.1.4. Sistemas operativos de 64 bits.

- Windows 7
- Windows Vista SP 0, SP 1, SP
- Windows Server 2008 R2, SP2, SP1, SP0
- Windows Server 2003 R2, SP2, SP1, SP0
- Windows XP Professional SP2
- Red Hat Enterprise 5.x
- Fedora 14, 13, 12
- Ubuntu 10.10, 10.04, 9.10, 9.04, 8.10
- CentOS 5.x
- Debian 5.0
- Suse Linux Enterprise Server 11, 10 SP2
- Suse Linux Enterprise Desktop 11
- OpenSUSE Linux 11.x
- Mandriva 2010, 2009
- Solaris 10
- Open Solaris 2009.06
- FreeBSD 8.x,7.x
- Mac OS X Leopard Server 10.5.x
- Mac OS X Snow Leopard Server 10.6.x

8.1.5. Características de la aplicación.

- Parallels fue diseñado específicamente pensando en las necesidades de los usuarios de aplicaciones de elevado consumo gráfico y alto desempeño en redes de comunicación.
- Parallels permite la visualización de exploraciones en distintas plataformas de SO.
- Parallels está creado para trabajar en sectores de trabajo como: industria, educativo, medico, laboratorios computacionales, laboratorios de investigación, gobiernos, empresas y compañías.
- Parallels permite trabajar en sistemas operativos de 32bits como 64 bits y la transición de sus respectivas aplicaciones.

- Parallels gracias a sus equipos remotos permite simultáneamente trabajar con múltiples usuarios en una workstation, lo que le ayuda a reducir costes y aumentar los niveles de seguridad y eficacia.
- Parallels permite acceder de una forma remota.
- Parallels cuenta con una herramienta de acceso remoto para ipad o iphones llamada Parallels Mobile si se desea tener acceso a nuestras aplicaciones y programas Windows.
- Parallels gracias a su motor multiplataforma permite trabajar en el sistema Operativo con el cual se trabajamos.
- Parallels trabaja sobre Windows Linux y Mac.
-

8.1.6. Plataformas en las que se puede utilizar.

Parallels es una herramienta de virtualización y automatización multiplataforma.

Trabaja sobre plataformas y sistemas operativos:

- Windows.
- Linux
- Mac

8.1.7. Funcionamiento y Pruebas de la aplicación.

8.1.7.1. Instalación de la Aplicación.

Parallels se conecta con el servidor y ver si existen versiones actualizadas disponibles, o simplemente la versión de instalación que viene con la licencia.

Instalación en Mac:

Imagen 1: Ventana Instalación Parallels



8.1.7.2. Cláusulas de instalación y Términos de Licencia

Imagen 2: Ventana contenido instalación Parallels

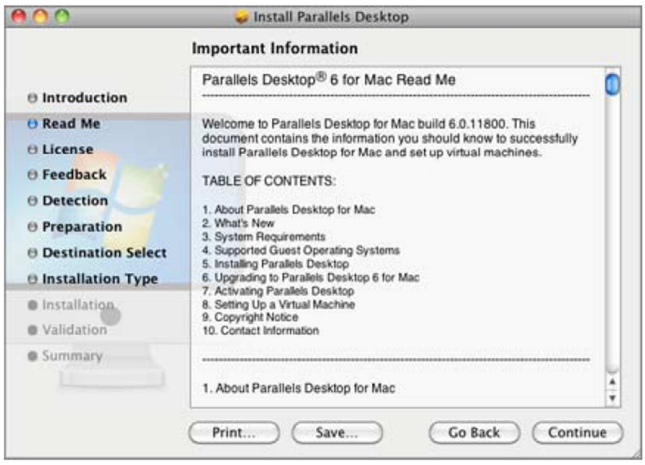
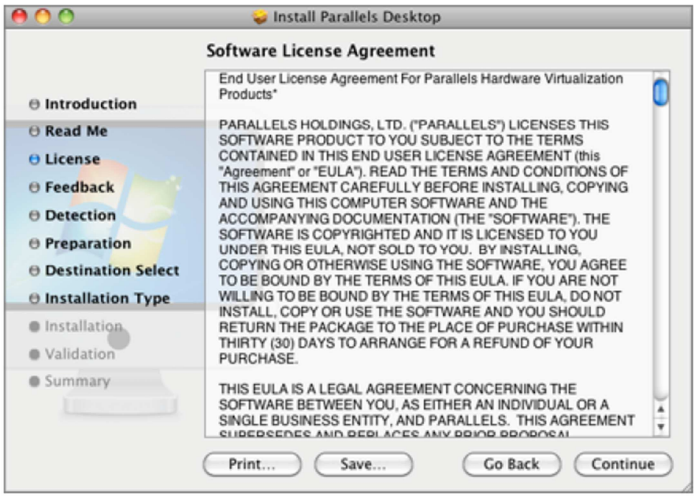
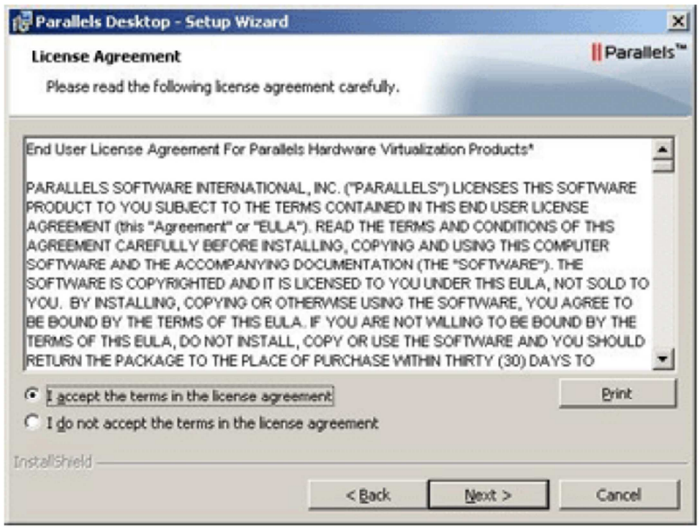


Imagen 3: Licencia Parallels



Instalación en Windows.



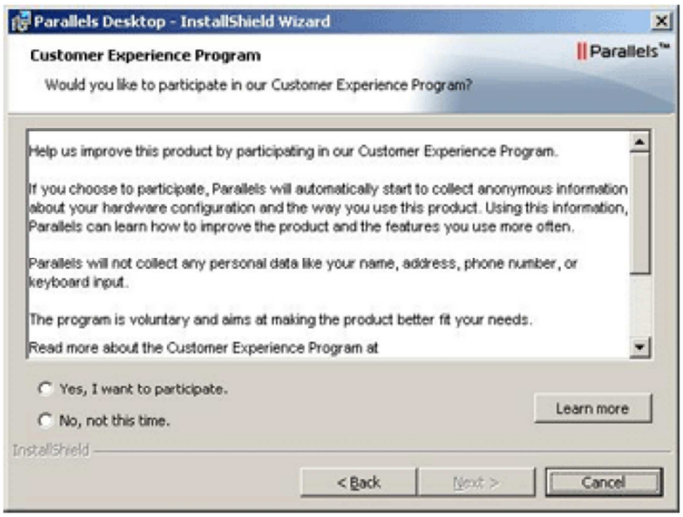


Imagen 5 -6: Términos de aceptación Licencia Parallels

Dentro de la instalación permite seleccionar un disco de destino para el software, como normalmente viene en los estándares de instalación de software.

Luego de seleccionar el disco de destino, se acepta las cláusulas de uso y de licencia de uso para Parallels, se continúa con los pasos de instalación.

Se ingresa el password de nuestra licencia y se continúa con los procesos de instalación hasta que se complete.

Terminada la instalación se creará un icono de la aplicación Parallels.

Esto tanto para lo que son las plataformas Windows Linux y Mac.

8.1.7.3. Aplicación en sistema operativo Mac.

Ventana de Acceso:

Imagen 7: Icono de la Aplicación Parallels

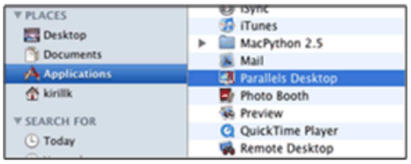


Imagen 8: Ventana de activación del producto



En esta ventana se ingresa un nombre de usuario, organización y la clave de activación del producto.

Imagen 9: Venta de asistente de creación de máquina virtual



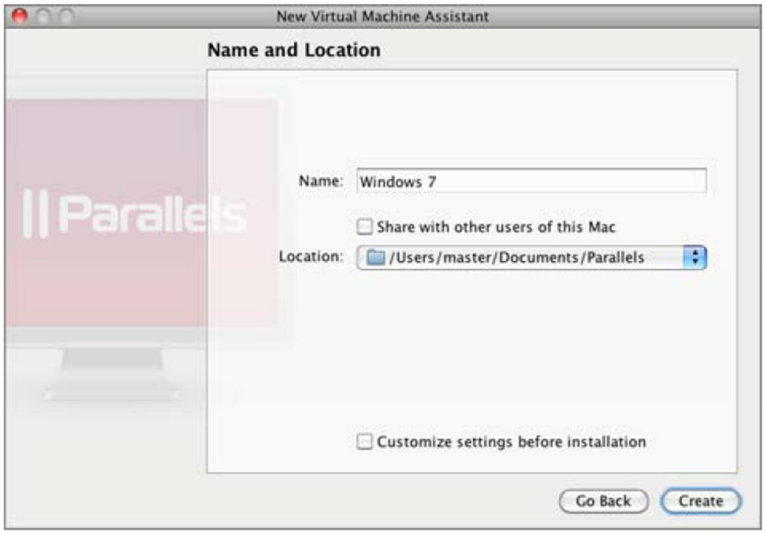
Imagen 10: Creación de máquina virtual Window 7



Imagen 11: Creación de máquina virtual Window 7



Imagen 12: Ventana de máquinas virtuales existentes.



Esta ventana muestra las máquinas virtuales que se posee con Parallels.

Imagen: Sistemas Operativos máquina virtual Parallels

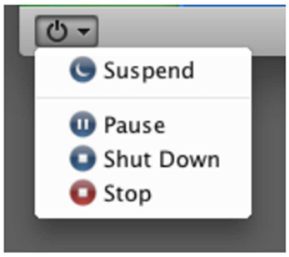


Para iniciar una máquina virtual se presiona en el botón de arranque.



En el botón de inicio existe una pestaña desplegable que sirve para suspender la virtualización, pausar y apagarla.

Imagen 14-15: Procesos de Virtualización con Parallels



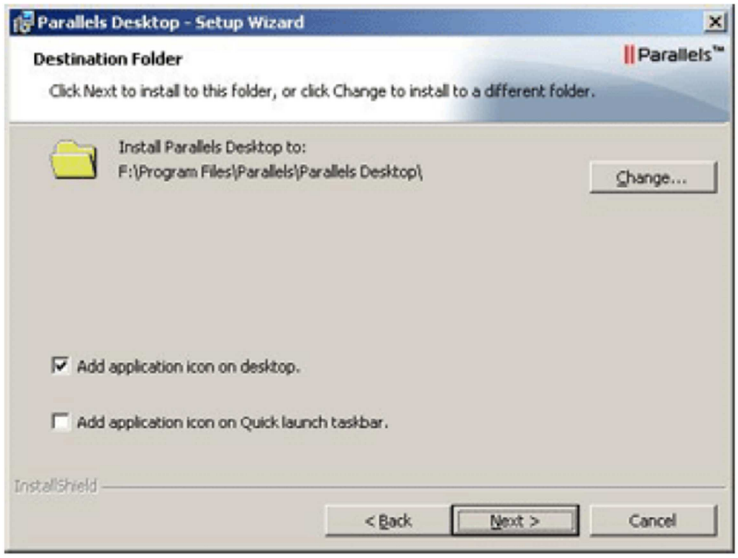


***** Imagen 1 a la 15: Imágenes de proceso de instalación y virtualización en motor Parallels

8.1.7.4. Aplicación con sistema operativo Windows.

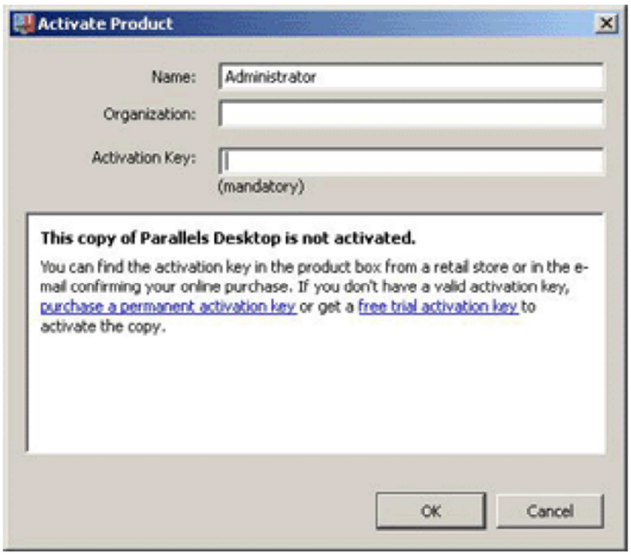
Folder destino para Parallels en Windows.

Imagen 1: Ventana de instalación Paralles Windows



Ventana de activación del producto, al igual que en Mac, los campos solicitados son nombre de usuario, organización y el password de activación del producto.

Imagen 2: Ventana de activación Parallels



Al igual que con la licencia de instalación para Mac debemos aceptar las políticas de uso de la Licencia.

Ventana de asistente de creación de máquina virtual.

Imagen 3: Ventanas de instalación Creación de máquina virtual

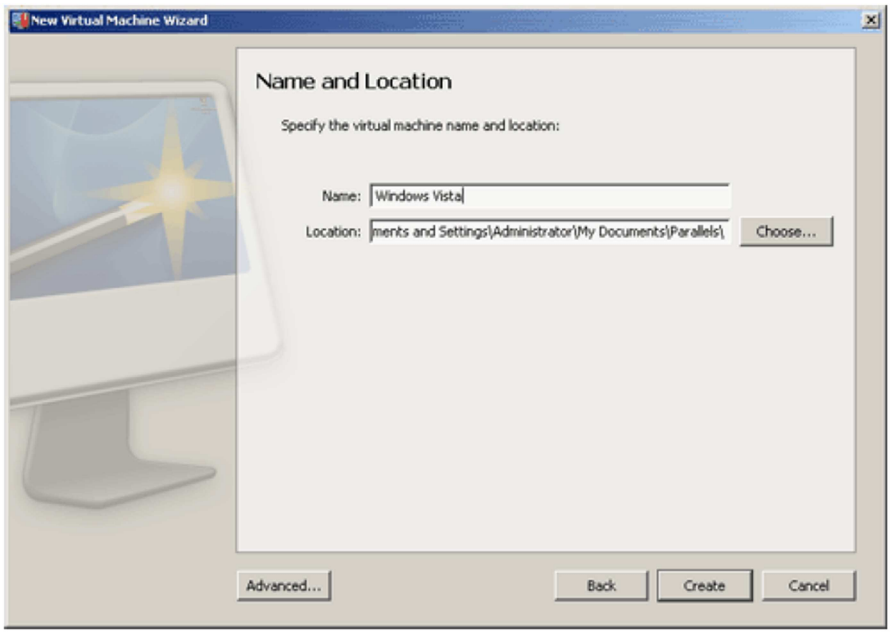
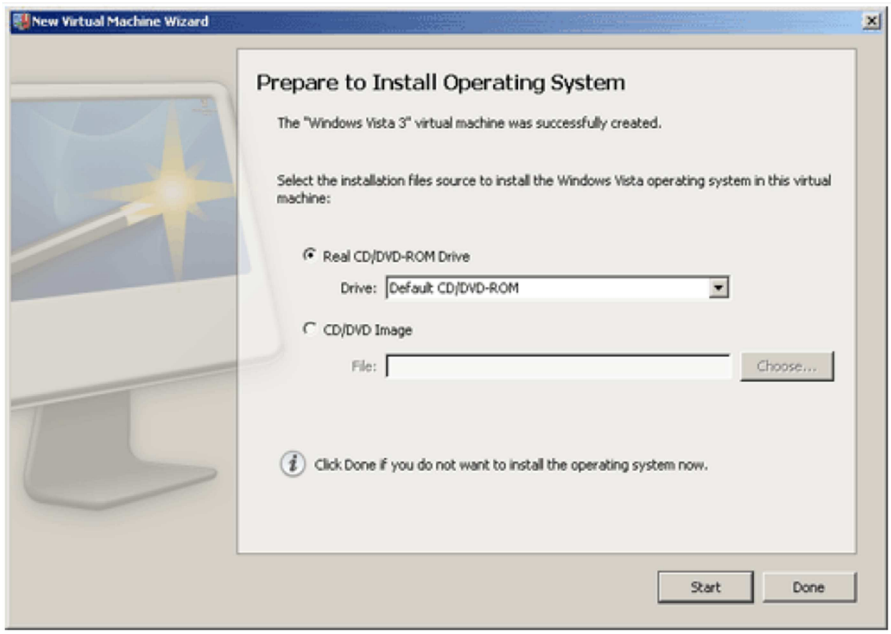


Imagen 4: Ventanas de instalación Creación de máquina virtual



Al igual que en la versión de Mac, para iniciar una máquina virtual se presiona en el botón de arranque.

Imagen 5: Botones control máquina virtual Parallels



Para detener la virtualización en el botón de Stop o Shut Down, para suspender la virtualización está el botón suspend.

Virtualización en Window con Paralles:

Imagen 6: Ventana de virtualización.

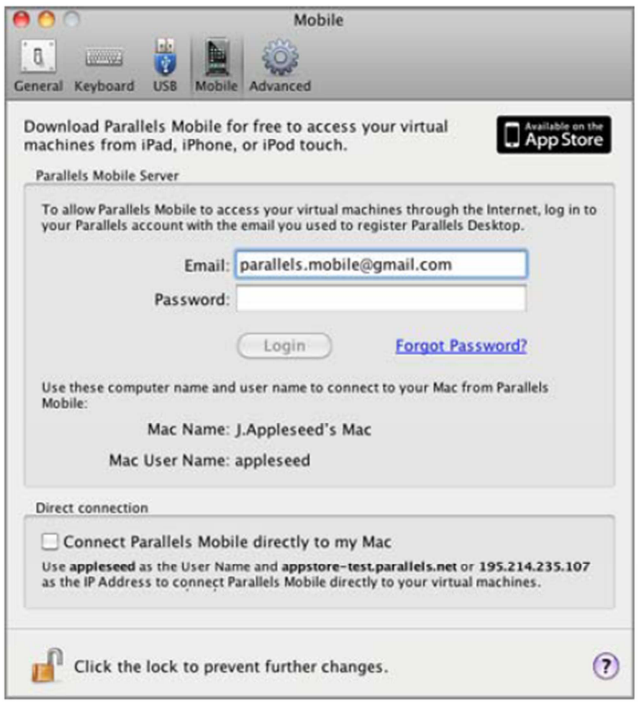


* Imagen 1 a la 6: Capturas de instalación procesos de virtualización en Windows

8.1.7.5. Aplicación Parallels Mobile.

Descargamos la Aplicación Parallels para dispositivos móviles, aquí se pedirá un email y un password para la creación de la cuenta de acceso, además de esto se debe configurar el acceso para que se direccione a la dirección IP de la máquina, para el acceso remoto.

Imagen 1: Aplicación Parallels en Mobile



Al momento de instalar la aplicación en dispositivos móviles, como puede ser Ipad o iPhone aparecerá un icono de acceso a Parallels.



Al acceder a la aplicación en el dispositivo móvil se tendrá la primera ventana de acceso.

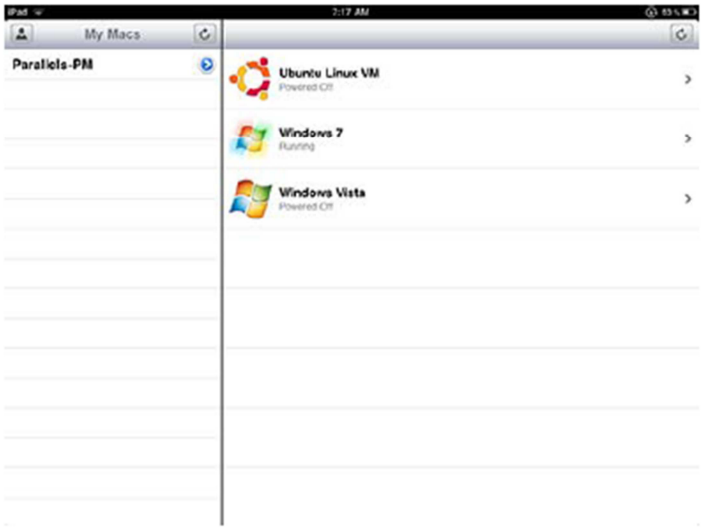
Donde se pedirá el mail y el password con el que se creara la cuenta.

Imagen 2: Ventana de ingreso aplicación Parallels



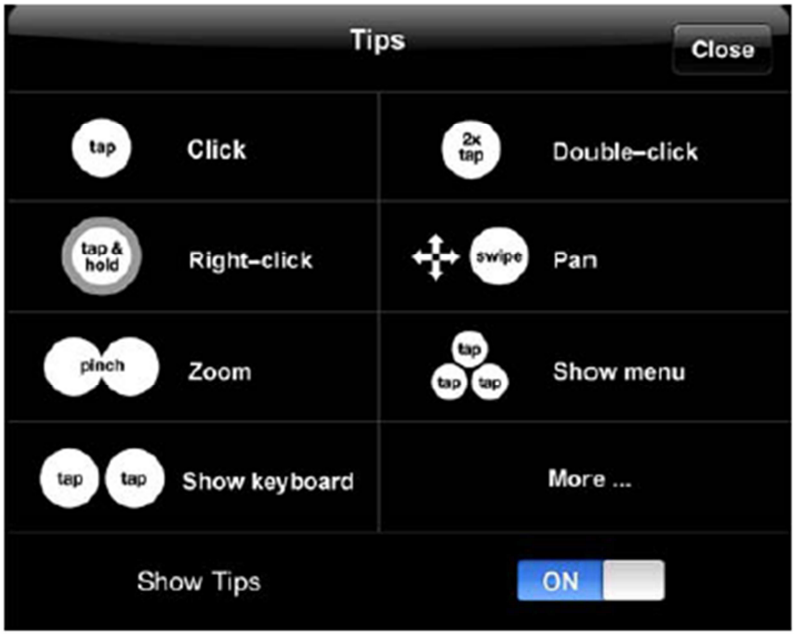
Al acceder a nuestra cuenta se mostrara las máquinas virtuales instaladas en la computadora y que mediante esta aplicación se puede acceder remota mente.

Imagen 3: Máquinas virtuales aplicación Mobile



Se cuenta con comandos especiales para la virtualización remota, desde un dispositivo móvil táctil.

Imagen 4: Mandos de control aplicación Mobile



Al seleccionar la virtualización que se desea correr en el dispositivo móvil, se mostrara una ventana con un icono de arranque.



 Este botón es para iniciar la máquina virtual si esta está detenida o para apagarla si esta está en ejecución.

 Este botón es para restaurar la máquina virtual.

 Este es botón para suspender su máquina virtual.

 Este botón es para pausar la máquina virtual.

 Este botón es para actualizar la instantánea en vivo de la máquina virtual.

Vista de la virtualización en dispositivo móvil.

Gráfico 5: Virtualización en Mobile



* Imagen 1 a la 5: Capturas de virtualización en Mobile plataforma Parallels

8.2. PRTG

PAESSLER
the network monitoring company

PRTG Network Monitor es un programa para Windows para monitorizar el ancho de banda y para analizar datos en redes.

Como administrador de sistemas, PRTG le facilita recibir datos en tiempo real, no solo referentes al estado actual de la red sino también estadísticas mostrando las tendencias de uso a largo plazo. Estos valores registrados facilitan optimizar el uso de capacidades de rendimiento, enrutadores, firewalls, servidores y otros componentes de red.

8.2.1. Requerimientos

Para instalar y trabajar con PRTG Network Monitor se necesita:

- Un ordenador, servidor o máquina virtual con la capacidad operativa mínima de un ordenador promedio construido en 2007 con min. 1024 MB RAM.
- Cualquier versión de Microsoft® Windows (a partir de XP, en versión Server o Workstation, 32 o 64-bit).
- Navegador de red tipo Google Chrome, Firefox, Safari o Internet Explorer (a partir de versión 8) para proveer acceso a la interface web.

8.2.2. Compatibilidad

Es compatible con todas las versiones de XP o siguientes, para servidores o Workstation, tanto en sistemas operativos de 32 o 64 bit.

Trabaja con la interfaz, AJAX based web site.

8.2.3. Características de la aplicación.

- PRTG opera 24 horas, 7 días a la semana en una máquina basada en Windows, monitorizando parámetros de uso de red.
- Los datos de monitorización por PRTG son guardados en una base de datos para poder generar reportes históricos.
- La interfaz de usuario de PRTG permite configurar el equipo y los sensores que desea monitorizar, como la medición de temperatura de ámbito o el uso de memoria o de procesador.
- PRTG permite evitar estrangulamientos de tráfico y ofrecer una mejor calidad de servicio a sus usuarios en la comunicación y tráfico de nuestra red.
- PRTG permite descubrir qué aplicaciones causan la mayor carga en la red.
- PRTG funciona bajo todos los sistemas operativos Windows, es de instalación fácil y rápida y de operación intuitiva.
- PRTG permite emitir reportes en tiempo real, o a través de su base de datos mostrarnos reportes a la fecha, calendarizando actividades y el estado del dispositivos y de la red.
- Como es una aplicación WEB opera mediante navegadores; tipo Google Chrome, Firefox, Safari o Internet Explorer (a partir de versión 8).
- PRTG trabaja con una interfaz WEB AJAX.
- PRTG permite monitorizar redes tipo LAN, WLAN, VPN.

8.2.4. Plataformas en las que se puede utilizar.

Por el momento PRTG solo trabajo sobre cualquier versión de Microsoft® Windows (a partir de XP, en versión Server o Workstation, 32 o 64-bit)

8.2.5. Funcionamiento y pruebas de la aplicación.

8.2.5.1. Instalación de la Aplicación PRTG.

PRTG posee dos versiones, la edición freeware de monitorizador de ancho de banda puede ser descargada no sólo para fines privados sino también para el uso comercial. Si desea monitorizar más de 10 sensores necesita la edición comercial (Licencia pagada).

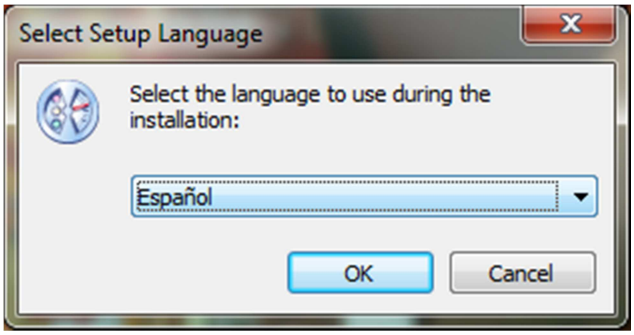
El software se puede bajar directamente de la página de PAESSLER.

http://www.es.paessler.com/prtg6



PRTG se encuentra disponible en los idiomas español, inglés y alemán.

Imagen 1: Instalación de PRTG



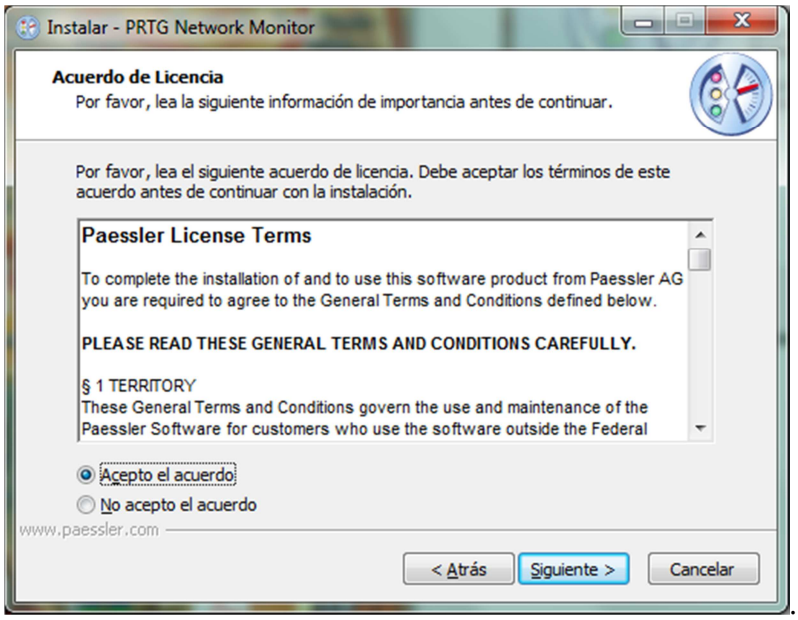
Para las pruebas se usará la versión Freeware.

Gráfico 2: Proceso de instalación PRTG



Cláusulas de instalación y Términos de Licencia PRTG

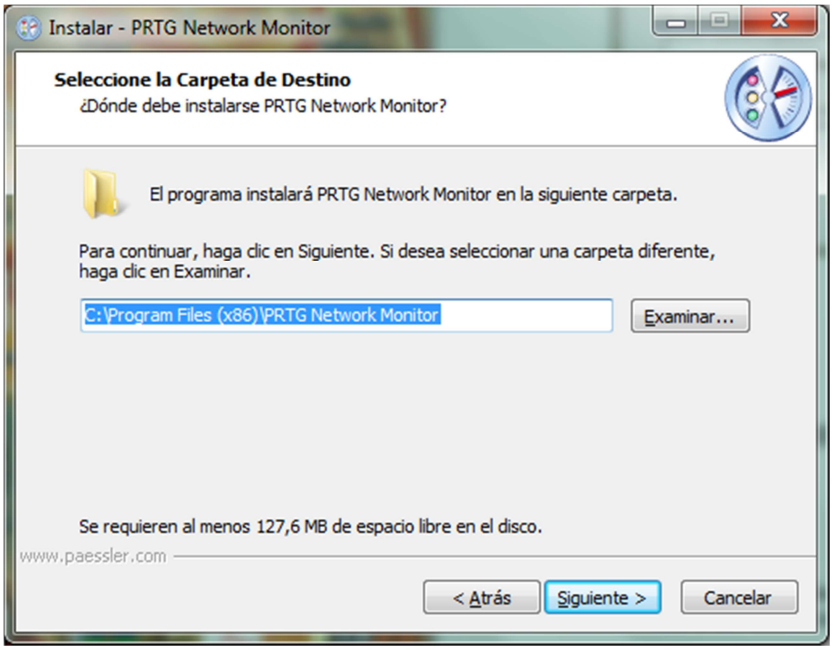
Imagen 3: Proceso de instalación y aceptación Licencia PRTG



* Imagen 1-2-3: Capturas Procesos de instalación en PRTG

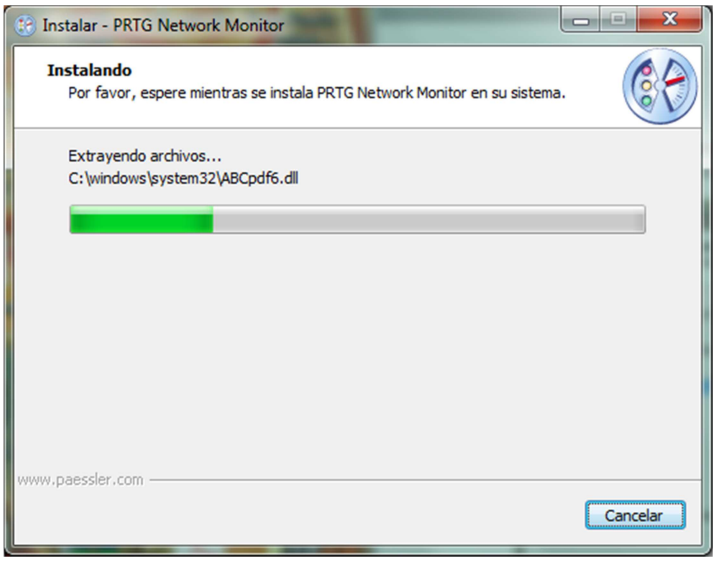
Dentro de la instalación nos permite seleccionar la ubicación o el disco de destino para el software, como normalmente viene en los estándares de instalación de software.

Imagen 4: Proceso de instalación PRTG



Proceso de instalación.

Imagen 5: Proceso de instalación PRTG



* Imagen 4-5: Capturas Procesos de instalación en PRTG

Terminada la instalación, se muestra una ventana de configuración de PRTG para el equipo.

Se pedirá una dirección de correo, para enviar las respectivas notificaciones y alertas.

Un nombre de registro, en nuestro caso como este software va a monitorear el laboratorio LTIC, el nombre a registrar es LTIC.

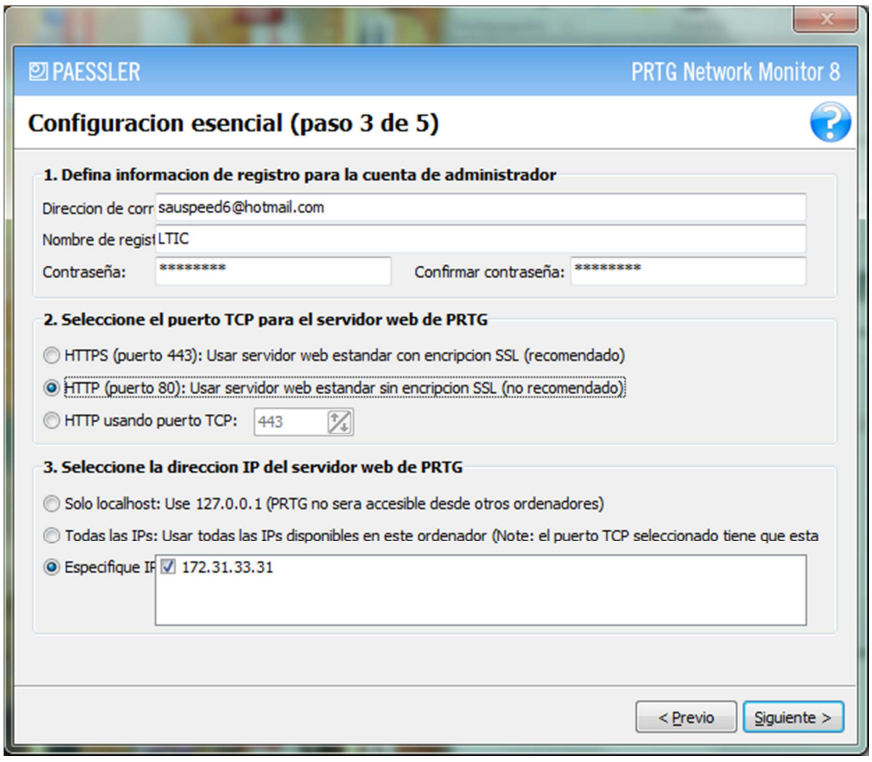
Una contraseña, la contraseña que usaremos es ltic1410.

La confirmación de la contraseña ltic1410

Se selecciona un puerto TCP para el servidor web de PRTG, el HTTP (puerto 80)

Se selecciona la dirección IP del servidor web de PRTG

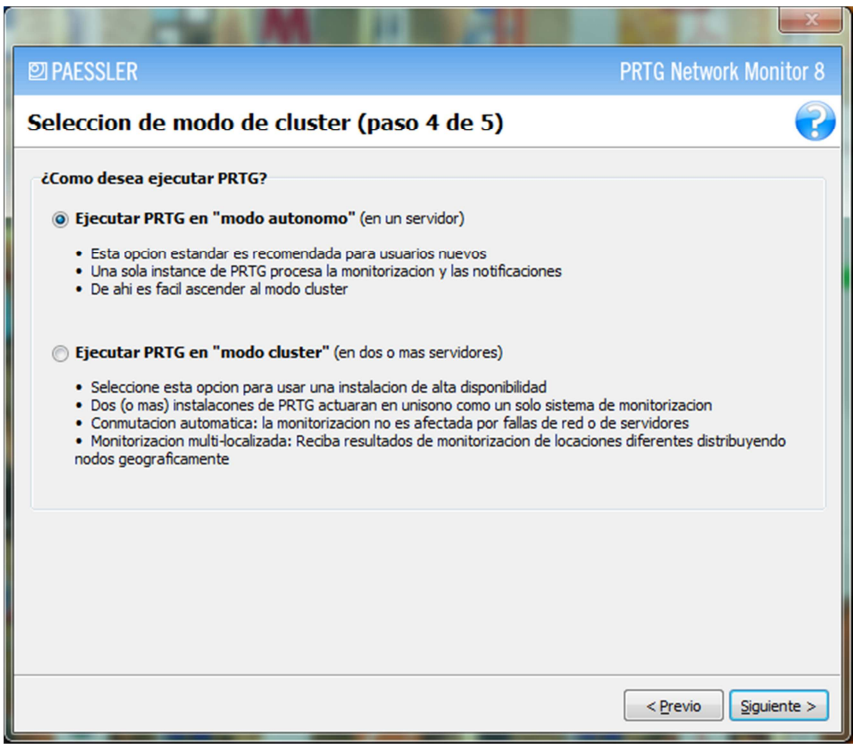
Imagen 6: Configuración PRTG



* Imagen 6: Capturas Procesos de instalación en PRTG

Para ejecutar PRTG se selecciona en modo autónomo.

Imagen 7: Procesos de instalación PRTG



Al finalizar la instalación se mostrara una ventana de instalación completada.

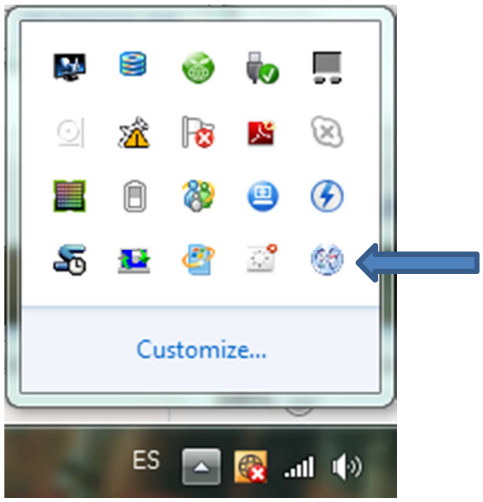
Imagen 8: Procesos de instalación PRTG



* Imagen 7 – 8: Capturas Procesos de instalación en PRTG

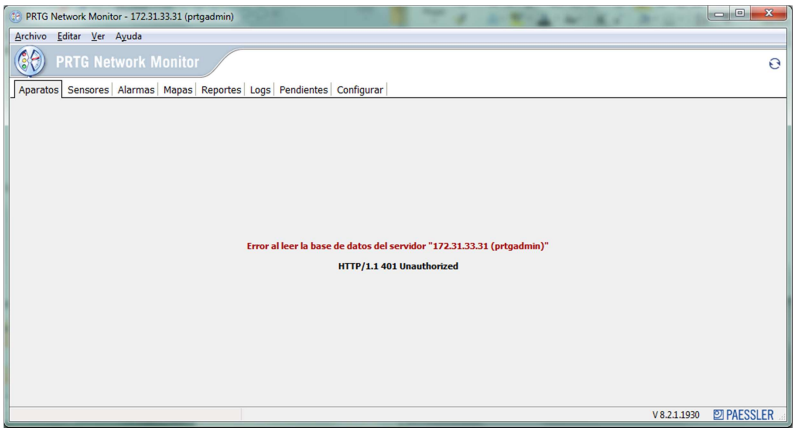
Se creara un icono en la barra de herramientas.

Imagen 9: Icono de control de PRTG en Windows



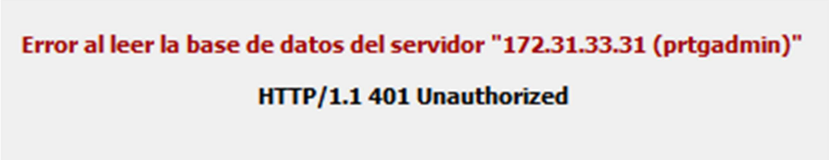
Se mostrara la ventana del software PRTG para escritorio.

Imagen 10: Ventana PRTG



Se mostrará el siguiente mensaje, para lo cual se realiza la respectiva configuración.

Imagen 10: Mensaje de control no autorizado en PRTG, error de conexión

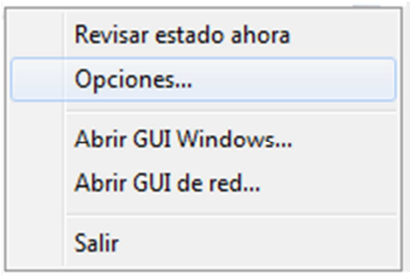


* Imagen 9: Captura imagen icono de instalación en Windows

* Imagen 10: Captura imagen error conexión PRTG

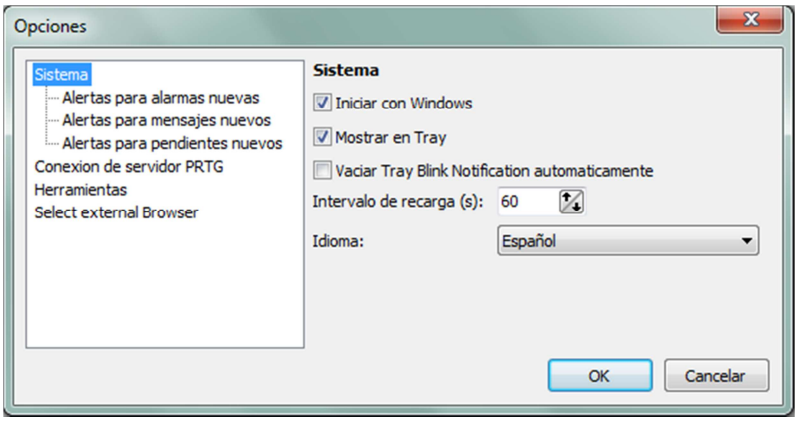
Para la configuración del equipo accedemos en el icono de PRTG.

Imagen 11: Opciones de configuración conexión con PRTG



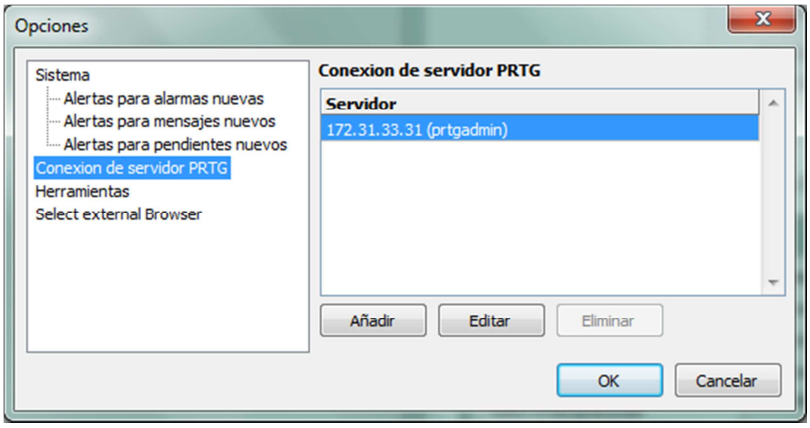
En las opciones para la configuración de PRTG son:

Imagen 12: Opciones de configuración conexión con PRTG



El error que dio es por la conexión con el servidor PRTG, para lo cual se accede a la opción

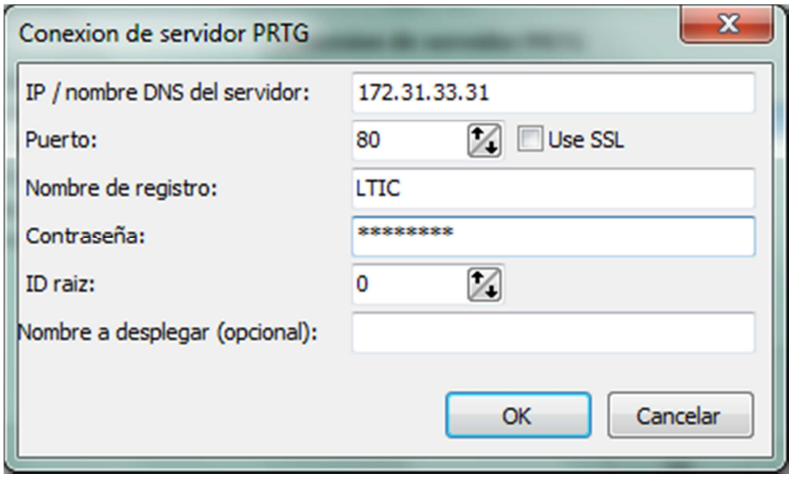
Imagen 13: Opciones de configuración conexión con PRTG



***** Imagen 11 - 12 – 13: Captura opciones de configuración conexión con PRTG

Dentro de la opción conexión de servidor PRTG se tiene la ventana

Imagen 14: configuración de IP, puerto nombre de registro contraseña id raíz para conexión PRTG

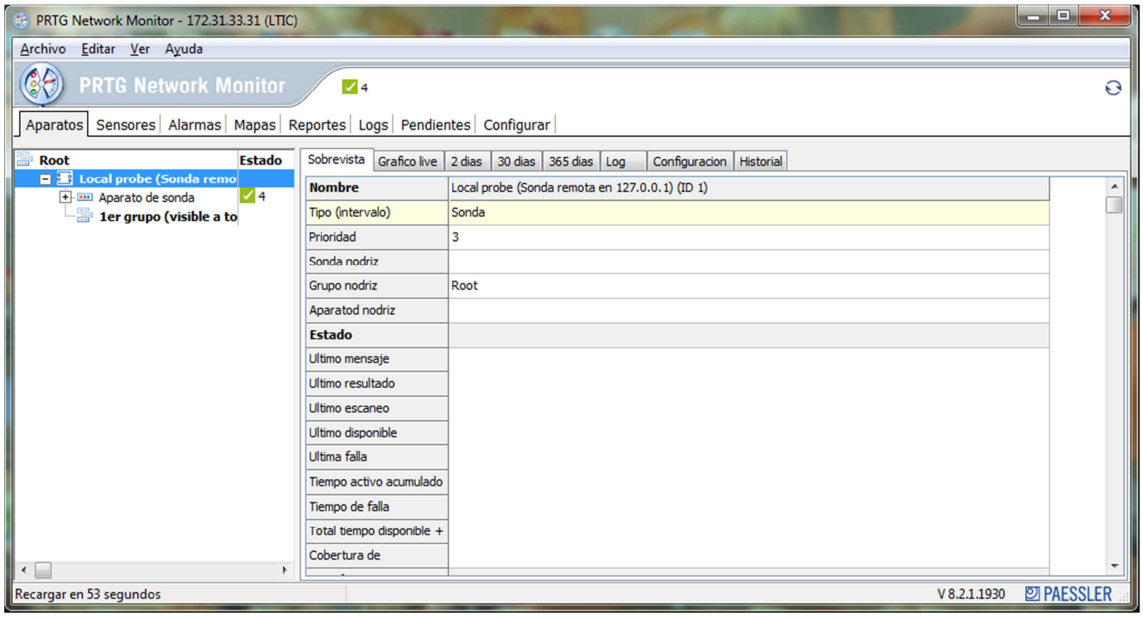


Aquí, se cambia la información por la que inicialmente ingresamos en la instalación.

El nombre de registro por LTIC y el password ltic1410

Después de la configuración se tiene acceso a la ventana de la aplicación PRTG

Imagen 15: Ventana de conexión PRTG configurada

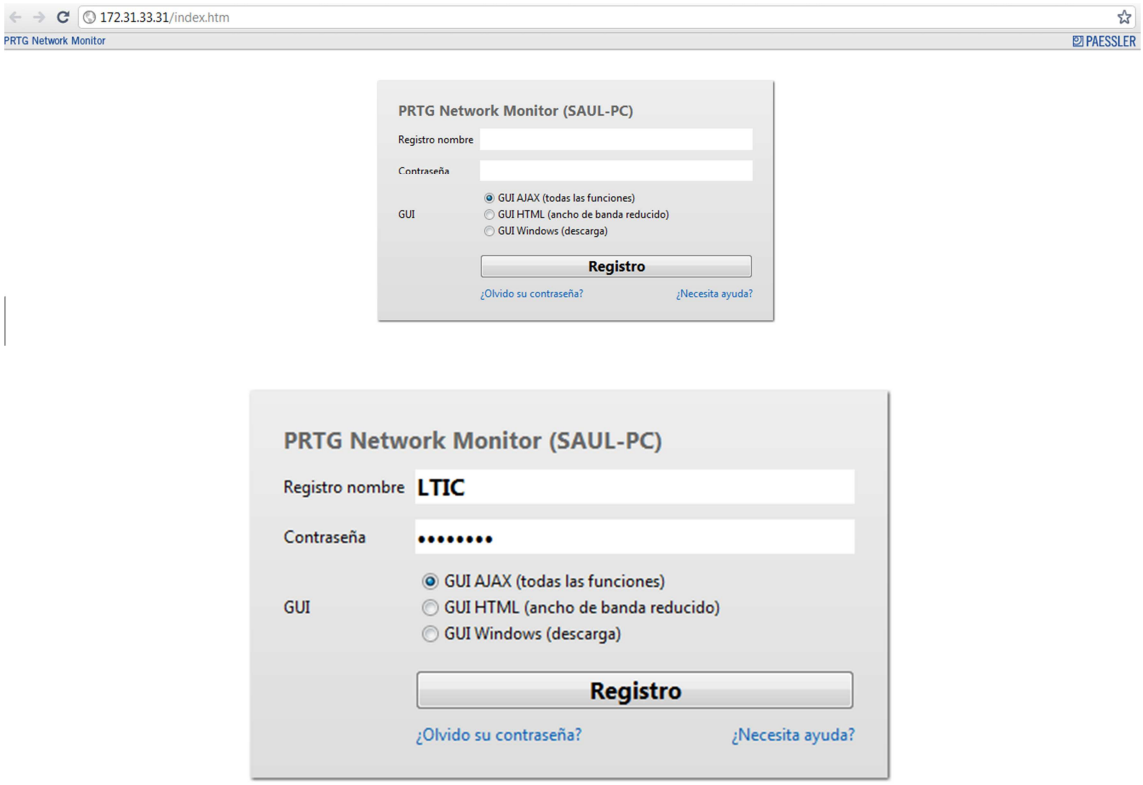


* Imagen 14: Captura de configuración de parámetros PRTG

* Imagen 15: Captura ventana con conexión PRTG

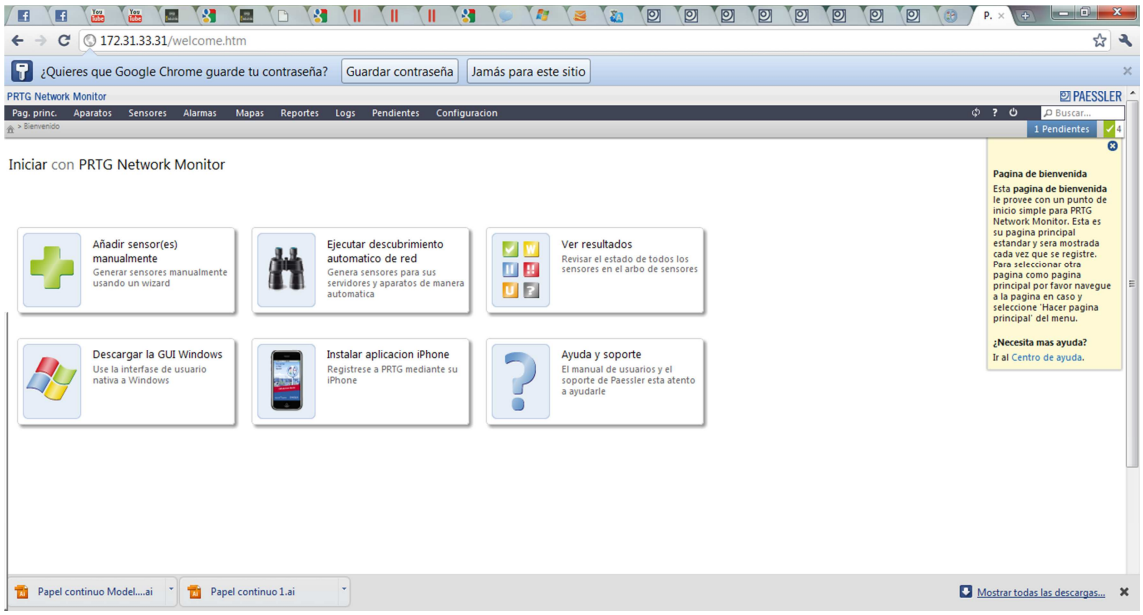
Además de esta tenemos la ventana de acceso de administración WEB

Imagen 1: Ventana de acceso web PRTG



Se ingresa al administrador web de PRTG

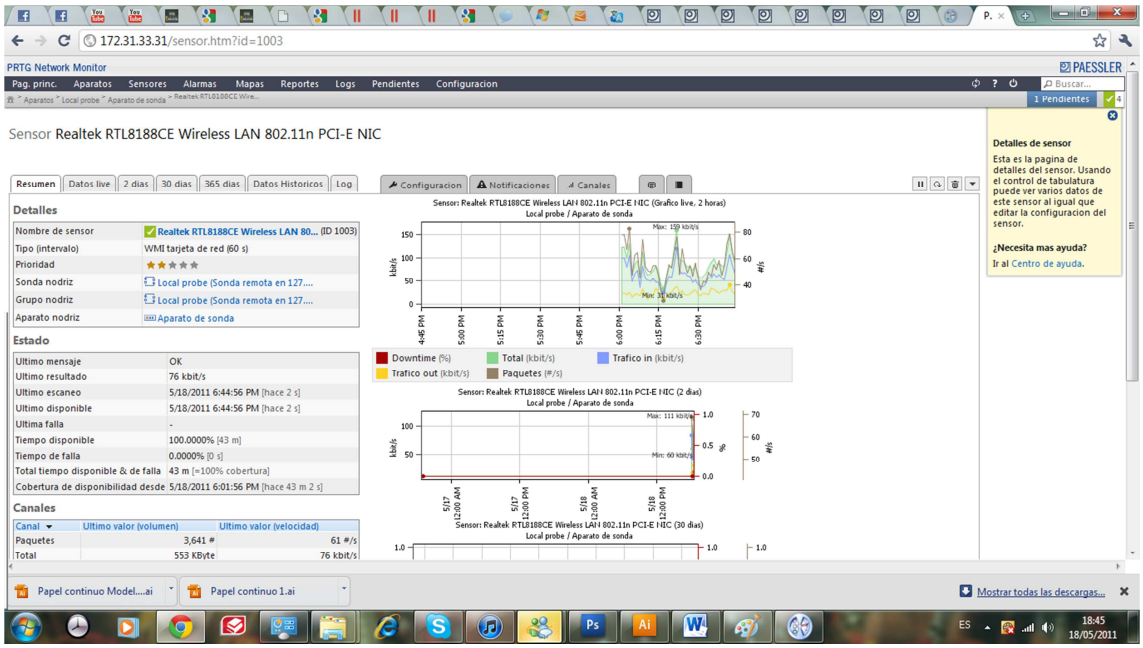
Imagen 2: Vista monitoreo y grafico de tráfico de la Red



* Imagen 1: Captura ventana de acceso

* Imagen 2: Vista monitoreo y grafico de tráfico de la Red

Imagen 3: Ventana de control PRTG



* Imagen 3: Captura ventana de control PRTG

8.3. SpiceWorks

SPICEWORKS es un software gratuito que genera información útil de la LAN de la organización, sacando estadísticas de cuántos dispositivos hay en la red, cuantos PC's, servidores, impresoras, switches etc, y de cada uno toma toda la información posible, qué sistema operativo tiene, qué software/parches tiene instalado, su configuración, datos físicos, etc.

Además de esto Spiceworks permite generar alertas.

8.3.1. Requerimientos

Spiceworks es un software diseñado para sistemas operativos Microsoft.

- Windows XP Pro SP2+, Windows Vista, Windows 7, Windows 2003 Server SP1+, and Windows 2008 Server.
- 1.5 GHz Pentium 4 class processor
- 1.0 GB RAM

8.3.2. Requerimientos de Explorador

Spiceworks oficialmente soporta

- Firefox 3.5+
- Internet Explorer 7.0+
- Safari
- Chrome

8.3.3. Compatibilidad

Es compatible con varios sistemas operativos Microsoft o bajo virtualización, es posible identificar las características físicas así como el software con el que cuenta el equipo.

- Windows XP Pro SP2+, Windows Vista, Windows 7, Windows 2003 Server SP1+, and Windows 2008 Server

8.3.4. Características de la aplicación.

- Spiceworks es una herramienta de software que permite genera información relevante de la red de laorganización.
- Gracias al manejo de identificación de dispositivos, se puede ver qué equipos se encuentran conectados a la red, tanto servidores, computadores de escritorio, laptops, switchs, routers, impresoras.
- Spiceworks permite identificar y sacar un reporte de las características de los equipos, como son marcas, procesadores, memoria, tarjetas gráficas, tarjetas de red, capacidad en disco, etc.
- Spiceworks además tiene la capacidad de generar un reporte de cada uno de los dispositivos, indicándo el sistema operativo como el software que se encuentra instalado en cada uno de ellos.
- Spiceworks genera alertas de los dispositivos y las genera en forma de reporte, tanto como actualizaciones o virus encontrados en los equipos.
- Nos permite mirar la estructura de la red mediante un mapa, donde se puede mirar cada equipo o dispositivo conectado como a su vez su identificador ID.

8.3.5. Plataformas en las que se puede utilizar.

Spiceworks está diseñado para utilizarse bajo plataforma Windows, pero tiene la capacidad de identificar equipos Mac y Linux conectados a nuestra red.

Además de esto está diseñado para equipos Intel o Amd, y a su vez con cualquier otra arquitectura de hardware.

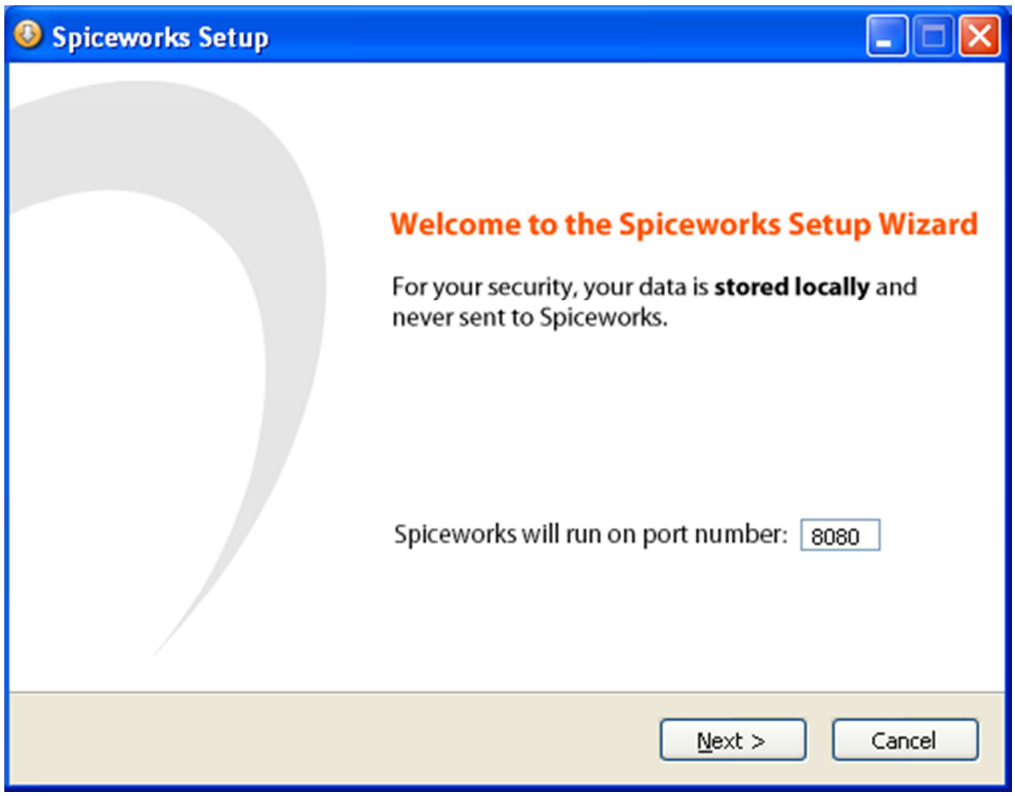
8.3.6. Funcionamiento y pruebas de la aplicación.

8.3.6.1. Instalación de la Aplicación Spiceworks.

SPICEWORKS es un software gratuito, se puede bajar desde la página
http://www.spiceworks.com/

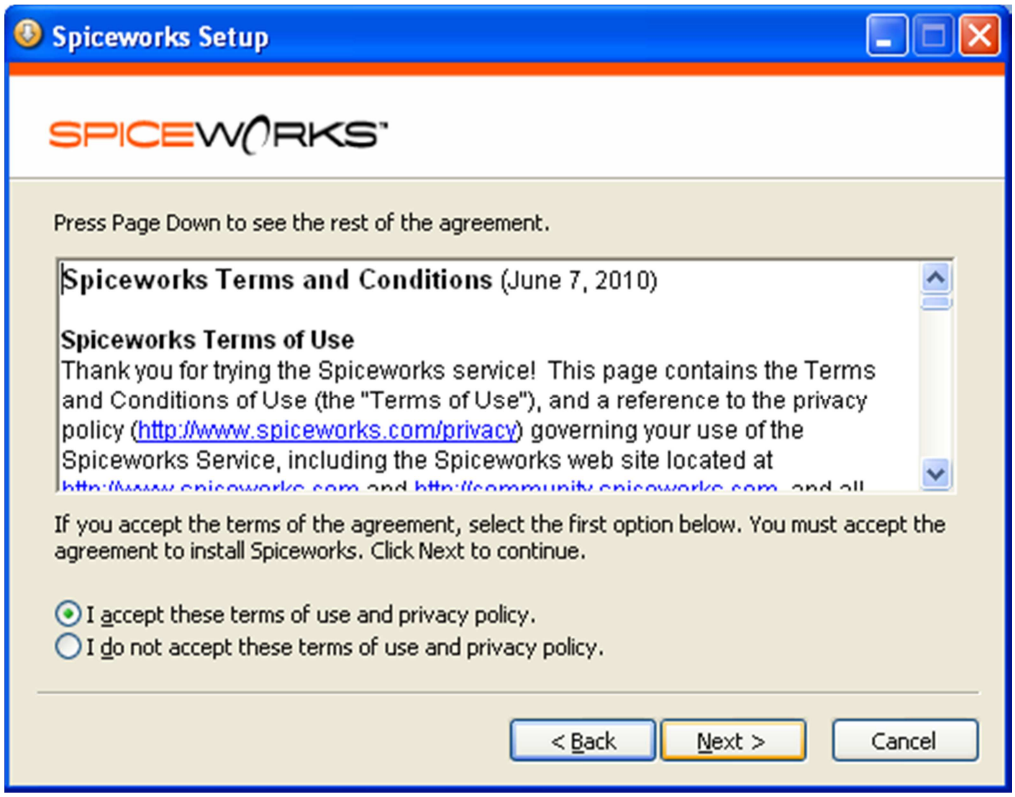
En la ventana inicial de instalación se pide el puerto de comunicación con el que trabaja la red y Spiceworks.

Imagen 1: Ventana de instalación Spiceworks



Cláusulas de instalación y Términos de Licencia Spiceworks.

Imagen 2: Ventana de instalación Spiceworks, aceptación de términos



Dentro de la instalación nos permite seleccionar la ubicación o el disco de destino para elsoftware, como normalmente viene en los estándares de instalación de software.

Imagen 3: Proceso de instalación Spiceworks

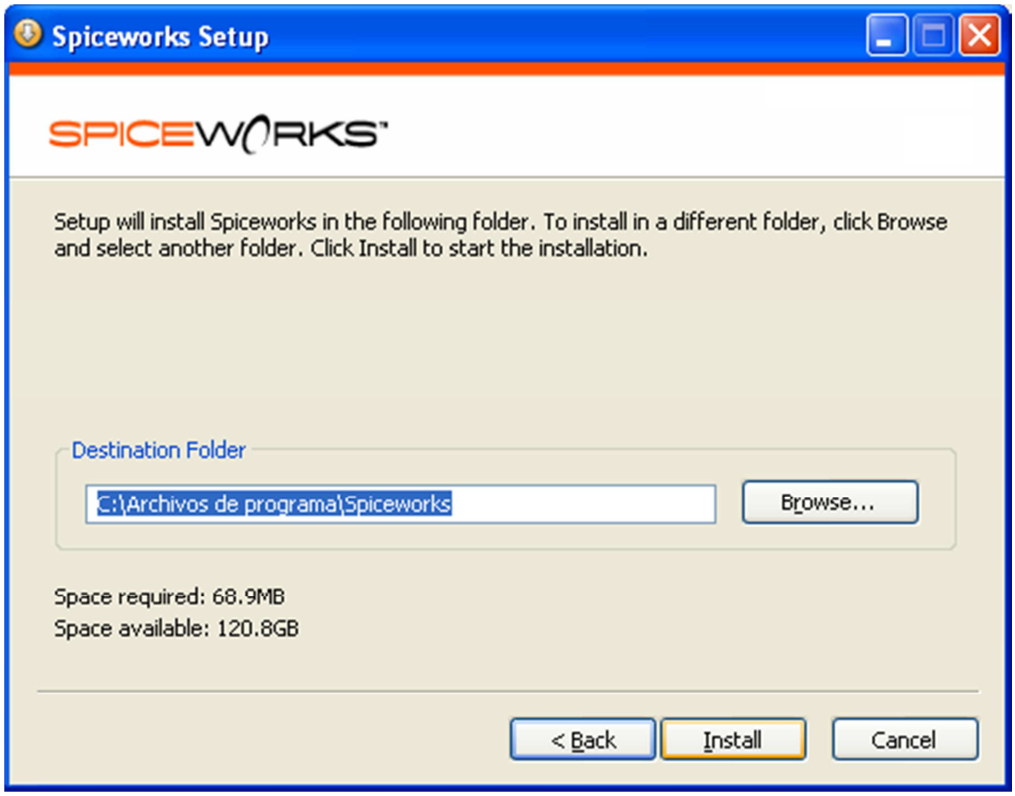
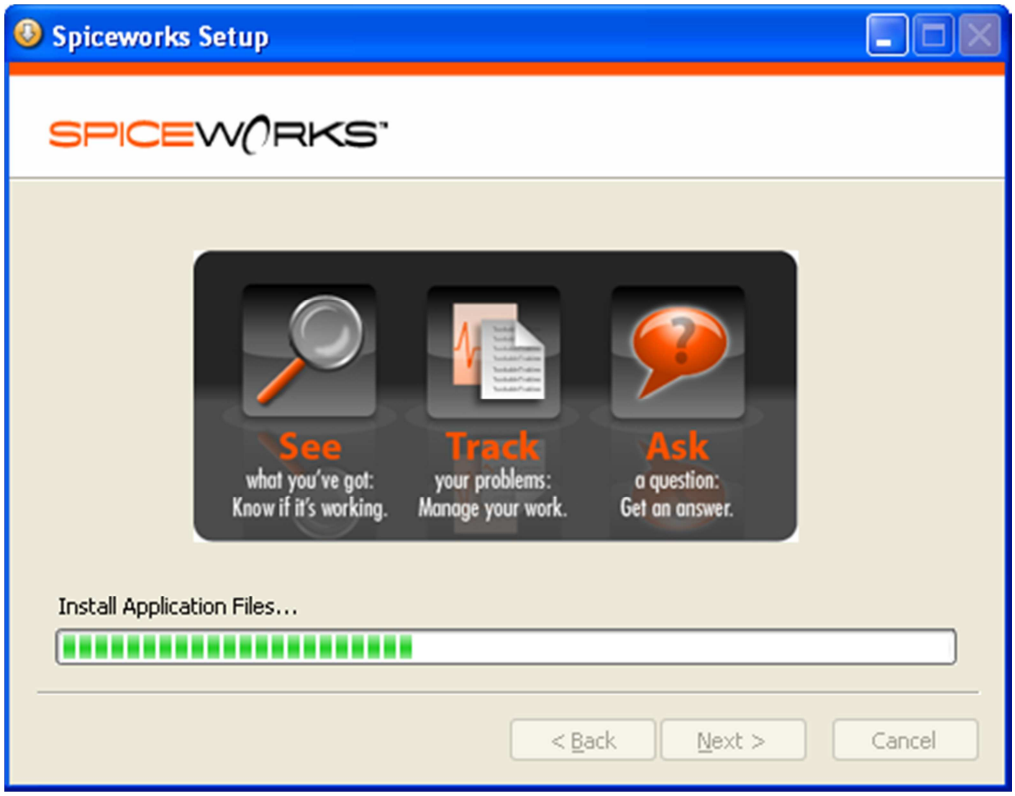
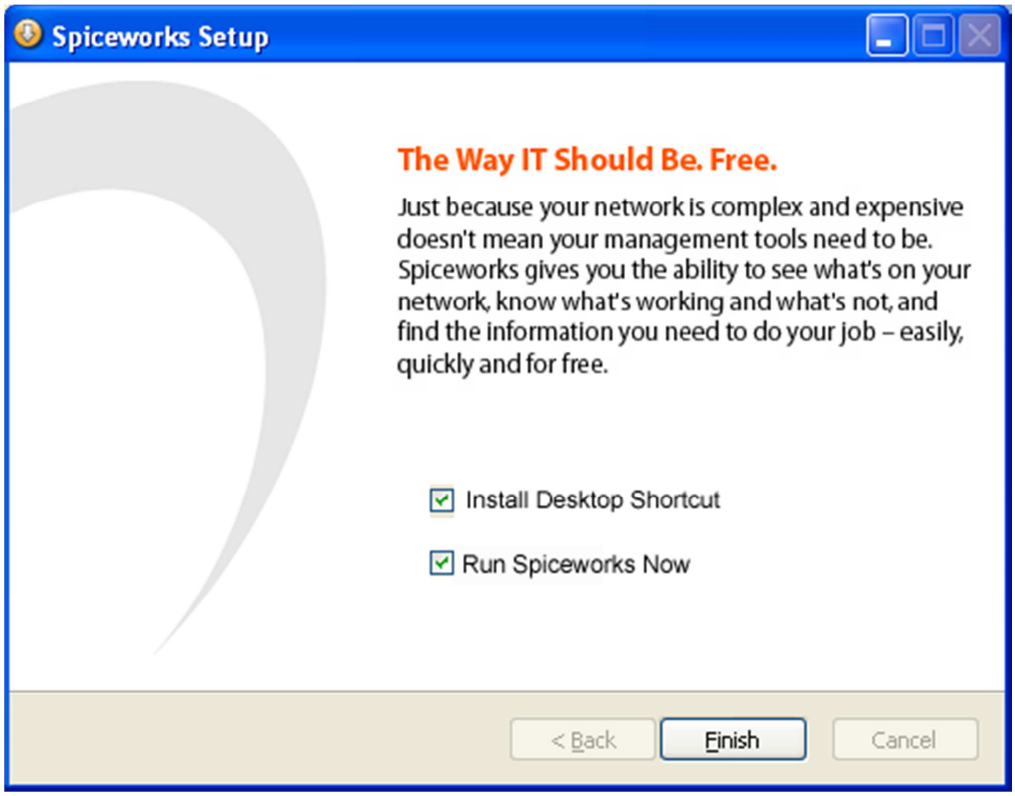


Imagen 4: Proceso de instalación Spiceworks



Terminada la instalación pedirá si se desea crear un icono de acceso en el escritorio y si se desea iniciar Spiceworks ahora.

Imagen 5: Proceso de instalación Spiceworks



* Imagen 1 a la 5: Capturas proceso de instalación spiceworks

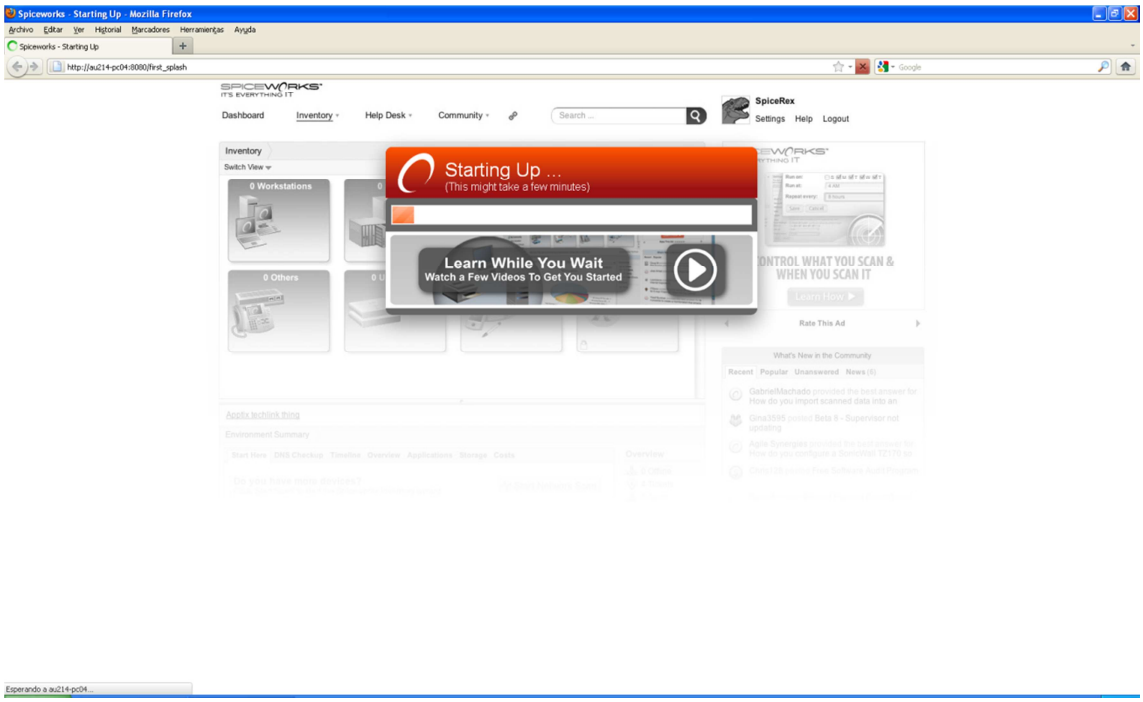
Al momento de ejecutar Spiceworks buscará el explorador determinado y se ejecutará, ya que es una herramienta de administración web.

Imagen 1: Proceso de arranque de la plataforma Spiceworks



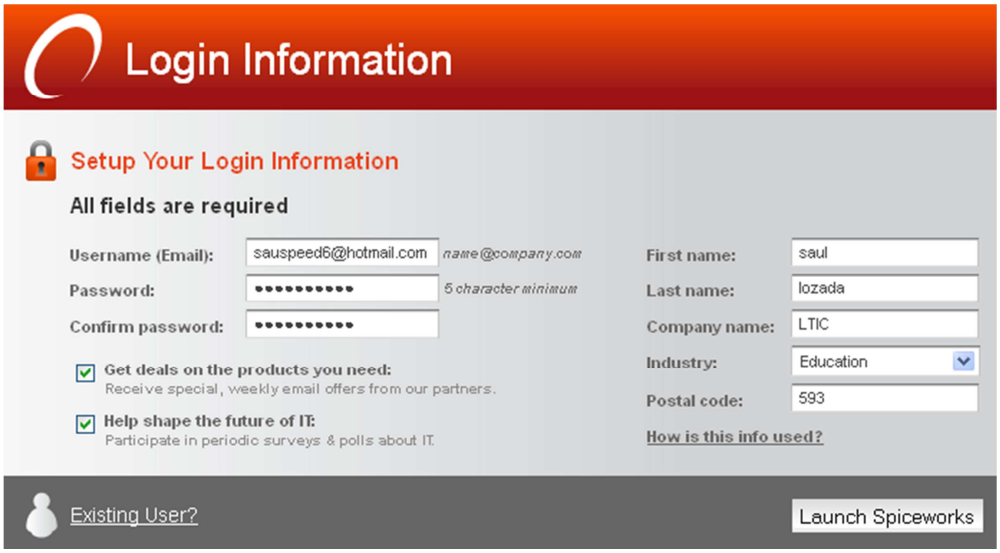
Ventana de carga de Spiceworks en Mozilla Firefox.

Imagen 2: Plataforma Web Spiceworks



Después de cargar la aplicación dentro del explorador, pedirá que se ingrese un registro para crear una cuenta de Spiceworks.

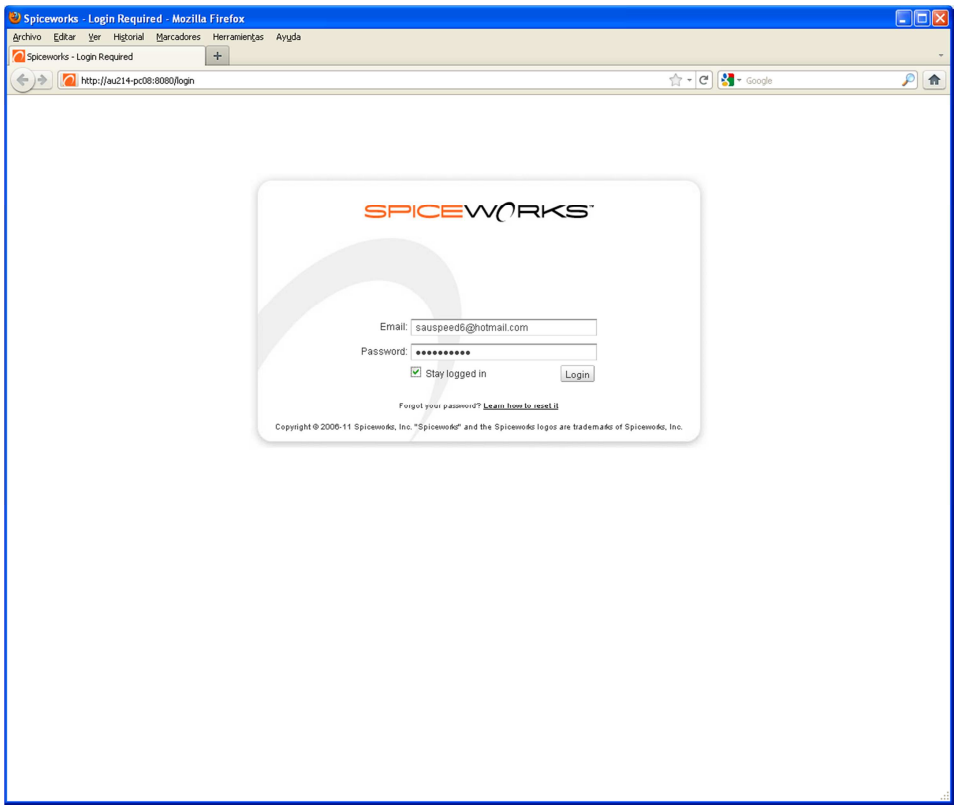
Imagen 3: Plataforma Web Spiceworks, configuración de cuenta



* Imagen 1 - 2 - 3: Capturas arranque y configuración plataforma web Spiceworks

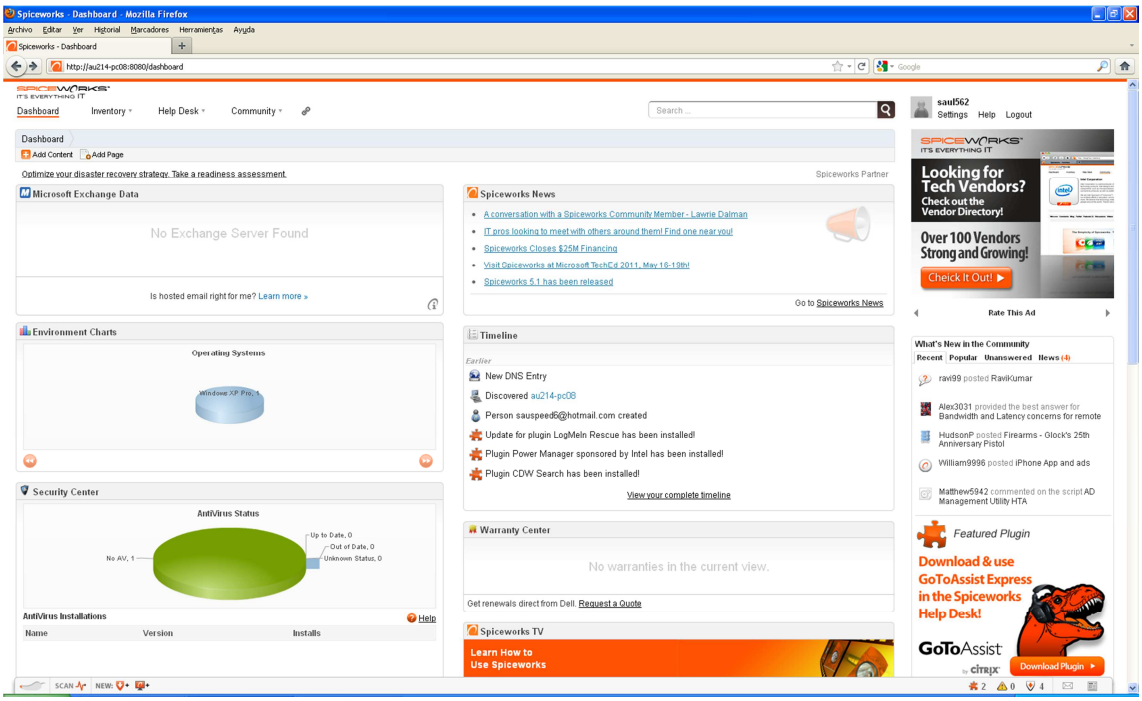
Al finalizar del registro se tendrá acceso a la herramienta web Spiceworks.

Imagen 4: Ventana de ingreso Spiceworks



En esta ventana se ingresa el email de registro y el password.

Imagen 5: Ventana de control interfaz Web Spiceworks.

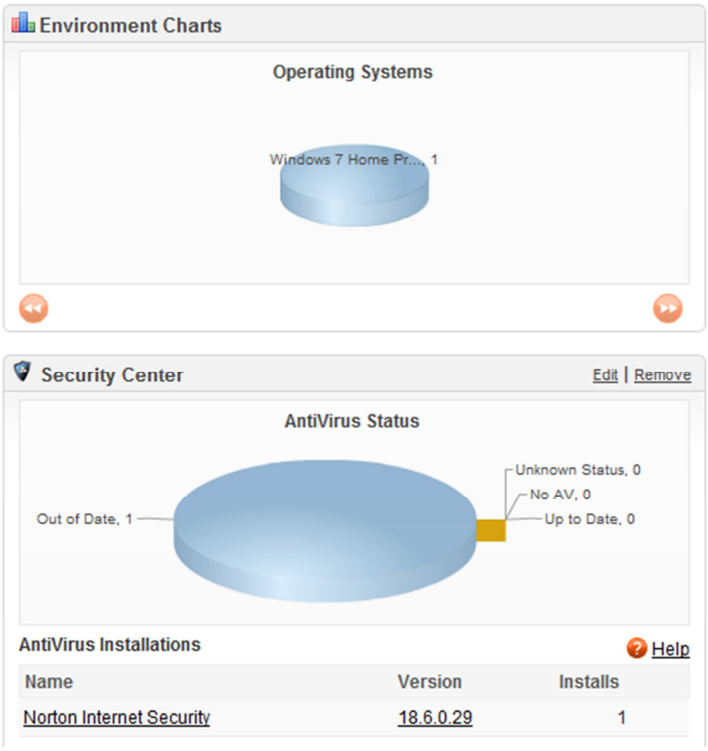


* Imagen 4 y 5: Capturas ingreso y menú plataforma web Spiceworks

Se visualiza la interfaz gráfica con la que trabaja la herramienta de administración Web.

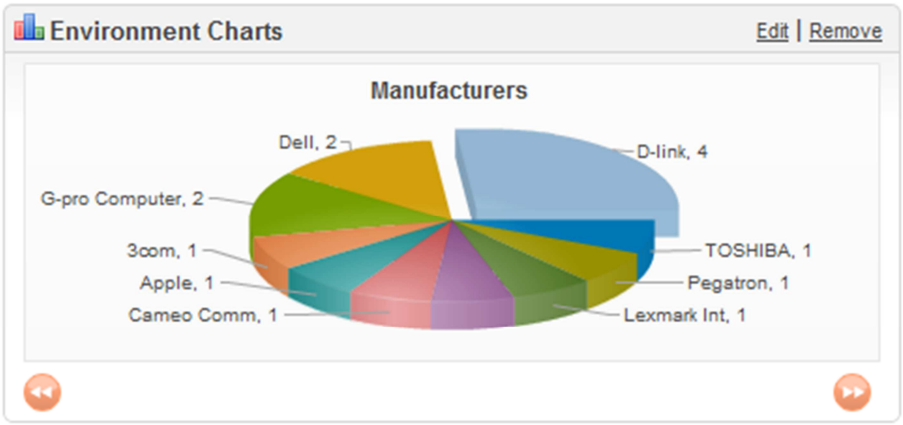
En la grafica podemos identificar el ambiente del equipo como es el sistema operativo y si posee un antivirus.

Imagen 1: Identificador de sistema Operativos y antivirus.



Además, se puede identificar las marcas y arquitecturas mediante el escaneo de la red.

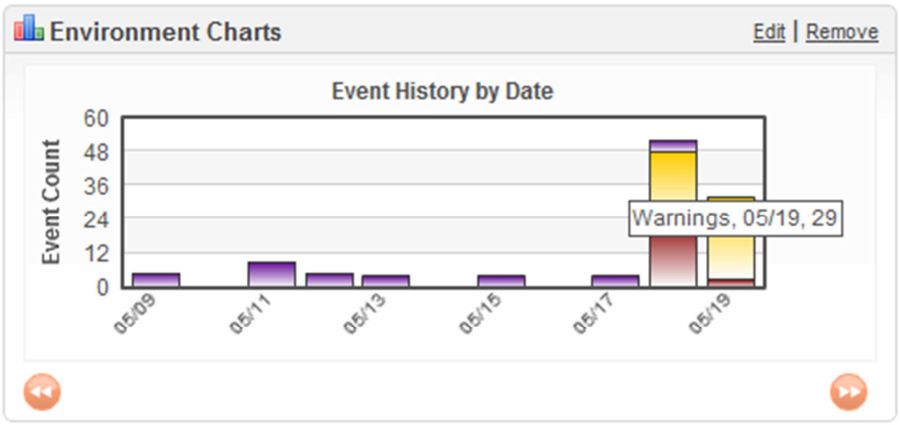
Imagen 2: Identificador de arquitecturas con la que contamos.



* Imagen 1 - 2: Identificadores de software y arquitecturas de equipos en Spiceworks

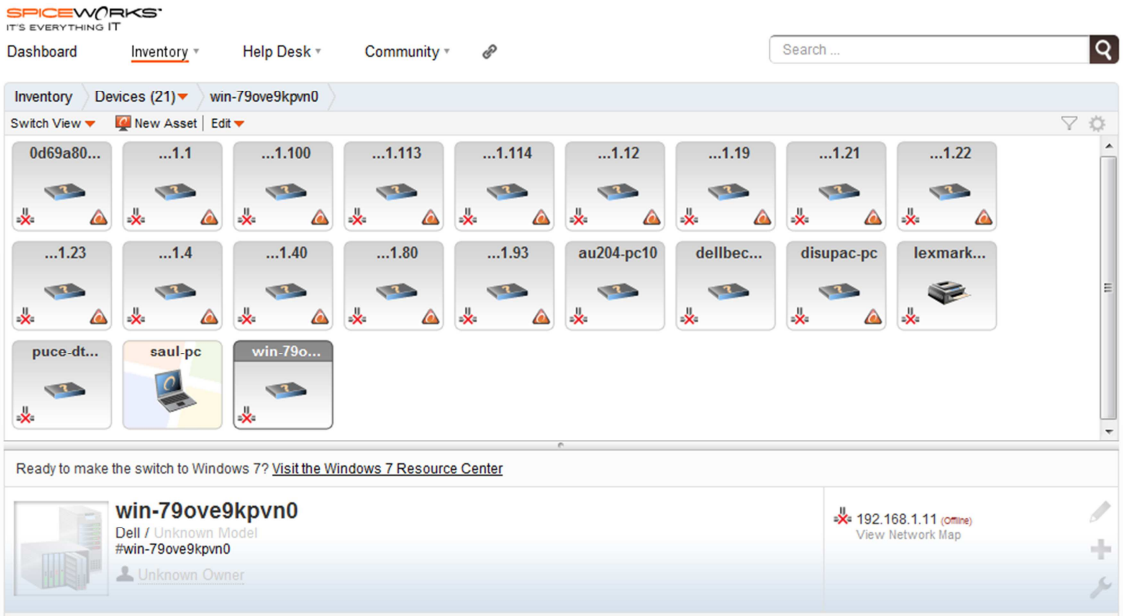
Spiceworks muestra el reporte de errores y advertencias que tiene el equipo.

Imagen 3: Identificador de errores y advertencias.



Spiceworks identifica cada uno de los equipos y dispositivos que se encuentran en la red.

Imagen 4: Identificador de dispositivos conectados a nuestra red.

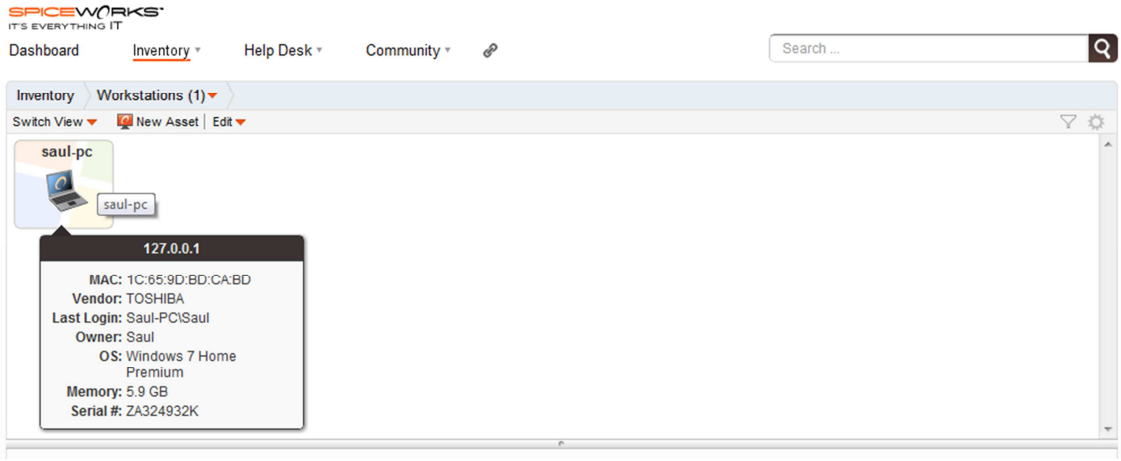


* Imagen 3: Captura identificador de errores Spiceworks.

* Imagen 4: Captura identificador de dispositivos conectados a nuestra red.

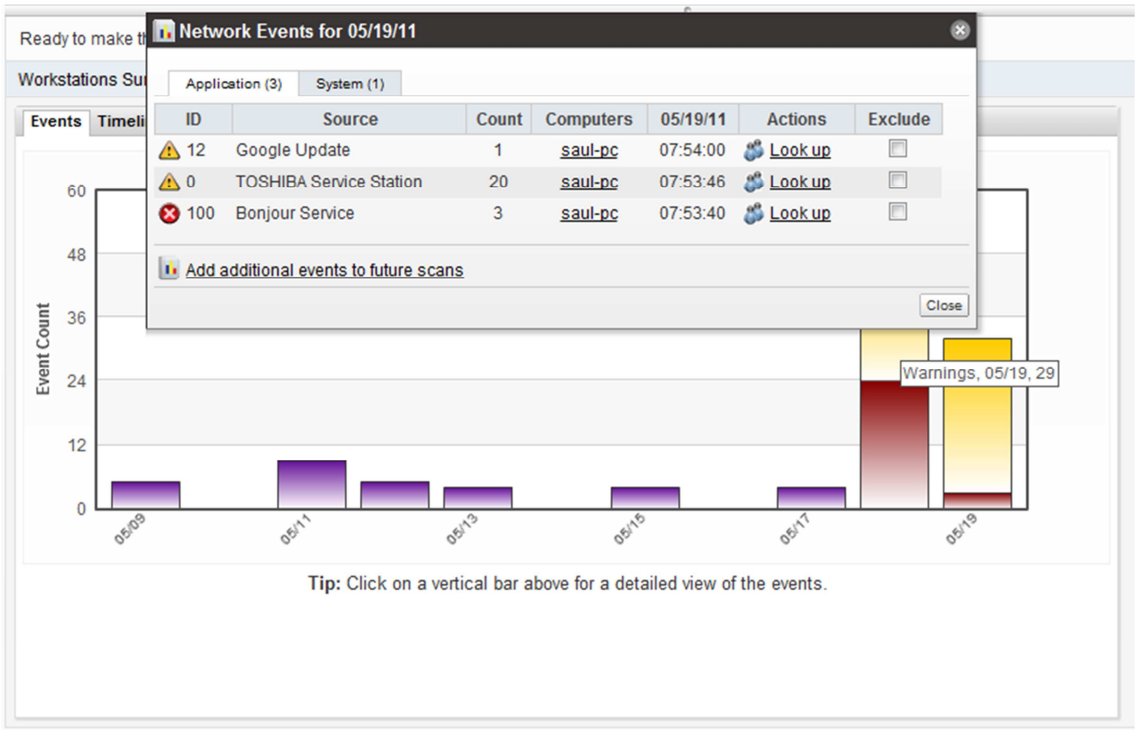
Mediante esta identificación se puede mirar cada una de las características que poseen los equipos.

Imagen 5: Información relevante de nuestro equipo mediante inventory – Spiceworks.



Alertas y actualizaciones de nuestro equipo

Imagen 6: Alertas y actualizaciones de nuestro equipo mediante inventory – Spiceworks.

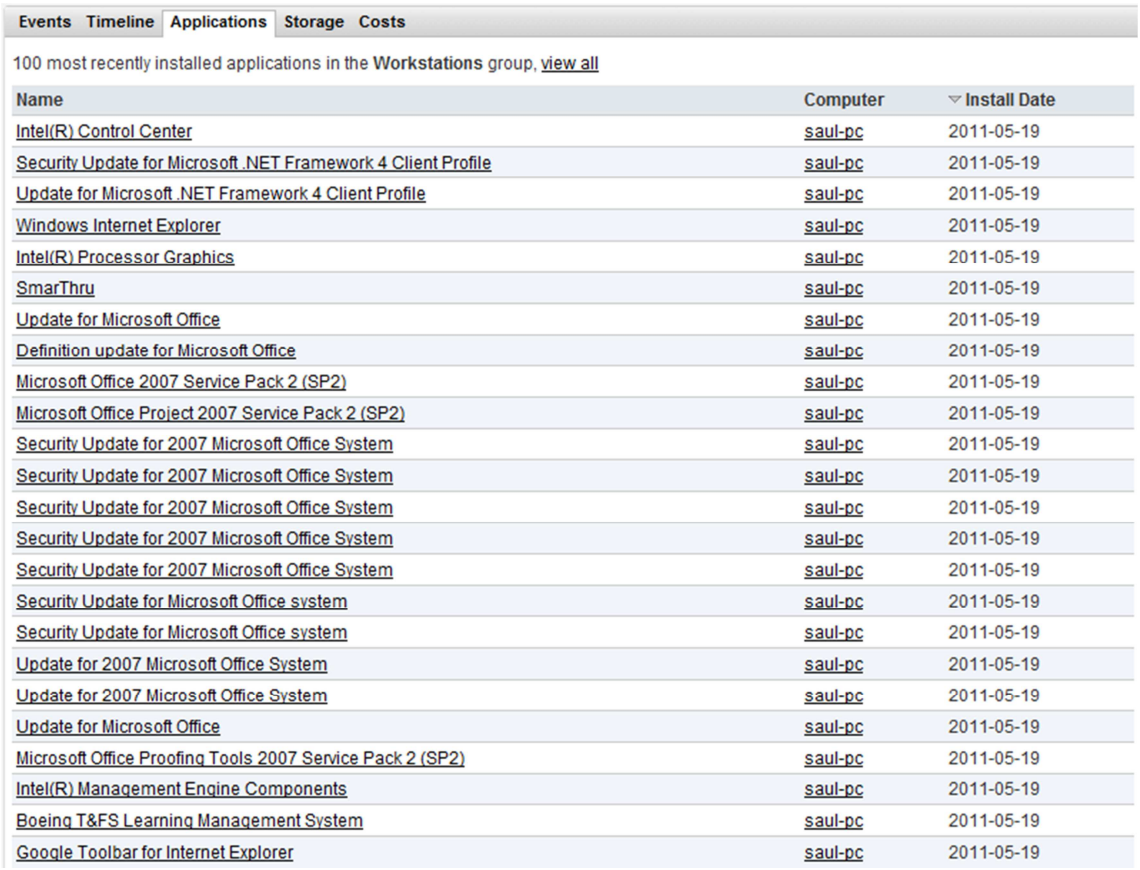


* Imagen 5: Captura información relevante de nuestro equipo.

* Imagen 6: Captura alertas y actualizaciones de nuestro equipo

Además realizar un reporte del software.

Imagen 7: Reporte de software con el que contamos en nuestros equipos.



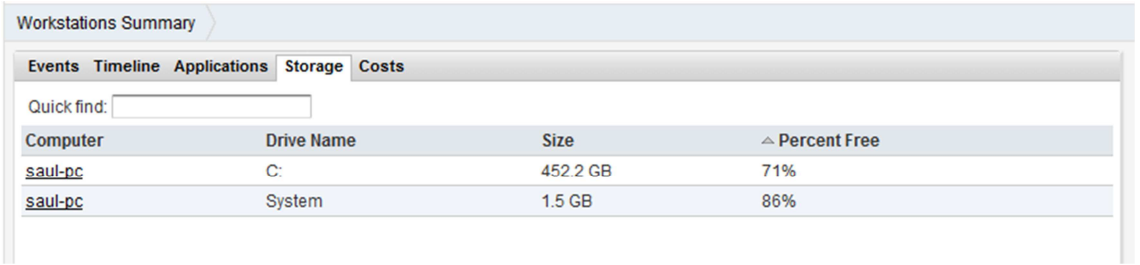
Events Timeline Applications Storage Costs

100 most recently installed applications in the **Workstations** group, view all

Name	Computer	Install Date
Intel(R) Control Center	saul-pc	2011-05-19
Security Update for Microsoft .NET Framework 4 Client Profile	saul-pc	2011-05-19
Update for Microsoft .NET Framework 4 Client Profile	saul-pc	2011-05-19
Windows Internet Explorer	saul-pc	2011-05-19
Intel(R) Processor Graphics	saul-pc	2011-05-19
SmarThru	saul-pc	2011-05-19
Update for Microsoft Office	saul-pc	2011-05-19
Definition update for Microsoft Office	saul-pc	2011-05-19
Microsoft Office 2007 Service Pack 2 (SP2)	saul-pc	2011-05-19
Microsoft Office Project 2007 Service Pack 2 (SP2)	saul-pc	2011-05-19
Security Update for 2007 Microsoft Office System	saul-pc	2011-05-19
Security Update for 2007 Microsoft Office System	saul-pc	2011-05-19
Security Update for 2007 Microsoft Office System	saul-pc	2011-05-19
Security Update for 2007 Microsoft Office System	saul-pc	2011-05-19
Security Update for 2007 Microsoft Office System	saul-pc	2011-05-19
Security Update for Microsoft Office system	saul-pc	2011-05-19
Security Update for Microsoft Office system	saul-pc	2011-05-19
Update for 2007 Microsoft Office System	saul-pc	2011-05-19
Update for 2007 Microsoft Office System	saul-pc	2011-05-19
Update for Microsoft Office	saul-pc	2011-05-19
Microsoft Office Proofing Tools 2007 Service Pack 2 (SP2)	saul-pc	2011-05-19
Intel(R) Management Engine Components	saul-pc	2011-05-19
Boeing T&FS Learning Management System	saul-pc	2011-05-19
Google Toolbar for Internet Explorer	saul-pc	2011-05-19

Así también, la capacidad de disco que poseen los equipos.

Imagen 8: Reporte de capacidad en disco con la que contamos



Workstations Summary

Events Timeline Applications Storage Costs

Quick find:

Computer	Drive Name	Size	Percent Free
saul-pc	C:	452.2 GB	71%
saul-pc	System	1.5 GB	86%

* Imagen 6: Captura reporte inventario de software.

* Imagen 7: Captura reporte capacidad en disco duro.

Capitulo III

9. Obtención de resultados.

A través de las herramientas utilizadas en el LTIC para la obtención de resultados en la problemática de la seguridad informática y la identificación de problemas se tiene lo siguiente:

10. Obtención de resultados con la herramienta Spiceworks.

10.1 Análisis y pruebas con la herramienta Spiceworks.

Mediante el análisis de la herramienta Spiceworks, se obtuvieron los siguientes resultados respecto a la Red del laboratorio LTIC, en orden jerárquico.

Servidor 1 para la obtención de resultados

Datos del servido con:

Dirección IP	**192.168.1.11**
SubNet	**255.255.255.0**
Puerta de enlace predeterminada	**199.168.1.1**

La herramienta Spiceworks permite obtener datos importantes como son:

- El serial identificador del equipo: win-79ove9kpvn0
- La marca y modelo del equipo: Dell / PowerEdge 2950
- El Serial #: GT9WPC1
- El tipo de usuario según su sistema operativo: en este caso nuestro servidor es Usuario Windows
- Mac Address: 00:19:B9:B9:50:2A
- El último inicio: INGENIERIA\Susana
- El Sistema Operativo que utiliza: Windows Server 2008 R2 Ent
- El tipo de procesador: Intel Xeon X53355 2.66 GHZ
- Memoria Ram: 4GB

Imagen 1: Pantalla Spiceworks información servidor

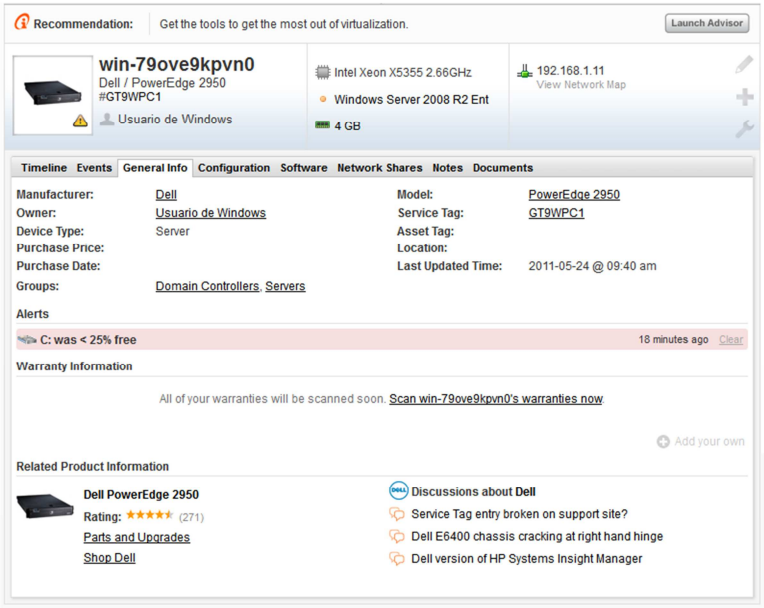
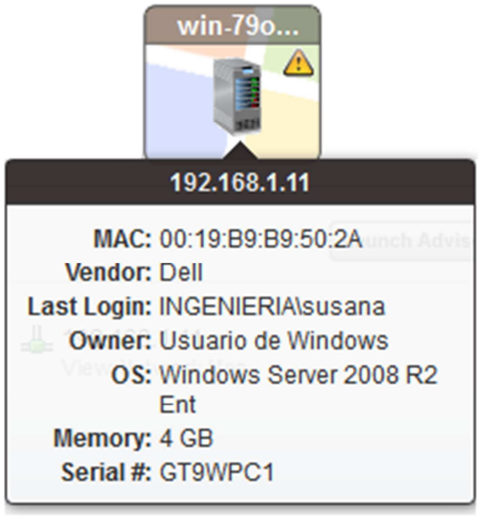


Imagen 2: Pantalla Spiceworks información equipo por icono



Este conjunto de datos se muestra mediante el menú de Inventario de la herramienta Spiceworks.

Un punto importante respecto a esta opción es que se puede visualizar en conjunto toda la Red. Como son todos los equipos pertenecientes a la red, tanto para las aulas, así también como para los equipos como laptops teléfonos o dispositivos móviles que se encuentran interconectados a la red, analiza a todos los equipos.

10.2. Scan e Identificación de equipos.

Dentro del análisis de la herramienta Spiceworks se obtuvieron los siguientes resultados para la Red LTIC:

- El servidor de archivos correspondiente a la dirección IP 192.168.1.11 donde se encuentran instaladas nuestras herramientas de software.
- Servidor HP identificador Cameo Comm para uso de UNTANGLE dirección IP 192.168.1.1
- Servidor Linux 127.0.0.1perteneciente al localhost de la Red LTIC
- Wireless LAN Switch WX1200 con IP 192.168.1.12 para el pasó de la señal inalámbrica e internet dentro del Laboratorio LTIC

* Imagen 1: Captura pantalla Spiceworks información servidor
* Imagen 2: Captura pantalla Spiceworks información equipo por icono

Las aulas, con sus respectivos equipos que fueron analizados son:.

Aula 201

Equipo	IP
Au201- pc01	192.168.1.186
Au201- pc02	192.168.1.187
Au201- pc03	192.168.1.188
Au201- pc04	192.168.1.189
Au201- pc05	192.168.1.191
Au201- pc06	192.168.1.192
Au201- pc07	192.168.1.193
Au201- pc08	192.168.1.194

Aula 203

Equipo	IP
Au203- pc01	192.168.1.57
Au203- pc02	192.168.1.58
Au203- pc03	192.168.1.59
Au203- pc04	192.168.1.60
Au203- pc05	192.168.1.61
Au203- pc06	192.168.1.62
Au203- pc07	192.168.1.63
Au203- pc08	192.168.1.64

Cuadro 1: aula 203

Aula 204

Equipo	IP
Au204- pc01	192.168.1.108
Au204- pc02	192.168.1.109
Au204- pc03	192.168.1.110
Au204- pc04	192.168.1.111
Au204- pc05	192.168.1.112
Au204- pc06	192.168.1.113

Cuadro 2: aula 204

* Cuadro 1 -2: identificadores de las aulas y los equipos pertenecientes a 203 -204

10.3. Identificación de problemas.

La herramienta Spiceworks, fuera de los dispositivos que se identificaron y que son parte del laboratorio LTIC, identifico alrededor de 249 dispositivos más asociados a la red, dentro de los cuales están laptops, pad, teléfonos celulares con conectividad inalámbrica y otros dispositivos, pertenecientes a estudiantes y docentes de la facultad de Ingeniería, así también como de los alrededores de la PUCE.

Spiceworks nos permite observar, como primera sugerencia, que dentro de los parámetros de la seguridad y la cobertura de la red del laboratorio LTIC, no se tienen establecidos límites para el uso de la misma, por eso la gran cantidad de dispositivos desconocidos y no identificados en el LTIC, este puede ser un problema a futuro ya que no se posee un control respecto al uso de la

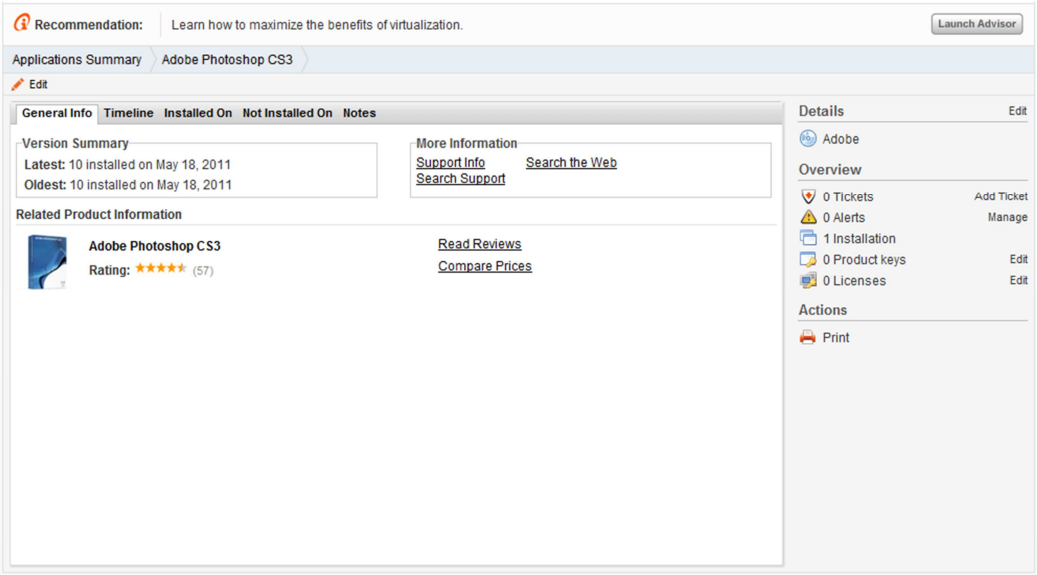
Red, esto puede acarrear inconvenientes como baja en el ancho de banda, así como interferencia al momento de la conectividad inalámbrica para el uso académico.

Además de esto, se identificaron algunos equipos no pertenecientes que pueden compartir la información de los servidores, en nuestro caso el servidor de archivos, otro de los problemas detectados y que pueden afectar el correcto funcionamiento e interferir con los servicios que presta el laboratorio LTIC.

10.4. Identificación de Software.

La Herramienta Spiceworks permite observar el tipo de software que se encuentra instalado en los equipos, esto es de ayuda ya que el laboratorio LTIC puede estar al tanto de las versiones o el software con el que se está trabajando y se posee a la hora de brindar sus servicios.

Imagen 3: Sumario de software Spiceworks



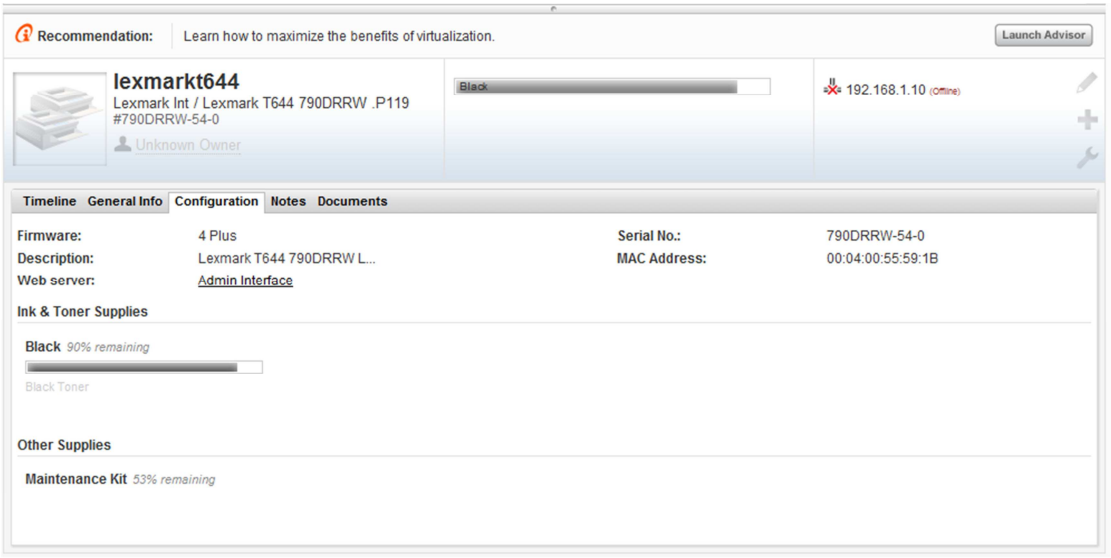
* Imagen 3: Captura sumario de software Spiceworks

10.5. Monitoreo de Dispositivos Externos.

Respecto a equipos como impresoras, Spiceworks también tiene la posibilidad de monitorear independientemente del equipo donde se encuentre instalado este tipo de dispositivos externos.

De esta forma no es necesario monitorear desde el servidor de impresión, al contrario, el administrador de Spiceworks permite observar el estado de la impresora así como de sus suministros.

Imagen 4: Dispositivo externo – monitoreo Spicework de Impresora



* Imagen 4: Captura dispositivo externo – monitoreo Spicework de Impresora.

10.6. Help Desk.

Spiceworks permite tener una supervisión centralizada de la red, gracias a la opción de Help Desk, esta es una herramienta que permite tanto al administrador, como al usuario, estar en contactó acerca de lo que está sucediendo en la máquina, envia un mensaje de notificación según escoja el administrador: sea vía mail, msm, u otro tipo de notificación.

En la configuración de administrador se pedirá ingresar el mail que está asociado a la cuenta, este mail será a donde lleguen los mensajes y notificaciones por parte del Help Desk de Spiceworks.

10.6.1. Para equipos y usuarios que están dentro de nuestra red.

Spicework tiene la opción de asociar los equipos y dispositivos por simple escaneo, ya que si se encuentran conectados vía Wireless o vía LAN, Spicework lo realiza automáticamente.
Los equipos escaneados también deben tener un solo requerimientos, su sistema operativo.
Dentro de los sistemas operativos y versiones SpiceWorks es compatible con:

- Windows 2000 Professional y Server
- Windows 2003 Server
- Windows 2008 Server R2
- Windows XP Professional
- Windows Vista
- Windows 7
- Macintosh OS X (SSH debe estar habilitado)
- Linux / Unix (SSH debe estar habilitado)

Spiceworks tiene la funcionalidad de trabajar con distintos sistemas operativos por lo cual es multiplataforma.

Tener en cuenta que para que se pueda asociar un equipo con un distinto sistema operativo, se deben clasificar por cuenta.

Para que Spicework pueda gestionar un equipo existen dos tipos de cuentas:

- **Cuenta Windows:** Se asigna como "usuario actual", esta es la cuenta con la que se registra en el momento de la instalación, debe ser una cuenta con privilegios de administrador de toda la red para poder acceder a los demás equipos remotamente sin tener que estar usando diferentes usuarios.

- **Cuenta SSH:** Esta es la cuenta que se utiliza en las máquinas UNIX o Mac's, estas cuentas deben ajustarse como una cuenta valida SSH, para así cumplir con las funciones que Spiceworks proporciona.

10.7. Reportes Spiceworks.

Spiceworks nos permite sacar un reporte de las incidencias dentro de nuestra red y de los equipos que pertenecen a ella, de esta manera se puede tener un completo control sobre los eventos que se suscitan en nuestra red y evitar posibles problemas respecto al entorno en el que esta se encuentra, respecto a actividad y prestación de servicios.
Spiceworks tiene la opción de generar reportes personalizados y de fácil manejo, estos pueden ser exportados a PDF, CSV o XLS.

Imagen 1: Pantalla de reportes Spiceworks.

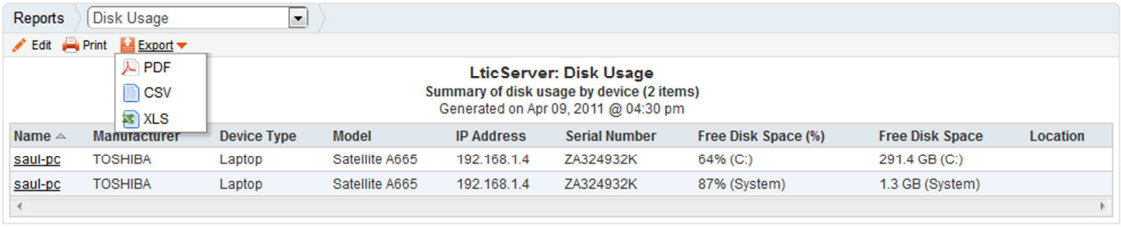
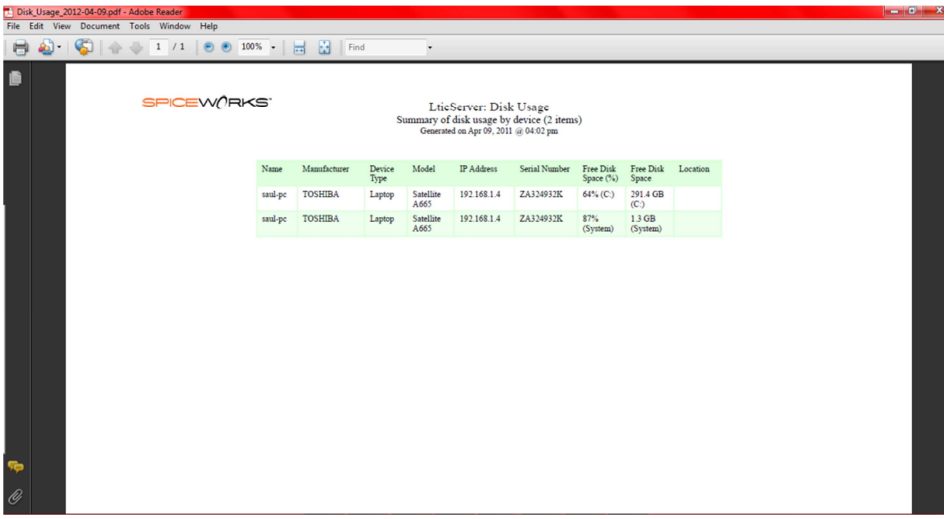


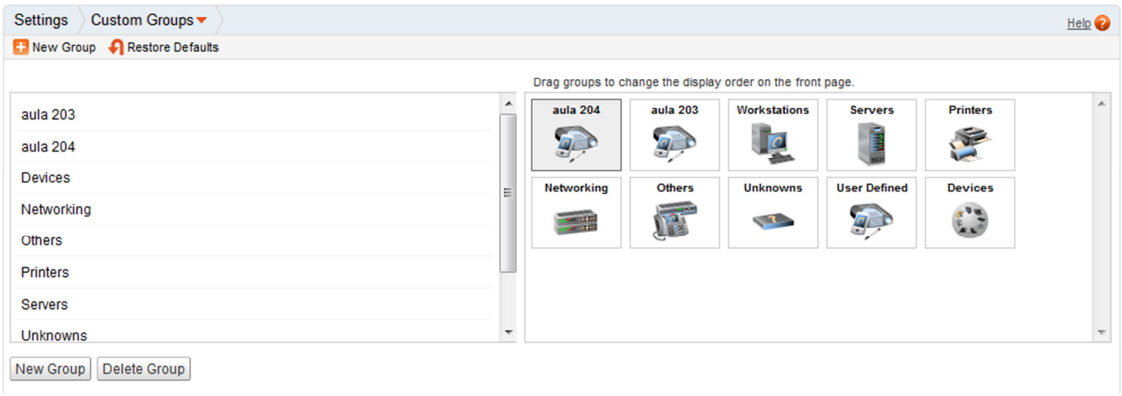
Imagen 2: Archivo reporte PDF



10.8. Grupos.

Spicework tienen la posibilidad de crear grupos, esto nos permitirá tener un mejor manejo a la hora del monitoreo, Se asignaron dos aulas del LTIC, el aula 203 y el aula 204, dentro de estos dos grupos podremos asignar nuestros equipos correspondientes a las aulas anteriormente mencionadas.

Imagen 3: Grupos en Spiceworks



* Imagen 1: Captura pantalla de reportes Spiceworks
* Imagen 2: Captura Archivo reporte PDF
* Imagen 3: Captura Grupos en Spicework

Tabla comparativa herramientas WEB investigación.

Identificador	Parallels	PRTG	Spiceworks
Acceso Web o Remoto	si	si	si
Compatibilidad sistema Operativo Win/Mac/Linux	si	si	si
Control Administrativo de Equipos de la Red	si	si	si
Identificación de Equipos externos a la Red	-	-	si
Identificación de errores equipos de la Red	-	si	si
Fácil manejo por parte del Usuario	si	si	si
Reporte para Usuarios y Administradores	-	si	si
Entorno gráfico Web Amigable	si	si	si
Diseñador de Red interactivo	-	si	si
Acceso rápido para Usuario vía Web	si	si	si

Compatibilidad multi exploradores web	si	si	Google Chrome recomendable / actualizaciones de Internet Explorer y Firefoz necesarias
Ingreso seguro para Administradores de seguridad	si	si	si

Tabla comparativa Herramientas WEB * Análisis por Saúl Lozada

11. Obtención de resultados con la herramienta PRTG.

11.1 Análisis y pruebas con la herramienta PRTG.

Mediante el análisis de la herramienta PRTG, obtuvimos los siguientes resultados respecto a la Red del laboratorio LTIC, en base y complemento con la herramienta Spiceworks.

El análisis respecto a la herramienta PRTG, se va enfocado a monitorear los equipos respectivos del aula 203 y el aula 204.

11.2. Análisis y pruebas en el Aula 203 para la semana del 18 de noviembre del 2013

Hasta el 20 de diciembre del 2013

Reporte salud de la sonda

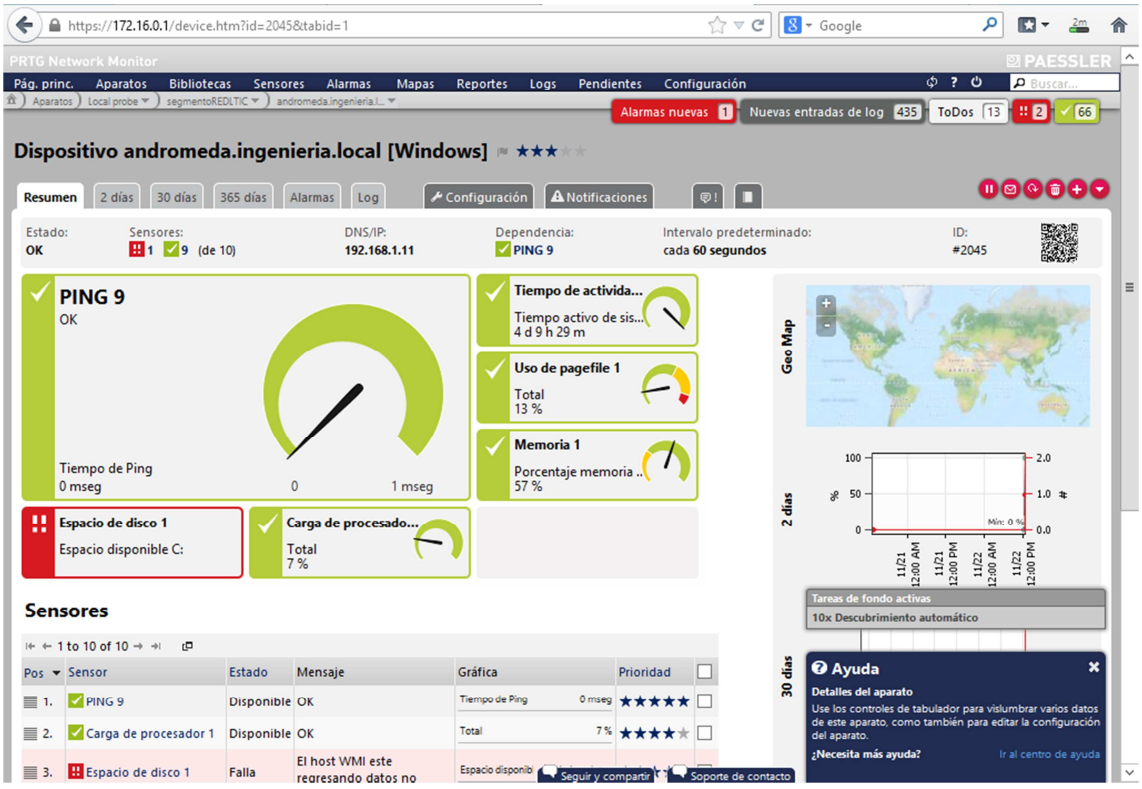


Imagen 1 * Dispositivos de sonda para el servidor y Aula 203

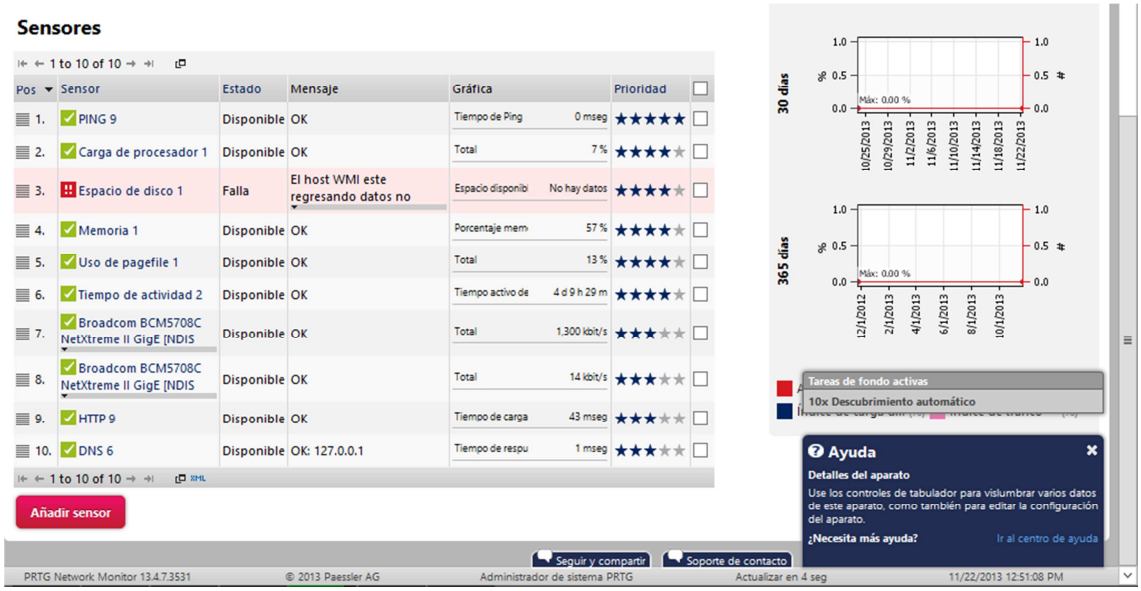


Imagen 2* Sensores de sonda

Detección de fallo en el gripo Grapo Raíz

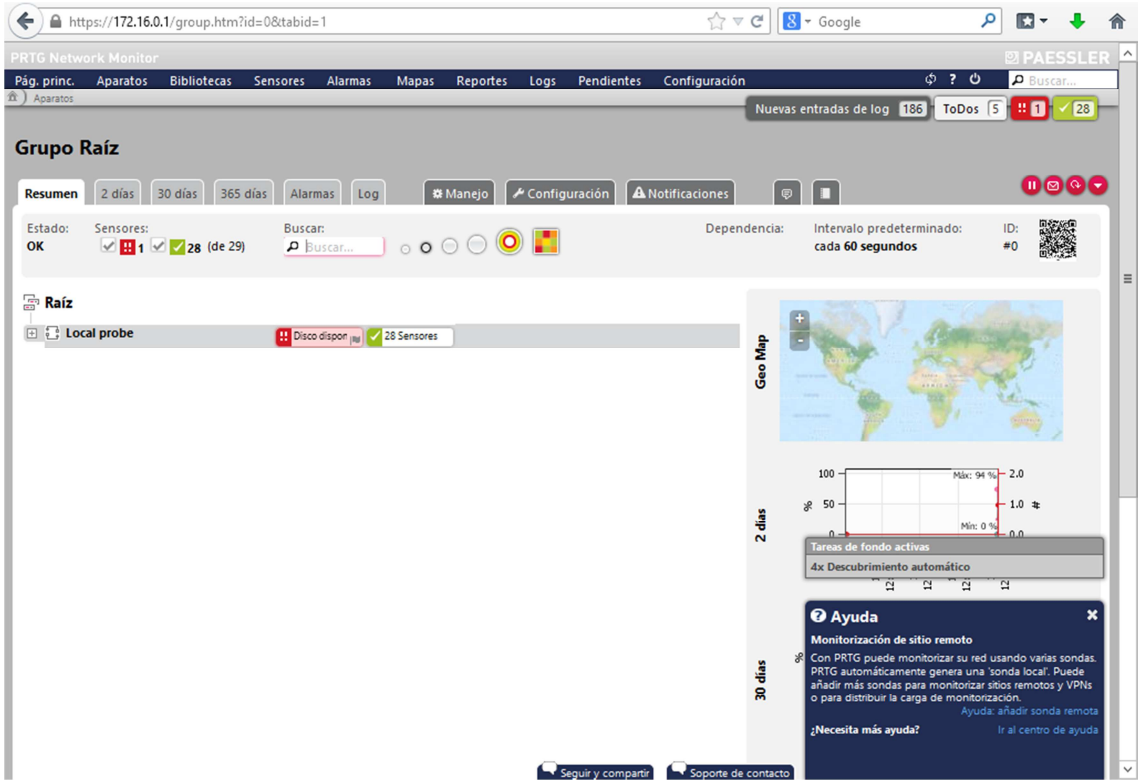


Imagen 3 * Error en Dispositivo de Disco

Detalle de Alarma para sensores de Sonda

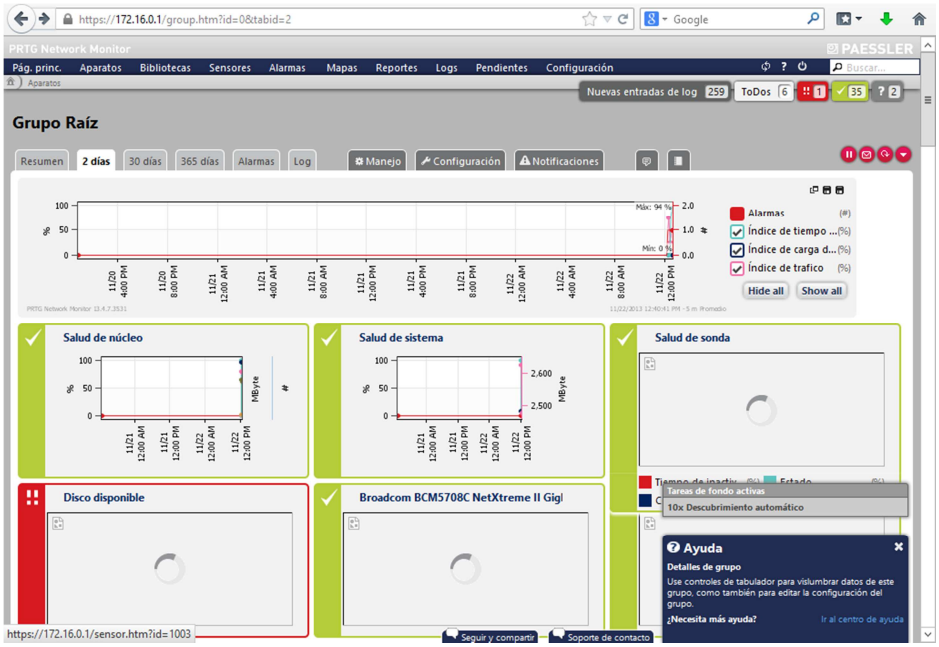
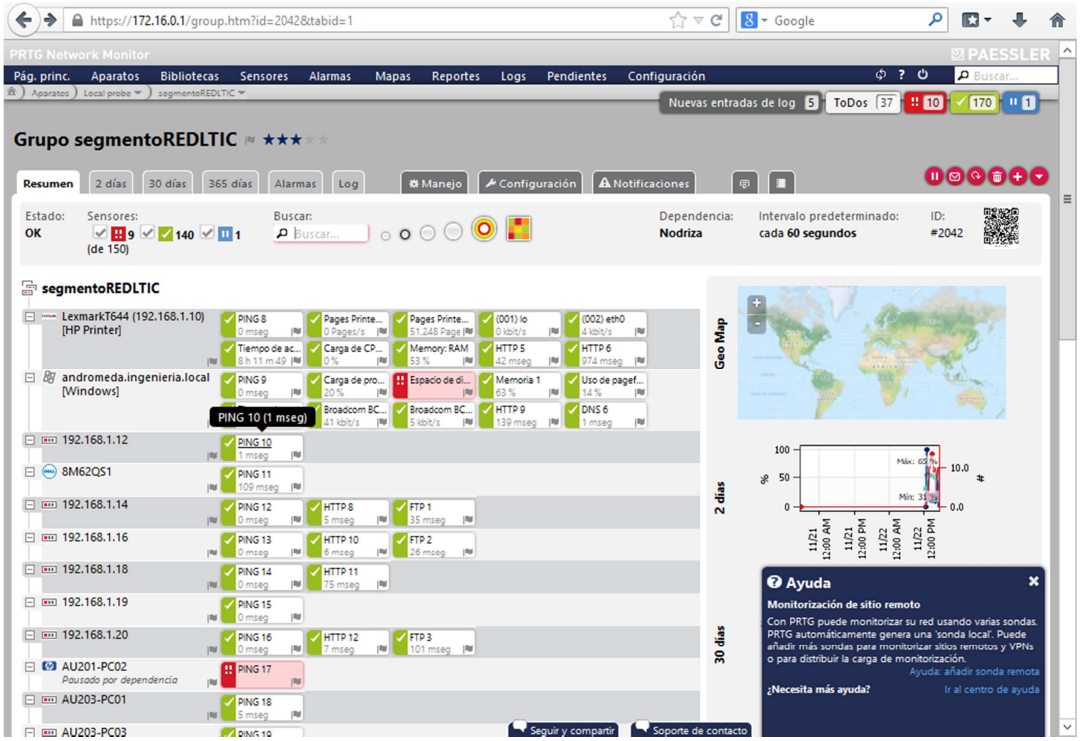


Imagen 4* Alarma de error en disco

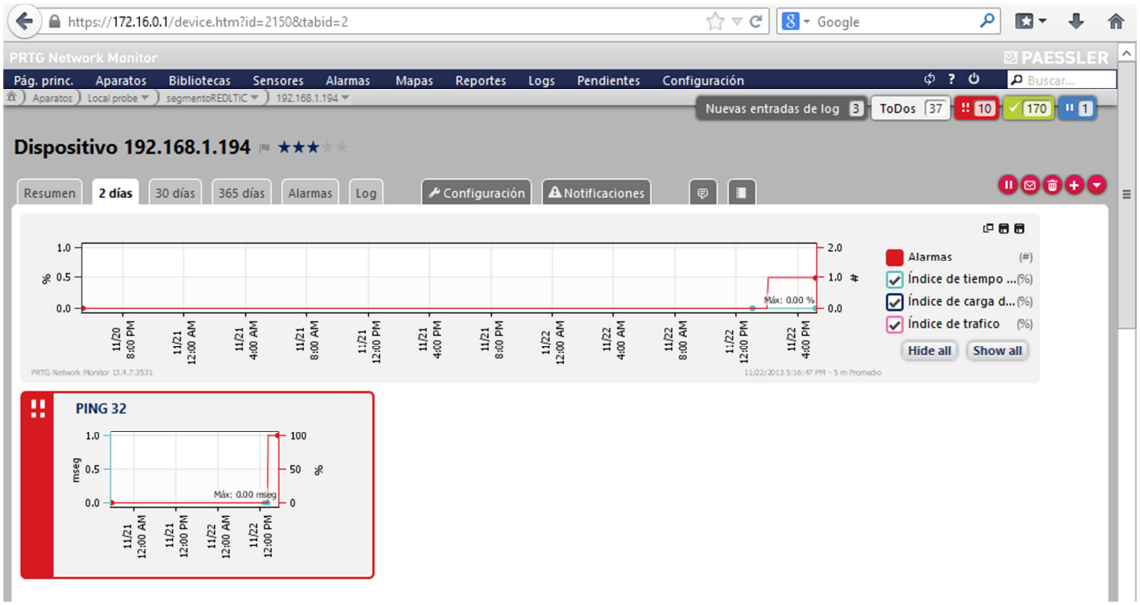
Según el monitoreo, el reporte de capacidad y salud de disco para el aula 203 reporta la existencia de fallas. El promedio para espacio disponible desde el 20 hasta el 22 de noviembre del 2013, no es suficiente y existen otros problemas físicos para su correcto funcionamiento.

Imagen 5 *Segmentos de la Red LTIC



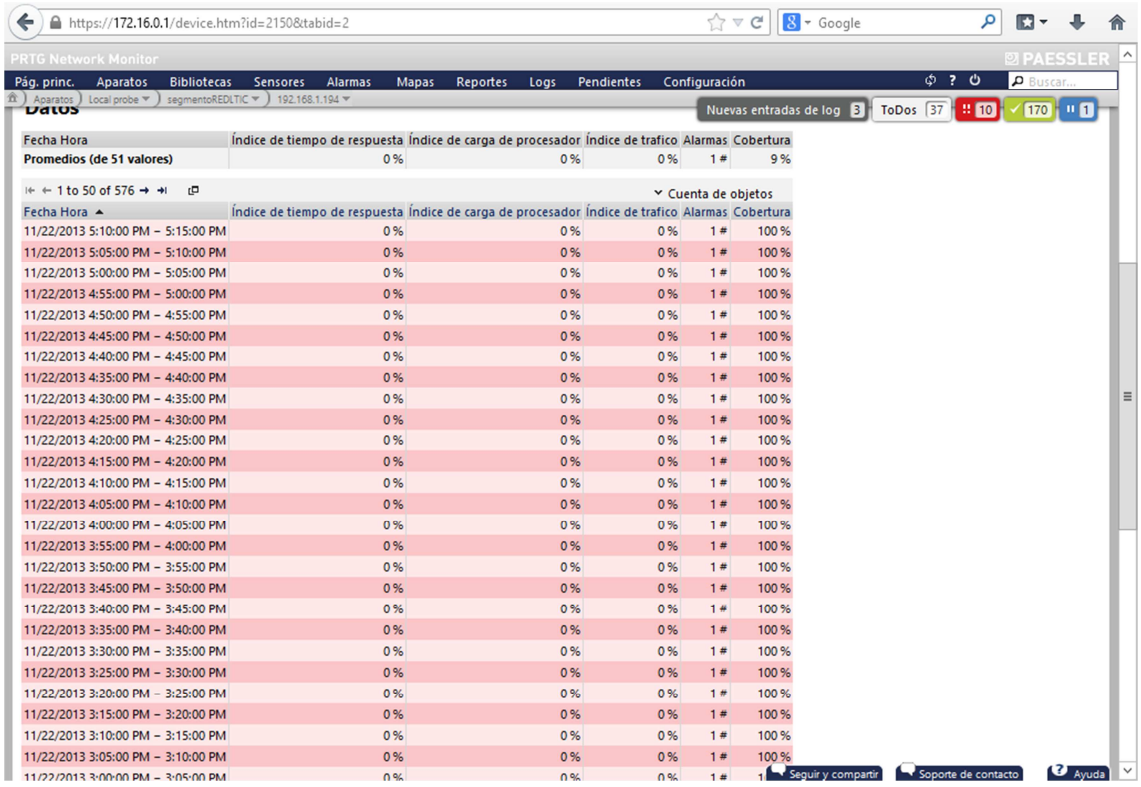
Errores detectados en la comunicación del servidor con el aula 201 y sus respectivos equipos.

Imagen 6 * Análisis de datos para el Dispositivo 192.168.1.194



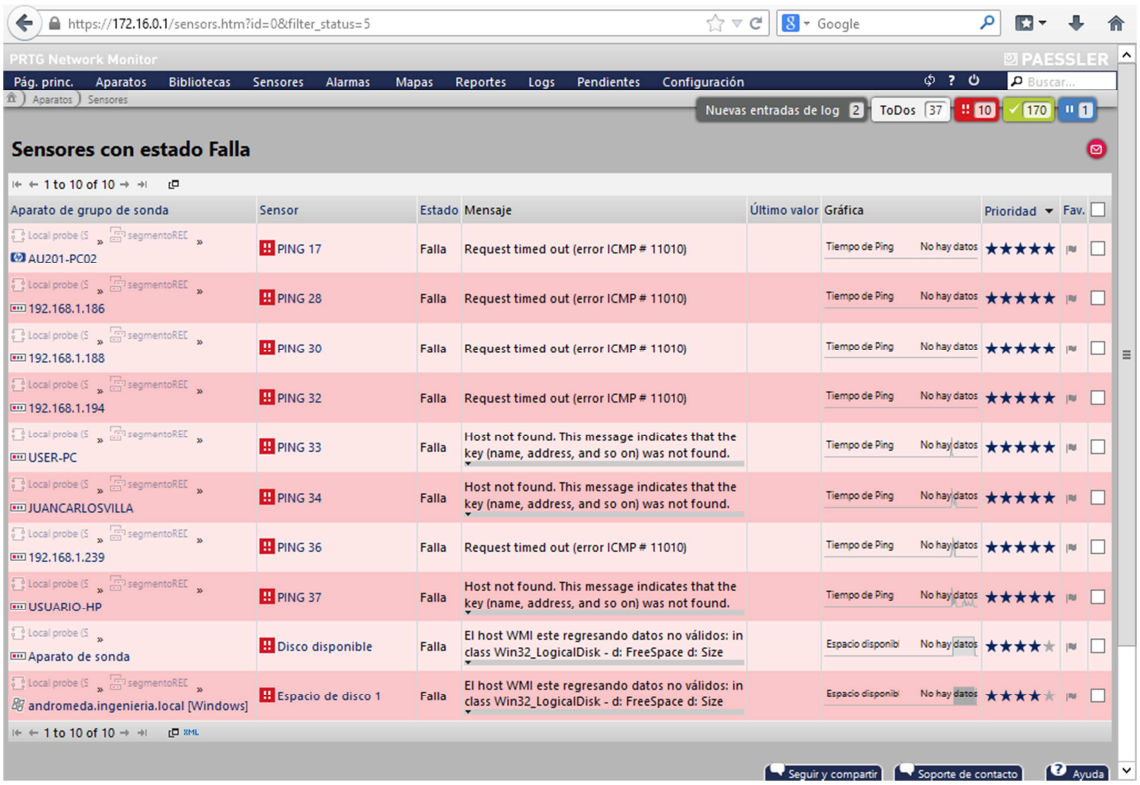
Perdida de conexión del servidor con el equipo Au201- pc08

Imagen 7 *Datos con tiempo de respuesta para equipo Au201- pc08

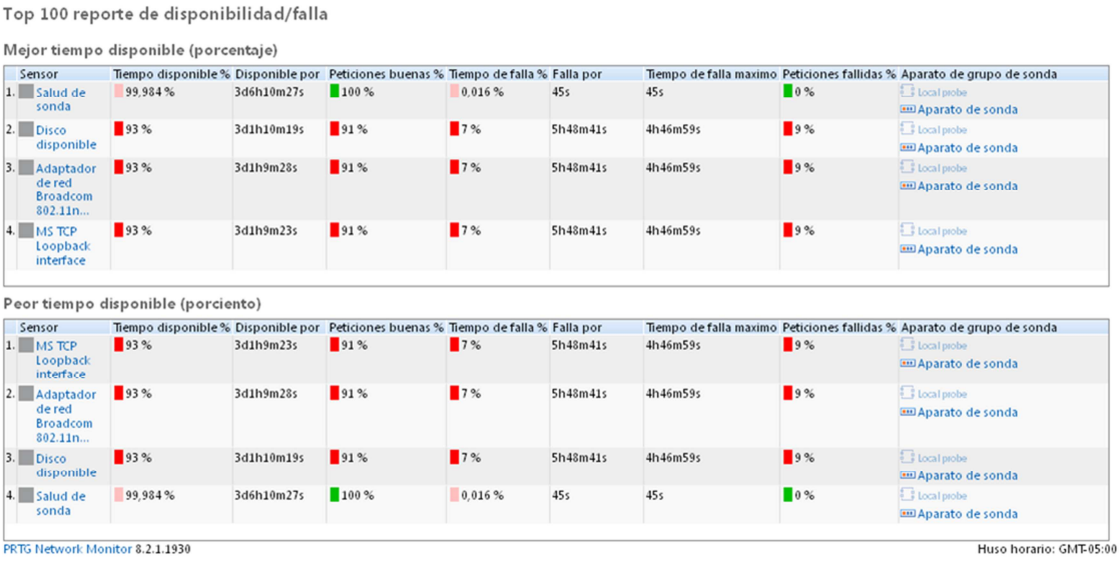


Existe una perdida en la conexión del servidor con los equipos del aula 201, esto se está dando debido a un problema en el cableado estructurado.

Imagen 8 * Sensores con estado de falla



Falla en la comunicación con los equipos au201 pc02, y los pertenecientes a las direcciones ip 192.168.1.86, 492.168.1.88, 192.168.194.



11.3 Reporte salud y capacidad del Disco, Reporte Trafico Wireless LAN, Reporte Loopback Interfase para el periodo del 18 de noviembre del 2013 al 20 de diciembre del 2013

Los reportes de falla y disponibilidad se pueden ver reflejados dentro de la tabla y dentro de los porcentajes indicados:

Disco = 4.928% fallo - 95.155% disponibilidad
Loopback Interfase = 4.919% fallo – 95.152 disponibilidad
Trafico Wireless LAN = 4.927% fallo – 95.151% disponibilidad

- Tráfico Lan para los sensores PING 17,28,30,32,33 falla en la comunicación y tiempo de respuesta agotado, este problema se suscita a momentos, alrededor de un 35% a 37% en la falla de comunicación con el aula 201 del total del 100% de la comunicación.

- Este problema se puede dar por problemas y puntos de red con fallas en el cableado estructurado. Por lo cual, la conexión del servidor con el aula 201 no es optima

- El porcentaje de disponibilidad sigue siendo mayor, por lo cual, se hará un seguimiento respecto al porcentaje mínino de falla, encontrar el respectivo error y póder aplicar una corrección.

- El Disco duro posee un problema físico, su funcionamiento es correcto, pero a momentos existen fallos en comunicación con el equipo.

El porcentaje de disponibilidad bajó hasta un 72% de capacidad, respeto al incremento de usuarios/ equipos para el aula 204, 203 y 201, el 27% de fallo respectivo para disco, trafico Wireless LAN y Loopback interfase que se ven afectados.

Capítulo IV

12. Síntesis de resultados obtenidos con la Propuesta para la detección de problemas de seguridad en la red del LTIC.

Durante el desarrollo de este tema de estudio, se utilizaron tres herramientas, Parallels, SpiceWorks y PRTG; estas tres herramientas de software, en conjunto, poseen un alto potencial respecto a la identificación de problemáticas en el tráfico, la comunicación, identificación de usuarios, identificación de dispositivos, errores con el hardware, errores con el software, y la seguridad informática, en este caso, la seguridad de la red LAN y WAN del LTIC.

Inicialmente se planteó trabajar con servidor de respaldo que posee el LTIC, de esta manera, los datos que posee el laboratorio no se vean afectados y corran riesgo durante el desarrollo del presente trabajo problemática.

Estado Actual

Para el desarrollo de la problemática, se tomaron dos de las aulas con mayor frecuencia de usuarios en el LTIC, aula 203 y el aula 204, con un total de 14 equipos computacionales, además de estos se monitorearon también los equipos de la oficina de becaria y un equipo con sistema operativo Linux (Ubuntu).

Servidores

Se manejaron varios tipos de servidores, la mayoría con software libre u open source pero sí hay algunos con software propietario o privativo. Tenemos al Firewall que está con la última versión de Untangle server 9.4.2, maneja dos direcciones de IP públicas, y tiene un tarjeta de red para la DMZ y otra para la LAN. Uno de los servidores más importantes es el servidor de dominio con Windows Server 2012, que maneja un Active Directory con todos los usuarios de los estudiantes y profesores, además de manejar las licencias de Windows y las licencias del MS Office, este está instalado en un servidor DELL Poweredge 2950.

Dominio PUCEING.EDU.EC

El dominio puceing.edu.ec es administrado en dos servidores de DNS con el esquema primario y secundario o maestro/esclave y están ubicados en la DMZ, con el servidor WEB1 alberga a la página web de la facultad, usa un proxy reverso para poder utilizar otros servidores web con la misma IP externa y es el servidor primario de DNS. El servidor de DNS secundario se llama DNS2 y sólo maneja este servicio. Estos servidores están instalados bajo Centos 6, en unos equipos clones.

Host Virtual

Luego se tiene el servidor de host virtuales en un HP Proliant DL380 G6, tiene 20 GB de Ram y un espacio en disco de 1.5 TB. Aquí están instalados varios servidores, un servidor WEB secundario, el servidor de correo con Zimbra que maneja el correo para el dominio puceing.edu.ec. Un servidor de Big Blue Button que permite dar clases a distancia y se conecta con el moodle de la Facultad (No es el mismo moodle de la PUCE). Todos estos servidores corren bajo Centos 6 a excepción del Big Blue Button que corre bajo Ubuntu 12.04 LTS. El servidor virtual Web2 se conecta al Active Directory para que los estudiantes puedan acceder a un mini servicio de hosting.

Este semestre se instaló un cluster de servidores con equipos antíguos con la distribución Rock N Roll Linux 6. Está basado en Centos 6.

Por último tenemos un servidor de archivos con Windows Server 2012 que no esta ubicado en la DMZ, está ubicado en la LAN.

Equipos de RED

Todas las aulas están en la misma red y se conectan en una serie de equipos en cascada. Tenemos 2 switches 3Com 4400 que se conectan por un cable UTP entre ellos y estos a la vez se conectan con los switches en cada aula que tiene cableado estructurado.

La DMZ se conecta con un Switch Cisco 2950.

La red inalámbrica usa un 3Com Wireless Lan Switch WX1200, está a la vez maneja el servicio de DHCP, hasta para la red cableada. Los equipos en las aulas tienen direcciones IP estáticas.

El acceso a las aulas se maneja por tarjetas magnéticas, estos equipos están en la misma red de la LAN.

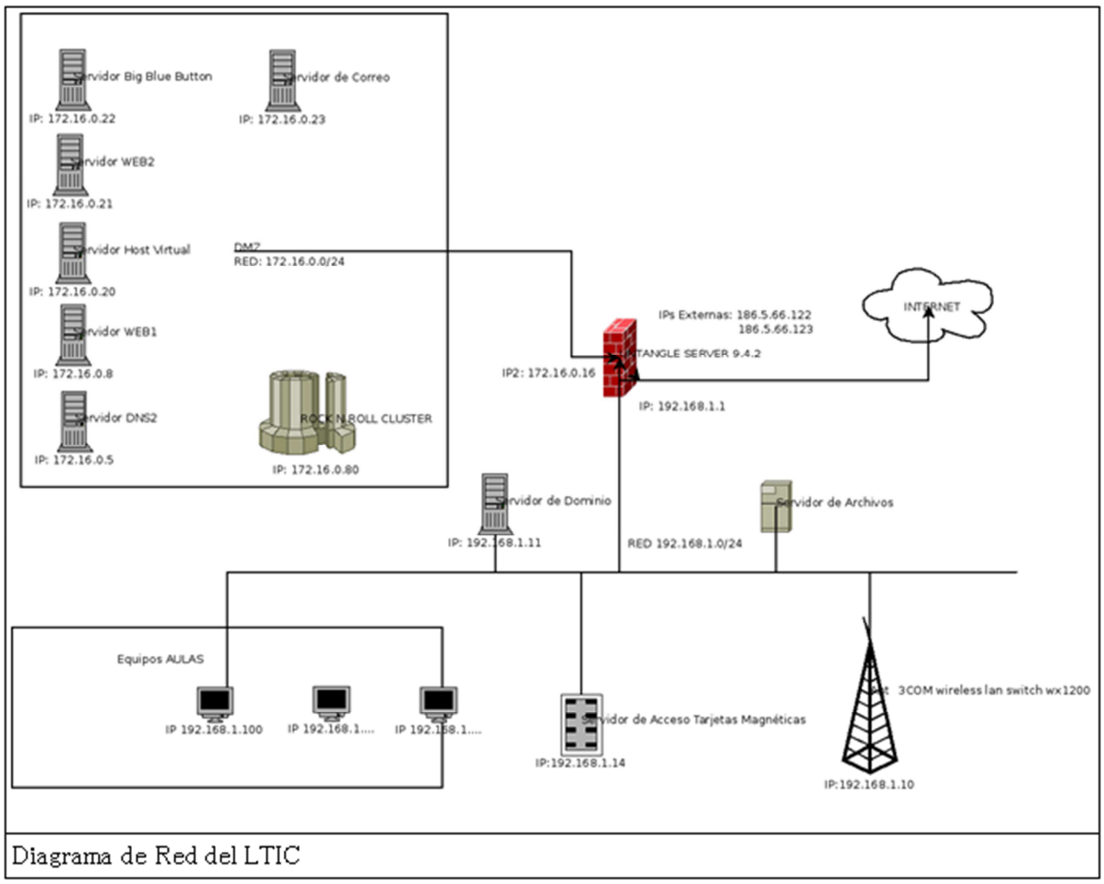


Imagen 1 * Diagrama de la Red LTIC

Otros equipos e instalaciones.

Por petición del laboratorio LTIC, el departamento informático de la PUCE, realizo la instalación de un Access point para cubrir las necesidades de los estudiantes respecto a la RED inalámbrica PUCEWIFI. Este Access point se encuentre en la planta del laboratorio LTIC.

La red originalmente se supone que está hecha en categoría 6. Se tiene una DMZ que este año fue arreglada y se tiene una LAN que se comparte con la red inalámbrica, lo que nos da un máximo de 254 equipos en la red.

Dentro del tiempo de desarrollo de la investigación, se pudo adquirir el sistema de tarjetas magnéticas, para limitar el inadecuado uso de las instalaciones y los equipos del LTIC.

Tomando en cuenta el alto flujo de usuarios dentro de la facultad de Ingeniería, respectivamente a los que hacen uso de los equipos en las aulas del LTIC, así también los que poseen equipos propios, se identificaron más equipos entre los cuales están laptops, tablets pc, teléfonos y dispositivos móviles, pertenecientes a los estudiantes de ingeniería.

Respecto a los dispositivos como Access point, que se encuentran ubicados dentro de la infraestructura que corresponde a la facultada de ingeniería como también el laboratorio LTIC, no se extiende más allá del edificio de ingeniería.

Problemas Actuales

Se tienen problemas con algunos puntos de la red que no cumplen exactamente el estándar de cableado estructurado de categoría 6.

La red inalámbrica no cubre de una manera propia a todo el laboratorio, se cae la conexión constantemente. La seguridad de la red inalámbrica se maneja solo con WPA, cualquier persona que sepa la clave se puede conectar.

El ancho de banda es de 2MB de subida y bajada. Compartimos cierto ancho con la universidad entonces a veces suele funcionar mejor.

No se posee una sola de tecnología, esto se refiere a que los equipos son de varias marcas, desde 3Com, Cisco y Motorola para la parte Wireless, lo cual genera varios problemas de compatibilidad.

Hay equipos de los cuales ya no tienen soporte en el país, esto es un limitante para el laboratorio LTC.

Los switches solo soportan 10/100 Mbps, lo cual hace lento el traspaso de información ahora que se manejaran información en Gigabytes en algunos casos.

Identificados con las herramientas de software

Mediante la herramienta SpiceWorks se pudo identificar que en las aulas 203 como 204, existían herramientas de software no autorizadas como video juegos y otras herramientas de ocio no necesarias.

Éstas estaban siendo utilizadas y el flujo de conexión de la RED pudo ser afectada y existir un decremento en el rendimiento.

Se Identificó además, que para poder instalar este tipo de software como son video juegos u otro software no autorizado, se necesitaba de una clave de administrador, la cual fue sustraída por medio remoto, fue facilitada o los equipos fueron vulnerados. Se efectuó la actualización de nuevas claves en las aulas tanto 203 y 204, como medida.

El LTIC, cuenta con un programa de seguridad para grabación continua, en puntos estratégicos, de esta manera se tiene un control de quién ingresa a las instalaciones.

El problema identificado, es el tipo de equipos con el que se cuenta, las cámaras de seguridad no son las adecuadas, ya que al momento de identificar rostros, no se tiene la calidad y la resolución adecuada.

Se instaló el sistema de tarjetas magnéticas en el laboratorio LTIC, de esta manera se pudo obtener un control respecto a quíenes ingresan a las instalaciones. Así también como del uso de las aulas y los equipos por parte de los estudiantes.

La herramienta Parallels, permite tener un control en forma remota, ya que no todos los miembros del LTIC poseen control total sobre los accesos y claves, Parallels remotamente permite manejar esto si los administradores no se encuentran dentro de las instalaciones del LTIC, ya que Parallels se puede interconectar a través de dispositivos móviles, o laptops a través de direccionar la IP del equipo o equipos en el que se encuentran instalados. En el caso de

la investigación Parallels nos permitía manejar remotamente el servidor de prueba donde se trabajó.

Dentro de la investigación, la herramienta que se explotó más, para el monitoreo exhaustivo durante todo el periodo de estudio, fue PRTG, con ella pudimos monitorear las aulas 203, 204 y los equipos de becaría.

PRTG, permitió observar las anormalidades en el tráfico y flujo de la RED LAN y WAN del LTIC, obteniendo resultados en tiempo real.

PRTG, permitió mediante los registros de actividades monitorear errores tanto respecto a la conectividad y comunicación de la RED LTIC, como también en los componentes de hardware de los equipos del LTIC.

Mediante PRTG, se identificó que existen problemas en la conectividad del servidor con varios puntos de RED en el Aula 204, existen algunos puntos de red muertos, esto se puede dar porque quizás se encuentren dañados.

Este tipo de problema se suscitó en horas clases, con algunos equipos que se quedaban colgados al momento de ingresar al dominio, no existía una respuesta del servidor con los equipos del aula 204.

A la vez PRTG, nos permitió identificar que algunos de los equipos tenían problemas en sus componentes como discos duros y tarjetas de red.

Se pudo identificar otro problema en la conectividad servidor equipos aula 204, el mal funcionamiento de los componentes de hardware de los mismos.

Capítulo V

13. Conclusiones y recomendaciones.

13.1. Conclusiones.

- Las herramientas de Software utilizadas en conjunto para el desarrollo de la investigación, Parallels, SpiceWorks y PRTG, permiten tener un monitoreo más exacto respecto a nuestra RED LAN y WAN, el control total respecto a los equipos que se encuentran conectados e identificados en la RED del LTIC así también como poder visualizar los dispositivos ajenos a la RED del laboratorio.

- Parallels, facilita visualizar, el servidor de pruebas donde se encuentra instalado todo el software de la investigación, al momento de no poder estar físicamente presente en el laboratorio del LTIC.

- Parallels, tiene una gran accesibilidad a la hora de utilizarse, en dispositivos móviles o pads, pudiendo de esta manera visualizar todo el servidor de datos remotamente, si se tiene acceso a internet, en tiempo real.

- Parallels posee un potente motor de virtualización, si lo que se desea es trabajar en un ambiente con gran cantidad de información, así también como un alto manejo de equipos. En el caso de la investigación, el ambiente de trabajo del LTIC fue adecuado para la herramienta de software.

- SpiceWorks, permitió tener un correcto y completo control, respeto a los dispositivos que se encuentran conectados a la RED del LTIC.

- Gracias a SpiceWorks, se pudo realizar un inventario del LTIC, ya que la herramienta de software posee un identificador de Hardware y Software, a través de un análisis por equipos, desde el servidor, los dispositivos de red, como son switchs, módems, routers, cámaras de seguridad, los equipos conectados en las aulas y sus respetivos componentes internos, el software que se encuentra instalado por aula, los dispositivos externos como impresoras scanners y equipos no pertenecientes a la RED, como son teléfonos celulares, pads, laptops.

- SpiceWorks, permite observar si ciertos equipos se encuentran con fallas en su software, en los casos encontrados por motivos de activación, incompatibilidad, caducidad e instalaciones erróneas.

- SpiceWorks, permitió identificar el excesivo uso de dispositivos que se encuentran conectados a la RED inalámbrica, visualizando que el número de dispositivos triplicaban la cantidad de estudiantes que posee la facultad de Ingeniería.

- SpiceWorks, permitió identificar el software no educativo que se encontraba instalado en el aula 203 y 204. Además de esto se pudo identificar que las claves de accesos y de administradores estaban siendo mal utilizadas.

- PRTG, permitió tener un monitoreo exhaustivo durante el periodo de investigación, para lo que fue el servidor de pruebas, los equipos en el aula 203, 204 y la sala de becaria.

- A través de PRTG, se pudo controlar el flujo de la RED del LTIC, en las aulas de estudio, observando que para los días con menos frecuencia, la cobertura de la RED sobrepasaba el 80%

que está dentro de los parámetros normales, para un laboratorio de informática e investigación; para los días con mayor acogida y mayor fluyo de información bajaba hasta casi el 60%. Pero esto también se debe al sin número de dispositivos identificados y que se encuentran conectados a la RED.

- PRTG, permitió identificar problemas del hardware durante el monitoreo, estos problemas, se mantuvieron hasta el final de la investigación. Pero que fueron reportados directamente al LTIC, para su posterior solución.

- PRTG, posee la opción de informarnos, mediante mensajes, si los equipos poseen alguna falla, se envía un mail de los fallos que estén asociados nuestros equipos.

- PRTG, permite obtener los resultados de la investigación, en base a reportes, tablas y gráficos, de esta forma el administrador de la RED del LTIC, podrá tener un mejor detalle y análisis respecto a los datos por equipo.

- PRTG, facilita el análisis por parte del administrador de la RED y que este a su vez pueda focalizar los problemas que se susciten, mediante el reporte de alertas.

13.2 Recomendaciones.

- El Laboratorio LTIC, debe implementar herramientas para el monitoreo de su RED LAN y WAN, como en esta investigación y que se puedan mantener como políticas nuevas, en base a la implementación de software.

- Las herramientas de monitoreo WEB y seguridad permiten, tener un manejo ordenado y correcto de la RED, de esta forma tener un control total en las actividades de un laboratorio de informática, como es el caso del LTIC.

- Acorde a la infraestructura y el equipamiento del LTIC, es necesario que se manejen herramientas de administración y seguridad WEB, de esta forma poder brindar un mejor servicio a los usuario, tanto estudiantes como docentes.

- El LTIC, debería tener un limitante respecto a los dispositivos que se conecten a la RED inalámbrica, ya que existe un incremento excesivo en el flujo de datos.

- Se debe hacer un chequeo respecto al cableado estructurado, ya que se encontraron varios puntos de red muertos, para el aula de estudio 204, así también como la categoría de los cables ya que se encuentran entre categoría 4 y categoría 5.

- Respecto a los equipos de red y comunicación sería recomendable migrar a una sola plataforma, en este caso con la plataforma que se posee, CISCO.

14. Bibliografía.

- Parallels Herramienta web para control y automatización computacional (productos adicionales si es necesario su implementación)
http://www.parallels.com/
Manuales de usuarios y técnicos formato PDF.

- PRTG Herramienta para monitoreo de red (Network Monitoring)
http://www.paessler.com/
Manuales de usuario y técnicos formato PDF.

- Spiceworks Software de gestión y control de red
http://www.spiceworks.com/

- Información y teoría sobre delitos informáticos y políticas de seguridad Microsoft
http://www.microsoft.com/business/smb/es-es/legal/informatica_forense.mspx

- Academia de seguridad Microsoft
http://www.microsoft.com/latam/technet/video/alsi.aspx

-Seguridad Linux
http://www.linux.com/news/technology-feature/security

- Seguridad informática y software libre
http://lucas.hispalinux.es/Informes/informe-seguridad-SL/informe-seguridad-SL.pdf

-Seguridad MacOSX
http://www.apple.com/es/macosx/security/

- Otros temas e información sobre seguridad – Internet- biblioteca PUCE

- Exploration CCNA
http://www.cisco.com/web/ES/edu/

- Políticas LTIC

- CEH
http://www.eccouncil.org/courses/certified_ethical_hacker.aspx