

Instalación, Configuración y Administración de  
Servidores Escolares, equipos Exomate, Redes y  
Software

# Aula Digital 1:1 - Manual de Referencia

**EXO S.A.**

Versión 1.03.x \*



\* Si tenés comentarios o correcciones,  
por favor envíanos un mail con las sugerencias: [sugerencias@exocampus.net](mailto:sugerencias@exocampus.net)

Copyright © 2010, EXO S.A. Todos los derechos reservados.

Algunas partes de este manual están basadas en el Manual de Soporte de Usuario de Intel Learning Series, Intel-powered classmate PC y la documentación de ayuda de Intel powered classmate PC Theft Deterrent Server.

EXO, exocampus y Exomate son marcas registradas de EXO S.A..

Intel, el logo de Intel, Intel Core, Intel Teach, y skool, son marcas registradas de Intel Corporation o sus subsidiarias en EE.UU. y otros países.

Microsoft, MSN, NetMeeting, Excel, Outlook, PowerPoint, Hotmail, Internet Explorer, Windows, Windows Media, Windows Live y Wingdings son marcas registradas o marcas comerciales de Microsoft Corporation o sus subsidiarias en EE.UU. o en otras regiones o países.

\*Otros nombres y marcas que se mencionan aquí pueden ser marcas registradas de sus respectivos propietarios.

\*La información contenida en este documento, incluidas las direcciones URL, de mail y otras referencias a sitios Web de Internet, está sujeta a cambios sin previo aviso.

Por sugerencias, reclamos y/o información de ayuda  
visite <http://www.exocampus.com/rtec>  
o envíenos un mail a [rtec@exo.com.ar](mailto:rtec@exo.com.ar)

EXO S.A., Av. Ing. Huergo 1433, C1107APB, Buenos Aires,  
Argentina

# Índice general

<b>I. Aula Digital 1:1</b>	<b>1</b>
1. Modelos de Uso	3
2. Componentes de Hardware	5
2.0.1. Exomate con tecnología Intel	5
2.0.2. Exomate Generación 3 modelo X352 - Especificaciones	6
3. Componentes de Software	7
3.1. Suite Educativa de Intel	7
3.2. Opciones Comunes del Software de Computadoras	8
3.3. Gestión del Aprendizaje	8
3.4. El Sistema Operativo	9
3.5. Software de prevención y bloqueo por robo	9
3.6. Software de la Exomate para Estudiantes y Docentes	10
<b>II. Servidor de Seguridad - Manual de Referencia del Administrador</b>	<b>15</b>
4. Sistema de Seguridad	17
5. Esquema de implementación sugerido	19
6. Servidor de Seguridad	21
6.1. Participantes	21
6.2. Gestión de Acceso	22
6.2.1. Accediendo	22
6.2.2. Cambiar Contraseña	22
6.2.3. Administración de Operaciones	23
6.2.4. Cuenta Temporal de Dispositivo	23
6.2.5. Administración de Dispositivos	25
6.2.6. Administración de Provisión	27
6.2.7. Recuperación de Código de Desbloqueo	29
6.2.8. Seguimiento de Dispositivos	29
6.3. Administración del Sistema	31
6.3.1. Administración de Operadores	31
6.3.2. Administración de Alumnos	31

6.3.3.	Administración de Registro . . . . .	32
6.3.4.	Administración de Datos . . . . .	32
6.3.5.	Administración de Seguridad . . . . .	33
6.3.6.	Administración de Servicios . . . . .	37
6.4.	Alumno . . . . .	38
6.4.1.	Acceso . . . . .	38
6.4.2.	Configuración del Perfil . . . . .	39
6.4.3.	Recuperación de Código de Desbloqueo . . . . .	39
6.5.	Autoridad de Usuario . . . . .	41
6.6.	Salir . . . . .	41
6.7.	Sistema de Ayuda en Línea . . . . .	41
6.8.	Recuperación de Desastre . . . . .	42
6.8.1.	Operaciones de Recuperación de Desastre . . . . .	42
6.9.	Preguntas Frecuentes . . . . .	44
<b>7.</b>	<b>Agente de Seguridad</b>	<b>47</b>
7.1.	Ícono en la Barra del Sistema . . . . .	48
7.2.	Interfaz Gráfica de Usuario . . . . .	48
7.2.1.	Configuración . . . . .	49
7.2.2.	Acceder al Servidor . . . . .	50
7.2.3.	Recuperación de Código de Desbloqueo . . . . .	51
7.2.4.	Ayuda . . . . .	51
7.2.5.	Acerca de . . . . .	51
7.3.	Descarga Automática de un Nuevo Certificado . . . . .	52
7.4.	Introduciendo un Código de Desbloqueo . . . . .	53
7.5.	Usando un Disco USB para Obtener Certificados . . . . .	53
7.6.	Preguntas Frecuentes . . . . .	54
7.7.	Mensajes de Error . . . . .	56
7.7.1.	Error al Conectar con el Servidor . . . . .	56
7.7.2.	Ocurrió una Excepción Desconocida . . . . .	56
<b>III.</b>	<b>Servidor Escolar EXO - Manual de Referencia del Administrador</b>	<b>57</b>
<b>8.</b>	<b>Webmin</b>	<b>59</b>
8.1.	Uso de Webmin . . . . .	59
8.2.	Reconocimiento del menú Webmin . . . . .	62
8.2.1.	Cambio de Idioma y Tema . . . . .	62
8.3.	Configuración de Webmin . . . . .	63
8.3.1.	Idioma . . . . .	63
8.3.2.	Mejorar versión Webmin . . . . .	63
8.3.3.	Autenticación . . . . .	64
8.3.4.	Referenciadores de confianza . . . . .	65
8.3.5.	Acceso anónimo a Módulo . . . . .	66
8.3.6.	Encriptación SSL . . . . .	66

---

<b>9. Servidor DHCP</b>	<b>69</b>
<b>10. Administración de impresoras</b>	<b>71</b>
<b>11. Servidor Web Apache</b>	<b>73</b>
11.1. Acceder al módulo Apache de Webmin . . . . .	73
11.2. Opciones globales . . . . .	75
11.2.1. Límites y Procesos . . . . .	75
11.2.2. Redes y direcciones . . . . .	76
11.2.3. Editar archivos de configuración . . . . .	76
11.3. Virtual hosts . . . . .	77
11.4. Control del servidor web Apache . . . . .	80
<b>12. IPTables: El firewall de Linux</b>	<b>81</b>
12.1. Pantalla inicial . . . . .	82
12.2. Vista de reglas . . . . .	83
12.3. Crear una regla nueva . . . . .	84
<b>13. ProFTPD</b>	<b>87</b>
<b>14. Samba</b>	<b>91</b>
14.1. Preparando el entorno para compartir . . . . .	93
14.1.1. Establecer grupos de usuarios . . . . .	94
14.2. Agregar carpetas para compartir . . . . .	95
14.3. Compartir Impresoras . . . . .	96
14.4. Compartición sin contraseñas . . . . .	97
14.5. Compartición con contraseñas . . . . .	100
<b>15. Servidor proxy Squid</b>	<b>105</b>
15.1. Características . . . . .	105
15.2. Proxy Web . . . . .	106
15.3. Squid en Webmin . . . . .	107
15.4. Puertos y trabajo en red . . . . .	108
15.5. Uso de memoria . . . . .	109
15.6. Opciones administrativas . . . . .	110
15.7. Configuración del redireccionamiento de puertos . . . . .	111
<b>16. SARG Generador de Informes de Análisis de Squid</b>	<b>113</b>
16.1. SARG en Webmin . . . . .	113
16.2. Opciones de informe . . . . .	117
16.3. Estilo de informe . . . . .	117
16.4. Generación de Informe planificado . . . . .	118
<b>IV. Apéndices</b>	<b>119</b>
<b>A. Manual de Usuario Exomate X352</b>	<b>121</b>

A.1.	Instrucciones de seguridad . . . . .	121
A.1.1.	Advertencias generales . . . . .	121
A.1.2.	Advertencias sobre el cable y el adaptador . . . . .	122
A.1.3.	Advertencias sobre la batería . . . . .	123
A.1.4.	Desecho de baterías . . . . .	124
A.1.5.	Reciclaje del equipo y/o de la batería . . . . .	124
A.1.6.	Indicaciones de seguridad adicionales para equipos con comunicaciones inalámbricas . . . . .	125
A.1.7.	Cuidados de la pantalla LCD . . . . .	125
A.2.	Guía rápida de instalación . . . . .	126
A.2.1.	Conexión del adaptador de alimentación . . . . .	126
A.2.2.	Encendido del equipo . . . . .	126
A.3.	Introducción al uso de la netbook . . . . .	127
A.3.1.	Vista de frente . . . . .	127
A.3.2.	Vista izquierda . . . . .	128
A.3.3.	Vista derecha . . . . .	128
A.3.4.	Vista posterior . . . . .	129
A.3.5.	Indicadores de LED status . . . . .	129
A.3.6.	Los controles de función (hot key) . . . . .	130
A.3.7.	Teclado . . . . .	130
A.3.8.	Pad de mouse . . . . .	131
A.3.9.	Batería . . . . .	131
A.3.10.	Como limpiar su equipo . . . . .	131
A.4.	Funcionamiento de la batería . . . . .	132
A.4.1.	Control de la carga de la batería . . . . .	132
A.4.2.	Medidor de potencia . . . . .	133
A.4.3.	Advertencia de batería baja . . . . .	133
A.4.4.	Preparación de la batería para el uso (calibración) . . . . .	133
A.4.5.	Carga de la batería . . . . .	134
A.4.6.	Almacenamiento de la batería . . . . .	134
A.4.7.	Funcionamiento con baterías adicionales . . . . .	134
A.4.8.	Maximización de la vida de la batería . . . . .	134
A.5.	Recuperación de Sistema . . . . .	135
A.5.1.	Recuperación de sistema Exomate . . . . .	135
<b>B.</b>	<b>Configuración de la Conexión Wireless para Exomate</b>	<b>139</b>
B.1.	Configuración de la Conexión Wireless en Windows . . . . .	139
<b>C.</b>	<b>Resguardo y recuperación del sistema de Exomate</b>	<b>141</b>
C.1.	Resguardo y recuperación del sistema utilizando un dispositivo USB de almacenamiento . . . . .	141
C.1.1.	Generar memoria USB de Recuperación . . . . .	141
C.1.2.	Iniciar una Exomate desde una memoria USB de Recuperación . . . . .	142
C.1.3.	Copia de seguridad del sistema . . . . .	142
C.1.4.	Restauración del sistema . . . . .	143

<b>D. e-Learning Class - Tutorial para el Docente</b>	<b>145</b>
D.1. Prerrequisitos del tutorial . . . . .	146
D.2. Iniciando una Clase Virtual . . . . .	147
D.2.1. Creación de un aula virtual . . . . .	147
D.2.2. Conecte las Exomate's a la computadora del profesor . . . . .	148
D.2.3. Conectando a un Alumno a una Clase Virtual . . . . .	149
D.2.4. Otorgar a un Alumno el Acceso al Aula Virtual . . . . .	150
D.3. Comprendiendo el Panel de e-Learning Class . . . . .	152
D.3.1. Panel de e-3.1 e-Learning Class . . . . .	152
D.3.2. Barras de herramientas de e-Learning Class . . . . .	153
D.3.3. Ícono de la barra de tareas de e-Learning Class . . . . .	155
D.4. Interactuando con los Alumnos . . . . .	155
D.4.1. Supervisar y controlar . . . . .	155
D.4.2. Control Remoto . . . . .	156
D.4.3. Difusión de la Pantalla . . . . .	158
D.4.4. Pluma . . . . .	159
D.4.5. Demostración del alumno . . . . .	160
D.4.6. Silencio . . . . .	162
D.4.7. Película en Red . . . . .	163
D.4.8. Distribución de Archivos . . . . .	164
D.4.9. Otras Funciones . . . . .	165
<b>E. Guía de Software My Storage</b>	<b>167</b>
E.1. Generalidades de la aplicación . . . . .	167
E.2. Utilizando la aplicación . . . . .	168
E.2.1. Inicio de My Storage . . . . .	168
E.2.2. Ícono de bandeja . . . . .	168
E.2.3. Menú de bandeja . . . . .	169
E.2.4. Ventana principal de My Storage . . . . .	170
E.2.5. Monitor de discos . . . . .	171
E.2.6. Liberador de espacio en disco . . . . .	171
E.2.7. Asistente para copia de seguridad de datos . . . . .	171
E.2.8. Copia de seguridad programada . . . . .	174
E.2.9. Copia de seguridad rápida . . . . .	175
E.2.10. Asistente para restauración de datos . . . . .	176
E.3. Opciones . . . . .	179
E.3.1. Configuración de la copia de seguridad programada . . . . .	179
E.3.2. Configuración de la copia de seguridad rápida . . . . .	180
E.3.3. Otras opciones . . . . .	180
<b>F. Guía de Software Parents Carefree</b>	<b>181</b>
F.1. Generalidades de la aplicación . . . . .	181
F.2. Utilizando la aplicación . . . . .	182
F.2.1. Menú del ícono de la bandeja del sistema . . . . .	182
F.2.2. Configuración de políticas . . . . .	183
F.2.3. Filtro de red . . . . .	184

F.2.4. Control de programas . . . . .	186
F.2.5. Agendar horario . . . . .	186
F.2.6. Configuración . . . . .	188
F.2.7. Revisión de registro . . . . .	190
<b>G. Guía de Software Firewall de Windows</b>	<b>193</b>
G.1. Activando el Firewall de Windows . . . . .	193
<b>H. Instructivo de Activación de Microsoft Office y Microsoft Math</b>	<b>195</b>
H.1. Activación Microsoft Office 2007 . . . . .	195
H.1.1. Activación por Internet . . . . .	198
H.1.2. Activación por teléfono . . . . .	199
H.1.3. Activación manual (si no aparece la opción automática) . . . . .	200
H.2. Activar Microsoft Math 3.0 . . . . .	201
<b>I. Glosario</b>	<b>205</b>



# Parte I.

## Aula Digital 1:1



# 1. Modelos de Uso

Hoy en día, los países reconocen cada vez más que los ciudadanos educados son cruciales para sus posibilidades de éxito en la economía digital mundial. Los estudiantes necesitan desarrollar un nuevo conjunto de habilidades, conocidas como las Habilidades del Siglo 21, para estar mejor preparados para esta realidad, y tener la oportunidad de triunfar.

Las Habilidades del Siglo 21 incluyen la tecnología y la alfabetización mediática, la comunicación efectiva, el pensamiento crítico, la solución de problemas, y la colaboración. Estas son las habilidades necesarias para que los ciudadanos puedan prosperar y tener éxito en la economía global de hoy.

Los programas de e-Learning equipan a los estudiantes con estas habilidades que les permiten –y a los países en los que viven– tener éxito en la economía global de hoy.

Los programas de e-Learning reúnen los elementos para la solución –tecnología, conectividad, contenido digital localizado, y métodos enseñanza mejorados con desarrollo profesional– y otras consideraciones necesarias para el éxito.

Felicitaciones por elegir para su institución la solución Exomate basada en la tecnología Classmate PC diseñada especialmente para la educación por Intel®. Comienza en este camino a partir de hoy un mundo de posibilidades que complementa su iniciativa e-Learning, y este manual será su guía de referencia.



## 2. Componentes de Hardware

El entorno de e-Learning 1:1 consiste en PCs Exomate para los estudiantes y profesores, uno o más servidores de la escuela para despliegues más grandes que un aula, y la conectividad a Internet y puntos de acceso inalámbrico que crean la red interna, como así también proporcionan una conexión a contenido externo.

En esta sección describimos brevemente los equipos Exomate con tecnología Intel.

### 2.0.1. Exomate con tecnología Intel

La plataforma de Exomate basada en tecnología Intel, es una solución pequeña y móvil desarrollada específicamente para estudiantes de todo el mundo. Estos dispositivos de aprendizaje, robustos pero livianos, están diseñados para proporcionar entornos de aprendizaje que están al alcance y que resultan colaborativos, tanto para los estudiantes como para sus profesores.

Las Exomates ejecutan Microsoft Windows o el sistema operativo Linux, y están hechas con resistencia a las caídas, con pantallas LCD en colores, conectividad inalámbrica integrada, cámara Web integrada. La Exomate también cuenta con teclado resistente al agua e incluye funciones y software específicos para la educación, los que serán discutidos más adelante en este manual.



## 2.0.2. Exomate Generación 3 modelo X352 - Especificaciones



**Tecnología:** basada en Classmate PC diseñada especialmente para la educación por Intel®

**Chasis:** personalizado y robusto con funda, resistente a golpes y caídas.

**Procesador:** Intel® Atom N450 – 1.66Ghz 512KB cache de bajo consumo eléctrico.

**Memoria:** 1 GIGABYTE DDR2 SODIMM 667Mhz, expandible a 2 Giga-bytes.

**Pantalla:** LCD con tecnología LED de 10.1" - resolución 1024x600.

**Cámara de video:** integrada 30fps – 640 x 480 puntos.

**Almacenamiento:** Disco Rígido de 160GB SATA.

**Lector de tarjetas de memoria:** para memorias SD/MMC/MS/MS Pro.

**Audio:** Sonido estéreo integrado. 2.1 canales con parlantes y micrófono incorporados.

**Interfaces:** 3 Puertos USB 2.0 / 1 RJ45 / salida auriculares / entrada de micrófono / salida VGA.

**Wireless:** WLAN 802.11b/g/n con antena integrada para conexión WIFI a redes e Internet .

**Lan:** 10/100Mb Ethernet.

**Teclado:** en español con 84 teclas de acceso directo, resistente a líquidos.

**Touchpad:** amplio con botones derecho e izquierdo.

**Chasis:** personalizado y robusto con funda, resistente a golpes y caídas.

**Seguridad:** TPM administración confiable de seguridad en redes por hardware.

**Sistema de Bloqueo por robo:** A través de un servidor se puede bloquear totalmente cualquier equipo, previniendo así el mal uso o reventa de un equipo robado o extraviado.

**Sistema Operativo:** Microsoft Windows XP PRO y Linux Pixart con arranque dual.

**E-learning Class:** herramienta de colaboración para el aula digital con CODEC para video-conferencia.

**Software:** Microsoft Office 2007, Open Office, Utilitarios y aplicaciones varias.

**Alimentación:** Batería recargable de 6 celdas con autonomía de 4 horas aprox.

**Adaptador de Carga:** 100-240 Volts, 50/60 Hz, 40 Watts.

**Medidas:** 25.4cm x 19,5cm x 3,8cm.

**Peso:** 1.5Kg

**Dispositivos Externos:** permite la conexión de unidades externas (no incluidas): lecto-grabadora de CD/DVD, memorias Flash, impresoras y multifunción, receptor / navegador GPS, Modem 3G USB.

**Dispositivos Internos:** opcionalmente de fábrica puede incluir Modem 3.75G o WiMax.



## 3. Componentes de Software

Es importante para el despliegue del entorno de e-Learning identificar los roles y las responsabilidades de todos los actores incluidos en el proceso de e-Learning, así también como ayudarlos a comprender las necesidades y la disponibilidad en lo que respecta a la infraestructura física.

Esta sección lo ayudará a identificar sus roles y responsabilidades, y a entender la infraestructura de su escuela y lo que se necesita para prepararla para el e-Learning 1:1.

### 3.1. Suite Educativa de Intel

El Grupo de Programas ("Suite") Educativos de Intel es un conjunto mínimo de aplicaciones que protegen a los estudiantes y a sus sistemas, además de promover la colaboración en el aula. Está diseñado específicamente para satisfacer las necesidades y requerimientos de la educación, con un fuerte énfasis en reforzar y mejorar la experiencia del estudiante con tecnología. Los componentes básicos son:

- **Gestión del aula:** Permite que los profesores administren las aulas y facilita las actividades diarias del aula a través del intercambio de archivos, las transmisiones en pantalla, transmisiones de video, la evaluación de los alumnos y la gestión del grupo.
- **Gestión de Acceso:** Permite que los padres y las escuelas creen un entorno informático seguro mediante la especificación de los sitios Web y de las aplicaciones que los estudiantes pueden visitar y ejecutar, y fijar límites de tiempo en el uso del sistema y el acceso a Internet.
- **Disuasión de Robos:** Permite que las escuelas desactiven por robo o pérdida las Exomates, mediante una solución de disuasión de robos basada en un hardware integrado.
- **Administración de las Computadoras:** Permite que los estudiantes determinen cuánto espacio de almacenamiento han utilizado, el espacio libre, y que hagan copias de seguridad de sus documentos a través de una interfaz fácil de usar.

## 3.2. Opciones Comunes del Software de Computadoras

Categoría	Uso
Productividad	Hojas de cálculo, calculadoras, software para presentaciones, editores de texto, procesadores de palabras, y más.
Multimedia	Edición de video, edición de fotografías, grabación y reproducción de sonido, pintura y dibujo, y más.
Plan de Estudios y Contenido	El profesor tiene acceso en línea al plan de estudios, y a un apoyo tal como planes de lecciones.
Seguridad	Firewalls ("Barreras de Protección"), control de robos, y software antivirus.
Colaboración/intercambio	Permite que los estudiantes envíen y reciban e-mails, mensajes instantáneos, y otras comunicaciones en línea.
Administrativo	Ayuda a los administradores con tareas tales como la creación de copias de seguridad y la restauración de archivos.
Navegador de Internet	Permite el acceso a sitios Web y su visualización.
Control del Profesor	Permite que los profesores se presenten a los alumnos, monitorear sus actividades, colaborar con ellos y ayudarlos a aprender.
Control de los Padres	Permite que los profesores y padres guíen a los estudiantes en el uso de las aplicaciones y en la visualización de los contenidos de Internet.
Control anti-robos	Ayuda a que las escuelas controlen sus bienes, evitando robos y la reventa de partes.

## 3.3. Gestión del Aprendizaje

Gestión del aprendizaje es un término general para los sistemas de software –a menudo instalados por su proveedor local– que se despliegan para apoyar la capacidad del profesor de crear planes de estudio, desarrollar planes de lecciones, implementar concursos de preguntas y otras actividades, y proporcionar e-content ("contenidos electrónicos"). Este software aumenta la facilidad de uso y la eficacia del sistema educativo 1:1.

Existen tres divisiones principales del Software de Gestión del Aprendizaje:

- **Sistema de Gestión del Aprendizaje:** esto típicamente se refiere a los más completos paquetes de software que permiten un completo desarrollo del plan de estudios, la planificación de lecciones y la gestión de acertijos y otras actividades.
- **Gestión de la actividad:** esto típicamente se refiere a los paquetes de software que permiten la planificación de lecciones individuales y la gestión de acertijos y actividades, pero sin incluir el desarrollo completo del plan de estudios.



- **Gestión de contenidos:** esto se refiere al software que proporciona una fácil gestión de contenido electrónico (tal como e-books –"libros electrónicos"–) para el entorno escolar.

## 3.4. El Sistema Operativo

Este es el elemento de software más fundamental. Es el responsable de la gestión de todos los aspectos de la computadora y permite al usuario ejecutar e interactuar con todos los demás programas, incluyendo las aplicaciones.

Existen dos opciones principales para un sistema operativo:

- **Windows XP PRO (o Windows 7):** Sistemas operativos de código fuente cerrado directamente provistos y respaldados por Microsoft. Los sistemas operativos de Windows representan la mayor cuota de participación en el mercado mundial.
- **Linux:** Un sistema operativo basado en Unix de código fuente abierto que se puede obtener sin costo alguno. (No obstante, el soporte no es gratuito.) Linux viene en varias versiones, como SuSE, Debian, Ubuntu, RHEL, Mandriva, Metaspins, y Fedora.

## 3.5. Software de prevención y bloqueo por robo

**Intel Theft Deterrent (para Windows y Linux):** Es un Sistema de Seguridad que inhabilitará el dispositivo en caso de desvincularse con la red de servicio a la cual se encuentra referenciado. Dicho sistema tiene un componente de hardware (TPM versión 1.2, administración confiable de seguridad en redes) en el equipo y un componente de software que se provee con el equipo. Para su funcionamiento el alumno necesita conectarse con un servidor de seguridad que debe ser configurado para dicho fin, el cual puede estar localizado en cada colegio o en forma centralizada.

Cuando se desea integrar una Exomate al Sistema de Seguridad, se configura de modo que le solicite certificados digitales al servidor configurado, que habilitarán a la Exomate a ser utilizada hasta la fecha de expiración del certificado (o una cantidad determinada de arranques).

La validez de los certificados es configurable desde el servidor de seguridad. Cuando dicho certificado está próximo a su vencimiento, la Exomate intentará comunicarse nuevamente con el servidor de seguridad, solicitándole un nuevo certificado con una nueva fecha de vencimiento posterior a la actual. En el caso en que el servidor emita un nuevo certificado para el equipo, estará habilitado para utilizarse hasta la nueva fecha de vencimiento, cerca de la cual volverá a consultar al servidor para repetir el proceso.

En los casos donde la Exomate no se comunique con el servidor, o cuando se comunique, pero el servidor no expida un certificado (por ejemplo, porque el equipo se ha reportado como robado), la Exomate se bloqueará automáticamente dejándola completamente inutilizada. Durante este bloqueo el usuario de la Exomate no podrá acceder a ninguna función del equipo, ni mucho menos a arrancar el sistema operativo ni ninguna otra función del equipo, la única pantalla que verá será una pantalla indicándole que el equipo se ha bloqueado por

seguridad y que la única manera de desbloquearlo provisoriamente es mediante un código de 10 dígitos que es válido solo para dicho bloqueo de dicha Exomate, y puede obtenerse únicamente desde el servidor de seguridad.

## 3.6. Software de la Exomate para Estudiantes y Docentes

Opcionalmente y dependiendo del sistema operativo, hay otras utilidades que se pueden encontrar en los equipos de los estudiantes, tales como:

### Colaboración y administración de clases

- **e-Learning Class (Windows):** Permite brindar apoyo a los alumnos desde el equipo del docente, posibilitando el monitoreo, control remoto de los equipos, distribución de archivos, creación, corrección y análisis de evaluaciones, chat, demostraciones del alumno y desde grupos de trabajo, configuración y apagado de todas las Exomates en forma remota. Es una herramienta que ayuda al docente a controlar una clase digital, generando un ambiente de colaboración e interacción con los alumnos y una vinculación bidireccional entre docente – alumno. e-Learning Class trabaja únicamente con Exomate y fue desarrollado por la empresa Mythware.
- **Italc (Linux):** iTalc es una poderosa herramienta didáctica para los profesores. Les permite ver y controlar otras computadoras en su red de diferentes formas. Soporta Linux y Windows 2000/XP/Vista y se puede usar en entornos mezclados en forma transparente. Además que el código fuente está disponible en forma gratuita, Ud. tiene la libertad de modificar el software para que cumpla sus necesidades siempre que respete los términos de la licencia de iTalc (GPL).

### Aplicaciones de productividad

- **Microsoft Office Suite:** incluye herramientas como:
  - ◆ Word: Un programa de procesamiento de texto que puede utilizar para crear, editar, formatear y guardar documentos.
  - ◆ Excel: Un programa de hoja de cálculo que puede realizar cálculos numéricos y tareas de contabilidad.
  - ◆ PowerPoint: Un programa de presentaciones ampliamente utilizado por profesionales, profesores y estudiantes
- **Open Office:** es una alternativa gratuita a Microsoft Office. Es un grupo de software de código fuente abierto fácil de usar, apto para principiantes absolutos. Incluye procesamiento de textos, hoja de cálculo, presentación, y aplicaciones gráficas, así como bases de datos y más. Está disponible en muchos idiomas y funciona en diferentes sistemas operativos. Almacena todos sus datos en un formato estándar internacional abierto y también puede leer y escribir archivos de otros paquetes de software de oficina común. Puede ser descargado y utilizado en forma totalmente gratuita para cualquier propósito.

## Software de Matemáticas

- **Microsoft Math (Windows):** Math es la utilidad de Microsoft dedicada a estudiantes ideal para asimilar conceptos de matemática mientras que la practican a su propio ritmo. La aplicación brinda, de manera muy accesible, material sobre álgebra, trigonométrica y cálculo, pero a su vez también incluye física y química. Microsoft Math incorpora diversas herramientas para facilitar el entendimiento de los estudiantes mientras aprehenden conceptos y profundizan en la materia. Encontraremos una avanzada calculadora para gráficos y capacidad de resolución de ecuaciones; un centenar de ecuaciones simples para partir desde lo básico; y una utilidad para convertir entre unidades de medición.

## Lectura de archivos PDF y eBooks

- **Foxit Reader (Windows):** Es una aplicación desarrollada por la compañía Foxit Software y que permite acceder al contenido de cualquier archivo PDF, soportando inclusive aquellos que requieren contraseña para abrirlos. El programa es notoriamente más rápido y estable que la aplicación de Adobe además de que incluye algunas otras herramientas complementarias. Este programa es capaz de integrarse con el navegador Web Firefox (mediante un addon incluido en su instalación) para que se pueda abrir documentos PDF directamente desde el navegador web sin la necesidad de descargarlo antes a la PC. Se trata de una aplicación de software muy liviana, toda vez que su instalación apenas supera los 10 mega-bytes y casi no consume recursos del equipo y la memoria RAM.
- **KPDF (Linux):** Es un lector libre de PDF; integrado en el entorno de escritorio KDE y basado en Xpdf. Sus principales características son: -Vista lateral en miniaturas del documento. -Modo presentación. -Posibilidad de controlar qué cantidad de memoria asigna el programa, para poder usar más o menos RAM disponible en el ordenador. -Tres maneras diferentes de buscar: a través del diálogo de búsqueda, a través de un filtro de búsqueda sobre las miniaturas de la imagen y una búsqueda mientras se teclea. -Selección de una manera sencilla de imágenes y texto creando un rectángulo que contenga la información que se quiera capturar. -Capacidad para añadir marcadores en las páginas.
- **FBReader (Windows):** Es un lector de libros electrónicos, es compatible con varios formatos: fb2, html, chm, rtf, plucker, etc. También admite la lectura directa desde archivos zip, tar, gzip y bzip2.

## Software para dibujar

- **Paint (Windows):** Microsoft Paint es una aplicación para procesar archivos bitmap de Windows. Microsoft Paint (o sencillamente Paint) es un pequeño pero muy útil programa de manipulación y creación de imágenes.
- **KolourPaint (Linux):** Es un editor de imagen para KDE, es de distribución gratuita. Su objetivo es ser fácil de entender y de usar, además, proporcionar un nivel de

funcionalidad orientada hacia el usuario medio. Es un excelente reemplazo o sustituto para MSPaint, sin embargo KolourPaint posee características más avanzadas. Asimismo, KolourPaint puede ejecutarse en otros entornos aparte de KDE, tales como Xfce y GNOME, además también funciona sobre algunos manejadores de ventanas como Fluxbox y Blackbox.

## Compresión/Descompresión de archivos

- **Izarc (Windows):** IZArc es un compresor y descompresor de archivos, gratuito y multilinguaje para Windows, que nos permitirá comprimir y descomprimir archivos de múltiples formatos, 7Zip, ace, arj, rar, tar, zip, etc., además de poder manipular imágenes de disco bin, cdi, img, iso, nrg, etc., y encriptar y reparar archivos, entre otras.
- **Konqueror (Linux):** Konqueror es compresor de archivos y carpetas, y además funciona como navegador web, administrador de archivos y visor de archivos. Forma parte oficial del proyecto KDE. Es software libre y de código abierto, y al igual que el resto de los componentes de KDE, está liberado bajo la licencia GPL. Konqueror soporta también la navegación por directorios locales, ya sea mediante la introducción de la ruta en la barra de direcciones o mediante la selección de iconos en los paneles.

## Fotos y realizar grabaciones con la cámara

- **Webcam Companion (Windows):** Este programa ofrece una amplia gama de aplicaciones diseñadas y optimizadas para la utilización de la Webcam. Permite capturar fotos, grabar videos, aplicar efectos o editar archivos capturados.
- **Cheese (Linux):** Es un programa open source que te permite hacer capturas de fotos y videos desde la Webcam. Además se puede aplicar una serie de efectos.

## Antivirus

- **Microsoft Security Essentials (Windows):** Proporciona protección en tiempo real contra virus, spyware y otros tipos de software malintencionado para tu PC doméstico. Microsoft Security Essentials se descarga de manera gratuita del sitio de Microsoft, es simple de instalar y usar y se mantiene siempre actualizado para que tengas la seguridad de tener tu PC siempre protegido con la tecnología más reciente. Es fácil saber si tu PC es seguro: cuando el color indicado es verde, está protegido. Es así de simple. Microsoft Security Essentials se ejecuta de forma silenciosa y eficiente en segundo plano con lo que puede utilizar con total libertad su equipo basado en Windows como desee, sin interrupciones ni largos tiempos de espera.
- **Rxart Antivirus (Linux):** Proporciona protección en tiempo real contra virus, spyware y otros tipos de software malintencionados, utiliza una herramienta de detección de virus confiable y estable, la cual es muy utilizada en la gran mayoría de los servidores de Internet (ClamAV).

## Software adicional de colaboración

- **Windows Live (Windows):** Permite acceder a redes sociales, chequear correos, compartir fotos y chatear. Windows Live da la posibilidad de tener todas las comunicaciones online juntas. Messenger, Hotmail y mucho más todo en un único sitio. Incluye:
  - ◆ Messenger: Para comunicarse de forma instantánea mediante texto, audio o incluso vídeo.
  - ◆ Hotmail: Correo electrónico, al que se puede acceder desde cualquier sitio.
  - ◆ Mail: Todas las cuentas de correo electrónico desde un único sitio.
  - ◆ SkyDrive: 25 GB para almacenar y compartir en línea archivos y documentos, protegidos mediante contraseña.
  - ◆ Galería Fotográfica: Organiza, edita y comparte fotos.
  - ◆ Grupos: Permite contactar y trabajar con compañeros de equipo, club, familiares y otros grupos de la vida real a través de Internet.
  - ◆ Calendario: Organiza agenda y permite compartirla.
  - ◆ Writer: Organiza, agrega y publica fotos y vídeos en blog personales.
  - ◆ Movie Maker: Crea y comparte películas a partir de fotos o vídeos.
  - ◆ Spaces: Comparte pensamientos a través de blogs personales.

## Sistema de Inventario y Actualización remota

- **Cliente de Sistema de Inventario y Actualización remota (Windows y Linux):** Es una herramienta que recopila información sobre el hardware y software de equipos remotos y permite instalar aplicaciones o actualizaciones remotamente, tanto en Windows como Linux, mediante un esquema distribuido.

## Generación de imágenes para Back-up

- **USB Generation Tool (Windows):** Es una herramienta dentro del sistema operativo que le permitirá crear un sistema de respaldo y restauración en un dispositivo de almacenamiento USB. Con este dispositivo podrá respaldar toda la información de su disco y recuperarla mas adelante en caso de necesitarlo. Permite respaldar el disco completo incluyendo tanto particiones Windows como Linux.
- **My Storage (Windows):** Permite que los estudiantes realicen fácilmente copias de seguridad y restauración de datos, monitorear el uso de espacio en disco y realizar una limpieza de disco.

## Prevención y control de accesos a sitios de Internet y políticas de seguridad

- **Parents Carefree (Windows):** El Parents Carefree es un soft destinado para el uso de los padres. Mediante este soft el padre puede disponer que cantidad de horas el estudiante podrá usar la Exomate por día o bien dentro de que rango horario la podrá utilizar, por ejemplo de 18 a 20hs. Además también el padre puede restringir a que páginas o aplicaciones se puede tener acceso, si puede tener acceso a una red o a Internet o bien puede revisar el historial de que programas y a que paginas accedió el estudiante.
- **Safe Life (Linux):** Permite establecer limitaciones a la hora de navegar evitando que los alumnos ingresen a sitios restringidos o aptos para mayores de edad.

### Nota:

- En general, antes de que una Exomate se envíe a los usuarios finales, la mayoría del software destinado para los estudiantes es previamente instalado en la computadora. Si determinada aplicación no está instalada, por favor remítase a los apéndices para más información. Lo mismo se aplica a la computadora portátil del profesor.

## **Parte II.**

# **Servidor de Seguridad - Manual de Referencia del Administrador**





## 4. Sistema de Seguridad

Se provee un Sistema de Seguridad que inhabilitará el dispositivo en caso de desvincularse con la red de servicio a la cual se encuentra referenciado. Dicho sistema tiene un componente de hardware (TPM versión 1.2, administración confiable de seguridad en redes) en el equipo y un componente de software que se provee con el equipo. Para su funcionamiento el alumno necesita conectarse con un servidor de seguridad que debe ser configurado para dicho fin, el cual puede estar localizado en cada colegio o en forma centralizada.

El componente de hardware del sistema de seguridad de cada equipo (TPM) crea y almacena de forma permanente e inalterable un Hardware ID (HWID) que permite identificar de manera única cada sistema.

Cuando se integra un equipo al sistema de seguridad, se configura de modo que le solicite certificados digitales al servidor que hemos configurado, que habilitarán al equipo a ser utilizado hasta la fecha de expiración del certificado (o una cantidad determinada de arranques).

La validez de los certificados es configurable desde el servidor de seguridad. Cuando dicho certificado está próximo a su vencimiento, la Exomate intentará comunicarse nuevamente con el servidor de seguridad, solicitándole un nuevo certificado con una nueva fecha de vencimiento posterior a la actual. En el caso en que el servidor emita un nuevo certificado para el equipo, estará habilitado para utilizarse hasta la nueva fecha de vencimiento, cerca de la cual volverá a consultar al servidor para repetir el proceso.

En los casos donde la Exomate no se comunique con el servidor, o cuando se comunique, pero el servidor no expida un certificado (por ejemplo, porque el equipo se ha reportado como robado), la Exomate se bloqueará automáticamente dejándola completamente inutilizada. Durante este bloqueo el usuario de la Exomate no podrá acceder ni siquiera al BIOS del equipo, ni mucho menos a arrancar el sistema operativo ni ninguna otra función del equipo, la única pantalla que verá será una pantalla indicándole que el equipo se ha bloqueado por seguridad y que la única manera de desbloquearlo provisoriamente es mediante un código de 10 dígitos que es válido solo para ese bloqueo particular de esa Exomate en particular, y puede obtenerse únicamente desde el servidor de seguridad.

El administrador del servidor de seguridad posee una herramienta de interfaz Web que sirve de control y administración de los equipos y le permite definir una lista negra de bloqueo de los equipos deseados.

La lista es obtenida a través de una comunicación segura con el Servidor de Seguridad, definido para el equipo, el cual puede estar alojado en la escuela o en forma centralizada y remota a través de Internet.

El protocolo para la autorización del uso de un equipo se basa en un sistema conocido como “certificado de arranque”. La lógica detrás del certificado es sencilla: el administrador define

el número de arranques y fecha final de uso del equipo. Cuando el equipo esté próximo a cumplir una de las dos condiciones deberá de actualizar su certificado con el servidor pues de no ser así el equipo será inhabilitado para su uso en base a la tecnología TPM.

La lógica del Sistema de Seguridad se puede resumir de la siguiente manera:

- El bloqueo de una Exomate depende de su certificado de arranque. Si su número de arranques no ha llegado a cero y si aun no ha llegado su fecha de caducidad, el mismo esta vigente y el equipo seguirá funcionando, de lo contrario será bloqueado físicamente.
- El equipo a través de una conexión con el Servidor de Seguridad puede pedir, recibir y actualizar su certificado cuantas veces sea necesario, siempre y cuando no se encuentre en la lista negra, obteniendo así un nuevo número de arranques y/o una nueva fecha de caducidad.
- Si el equipo está en la lista negra y el Servidor lo detecta en línea, le mandará un certificado caduco el cual forzará a que la siguiente vez que se encienda el equipo, este se bloquee.
- Si el equipo está en la lista negra y nunca más se conecta a la red entonces su certificado de arranque vencerá tarde o temprano pues su número de arranques llegara a cero o llegará la fecha de caducidad establecida por el administrador.

El Sistema de Seguridad no depende del no acceso u ocultamiento ya que está basado en una solución de software y hardware siendo precisamente el hardware (TPM) su principal sostén. El software simplemente sirve como medio de comunicación con el Servidor de Seguridad para actualizar su certificado de arranque por lo que si el software es modificado para saltar la seguridad se obtiene un efecto contrario ya que se garantiza el bloqueo inminente de la Exomate. Incluso cambiando el disco rígido el equipo se bloquearía.

## 5. Esquema de implementación sugerido

Dada la criticidad del servicio prestado por el servidor de seguridad, se recomienda que el servidor se encuentre un lugar apropiadamente resguardado. Se recomienda una estructura de red centralizada donde el servidor entregue los certificados para todos los equipos a través de Internet u otra red que comunique o integre a todos los colegios, y mantenga relación con los equipos del mismo modo.

Las bases de datos y configuraciones del Servidor de Seguridad deben ser backupearadas regularmente para asegurar la disponibilidad del sistema ante una eventual caída del servicio. Dichos backups deben ser resguardados adecuadamente ya que son una posible vía de autorización de uso de Exomates en estado “robado” ante la eventual duplicación no autorizada del servidor. Ante cualquier falla total del equipo, el sistema puede volver a ponerse en marcha si contamos con el backup correspondiente sin detrimento de ninguno de los equipos involucrados con el servidor.

Las tareas administrativas del servidor pueden ser realizadas remotamente y se detallan en el instructivo paso a paso que se encuentra mas adelante en este documento.



# 6. Servidor de Seguridad

## 6.1. Participantes

La interfaz del Servidor de Seguridad Intel para equipos Exomate funciona como una herramienta de administración tanto para el operador como para el administrador del servidor. La interfaz del servidor es usada principalmente para administrar equipos Exomate basados en Tecnología Intel. Existen tres usuarios para la interfaz: operadores, administradores y alumnos.

1. **El Operador:** El operador es una cuenta de usuario estándar. Un operador tiene la autoridad de gestionar el servidor, pero no puede realizar todas las operaciones de un administrador. Entre las tareas permitidas para este tipo de usuario están:
  - Mantener cuentas del servidor, incluyendo Agregar, Borrar, Modificar y Consultar.
  - Generar el “Código de Desbloqueo” del certificado al recibir una solicitud.
  - Actualizar el periodo de uso legal de los equipos Exomate conectados a este servidor.
  - Mantener la información de rastreo de dispositivos, como Ver, Borrar y Exportar el Registro de Rastreo para los equipos Exomate basados en Tecnología Intel conectados a este servidor.
2. **El Administrador:** El administrador es una cuenta de súper usuario. Un administrador tiene autoridad total sobre el sistema del servidor. El administrador puede gestionar al operador y el registro del servidor. Un administrador puede realizar las siguientes operaciones:
  - Mantener cuentas de servidor, incluyendo Agregar, Borrar, Modificar y Consultar.
  - Actualizar el periodo de uso legal de los equipos Exomate conectados a este servidor.
  - Generar el formato de “Código de Desbloqueo” del certificado al recibir una solicitud.
  - Mantener cuentas de operador, incluyendo Agregar, Borrar, Modificar y Consultar.
  - Mantener la información de rastreo de dispositivos, como Ver, Borrar y Exportar el Registro de Rastreo para los equipos Exomate basados en Tecnología Intel conectados a este servidor.
  - Mantener la información del registro, como Ver, Borrar, Exportar y Buscar.
3. **El Alumno:** El alumno es una cuenta estándar. Los alumnos pueden configurar sus contraseñas, pedir códigos de desbloqueo y establecer información de perfil.



**Nota:** El equipo Exomate es llamado 'dispositivo' o 'equipo' a lo largo de esta sección.

## 6.2. Gestión de Acceso

Esta sección está dedicada a administradores y operadores.

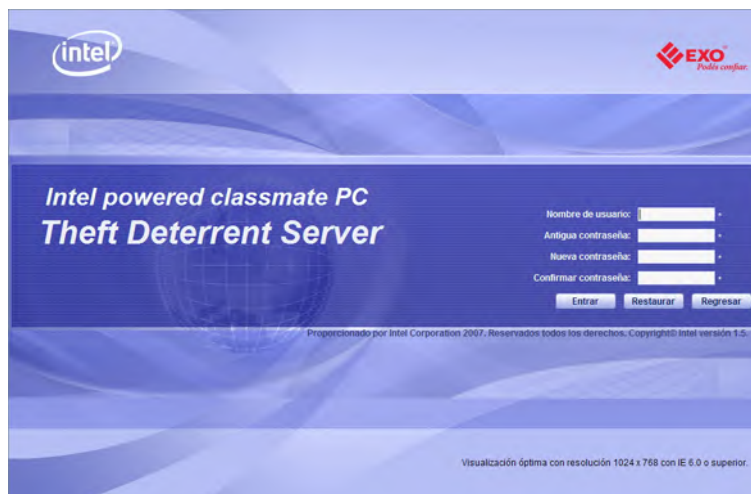
### 6.2.1. Accediendo

Por razones de seguridad, el usuario debe acceder inicialmente mediante un nombre de usuario y una contraseña. Si se trata del primer acceso del administrador, se utiliza la contraseña por defecto y deberá ser cambiada inmediatamente por seguridad.



### 6.2.2. Cambiar Contraseña

Después de acceder, la contraseña del administrador deberá ser cambiada inmediatamente por seguridad.



Para cambiar su contraseña - Introduzca su nombre de usuario, contraseña vieja, contraseña nueva, y confirme la contraseña nueva. **Restablecer**: Limpia todos los campos en la ventana de Cambio de Contraseña. **Regresar**: Lo lleva de regreso a la ventana de Acceso. **Introducir**: Haga clic en este botón una vez que haya introducido la información correcta.

### 6.2.3. Administración de Operaciones

Una vez que el administrador accede, la siguiente pantalla aparecerá.

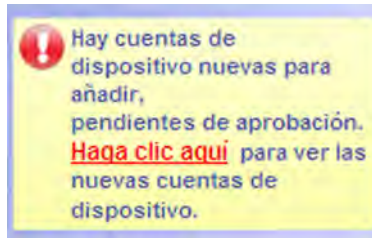


### 6.2.4. Cuenta Temporal de Dispositivo

Cuando un nuevo dispositivo se agrega al servidor, un link a la lista temporal de dispositivos se despliega en la pantalla de Bienvenida.



También hay un link a la lista temporal de dispositivos que se despliega cada vez que exista una cuenta temporal de dispositivo. Se localiza en la parte inferior de la columna de selección de tareas, en la parte izquierda de la interfaz, independientemente de la ventana desplegada en ese momento.



Para acceder a la lista temporal de dispositivos, use el link “**Haga clic aquí**”. La ventana de la lista temporal de dispositivos se desplegará.



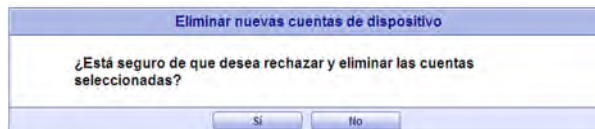
Esta ventana le provee las siguientes funciones:	
<b>Buscar:</b> Le permite buscar registros. Si deja los textos en blanco, todos los registros aparecerán.	
Si se encuentran registros, los botones <b>Aprobar</b> y <b>Rechazar</b> se activarán al tildarlos.	
<b>Aprobar dispositivos:</b> Para aprobar un registro de dispositivo, seleccione el dispositivo que desee aprobar haciendo clic en su recuadro (check) correspondiente y después en Aprobar. Un diálogo de confirmación aparece. <b>Si:</b> los registros seleccionados se aprueban ya no aparecerán en búsquedas posteriores. <b>No:</b> los registros no se aprueban.	



**Rechazar dispositivos:** Para rechazar un registro de dispositivo, seleccione el dispositivo que desee rechazar haciendo clic en su recuadro (check) correspondiente y después en Rechazar. Un diálogo de confirmación aparece.

**Si:** los registros seleccionados se rechazan y ya no aparecerán en búsquedas posteriores.

**No:** los registros no se rechazan.



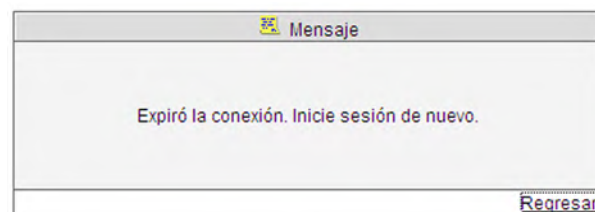
### 6.2.5. Administración de Dispositivos

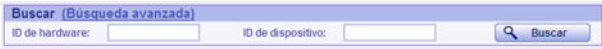



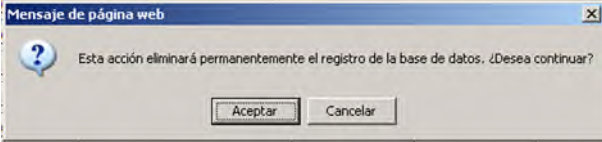

Para abrir la ventana de Administración de Dispositivos, haga clic en Administración de Dispositivos en la columna de selección de tareas del lado izquierdo.



Use esta ventana para agregar y modificar la información de la cuenta o declararla robada.

Si el tiempo de espera de la interfaz del servidor termina, aparecerá el siguiente mensaje y tendrá que acceder de nuevo.



<p><b>Buscar:</b> Le permite buscar registros. Si deja los textos en blanco, todos los registros aparecerán.</p>	
<p>También puede usar la función de <b>Búsqueda Avanzada</b> para reducir el número de resultados.</p>	
<p>Si se encuentran registros, los botones, <b>Agregar</b> y <b>Borrar</b> serán activados.</p>	
<p><b>Agregar un dispositivo:</b> Haga clic en el botón Agregar para agregar un dispositivo al servidor. La ventana Agregar Nuevo Dispositivo aparecerá. Introduzca la información necesaria y haga clic en el botón <b>Agregar</b>.</p>	
<p><b>Borrar un dispositivo:</b> Le permite borrar uno o más registros encontrados en la base de datos. Una ventana de diálogo aparecerá pidiéndole confirmación.</p>	
<p><b>Editar:</b> Para editar la información de un dispositivo, haga clic en el link del ID de Hardware que corresponde al dispositivo que desea editar. La ventana de diálogo Editar Dispositivo aparece. La ventana de diálogo Editar Dispositivo le permite editar información acerca del nombre de alumno, el ID del dispositivo, y el estado de robo. Tildando la opción <b>Si</b> en la sección <b>Estado robado</b> declarará al dispositivo como robado y no podrá recibir mas certificados hasta que usted no cambie esta opción a <b>No</b>. Ya editada la información del dispositivo, haga clic en <b>Guardar</b>. La nueva información será almacenada en la base de datos. Para cerrar la ventana de diálogo, haga clic en <b>Cancelar</b>.</p>	

## 6.2.6. Administración de Provisión

De la columna izquierda de la ventana de Administración de Operaciones, haga clic en **Administración de Provisión**. La ventana de Administración del Paquete de Suministro aparece.



La ventana provee las siguientes funciones:

### Certificado de Arranque Común

Para abrir la ventana de gestión del Certificado de Arranque Común, haga clic en la pestaña **Certificado de Arranque Común**. Introduzca los **Ajustes del Certificado de Arranque** y haga clic en **Guardar**.

**Nota:**

- Los "Días" deben ser mayores que 14, y menores que 1000.
- Las "Veces/Día" deben ser menores que 1000 y mayores que 0.
- El "Número total de arranques" equivale al producto de "Veces/Día", por el valor de "Días". El "Número total de arranques" debe ser mayor que 99, y menor que 65,000.



## Certificado de Arranque Único

Haga clic en la pestaña de **Certificado de Arranque Único** para abrir la ventana de gestión del Certificado de Arranque Único.



El Certificado de Arranque Único puede ser implementado en dos casos:

1. Un alumno pide vacaciones largas y no puede recuperar los Certificados de Arranque Común en los tiempos adecuados.
2. Un alumno se gradúa y se lleva el dispositivo consigo, por lo que desea obtener un Certificado de Arranque Permanente.

Para crear Certificados de Arranque Únicos: seleccione el dispositivo y haga clic en **Crear** para desplegar la ventana de diálogo del Certificado de Arranque Único. Introduzca datos en uno o más espacios y haga clic en **Guardar**.

Para designar al certificado como Permanente, haga clic en el recuadro **Permanente** y después haga clic en **Guardar**. Para convertir el Certificado de un Arranque a Certificado Común, haga clic en **Quitar**.

**Nota:**

- El "Número de Arranques" debe ser menor que 1000, y mayor que 0.
- La fecha de expiración debe ser introducida en el formato: "MM-DD-AAAA". El año debe ser entre 2000 y 2098.

## 6.2.7. Recuperación de Código de Desbloqueo

El código de desbloqueo es un tipo de certificado de arranque en la forma de un número de 10 dígitos para desbloquear el dispositivo Exomate cuando el certificado de arranque oficial ha caducado. Para abrir la ventana de Generación de Código de Desbloqueo, haga clic en **Recuperación de Código de Desbloqueo** de la columna izquierda de la ventana de Gestión de PC.



Busque dispositivos y elija el deseado. Haga clic en **Generar Código de Desbloqueo**.

Introduzca un valor en el cuadro de texto Arranque. Sólo acepta números y tiene una longitud máxima de seis dígitos. Este valor debe ser provisto por el cliente.

Tenga en cuenta que una vez introducido el código de desbloqueo, el equipo tendrá un certificado provisorio por 10 arranques o 2 días, dentro de ese período el equipo debe conectarse a la red del servidor para descargar el certificado común, de otro modo volverá a bloquearse.

## 6.2.8. Seguimiento de Dispositivos

De la columna izquierda de la ventana de Administración del Sistema, haga clic en **Seguimiento de Dispositivos**. La ventana de Seguimiento de Dispositivos aparece.



La ventana de Seguimiento de Dispositivos le permite borrar y exportar información de seguimiento de Dispositivos.

**Exportar un registro:** Para exportar un registro de la ventana de Seguimiento de Dispositivos, haga clic en **Exportar**. La ventana Exportar aparecerá y toda la información de rastreo correspondiente al “ID de Hardware” seleccionado será exportada.

Si el archivo es exportado con éxito, un link al archivo XML aparecerá junto al siguiente mensaje:

**Los registros del dispositivo se han exportado correctamente. Haga clic con el botón secundario en el vínculo siguiente para guardar la exportación del archivo.**

[Haga clic con el botón secundario para guardar el archivo.](#)

Haga clic derecho en el link para guardar el archivo XML a una ubicación específica. Para ver el resultado de la operación, haga clic izquierdo en el link. Los resultados típicos se muestran en la siguiente figura.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <TRACKING_INFO COUNT="5">
  <TRACKING device_hw_id="002185F3E006" dns_ip="200.80.206.11;200.80.206.12"
    gateway_ip="192.168.0.1" network_ip="192.168.0.106" owner_local_time="27-01-
    2010 17:18:22" reg_time="27-01-2010 17:18:14" stolen_flag="0"
    student_name="123456" tracking_id="8" wins_ip="" />
  <TRACKING device_hw_id="002185F3E006" dns_ip="200.80.206.11;200.80.206.12"
    gateway_ip="192.168.0.1" network_ip="192.168.0.106" owner_local_time="27-01-
    2010 17:08:18" reg_time="27-01-2010 17:08:13" stolen_flag="0"
    student_name="123456" tracking_id="7" wins_ip="" />
  <TRACKING device_hw_id="002185F3E006" dns_ip="200.80.206.11;200.80.206.12"
    gateway_ip="192.168.0.1" network_ip="192.168.0.106" owner_local_time="27-01-
    2010 16:58:18" reg_time="27-01-2010 16:58:14" stolen_flag="0"
    student_name="123456" tracking_id="6" wins_ip="" />
  <TRACKING device_hw_id="002185F3E006" dns_ip="200.80.206.11;200.80.206.12"
    gateway_ip="192.168.0.1" network_ip="192.168.0.106" owner_local_time="27-01-
    2010 16:48:18" reg_time="27-01-2010 16:48:13" stolen_flag="0"
    student_name="123456" tracking_id="10" wins_ip="" />
  <TRACKING device_hw_id="002185F3E006" dns_ip="200.80.206.11;200.80.206.12"
    gateway_ip="192.168.0.1" network_ip="192.168.0.106" owner_local_time="27-01-
    2010 16:38:18" reg_time="27-01-2010 16:38:12" stolen_flag="0"
    student_name="123456" tracking_id="9" wins_ip="" />
</TRACKING_INFO>
```

## 6.3. Administración del Sistema

### 6.3.1. Administración de Operadores

Cuando accede con una cuenta de administrador, usted obtiene derechos de administrador. Puede ver la ventana de Administración de Operadores al acceder al sistema.

De la columna izquierda de la ventana de Administración del Sistema, haga clic en **Administración de Operadores**. Aparecerá la ventana de Administración de Operadores que le permite buscar, agregar y editar cuentas de operador.



### 6.3.2. Administración de Alumnos



De la columna izquierda de la ventana de Administración del Sistema, haga clic en **Administración de Alumnos**. La ventana de Administración de Alumnos aparece.

La ventana de Administración de Alumnos le permite buscar, borrar y editar cuentas de alumnos.

### 6.3.3. Administración de Registro

Este módulo registra, principalmente, las operaciones detalladas del servidor, incluyendo el tiempo de operación, el nombre del operador, y otra información. Permite el mantenimiento y la autenticación de la base de datos del servidor.



Cuando accede con una cuenta de administrador, usted obtiene derechos de administrador. Puede ver la página de Administración de Registro, así como buscar, borrar, ver y exportar registros.

La ventana de Administración de Registro le permite buscar, borrar y exportar registros.

### 6.3.4. Administración de Datos

De la columna izquierda de la ventana de Administración del Sistema, haga clic en **Administración de Datos** para desplegar la ventana de Administración de Datos.

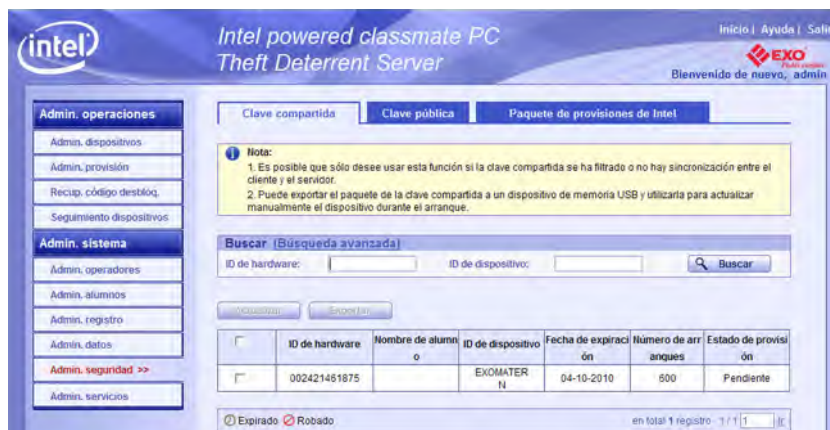


La ventana de Administración de Datos le permite importar, exportar y borrar registros.



### 6.3.5. Administración de Seguridad

De la columna izquierda de la ventana de Administración del Sistema, haga clic en **Administración de Seguridad**. La ventana de Administración de Seguridad aparece:



Esta ventana contiene las pestañas para la Clave Compartida, la Clave Pública y el Paquete de Suministro Intel. En esta página usted puede buscar y actualizar registros.

#### Clave compartida

**Búsqueda** La función Buscar aparece en la mitad superior de la ventana Administración de seguridad. Para consultar los registros, especifique la información de cuenta que desea buscar en los cuadros de texto y haga clic en **Buscar**. Si se especifica una información que no es válida, aparece un mensaje que indica esta circunstancia. Si deja los cuadros de texto en blanco, aparecen todos los registros. La siguiente figura muestra la sección Buscar de la ventana Administración de seguridad.



**Búsqueda avanzada** Haga clic en **Búsqueda avanzada**. Aparece el cuadro de diálogo Búsqueda avanzada.

- El cuadro de texto ID de hardware sólo puede aceptar números o letras de "a" a "f" y de "A" a "F".
- Los cuadros ID de dispositivo y Nombre de alumno aceptan todos los caracteres excepto "%", "\", "<", ">", "'", "''".
- Los cuadros ID de hardware, Nombre de alumno e ID de dispositivo admiten una búsqueda parcial. La relación de cálculo de los campos es AND.
- El formato para el cuadro de texto Fecha de expiración es "DD-MM-AAAA". El año debe estar entre 2000 y 2098.

- El campo del menú Estado de provisión permite elegir el tipo de estado que desea buscar. Se pueden buscar dos tipos: Normal y Pendiente. Déjelo en blanco para ver todos los tipos de estado.

La función Búsqueda avanzada es la misma que Buscar. Para borrar los datos de todos los campos de la ventana Búsqueda avanzada, haga clic en **Restaurar**. Para volver a la ventana de Inicio de sesión, haga clic en **Cancelar**.

**Actualización de la clave compartida** Para actualizar la clave compartida, marque la casilla de selección para las cuentas que desee actualizar. A continuación, haga clic en **Actualizar**.

ID de hardware	Nombre de alumno	ID de dispositivo	Fecha de expiración	Cantidad de arreglos	Estado de provisión
0630D5EF6741	student1	56	12-03-2008	800	Pendiente
20830D7299BE	student2	cmpc-aan	12-03-2008	800	Pendiente
00030D7299BE	student2	cmpc-21	12-03-2008	800	Pendiente
3232011EEDMF	student3	cmpc-18	12-03-2008	800	Pendiente
005DE8654CAA	student4		12-03-2008	800	Pendiente
1630D5EF6741	student5	12	12-03-2008	800	Pendiente

Si la actualización se completa correctamente, aparecerá la siguiente ventana.

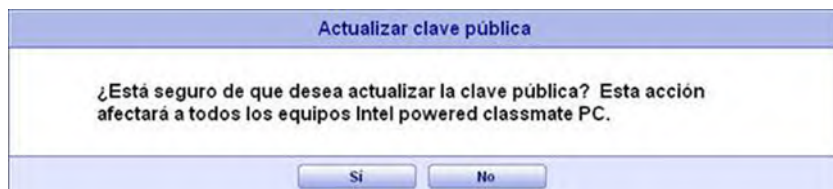
**Exportación de clave compartida** Para exportar la clave compartida, seleccione las cuentas que desee exportar. A continuación, haga clic en **Exportar**. Guarde el archivo y asígnele el nombre tcopp.bin.

## Clave Pública

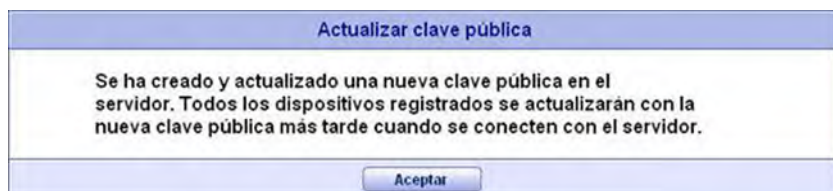
Haga clic en la ficha **Clave pública** para abrir la ventana de administración de la clave pública.



**Actualización de clave pública** Para actualizar la clave pública, haga clic en **Actualizar**. Aparece un mensaje de confirmación.



Haga clic en **Sí** para actualizar la clave pública. Si la actualización se completa correctamente, aparecerá la siguiente ventana.



**Exportación de clave pública** Haga clic en **Exportar** para exportar la clave pública. Aparecerá la siguiente ventana.

El archivo de clave pública se ha exportado correctamente. Haga clic con el botón secundario en el vínculo siguiente para guardar la exportación del archivo.

Haga clic con el botón secundario para guardar.

Haga clic con el botón derecho en el vínculo para guardar el archivo en una ubicación específica. El archivo recibe el nombre tcopp.bin.

## Paquete de provisiones de Intel

Haga clic en la ficha **Paquete de provisiones de Intel** para abrir la ventana del paquete de provisiones de Intel.



Seleccione el hiper-vínculo **Haga clic aquí**. Aparecerá el siguiente mensaje.

Procedimientos detallados
1. Instale el software Theft Deterrent Server.
2. Exporte la nueva clave pública de servidor.
3. Obtenga el número de provisión de cualquier equipo Intel powered classmate PC siguiendo uno de estos pasos: a) Obténgalo de la pantalla de entrada del código de desbloqueo si Intel powered classmate PC está bloqueado. b) Obténgalo del perfil de Theft Deterrent Agent si Intel powered classmate PC no está bloqueado.
4. Llame al distribuidor regional de Intel powered classmate PC para obtener los datos de contacto del centro de asistencia al cliente de Theft Deterrent.
5. Llame a un técnico de asistencia al cliente de Theft Deterrent e identifíquese para el servicio de recuperación.
6. Envíe por correo electrónico al técnico de asistencia el número de provisión y la nueva clave pública de servidor en un archivo adjunto.
7. Obtenga un mensaje de correo electrónico del técnico de asistencia al cliente con un paquete de provisiones de recuperación con la firma digital de Intel.
8. Para volver a configurar los equipos Intel powered classmate PC desbloqueados: a) Importe el paquete de provisiones en el nuevo Theft Deterrent Server, en el módulo de administración de seguridad. b) Conecte los equipos Intel powered classmate PC al servidor para su configuración automática.
9. Para volver a configurar los equipos Intel powered classmate PC bloqueados: a) Copie el paquete de provisiones en un dispositivo de memoria USB. b) Conecte la memoria USB a cada equipo Intel powered classmate PC bloqueado y enciéndalo. c) Presione las teclas de acceso rápido (Ctrl + Insertar) para iniciar el proceso de recuperación cuando aparezca la ventana que solicita el código de desbloqueo. d) Reinicie el equipo.
10. Listo.
<input type="button" value="Cerrar"/>

Seleccione el archivo de paquete de provisiones de Intel que desee importar.



A continuación, haga clic en **Importar** para importar el archivo. Si la importación se realiza correctamente, aparece la siguiente ventana.



Si no hay ningún registro en la base de datos, se producirá un error en la información del resultado.

### 6.3.6. Administración de Servicios

De la columna izquierda de la ventana de Administración del Sistema, haga clic en **Administración de Servicios** para desplegar la ventana de Administración de Servicios.



Seleccione **Encendido** o **Apagado** para encender o apagar el proceso de control de transmisión del servidor y después haga clic en **Guardar** para guardar su selección.

## 6.4. Alumno

Las cuentas de alumno en el servidor son muy limitadas en cuestión de las acciones que pueden realizar. Las únicas acciones que se permite realizar a los alumnos son actualizar su información de cuenta (nombre, fecha de nacimiento y contraseña) y pedir un Código de Desbloqueo para una Exomate que ha sido bloqueada.

### 6.4.1. Acceso

La siguiente figura muestra la página de acceso inicial para un alumno cuya contraseña no se ha establecido.



Una vez que la cuenta del alumno ha sido activada con éxito, la siguiente imagen se despliega. También, la pantalla de acceso que se muestra es la pantalla de acceso típica para cuentas de alumno activadas (es decir, cuya contraseña ha sido establecida).



### 6.4.2. Configuración del Perfil

Después de un acceso exitoso, la siguiente ventana aparece. Para cambiar el nombre del alumno, fecha de nacimiento o contraseña, introduzca la nueva información y haga clic en **Guardar**. Para limpiar todos los campos, haga clic en **Restablecer**.

The screenshot shows the 'Configuración de perfil' section of the user interface. On the left, there is a sidebar with 'Mi cuenta' and two links: 'Configuración de perfil >>' (highlighted) and 'Recup. código desbloq.'. The main content area is titled 'Configuración de perfil' and contains the following fields:

- Información personal:**
  - Nombre de alumno: [input field]
  - Fecha de nacimiento: [DD-MM-AAAA input field]
- Cambiar contraseña:** (Deje el campo en blanco si no desea cambiar la contraseña)
  - Antigua contraseña: [input field]
  - Nueva contraseña: [input field]
  - Confirmar contraseña: [input field]

At the bottom of the form are two buttons: 'Guardar' and 'Restaurar'. The Intel logo and 'EXO Podés confiar.' are visible in the footer.

### 6.4.3. Recuperación de Código de Desbloqueo

Para generar un Código de Desbloqueo, haga clic en **Recuperación de Código de Desbloqueo** en la columna izquierda de la ventana.

The screenshot shows the 'Recup. código desbloq.' section of the user interface. On the left, the sidebar has 'Recup. código desbloq. >>' highlighted. The main content area is titled 'Recup. código desbloq.' and contains the following fields:

- ID de hardware: 002421461875
- Marca de arranque: [input field] \* (Puede obtenerlo en la pantalla del equipo Intel powered classmate PC bloqueado)

At the bottom of the form is a button: 'Generar código de desbloqueo'. The Intel logo and 'EXO Podés confiar.' are visible in the footer.

En la pantalla de la Exomate bloqueada encontrará la marca de arranque en formato hexadecimal como medida adicional de seguridad, pasarlo a decimal e introducirlo en el casillero del Server. Después, haga click en **Generar Código de Desbloqueo**. Aparecerá el siguiente mensaje con el código de desbloqueo:

<b>El código de desbloqueo es</b>
<b>5607267132</b>
<input type="button" value="Aceptar"/>



## 6.5. Autoridad de Usuario

Las tareas a nivel de sistema que están disponibles para los tres tipos de usuarios del servidor se describen en la siguiente tabla.

Autoridad de Nivel de Usuario	Especificación	
Operador	Administración de Operaciones	
	Administración de Sistema	Administración de Alumnos
		Administración de Datos
Administrador	Administración de Operaciones (igual que el Operador)	
	Administración de Sistema	Administración de Operadores
		Administración de Alumnos
		Administración de Registro
		Administración de Datos
Alumno	Configuración de Perfil	
	Recuperación de Código de Desbloqueo	

## 6.6. Salir

Para salir de la interfaz de usuario del servidor, haga clic en **Salir** en la esquina superior derecha de la interfaz. Cuando usted hace clic en **Salir**, la ventana de Acceso inferior es desplegada.



## 6.7. Sistema de Ayuda en Línea

Para ejecutar el sistema de ayuda en línea del software del servidor, haga clic en **Ayuda** en la esquina superior derecha de la interfaz. El sistema de ayuda es sensible al contexto, lo que significa que la ayuda se despliega para la página específica desde la cual se invocó la ayuda.



## 6.8. Recuperación de Desastre

Sólo un administrador puede realizar operaciones de recuperación de desastre.

### 6.8.1. Operaciones de Recuperación de Desastre

Condición de Desastre	Solución
El Servidor de Seguridad Intel para Exomate se ha colapsado.	Si el Par de Claves del servidor necesita ser actualizado debido a un colapso en el sistema, actualice la Clave Pública del Servidor, y todas las Exomate basadas en Tecnología Intel la obtendrán automáticamente. Vea la sección Clave Pública bajo Administración de Seguridad para instrucciones detalladas.

Condición de Desastre	Solución
La Exomate está bloqueada y la Clave Compartida no coincide.	<p>Si la Exomate está bloqueada y la Clave Compartida no coincide con el de la base de datos del servidor, siga los pasos descritos a continuación:</p> <ol style="list-style-type: none"> <li>1. Actualice la Clave Compartida usando los procedimientos en la Sección Actualizando la Clave Compartida bajo Administración de Seguridad.</li> <li>2. Genere un Código de Desbloqueo para introducirlo cuando la Exomate arranque. Vea la sección Recuperación de Código de Desbloqueo para los pasos.</li> </ol> <p>Para importar la Clave Compartida fuera de línea, siga estos pasos:</p> <ol style="list-style-type: none"> <li>1. Exporte la Clave Compartida a un disco USB. Para hacerlo, inserte un disco USB y seleccione la cuenta. Haga clic en Exportar. Haga clic derecho en el link y guarde el archivo exportado al disco USB.</li> <li>2. Inserte el disco USB en el puerto USB de la Exomate y presione <b>Ctrl + Insert</b> para acceder en Modo de Recuperación de Desastre.</li> </ol>

Condición de Desastre	Solución
La Exomate está bloqueada, la Clave Compartida no coincide y el Par de Claves del servidor se ha perdido.	<p>Si la Exomate está bloqueada, la Clave Compartida no coincide, y al mismo tiempo el Par de Claves del servidor se ha perdido, siga los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. Actualice la Clave Pública del Servidor. Vea la sección Clave Pública bajo Administración de Seguridad para instrucciones detalladas.</li> <li>2. Exporte la Clave Compartida a un disco USB. Para hacerlo, inserte un disco USB y seleccione la cuenta. Haga clic en Exportar. Haga clic derecho en el link y guarde el archivo exportado al disco USB.</li> <li>3. Inserte el disco USB en el puerto USB de la Exomate y presione <b>Ctrl + Insert</b> para acceder en Modo de Recuperación de Desastre.</li> </ol>

Condición de Desastre	Solución
El Servidor de Seguridad Intel para Exomate se ha colapsado.	<p>Si la Clave Privada original del servidor se ha perdido, y no puede generar el Paquete de Suministro de la Clave Pública:</p> <ol style="list-style-type: none"> <li>1. Configure un nuevo servidor.</li> <li>2. Envíe la clave Pública a Soporte a Clientes de EXO, junto con el número especial generado por el Agente de Seguridad Intel para Exomate. Se generará un Paquete Firmado por Intel, y lo enviará al administrador del servidor.</li> <li>3. En el servidor, importe el Paquete Firmado por Intel. Vea la sección Paquete de Suministro Intel bajo Administración de Seguridad.</li> </ol> <p>Una vez que importe el Paquete de Suministro Intel, todas las Exomates bloqueadas obtendrán el paquete a través de la red de forma automática. Si algún dispositivo permanece bloqueado, importe el Paquete de Suministro Intel a esa PC mediante estos pasos:</p> <ol style="list-style-type: none"> <li>1. En el servidor, copie el Paquete de Suministro Intel a un disco USB.</li> <li>2. Inserte el disco USB en el puerto USB de la Exomate y presione <b>Ctrl + Insert</b> para acceder en Modo de Recuperación de Desastre.</li> </ol>

## 6.9. Preguntas Frecuentes

### 1. La respuesta del servidor es lenta. ¿Qué puedo hacer al respecto?

La razón más probable es que el desempeño de su base de datos se ha reducido. Si tiene un alto volumen de datos en ella, considere mejorar el hardware de su servidor.

### 2. No puedo acceder con éxito. El proceso de acceso se detiene en la página login\_deal.jsp, y la página de mensaje no muestra nada. ¿Qué debo hacer?

Revise la configuración de seguridad en Internet Explorer para asegurarse que JavaScript esté habilitado.

### 3. Puedo acceder con éxito, pero el botón Importar está deshabilitado (en gris). ¿Qué debo hacer?

Asegúrese que está accediendo al servidor. La función importar sólo está disponible en el servidor.

### 4. ¿Por qué no puedo exportar con éxito?

Abra Inicio -> Programas -> Apache Tomcat 5.0 -> ConTomcat y haga clic en la pestaña de Inicio y Apagado. Revise la Ruta de Trabajo para asegurar que la ruta se ha establecido.

### 5. Puedo acceder con éxito, pero no encuentro la Administración de Operadores. ¿Por qué?

Asegúrese que está accediendo como un administrador. La función de Administración de Operadores sólo está disponible para usuarios con privilegios de administrador.

### 6. El tiempo de respuesta es lento. ¿Qué puedo hacer al respecto?

Intente configurando el programa Tomcat. Abra Inicio -> Programas -> Apache Tomcat 5.0 -> Con Tomcat y haga clic en la pestaña Java. Configure el banco de memoria Inicial a 400 y el banco de memoria Máximo a 512.

### 7. Accedo al sistema como administrador, y me pide cambiar mi contraseña, ¿cuál es el criterio que debo seguir al elegir una contraseña?

En Internet Explorer, asegúrese que JavaScript está habilitado.

Un nombre de usuario no puede exceder los 30 caracteres y puede incluir sólo los

siguientes: caracteres del alfabeto (A-Z, a-z), números (0-9), y “\_” (guión bajo).

Una contraseña debe incluir por lo menos un caracter alfabético en minúsculas (a-z), un caracter alfabético en mayúsculas (A-Z), y un caracter especial (\$#%@,.).

Una contraseña no puede incluir caracteres introducidos usando Alt+128 hasta Alt+255.

#### 8. **¿Por qué no puedo aprobar nuevas cuentas temporales?**

Sólo los administradores tienen la autoridad de aprobar nuevas cuentas temporales.

#### 9. **Estoy tratando de buscar por un ID de Hardware, no puedo encontrar el registro.**

La caja de texto para el ID de Hardware sólo acepta números o letras de la “a” a la “f”, y de la “A” a la “F”.

El campo del ID de Hardware soporta búsquedas difusas. La relación de cálculo de los campos es Y (como en, “esto Y aquello”).

#### 10. **Aparece un mensaje de error cuando trato de agregar un dispositivo al servidor.**

Asegúrese de seguir estos criterios:

El asterisco (\*) al lado de un campo indica que es un campo requerido.

La caja de texto para el ID de Hardware sólo acepta números o letras de la “a” a la “f”, y de la “A” a la “F”, y tiene una longitud máxima de 12 caracteres.

El ID del Dispositivo y el Nombre del Alumno pueden incluir todos los caracteres excepto “%”, “\”, “<”, “>”, “””, “””. La longitud total no puede exceder los 30 caracteres.

El cuadro de comentario no puede exceder los 150 caracteres.



## 7. Agente de Seguridad

El Agente de Seguridad Intel para Exomates corre en la Exomate del alumno y está específicamente diseñado con la seguridad del equipo en mente.

El Agente de Seguridad Intel para Exomates provee una simple interfaz de usuario para realizar las siguientes funciones:






- Cambiar opciones de conexión
- Desplegar el estado actual del certificado y de la información del dispositivo
- Revisar el certificado de autorización cada vez que la PC se inicia
- Recordar al propietario obtener un nuevo certificado de autorización si el certificado actual está por expirar o ya expiró

El propietario de la Exomate obtiene un certificado de autorización periódicamente lo verifica y determina por cuánto tiempo la Exomate puede ser usada.

Si una Exomate es robada, el Servidor de Seguridad Intel generará una petición especial de certificado de arranque único, con “hoy” como la Fecha de Expiración y “0” como el Conteo de Arranques (el Conteo de Arranques es el número de veces que el sistema puede iniciarse). Una vez que la Exomate reciba este certificado, se apagará y no permitirá nuevos reinicios. Esta función está diseñada para reducir el riesgo de robo de las Exomate PCs basadas en Tecnología Intel.

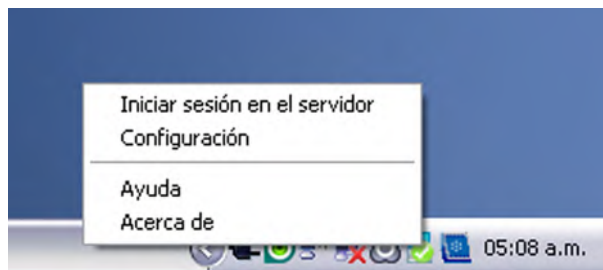
## 7.1. Ícono en la Barra del Sistema

El Agente de Seguridad para Exomates se inicia automáticamente cuando el sistema operativo inicia. El programa corre de forma minimizada, apareciendo como un ícono en la barra del sistema de Microsoft Windows y Linux. El color del ícono cambia para indicar el estado del agente. Un mensaje emergente se despliega cuando se mueve el ratón por encima del ícono.

Ícono	Estado	Descripción
	Normal	El mensaje emergente muestra "Normal".
	Advertencia	La PC tiene menos de X días o menos de cinco inicios antes de la fecha de expiración. El mensaje muestra "Advertencia" El Agente de Seguridad descargará un certificado de arranque común automáticamente.
	No activado	La cuenta en la PC no ha sido aprobada en el Servidor de Seguridad Intel® para Exomates. El mensaje emergente muestra "No activado".
	No se puede conectar con el servidor	La PC no se puede conectar al servidor. El mensaje emergente muestra "No se puede conectar con el servidor". Revise la conectividad de red para asegurar que la PC se pueda conectar al servidor.
	No se puede conectar con el servidor y no activado	La PC no se puede conectar al servidor y la cuenta no ha sido aprobada. El mensaje emergente muestra "No se puede conectar con el servidor".

## 7.2. Interfaz Gráfica de Usuario

Haga clic derecho en el ícono de la barra del sistema para desplegar un menú con las siguientes cuatro opciones: “**Acceder al servidor**”, “**Configuración**”, “**Ayuda**”, y “**Acerca de**”. Estas opciones de menú se describen a detalle en las siguientes secciones. Para ejecutar la interfaz de usuario gráfica (GUI) del Agente de Seguridad Intel para Exomates, haga doble clic en el ícono, o seleccione **Configuración**.





## 7.2.1. Configuración

1. El agente automáticamente detecta la dirección del servidor durante la instalación. Usted también puede introducir manualmente la dirección del Servidor de Prevención de Robo. Haga clic en **Aplicar** o en **OK** para guardar la información.

Intel powered classmate PC Theft Deterrent Agent

Información del servidor

Dirección de Theft Deterrent Server:

Dirección del servidor

Información del servidor proxy

Utilizar servidor proxy

Servidor proxy de Theft Deterrent:

Nombre de usuario de servidor proxy de Theft Deterrent:

Contraseña de servidor proxy de Theft Deterrent:

Aceptar Cancelar Aplicar

2. Si usted usa un servidor proxy, éste obtendrá la configuración automáticamente desde Internet Explorer. También puede introducir la dirección del servidor proxy manualmente. Una vez introducida, escriba el nombre de usuario y contraseña para el servidor proxy.. Haga clic en **Aplicar** o en **Aceptar** para guardar la información.

Intel powered classmate PC Theft Deterrent Agent

Información del servidor

Dirección de Theft Deterrent Server:

Dirección del servidor

Información del servidor proxy

Utilizar servidor proxy

Servidor proxy de Theft Deterrent: Dirección del Proxy

Nombre de usuario de servidor proxy de Theft Deterrent: USUARIO

Contraseña de servidor proxy de Theft Deterrent: \*\*\*\*\*

Aceptar Cancelar Aplicar

## 7.2.2. Acceder al Servidor

Siga estos pasos para acceder al servidor:

1. Este menú lleva a la página de acceso. La siguiente figura muestra la página de acceso inicial. Establezca su contraseña personal. Después de este acceso inicial, sólo se le pedirá la contraseña para acceder.

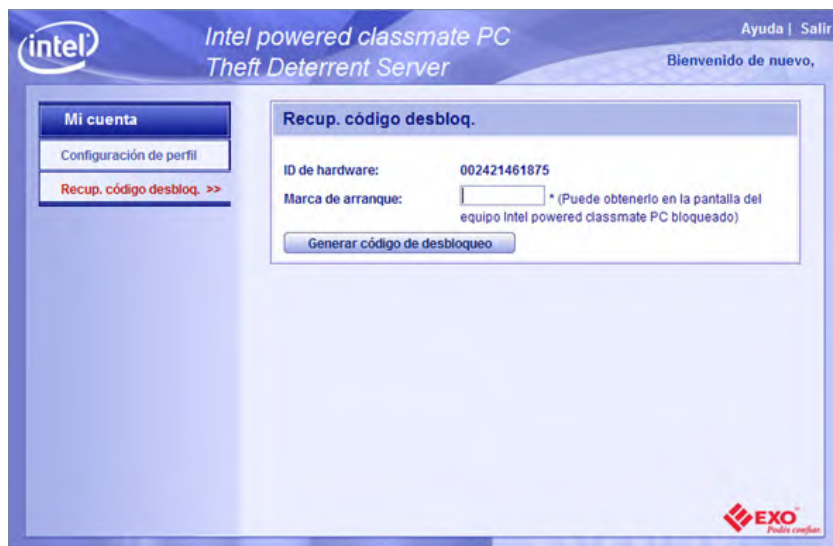
The screenshot shows the 'Activación de cuentas personales' (Personal account activation) page. It features the Intel logo and the text 'Intel powered classmate PC Theft Deterrent Server Para alumnos'. The main heading is 'Activación de cuentas personales'. Below this, there is a paragraph explaining that a personal account allows login to the student module and can be used to update the profile or recover the unlock code. The form includes four input fields: 'Nueva contraseña', 'Confirmar contraseña', 'Nombre de alumno', and 'Fecha de nacimiento' (with a DD-MM-AAAA format). There are 'Guardar' (Save) and 'Restaurar' (Restore) buttons at the bottom. A footer note states: 'Proporcionado por Intel Corporation 2007. Reservados todos los derechos. Copyright© Intel versión 1.5. /Visualización óptima con resolución 800 x 600 con IE 6.0 o superior.'

2. Después de un acceso exitoso, la siguiente ventana se despliega.

The screenshot shows the 'Configuración de perfil' (Profile configuration) page. It features the Intel logo and the text 'Intel powered classmate PC Theft Deterrent Server'. The page is titled 'Configuración de perfil' and includes a 'Bienvenido de nuevo,' (Welcome back,) message. On the left, there is a navigation menu with 'Mi cuenta' (My account) selected, and sub-options for 'Configuración de perfil >>' and 'Recup. código desbloq.'. The main content area is titled 'Configuración de perfil' and contains 'Información personal' (Personal information) with fields for 'Nombre de alumno' and 'Fecha de nacimiento' (DD-MM-AAAA). Below this is a section for 'Cambiar contraseña' (Change password), with a note '(Deje el campo en blanco si no desea cambiar la contraseña)'. It includes fields for 'Antigua contraseña', 'Nueva contraseña', and 'Confirmar contraseña'. There are 'Guardar' (Save) and 'Restaurar' (Restore) buttons at the bottom. The EXO logo is visible in the bottom right corner.

### 7.2.3. Recuperación de Código de Desbloqueo

Para generar un código de desbloqueo, haga clic en **Recuperación de Código de Desbloqueo** en la columna izquierda de la ventana.



Introduzca la marca de arranque, la cual se despliega en la pantalla de la Exomate bloqueada. Después, haga clic en **Generar Código de Desbloqueo**. El siguiente mensaje aparece:



### 7.2.4. Ayuda

Este menú despliega el sistema de ayuda en línea.

### 7.2.5. Acerca de

Este menú despliega la versión y la información de copyright para esta Exomate PC basada en Tecnología Intel.



### 7.3. Descarga Automática de un Nuevo Certificado

El Agente de Seguridad Intel para Exomates automáticamente descarga un nuevo certificado cuando la PC inicia, independientemente del estado del agente (**Normal**, **Advertencia**, **No Activado**, o **No se Puede Conectar con el Servidor**). Una vez que el sistema inicia, el agente intentará diez veces descargar un certificado. El Agente de Seguridad Intel para Exomates intenta descargar un nuevo certificado automáticamente cada 10 minutos una vez iniciada la PC.

**Nota:**

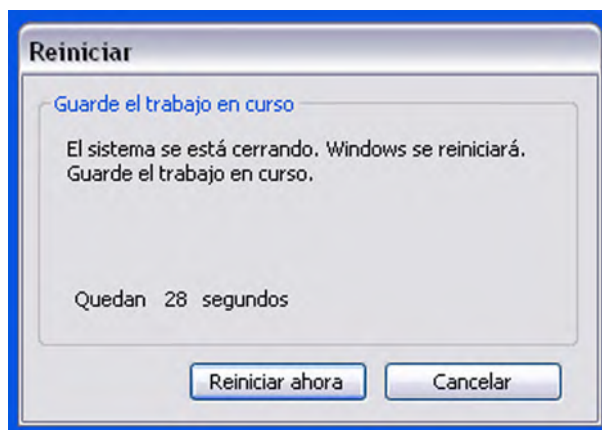
- Existe un intervalo de 10 segundos entre intentos de descarga. El agente deja de intentar después de la primera descarga exitosa.
- Si el estado del Agente de Seguridad para Exomates es “Advertencia”, el agente intentará descargar un Certificado de Arranque Común. Una vez que lo descarga con éxito, no descargará uno nuevo hasta la siguiente ocasión en la que el estado sea “Advertencia”.
- Si el Agente de Seguridad para Exomates recibe un certificado con éxito, y el certificado no es un Certificado de Arranque Común, no intentará descargar un nuevo certificado hasta la siguiente vez que el sistema sea iniciado.



Si el certificado es uno de los siguientes. . .

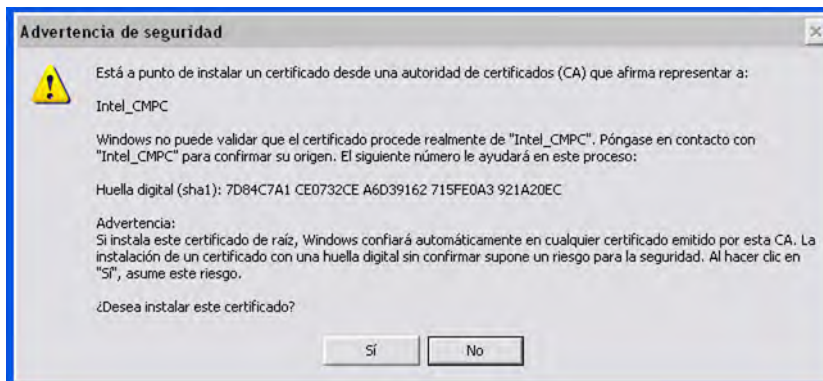
- Clave Compartida
- Certificado de Arranque Único
- Paquete de Suministro Automático
- Clave Pública del Servidor
- Clave Pública Intel

. . . el mensaje de la siguiente figura se despliega. Para reiniciar la PC de forma inmediata, haga clic en **Reiniciar ahora**. Si no desea reiniciar la PC en ese momento, haga clic en **Cancelar**.



Para instalar el certificado, haga clic en **Reiniciar ahora** para reiniciar la PC de inmediato.

Si el certificado recibido es un certificado de Autoridad de Certificación (CA por sus siglas en inglés), el siguiente mensaje se despliega. Haga clic en Si para instalar el certificado CA.



## 7.4. Introduciendo un Código de Desbloqueo

Si la fecha del sistema excede la fecha de expiración, o el contador de inicios es cero, el BIOS de TPM no dejará cargar el sistema operativo. Si el sistema no pasa el chequeo pre-arranque, el BIOS proveerá una oportunidad para que usted introduzca un Código de Desbloqueo, como se muestra a continuación. Para obtener el código de desbloqueo, deberá solicitárselo al administrador, indicando los datos que entrega el equipo en pantalla.

Si el Código de Desbloqueo es válido, el BIOS reservará dos días y 10 arranques para permitirle actualizar el Certificado de Arranque. Aún así, le recomendamos hacer esto inmediatamente. El BIOS entonces cargará el sistema operativo.

Si el código no es válido, el BIOS desplegará lo siguiente:

“Lo sentimos, el Código de Desbloqueo que ha introducido es incorrecto! Por favor inténtelo de nuevo.”

Si introduce un Código de Desbloqueo inválido tres veces, el BIOS desplegará el siguiente mensaje y apagará la PC:

“Lo sentimos, ha introducido el código incorrecto tres veces. El sistema se apagará inmediatamente.”

## 7.5. Usando un Disco USB para Obtener Certificados

Si la PC está bloqueada, usted puede desbloquearla al usar certificados en un disco USB, el cuál puede obtener de su Administrador. Inserte el disco USB en un puerto USB y presione la combinación especial de teclas Ctrl + Insert. El BIOS interpretará el certificado automáticamente.

## 7.6. Preguntas Frecuentes

1. **Si la dirección del servidor ha cambiado, ¿tengo que cambiar la dirección del servidor manualmente?**

No. El Agente de Seguridad Intel para Exomates puede recuperar la dirección del servidor automáticamente cuando detecta que la dirección no es correcta.

2. **¿Por qué el Agente de Seguridad para Exomates no provee un atajo de inicio y un método de apagado?**

Ya que es un programa de administración responsable del mantenimiento del estado del sistema, el Agente de Seguridad para Exomates debe permanecer en ejecución todo el tiempo. No debe ser apagado por los usuarios.

3. **Si el Agente de Seguridad para Exomates se apaga, ¿la función de prevención de robo sigue aplicando si la PC es robada?**

Si. Aún si el Agente de Seguridad para Exomates no está en ejecución, el BIOS seguirá sin cargar el sistema operativo después de la fecha de expiración. Además, la siguiente vez que la PC inicie, el Agente de Seguridad para Exomates se iniciará automáticamente.

4. **¿Puedo desinstalar el Agente de Seguridad para Exomates? ¿Si es así, que pasa si lo desinstalo?**

Al tratarse de un programa de administración, el Agente de Seguridad para Exomates debe permanecer en ejecución todo el tiempo. De cualquier manera, puede desinstalar el programa utilizando “Agregar o Quitar Programas” en el Panel de Control.

5. **¿Encenderá la Exomate, aún cuando sólo una de las condiciones de expiración se ha cumplido (por ejemplo, el número de arranques es válido todavía, pero la fecha es posterior a la fecha de expiración)?**

Cuando cualquiera de las dos condiciones de expiración (fecha o número de arranques) se cumple, la Exomate no iniciará.

6. **¿El estado “Advertencia” afecta las funciones de la PC (es decir, esta condición prevendrá que algunas funciones se realicen)?**

No. El estado Advertencia simplemente le informa al usuario que debe descargar un nuevo Certificado de Arranque para continuar con el uso normal.

### 7. ¿Qué es un Código de Desbloqueo?

El Código de Desbloqueo le permite usar la Exomate por dos días y un total de 10 inicios de sistema (hasta 2099/12/31), aún si no ha obtenido un nuevo Certificado de Arranque desde el servidor. Durante estos dos días, usted debe obtener un nuevo certificado al descargar uno del servidor configurado.

### 8. ¿Puede extenderse el tiempo utilizable de la PC al modificar la fecha y la hora del sistema?

Si. Cambiar la fecha y la hora del sistema puede extender el tiempo utilizable de la PC. Sin embargo, cambiar la fecha y la hora del sistema evitará que el Agente de Seguridad para Exomates descargue un nuevo Certificado de Arranque del Servidor de Seguridad para Exomates. Ya que el número de arranques antes de la expiración no se afecta por un cambio en la hora o en la fecha, el certificado eventualmente expirará cuando el número de inicios permitidos se ha alcanzado, independientemente de si la fecha de expiración llega.

## 7.7. Mensajes de Error

Si ocurre un error al descargar un certificado, la causa del error será registrada en el archivo agentlog.txt. El siguiente es un ejemplo de mensaje de error cuando el dispositivo Ethernet no inicializa correctamente: “Ha ocurrido un error al intentar conectar con el servidor.”

### 7.7.1. Error al Conectar con el Servidor

Valor	Significado (El error pudo haber sido resultado de las siguientes causas)
00	El punto de servicio remoto no pudo ser contactado en la capa de transporte - TCP
01	La conexión se cerró prematuramente.
02	La conexión por una petición que especifica el encabezado mantener-vivo se cerró de manera inesperada.
03	Un mensaje excede el límite especificado al enviar la petición o al recibir respuesta del servidor.
04	El nombre del destino no pudo ser resuelto por DNS.
05	Una petición asíncrona interna está pendiente.
06	La respuesta recibida del servidor estuvo completa pero indicó un error a nivel de protocolo. Por ejemplo, un error de protocolo HTTP como el 401 Acceso Denegado usaría este estado.
07	El nombre del proxy destino no pudo ser resuelto por DNS.
08	No se recibió una respuesta completa del servidor remoto.
09	La petición fue cancelada.
10	Ocurrió un error al establecer una conexión utilizando SSL.
11	No se pudo enviar una petición completa al servidor remoto.
12	La respuesta del servidor no fue una respuesta HTTP válida.
13	No se recibió respuesta durante el periodo de espera para una petición.
14	Excepción de formato URL.

### 7.7.2. Ocurrió una Excepción Desconocida

El siguiente es un ejemplo de mensaje de error cuando ocurre una excepción desconocida: “Ocurrió una excepción desconocida!”

Valor	Significado(El error pudo haber sido resultado de las siguientes causas)
00	Posesión ilegal de este dispositivo!
01	Una excepción de tipo desconocido ha ocurrido.
02	Ocurrió una excepción desconocida al fallar la descarga, pero el error no se definió.
03	Ocurrió una excepción desconocida al guardar el certificado.
04	Ocurrió una excepción desconocida!



## **Parte III.**

# **Servidor Escolar EXO - Manual de Referencia del Administrador**



## 8. Webmin

Siguiendo la línea de las aplicaciones que van apareciendo con el fin de facilitar las tareas complejas de administración, nos encontramos con una realmente útil: Webmin, una interfaz gráfica que, vía navegador web, nos ofrece la posibilidad de configurar cuentas del sistema, servicios (Apache, MySQL, PHP, DNS, . . .), y en general, administrar tanto máquinas locales, como remotas, pudiendo incluso administrar un cluster de máquinas. Esto hace que Webmin sea muy útil tanto para el administrador novato como para el experto, ya que ofrece una gran potencialidad asociando visión más “gráfica” del entorno de administración.

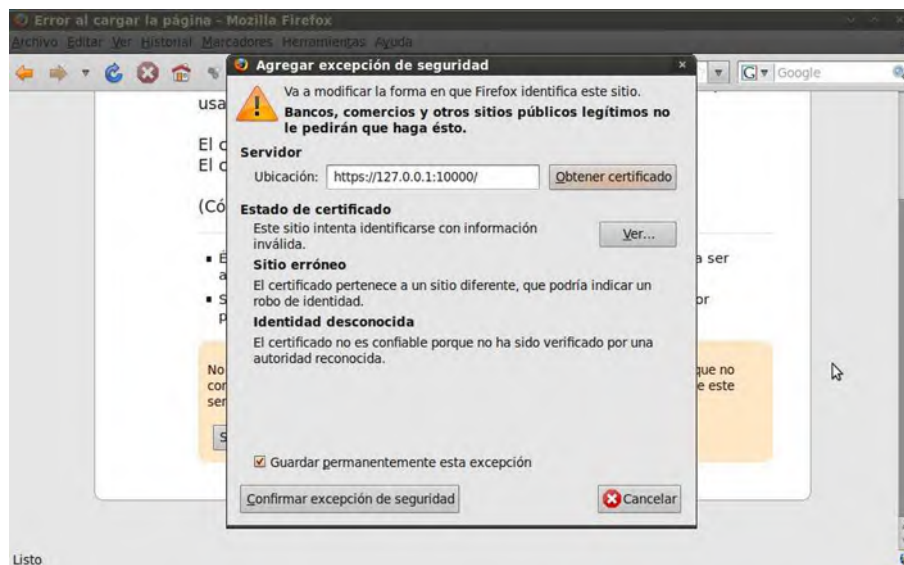
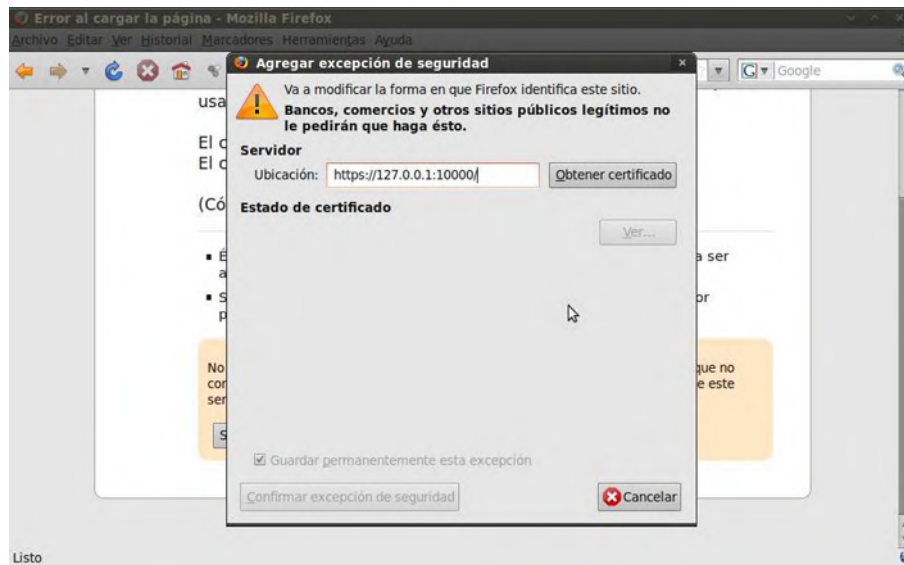
Ya encontrará Webmin instalado en su servidor escolar, no obstante, si se necesitara obtener una nueva descarga o información extra del sistema, puede hacerse desde <http://www.webmin.com>

### 8.1. Uso de Webmin

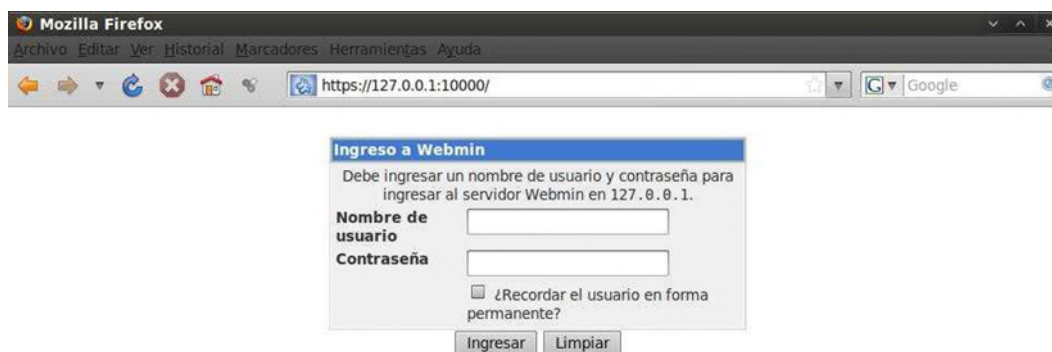
Para acceder a Webmin hay que loguearse en <https://127.0.0.1:10000> con una cuenta de superusuario.

Al ingresar por primera vez seguramente el navegador pedirá que autentiquemos el certificado de seguridad emitido por Webmin. En ese caso, simplemente con autenticarlo podremos acceder al menú de login.





Una vez autenticado, ya se nos presentará el login de forma correcta.



Al ingresar, nos encontraremos con una ventana informando brevemente sobre el sistema anfitrión como así también el menú general del sistema.



## 8.2. Reconocimiento del menú Webmin

### 8.2.1. Cambio de Idioma y Tema

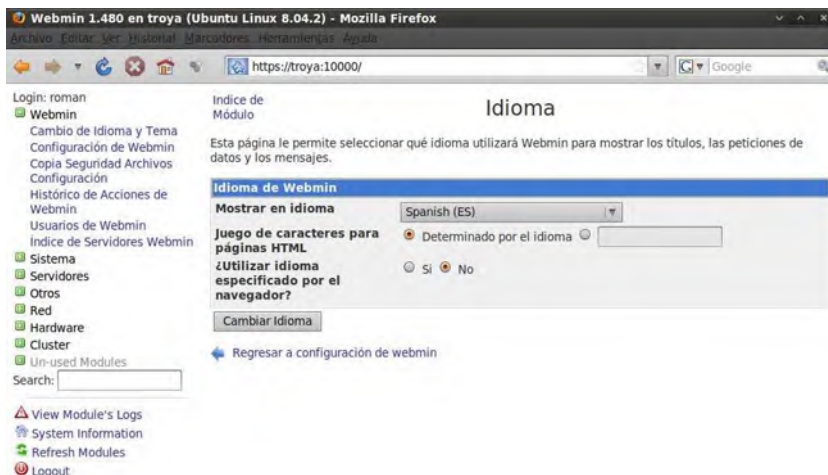


En primera instancia, Webmin aparecerá en idioma Inglés, así que una de las primeras cosas que deberemos hacer es cambiar el idioma a español. Aquí también tenemos la opción de cambiar el tema o skin del sistema, Webmin viene con 4 estilos distintos.

Normalmente, cuando cambiamos el tema de la UI, pueden presentarse algunos errores en el navegador, no es un tema de preocupación ya que haciendo un refresh del browser ya se podrá ver el sistema con su nuevo tema sin inconvenientes.

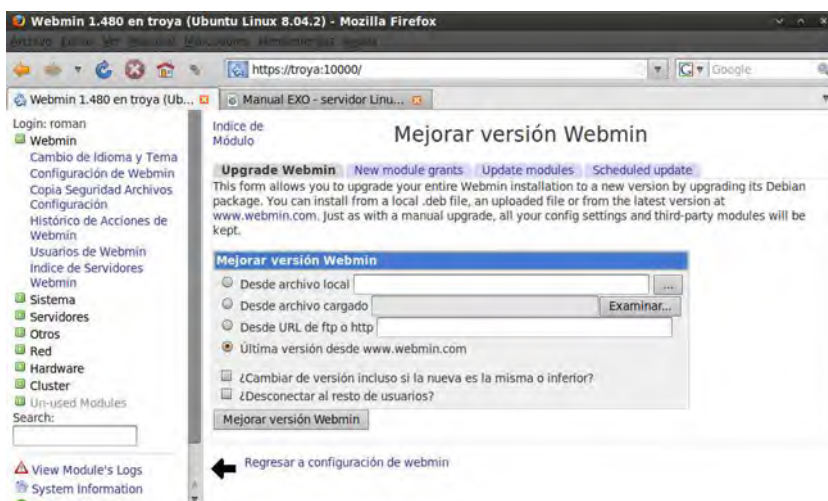
## 8.3. Configuración de Webmin

### 8.3.1. Idioma



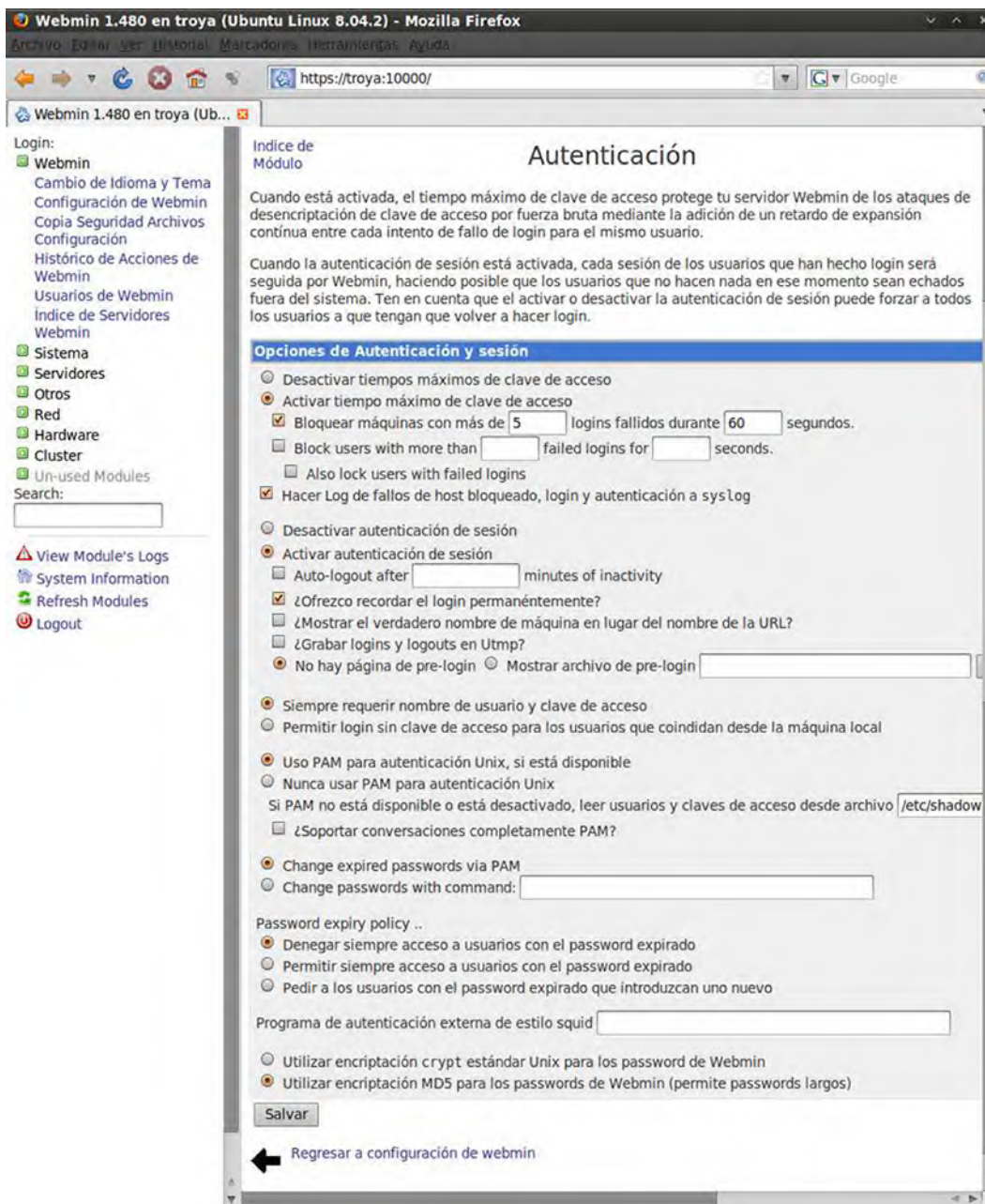
Si bien ya vimos desde dónde cambiar el idioma de la UI, deberemos cambiar esta opción también para que los mensajes desde el sistema también sean en un idioma determinado.

### 8.3.2. Mejorar versión Webmin



Desde aquí podremos hacer un upgrade del sistema en si, o de alguno de sus módulos. Ya sea habiendo descargado ya los archivos y actualizarlo en forma local, o bien haciendo que el mismo sistema se encargue de la descarga. Estos trabajos de actualización podremos hacerlos también como una tarea programada.

### 8.3.3. Autenticación



Webmin provee excelentes opciones para prevenir ataques al servidor ya sea por fuerza bruta o crackeo como así también provee protección para los “usuarios olvidadizos”.

Si su servidor Webmin es accesible desde muchos equipos esta opción es fundamental para mejorar la seguridad del sistema. Dependiendo de las cláusulas de seguridad que se necesiten usar, podrán usar algunas o todas las opciones disponibles en el módulo.

**Tiempos máximos de claves de acceso:** provee lo referente para prevenir ataques por fuerza bruta limitando la frecuencia de intentos de logeo por un determinado usuario y/o equipo ya sea desde una misma terminal o varias. Si está activado, Webmin bloqueará la



terminal y/o usuario que tenga un determinado número de intentos de acceso fallidos en un determinado tiempo. El tiempo a mantener bloqueado el equipo es configurable en segundos.

Todos estos eventos pueden almacenarse en el syslog y usualmente aparecerán en los detalles de secure y auth del directorio del syslog.

**Autenticación de sesión:** es la forma en que los usuarios puedan desloguearse después de un tiempo de inactividad especificado. Esto ayuda a la prevención de accesos por parte de usuarios no autorizados a través del uso de equipos que hayan tenido acceso. Esto no es una medida infalible ya que actualmente muchos navegadores tienen la opción de guardar las claves de acceso en los equipos, haciéndolos accesibles para cualquiera que acceda a ese equipo.

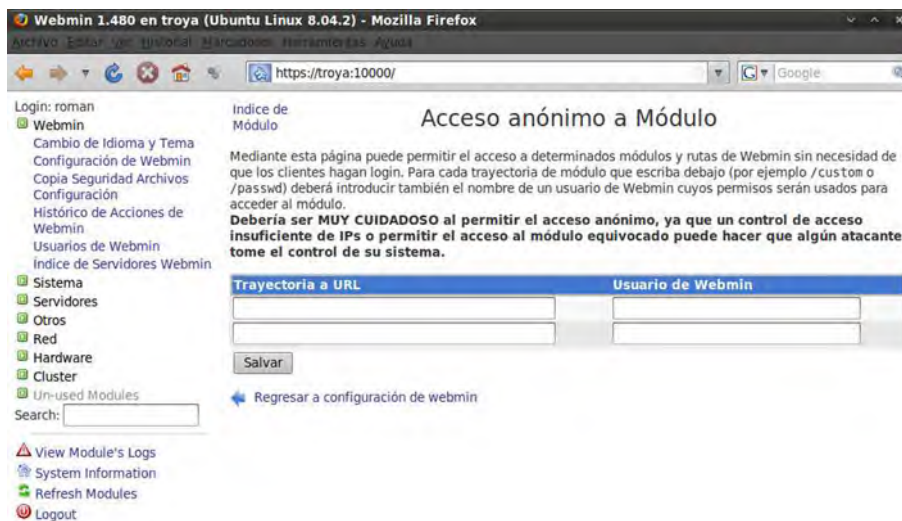
Podremos también ofrecer la opción de recordar el login en forma permanente, aunque todas estas políticas de acceso deberán ser tratadas basándose puntualmente en las necesidades de cada lugar. Hay que recordar que Webmin corre solamente con privilegios de superusuarios, esto hace que el que tenga acceso a Webmin pueda acceder a la administración global del sistema, por lo tanto, es importante analizar en profundidad quienes y desde dónde se podrá acceder al sistema.

### 8.3.4. Referenciadores de confianza



Debido a que Webmin es un sistema basado en web al cual se accede a través de un navegador, almacenando y reenviando información de autenticación desde y hacia el server, existe la posibilidad de que accesos desde otros sitios web intenten generar acciones maliciosas en el servidor donde tenemos Webmin. Esta sección ayuda a configurar los hosts que entraran en nuestra lista de confianza.

### 8.3.5. Acceso anónimo a Módulo

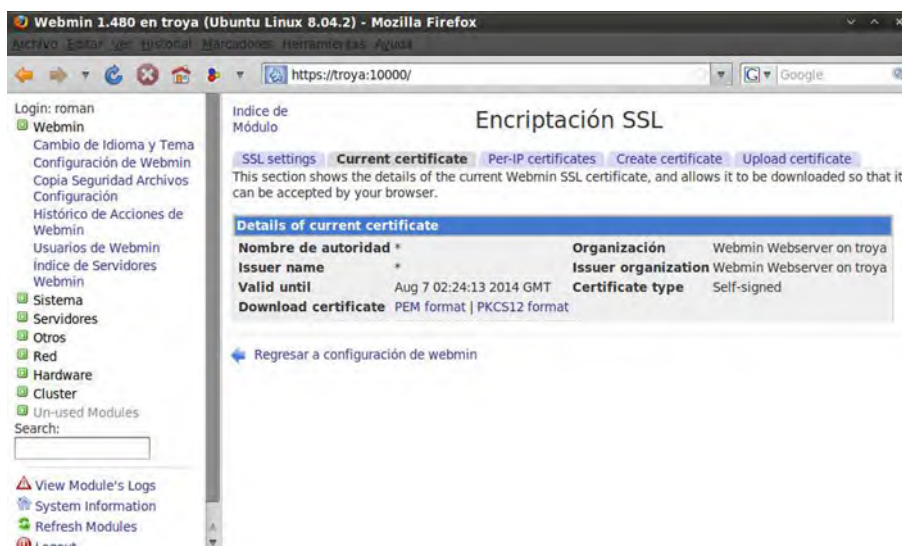


En algunas circunstancias puede ser de ayuda que algunos módulos de Webmin sean accesibles para todos los usuarios sin tener la necesidad de autenticarse el acceso. Por ejemplo, puede ser útil el permitir a visualización de las estadísticas del server, o permitir el montaje de algún dispositivo a través de algún comando. Es un módulo que debe usarse con precaución porque se podría exponer considerablemente la seguridad del sistema.

### 8.3.6. Encriptación SSL



El uso de conexiones con encriptación SSL incrementa la seguridad de su servidor. Dentro de la primer pestaña del menú podremos desactivar el modulo, como así también si queremos ingresar algún certificado en forma manual.



The screenshot shows the Webmin interface in a Mozilla Firefox browser window. The address bar displays `https://troya:10000/`. The page title is "Webmin 1.480 en troya (Ubuntu Linux 8.04.2) - Mozilla Firefox". The main content area is titled "Encriptación SSL" and shows the "Current certificate" details. The "Current certificate" section includes a table with the following information:

Details of current certificate		
Nombre de autoridad *	Organización	Webmin Webserver on troya
Issuer name	Issuer organization	Webmin Webserver on troya
Valid until	Certificate type	Self-signed

Below the table, there is a "Download certificate" link with options for "PEM format" and "PKCS12 format". A "Regresar a configuración de webmin" link is also present.

En la siguiente pestaña podremos ver la información referente al certificado actual del sistema. El cual es el mismo que tuvimos que validar para poder comenzar la primer sesión con Webmin.



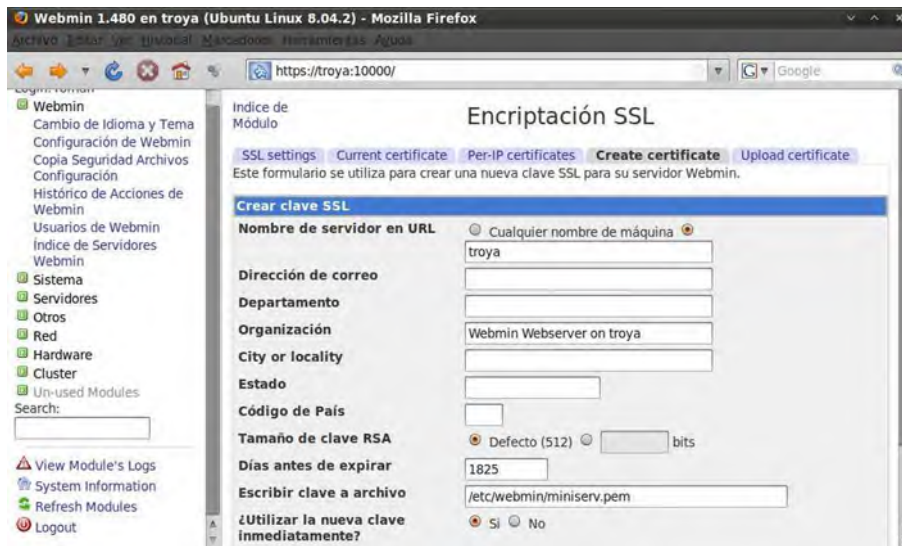
The screenshot shows the Webmin interface in a Mozilla Firefox browser window. The address bar displays `https://troya:10000/`. The page title is "Webmin 1.480 en troya (Ubuntu Linux 8.04.2) - Mozilla Firefox". The main content area is titled "Encriptación SSL" and shows the "Per-IP certificates" section. The "Per-IP certificates" section includes a message:

**No se ha definido aún ninguna clave SSL específica de IP.**

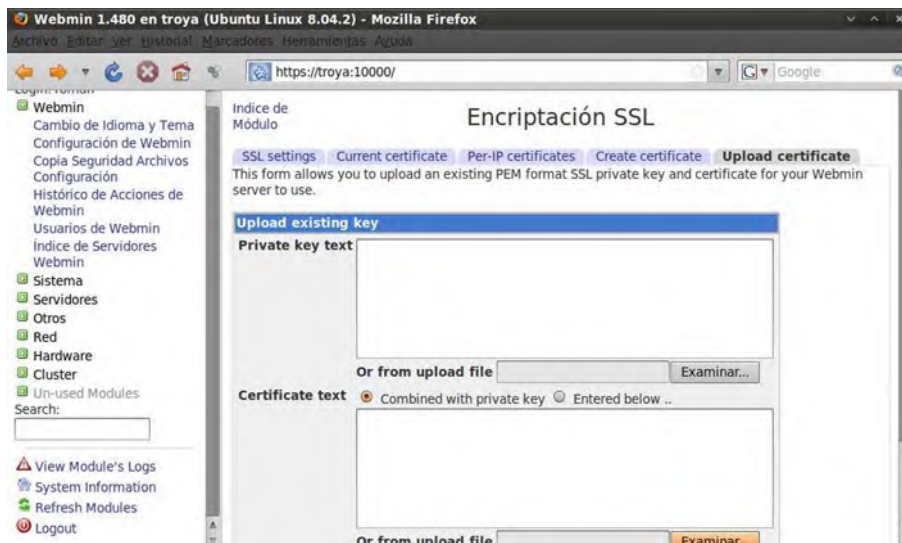
Añadir una nueva clave SSL específica de IP.

Below the message, there is a "Regresar a configuración de webmin" link.

Para el caso en que necesitemos utilizar distintos certificados para cada dirección IP en concreto deberemos dirigirnos a la pestaña "Per-IP Certificates".



En "Create Certificate" podremos crear nuestros propios certificados, permitiendo no solo introducir nueva información corporativa sino que tan bien el largo de clave, como así también la utilización en forma inmediata de la clave generada.



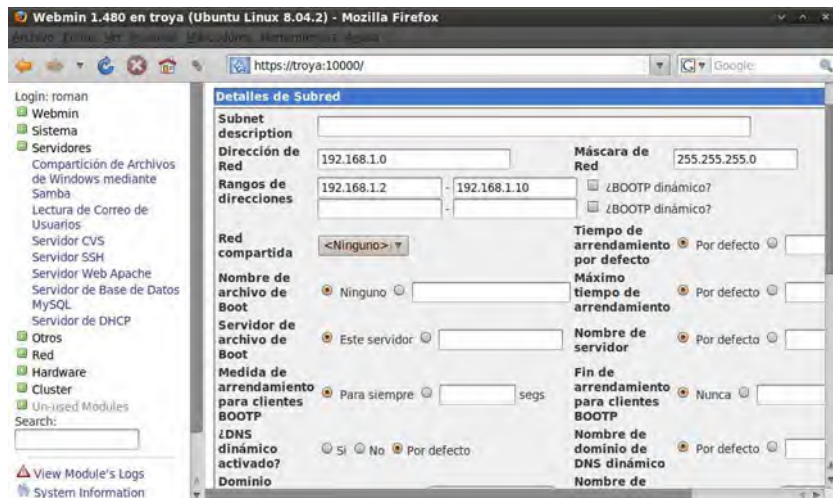
Pueden presentarse casos en los que se requiera autenticar con certificados de terceros o generados anteriormente desde otro equipo se deberá usar las opciones de la pestaña "Upload certificate".

## 9. Servidor DHCP



DHCP es un protocolo que nos permite asignar direcciones IP a los equipos que la requieran dentro de la LAN. Su servidor escolar viene equipado con 2 placas de red, las cuales una se utilizará para el acceso a la WAN y la segunda placa para la comunicación dentro de la LAN.

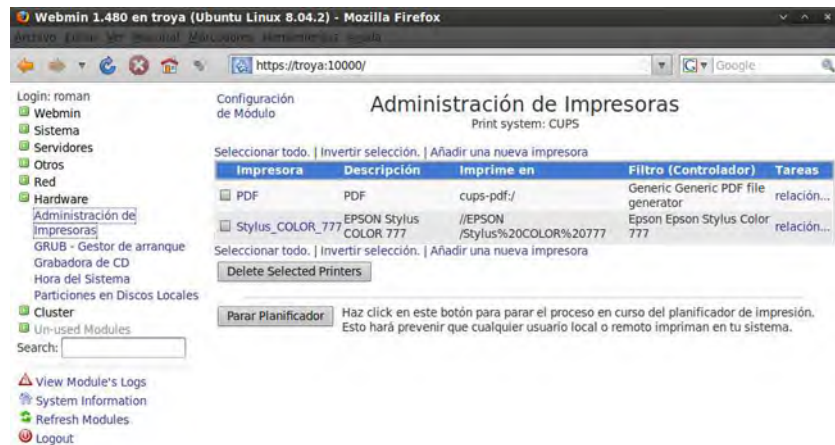
Para entrar en la configuración de la LAN, habrá que elegir el ícono correspondiente a la placa asignada para tal fin.



Una vez seleccionada la placa, accederemos a la configuración para asignar rangos de direcciones IP como así para establecer los rangos para las terminales que arranquen bajo BOOTP.

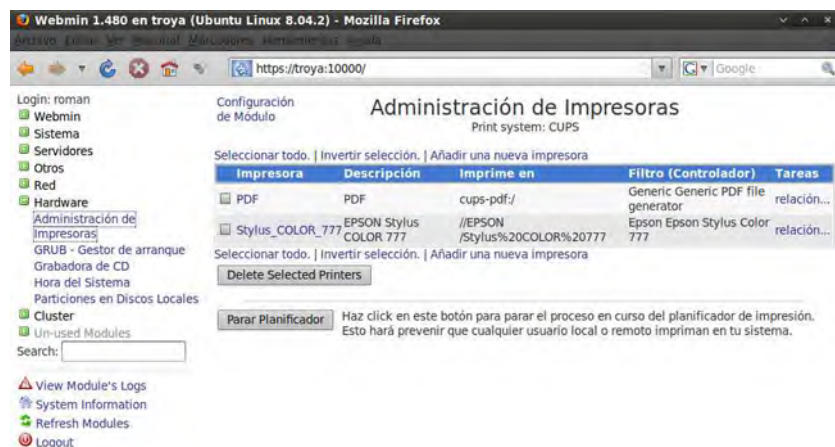


# 10. Administración de impresoras



Como otros SO, Linux puede imprimir tanto en impresoras conectadas al sistema como así también en impresoras conectadas en otro sistema de la red.

En el menú principal de Administración de Impresoras veremos las impresoras activas en el equipo, para acceder a la configuración directamente hay que seleccionar la impresora.



Desde aquí, se puede configurar cada impresora, estableciendo tanto que esté accesible desde los demás equipos como el driver a utilizar.

Desde el menú de administración eligiendo el área de tareas se puede ver si hay trabajos de impresión pendientes o en curso.





# 11. Servidor Web Apache

En esta sección les mostraremos que es y como se utiliza el servidor web Apache.

Para los que no lo conozcan, se trata del servidor web que más instalaciones tiene en toda Internet.

## Nota:

- Haremos toda la administración de nuestro/s sitio/s desde Webmin.
- Los archivos que Apache publicará (muestra hacia afuera) estarán en /var/www de nuestro equipo.

## 11.1. Acceder al módulo Apache de Webmin

Como ya hemos visto, para acceder a Webmin deberemos apuntar a la IP de nuestro servidor escolar y al puerto 10000 del mismo, desde un navegador. Es decir que en la barra de dirección puede verse algo así:

**https://localhost:10000** (accediendo desde el mismo servidor escolar)

**https://127.0.0.1:10000** (accediendo desde el mismo servidor escolar)

**https://172.16.0.1:10000** (accediendo desde cualquier máquina de la red LAN)

Cuando introducimos el usuario y contraseña del sistema (el mismo que tiene permisos de hacer sudo), nos encontramos en la ventana de inicio.

Allí desplegamos el grupo “Servidores” de la barra lateral y allí elegimos “Servidor Web Apache”, tal como vemos en la siguiente imagen:



Una vez que entramos al módulo de Apache, nos encontraremos con la siguiente pantalla:



Estas opciones se aplicarán a todos los sitios que tengamos activos en el sitio, ya sea solo uno o varios.

## 11.2. Opciones globales

### 11.2.1. Límites y Procesos

Este Módulo de MultiProcesamiento (MPM) de apache, implementa un servidor híbrido multiprocesomultihebra. Usando hebras para atender peticiones, el servidor puede servir un mayor número de peticiones con menos recursos de sistema que un servidor basado únicamente en procesos. No obstante, se mantiene casi por completo la estabilidad de un servidor basado en procesos manteniendo la capacidad multiproceso, pudiendo cada proceso tener muchas hebras.

Las directivas más importantes que se usan para controlar este MPM son `ThreadsPerChild`, que controla el número de hebras que tiene cada proceso hijo y `MaxClients`, que controla el número máximo de hebras que pueden crearse.

Para el caso de Webmin, debemos tener en cuenta que “hebras” es lo mismo que “requerimientos”.

Tenemos algunas opciones configuradas Por defecto. No nos meteremos con esas que son muy específicas de lograr optimizaciones del servidor y requieren mayor conocimiento de Apache.

**Máximo número de requerimientos por proceso de servidor:** Por defecto viene en 0 (cero), es decir que esta capacidad de multiprocesomultihebra está desactivada. Para el caso que queramos mejorar el rendimiento si nuestro apache empieza a tener mucho tráfico continuo, deberemos subir este número hasta notar una mejora sustancial.

**Máximo número de procesos libres del servidor:** Durante el funcionamiento del servidor, Apache calcula el número total de hebras en espera, entre todos los procesos, y crea o elimina procesos para mantener ese número por debajo de lo que especifiquemos acá.

**Mínimo número de procesos libres del servidor:** De igual manera a la directiva anterior, Apache calcula el número total de hebras en espera, entre todos los procesos, y crea o elimina procesos para mantener ese número por encima de lo que especifiquemos acá.

**Procesos iniciales del servidor:** Apache siempre intenta mantener en reserva cierto número de hebras de sobra o en espera, que están preparadas para servir peticiones en el momento en que lleguen. Así, los clientes no tienen que esperar a que se creen nuevas hebras o procesos para que sean atendidas sus peticiones. El número de procesos que se crean al principio está determinado por esta directiva.

## 11.2.2. Redes y direcciones

Indice de Módulo Aplicar Cambios  
Parar Apache

### Redes y Direcciones

**Redes y Direcciones**

**Escuchar en direcciones y puertos**

Dirección	Puerto
<input type="radio"/> Ninguno <input checked="" type="radio"/> Todos <input type="text"/>	80
<input checked="" type="radio"/> Ninguno <input type="radio"/> Todos <input type="text"/>	<input type="text"/>

**Direcciones para servidores virtuales de nombres**

Incluir todas las direcciones

**Requerimientos múltiples por conexión**  Ninguno  Por defecto

**Tiempo de espera para mantener vivos**  Por defecto

**Tiempo de espera para requerimientos**  Por defecto

**Tamaño de cola para escuchar**  Por defecto

**Tamaño de búfer de envío de TCP**  Por defecto de SO

Usaremos esta opción para configurar nuestro servidor para que escuche (ponga páginas web) en otros puertos. Esto es particularmente útil cuando necesitamos poner algunas páginas que no queremos que todo el mundo vea con solo escribir una dirección simple.

Así como dice que todos los dominios están en el puerto 80, podremos ir poniendo en otros puertos los demás.

## 11.2.3. Editar archivos de configuración

El resto de las opciones se irán volviendo más importantes cuando el administrador comience a conocer más los detalles de apache y sus configuraciones.

Para aprender más sobre el mismo, recomendamos mucho la información propia de Apache, que está en: <http://httpd.apache.org/docs/2.2/>

Pero una vez aprendidos estos conceptos, no significa que no usaremos más Webmin, sino que empezaremos a usar la opción “Editar archivos de configuración”, tal como vemos en la siguiente figura:

Indice de Módulo Editar Archivos de Configuración

Editar Directivas en Archivo:

```

# Based upon the NCSA server configuration files originally by Rob McCool.
#
# This is the main Apache server configuration file. It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.2/ for detailed information about
# the directives.
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# The configuration directives are grouped into three basic sections:
# 1. Directives that control the operation of the Apache server process as a
#    whole (the 'global environment').
# 2. Directives that define the parameters of the 'main' or 'default' server,
#    which responds to requests that aren't handled by a virtual host.
#    These directives also provide default values for the settings
#    of all virtual hosts.
# 3. Settings for virtual hosts, which allow Web requests to be sent to
#    different IP addresses or hostnames and have them handled by the
  
```

## 11.3. Virtual hosts

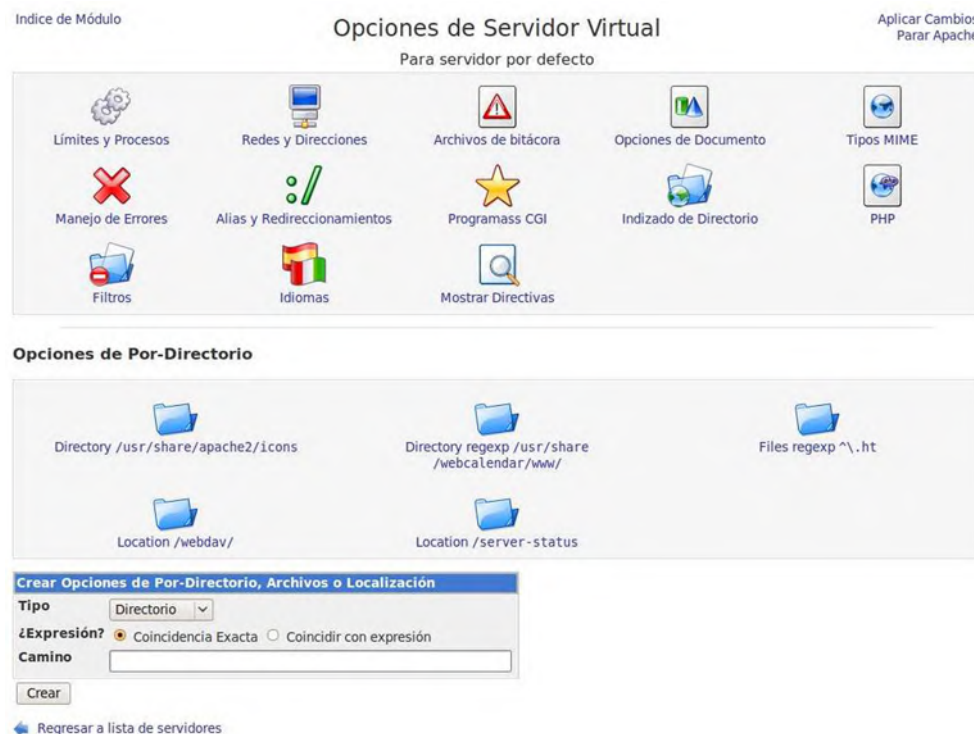
La capacidad de crear virtual hosts en un mismo servidor web, fue una de las principales razones por las que los proveedores de hosting adoptaron tempranamente a Apache como su servidor web.

Esto significa que en un mismo servidor, podemos tener muchos dominios y subdominios trabajando en forma independiente entre ellos, sin que se molesten o deban compartir características entre ellos.

Cuando entramos al módulo de administración de Apache de Webmin, por defecto, siempre nos lleva a la siguiente pantalla:



Esta pestaña, la segunda, luego de la de configuraciones globales, nos muestra inicialmente dos ítems: el de Servidor por Defecto es nuestro servidor apache propiamente dicho, con todas las opciones que se aplicarán luego a los servidores virtuales que vayamos creando. Si hacemos clic sobre el mundo o el enlace homónimo veremos lo siguiente:



Todos los cambios que hagamos en estos iconos, se aplicarán a todos los directorios de nuestro sistema de archivos /var/www en conjunto.

Si hacemos clic en el otro ítem que dice “Servidor virtual” en la pestaña “Existing virtual hosts”, entonces veremos lo siguiente:

The screenshot shows the Apache Virtual Host Options configuration window. At the top, it says "Opciones de Servidor Virtual" and "Para \*". Below this is a grid of 15 icons representing different configuration options: Límites y Procesos, Redes y Direcciones, Archivos de bitácora, Opciones de Documento, Tipos MIME, Manejo de Errores, Alias y Redireccionamientos, Programass CGI, Indizado de Directorio, PHP, Filtros, Idiomas, Mostrar Directivas, and Editar Directivas. Below the grid is a section titled "Opciones de Por-Directorio" showing four directory icons: Directory /, Directory /var/www/, Directory /usr/lib/cgi-bin, and Directory /usr/share/doc/. Below this is a form titled "Crear Opciones de Por-Directorio, Archivos o Localización" with fields for Tipo (Directory), ¿Expresión? (Coincidencia Exacta), and Camino. At the bottom is another form titled "Opciones de Servidor Virtual" with fields for Dirección, Puerto, Raíz de Documento (set to /var/www/), and Nombre de Servidor. A "Regresar a lista de servidores" link is at the bottom left.

Obsérvese que la diferencia con el anterior es que acá los cambios se aplicarán solo a las carpetas que están dentro del servidor virtual especificado.

Cuando vayamos creando nuevos servidores virtuales, aparecerán cada uno en un nuevo ítem de la ventana “Existing virtual hosts”.

Para crear estos servidores virtuales, solo debemos recurrir a la tercer pestaña de este módulo de control de Apache.

The screenshot shows the Apache 2.2.8 control panel with the 'Create virtual host' tab selected. The window title is 'Servidor Web Apache' and the version is 'Apache versión 2.2.8'. The main heading is 'Crear un Nuevo Servidor Virtual'. The configuration options are as follows:

- Manejar conexiones para direccionar:**
  - Aquellas no manejadas por otro servidor
  - Cualquier dirección
  - Dirección específica .. [input field]
  - Añadir dirección de servidor virtual de nombres (si es necesario)
  - Escuchar en dirección (si es necesario)
  - Por defecto  Cualquiera [input field]
- Puerto:** [input field]
- Raíz para Documentos:** [input field] ...
- Permitir acceso a este directorio
- Nombre del Servidor:**  Automático [input field]
- Agregar servidor virtual a archivo:**
  - Archivo httpd.conf estándar
  - Nuevo archivo bajo el directorio de servidores virtuales /etc/apache2/sites-available
  - Archivo seleccionado.. [input field] ...
- Copiar directivas desde:** [dropdown menu] En ningún lugar

A 'Crear Ahora' button is located at the bottom left of the configuration window.

Las directivas mínimas e indispensables para crear un servidor virtual, son solo dos:

- **Manejar conexiones para direccionar:** Acá seleccionaremos “Dirección específica” y pondremos la dirección que queremos que los usuarios utilicen para conectarse a ese sitio. También podremos cambiar desde acá el puerto de escucha para ese servidor virtual solamente.
- **Raíz para documentos:** Acá ingresaremos la ubicación de los archivos de ese sitio en nuestro sistema local. Algo como “/var/www/sitio\_nuevo”. Luego de esto, solo resta pulsar el botón “Crear ahora”.

## 11.4. Control del servidor web Apache

Esta tarea es recomendable hacerla desde una consola de texto y con un usuario con permisos de administrador (generalmente el mismo que se utilizó para la instalación o el que esté especificado por el instalador del sistema).

Para comandar el servidor Apache en su totalidad (iniciar, detener, reiniciar, etc.). Veamos cada variante:

```
sudo apache2ctl start
```

Es la forma normal de iniciar el servidor web Apache. Si ya está corriendo el servicio, nos dará error.

```
sudo apache2ctl stop
```

Detiene en el momento el servidor.

```
sudo apache2ctl restart
```

Reinicia instantáneamente el servidor.

```
sudo apache2ctl fullstatus
```

Entrega todos los datos del servidor en funcionamiento actualmente. Requiere tener instalado el módulo `mod_status` y activado.

```
sudo apache2ctl status
```

Entrega solo los datos básicos del servidor en funcionamiento actualmente. Requiere tener instalado el módulo `mod_status` y activado. módulo `mod_status` y activado.

```
sudo apache2ctl graceful
```

Reinicia el servidor, pero no de inmediato, sino que va esperando que se cierren todas las conexiones existentes.

```
sudo apache2ctl graceful-stop
```

Detiene el servidor, pero no de inmediato, sino que va esperando que se cierren todas las conexiones existentes.

Tenga en cuenta estos comandos para realizar las tareas de control en el servidor.



## 12. IPTables: El firewall de Linux

Netfilter es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho framework permite realizar el manejo de paquetes en diferentes estados del procesamiento. Netfilter es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux.

El componente más popular construido sobre Netfilter es IPTables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log. El proyecto ofrecía compatibilidad hacia atrás con ipchains hasta hace relativamente poco, aunque hoy día dicho soporte ya ha sido retirado al considerarse una herramienta obsoleta. El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías.

IPTables es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. El nombre IPTables se utiliza frecuentemente de forma errónea para referirse a toda la infraestructura ofrecida por el proyecto Netfilter. Sin embargo, el proyecto ofrece otros subsistemas independientes de IPTables tales como el connection tracking system o sistema de seguimiento de conexiones, o que, que permite encolar paquetes para que sean tratados desde espacio de usuario. IPTables es un software disponible en prácticamente todas las distribuciones de Linux actuales.

IPTables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en cadenas: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en tablas: cada tabla está asociada con un tipo diferente de procesamiento de paquetes. Cada regla especifica qué paquetes la cumplen y un destino que indica qué hacer con el paquete si éste cumple la regla. Cada paquete de red que llega a una computadora o que se envía desde una computadora recorre por lo menos una cadena y cada regla de esa cadena se comprueba con el paquete.

Si la regla cumple con el datagrama, el recorrido se detiene y el destino de la regla dicta lo que se debe hacer con el paquete. Si el paquete alcanza el fin de una cadena predefinida sin haberse correspondido con ninguna regla de la cadena, la política de destino de la cadena dicta qué hacer con el paquete.

Si el paquete alcanza el fin de una cadena definida por el usuario sin haber cumplido ninguna regla de la cadena o si la cadena definida por el usuario está vacía, el recorrido continúa en la cadena que hizo la llamada. Solo las cadenas predefinidas tienen políticas.

En IPTables, las reglas se agrupan en cadenas. Una cadena es un conjunto de reglas para paquetes IP, que determinan lo que se debe hacer con ellos.

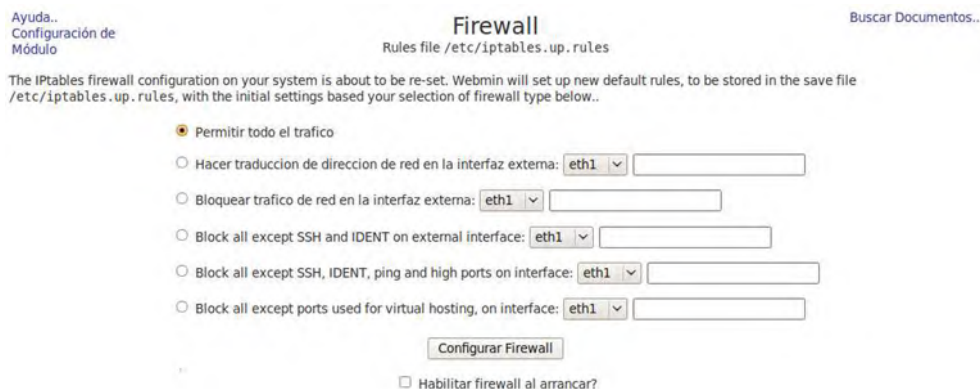
Cada regla puede desechar el paquete de la cadena (cortocircuito), con lo cual otras cadenas no serán consideradas.

Una cadena puede contener un enlace a otra cadena: si el paquete pasa a través de esa cadena entera o si cumple una regla de destino de retorno, va a continuar en la primera cadena. No hay un límite respecto de cuán anidadas pueden estar las cadenas. Hay tres cadenas básicas (INPUT, OUTPUT y FORWARD) y el usuario puede crear tantas como desee.

### 12.1. Pantalla inicial



Una vez que ingresamos a la opción “Cortafuegos Linux” en el menú lateral, opción “Red”. Veremos una pantalla como esta:



Esta vista nos dice que el firewall no está configurado en este momento. Razón por la que nos ofrece algunas opciones básicas para configurarlo inicialmente.

Para este ejemplo usaremos “Block all except SSH, IDENT, ping and high ports on interface eth1” (bloquear todo excepto SSH, IDENT, ping y puertos altos en la interface eth1). Lo que significa que no dejará pasar nada desde afuera del equipo, salvo la conexión segura ssh, identificación del servidor, los ping y acceso a puertos altos. Todo si la interface eth1 es la que está conectada a Internet.

Es útil también, configurar que todo esto se habilite al arranque del equipo, para que si se corta la luz, al volver a arrancar, no tenga problemas por falta de firewall.

Pulsamos el botón “Configurar Firewall” y vemos como se autoconfigura.

## 12.2. Vista de reglas

Esto que vemos en la pantalla es el resultado de la acción anterior que nos creó todas las reglas en las cadenas por defecto.

En la primer cadena, INPUT, es donde están todo el conjunto de reglas. Lo cual es muy lógico, porque la función principal de nuestro firewall es evitar que “entren” peticiones desde afuera.

Por ejemplo, la primera regla dice que el firewall debe aceptar todos los paquetes, siempre que la interfaz de entrada NO sea eth1.

Esto es porque nosotros le dijimos que eth1 era la interfaz a proteger (generalmente porque es la que tenemos conectada al Modem). Es decir que las otras placas de red, son las que están conectadas a las múltiples LANs que podemos llegar a tener internamente. Y no queremos que nos filtre los paquetes que llegan desde la LAN al servidor (por lo menos inicialmente).

Obsérvese también que se fijó una política por defecto para la cadena INPUT, que es “Drop” (patear) para cualquier paquete que pase por todo ese conjunto de reglas.

En conclusión, solo entran los paquetes que cumplan una regla del tipo “Aceptar”.

The screenshot shows the Firewall configuration interface. At the top, it says "Firewall" and "Rules file /etc/iptables.up.rules". Below that, there are buttons for "Mostrando Firewall:" (set to "Filtrador de paquetes (filter)") and "Añadir nueva cadean llamada:". The main section is titled "Paquetes entrantes (INPUT)" and contains a table of rules. Below the table, there are buttons for "Establecer accion por defecto a:" (set to "Drop"), "Delete Selected", and "Añadir regla". There are also sections for "Paquetes redirigidos (FORWARD)" and "Paquetes salientes (OUTPUT)", both with "No hay reglas definidas para esta cadena." and "Establecer accion por defecto a:" (set to "Accept") and "Añadir regla" buttons. At the bottom, there are buttons for "Aplicar configuracion", "Revertir configuracion", "Activar al arrancar" (with radio buttons for "Si" and "No"), and "Reset Firewall".

Accion	Condición	Mover	Añadir
<input type="checkbox"/> Aceptar	Si interfaz de entrada no es <b>eth1</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>TCP</b> y los flags TCP <b>ACK</b> (de <b>ACK</b> ) estan establecidos	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si el estado de conexion es <b>ESTABLISHED</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si el estado de conexion es <b>RELATED</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>UDP</b> y el puerto destino es <b>1024:65535</b> y el puerto origen es <b>53</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>ICMP</b> y el tipo ICMP es <b>echo-reply</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>ICMP</b> y el tipo ICMP es <b>destination-unreachable</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>ICMP</b> y el tipo ICMP es <b>source-quench</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>ICMP</b> y el tipo ICMP es <b>time-exceeded</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>ICMP</b> y el tipo ICMP es <b>parameter-problem</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>TCP</b> y el puerto destino es <b>22</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>TCP</b> y el puerto destino es <b>auth</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>ICMP</b> y el tipo ICMP es <b>echo-request</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Denegar	Si protocolo es <b>TCP</b> y el puerto destino es <b>2049:2050</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Denegar	Si protocolo es <b>TCP</b> y el puerto destino es <b>6000:6063</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Denegar	Si protocolo es <b>TCP</b> y el puerto destino es <b>7000:7010</b>	↓ ↑	↓ ↑
<input type="checkbox"/> Aceptar	Si protocolo es <b>TCP</b> y el puerto destino es <b>1024:65535</b>	↑	↓ ↑

Las cadenas FORWARD y OUTPUT, por el contrario, no tienen reglas y la política por defecto es “Accept” (aceptar) cualquier paquete que quiera pasar o salir del firewall.

Los botones del pie de página sirven para comandar el firewall, de manera que no necesitemos aplicar comandos por consola para:

- Aplicar la configuración
- Revertir la configuración
- Resetear el firewall (borrar todas las reglas)

También nos permite volver a definir si queremos que se active el firewall automáticamente al arrancar el equipo. Reiteramos que es muy importante que esto sea así, para evitar que ante un corte de corriente se desactive que mismo.

### 12.3. Crear una regla nueva

Indice de Modelo

### Añadir regla

**Detalles de cadena y acción**

Parte de la cadena: Reglas entrantes (INPUT)

Rule comment: web

Acción a ejecutar:  Aceptar  Denegar  Reject  Userspace

No hacer nada  Salir de cadena  Log packet  Ejecutar cadena

Reject with ICMP type:  Defecto  Type: icmp-net-unreachable

La acción seleccionada abajo solo será llevada a cabo si **todas** las condiciones de aquí se cumplen.

**Detalles de condición**

direccion o red origen: <Cualquiera>

Dirección o red de Destino: <Cualquiera>

Interfaz entrante: <Cualquiera> eth1

Interfaz saliente: <Cualquiera> eth1

Fragmentación:  Cualquiera  Esta fragmentada  No esta fragmentado

Protocolo de Red: Igual a TCP

Puerto TCP o UDP Origen: <Cualquiera> Puerto(s)

Puerto TCP o UDP Destino: Igual a Puerto(s) 80

Puerto(s) de origen y destino: <Cualquiera>

Flags TCP establecidos: <Cualquiera>  SYN  ACK  FIN  RST  URG  PSH fuera de  SYN  ACK  FIN  RST  URG  PSH

El numero de opcion TCP esta establecido: <Cualquiera>

Tipo de paquete ICMP: <Cualquiera> any

Dirección Ethernet: <Cualquiera>

Ratio de flujo de paquetes: <Cualquiera> / second

Ratio de paquetes: <Cualquiera>

Estados de conexiones: <Cualquiera> Nueva conexión (NEW) Conexión existente (ESTABLISHED) Relacionado con existente (RELATED) No es parte de ninguna conexión (INVALID)

Tipo de servicio: <Cualquiera> Minimize-Delay (0x10)

Additional IPTables modules:

Additional parameters:

Crear

[Regresar a lista de reglas](#)

Es de esperarse que en algún momento pongamos algún servicio que queremos que se pueda acceder desde Internet, por lo que deberemos crear una regla que abra un agujero en nuestro firewall para que esto se pueda hacer.

Para esto usaremos la opción del enlace que figura en la última columna de las reglas y que tiene un dibujo de una flecha celeste apuntando para arriba.

En este caso estoy creando una regla para que el servidor web pueda publicar sus páginas hacia Internet.

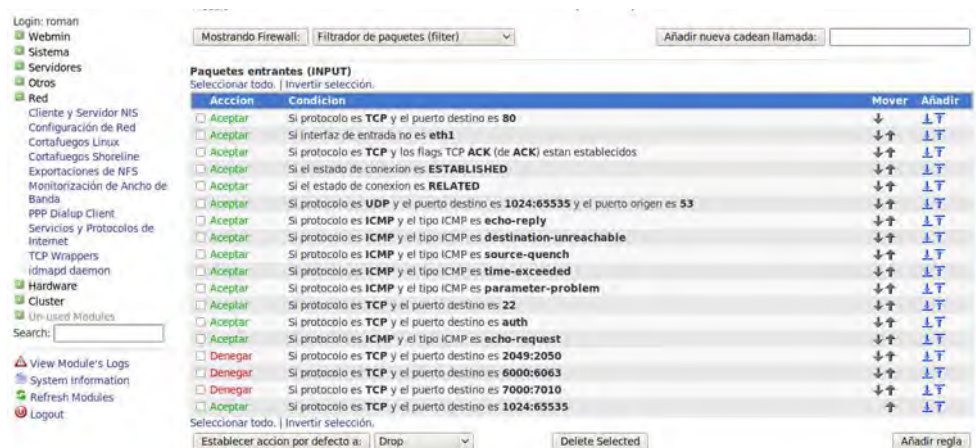
Primero le pongo un comentario para que pueda reconocer rápidamente la regla cuando la vea entre todas las otras. Es el primer recuadro.

En el siguiente recuadro le digo que lo que quiero que haga esta regla es “Aceptar” las peticiones que coincidan con los criterios.

El protocolo que utilizan las páginas web es TCP, por lo que debo cambiar ambas opciones del tercer recuadro: “Igual a” y “TCP”.

El último recuadro, tal vez el más importante, es donde le digo que el puerto de escucha del servidor será el 80 (es fundamental que en el campo anterior diga “Igual a”).

Una vez terminado esto, solo nos resta pulsar el botón “Crear”.



En nuestra nueva cadena INPUT tenemos la regla creada como la primera de todas las que controlará nuestro firewall.

Como el control de reglas se hace de arriba hacia abajo, el firewall no se verá recargado de trabajo aunque tengamos mucho tráfico en nuestra web, puesto que al primer control, ya dejará pasar los paquetes.

Este mismo procedimiento deberemos repetirlo si queremos tener un FTP o cualquier otro servicio que se publique hacia Internet (salvo SSH que ya está abierto a peticiones por la regla número 12).



# 13. ProFTPD

Podremos configurar ProFTPD desde el menú de servidores dentro de Webmin, no obstante, cuando ingresemos por primera vez, notaremos que no está instalado. Para proceder con la instalación deberemos ir a la sección Unused modules e instalarlo desde ahí.



Una vez instalado, podremos ver las opciones que nos presenta.



**Opciones de Red:** configuraciones de tiempos de espera y propiedades del servidor respecto a las sesiones abiertas.

Índice de  
Módulo

## Opciones de Red

Apply Changes  
Stop ProFTPD

Opciones de Red

<p><b>Máximas sesiones concurrentes</b> <input type="radio"/> Defecto <input checked="" type="radio"/> <input style="width: 40px;" type="text" value="30"/></p> <p><b>Tipo de servidor</b> <input type="text" value="Demonio solitario"/></p> <p><b>Tiempo sin hacer nada antes de desconectar</b> <input type="radio"/> Defecto <input checked="" type="radio"/> <input style="width: 40px;" type="text" value="1200"/> segundos</p> <p><b>Tiempo a esperar por primera transferencia</b> <input type="radio"/> Defecto <input checked="" type="radio"/> <input style="width: 40px;" type="text" value="600"/> segundos</p> <p><b>¿Hago búsqueda inversa de DNS de direcciones de cliente?</b> <input type="radio"/> Si <input type="radio"/> No <input checked="" type="radio"/> Defecto</p> <p><b>¿Permito transferencias forasteras de datos?</b> <input type="radio"/> Si <input type="radio"/> No <input checked="" type="radio"/> Defecto</p> <p><b>¿Permito reiniciar cargas?</b> <input type="radio"/> Si <input type="radio"/> No <input checked="" type="radio"/> Defecto</p> <p><b>Modo de transferencia por defecto</b> <input type="text" value="Defecto"/></p> <p><b>Mensaje de conexión de cliente</b> <input type="radio"/> Si <input type="radio"/> No <input checked="" type="radio"/> Defecto</p> <p><b>Máximos logins concurrentes</b> <input checked="" type="radio"/> Defecto <input type="radio"/> Ilimitados <input type="text" value=""/></p> <p>Mensaje de error de login <input style="width: 100%;" type="text"/></p> <p><b>Máximos logins concurrentes falta o es inválido</b> <input checked="" type="radio"/> Defecto <input type="radio"/> Ilimitados <input type="text" value=""/></p> <p>Mensaje de error de login <input style="width: 100%;" type="text"/></p> <p><b>Rango de puerto PASV</b> <input checked="" type="radio"/> Defecto <input type="radio"/> Mín - máx <input style="width: 40px;" type="text"/> - <input style="width: 40px;" type="text"/></p> <p><b>Client connection message</b> <input type="radio"/> Defecto <input type="radio"/> Ninguno <input type="radio"/> Show default message <input style="width: 100%;" type="text"/></p> <p><b>¿Uso opción de socket TCP_NODELAY (TCP_SinRETARDO)?</b> <input type="radio"/> Si <input type="radio"/> No <input checked="" type="radio"/> Defecto</p>	<p><b>¿Enviar respuesta de estilo RFC2228?</b> <input checked="" type="radio"/> Si <input type="radio"/> No <input type="radio"/> Defecto</p> <p><b>¿Sólo fuerza a puertos necesarios?</b> <input type="radio"/> Si <input type="radio"/> No <input checked="" type="radio"/> Defecto</p> <p><b>Tiempo a esperar por autenticación</b> <input checked="" type="radio"/> Defecto <input type="radio"/> <input style="width: 40px;" type="text"/> segundos</p> <p><b>Tiempo a esperar por atasco en transferencia de datos</b> <input type="radio"/> Defecto <input checked="" type="radio"/> <input style="width: 40px;" type="text" value="600"/> segundos</p> <p><b>Tamaño de cola de respaldo de diario TCP</b> <input checked="" type="radio"/> Defecto <input type="radio"/> <input style="width: 40px;" type="text"/></p> <p><b>¿Permito reiniciar descargas?</b> <input type="radio"/> Si <input type="radio"/> No <input checked="" type="radio"/> Defecto</p> <p><b>Tamaño máximo de comando FTP</b> <input checked="" type="radio"/> Defecto <input type="radio"/> <input style="width: 40px;" type="text"/></p> <p><b>¿Difiero mensaje de bienvenida hasta haber hecho login?</b> <input type="radio"/> Si <input type="radio"/> No <input checked="" type="radio"/> Defecto</p>
---	--

[← Regresar a menú principal](#)



Principalmente hay que tener en cuenta algunos puntos de esta sección:

- El tipo de servidor (que debería quedar como solitario, pero si se maneja bien el inetd se puede cambiar)
- Número máximo de sesiones concurrentes, debido a que cualquier conexión obtenida en el servidor es considerada como sesión y puede haber equipos que se encuentren sin actividad o tengan una conexión lenta.
- Tiempos de espera sin actividad y de espera por la primer transferencia: en ambos casos se podría considerar como usuarios inactivos que sólo utilizan un slot pero que no generan carga del servidor. Aquí se podrá cambiar el tiempo de espera con valores expresados en segundos.

**Opciones de Diario:** forma en que puede almacenarse el log de actividades del servidor.

**Archivos y Directorios:** customización de presentación de directorios para el acceso de los usuarios.

**Control de Acceso:** formas de loguearse al servidor como así también personalizar los mensajes para los usuarios.

**Usuarios de FTP denegados:** utilizarlo para excluir usuarios puntualmente del acceso al servidor.

**Editar Archivos de Configuración:** desde aquí podremos editar directamente el archivo de configuración del módulo.



# 14. Samba

Samba es un software que permite a tu ordenador con Ubuntu poder compartir archivos e impresoras con otras computadoras en una misma red local. Utiliza para ello un protocolo conocido como SMB/CIFS compatible con sistemas operativos UNIX o Linux , como Ubuntu, pero además con sistemas Windows (XP, NT, 98...), OS/2 o incluso DOS. También se puede conocer como LanManager o NetBIOS.

Configuración de Módulo **Gestor de Comparticiones Samba** Versión 3.32 de Samba Buscar Documentos..

Seleccionar todo. | Invertir selección. | Crear una nueva compartición de archivo | Crear una nueva compartición de impresora | Crear una nueva copia | Ver Todas las Conexiones

Nombre de Compartición	Trayectoria	Seguridad
<input type="checkbox"/> printers	Todas las Impresoras	Imprimible para todos los usuarios conocidos
<input type="checkbox"/> print\$	/var/lib/samba/printers	Sólo lectura para todos los usuarios conocidos

Seleccionar todo. | Invertir selección. | Crear una nueva compartición de archivo | Crear una nueva compartición de impresora | Crear una nueva copia | Ver Todas las Conexiones

---

### Configuración Global



Red de Unix



Red de Windows



Autenticación



Impresión de Windows a Unix



Opciones Varias



Winbind Options



Valores por defecto de Compartición de Archivos



Valores por defecto de Compartición de Impresoras



AddType  
Alias  
SetHeader  
Edit Config File

**Samba Users****Rearrancar Servidores Samba**

Haz click en este botón para rearrancar los servidores samba en ejecución de tu sistema. Esto forzará que la actual configuración sea aplicada. Esto también desconectará cualquier conexión con el servidor. Por ello, si no quieres que la configuración en curso sea aplicada inmediatamente, deberías esperar 1 minuto hasta que Samba vuelva a cargar la configuración automáticamente.

**Stop Samba Servers**

Click this button to shut down the running Samba servers on your system. All currently logged in users will be forcibly disconnected.

En el menú principal del módulo, vamos a encontrar en primer lugar las impresoras declaradas en el entorno, luego las opciones de configuración y finalizando, la declaración de usuarios y grupos para el entorno de trabajo.

## 14.1. Preparando el entorno para compartir

En primera instancia tenemos que ir a Opciones de Red de Windows y definir el nombre del grupo de trabajo para que sea similar al que usamos dentro de la red de Windows.

Indice de Módulo

### Opciones de Red de Windows

**Opciones de Red de Windows**

**Grupo de Trabajo**  Defecto  WORKGROUP

**modo WINS**  Ser un servidor WINS  Usar servidor   Ninguno(a)

**Descripción del servidor**  Defecto  None  %h server (Samba, Ubuntu)

**Nombre del servidor**

**Aliases del Servidor**

**Servicio por defecto** Ninguno ▾

**Mostrar siempre los servicios** global  
printers  
print\$ ▾

**Máxima medida reportada de disco**  Ilimitada   kB

**Comando para Winpopup (Enviar mensaje)**

**Prioridad del hojeador maestro** 20

**Protocolo mayor** Defecto ▾

**¿Hojeador maestro?**  Si  No

**Seguridad** Defecto ▾

**Servidor de Claves de Acceso**

**El remoto se anuncia a**  Ninguno  Desde la lista...

Dirección IP	Como Grupo de Trabajo (opcional)
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Salvar

[← Regresar a lista de comparticiones](#)

Una vez que igualamos el nombre del grupo de trabajo, podremos agregar carpetas e impresoras para el uso compartido.

### 14.1.1. Establecer grupos de usuarios

Dentro del sistema tendremos que establecer nombres de grupos y asignarles privilegios, de esta forma, podremos asignar esos privilegios a los usuarios de forma más dinámica.



Desde Add and edit Samba groups, podremos asignar los privilegios al grupo que agreguemos.



**Group name:** es el nombre que le demos dentro de Samba

**Group type:** aquí la opción dependerá de que si nuestra LAN esta con un servidor de dominios (domain group), si el manejo es desde un servidor NT, o es un grupo local cuyo nombre de grupo no tiene que validarse en otro equipo. Normalmente es Local group.

**Unix group:** esta es la categoría de grupo que queramos asociar.

## 14.2. Agregar carpetas para compartir

Desde el menú principal del módulo tenemos que seleccionar “Crear una nueva compartición de archivo”.



De ahí, se nos presentará otra sección en la cual, hay que agregar los detalles de la carpeta a compartir.



**Nombre de la compartición:** es el nombre con el que se va a compartir.

**Directorio a compartir:** desde ahí se seleccionará el directorio que quiere ser mostrado en el sistema.

También podremos asignar el usuario y grupo propietario de la carpeta y configurar los permisos mediante códigos de CHMOD en modo octal.

**Comentario de la Compartición:** es el comentario que se verá sobre el recurso, ya sea antes de conectarse y cuando veamos información del recurso compartido.

## 14.3. Compartir Impresoras



**Nombre de compartición:** es el nombre que le asignaremos dentro de la red. El mismo debe ser único ya que si hubiera otro nombre igual se generaría un conflicto.

**Impresora de Unix:** es el nombre que se le asignará dentro de la red Unix/Linux, es recomendable no completarlo para que sea asignado un nombre por defecto.

**Directorio de Spool:** podremos asignar un directorio específico para recibir los archivos de impresión. Al igual que el nombre en Unix, es recomendable dejarlo en blanco para que el módulo le asigne el lugar por defecto.

**Disponible:** habilitamos o no el uso del recurso.

**Hojeable:** al deshabilitarlo, hacemos que no podamos visualizar el recurso, pero si el estado del mismo es “disponible” podremos utilizarlo igual.

**Comentario de la compartición:** Es el nombre largo que le asignaremos al recurso, pudiéndolo utilizar como referencia para los otros usuarios.



## 14.4. Compartición sin contraseñas

En primer lugar, ir a “Red de Windows”



Colocar el nombre del grupo de trabajo que coincida con el de la red Windows (generalmente es WORKGROUP).

En seguridad cambiarlo por “Nivel de compartición”

Indice de Módulo

### Opciones de Red de Windows

**Opciones de Red de Windows**

**Grupo de Trabajo**  Defecto  WORKGROUP

**modo WINS**  Ser un servidor WINS  Usar servidor   Ninguno(a)

**Descripción del servidor**  Defecto  None  %h server (Samba, Ubuntu)

**Nombre del servidor**  **Alias del Servidor**

**Servicio por defecto** Ninguno **Mostrar siempre los servicios** global printers print\$

**Máxima medida reportada de disco**  Ilimitada   kB

**Comando para Winpopup (Enviar mensaje)**  **Prioridad del hojeador maestro** 20

**Protocolo mayor** Defecto **¿Hojeador maestro?**  Si  No

**Seguridad** Defecto **Servidor de Claves de Acceso**

**El remoto se anuncia a**  Ninguno  Desde la lista...

Dirección IP	Como Grupo de Trabajo (opcional)
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Salvar

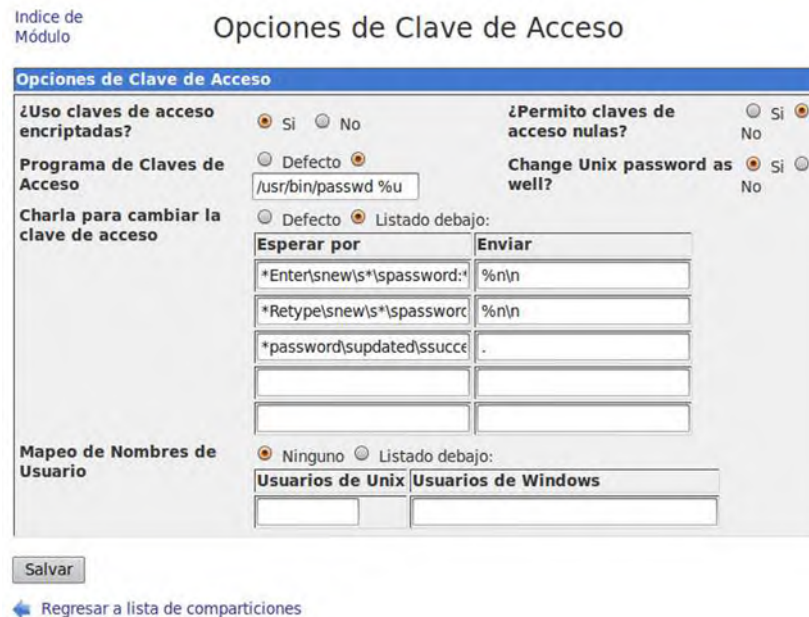
Regresar a lista de comparticiones

Luego, volviendo al menú principal del módulo, hay que ingresar a “Autenticación”

### Configuración Global



Y dentro de la opción “Autenticación” dejar activado el “Uso de claves de acceso encriptadas”



Ahora, volviendo nuevamente al menú principal del módulo, hay que ingresar a “Valores por defecto de la Compartición de Archivos”.

### Configuración Global



Y desde ahí, a “Control de Seguridad y Acceso”.

Indice de Módulo

## Valores por defecto de Compartición de Archivos

**Información de Compartición**


Directorio a compartir  ...


¿Disponible?  Sí  No      ¿Hojeable?  Sí  No


Comentario de Compartición


Note - these settings also effect the defaults for all printer shares.

**Otras opciones de Compartición**

  
Control de Seguridad y Acceso

  
Permisos de Archivo

  
Cómo dar Nombre a Archivos

  
Opciones varias

[Regresar a lista de comparticiones](#)

En “Máquinas a autorizar” hay que colocar las direcciones IP de las estaciones de trabajo Windows. Si queremos que solo algunos equipos puedan usar este servicio.

O dejarlo en “Todos(as)” si queremos que sea una carpeta/archivo abierto a todo el que esté dentro de la LAN.

Luego, si se han definido los grupos, se los pueden declarar asignándoles los privilegios.

Indice de Módulo

## Valores por defecto de Seguridad

**Control de Seguridad y Acceso**

¿Se puede escribir?  Sí  No

¿Acceso de Invitado?  Ninguno  Sí  Sólo invitado

Usuario invitado de Unix  ...

¿Limito a lista de posibles?  Sí  No

Máquinas a autorizar  Todos(as)  Sólo permitir:

Máquinas a denegar  Ninguno  Sólo denegar:

¿Revalidar usuarios?  Sí  No

Usuarios válidos  ...

Grupos válidos  ...

Usuarios inválidos  ...

Grupos inválidos  ...

Usuarios posibles  ...

Grupos posibles  ...

Usuarios de sólo lectura  ...

Grupos de sólo lectura  ...

Usuarios de lectura/escritura  ...

Grupos de lectura/escritura  ...

[Regresar a compartición de archivos](#) | [Regresar a lista de comparticiones](#)

Elegimos “Salvar” y volvemos al menú anterior.

Desde ahí dejamos activado las opciones “Disponible” y “Hojeable” y usamos el botón de “Salvar”.

Indice de Módulo

### Valores por defecto de Compartición de Archivos

**Información de Compartición**

Directorio a compartir  ...

¿Disponible?  Sí  No      ¿Hojeable?  Sí  No

Comentario de Compartición

Note - these settings also effect the defaults for all printer shares.

Salvar

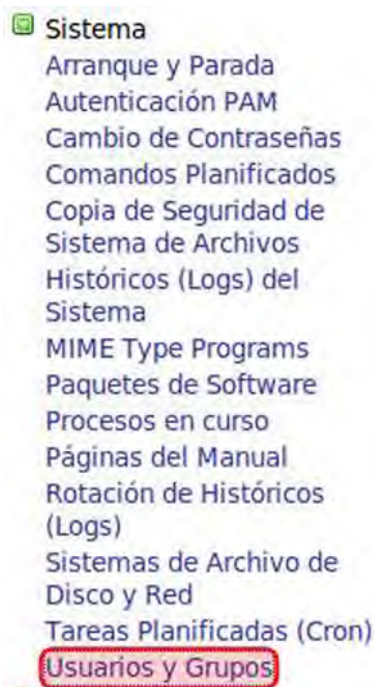
Para finalizar, reiniciar el servidor Samba.

**Rearranicar Servidores Samba** Haz click en este botón para rearrancar los servidores samba en ejecución de tu sistema. Esto forzará que la actual configuración sea aplicada. Esto también desconectará cualquier conexión con el servidor. Por ello, si no quieres que la configuración en curso sea aplicada inmediatamente, deberías esperar 1 minuto hasta que Samba vuelva a cargar la configuración automáticamente.

**Stop Samba Servers** Click this button to shut down the running Samba servers on your system. All currently logged in users will be forcibly disconnected.

## 14.5. Compartición con contraseñas

1. Puede utilizar el nombre predeterminado o introducir otro nombre para la copia de seguridad. Si hay más de un dispositivo de almacenamiento externo conectado, seleccione en la lista desplegable el destino en el que desea crear la copia de seguridad de los datos. Haga clic en **Siguiente** para continuar.



2. Debemos crear un usuario en el servidor para que pueda tener un directorio para compartir y pueda servir para validar con contraseña el ingreso.

Le pondremos “/bin/false” como shell, de esta manera evitamos que este usuario pueda loguearse en el servidor. Por cuestiones de seguridad.

Podemos poner una contraseña común o no ponerle... luego tendremos que, de todas maneras, modificar esto.

Si queremos, podemos activar el “Forzar cambio en el siguiente login”

Indice de Módulo  
Ayuda..

### Crear Usuario

**Detalles de Usuario**

**Nombre de Usuario**

**ID de Usuario**  Automático  Calculado

**Nombre Real**

**Directorio inicial**  Automático  Directory

**Shell**

**Contraseña**

No se pide contraseña

No está permitido el login

Contraseña normal

Clave de acceso pre-encryptada

Login temporalmente deshabilitado

**Opciones de Contraseña**

**Contraseña cambiada**  **Fecha de Expiración**  /  /

**Días mínimos**  **Días máximos**

**Días de Aviso**  **Días inactivos**

**¿Forzar cambio en el siguiente login?**  Sí  No

**Afiliación del Grupo**

**Grupo primario**

Nuevo grupo con el mismo nombre que el usuario

Nuevo grupo

Grupo existente

**Grupos secundarios**

**All groups**  
root  
daemon  
bin  
sys  
adm

**In groups**

-> <-

**Al Crear...**

**¿Crear directorio inicial?**  Sí  No

**¿Copiar archivos a directorio inicial?**  Sí  No

**¿Crear usuario en otros módulos?**  Sí  No

[← Regresar a lista de usuarios y grupos](#)

- Entramos a la opción “Red de Windows” del índice del módulo Samba.



Donde veremos esta pantalla y cambiaremos el tipo de compartición a “Nivel de usuario”. Y Pulsamos en “Salvar”.

Índice de Módulo

### Opciones de Red de Windows

**Opciones de Red de Windows**

**Grupo de Trabajo**  Defecto  WORKGROUP

**modo WINS**  Ser un servidor WINS  Usar servidor   Ninguno(a)

**Descripción del servidor**  Defecto  None  %h server (Samba, Ubuntu)

**Nombre del servidor**

**Servicio por defecto**  Ninguno

**Máxima medida reportada de disco**  Ilimitada   kB

**Comando para Winpopup (Enviar mensaje)**

**Protocolo mayor**  Defecto

**Seguridad**  Nivel de Usuario

**El remoto se anuncia a**  Ninguno  Desde la lista...

**Aliases del Servidor**

**Mostrar siempre los servicios**  global printers print\$

**Prioridad del hojeador maestro**  20

**¿Hojeador maestro?**  Si  No

**Servidor de Claves de Acceso**

**Dirección IP**

**Como Grupo de Trabajo (opcional)**

Salvar

- Pulsamos el botón:



Para que Samba reconozca al usuario recién creado. Lo que nos mostrará la siguiente pantalla:

Índice de Módulo

### Convertir Usuarios

Este formulario te permite sincronizar la lista de usuarios de Unix y Samba. Cuando Samba usa claves de acceso encriptadas, se usa una lista separada de usuarios y claves de acceso en vez de la lista de usuarios del sistema. The list of users not to convert can contain usernames, UIDs, group names prefixed with an @, or UID ranges like 500-1000 or 500.

No convertir o quitar estos usuarios:  -499

Actualizar los usuarios ya existentes en Samba a partir de sus detalles en Unix

Añadir nuevos usuarios de Samba a partir de la lista de usuarios de Unix

Borrar los usuarios de Samba que no existen en Unix

Para los recién creados usuarios, poner la clave de acceso a:

Sin clave de acceso

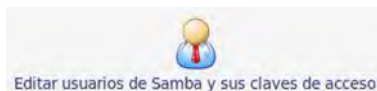
Cuenta bloqueada

Usa esta clave de acceso

Convertir Usuarios

Con estas opciones convertimos los usuarios para que ya Samba los pueda reconocer.

5. El paso siguiente es poner la contraseña final para que use el usuario en Samba. Para eso pulsamos el botón:



Y en la siguiente pantalla, ponemos una contraseña definitiva.

Indice de Módulo

### Editar Usuario de Samba

**Editar Usuario de Samba**

Nombre de usuario *pepe* UID de Unix 1005

Clave de Acceso  Clave de acceso actual  Nueva clave de acceso

Opciones de usuario  Usuario normal

No se requiere clave de acceso

Cuenta desactivada

La clave no caduca

Cuenta fiable de estación de trabajo

Salvar Borrar

6. Creamos la compartición del directorio. Para eso pulsamos el botón

[Crear una nueva compartición de archivo](#)

Y en la siguiente pantalla, configuramos de la siguiente manera:

Indice de Módulo

### Crear Compartición de Archivo

**Información de Compartición**

Nombre de Compartición  pepe  Compartición de Directorios de Inicio

Directorio a compartir /home/pepe

Automatically create directory?  Si  No Create with owner root

Create with permissions 755 Create with group root

¿Disponible?  Si  No ¿Hojeable?  Si  No

Comentario de Compartición

Crear

7. Ya casi terminando, hacemos clic en el enlace que muestra la nueva compartición: Y allí pulsamos sobre el botón “control de Seguridad y Acceso”.

Allí deberemos poner en Sí la opción a “Revalidar usuarios”, agregar a nuestro nuevo usuario como usuario válido y si queremos, a otros usuarios existentes para solo lectura o cualquier otra opción que nos parezca útil para nuestro caso.

Por último salvar estas opciones y volver al índice del módulo Samba.

8. El último paso es reiniciar el servidor Samba, desde el botón correspondiente del pie del índice del módulo.

**Rearrancar Servidores Samba**

Luego podremos probar desde cualquier Windows o Linux de la red que el recurso existe y que podemos acceder con la contraseña correspondiente.



# 15. Servidor proxy Squid

Squid es un popular programa de software libre que implementa un servidor proxy y un demonio para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Aunque orientado a principalmente a HTTP y FTP es compatible con otros protocolos como Internet Gopher. Implementa varias modalidades de cifrado como TLS, SSL, y HTTPS.

## 15.1. Características

Squid posee las siguientes características:

- **Proxy y Caché de HTTP, FTP, y otras URL:** Squid proporciona un servicio de Proxy que soporta peticiones HTTP, HTTPS y FTP a equipos que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentra fuera de la red interna.
- **Proxy para SSL:** Squid también es compatible con SSL (Secure Socket Layer) con lo que también acelera las transacciones cifradas, y es capaz de ser configurado con amplios controles de acceso sobre las peticiones de usuarios.
- **Jerarquías de caché:** Squid puede formar parte de una jerarquía de caches. Diversos proxys trabajan conjuntamente sirviendo las peticiones de las páginas. Un navegador solicita siempre las páginas a un sólo proxy, si este no tiene la página en la caché hace peticiones a sus hermanos, que si tampoco las tienen las hacen a su/s padre/s... Estas peticiones se pueden hacer mediante dos protocolos: HTTP e ICMP.
- **ICP, HTCP, CARP, caché digests:** Squid sigue los protocolos ICP, HTCP, CARP y caché digests que tienen como objetivo permitir a un proxy "preguntarle" a otros proxys caché si poseen almacenado un recurso determinado.
- **Caché transparente:** Squid puede ser configurado para ser usado como proxy transparente de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin embargo

se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.

- **WCCP:** A partir de la versión 2.3 Squid implementa WCCP (Web Cache Control Protocol). Permite interceptar y redirigir el tráfico que recibe un router hacia uno o más proxys caché, haciendo control de la conectividad de los mismos. Además permite que uno de los proxys caché designado pueda determinar como distribuir el tráfico redirigido a lo largo de todo el array de proxys caché.
- **Control de acceso:** Ofrece la posibilidad de establecer reglas de control de acceso. Esto permite establecer políticas de acceso en forma centralizada, simplificando la administración de una red.
- **Aceleración de servidores HTTP:** Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché, si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet. Esta función permite navegar rápidamente cuando los objetos ya están en el caché y además optimiza enormemente la utilización del ancho de banda.
- **SNMP:** Squid permite activar el protocolo SNMP, este proporciona un método simple de administración de red, que permite supervisar, analizar y comunicar información de estado entre una gran variedad de máquinas, pudiendo detectar problemas y proporcionar mensajes de estados.
- **Caché de resolución DNS:** Squid está compuesto también por el programa dnserver, que se encarga de la búsqueda de nombres de dominio. Cuando Squid se ejecuta, produce un número configurable de procesos dnserver, y cada uno de ellos realiza su propia búsqueda en DNS. De este modo, se reduce la cantidad de tiempo que la caché debe esperar a estas búsquedas DNS.

### 15.2. Proxy Web

El proxy caché es una manera de guardar los objetos solicitados de Internet (por ejemplo, datos como páginas web) disponibles vía protocolos HTTP, FTP y Gopher en un sistema más cercano al lugar donde se piden. Los navegadores web pueden usar la caché local Squid como un servidor proxy HTTP, reduciendo el tiempo de acceso así como el consumo de ancho de banda. Esto es muchas veces útil para los proveedores de servicios de Internet para incrementar la velocidad de sus consumidores y para las redes de área local que comparten la conexión a Internet.

Debido a que también es un proxy (es decir, se comporta como un cliente en lugar del cliente real), puede proporcionar un cierto grado de anonimato y seguridad. Sin embargo, también puede introducir problemas significativos de privacidad ya que puede registrar mucha información, incluyendo las URL solicitadas junto con otra información adicional como la fecha de la petición, versión del navegador y del sistema operativo, etc.

Un programa cliente (por ejemplo, un navegador) o bien tiene que especificar explícitamente el servidor proxy que quiere utilizar (típico para consumidores de ISP) o bien podría estar

usando un proxy sin ninguna configuración extra. A este hecho se le denomina caché transparente, en el cual todas las peticiones HTTP son interceptadas por Squid y todas las respuestas guardadas en caché. Esto último es típico en redes corporativas dentro de una red de acceso local y normalmente incluye los problemas de privacidad mencionados previamente.

Squid tiene algunas características que pueden facilitar establecer conexiones anónimas. Características tales como eliminar o modificar campos determinados de la cabecera de peticiones HTTP de los clientes. Esta política de eliminación y alteración de cabeceras se establece en la configuración de Squid. El usuario que solicita páginas a través de una red que utiliza Squid de forma transparente, normalmente no es consciente de este proceso o del registro de información relacionada con el proceso.

### 15.3. Squid en Webmin

Tal como con otros servicios, Squid puede controlarse casi por completo desde la interfaz web de Webmin. Esto nos da una gran flexibilidad, porque podemos tocar la configuración desde cualquier computadora de la red.

Para acceder a Webmin deberemos apuntar a la IP de nuestro servidor escolar y al puerto 10000 del mismo, desde un navegador. Es decir que en la barra de dirección puede verse algo así:

**https://localhost:10000** (accediendo desde el mismo servidor escolar)

**https://127.0.0.1:10000** (accediendo desde el mismo servidor escolar)

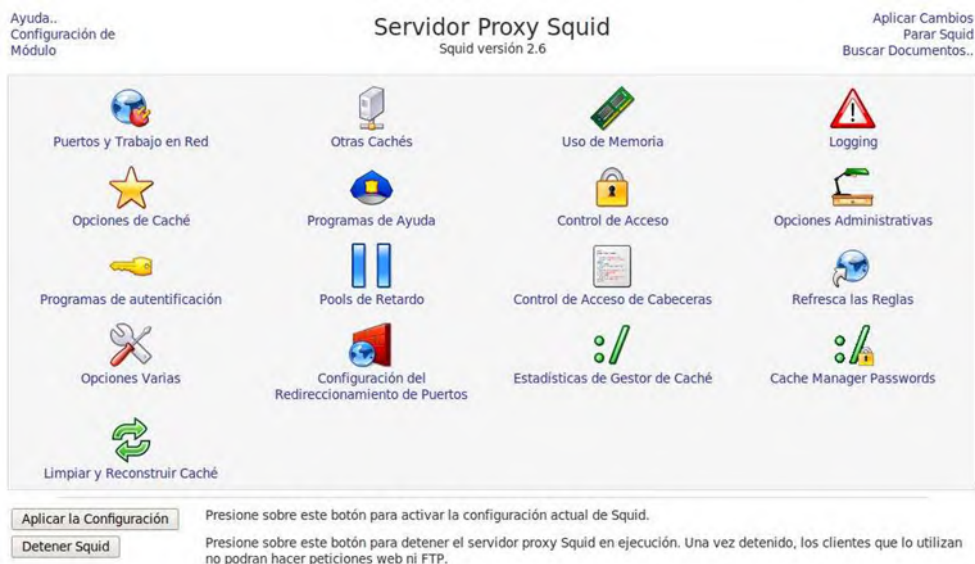
**https://172.16.0.1:10000** (accediendo desde cualquier máquina de la red LAN)

Cuando introducimos el usuario y contraseña del sistema (el mismo que tiene permisos de hacer sudo), nos encontramos en la ventana de inicio.

Allí desplegamos el grupo “Servidores” de la barra lateral y allí elegimos “Squid – Servidor Proxy”, tal como vemos en la siguiente imagen:



Luego de esta acción, nos encontraremos con la siguiente pantalla.



En principio, tenemos unos botones al pie que nos permiten comandar el servicio. En este caso vemos el botón “Detener Squid”, así como otro botón para reiniciar el servicio cuando cambiamos la configuración, el botón “Aplicar la Configuración”.

Ahora desarrollaremos los ítems fundamentales para que el servidor proxy pueda funcionar mínima y funcionalmente. Recomendamos profundizar el aprendizaje sobre las particularidades de Squid en los siguientes lugares:

<http://www.squidcache.org>

<http://www.idesoft.es/www2/squid>

### 15.4. Puertos y trabajo en red

No tocaremos los parámetros de este ítem, pero es importante saber que acá tenemos la configuración del puerto de escucha del servidor. Que por defecto es el 3128.

El Servidor Escolar ya se encuentra preconfigurado para actuar como proxy transparente, es decir que no requiere que estemos tocando la configuración de los clientes para que pasen por el proxy, sino que el firewall redirecciona todas las peticiones de los navegadores de la red LAN hacia este puerto.

No toque estos parámetros salvo que ya sepa mucho más sobre el funcionamiento de Squid.

## 15.5. Uso de memoria

The screenshot shows the 'Uso de Memoria' configuration window in Squid. It contains several settings for memory and disk usage, each with a radio button for 'Por defecto' and a text input field. The settings are:

- Límite de uso de memoria:** Por defecto, [ ] kBs
- Medida de caché FQDN:** Por defecto, [ ]
- Marca de Pleamar de Disco:** Por defecto, [ ] %
- Marca de Bajamar de Disco:** Por defecto, [ ] %
- Medida máxima de objeto de caché:** Por defecto, [ ] kBs
- Medida de caché de dirección IP:** Por defecto, [ ] entradas
- Marca de Pleamar de caché IP:** Por defecto, [ ] %
- Marca de Bajamar de caché IP:** Por defecto, [ ] %
- Política de reemplazo de disco:** Por defecto
- Política de reemplazo de Memoria:** Por defecto

Buttons for 'Aplicar Cambios' and 'Parar Squid' are in the top right, and a 'Salvar' button is at the bottom left.

- Límite de uso de memoria:** Por defecto, Squid viene configurado a 8 Mb, lo que es bastante poco teniendo en cuenta la cantidad de memoria RAM que hoy en día traen los equipos. Recomendamos cambiar este parámetro a 32 Mb para aumentar la aceleración de la navegación web. Igualmente, la optimización del funcionamiento de un proxy debe tomarse con calma y a través de un proceso de prueba y error, encontrar el conjunto de parámetros que mejor resultado traiga para cada lugar de implementación. La recomendación general es empezar usando la configuración por defecto y luego de algunos días, cambiarla a la recomendada, si todavía no se está conforme con los resultados se puede probar con 64 Mb o seguir subiendo. Llegará un punto en el que no se notará mejora, eso nos dice que debemos bajar uno o dos pasos en la subida del límite.
- Medida de caché NDCC (FQDN):** Por defecto es 1024. Número máximo de entradas de caché de Nombre de Dominio Completamente Calificado. La recomendación es no tocar primariamente este parámetro.
- Marca de pleamar de Memoria:** Por defecto es 95 %. Al alcanzar esta marca de pleamar, los objetos calientes y los en tránsito se liberan de memoria. La recomendación es no tocar primariamente este parámetro.
- Marca de bajamar de Memoria:** Por defecto es 90 %. Tras alcanzar la marca de pleamar, Squid liberará memoria hasta que el uso baje por debajo de la marca de bajamar. Una vez que comience a optimizar su Squid, esto se puede reconfigurar para que libere a menos del 90 %, digamos al 80 %. Lo que debería hacer que se alcance la pleamar menos seguido y por lo tanto, el servidor trabaje menos.
- Marca de pleamar de disco:** Por defecto es 95 %. Al alcanzar esta marca de pleamar, Squid empezará a limpiar el disco agresivamente. La recomendación es no tocar primariamente este parámetro.
- Marca de bajamar de disco:** Por defecto es 90 %. Tras alcanzar la marca de pleamar, Squid continuará limpiando el disco hasta llegar por debajo de esta marca de bajamar. Una vez que comience a optimizar su Squid, esto se puede reconfigurar para que libere a menos del 90 %, digamos al 80 %. Lo que debería hacer que se alcance la pleamar menos seguido y por lo tanto, el servidor trabaje menos.
- Medida máxima de objeto de caché:** Por defecto 4096 KB. Este valor limita la medida de los objetos que se almacenarán en la caché. Cualquier cosa por encima de esta medida nunca será puesta en caché y debe de ser cargada desde el servidor original

cada vez.

Este valor también puede incrementarse usando la misma estrategia que en el caso de el Límite de uso de memoria.

- **Medida de caché de la dirección IP:** Por defecto es 1024. Número de entradas a almacenar en la caché de IP.  
La recomendación es no tocar primariamente este parámetro.
- **Marca de pleamar de caché IP:** Por defecto es 95 %. El punto en el cual Squid limpia las entradas de caché de IP.  
La recomendación es no tocar primariamente este parámetro.
- **Marca de bajamar de caché IP:** Por defecto es 90 %. Tras empezar el vaciado de caché IP, este continuará hasta que el número de entradas en la caché IP caiga por debajo de este porcentaje.
- **Políticas de reemplazo de memoria y disco:** La recomendación es no tocar primariamente este parámetro.

## 15.6. Opciones administrativas

The screenshot shows the 'Opciones Administrativas' (Administrative Options) section of the Squid configuration web interface. The window title is 'Opciones Administrativas y de Anuncio'. It contains several configuration fields:

- Ejecutar como usuario Unix:** Radio buttons for 'Sin cambios' and 'roman' (selected).
- Ejecutar como grupo Unix:** Radio buttons for 'Sin cambios' and 'roman' (selected).
- Dirección e-mail del gestor de caché:** Radio buttons for 'Por defecto' and an empty text field.
- Nombre de máquina visible:** Radio buttons for 'Automático' and 'troya' (selected).
- Nombre de máquina única:** Radio buttons for 'Automático' and an empty text field.
- Otros nombres de caché DNS:** Radio buttons for 'Ninguno' and an empty text field.
- Máquina de anuncio de caché:** Radio buttons for 'Por defecto' and an empty text field.
- Puerto de anuncio de caché:** Radio buttons for 'Por defecto' and an empty text field.
- Archivo de anuncio de caché:** Radio buttons for 'Ninguno' and an empty text field.
- Período de Anunciación:** Radio buttons for 'Por defecto' and a dropdown menu set to 'horas'.

Buttons for 'Aplicar Cambios', 'Parar Squid', and 'Salvar' are visible.

Mínimamente, debemos cambiar dos parámetros en este apartado.

- **Ejecutar como usuario Unix:** En este lugar deberemos poner el nombre del usuario administrador del sistema para que al aplicar la configuración no tengamos mensajes de error. El grupo es el mismo nombre de usuario.
- **Nombre de máquina visible:** Acá pondremos el nombre del equipo nuestro, donde funciona el Squid. Si tenemos dudas al respecto, podemos abrir una consola de texto (siempre que estemos trabajando en el mismo servidor) y escribir el comando:

```
hostname
```

Que nos responderá lo que necesitamos poner en este campo.

## 15.7. Configuración del redireccionamiento de puertos

Indice de Módulo Configuración del Redireccionamiento de Puertos

Squid puede hacer proxy HTTP transparente para las peticiones en el puerto 80, pero configurando las reglas del cortafuegos para redireccionarlas automáticamente y en el puerto 3128, que es en el que escucha Squid. Esto sólo funcionará si el sistema que está ejecutando Squid también es el router de su red. Puede hacerse añadiendo una regla de IPTables al cortafuegos, asumiendo que está gestionado con el módulo Cortafuegos Linux.

El redireccionamiento de puertos esta desactivado

El redireccionamiento de puertos esta activado para los clientes de la red

La redirección de puerto está habilitada, para clientes en el interfaz

¿Aplicar la configuración del cortafuegos y de Squid?

Este apartado es el que hace la magia. Acá se vuelve transparente el proxy.

Si bien se encuentra dentro de las opciones de Squid, lo que esto hace es modificar nuestro firewall para que tome las peticiones normales de los navegadores de la red y los redireccione hacia el puerto 3128 del proxy.

Podemos elegir la placa a la que están conectadas las máquinas de la LAN o bien la especificación de la LAN misma.





# 16. SARG Generador de Informes de Análisis de Squid

SARG (Squid Analysis Report Generator) es una muy buena herramienta desarrollada por un brasileño llamado Pedro Orso, que permite saber dónde han estado navegando los usuarios en Internet , a través del análisis del fichero de log “access.log” del famoso proxy Squid. El poder de esta herramienta es increíble, pudiendo saber qué usuarios accedieron a qué sitios, a qué horas, cuantos bytes han sido descargados, relación de sitios denegados, errores de autenticación... entre otros. La flexibilidad que puede obtener con Ubuntu es muy alta, principalmente para las organizaciones que quieren tener un control de accesos y ancho de banda de acceso a Internet.

## 16.1. SARG en Webmin

SARG puede controlarse por completo desde la interfaz web de Webmin. Esto nos da una gran flexibilidad, porque podemos tocar la configuración desde cualquier computadora de la red.

Para acceder a Webmin deberemos apuntar a la IP de nuestro servidor escolar y al puerto 10000 del mismo, desde un navegador. Es decir que en la barra de dirección puede verse algo así:

**https://localhost:10000** (accediendo desde el mismo servidor escolar)

**https://127.0.0.1:10000** (accediendo desde el mismo servidor escolar)

**https://172.16.0.1:10000** (accediendo desde cualquier máquina de la red LAN)

Cuando introducimos el usuario y contraseña del sistema (el mismo que tiene permisos de hacer sudo), nos encontramos en la ventana de inicio.

Allí desplegamos el grupo “Servidores” de la barra lateral y allí elegimos “Generador de Informes de Análisis de Squid”, tal como vemos en la siguiente imagen:



Luego de hacer clic en ese enlace nos encontraremos con la ventana inicial de configuración de SARG. Tal como la siguiente figura lo demuestra.



Tal como podemos ver, no requiere demasiadas configuraciones. Unas pocas y SARG creará automáticamente una serie de informes que podremos luego ver ingresando a:

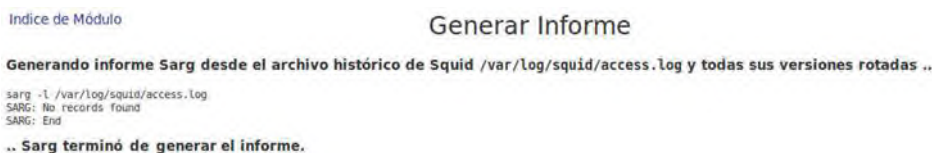
**<http://localhost/squidreports/index.html>** (accediendo desde el mismo servidor escolar)

**<http://127.0.0.1/squidreports/index.html>** (accediendo desde el mismo servidor escolar)

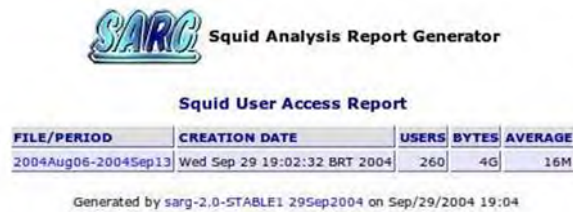
**<http://172.16.0.1/squidreports/index.html>** (accediendo desde cualquier máquina de la red LAN)

Pero antes de poder ver el informe deberemos generarlo por primera vez. Para esto usaremos el botón que dice “Generar informe ahora” que está al pié de la pantalla principal de SARG.

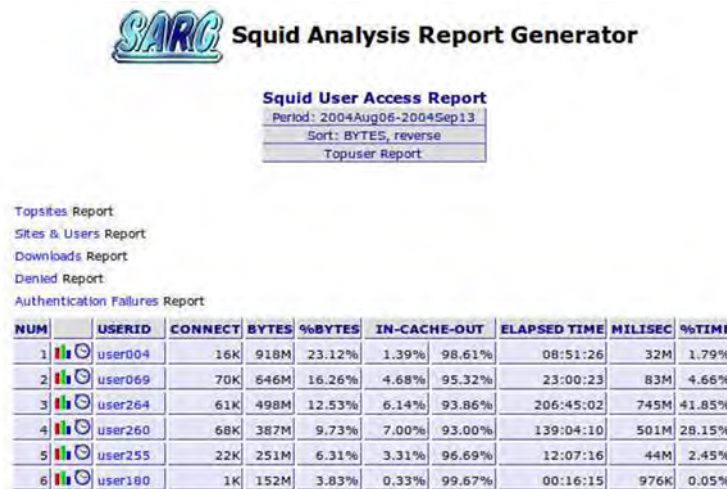
Si todo va bien, nos debería aparecer una pantalla como esta:



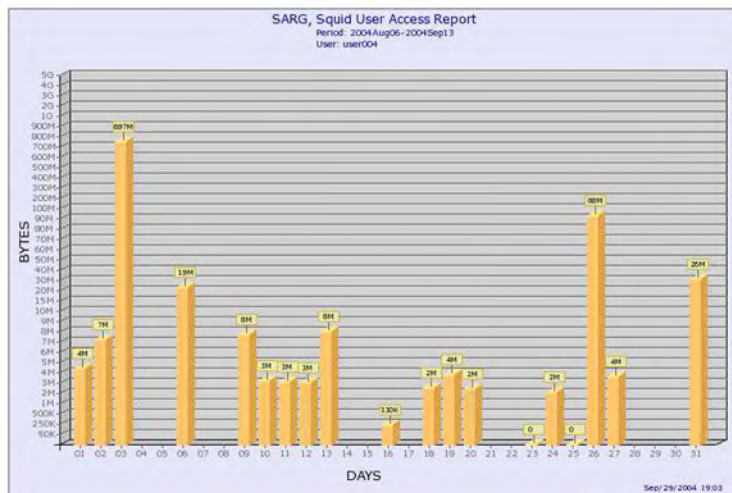
Luego de lo cual, podremos acceder con el navegador a un informe que se verá así:



Si hacemos clic en el enlace que marca la fecha del informe, veremos lo siguiente:

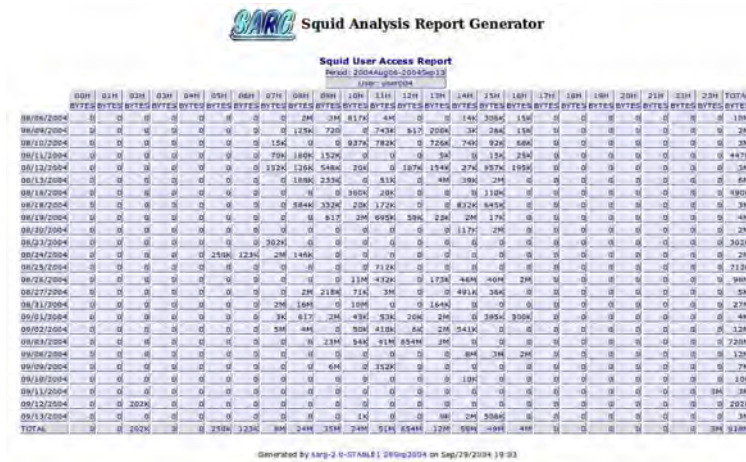


Este informe nos da ya un resumen por usuario que puede sernos de gran utilidad, pero no es lo más que obtendremos ya que por cada usuario también tenemos tres informes detallados extra. Que podremos acceder a través de los enlaces de la segunda y tercera columna del informe.



## 16. SARG Generador de Informes de Análisis de Squid

El primer enlace nos lleva a un gráfico detallado de la cantidad de bytes descargados en función de los últimos días.



El segundo enlace nos muestra una detallada tabla con la misma información que el gráfico anterior, solo que acá podremos tener mayor precisión con los datos.

The screenshot shows the SARG Squid User Access Report for user 'user004' from August 6, 2004, to September 13, 2004. The report is sorted by bytes in descending order. The table provides detailed information for each accessed site, including the number of connections, bytes transferred, cache status, and elapsed time.

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME
www.iaa.de	2	693M	75.41%	0.00% 100.00%	01:18:21	5M	14.74%
download3.vmware.com	2	83M	8.94%	0.00% 100.00%	00:04:00	241K	0.75%
ftp.gnome.org	4	22M	2.37%	0.00% 100.00%	00:01:58	119K	0.37%
www.cracksoft.net.pk	34	8M	0.83%	48.90% 51.10%	00:04:19	260K	0.81%
sch.ch.sourceforge.net	2	8M	0.80%	0.00% 100.00%	00:00:32	33K	0.10%
aleron.dl.sourceforge.net	1	7M	0.69%	0.00% 100.00%	00:00:21	21K	0.07%
optusnet.dl.sourceforge.net	1	5M	0.46%	0.00% 100.00%	00:00:33	34K	0.11%
ftp.mozilla.org	14	5M	0.46%	0.00% 100.00%	00:00:26	27K	0.08%
search.yahoo.com	115	5M	0.44%	0.00% 100.00%	00:03:00	180K	0.57%
www.clanpeters.com	1	4M	0.36%	0.00% 100.00%	00:00:37	37K	0.12%
www.onda.com.br	1K	4M	0.33%	2.85% 97.15%	00:00:27	27K	0.09%
fpdownload.macromedia.com	3	3M	0.28%	61.86% 38.14%	00:00:54	54K	0.17%
www.distlab.dk	4	3M	0.24%	0.00% 100.00%	00:00:15	15K	0.05%
www.penguin-tech.com.br	234	2M	0.21%	0.42% 99.58%	00:03:19	200K	0.63%
xcdraast.sourceforge.net	8	2M	0.20%	0.00% 100.00%	00:00:14	15K	0.05%
ads.osdn.com	244	2M	0.20%	0.00% 100.00%	00:05:56	357K	1.12%
www.directv.com.br	554	2M	0.18%	12.94% 87.06%	00:00:15	16K	0.05%
www.fireburner.com	1	2M	0.16%	0.00% 100.00%	00:01:25	85K	0.27%
www.carteroffice.com	27	2M	0.14%	0.00% 100.00%	00:00:12	13K	0.04%
members.msn.com	184	2M	0.13%	5.35% 94.65%	00:00:51	52K	0.16%
www.sylc.com.br	19	2M	0.13%	0.00% 100.00%	00:00:13	13K	0.04%
www.promsbrasli.it	125	2M	0.12%	0.00% 100.00%	00:00:54	55K	0.17%
www.connthians.com.br	200	2M	0.12%	0.00% 100.00%	00:00:46	47K	0.15%
www.ibiblio.org	5	2M	0.12%	0.00% 100.00%	00:00:17	18K	0.06%
www.sky.tv.br	157	2M	0.12%	32.59% 67.41%	00:00:44	45K	0.14%

En la tercer columna tendremos el enlace que nos dice el nombre del usuario y allí podremos ver exactamente por cuales páginas ha estado navegando en ese período.

Obsérvese que en la 5ª columna podremos tener datos de cuanto de la navegación se pudo cachear con el proxy. Es decir que acá podemos observar los datos que nos permitan optimizar la configuración de Squid para nuestro Servidor Escolar.

## 16.2. Opciones de informe

En este ítem podremos profundizar sobre la adecuación de SARG a nuestra necesidad. No es requerido que lo toquemos y no lo recomendamos inicialmente.

Para entender más sobre el uso de SARG podemos buscar información en: <http://sarg.sourceforge.net/>

## 16.3. Estilo de informe

En el ítem del mismo nombre podemos configurar la manera en la que se hará el informe que hemos visto.

Uno de los detalles cosméticos que podremos configurar es el idioma y la codificación que usaremos para las etiquetas de los informes, el título que tendrá, si queremos cambiar los colores de los fondos o tipografías, si queremos el logo de la organización puesto en el mismo, etc.

Si bien no es imprescindible configurar esto (podría quedar como viene por defecto), suele ser buena idea adecuarlo a nuestro gusto.

Indice de Módulo Estilo de Informe

**Opciones de color de estilo HTML de informe**

**Idioma de Informe** Spanish ▾

**Juego de caracteres de informe** Latin1 ▾

---

**Título de informe**  Defecto  Squid User Access Reports

**Color de título**  Defecto  green

**Fuente de cuerpo de informe**  Defecto  Tahoma,Verdana,Arial

**Color de cabecera**  Defecto  darkblue

**Color de fondo de cabecera**  Defecto  blanchetalmond

**Tamaño de fuente de cabecera**  Defecto (9px)

**Color de texto**  Defecto  #000000

**Color de fondo de texto**  Defecto  lavender

---

**Referencia de imagen para logo**  Defecto (none)

**Tamaño de imagen (ancho y alto)**  Defecto (80 45)

**Texto para logo**  Defecto

**Color de texto para logo**  Defecto (#000000)

---

**Referencia de imagen para fondo**  Defecto (none)

**Color de fondo**  Defecto  white

[Regresar a índice del módulo](#)

## 16.4. Generación de Informe planificado

Indice de Módulo Generación de Informe Planificado

**Opciones de informe programado**

¿Habilitar informes planificados?  No  Sí, en las horas seleccionadas abajo ..

Directorio de informe /var/www/squid-reports

¿Limpiar directorio de informe cada vez?  Sí  No

Generar informe para rango de fechas  Todas las entradas en archivo histórico  Aquellos entre  y  días atrás

Planificación simple .. Diariamente (a la medianoche) ▾  Horas y fechas seleccionadas abajo ..

Minutos	Horas	Días	Meses	Días de Semana																																																																																																																																											
<input checked="" type="radio"/> Todos <input type="radio"/> Seleccionado...	<input checked="" type="radio"/> Todos <input type="radio"/> Seleccionado...	<input checked="" type="radio"/> Todos <input type="radio"/> Seleccionado...	<input checked="" type="radio"/> Todos <input type="radio"/> Seleccionado...	<input checked="" type="radio"/> Todos <input type="radio"/> Seleccionado...																																																																																																																																											
<table border="1"> <tr><td>0</td><td>12</td><td>24</td><td>36</td><td>48</td></tr> <tr><td>1</td><td>13</td><td>25</td><td>37</td><td>49</td></tr> <tr><td>2</td><td>14</td><td>26</td><td>38</td><td>50</td></tr> <tr><td>3</td><td>15</td><td>27</td><td>39</td><td>51</td></tr> <tr><td>4</td><td>16</td><td>28</td><td>40</td><td>52</td></tr> <tr><td>5</td><td>17</td><td>29</td><td>41</td><td>53</td></tr> <tr><td>6</td><td>18</td><td>30</td><td>42</td><td>54</td></tr> <tr><td>7</td><td>19</td><td>31</td><td>43</td><td>55</td></tr> <tr><td>8</td><td>20</td><td>32</td><td>44</td><td>56</td></tr> <tr><td>9</td><td>21</td><td>33</td><td>45</td><td>57</td></tr> <tr><td>10</td><td>22</td><td>34</td><td>46</td><td>58</td></tr> <tr><td>11</td><td>23</td><td>35</td><td>47</td><td>59</td></tr> </table>	0	12	24	36	48	1	13	25	37	49	2	14	26	38	50	3	15	27	39	51	4	16	28	40	52	5	17	29	41	53	6	18	30	42	54	7	19	31	43	55	8	20	32	44	56	9	21	33	45	57	10	22	34	46	58	11	23	35	47	59	<table border="1"> <tr><td>0</td><td>12</td></tr> <tr><td>1</td><td>13</td></tr> <tr><td>2</td><td>14</td></tr> <tr><td>3</td><td>15</td></tr> <tr><td>4</td><td>16</td></tr> <tr><td>5</td><td>17</td></tr> <tr><td>6</td><td>18</td></tr> <tr><td>7</td><td>19</td></tr> <tr><td>8</td><td>20</td></tr> <tr><td>9</td><td>21</td></tr> <tr><td>10</td><td>22</td></tr> <tr><td>11</td><td>23</td></tr> </table>	0	12	1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11	23	<table border="1"> <tr><td>1</td><td>13</td><td>25</td></tr> <tr><td>2</td><td>14</td><td>26</td></tr> <tr><td>3</td><td>15</td><td>27</td></tr> <tr><td>4</td><td>16</td><td>28</td></tr> <tr><td>5</td><td>17</td><td>29</td></tr> <tr><td>6</td><td>18</td><td>30</td></tr> <tr><td>7</td><td>19</td><td>31</td></tr> <tr><td>8</td><td>20</td><td></td></tr> <tr><td>9</td><td>21</td><td></td></tr> <tr><td>10</td><td>22</td><td></td></tr> <tr><td>11</td><td>23</td><td></td></tr> <tr><td>12</td><td>24</td><td></td></tr> </table>	1	13	25	2	14	26	3	15	27	4	16	28	5	17	29	6	18	30	7	19	31	8	20		9	21		10	22		11	23		12	24		<table border="1"> <tr><td>Enero</td></tr> <tr><td>Febrero</td></tr> <tr><td>Marzo</td></tr> <tr><td>Abril</td></tr> <tr><td>Mayo</td></tr> <tr><td>Junio</td></tr> <tr><td>Julio</td></tr> <tr><td>Agosto</td></tr> <tr><td>Setiembre</td></tr> <tr><td>Octubre</td></tr> <tr><td>Noviembre</td></tr> <tr><td>Diciembre</td></tr> </table>	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre	Diciembre	<table border="1"> <tr><td>Domingo</td></tr> <tr><td>Lunes</td></tr> <tr><td>Martes</td></tr> <tr><td>Miércoles</td></tr> <tr><td>Jueves</td></tr> <tr><td>Viernes</td></tr> <tr><td>Sábado</td></tr> </table>	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado
0	12	24	36	48																																																																																																																																											
1	13	25	37	49																																																																																																																																											
2	14	26	38	50																																																																																																																																											
3	15	27	39	51																																																																																																																																											
4	16	28	40	52																																																																																																																																											
5	17	29	41	53																																																																																																																																											
6	18	30	42	54																																																																																																																																											
7	19	31	43	55																																																																																																																																											
8	20	32	44	56																																																																																																																																											
9	21	33	45	57																																																																																																																																											
10	22	34	46	58																																																																																																																																											
11	23	35	47	59																																																																																																																																											
0	12																																																																																																																																														
1	13																																																																																																																																														
2	14																																																																																																																																														
3	15																																																																																																																																														
4	16																																																																																																																																														
5	17																																																																																																																																														
6	18																																																																																																																																														
7	19																																																																																																																																														
8	20																																																																																																																																														
9	21																																																																																																																																														
10	22																																																																																																																																														
11	23																																																																																																																																														
1	13	25																																																																																																																																													
2	14	26																																																																																																																																													
3	15	27																																																																																																																																													
4	16	28																																																																																																																																													
5	17	29																																																																																																																																													
6	18	30																																																																																																																																													
7	19	31																																																																																																																																													
8	20																																																																																																																																														
9	21																																																																																																																																														
10	22																																																																																																																																														
11	23																																																																																																																																														
12	24																																																																																																																																														
Enero																																																																																																																																															
Febrero																																																																																																																																															
Marzo																																																																																																																																															
Abril																																																																																																																																															
Mayo																																																																																																																																															
Junio																																																																																																																																															
Julio																																																																																																																																															
Agosto																																																																																																																																															
Setiembre																																																																																																																																															
Octubre																																																																																																																																															
Noviembre																																																																																																																																															
Diciembre																																																																																																																																															
Domingo																																																																																																																																															
Lunes																																																																																																																																															
Martes																																																																																																																																															
Miércoles																																																																																																																																															
Jueves																																																																																																																																															
Viernes																																																																																																																																															
Sábado																																																																																																																																															

Nota: Ctrl-click (ó comando-click en Mac) para seleccionar y deseleccionar minutos, horas, días y meses.

Desde esta pantalla, podremos configurar el momento en que queremos que se genere el informe, cada cuanto tiempo y otros detalles.

Si bien se puede dejar con las opciones por defecto, tal vez se quiera eliminar algunos datos que no requerimos para ganar en limpieza de nuestros reportes y ahorrar carga al procesador de nuestro servidor.

# Parte IV.

## Apéndices





# A. Manual de Usuario Exomate X352

## A.1. Instrucciones de seguridad

Siga las siguientes normas de seguridad para asegurar su protección y la de su computadora.

### A.1.1. Advertencias generales

- No utilice su computadora portátil con la base directamente apoyada sobre el cuerpo durante lapsos de tiempo extensos, ya que el calor podría acumularse en la base. El contacto prolongado con la piel podría causar molestias o, incluso, quemaduras.
- No intente revisar la computadora por su cuenta. Siempre siga las instrucciones de instalación cuidadosamente.
- A fin de evitar heridas causadas por descargas eléctricas o fuego:
  - ◆ Apague la computadora completamente al cambiar módulos de memoria, realizar una limpieza de ella, sus componentes o la carcasa; así como también al realizar operaciones que requieran de procedimientos similares. Para ello, apague el interruptor principal, quite la batería y, luego desconecte el adaptador (fuente de alimentación) del toma corriente o de cualquier otro tipo de fuente de energía externo, tal como baterías externas.
  - ◆ No utilice la computadora cerca del agua, por ejemplo, cerca de una bañera, pileta de cocina o para lavar la ropa, en un sótano húmedo, junto a una piscina o bajo la lluvia.
  - ◆ No conecte ni desconecte ningún cable o realice un mantenimiento o reconfiguración de este producto durante una tormenta eléctrica.
  - ◆ No coloque ningún objeto dentro de las salidas de aires o aberturas de su computadora o accesorios. Esta acción podría dañar los componentes internos y provocar un incendio o descarga eléctrica.
  - ◆ Al instalar los módulos de memoria, protéjase tocando una superficie conductiva con conexión a tierra, tal como un dispositivo con enchufe con toma de tierra. Evite tocar los pines y cables del módulo de memoria o del circuito interno de la computadora.
- Cuando se disponga a utilizar la computadora, colóquela sobre una superficie plana.
- Manipule los componentes con cuidado. Sostenga los componentes, tales como los módulos de memoria, por sus bordes, no por los pines.

- En caso de que la batería pierda líquido y éste entrara en sus ojos, no se los frote. Lávese los ojos con agua e inmediatamente consulte al médico, de lo contrario, podría causarle una herida ocular.
- Lave su piel o ropa inmediatamente si la batería perdiera ácido y éste entrara en contacto con ellas. En caso contrario, podría sufrir una inflamación cutánea.
- Utilice la computadora dentro del rango de temperatura recomendado: de 5°C a 35°C. Guárdela a una temperatura de entre -20°C a +60°C.
- Evite exponer la netbook a fuertes sacudidas.
- Mantenga al equipo alejado de grandes fuentes de calor y no lo exponga a las radiaciones directas del sol, ni lo deje dentro de vehículos expuestos al sol.
- Proteja la netbook frente a las interferencias electromagnéticas. De esta manera también evitará una posible pérdida de datos.

### **A.1.2. Advertencias sobre el cable y el adaptador**

- Lea las instrucciones de instalación antes de enchufar el cable y el adaptador/ cargador.
- Los cables que se utilizan en otros países deben cumplir con los normas de ese país. Utilice el adaptador de corriente alterna y cable de alimentación apropiados para su lugar de residencia.
- Si utiliza un alargador con su adaptador de corriente alterna, asegúrese de que el amperaje de los productos enchufados no exceda el del alargador.
- Cuando utilice el cable de alimentación, asegúrese de no colocarlo alrededor de objetos que puedan cortarlo o dañarlo.
- Cuando desconecte un cable, tire del conector tomando del cuerpo aislante del enchufe, no del cable. Mientras retira el enchufe, manténgalo alineado de forma uniforme para evitar doblar los pines conectores. Asimismo, antes de conectar un cable, asegúrese de que ambos conectores estén correctamente orientados y alineados.
- Asegúrese de que no haya ningún elemento apoyado sobre el adaptador y que el cable no esté ubicado en un lugar donde alguien pueda tropezarse o pisarlo.
- Use sólo los adaptadores de ca que son compatibles con esta computadora. Utilizar cualquier otro tipo de adaptador podría provocar un incendio o explosión.
- Antes de conectar la computadora a una fuente de energía, asegúrese de que el voltaje del adaptador concuerde con el de la fuente de energía.
  - ◆ 115 V/60 hz: en la mayoría de los países de América del norte y del sur y en algunos países del lejano oriente, tales como corea del sur y Taiwán.
  - ◆ 100 V/50 hz: en japon oriental y 100 v/60hz en japon occidental.
  - ◆ 220 V/50 hz: argentina, la mayoría de los países de Europa, el oriente medio y el lejano oriente.

- Cuando encienda la computadora o cargue la batería, coloque el adaptador en un área ventilada, como por ejemplo, un escritorio o en el suelo. No cubra el adaptador con papeles u otros objetos que puedan reducir la ventilación. Asimismo, no utilice el adaptador cuando esté dentro de un portafolio.
- A fin de que la computadora quede libre de corriente, apáguela, retire la batería y desconecte el adaptador del toma corriente.
- El adaptador adapta la corriente eléctrica alterna domiciliaria de 110 o 220 Volts a corriente continua que alimenta a la netbook y también recarga la batería de la misma. Lo correcto es que en su domicilio este siempre conectado para mantener cargada la batería y evitar ciclos de carga y descarga de la misma que acorten su vida útil.
- Conecte el cable de alimentación a la red eléctrica (220V) con conexión a tierra correctamente instalada.



Advertencia: (!) ¡PELIGRO DE MUERTE!  
¡NUNCA ABRA LA FUENTE DE ALIMENTACIÓN!



### A.1.3. Advertencias sobre la batería



(!) ¡PELIGRO! El impropio uso de la batería puede causar calor, fuego, explosión y daño.





- No lleve la batería en el bolsillo, dentro de un bolso o de cualquier otro elemento donde algún objeto metálico (por ejemplo, las llaves del auto) pueda causar un cortocircuito en los terminales. El excesivo flujo de corriente podría provocar temperaturas altas extremas y esto podría ocasionar quemaduras.
- Existe riesgo de explosión si no se reemplaza la batería por una adecuada. Utilice otra que sea igual o similar a la recomendada por el fabricante. No arroje las baterías al fuego, ya que podrían explotar. Consulte con las autoridades locales respecto a las instrucciones de desechos de residuos.
- No utilice o deje la batería cerca de una fuente de calor. El calor podría derretir el aislante y dañar otros componentes de seguridad, provocando, de esta forma, que la batería filtre ácido, se recaliente, emane humo, estalle o inflame. No deje la batería o el equipo dentro de un vehículo expuesto al sol.
- No sumerja la batería en agua o permita que se moje. Esto podría dañar sus componentes de protección y dar lugar a reacciones químicas anómalas, causando que la batería filtre ácido, se recaliente, emane humo, estalle o inflame.

- No golpee, desarme, pinche o incinere los contactos externos de la batería.
- No conecte los terminales positivo (+) y negativo (-) con un objeto de metal tal como alambre. Esto podría originar un cortocircuito, haciendo que la batería filtre ácido, se recaliente, emane humo, estalle o inflame.
- No utilice baterías que, en apariencia, estén deformadas o dañadas, ya que podría hacer que la batería filtrara ácido, se recalentara, emanara humo, estallara o inflamara.
- Si la batería perdiera, emanara un olor desagradable, generara calor, se decolorara o deformara, o, de alguna forma, su apariencia normal se viera alterada durante el uso, recarga o almacenamiento, quítela inmediatamente de la computadora o cargador y cese su uso.
- Utilice solo baterías diseñadas exclusivamente para este equipo.
- Cargue la batería estando ésta insertada en el equipo.
- No intente reparar usted mismo una batería defectuosa.
- Conserve la batería averiada en un lugar seguro, fuera del alcance de los niños, y deséchela lo antes posible según las indicaciones.

#### A.1.4. Desecho de baterías

- Deseche las baterías de litio-ion únicamente en los lugares de desechos de residuos autorizados. Para ubicar un sitio adecuado, consulte a las autoridades de desechos de residuos sólidos de su lugar de residencia o busque algún sitio en Internet que trate sobre el reciclado de baterías y que detalle los lugares de desechos próximos a su domicilio.
- No arroje las baterías al fuego, arrójelas en un cesto para residuos, en un contenedor de reciclaje o, de lo contrario, deséchelas de forma tal que no resulte perjudicial para el medio ambiente.

**Advertencia de Pila de Litio:**

 Este equipo contiene una pila de litio para alimentar el circuito de reloj y de calendario. Nunca intente reemplazarlo. De ser necesario, contacté a un técnico autorizado. 

#### A.1.5. Reciclaje del equipo y/o de la batería

EXO S.A. acepta la entrega de los equipos usados. Los equipos usados que se reciben son utilizados para su reutilización o bien son desechados según las normativas de protección del medio ambiente. Nunca deseche las baterías junto a la basura doméstica.

El embalaje de cartón y las demás partes de cartón del interior pueden desecharse junto al papel usado.

### **A.1.6. Indicaciones de seguridad adicionales para equipos con comunicaciones inalámbricas**

En su equipo hay integrado dispositivos de comunicaciones inalámbricas, de modo que, al trabajar con su equipo, debe cumplir siempre las siguientes indicaciones de seguridad:

- Desconecte el equipo si se encuentra en un avión.
- Si se encuentra en un hospital, en un quirófano o en la proximidad de equipos médicos electrónicos, desconecte el elemento radioeléctrico de la computadora. Las ondas radioeléctricas que emite pueden dañar la función de los equipos médicos.
- Mantenga el equipo al menos a 20 cm de distancia de un marcapasos, ya que en caso contrario las ondas radioeléctricas pueden perjudicar el funcionamiento correcto del marcapasos.
- La emisión de ondas radioeléctricas puede producir interferencias en los audífonos.
- No acerque el equipo a gases inflamables o a una zona potencialmente explosiva (por ejemplo a un taller de barnizado) ya que la emisión de ondas radioeléctricas puede ocasionar una explosión o producir un incendio.
- El alcance de la radiocomunicación depende de las condiciones medioambientales.
- Durante la comunicación de datos con sistemas inalámbricos es posible recibir datos no autorizados.

### **A.1.7. Cuidados de la pantalla LCD**

Las pantallas LCD son dispositivos delicados que requieren cuidados. Preste atención a las siguientes precauciones:

- No golpee la pantalla al cerrarla.
- No coloque ningún objeto encima estando cerrado o abierto.
- No coloque objetos arriba del teclado o el Mouse Pad, al cerrar el equipo puede quebrar la pantalla.
- Cuando no este usando el equipo, mantenga la pantalla cerrada para protegerla del polvo.

## A.2. Guía rápida de instalación

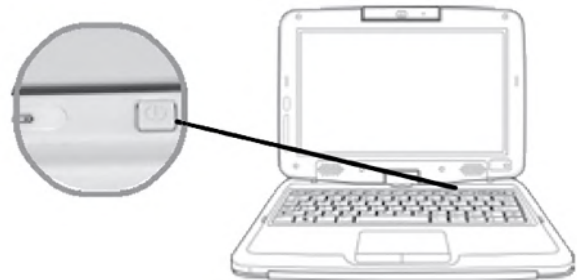
### A.2.1. Conexión del adaptador de alimentación

1. Conecte el cable de alimentación al adaptador.
2. Conecte el cable de alimentación a la toma de corriente (220V).
3. Coloque el enchufe de alimentación tipo plug a la netbook.



### A.2.2. Encendido del equipo

- Botón Interruptor/Suspensión
- Oprima momentáneamente para encender el sistema.
- Oprima y sostenga por lo menos 4 segundos para apagar el sistema.
- Oprima el botón Interruptor/Suspensión otra vez para volver al modo suspensión.
- Luz azul persistente indica ENCENDIDO.

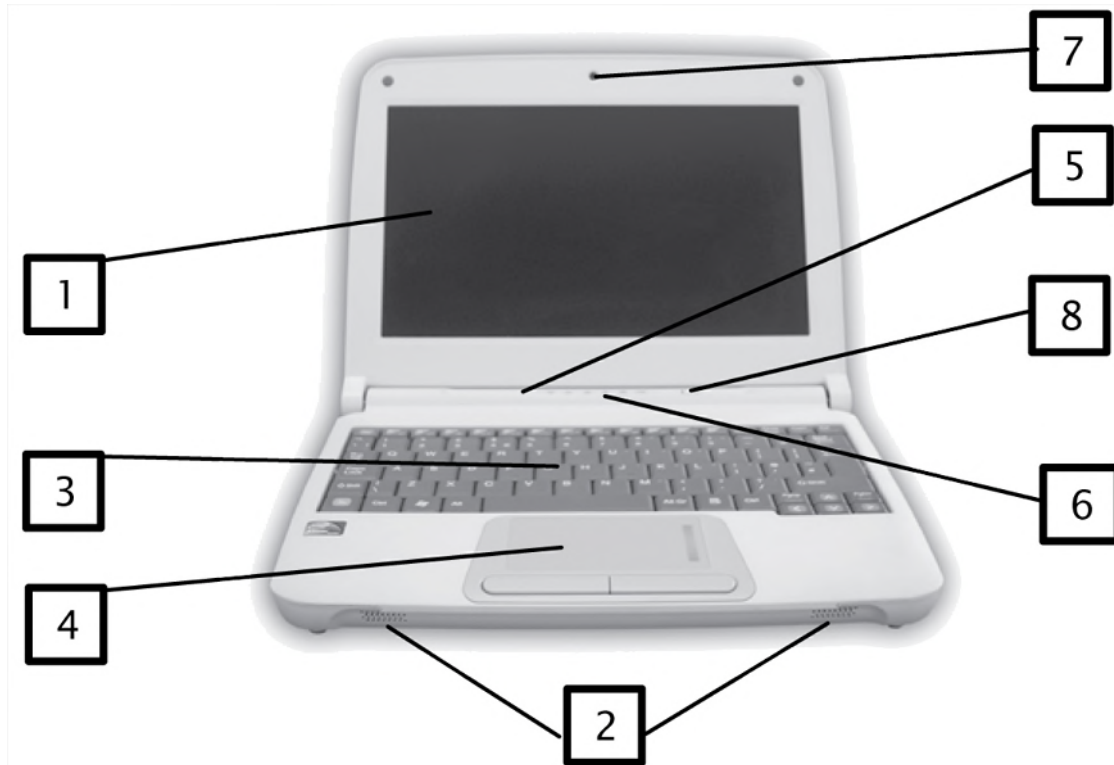


Nunca apague su equipo mientras el disco rígido esta en uso. Podría resultar en pérdida o destrucción de datos. Siempre aguarde un mínimo de 6 segundos después de apagar su equipo antes de encenderlo de nuevo o moverlo. Encender y apagar en sucesiones rápidas puede dañar el circuito eléctrico del equipo.



## A.3. Introducción al uso de la netbook

### A.3.1. Vista de frente



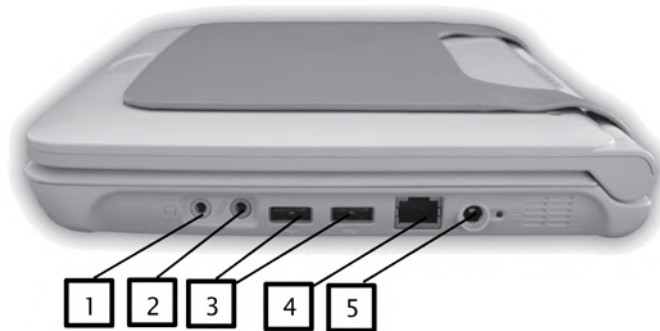
1. **Display LCD:** Los contenidos del sistema operativo son expuestos aquí.
2. **Parlantes stereo:** Los parlantes stereo permiten la salida de sonido.
3. **Teclado:** Utilice el teclado para introducir la información.
4. **Touch-Pad:** Utilice el Touch-Pad y los dos botones como un Mouse.
5. **Micrófono:** El micrófono incorporado permite que su netbook reciba audio de entrada.
6. **Indicadores LED de Status:** El estado operacional de su netbook se muestra aquí.
7. **Cámara:** Use esta cámara para cualquier aplicación de vídeo conferencia
8. **Botón Interruptor/Suspensión:**
  - Oprima momentáneamente para encender el sistema.
  - Oprima y sostenga por lo menos 4 segundos para apagar el sistema.
  - Oprima el botón Interruptor/Suspensión otra vez para volver al modo suspensión.
  - Luz azul persistente indica ENCENDIDO.

### A.3.2. Vista izquierda



1. **Puerto para Monitor Externo:** Utilice este puerto para conectar un monitor externo.
2. **Puerto USB:** Utilice este puerto para conectar dispositivos de Bus Serial Universal (USB – “Universal Serial Bus”). El puerto está preparado para la v2.0 del USB estándar.
3. **Ranura para Tarjeta de Memoria:** Inserte una tarjeta de memoria en la ranura para la lectura de datos guardados en las mismas.
4. **Ranura de Seguridad Kensington:** Permite la inserción de la traba de seguridad Kensington para sujetar su Exomate a una superficie.

### A.3.3. Vista derecha



1. **Conector de Auriculares:** Utilice la toma de auriculares para conectar un auricular externo.
2. **Conector de Micrófono:** Utilice la toma de micrófono para conectar un micrófono externo.
3. **2 Puertos USB:** Utilice estos puertos para conectar dispositivos de Bus Serial Universal (USB – “Universal Serial Bus”). Los puertos están preparados para la v2.0 del USB estándar.
4. **Conector RJ45:** Utilizado para placa de red.
5. **Adaptador de Corriente:** Conecte su adaptador de CA (Corriente Alterna) a este puerto para cargar la batería de su netbook. Luz azul indica pila completamente cargada.



### A.3.4. Vista posterior



1. **Puerto de la Batería:** La batería es guardada aquí.
2. **Interruptor de Bloqueo de Batería:** Utilice el interruptor de bloqueo de la batería para calzarla en el Puerto de la Batería.
3. **Pestillo de Liberación de la Batería:** Utilice el Pestillo de Liberación de la Batería para liberar la misma de su puerto.
4. **Apertura de Ventilación:** La apertura de ventilación permite que la netbook se enfríe y previene el sobrecalentamiento de la misma. No bloquear esta apertura cuando la netbook está encendida.

### A.3.5. Indicadores de LED status



Luz azul indica que el Bloq-Num está activado.



Luz azul indica que el Bloq-Mayus se encuentra Activado.



Luz azul indica que el sistema se encuentra leyendo/escribiendo.

**Información: Nunca apague su equipo mientras el disco rígido está en uso.**



Luz azul indica que el sistema esta encendido.



Una luz verde indica que la batería se encuentra completamente cargada o que el cargador está conectado.

Una luz naranja indica que la batería se está cargando.

Una luz parpadeante de color naranja indica que la batería tiene poca carga. Cuando no hay luz implica que la batería no está instalada en la netbook.





















Luz verde -> Of -> Luz naranja -> Of -> Luz verde, indica que la temperatura de la batería es demasiado Alta.



Luz AZUL parpadeante indica que una operación WLAN está en proceso.


Luz AZUL encendida indica que el WLAN se encuentra encendido.

### A.3.6. Los controles de función (hot key)

Acción	Función
 + 	Enciende / Apaga la placa de red inalámbrica.
 + 	Entra en modo de suspensión.
 + 	Mudo / Sonido – Audio no mudo / bip PC
 + 	Disminuye el volumen del altavoz.
 + 	Incrementa el volumen del altavoz.
 + 	Cambia el modo de pantalla: Solo LCD, solo CRT y LCD&CRT.
 + 	Disminuye el nivel de brillo.
 + 	Incrementa el nivel de brillo.
 + 	Desactiva módem 3G
 + 	Bloqueo de Pad de Mouse

### A.3.7. Teclado

Algunas teclas en su netbook tienen un tercer símbolo en la parte inferior derecha de la tecla.

Por ejemplo:  Dicho símbolo se utiliza manteniendo presionada la tecla AltGr que se encuentra en su teclado a la derecha de la barra espaciadora.

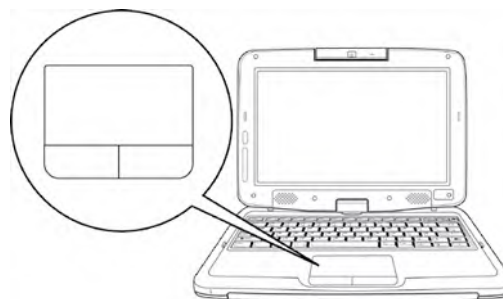
Por ejemplo: Para hacer el símbolo @ presionar AltGr+”Q”  
Para hacer el símbolo \ presionar AltGr+”?”

También encontrará teclas que tienen algún símbolo dibujado en color. Dichos símbolos se utilizan manteniendo presionada la tecla Fn que se encuentra en la parte inferior izquierda de su teclado.

Por ejemplo: Para subir el brillo de su pantalla , presionar Fn + F8  
Para subir el volumen de audio, presionar Fn + F5

### A.3.8. Pad de mouse

El mouse trabaja como cualquier otro mouse de escritorio, solo debe apoyar el dedo y deslizarlo hacia la dirección deseada. Los botones derecho e izquierdo del mouse tienen las mismas funciones de un mouse de escritorio.



### A.3.9. Batería

Con la Batería cargada e instalada usted puede usar su Netbook sin estar conectado a la red eléctrica, aunque lo más conveniente es usarla conectada a la red eléctrica.

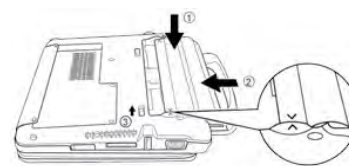
#### Colocación de la batería

1. Deslice la batería dentro de la bahía.
2. Presiónela suavemente pero con firmeza hasta que el pestillo se trabaje en su lugar.



#### Procedimiento para remover la batería

1. Mueva el interruptor de bloqueo de la batería hacia la derecha.
2. Mueva el pestillo de liberación de la Batería hacia la izquierda y remueva la batería de la Netbook.



### A.3.10. Como limpiar su equipo

Antes de comenzar cualquiera de los procedimientos aquí descriptos, siga las instrucciones y advertencias de Seguridad de este manual.

**PRECAUCIÓN:** Antes de limpiar el equipo, desconecte el adaptador eléctrico del toma corriente, desconecte el equipo del adaptador y extraiga la batería instalada.

- Limpie el equipo con un paño suave humedecido con agua. No utilice limpiadores en aerosol o líquidos, que podrían contener sustancias inflamables. Nunca aplique agentes limpiadores directamente sobre el equipo y no utilice limpiadores volátiles (destilados

del petróleo) o abrasivos. Utilice únicamente productos diseñados específicamente para la limpieza de equipos y pantallas informáticas, y siga las instrucciones incluidas con el producto.

- Utilice un bote de aire comprimido para forzar la salida al exterior del polvo acumulado entre las teclas del teclado y para eliminar cualquier resto de suciedad de la pantalla.
- Humedezca un paño suave y sin pelusa con agua o un agente limpiador especial para pantallas. No utilice alcohol ni soluciones a base de amoníaco. Limpie cuidadosamente la pantalla, desde el centro hasta los bordes, hasta haber eliminado todo resto de suciedad y huellas dactilares. No ejerza una presión excesiva sobre la pantalla. No permita que el agua contenida en el paño se filtre entre la pantalla y el marco.
- Humedezca un paño suave y sin pelusa con agua y limpie el ordenador, el teclado y el Pad de Mouse. No permita que el agua contenida en el paño se filtre entre el Pad de Mouse y el apoyamanos que lo rodea.

## A.4. Funcionamiento de la batería

El funcionamiento de la batería puede variar de acuerdo con las condiciones de uso. Su batería podría tener una menor duración si utiliza programas que demanden un alto consumo de energía o ha seleccionado la opción de alto brillo o utiliza dispositivos inalámbricos o USB.

Asegúrese de que la batería que utiliza sea compatible con la original de fábrica. De no hacerlo, podría ocurrir un incendio o explosión. Para mayor información sobre la compra de baterías compatibles, contacte a su proveedor.



Las baterías nunca deben ser desechadas junto con los residuos domésticos. Consulte con la Secretaria de Medio Ambiente o Desecho de Residuos de su ciudad respecto a la eliminación de baterías de litio-ion usadas.

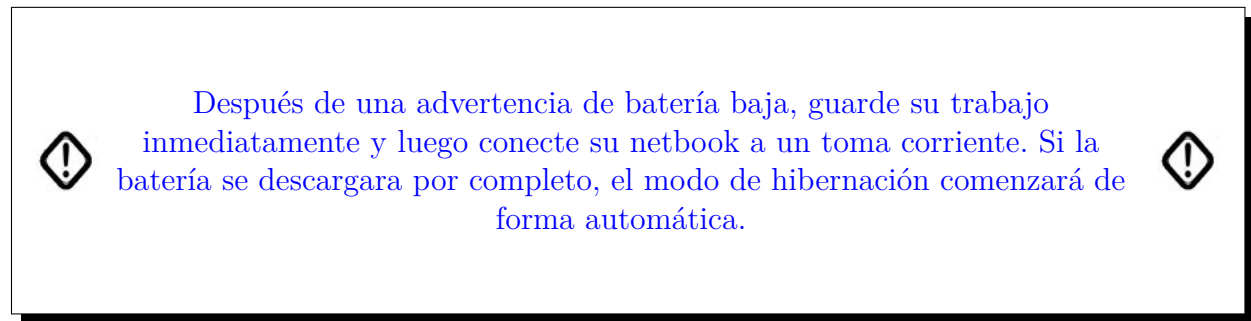
### A.4.1. Control de la carga de la batería

Estado de la batería	Funcionamiento del indicador
Cargando	Ámbar intenso
Completamente cargada	Verde intenso
Descargando	Apagado
Muy baja	Ámbar titilante > aproximadamente 3 minutos restantes; el sistema emite un sonido.

## A.4.2. Medidor de potencia

El medidor de potencia indica la carga de energía restante. Cuando su netbook funciona con la energía de la batería, puede verificar la carga restante haciendo doble clic en el ícono de la barra de tareas.

## A.4.3. Advertencia de batería baja



Escuchará la advertencia de batería baja cuando la misma esté descargada en un 90 por ciento. Si no conectara su netbook a una fuente de energía alternativa durante este lapso, se producirá un sonido reiterado. Si la batería se descargara considerablemente, su netbook entrará en modo de hibernación de forma automática.

## A.4.4. Preparación de la batería para el uso (calibración)

Antes de usar la batería por primera vez, la batería debe ser calibrada con el fin de obtener informes precisos del estado de la batería.

Para calibrar la batería siga las siguientes instrucciones:

1. Insertar la batería en el compartimento de la batería y encender su netbook. Si la batería está completamente sin energía ir al siguiente paso. De lo contrario, dejar que la batería se descargue hasta que la alarma de batería baja emita sonidos de aviso. El sistema entrará automáticamente en modo de suspensión.
2. Apagar su netbook. Conectar el adaptador de A/C y dejar que la batería se recargue completamente. Cuando el indicador de carga de la batería se apaga, la batería está completamente cargada.
3. Encender su netbook, y dejar que la batería se descargue hasta que la alarma de batería baja emita sonidos de aviso. El sistema entrará automáticamente en modo de suspensión. Ahora conectar el adaptador de A/C para recargar la batería.
4. La batería está calibrada correctamente.

Esta operación realizada cada mes ayudará con el correcto control de la capacidad de la batería. En toda otra ocasión es perjudicial dejar que la batería agote su carga.

La batería se cargará si falta carga y si su netbook está conectada a la corriente eléctrica mediante su adaptador. No se cargará si estuviera demasiado caliente, ya sea por el uso

o por la temperatura ambiental. Si esto ocurriera, el indicador de batería emitirá una luz ámbar. Desconecte la netbook y permita que la batería adopte la temperatura ambiente. El indicador de batería también emitirá una luz ámbar si la batería está dañada y necesita ser reemplazada.

#### **A.4.5. Carga de la batería**

Una batería descargada en su totalidad debe conectarse a un toma corriente entre 3 y 6 horas (dependiendo de si su netbook está encendida o no y qué programas se están ejecutando). Puede dejar la batería en su netbook cargando tanto tiempo como desee. El circuito interno de la batería evita su sobrecarga, pero evite que su temperatura supere los 50° C.

#### **A.4.6. Almacenamiento de la batería**

En caso de que su netbook deba permanecer guardada durante un lapso prolongado, es conveniente que la batería quede a media carga, extraiga la batería y guárdela en un lugar fresco. Cargue la batería por completo antes de usar la netbook nuevamente.

#### **A.4.7. Funcionamiento con baterías adicionales**

Si pasa mucho tiempo viajando y usando su netbook sin que esté conectada a un toma corriente, sería conveniente que llevara baterías adicionales a fin de que pueda reemplazarlas rápidamente sin que la batería se descargue y así poder seguir trabajando. Debe alternar el uso de las baterías adicionales.

#### **A.4.8. Maximización de la vida de la batería**

Es posible recargar una batería numerosas veces, pero transcurrido un tiempo, perderá su capacidad de mantener la carga. A fin de maximizar la vida de la batería:

- Siempre que pueda, utilice su netbook conectada con el adaptador de corriente.
- No deje que la batería se descargue totalmente.
- Evite el calor. pues deteriora las células de ión-litio. Por eso no la deje en lugares calientes o dentro de un auto expuesto a la luz del sol. Encendida encima de camas, lugares blandos o sobre las piernas del usuario es perjudicial, ya que tapa las zonas de ventilación. La humedad también es nociva para la netbook, evite los lugares húmedos. Lo ideal es que la netbook se mantenga lo más cerca posible de los 22°C - a temperatura ambiente -, pero su uso entre los 10°C y los 35°C también es aceptable. Las baterías de Litio-ion son insumos y proveen unos 500 ciclos de carga/descarga completos a una temperatura ambiente de 25° C dependiendo de los patrones de uso. Con el correr del tiempo y la acumulación de ciclos de carga/descarga se va produciendo una disminución en la capacidad de almacenamiento de energía que se considera normal en este tipo de insumos. Las cargas y descargas parciales se suman hasta totalizar un ciclo completo.

## A.5. Recuperación de Sistema

### A.5.1. Recuperación de sistema Exomate

**Recomendación para los usuarios:** Se recomienda generar el pen drive de restauración para su equipo, que volverá a su equipo al estado actual o inicial en caso de necesitarlo.

Para esto debe tener un pen drive de al menos 8GB sin información útil almacenada en su interior, puesto que durante la preparación del proceso de restauración borrará el contenido de su pen drive. El proceso de restauración consta de 3 Instancias y un opcional.

- A) Generación de pen drive para la recuperación
- B) Copia de Backup del sistema inicial
- C) Sistema de Restore (Recuperación al estado inicial)
- D) Creación de imagen personalizada

**Nota:** Si usted realizara modificaciones en el equipo que desee incluir en una imagen personalizada como se menciona en el punto (D) le recomendamos que se base siempre en un equipo con la restauración inicial (B) recién instalada, de esa manera garantizará que parte de una imagen sin errores de configuración, virus, archivos temporales, etc.

#### A) Generación de pen drive para la recuperación

**Requisitos para el proceso:**

- Pen drive de al menos 8GB sin información útil en su interior.

**Proceso:**

Dentro del sistema operativo Microsoft Windows XP de su Exomate:

1. Insertar pen drive en su Exomate.
2. Debe dirigirse al botón de “Inicio” y presionar clic izquierdo sobre el mismo.
3. Debe presionar clic izquierdo sobre el menú “Todos los programas” luego sobre el menú con el nombre “Intel(R) Education Administrator” y por ultimo sobre el aplicativo “USB Generation Tool” Aparecerá una nueva ventana de trabajo con el nombre: “Intel(R) Education Administrator USB Generation Tool”
4. Debe presionar clic izquierdo sobre el botón de acción con el nombre “Generar memoria USB de Recuperación” a la izquierda de su pantalla.
5. Debe presionar clic izquierdo sobre el botón de acción con el nombre “Generar memoria USB de recuperación” que aparece abajo a la derecha.
6. Seleccione en el menú de la izquierda el dispositivo a utilizar y luego presionar “Generar”. Posterior a la acción del paso anterior, aparecerá en pantalla una ventana emergente dando aviso que si continua con este procedimiento toda la información almacenada en su pen drive será eliminada. Por favor seleccione la opción “Si” para continuar el proceso. Este proceso puede tardar varios minutos, espere a que finalice el proceso sin apagar ni reiniciar el equipo.

7. Debe presionar clic izquierdo sobre el botón “Aceptar” y cerrar la ventana actual de trabajo para finalizar el presente proceso.

## **B) Copia de Backup del sistema inicial**

Una imagen del sistema tal y como se encontraba cuando salió de fábrica está ubicada en el servidor escolar de la institución educativa. Usted puede utilizar esta imagen cada vez que desee volver al estado inicial del equipo aunque no haya realizado backups anteriormente.

Para ello siga estas instrucciones:

1. Realice el paso (A) completo.
2. Inserte el Pen Drive generado en el paso anterior en el servidor escolar y copie la carpeta “IEA” que se encuentra en la carpeta personal del usuario administrador dentro de la subcarpeta “Backup Exomate” directamente dentro del pen drive.
3. Asegúrese de que la carpeta quede marcada como de “solo lectura”.
4. Ahora para recuperar un sistema en cualquier Exomate siga los pasos mencionados en (C).

## **C) Sistema de Restore (Recuperación de las que luego desee hacer backup al estado inicial)**

El sistema de Restore recuperado el estado de la copia de información generada al momento de utilizar el pen drive junto al sistema de backup. Incluye a los sistemas operativos Windows y Linux, las aplicaciones instaladas y datos de usuario.

**Requisitos para el proceso:**

- Pen drive configurado en el punto B) SISTEMA DE BACKUP (COPIA DE INFORMACIÓN)

**Proceso:**

1. Insertar pen drive en su Exomate
2. Debe reiniciar su equipo y presionar en reiteradas oportunidades la tecla F11 para ingresar al menú de inicio (Boot Menu) de su Exomate
3. Seleccionar la opción de su dispositivo USB en el menú de inicio (Boot Menu) utilizando las teclas de desplazamientos (↑↓). Por ejemplo USB HDD: {Marca/ modelo del dispositivo USB} - Presionar la tecla “Enter” para confirmar su selección.
4. Debe presionar clic izquierdo sobre el menú “Restauración de Sistema” a la izquierda de la nueva ventana de trabajo, luego presionar clic izquierdo sobre el de botón de acción “Restaurar” para iniciar el proceso de recuperación sobre su Exomate. Posterior a la acción del paso anterior, aparecerá en pantalla una ventana emergente dando aviso que si continua con este procedimiento toda la información almacenada en su Exomate será eliminada. Por favor seleccione la opción “Si” para continuar el proceso. Este proceso puede tardar varios minutos, espere a que finalice el proceso sin apagar ni reiniciar el equipo. El proceso mostrará en pantalla una nueva ventana indicando que la restauración se ha completado.



5. Debe quitar su dispositivo USB y presionar clic izquierdo sobre el botón de acción “Si”.

Su Exomate se reiniciará automáticamente, dando por finalizado el presente proceso.

EL EQUIPO QUEDARÁ EN EL ESTADO DEL MOMENTO EN QUE SE REALIZÓ EL SISTEMA DE BACKUP.

## **D) Creación de imagen personalizada**

El sistema de backup, genera una copia completa en el pen drive del estado actual del equipo. Incluye a los sistemas operativos Windows y Linux, las aplicaciones instaladas y datos de usuario.

### **Requisitos para el proceso:**

- Pen drive configurado en el punto A) GENERACIÓN DE PEN DRIVE PARA LA RECUPERACIÓN

### **Proceso:**

Dentro del sistema operativo Microsoft Windows XP de su Exomate.

1. Insertar pen drive en su Exomate.
2. Debe reiniciar su equipo y presionar en reiteradas oportunidades la tecla F11 para ingresar al menú de inicio (Boot Menu) de su Exomate.
3. Seleccionar la opción de su dispositivo USB en el menú de inicio (Boot Menu) utilizando las teclas de desplazamientos (↑↓). Por ejemplo USB HDD: {Marca/ modelo del dispositivo USB} - Presionar la tecla “Enter” para confirmar su selección.
4. Debe presionar clic sobre el botón “Copia de Seguridad del sistema” a la izquierda de la pantalla para iniciar el proceso de copia de la información almacenada en el disco del equipo, y luego clic sobre el botón “Copia de Seguridad”. Este proceso puede tardar varios minutos, espere a que finalice el proceso sin apagar ni reiniciar el equipo. El proceso mostrará en pantalla una nueva ventana indicando que el backup se ha completado.
5. Debe quitar su dispositivo USB y presionar clic izquierdo sobre el botón de acción “Si”.

Su Exomate se reiniciará automáticamente, dando por finalizado el presente proceso.

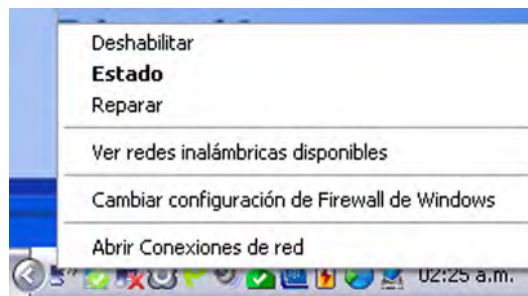
En caso de querer restaurar la imagen personalizada creada se deberá seguir las instrucciones del punto (C).



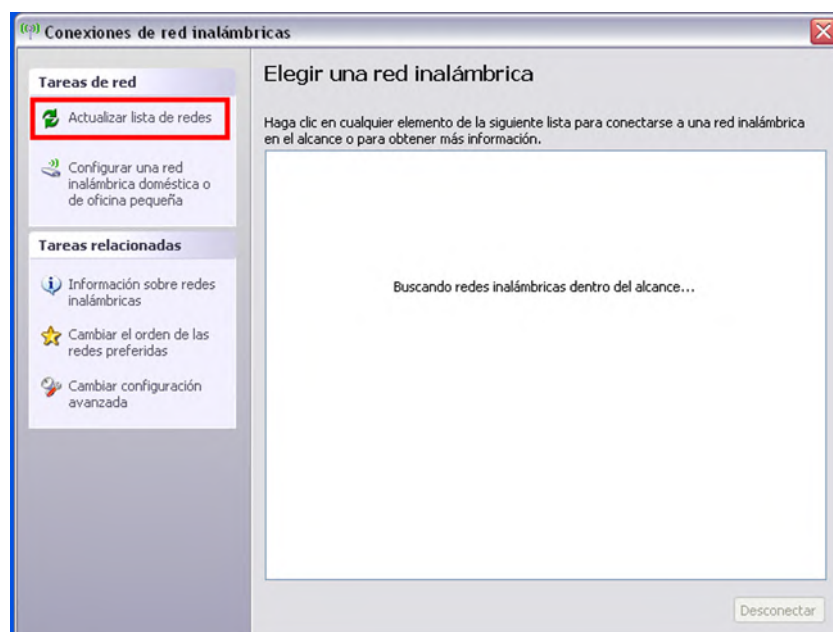
## B. Configuración de la Conexión Wireless para Exomate

### B.1. Configuración de la Conexión Wireless en Windows

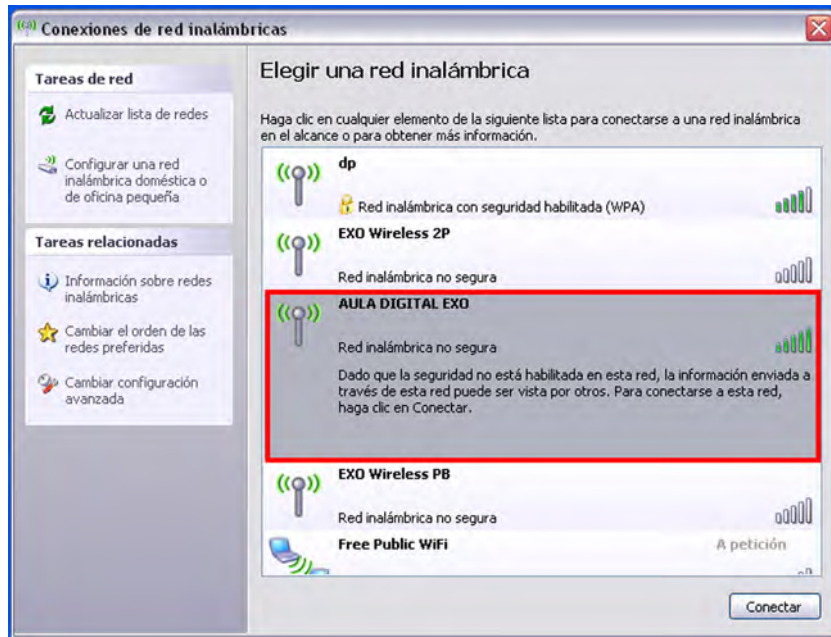
1. Verificar que el modulo de WLAN se encuentre activo (El ícono de Wireless en el panel de luces debe encontrarse azul). Si este no se encuentra activo, presione simultáneamente las teclas Fn y F1.
2. Haga Clic derecho sobre el ícono de **Conexiones de redes Inalámbricas** en el sector derecho de la barra de tareas y seleccione con un clic la opción **Ver redes inalámbricas disponibles**.



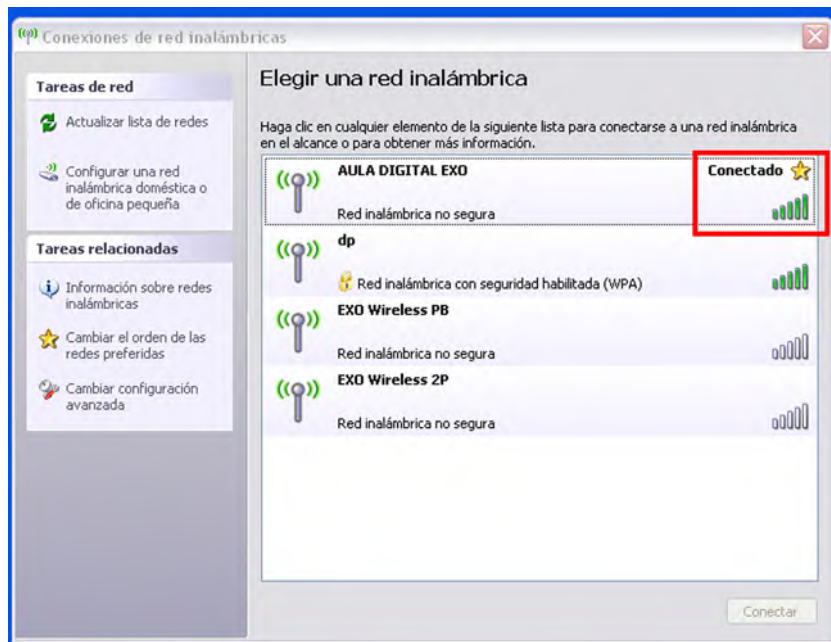
3. Cuando aparezca la ventana de “Conexiones de redes Inalámbricas” haga Clic en **Actualizar lista de redes** para buscar las redes disponibles.



4. La red inalámbrica con el nombre que usted busca aparecerá en pantalla. Haga doble clic sobre ella.



5. Cuando el equipo esté conectado a la red, aparecerá el mensaje de “conectado” por arriba del indicador de señal que posee la misma.



## C. Resguardo y recuperación del sistema de Exomate

!!!ADVERTENCIA!!!

Este proceso Formateará el Pendrive para generar el sistema de recuperación por lo que todos los datos del mismo serán eliminados. Por favor tome las medidas para que no se pierde información valiosa.

### C.1. Resguardo y recuperación del sistema utilizando un dispositivo USB de almacenamiento

Los estudiantes y administradores pueden utilizar la aplicación USB Generation Tool para crear un resguardo del sistema o recuperar el mismo.

#### C.1.1. Generar memoria USB de Recuperación

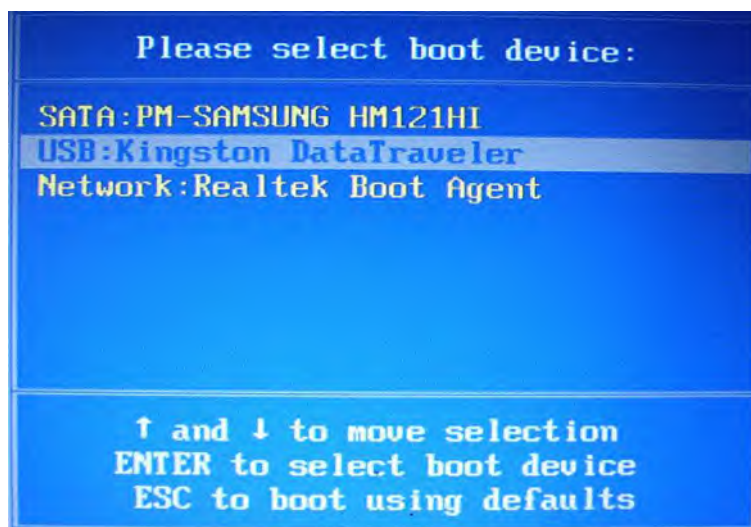
1. En la Exomate, haga doble clic sobre el ícono de **USB Generation Tool** en el escritorio o ejecútelo desde **Inicio -> Todos los Programas -> Intel -> Intel Learning Series -> Intel® Education Administrator -> USB Generation Tool**.



2. Inserte el dispositivo USB en la Exomate.
3. Desde la ventana principal de USB Generation Tool Seleccione la opción **Generar memoria USB de Recuperación** y haga clic sobre **Generar memoria USB de Recuperación**.

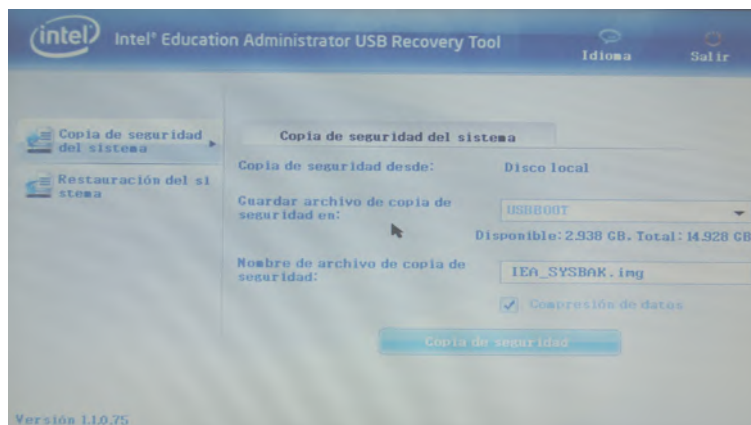
### C.1.2. Iniciar una Exomate desde una memoria USB de Recuperación

1. Inicie la Exomate desde la memoria USB generada anteriormente:
  - Apague el Equipo e inserte el USB de Recuperación.
  - Encienda la Exomate y presione **F11** para entrar al menú de Arranque.
  - Seleccione el arranque desde la memoria USB de recuperación.



### C.1.3. Copia de seguridad del sistema

1. Cuando inicie USB Recovery Tool, seleccione la solapa **Copia de seguridad del sistema**.



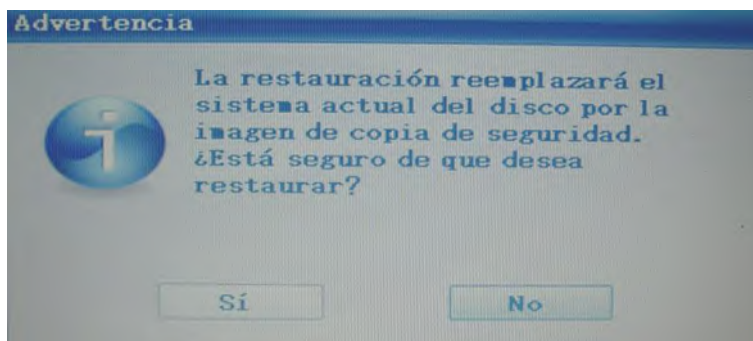
2. Modifique el nombre del archivo y presione el botón **Crear copia de seguridad**.

### C.1.4. Restauración del sistema

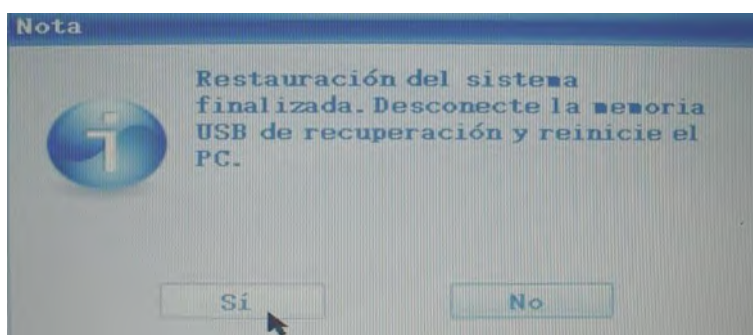
1. Cuando inicie USB Recovery Tool, seleccione la solapa **Copia de seguridad del sistema**.
2. Seleccionaremos el archivo de imagen y haremos clic sobre el botón **Restaurar**.



3. Antes de comenzar con la restauración de la imagen el programa lanzara una Advertencia, esta indica que los datos que se encuentren en el equipo serán borrados.



4. Para terminar con el proceso quitaremos el medio USB y presionaremos sobre el botón **Si** para que el equipo se reinicie y podamos acceder al sistema recuperado.



5. Modifique el nombre del archivo y presione el botón **Crear copia de seguridad**.





## D. e-Learning Class - Tutorial para el Docente

El propósito de esta guía es proporcionar un apoyo al profesor para el uso en el aula de la Exomate. Esta guía le proporcionará apoyo técnico, ideas para sus lecciones y ayuda en el uso del Programa e-Learning Class (Maestro) del Profesor y apoyo para los programas de los alumnos en cada Exomate.

Exomate está diseñada para que el profesor la use de inmediato. El Programa Maestro deberá estar instalado en la computadora del profesor. Este programa le permitirá monitorear fácilmente y dar apoyo a las computadoras de los alumnos, haciendo posible una positiva y productiva interacción con sus alumnos mientras usan sus netbooks en clase.

Las capacidades del software de e-Learning Class incluyen:

- Las computadoras tanto del profesor como de los alumnos cuentan con tecnología inalámbrica para que puedan “verse” entre ellos en forma virtual y conectar las computadoras entre si para crear un aula virtual en red.
- Los profesores pueden monitorear en forma remota o controlar las pantallas de los alumnos, asegurándose de esta manera que el alumno está trabajando, y que está seguro y productivo durante clase.
- Los profesores pueden en forma temporal desactivar las computadoras de los alumnos si así lo desean para tener la atención de éstos en tareas que no requieren computadora.
- Los profesores pueden compartir el contenido de su pantalla con los alumnos o enviar material multimedia a sus computadoras.

## D.1. Prerrequisitos del tutorial

Con el propósito de obtener el máximo provecho de esta guía, usted deberá configurar una pequeña aula “virtual” comprimida en una Exomate o en su propia laptop. Esto le permitirá practicar las características de estas computadoras antes de introducir a los alumnos en el uso de las mismas. Será necesario contar con lo siguiente para poder configurar esta pequeña aula:

- Necesita una PC del Profesor y al menos una Exomate.
- Instale el software e-Learning Class del Profesor en la PC del profesor.
- Las Exomates deben tener ya instalado el e-Learning Class, por tanto no será necesario que usted lo instale a menos que la versión instalada no sea compatible con la versión del profesor.
- Tanto la computadora del Profesor como las unidades Exomate deben estar conectadas a la misma red.
- Tanto la computadora del Profesor como las unidades Exomate deben estar conectadas a la red mediante el mismo método (ya sea que ambas estén conectadas con cable o ambas estén conectadas en forma inalámbrica).

## D.2. Iniciando una Clase Virtual

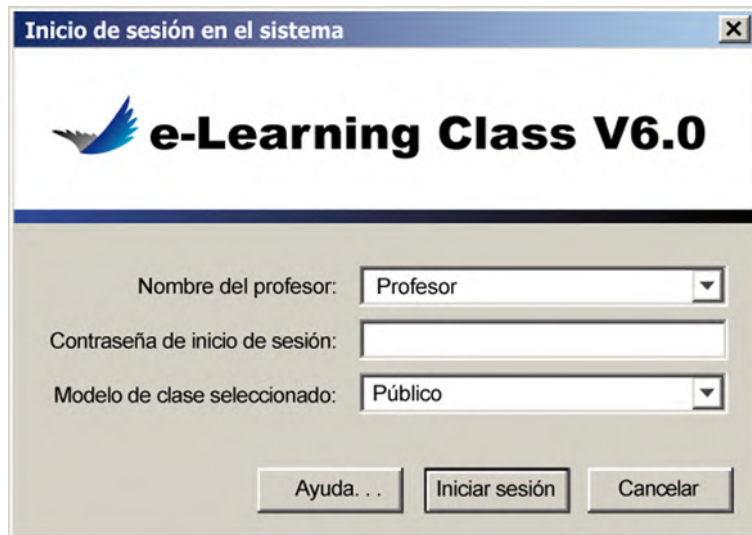
### D.2.1. Creación de un aula virtual

El software e-Learning Class le permite crear un ambiente seguro y comprometido en su aula. Sus alumnos podrán usar sus computadoras para ingresar información, para colaborar entre ellos, para ver materiales en su computadora y crear sus propios materiales que demuestren su entendimiento.

- El aula virtual se maneja desde la computadora del profesor.
- El aula virtual (también llamada clase modelo) inicia cuando usted ingresa y termina hasta que usted sale del sistema.
- Un aula virtual requiere de al menos un alumno activo conectado al sistema para que puedan trabajar la mayoría de las funciones e-Learning.

#### Pasos para crear un aula virtual:

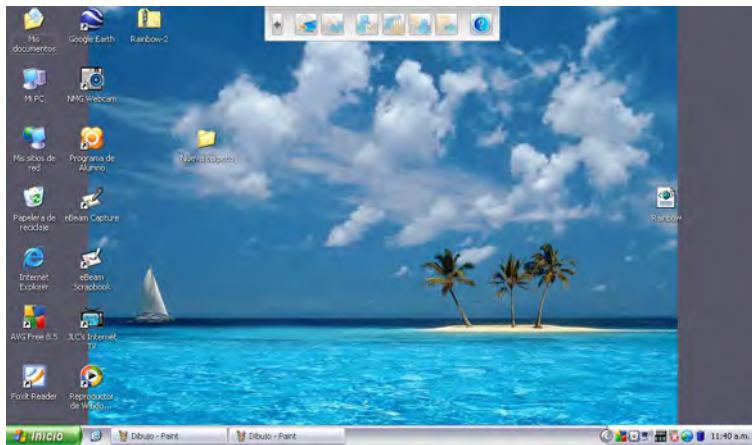
1. Inicie el Programa Maestro dando clic en el objeto en su pantalla.
  - Se accede vía acceso de escritorio directo
  - Se accede vía Menú Inicio - Programa (**Inicio -> Mythware -> e-Learning Class -> Programa Maestro**)
2. **IMPORTANTE:** La primera vez que usted abre el programa usted deberá poner su nombre y una contraseña en el sistema. Este nombre será visible para sus alumnos, por tanto use uno que ellos reconozcan, por ejemplo Sra. Morales).
  - La primera vez que ingrese al software también estará creando una contraseña para el software, esto le asegurará que nadie excepto usted pueda entrar al sistema.
  - Seleccione una contraseña que pueda recordar con facilidad, pero que a la vez no sea demasiado obvia para sus alumnos.
  - Se le pedirá que ingrese la contraseña de profesor cada vez que entre al sistema. Tome en cuenta que cuando usted ingresa su contraseña, aparecerá un asterisco en el campo contraseña, por tanto, asegúrese de teclear con cuidado la contraseña correcta.
3. Ingrese a la clase virtual



Una vez que se haya usted identificado, se habilitará el botón **Iniciar sesión** (login)

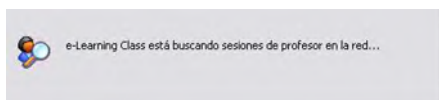
## D.2.2. Conecte las Exomate's a la computadora del profesor

e-Learning Class está pre-instalado en la Exomate.

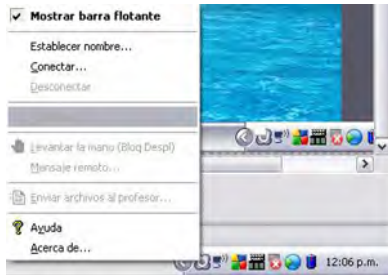


Si el ícono e-Learning de la barra de tareas está activado, indica que la Exomate está lista para unirse al aula virtual. La Exomate se unirá usando uno de dos métodos dependiendo de si el profesor ha iniciado o no la clase virtual en el momento en que el alumno se conecta a la red.

**Método Automático:** El profesor ha iniciado una clase virtual antes de que el alumno se conecte a la red

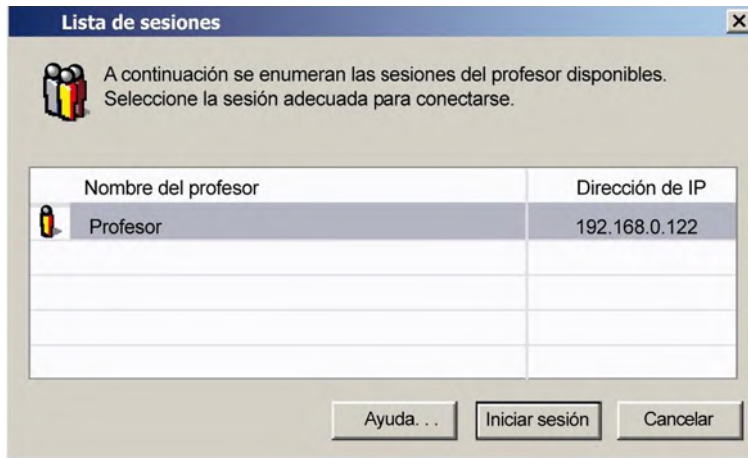


1. Conectarse a la red
2. e-Learning Class buscará al profesor en forma automática y desplegará la siguiente ventana emergente en el escritorio del alumno.
3. Se desplegará la lista de profesores



**Método Manual:** El profesor aún no ha iniciado la clase virtual cuando el alumno se conecta a la red.

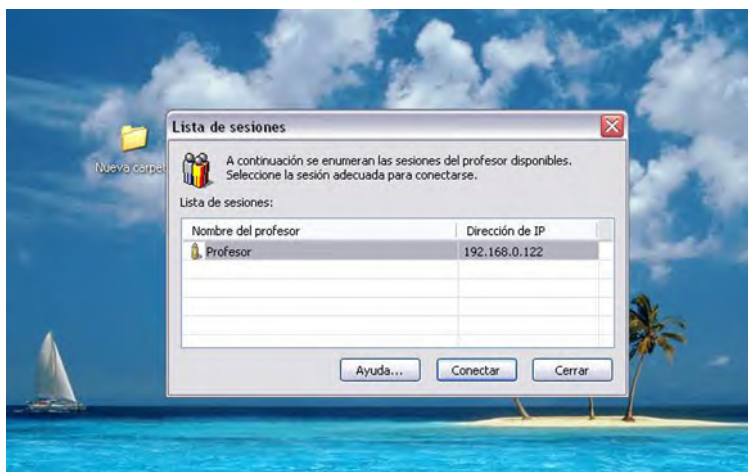
1. Clic derecho en el ícono e-Learning Class localizado en la barra de tareas.
2. Seleccione Conectar
3. Se desplegará la lista de profesores.



El nombre del profesor es el nombre de ingreso del profesor

### D.2.3. Conectando a un Alumno a una Clase Virtual

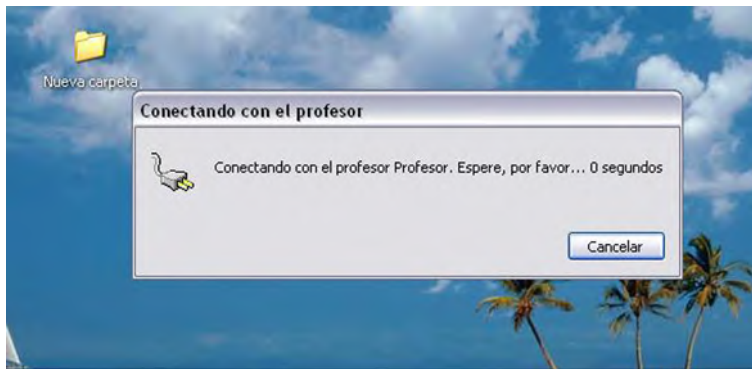
Después de detectar uno o más profesores en la lista de profesores, el alumno deberá especificar a que clase desea conectarse.



1. Elija el profesor que desea y presione Conectar  
Cada profesor especificó un nombre cuando ingresaron a sus respectivas



2. Ingrese un nombre de alumno y presione OK para intentar unirse a la clase virtual del profesor virtual classroom. Cada alumno debe proporcionar su nombre para ingresar en la clase virtual. Todos los nombres de los alumnos se deben guardar para futuras sesiones.



3. Espere a recibir la aprobación del profesor.



**Nota:** La aprobación del Profesor es un paso que se realiza una sola vez. Después de la primera vez, el alumno podrá unirse a las clases virtuales sin necesidad de pedir autorización.

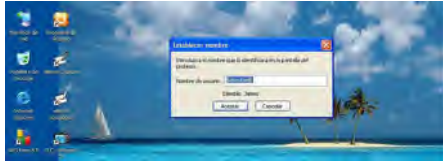
#### D.2.4. Otorgar a un Alumno el Acceso al Aula Virtual

El profesor identifica a los alumnos que pertenecen a sus clases virtuales. Utilizan e-Learning Class para otorgarles el acceso a su aula virtual.

La primera vez que un alumno trata de conectarse a su clase virtual, se considera usuario no identificado, por tanto se le solicita que se registre. Usted podrá interactuar únicamente con aquellos alumnos que estén registrados en su clase, por fortuna, el registro se hace únicamente una vez y en el futuro los alumnos registrados ingresarán en su clase en forma automática.

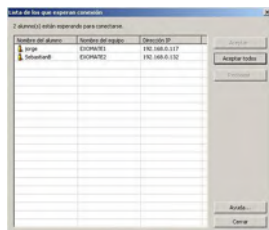
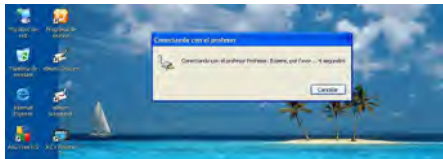
### En la Exomate (alumno)

1. Teclee su nombre y presione OK
2. Una ventana emergente aparecerá para notificar al alumno que se está en espera de la aprobación del profesor.
3. Una vez que el profesor autoriza la entrada del alumno, su Exomate se unirá a la clase virtual y el color de la pantalla del ícono que aparece en su barra de tareas cambiara de negro a azul para indicarle al alumno que está conectado a la computadora del profesor.
4. El alumno puede continuar trabajando en su Exomate.



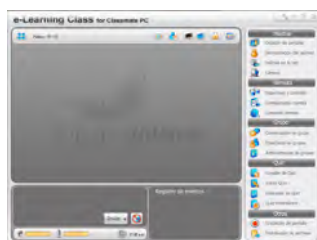
### En la pantalla del profesor

1. Los alumnos deben unirse al aula virtual para iniciar su proceso de aprendizaje
2. Una ventana emergente le notificará cuando un alumno se une por primera vez a su clase virtual.
3. Una vez que el alumno ha sido aceptado en su clase, un pequeño ícono lo identificará en el panel. En este punto, usted ya puede interactuar con ellos.



### En la pantalla del profesor

Puede aceptar o rechazar a más de un alumno al mismo tiempo



### En la pantalla del profesor

El alumno está en línea y listo para aprender

## D.3. Comprendiendo el Panel de e-Learning Class

### D.3.1. Panel de e-3.1 e-Learning Class



1. **Modelo de Clase:** Despliega los usuarios de Exomate que están registrados como alumnos de su clase virtual
2. **Ícono de status del alumno:** Indica aquellos alumnos que están conectados a su clase virtual y le indica el status de cada uno mediante el color del ícono.
3. **Bloquear/desbloquear alumnos:** Permite a los alumnos de su Modelo de Clase conectarse automáticamente a su clase virtual una vez que usted ha ingresado a ésta. Los alumnos no se podrán desconectar de su computadora si están bloqueados.
4. **Configuración de grabación:** Controla el volumen de su micrófono en la clase virtual de e-Learning Class
5. **Configuración de reproducción:** Controla el volumen de reproducción del software e-Learning Class
6. **Ingreso a eventos:** Despliega los eventos, quien es el responsable de cada uno y cuando ocurrieron
7. **Barra de mensaje remoto:** Envía mensajes en pantalla a alumnos que estén en línea
8. **Barra de función:** Le permite interactuar con alumnos en línea.



### D.3.2. Barras de herramientas de e-Learning Class

#### Barra de función

Disponible en el panel de e-Learning Class

Le permite crear y apoyar actividades de aprendizaje significativas para sus alumnos.



### Barra flotante

Disponible en: Esta barra de herramientas se encuentra en la parte superior derecha del escritorio del profesor y es visible únicamente cuando se minimiza la ventana de e-Learning Class. Esta barra de herramientas le permite realizar otros trabajos en su computadora mientras sus alumnos están ocupados aprendiendo. Al igual que la barra de funciones, le permite interactuar con alumnos que estén en línea en su clase virtual, manejando actividades pedagógicas como trabajo en equipo. La diferencia principal con la Barra de función es que ésta no tiene todas las funciones, aunque proporciona mayor flexibilidad permitiéndole el acceso a su escritorio y a otras herramientas del sistema.



### Barra de herramientas Monitoreo

Disponible en: Esta barra de herramientas se encuentra en la parte superior derecha del escritorio del profesor cuando éste se encuentra monitoreando a los alumnos. Le permite a usted como profesor monitorear las actividades de los alumnos.



### Barra de herramientas de control

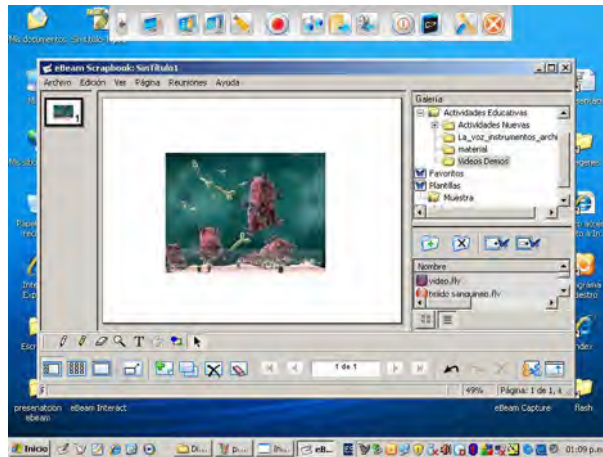
Disponible en: La parte superior derecha del escritorio de la Exomate cuando el profesor está controlando la unidad. Le permite como profesor controlar la Exomate de los alumnos, proporcionándole una forma fácil de guiar a éstos cuando requieren de ayuda adicional.



### D.3.3. Ícono de la barra de tareas de e-Learning Class

En ocasiones usted necesitará minimizar e-Learning Class a la barra de tareas para usar otros programas.

Es importante hacer notar que, aún minimizado, podemos tener acceso a la mayoría de las funciones interactivas que e-Learning Class ofrece usando la Barra Flotante localizada en la esquina superior izquierda de su escritorio o dando doble clic con el botón derecho en el ícono del Programa Maestro en la Barra de Tareas.



## D.4. Interactuando con los Alumnos

### D.4.1. Supervisar y controlar

**Descripción:** Le permite monitorear el escritorio de un alumno.

**Uso típico:** Asegurarse de que los alumnos están trabajando.

**Ícono del status del alumno:**



**Pasos:**

1. En la interfaz principal, seleccione el o los alumnos que desea monitorear.
2. Presione Supervisar y controlar.
3. e-Learning Class se minimizará a la barra de tareas.
4. El o los escritorios de los alumnos aparecerán como ventanas pequeñas en su computadora.
5. Hay 4 formas diferentes de detener la emisión:
  - Presione Monitor y Control en la Barra de Funciones. Presione Detener (Stop) en la barra de herramientas Monitorear

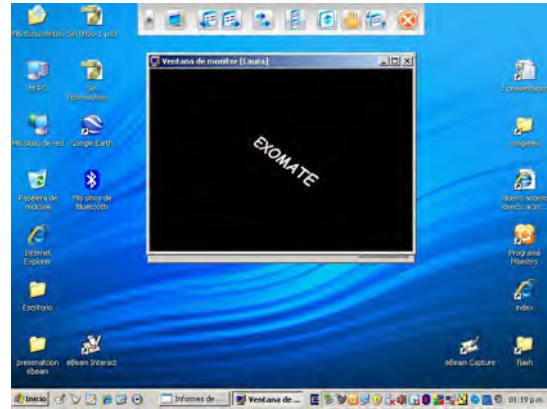
- Alt+F4 en la ventana del alumno
- Haga clic en la X en la esquina superior derecha de la Ventana Monitorar
- Clic con botón derecho en la ventana del alumno y seleccione la opción Cerrar esta ventana

En la pantalla del alumno



El alumno no recibe ninguna indicación de que está siendo monitoreado

En la pantalla del profesor



Cuando esté monitoreando, ambas unidades continuarán trabajando sin que haya impacto alguno en su desempeño.



Barra de herramientas del Supervisor y controlar



**Nota:** Esta función Monitoreo y Control requiere que al menos un alumno esté en línea en su aula virtual. Cada vez que usted monitoree a un alumno, e-Learning Class se minimizará en la barra de tareas y la barra de herramientas del monitor quedará disponible al colocar el puntero del Mouse en el borde superior derecho de su escritorio. Mientras esté monitoreando a un alumno, las funciones adicionales como el control remoto, están disponibles y se puede acceder a ellas dando clic con botón derecho en la Ventana Monitorar.

## D.4.2. Control Remoto

**Descripción:** Le permite monitorear el escritorio de un alumno.

**Uso típico:** Le permite controlar una Exomate.

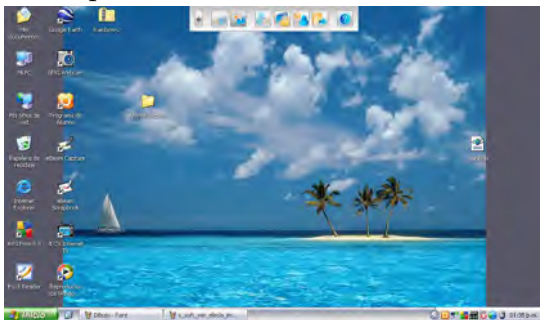
**Ícono del status del alumno:**



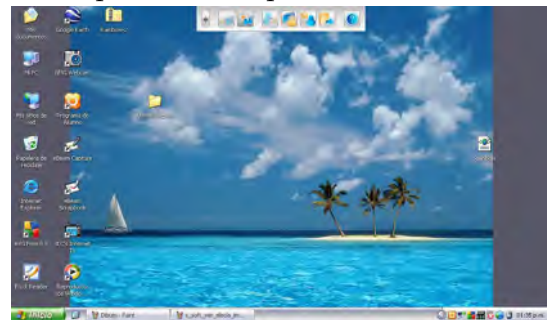
**Pasos:**

1. En el panel principal seleccione el alumno que va a monitorear.
2. Presione Monitor y Control.
3. e-Learning Class se minimizará en la barra de tareas.
4. En su escritorio aparecerá una ventana que mostrará el escritorio del alumno seleccionado.
5. Seleccione la ventana del alumno y haga clic con botón derecho en ésta para desplegar el menú de funciones monitor y control.
6. Seleccione Control Remoto.
7. La ventana del alumno se desplegará como pantalla completa de su computadora permitiéndole el control sobre la Exomate del alumno.
8. Para detener el control, seleccione Detener (Stop) control en la barra de herramientas. Control colocando el puntero del Mouse en la esquina superior derecha de su pantalla y seleccione Detener Control.

En la pantalla del alumno



En la pantalla del profesor



Barra de herramientas de Control

**Nota:** La función Control requiere que al menos monitoree a un alumno que se encuentre en línea.

Cada vez que usted controla una Exomate, la pantalla del alumno se maximizará en la suya, esto activará la barra de herramientas Control, la que se despliega colocando el puntero del Mouse en la esquina superior derecha de su pantalla.

Mientras está monitoreando una Exomate, las funciones adicionales como la pluma electrónica estarán disponibles. Por omisión, el alumno no tendrá control sobre su Exomate cuando usted esté controlando ésta. Dar doble clic en Bloquear Alumno para devolver a éste el control de su computadora.



### D.4.3. Difusión de la Pantalla

**Descripción:**

Le permite compartir su pantalla con los alumnos que se encuentren en su aula virtual.

**Uso típico:**

Dirija la clase compartiendo el contenido y presentaciones que se encuentran en la pantalla del profesor.

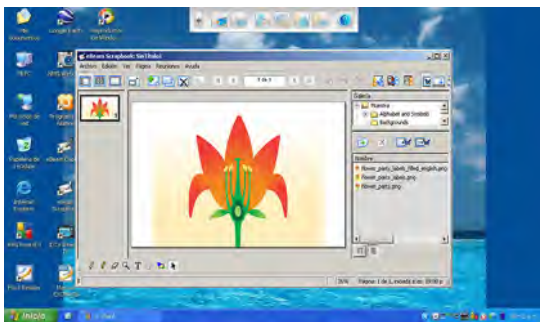
**Ícono del status del alumno:**



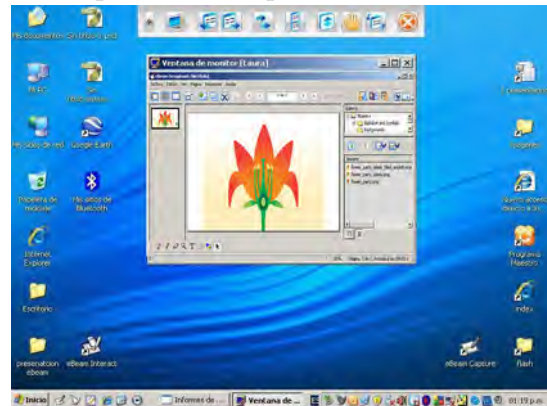
**Pasos:**

1. En el panel principal, seleccione el o los alumno(s) con quienes desea compartir su pantalla.
2. Seleccione Difusión de la Pantalla
3. Su consola se minimizará en la barra de tareas
4. El o los alumnos seleccionados podrán ver su pantalla en su Exomate
5. Para detener la emisión:
  - Seleccione Emisión de Pantalla en la Barra de funciones de la Consola del Profesor
  - Haga clic en el botón Resetear Todo en la barra de herramientas Emisión de Pantalla

En la pantalla del alumno



En la pantalla del profesor



Debido al tamaño limitado de la pantalla, su imagen compartida puede ocupar la mayoría o toda la pantalla de la Exomate.

Los alumnos verán el área que se encuentra alrededor de su cursor en la Exomate.



Barra de herramientas flotante

**Nota:** Por omisión si usted no selecciona ningún alumno, después de dar clic en Emisión de Pantalla, todos los asistentes a su clase virtual verán su pantalla.

La función Emisión de Pantalla requiere que por lo menos haya un alumno en línea en su aula virtual.

Cada vez que usted comparta lo que hay en su pantalla, la Barra de Herramientas Flotante estará disponible al colocar el puntero del Mouse en el borde superior derecho de su escritorio.

Mientras esté transmitiendo lo que está en su pantalla, las funciones adicionales como la pluma digital, micrófono, bloqueo, etc., estarán disponibles.



#### D.4.4. Pluma

**Descripción:** Le permite escribir notas o comentarios sobre su computadora o en la computadora del alumno.

**Uso típico:** Hacer énfasis en forma gráfica, en algunas secciones específicas del contenido compartido.

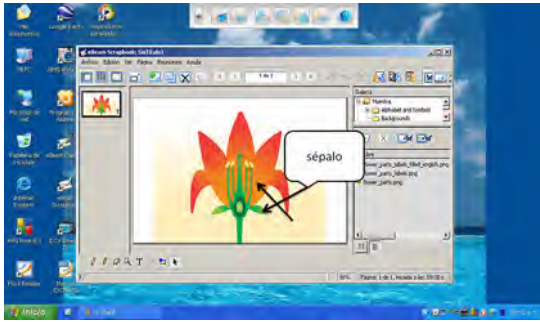
**Ícono del status del alumno:**



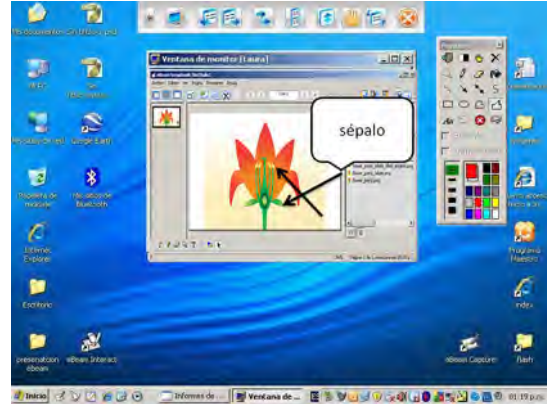
#### Pasos:

1. En el panel principal, seleccione el o los alumno(s) que compartirán su pantalla.
2. Seleccione Difusión de la Pantalla
3. e-Learning Class se minimizará en la barra de tareas
4. Los alumnos seleccionados observarán su pantalla en sus Exomate's
5. Coloque el puntero del Mouse en la esquina superior derecha de su pantalla.
6. Una vez que aparezca la Barra de Herramientas flotante, seleccione Pluma electrónica
7. A partir de este momento, su pantalla se convertirá en un pizarrón y usted podrá dibujar en ella con las herramientas disponibles en la barra de herramientas de puntero.
8. Para detener el uso de la Pluma:
  - Cierre la barra de herramientas del puntero
  - Presione ocultar puntero en la barra de herramientas

En la pantalla del alumno



En la pantalla del profesor



Con la pluma usted puede dibujar en la pantalla para dar mayor énfasis a cierto contenido.



Barra de herramientas del puntero



Barra de herramientas flotante



**Nota:** La función Difusión de la Pantalla requiere que al menos un alumno esté en línea. Cada vez que usted comparte su pantalla, la Barra de Herramientas Flotante estará disponible colocando el puntero el Mouse en la esquina superior derecha de su pantalla. Mientras dibuja con la Pluma Electrónica, usted no podrá realizar las funciones normales del ratón como es el clic derecho.

#### D.4.5. Demostración del alumno

**Descripción:**

Permite al alumno compartir su pantalla con otros alumnos.

**Uso típico:**

El alumno comparte el contenido educativo con el resto de la clase, permitiéndole al mismo tiempo tomar el control de la clase.

**Ícono del status del alumno:**

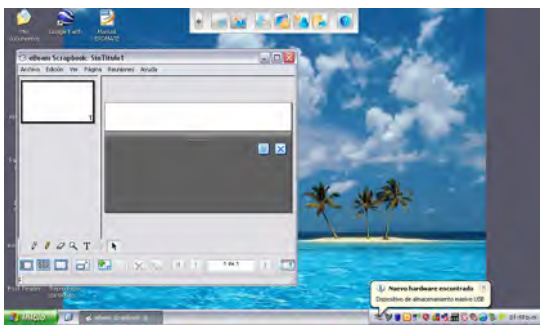




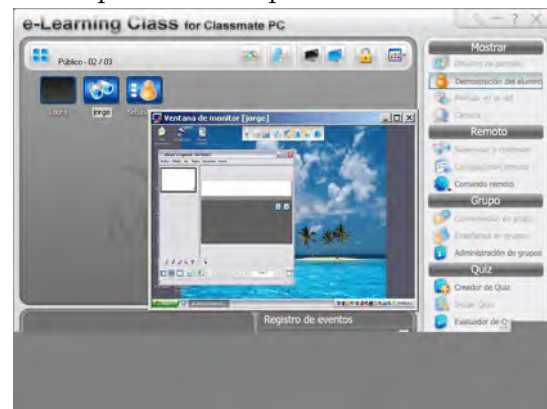
**Pasos:**

1. En el panel principal seleccione el alumno que dirigirá la clase.
2. Presione demostración del alumno
3. e-Learning Class iniciará la difusión de la pantalla del alumno seleccionado a toda la clase.
4. Para detener la demostración del alumno:
  - Cierre la ventana del alumno en su notebook/PC
  - Seleccione demostración del alumno en la Barra de Funciones
  - Alt + F4 en la ventana del alumno
  - Clic con botón derecho en la ventana del alumno y seleccionar la opción Cerrar esta ventana.

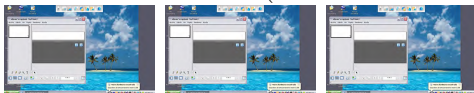
Exomate del alumno que dirige la clase



En la pantalla del profesor



Pantalla de Exomate (Otros alumnos)



El alumno está enseñando a la clase como abrir un programa de Exomate

¡Mientras el alumno dirige la clase, usted como profesor puede monitorear aun trabajar preparando la siguiente lección!

**Nota:** Únicamente un alumno puede dirigir la clase a la vez.

Con el propósito de que los demás alumnos no se distraigan durante la demostración, únicamente el alumno que está dirigiendo la clase puede tener control sobre su Exomate.

Usted, como profesor, puede continuar preparando material educativo en su computadora sin afectar la demostración del alumno.



## D.4.6. Silencio

- Descripción:** Desactiva todas las entradas y salidas de las Exomates.
- Uso típico:** Evitar que los alumnos se distraigan con las Exomates cuando el profesor está interactuando con los alumnos en otras formas, como puede ser una presentación.

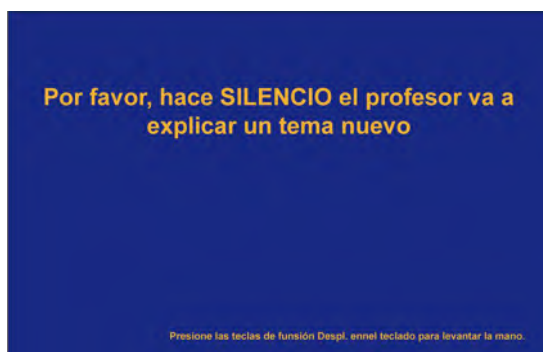
**Ícono del status del alumno:**



**Pasos:**

1. En la interfaz principal, seleccione la(s) PC(s) que se silenciarán
2. Seleccione Silencio
3. El o los alumnos seleccionados notarán que sus Exomates empiezan a desplegar el protector de pantalla de e-Learning Class V6; con esto, todas las entradas y salidas a la Exomate quedarán desactivadas.

En la pantalla del alumno



En la pantalla del profesor



Ubicación del ícono Silencio en la Barra de Funciones


**Nota:** Únicamente el profesor puede desbloquear una Exomate silenciada.

Una vez que el profesor sale de un aula virtual, los alumnos que tienen su computadora silenciada recobrarán el control de sus unidades.

El mensaje en la Pantalla Silencio puede cambiarse seleccionando OPCIÓN, lo que abrirá la Ventana Opción. Seleccione Silencio a la izquierda y luego ingrese un nuevo mensaje.



## D.4.7. Película en Red

<b>Descripción:</b>	Video que se reproduce en todas las Exomates basadas en tecnología Intel
<b>Uso típico:</b>	Le permite compartir el contenido de un video educativo con sus alumnos
<b>Ícono del status del alumno:</b>	

### Pasos:

1. En el panel principal seleccione el o los alumnos que verán el video, si no se seleccionan alumnos, el video se transmitirá a todos los alumnos.
2. Seleccione Película en la Red.
3. e-Learning Class abrirá la Ventana Película en la Red y la Barra de herramientas de Película en la Red.
4. En la barra de herramientas de película en red, presione Abrir
5. Seleccione el video que desea reproducir
6. Haga clic en Abrir
7. El video empezará a transmitirse en todas las Exomate's.
8. Para cerrar Película en la red:
  - Haga clic en el botón Cerrar en la Barra de herramientas Película en la Red

En la pantalla del alumno



En la pantalla del profesor



Mientras los alumnos ven el video, usted puede trabajar en otros programas

**Nota:** Mientras el profesor está seleccionando el video que se va a ir, las Exomates seleccionadas estarán en silencio.

Los archivos de video aceptados son aquellos que puede aceptar la computadora del profesor.



No todos los archivos se pueden compartir debido a restricciones en la anchura de la banda de la red y/o a los bits que contenga el video (mayor cantidad de bits requiere una banda más ancha).

Si su red tiene banda lo suficientemente ancha y aún así usted no puede compartir el video, favor de incrementar la velocidad de transmisión al máximo en la barra de Funciones e-Learning Class a Opción a Red a velocidad máxima de transmisión.

### D.4.8. Distribución de Archivos

**Descripción:**

Le permite distribuir archivos a sus alumnos

**Uso típico:**

Compartir documentos o archivos multimedia con sus alumnos

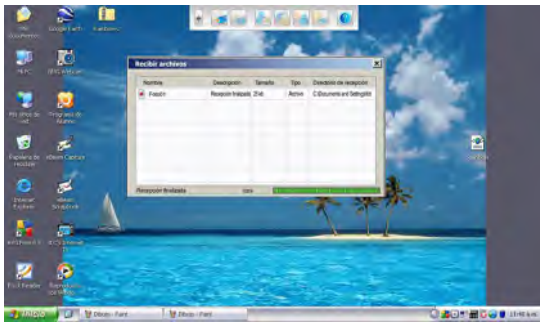
**Ícono del status del alumno:**



**Pasos:**

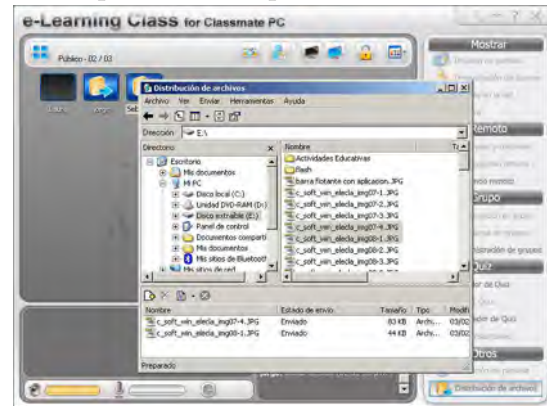
1. En el panel principal, seleccione la o las PCs de los alumnos a las cuales enviará archivo(s).
2. Presione Distribución de Archivos. Una vez que lo haya hecho usted notará:
  - Una ventana de distribución de archivos en e-Learning Class en la pantalla del profesor.
  - Una ventana Recibir Archivo en la Exomate
3. En la pantalla Distribución de Archivos, seleccione el o los archivos que enviará y haga clic en el botón Añadir.
4. Una vez que lo haya hecho, abra el menú Transferir y seleccione Enviar a
5. Elija la carpeta de Destino (altamente recomendado < Mis Documentos >)
6. Haga clic en OK
7. El (los) archivo(s) se enviará(n) a las Exomates de los alumnos
8. Para cerrar tanto Distribución de Archivo como la ventana Recibir Archivo, cierre la ventana Distribución de Archivos en su notebook/PC.

En la pantalla del alumno



Ventana Recibir Archivo aparece en la Exomate

En la pantalla del profesor



Pantalla de Distribución de archivo en la computadora del profesor

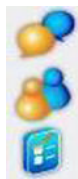
**Nota:** La Distribución de Archivo requiere que al menos haya un alumno en línea en su clase virtual.

Los alumnos no pueden cerrar la ventana Recibir Archivo



## D.4.9. Otras Funciones

**Grupo de Chat y Enseñanza Otras funciones**



Selecciona y divide a los alumnos en pequeños grupos para trabajar o para chatear.

**Uso típico:**

Trabajo de equipo entre los alumnos

**Status del alumno:**

**Cámara**

Permite difusión en vivo a todas las Exomate's

**Uso típico:**

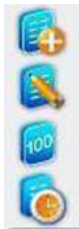
Permite que el profesor enseñe a los alumnos por medio de un video y en forma remota cuando el profesor y los alumnos se encuentran conectados a la misma red pero no se encuentran físicamente en el mismo lugar

**Status del alumno:**



---

### Quiz y Exámenes



Crear, distribuir y calificar pruebas con e-Learning Class

**Uso típico:**

Permite al profesor aplicar pruebas en línea y llevar un registro de los resultados de los alumnos

Status del alumno:

---

### Comando Remoto



Permite la interacción con una Exomate en base a acciones predefinidas

**Uso típico:**

Simplifica y hace más rápidas aquellas actividades que llevan mucho tiempo como la apertura y cierre de programas, dejando más tiempo para el aprendizaje.

Status del alumno:

---

### Configuración Remota



Permite la configuración remota de algunas propiedades básicas del sistema de Exomate

**Uso típico:**

Simplificar cambios en la configuración del sistema básico

Status del alumno:

# E. Guía de Software My Storage

## E.1. Generalidades de la aplicación

My Storage proporciona herramientas fáciles de utilizar para que los usuarios puedan crear copias de seguridad, restaurar datos y supervisar el uso del espacio en disco.

Las funciones principales de My Storage son las siguientes:

- **Monitor de discos:** muestra visualmente el nivel de uso del disco local. El Monitor de discos también proporciona información detallada como, por ejemplo, la capacidad del disco, el espacio utilizado y el espacio libre.
- **Asistente para copia de seguridad de datos:** permite crear una copia de seguridad de los datos locales del equipo en dispositivos de almacenamiento externo como, por ejemplo, un disco U o un disco extraíble.
- **Asistente para restauración de datos:** permite restaurar la copia de seguridad de los datos desde un disco externo al equipo local.
- **Copia de seguridad programada:** permite crear una copia de seguridad de datos predefinidos en un dispositivo externo según la programación definida por el usuario.
- **Copia de seguridad rápida:** método de copia de seguridad en un solo clic que permite al usuario crear una copia de seguridad de datos predefinidos.
- **Liberador de espacio en disco:** cuando quede poco espacio libre en el equipo, también se cargará una herramienta de liberación de espacio en disco para eliminar los archivos innecesarios con el fin de liberar espacio en el disco local.

## E.2. Utilizando la aplicación

### E.2.1. Inicio de My Storage

My Storage se ejecutará automáticamente en segundo plano mientras el usuario de Windows esté conectado.

Si cierra My Storage y desea volver a iniciarlo, vaya a “Inicio -> Todos los programas -> Intel Education Stack -> My Storage” y haga clic en **My Storage**.



### E.2.2. Ícono de bandeja

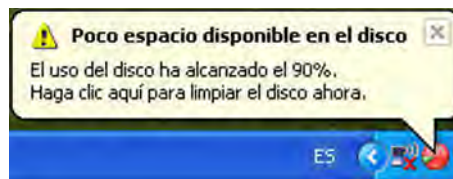
Cuando se está ejecutando My Storage, aparece un ícono de bandeja en la bandeja del sistema.



Puede pasar el cursor sobre este ícono para obtener una descripción breve del espacio que hay en el disco local.



Si cambia el estado del espacio en el disco local, aparecerá un globo de notificación.



Además, el color del ícono de bandeja de My Storage cambia según el espacio que quede disponible en el disco local.

Estado	Uso del espacio en disco	Ícono de bandeja	Acción tras hacer clic en el globo
Bueno	Menos del 80 %	(Azul) 	Se abre el cuadro de diálogo Monitor de discos
Advertencia	Entre un 80 % y un 90 %	(Amarillo) 	Se abre el cuadro de diálogo Monitor de discos
Bajo	Espacio utilizado superior al 90 %	(Rojo) 	Se inicia la utilidad Liberador de espacio en disco



### E.2.3. Menú de bandeja

Puede obtener acceso a las funciones principales de My Storage a través del menú de bandeja. Para abrir este menú, haga clic con el botón primario o secundario del ratón en el ícono de bandeja.



- **Iniciar My Storage:** permite abrir la ventana principal de My Storage.
- **Monitor de discos:** permite abrir el Monitor de discos.
- **Copia de seguridad rápida:** permite crear inmediatamente una copia de seguridad de los datos definidos en el cuadro de diálogo Opciones.
- **Asistente para copia de seguridad de datos:** permite iniciar el Asistente para copia de seguridad de datos.
- **Asistente para restauración de datos:** permite iniciar el Asistente para restauración de datos.
- **Opciones:** permite abrir el cuadro de diálogo Opciones.
- **Acerca de:** permite abrir el cuadro de diálogo Acerca de.
- **Salir:** permite salir de My Storage.

## E.2.4. Ventana principal de My Storage

Puede obtener acceso a las funciones principales de My Storage a través de la ventana principal.

Hay dos maneras de abrir esta ventana:

- Haga doble clic en el ícono de bandeja de **My Storage**.
- Haga clic con el botón primario o secundario del ratón en el ícono de bandeja y seleccione Iniciar My Storage.



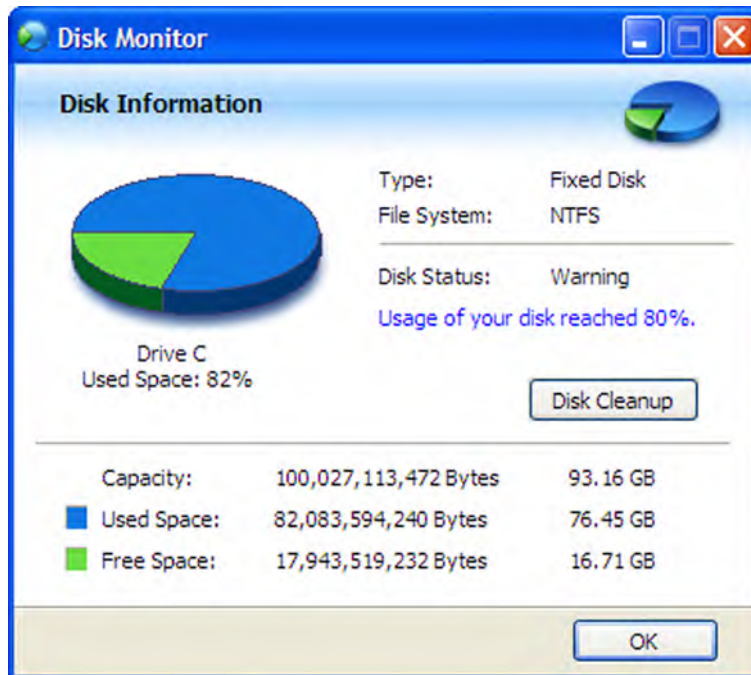
### Nota:

-Si necesita obtener ayuda, haga clic en el botón “Ayuda” o pulse “F1” en la ventana principal.

## E.2.5. Monitor de discos

Hay dos maneras de iniciar el Monitor de discos:

- Haga clic con el botón primario o secundario del ratón en el ícono de bandeja y seleccione **Monitor de discos** del menú de bandeja.
- Haga clic en **Monitor de discos** en la ventana principal.



El Monitor de discos muestra el estado de almacenamiento de los discos. Desde este diálogo puede acceder también al Liberador de espacio en disco.

## E.2.6. Liberador de espacio en disco

El usuario puede iniciar la herramienta Liberador de espacio en disco para liberar espacio en el disco local. Esta herramienta la proporciona el sistema operativo. Consulte el manual del usuario de Liberador de espacio en disco para obtener información detallada.

Hay dos maneras de iniciar la herramienta Liberador de espacio en disco:

- Haga clic en el botón Liberar del cuadro de diálogo **Monitor de discos**.
- Haga clic en el globo de advertencia que aparece cuando el nivel de uso del disco es superior al 90 %.

## E.2.7. Asistente para copia de seguridad de datos

El Asistente para copia de seguridad de datos permite crear una copia de seguridad de los datos locales del equipo en dispositivos de almacenamiento externo como, por ejemplo, un disco o un disco extraíble.

## Inicio del Asistente para copia de seguridad de datos

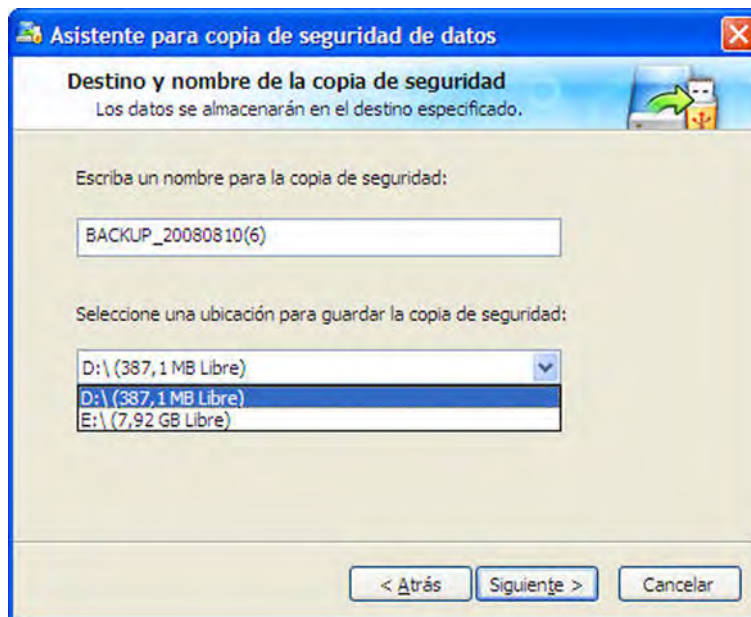
Hay dos maneras de iniciar el Asistente para copia de seguridad de datos:

- Haga clic con el botón izquierdo o derecho del ratón en el ícono de bandeja **My Storage** y seleccione **Asistente para copia de seguridad de datos** del menú de bandeja.
- Haga clic en el botón **Asistente para copia de seguridad de datos** de la ventana principal.

## Copia de seguridad de los datos

Para crear una copia de seguridad de los datos, siga los pasos que se indican a continuación:

1. Tras iniciar el Asistente para copia de seguridad, aparecerá un cuadro de diálogo de bienvenida. Haga clic en **Siguiente** para continuar.
2. Puede utilizar el nombre predeterminado o introducir otro nombre para la copia de seguridad. Si hay más de un dispositivo de almacenamiento externo conectado, seleccione en la lista desplegable el destino en el que desea crear la copia de seguridad de los datos. Haga clic en **Siguiente** para continuar.

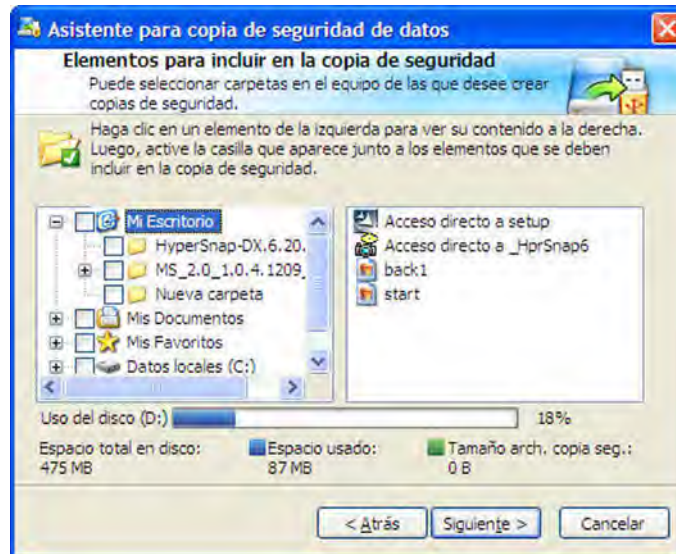


### Nota:

- Si no se detecta ningún disco externo, en este cuadro de diálogo aparecerá un mensaje de advertencia. Inserte un disco para continuar.
  - Si no queda espacio disponible en el disco externo, éste no se agregará al cuadro combinado.
3. Active la casilla situada junto a los elementos que se deben incluir en la copia de seguridad. El tamaño de las carpetas seleccionadas se calcula automáticamente y el nivel de uso del espacio en disco del disco de destino se muestra en la parte inferior.

Si el tamaño del total de datos que desea incluir en la copia de seguridad es superior a la cantidad de espacio disponible en el disco de destino, la barra indicadora cambiará a rojo. Libere una cantidad de espacio suficiente en el disco externo o reduzca la cantidad de datos que se debe incluir en la copia de seguridad.

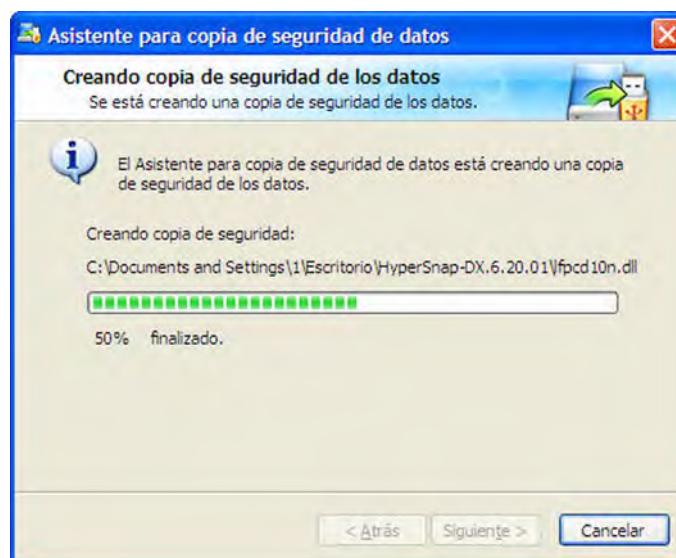
Haga clic en **Siguiente** para continuar.



**Nota:**

- Sólo se pueden seleccionar carpetas.
- En este cuadro de diálogo, las carpetas del sistema, tales como Windows y Archivos de programa, están filtradas. Tampoco se mostrarán las carpetas ocultas.

4. Se mostrará el progreso de la creación de la copia de seguridad. Si desea cancelar la operación, haga clic en el botón **Cancelar**.



**Nota:**

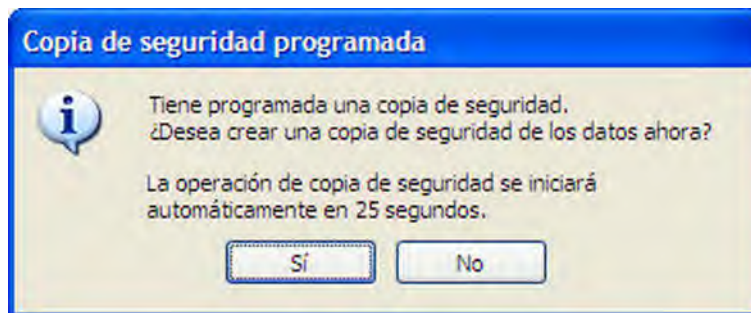
- No extraiga el disco de destino durante el proceso de copia de seguridad.

5. Una vez finalizada la operación, se mostrará la información acerca de la copia de seguridad. Haga clic en **Finalizar** para cerrar el asistente.

### E.2.8. Copia de seguridad programada

Para utilizar la función **Copia de seguridad programada**, deberá configurar las opciones correspondientes en el cuadro de diálogo **Opciones de My Storage** (consulte la sección Opciones para obtener más información).

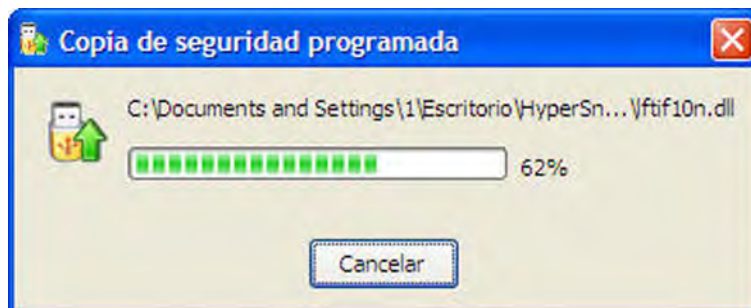
My Storage iniciará la operación de copia de seguridad según la hora predefinida. Antes de que se procese la copia de seguridad programada, aparecerá un cuadro de diálogo. Haga clic en **Sí** para iniciar la creación de la copia de seguridad. Si no responde de ninguna forma a este cuadro de diálogo, la copia de seguridad se iniciará automáticamente transcurridos 30 segundos.



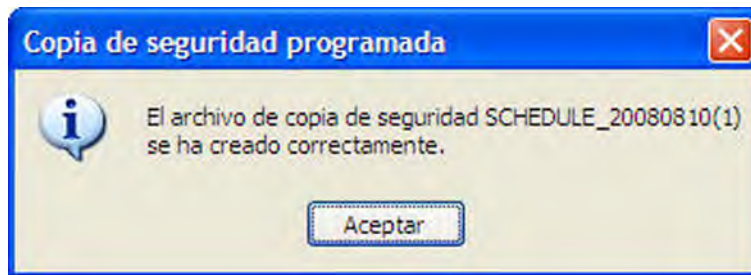
Si se detecta más de un disco externo, aparecerá el cuadro de diálogo siguiente. Seleccione el disco de destino y haga clic en **Aceptar** para continuar.



El progreso de la copia de seguridad programada se muestra en el cuadro de diálogo siguiente:



Una vez finalizada la operación, aparecerá el cuadro de diálogo siguiente:



**Nota:**

- Si no se detecta ningún disco externo, aparecerá un mensaje de advertencia. Inserte un disco para continuar.
- Si no hay suficiente espacio libre en el disco de destino, aparecerá un mensaje de advertencia. Haga clic en Aceptar para abandonar el proceso de copia de seguridad.
- No extraiga el disco de destino durante el proceso de copia de seguridad.

### E.2.9. Copia de seguridad rápida

Para utilizar la función Copia de seguridad rápida, deberá configurar las opciones correspondientes en el cuadro de diálogo **Opciones de My Storage** (consulte la sección Opciones para obtener más información).

Para iniciar la Copia de seguridad rápida, haga clic con el botón primario o secundario del ratón en el ícono de bandeja y seleccione **Copia de seguridad rápida** del menú de bandeja.

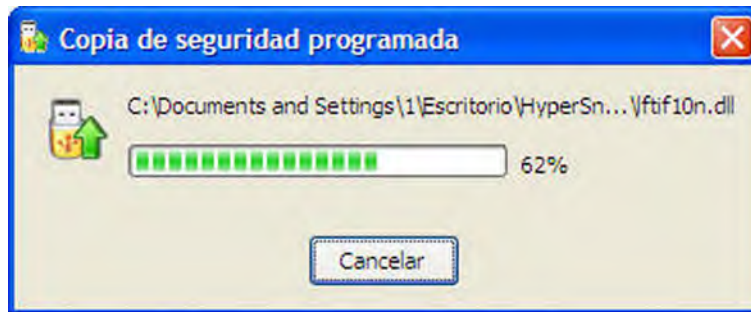
**Nota:**

- Si no hay ningún disco externo conectado, el elemento **Copia de seguridad rápida** no estará activado en el menú de bandeja.

Si se detecta más de un disco externo, aparecerá el cuadro de diálogo siguiente. Seleccione el disco de destino y haga clic en **Aceptar** para continuar.



El progreso de la copia de seguridad rápida se muestra en el cuadro de diálogo siguiente:



**Nota:**

- Si no hay suficiente espacio libre en el disco de destino, aparecerá un mensaje de advertencia. Inserte un disco para continuar.

## E.2.10. Asistente para restauración de datos

### Inicio del Asistente para restauración de datos

Hay dos maneras de iniciar el **Asistente para restauración de datos**:

- Haga clic con el botón izquierdo o derecho del ratón en el ícono de bandeja **My Storage** y seleccione **Asistente para restauración de datos** del menú de bandeja.
- Haga clic en el botón **Asistente para restauración de datos** de la ventana principal.

**Nota:**

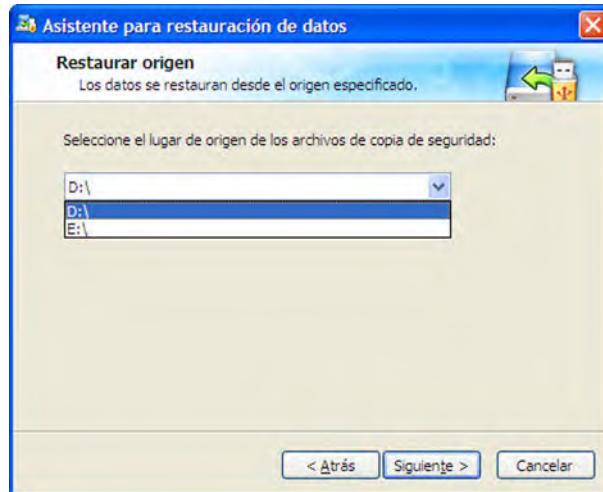
- El **Asistente para restauración** no se puede iniciar si el **Asistente para copia de seguridad** o las opciones **Copia de seguridad rápida/Copia de seguridad programada** no han finalizado.

### Restauración de datos

Para restaurar los datos, realice los pasos siguientes:

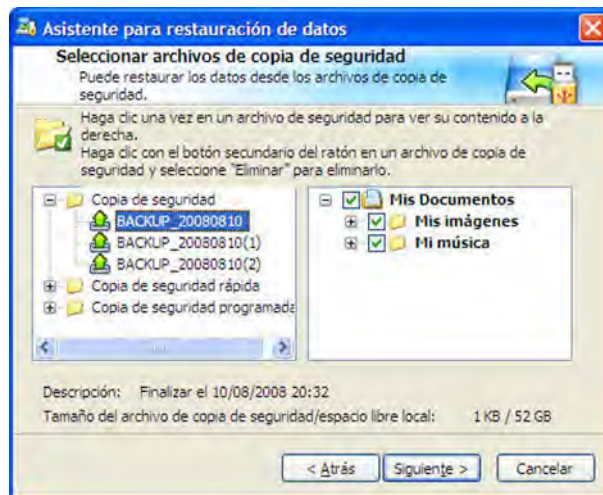
1. Tras iniciar el **Asistente para restauración de datos**, aparecerá un cuadro de diálogo de bienvenida. Haga clic en **Siguiente** para continuar.
2. Seleccione el disco de origen desde el que desea restaurar los datos.





**Nota:**

- El Asistente para restauración no se puede iniciar si el Asistente para copia de seguridad o las opciones Copia de seguridad rápida/Copia de seguridad programada no han finalizado.
3. Hay tres tipos de archivos de copia de seguridad: **Copia de seguridad**, **Copia de seguridad rápida** y **Copia de seguridad programada**. Éstos se ordenan en forma de árbol de carpetas. Haga clic en un archivo de copia de seguridad para ver su contenido a la derecha. Active la casilla situada junto al archivo que desee restaurar.

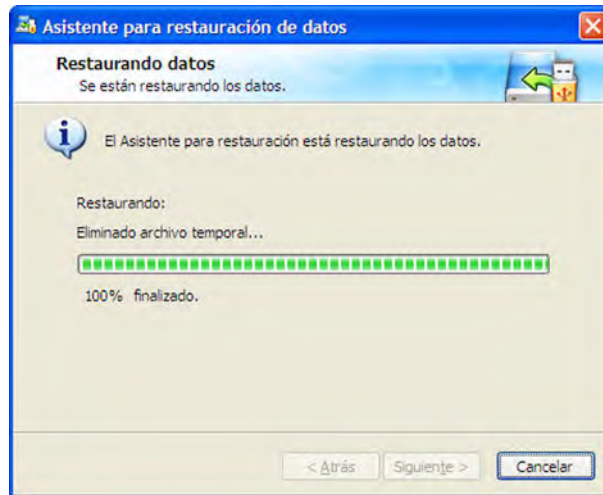


Haga clic en **Siguiente** para continuar.

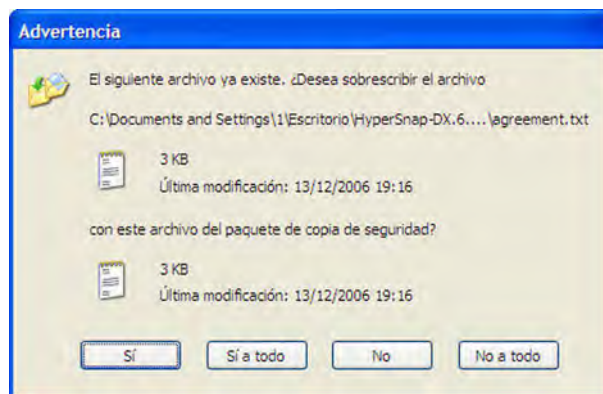
**Nota:**

- Si desea eliminar los archivos de copia de seguridad del disco externo, haga clic con el botón secundario del ratón en el nombre del archivo y seleccione Eliminar.
- Si no hay archivos de copia de seguridad en el disco externo seleccionado, aparecerá un mensaje de error.

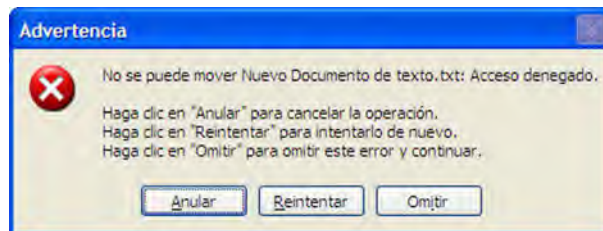
4. Todos los archivos seleccionados en el paso anterior se restaurarán en la ruta de acceso original del disco local.



Si el archivo ya existe, aparecerá el siguiente cuadro de diálogo que habrá que confirmar para que el archivo se sobrescriba. Si desea sobrescribir el archivo del disco local, haga clic en el botón **Sí**. De lo contrario, haga clic en **No**. Si desea sobrescribir todos los archivos existentes, haga clic en **Sí a todo**. De lo contrario, haga clic en **No a todo**.



Si el programa no consigue restaurar el archivo en el disco local, aparecerá un cuadro de diálogo de advertencia que indica el posible motivo del error.



5. Una vez finalizada la operación, se mostrará la información acerca de la restauración. Haga clic en **Finalizar** para cerrar el asistente.

**Nota:**

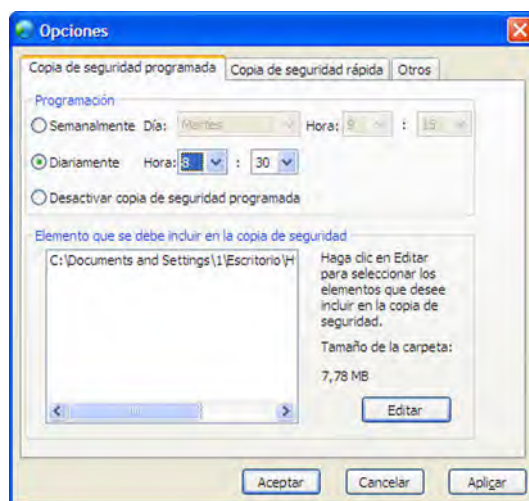
- Si el Asistente para restauración de datos sobrescribe el archivo, esta operación no se puede deshacer; incluso si se cancela el asistente.

## E.3. Opciones

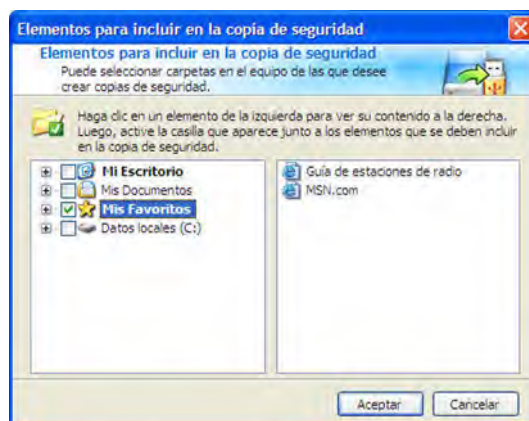
Es posible programar una copia de seguridad y configurar la **Copia de seguridad rápida** en el cuadro de diálogo **Opciones**. Para abrir este cuadro de diálogo, haga clic con el botón primario o secundario del ratón en el ícono de bandeja My Storage y seleccione **Opciones**.

### E.3.1. Configuración de la copia de seguridad programada

Haga clic en la ficha **Copia de seguridad programada** para configurar la hora en la que desea crear una copia de seguridad de los datos. A continuación, haga clic en **Editar** para abrir el cuadro de diálogo “**Elementos para incluir en la copia de seguridad**”.



Seleccione las carpetas que desea incluir en la copia de seguridad y haga clic en **Aceptar** para volver a Opciones.



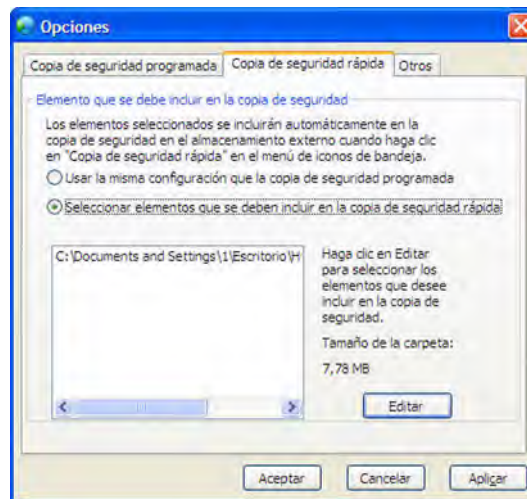
#### Nota:

- Las opciones no se pueden guardar si se activa la opción de copia de seguridad programada sin seleccionar elementos para incluir en la copia de seguridad.

### E.3.2. Configuración de la copia de seguridad rápida

Puede hacer clic en el botón **Usar la misma configuración que la copia de seguridad programada**.

Si desea incluir elementos diferentes en la copia de seguridad, haga clic en el botón **Seleccionar elementos que se deben incluir en la copia de seguridad rápida**. A continuación, haga clic en **Editar** para seleccionar los elementos que se deben incluir en la copia de seguridad.

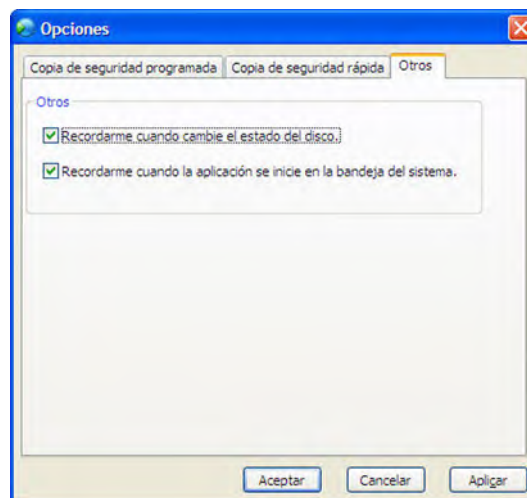


**Nota:**

- Si no ha configurado la función Copia de seguridad rápida en el cuadro de diálogo Opciones, aparecerá un mensaje de advertencia al hacer clic en el botón correspondiente del menú de bandeja. Haga clic en Aceptar para ir a Opciones y establecer la configuración.

### E.3.3. Otras opciones

En la sección **Otros** se pueden activar o desactivar los globos de notificaciones y las sugerencias.



# F. Guía de Software Parents Carefree

## F.1. Generalidades de la aplicación

El Parents Carefree es un software destinado para el uso de docentes o padres. Mediante este software el docente o padre puede disponer que cantidad de horas el alumno podrá usar la Exomate por día o bien dentro de que rango horario la podrá utilizar, por ejemplo de 18 a 20hs.

Además, puede restringir las páginas o aplicaciones que puede tener acceso, aplicando las políticas de seguridad de la institución educativa, o bien revisar el historial de ejecución de programas y las páginas a las que accedió el alumno.

## F.2. Utilizando la aplicación

### F.2.1. Menú del ícono de la bandeja del sistema



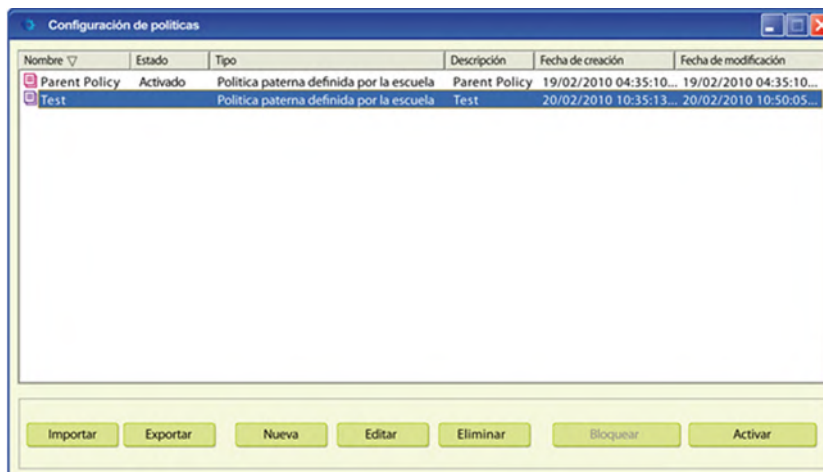
Haciendo un clic sobre el ícono de Parents Carefree de la barra de tareas de Windows se podrá acceder a las funcionalidades del programa que se describen a continuación:



1. **Configuración de políticas:** abre la interfaz de configuración de políticas.
2. **Configuración:** proporciona las opciones de conexión al servidor de política escolar y permite modificar la contraseña de administración, las teclas de acceso rápido y la configuración del registro.
3. **Revisión de registro:** puede ver el registro de los sitios Web, el registro de actividad en la computadora, el registro del programa y la presentación de instantáneas de pantalla.
4. **Modo de control:** proporciona tres modos de control: control escolar, control paterno y control desactivado; cuando el programa Parents Carefree Client se conecta a Parents Carefree Server, el primero cambiará automáticamente al modo de control escolar.
5. **Ocultar este ícono:** se ocultará de la bandeja del sistema el ícono del programa Parents Carefree Client y podrá usar teclas de acceso rápido o hacer clic en el acceso directo del menú de inicio para volver a mostrar el ícono en la bandeja.
6. **Desinstalar:** desinstala del PC el programa Parents Carefree Client.
7. **Ayuda:** abre el manual de usuario del programa Parents Carefree Client.
8. **Acerca de:** muestra la versión del programa Parents Carefree Client, asistencia técnica e información adicional.
9. **Salir:** permite salir del programa Parents Carefree Client.

## F.2.2. Configuración de políticas

Las políticas se pueden administrar y configurar desde el siguiente cuadro de diálogo:



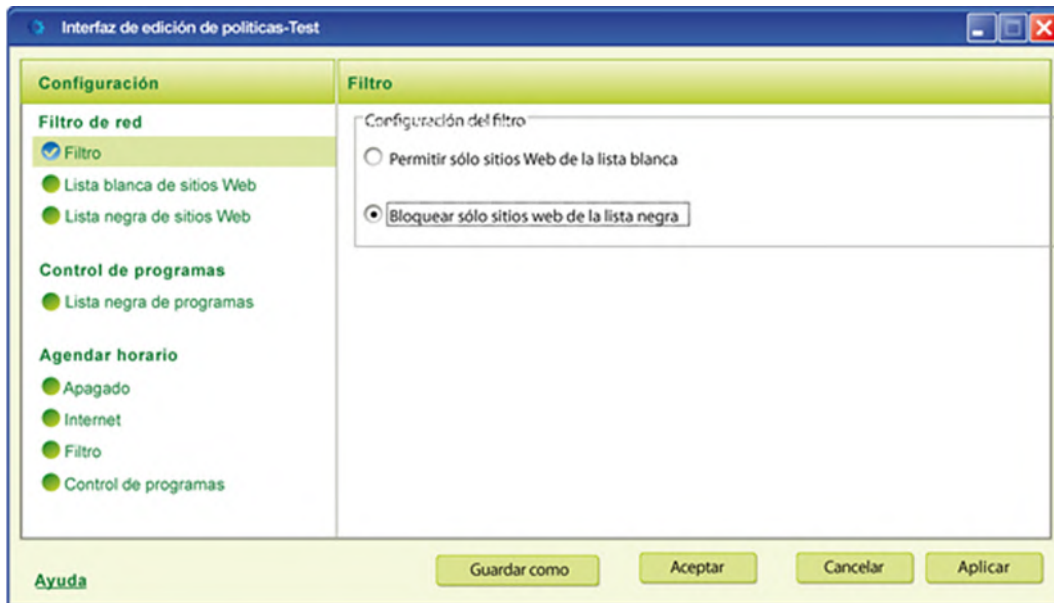
1. **Importar:** importa un archivo de política existente al cuadro de la lista de políticas. El cliente sólo puede importar políticas paternas.
2. **Exportar:** exporta la política seleccionada del cuadro de la lista de políticas a la carpeta que especifique. Además, no puede exportar políticas paternas definidas por la escuela.
3. **Nueva:** los padres pueden hacer clic en este botón para crear políticas paternas.
4. **Editar:** seleccione la política que desea editar del cuadro de la lista de políticas y haga clic en el botón Editar para abrir la interfaz de edición. Puede cambiar la configuración de la política como desee.
5. **Eliminar:** en el cuadro de lista de políticas, seleccione una política y haga clic en el botón Eliminar para eliminarla.
6. **Bloquear/Desbloquear:** el botón Bloquear se puede usar solamente para las políticas paternas definidas por la escuela. Si la política paterna definida por la escuela está bloqueada, Parents Carefree Client no podrá descargar la política actualizada.
7. **Activar:** obtenga una política en el cuadro de lista de políticas activado. Si el programa Parents Carefree Client se encuentra en el modo Control paterno, se aplicará esta política.

**Nota:**

- Es posible crear un máximo de 40 políticas.
- Sólo es posible visualizar la política paterna definida por la escuela; no se puede exportar, editar, ni eliminar.



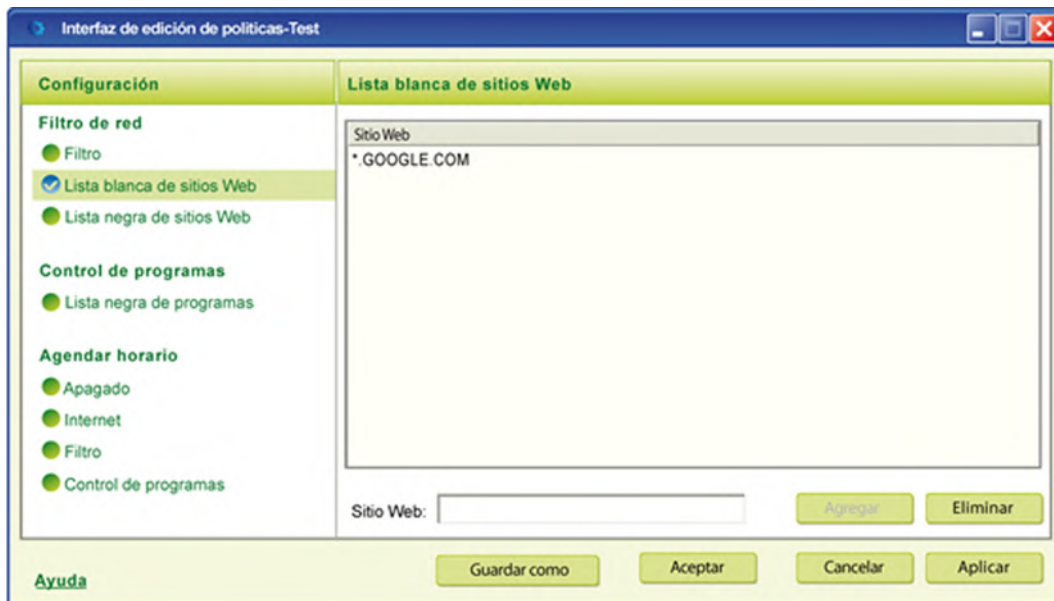
### F.2.3. Filtro de red



1. **Permitir sólo sitios Web de la lista blanca:** sólo se pueden visitar los sitios Web de la lista blanca, el resto quedarán bloqueados.
2. **Bloquear sólo sitios Web de la lista negra:** sólo están bloqueados los sitios Web de la lista negra, los demás se pueden visitar.



## Configuración de las listas blanca y negra de sitios Web



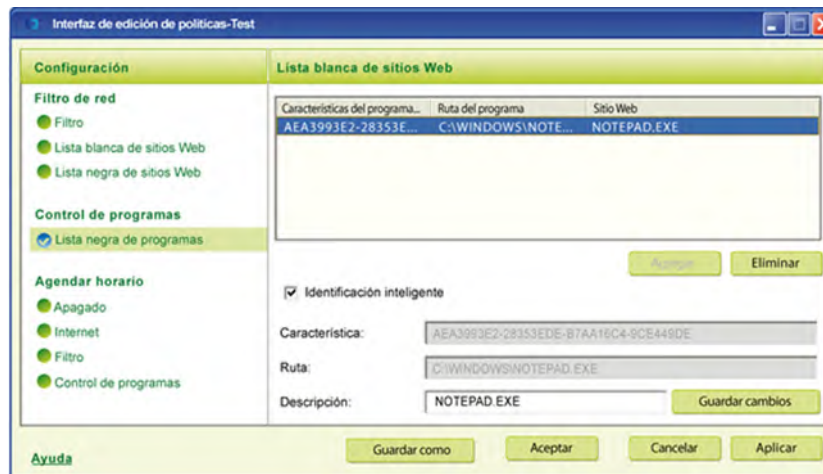
1. **Agregar:** coloque el sitio Web en el marco de edición y haga clic en el botón **Agregar** para completar la operación.
2. **Eliminar:** seleccione el sitio Web que desee eliminar de la lista. Haga clic en el botón **Eliminar**. Tras confirmar en la ventana emergente, el sitio Web se eliminará por completo.

### **Nota:**

- Los usuarios pueden utilizar el asterisco (\*) como comodín para agregar sitios Web,. Por ejemplo, *www.yahoo.com* se puede cambiar a *\*.yahoo.com* (el asterisco representa los sitios Web secundarios arbitrarios).
- Si el usuario especifica una dirección Web que comienza con *www*, el programa Parents Carefree Client cambiará automáticamente la dirección por un asterisco (\*). Por ejemplo, si escribe *www.google.com* y hace clic en **Agregar**, el programa Parents Carefree Client agregará *\*.google.com* al cuadro de lista de sitios Web.



## F.2.4. Control de programas



Si desea bloquear algún programa de modo que su hijo no pueda ejecutarlo (por ejemplo, un juego), puede agregarlo a la lista negra de programas.

Podrá hacer clic en el botón **Agregar** para seleccionar el programa que desee bloquear y la aplicación Parents Carefree Client mostrará en el cuadro de edición de información los datos relacionados con el programa.

Puede modificar la información descriptiva y el método de reconocimiento del programa. Además, puede elegir el programa que desea eliminar y, a continuación, hacer clic en el botón **Eliminar** para desbloquearlo.

## F.2.5. Agendar horario

La función de programación de horario le ayuda a limitar el tiempo que sus hijos - alumnos acceden a Internet, a sitios Web y a programas.



1. **Apagado:** esta función le permite programar el tiempo de acceso para cada media hora de uso del equipo. La configuración se aplicará según el modo de control. Cada media hora se divide en secciones grises y azules, que se corresponden con la siguiente configuración:
  - **Gris:** estado predeterminado, permite el uso del equipo.
  - **Azul:** en este estado, no se podrá utilizar el equipo, excepto si se escribe la contraseña de administración de Parents Carefree para modificar el perfil de programación de apagado. Si no se introduce ninguna contraseña o la contraseña es incorrecta, aparecerá un mensaje en el que se notificará al usuario que el equipo se apagará en 120 segundos.
2. **Internet:** esta función le permite crear una configuración de acceso a la red diferente para cada media hora de uso del equipo. La configuración se aplicará según el modo de control. Cada media hora se divide en secciones grises y azules, que se corresponden con la siguiente configuración:
  - **Gris:** estado predeterminado, permite el uso de Internet.
  - **Azul:** en este estado, Parents Carefree cerrará la conexión a Internet del equipo y bloqueará el uso de Internet. Los alumnos podrán utilizar el equipo pero no se les permitirá acceder a Internet.
3. **Filtro:** esta función le permite crear una configuración de filtrado de sitios Web diferente para cada media hora de uso del equipo. La configuración se aplicará según el modo de control. Cada media hora se divide en secciones grises y azules, que se corresponden con la siguiente configuración:
  - **Gris:** desactiva el filtro de sitios Web.
  - **Azul:** activa el filtro de sitios Web.
4. **Control de programas:** esta función le permite crear una configuración de control de programas diferente para cada media hora de uso del equipo. Podrá controlar los programas que los alumnos pueden usar. La configuración se aplicará según el modo de control. Cada media hora se divide en secciones grises y azules, que se corresponden con la siguiente configuración:
  - **Gris:** permite que se ejecuten todos los programas.
  - **Azul:** estado predeterminado. En este estado, únicamente se bloqueará la ejecución de los programas de la lista negra.

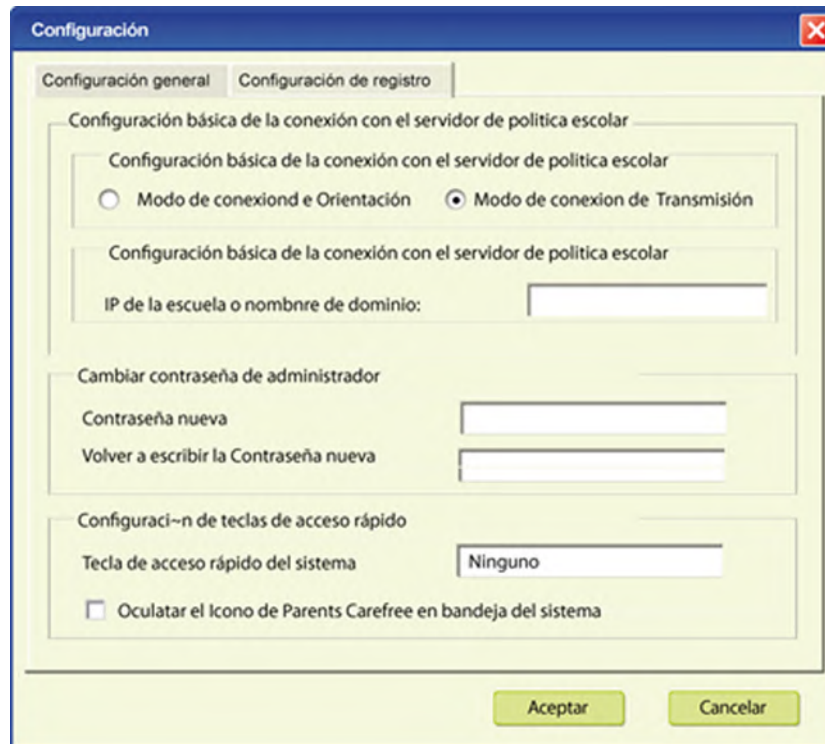
**Nota:** Cuando utilice la función Programación, compruebe que la configuración de huso horario del sistema sea correcta.



## F.2.6. Configuración

Si es la primera vez que usa el programa Parents Carefree Client, deberá completar la configuración de la contraseña de administración y las teclas de acceso rápido.

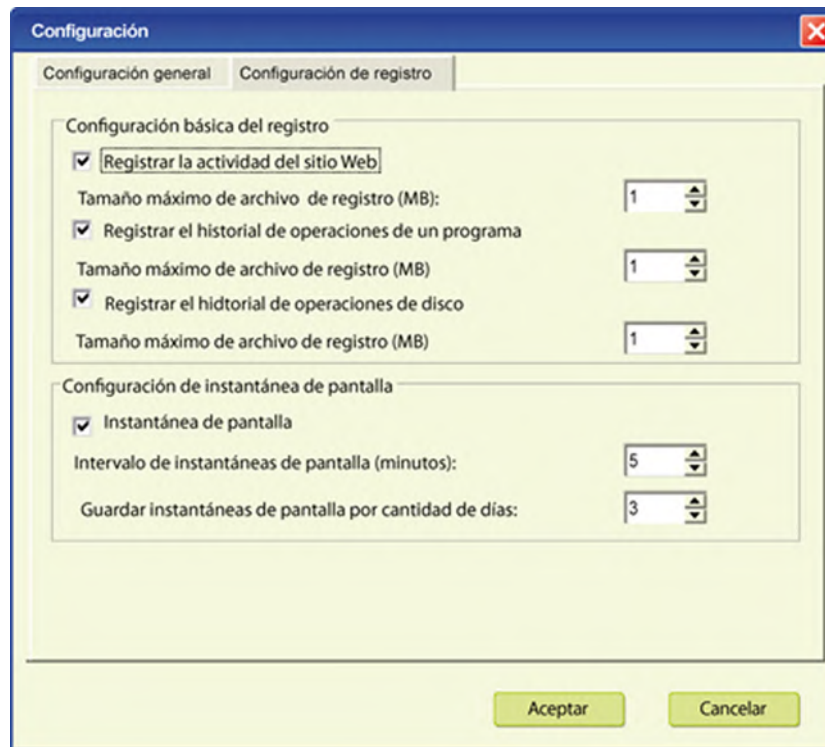
### Configuración general



1. **Configuración de la conexión con el servidor de política escolar:** puede especificar el método de comunicación para conectarse al servidor de política escolar. Si selecciona el modo de conexión de Orientación, deberá especificar la dirección IP o nombre de dominio de la escuela. En cambio, si selecciona “Modo de conexión de Transmisión”, el programa Parents Carefree Client buscará automáticamente el servidor de política escolar.
2. **Cambiar contraseña de administración:** para modificar la contraseña de administración de Parents Carefree, haga clic en Cambiar contraseña de administración y escriba la contraseña dos veces. Tenga en cuenta que las dos contraseñas introducidas deben coincidir.
3. **Configuración de las teclas de acceso rápido:** para configurar las teclas de acceso rápido de Parents Carefree, deberá presionar algunos botones del teclado simultáneamente, por ejemplo, establezca la tecla de acceso rápido en **Ctrl + Alt + F** y, a continuación, active la opción “Ocultar el ícono de Parents Carefree en la bandeja del sistema”.

Si el ícono del programa Parents Carefree Client está oculto en la bandeja del sistema, puede usar teclas de acceso rápido o hacer clic en **Inicio->Todos los programas->Parents Carefree** para que aparezca el cuadro de diálogo de inicio de sesión de Parents Carefree.

## Configuración de registro

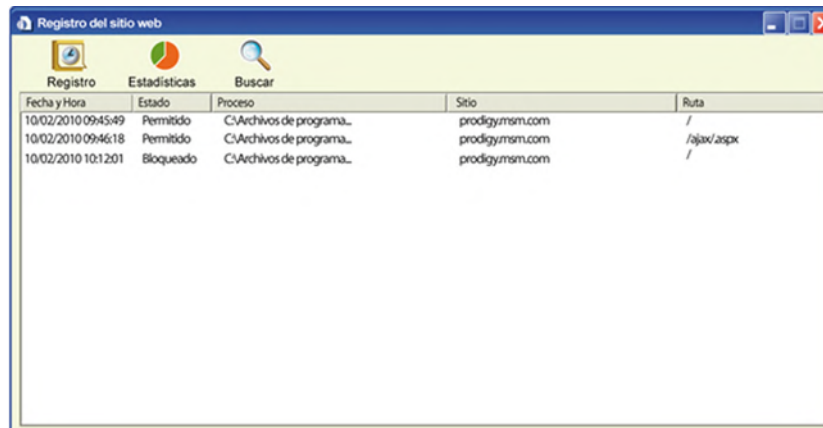


La configuración de registro determina si se debe guardar la información de registro y el intervalo del tamaño de los archivos de registro. Es práctico y fácil de usar.

1. **Tamaño máximo de archivo de registro (MB):** 1 MB es el tamaño recomendado; el intervalo de tamaño de los archivos de registro que puede configurar es de 1 a 5 MB.
2. **Intervalo de instantáneas de pantalla (minutos):** 5 minutos es el intervalo recomendado; este parámetro grabará una imagen de la pantalla a intervalos de 5 minutos. Puede definir los intervalos de 5 a 60 minutos.
3. **Guardar instantáneas de pantalla por cantidad de días:** 3 días es el valor recomendado. Puede definir los días de retención entre 1 y 20.

## F.2.7. Revisión de registro

### Registro de sitios Web



Fecha y Hora	Estado	Proceso	Sitio	Ruta
10/02/2010 09:45:49	Permitido	C:\Archivos de programa...	prodigymsm.com	/
10/02/2010 09:46:18	Permitido	C:\Archivos de programa...	prodigymsm.com	/ajax.aspx
10/02/2010 10:12:01	Bloqueado	C:\Archivos de programa...	prodigymsm.com	/

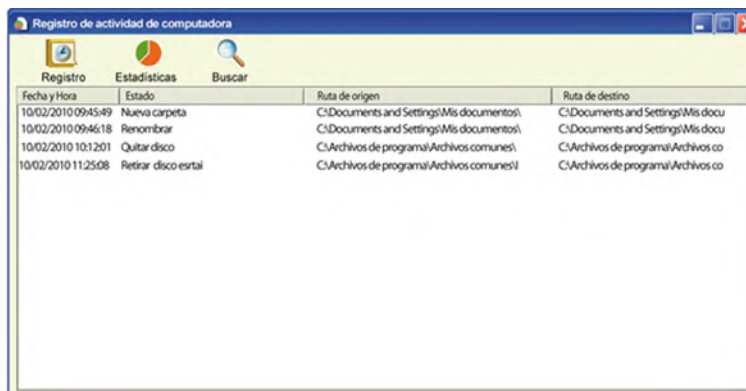
Esta funcionalidad de Parents Carefree registra información sobre los sitios Web que han visitado los alumnos, incluida la hora y la ruta. Esto refleja las actividades de Internet de los alumnos. Puede consultar la sección Estadísticas en los datos de registro y simular el acceso a estos sitios Web con el fin de obtener más información acerca de las actividades de Internet de los alumnos.

Para poder acceder haga clic en el ícono de Parents Carefree Client de la bandeja del sistema y seleccione **Revisión de registro->Registro de sitios Web**. Aparecerá la ventana del registro de los sitios Web en la que se almacena la información del registro de sitios Web. Puede hacer clic en Abrir en el registro de sitios Web para visitar una página y simular el uso. Asimismo, puede buscar en la información de registro según los procesos y sitio y, a continuación, seleccionar Estadísticas en los datos de registro de sitios Web.



**Nota:** Podrá obtener más información acerca de las actividades de Internet de los alumnos si visualiza los registros de sitios Web. Si encuentra registros de sitios Web inadecuados, podrá agregarlos a la lista negra de sitios Web.

## Registro de actividad en la computadora

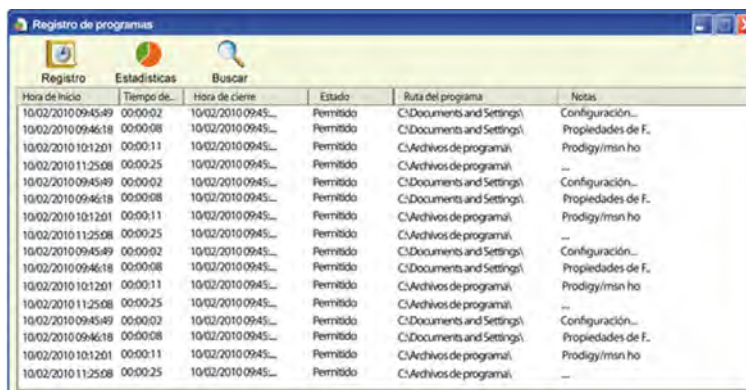


Fecha y Hora	Estado	Ruta de origen	Ruta de destino
10/02/2010 09:45:49	Nueva carpeta	C:\Documents and Settings\Mis documentos\	C:\Documents and Settings\Mis docu
10/02/2010 09:46:18	Renombrar	C:\Documents and Settings\Mis documentos\	C:\Documents and Settings\Mis docu
10/02/2010 10:12:01	Quitar disco	C:\Archivos de programa\Archivos comunes\	C:\Archivos de programa\Archivos co
10/02/2010 11:25:08	Retirar disco esrtal	C:\Archivos de programa\Archivos comunes\	C:\Archivos de programa\Archivos co

Esta utilidad registra la actividad de desplazamiento, copia, eliminación y cambio de nombre de archivos y directorios, así como los eventos de todos los discos CD-ROM, dispositivos USB y disquetes. Puede seleccionar la opción Estadísticas en los datos de registro y hacer clic en Buscar para buscar información en el registro de programas.

El uso de Registro de actividad en la computadora es similar al de la opción **Registro de sitios Web**. Para obtener más información, consulte **Registro de sitios Web**.

## Registro de programas



Hora de inicio	Tiempo de...	Hora de cierre	Estado	Ruta del programa	Notas
10/02/2010 09:45:49	00:00:02	10/02/2010 09:45:...	Permitido	C:\Documents and Settings\	Configuración...
10/02/2010 09:46:18	00:00:08	10/02/2010 09:45:...	Permitido	C:\Documents and Settings\	Propiedades de F.
10/02/2010 10:12:01	00:00:11	10/02/2010 09:45:...	Permitido	C:\Archivos de programa\	Prodigy/msn ho
10/02/2010 11:25:08	00:00:25	10/02/2010 09:45:...	Permitido	C:\Archivos de programa\	...
10/02/2010 09:45:49	00:00:02	10/02/2010 09:45:...	Permitido	C:\Documents and Settings\	Configuración...
10/02/2010 09:46:18	00:00:08	10/02/2010 09:45:...	Permitido	C:\Documents and Settings\	Propiedades de F.
10/02/2010 10:12:01	00:00:11	10/02/2010 09:45:...	Permitido	C:\Archivos de programa\	Prodigy/msn ho
10/02/2010 11:25:08	00:00:25	10/02/2010 09:45:...	Permitido	C:\Archivos de programa\	...
10/02/2010 09:45:49	00:00:02	10/02/2010 09:45:...	Permitido	C:\Documents and Settings\	Configuración...
10/02/2010 09:46:18	00:00:08	10/02/2010 09:45:...	Permitido	C:\Documents and Settings\	Propiedades de F.
10/02/2010 10:12:01	00:00:11	10/02/2010 09:45:...	Permitido	C:\Archivos de programa\	Prodigy/msn ho
10/02/2010 11:25:08	00:00:25	10/02/2010 09:45:...	Permitido	C:\Archivos de programa\	...
10/02/2010 09:45:49	00:00:02	10/02/2010 09:45:...	Permitido	C:\Documents and Settings\	Configuración...
10/02/2010 09:46:18	00:00:08	10/02/2010 09:45:...	Permitido	C:\Documents and Settings\	Propiedades de F.
10/02/2010 10:12:01	00:00:11	10/02/2010 09:45:...	Permitido	C:\Archivos de programa\	Prodigy/msn ho
10/02/2010 11:25:08	00:00:25	10/02/2010 09:45:...	Permitido	C:\Archivos de programa\	...

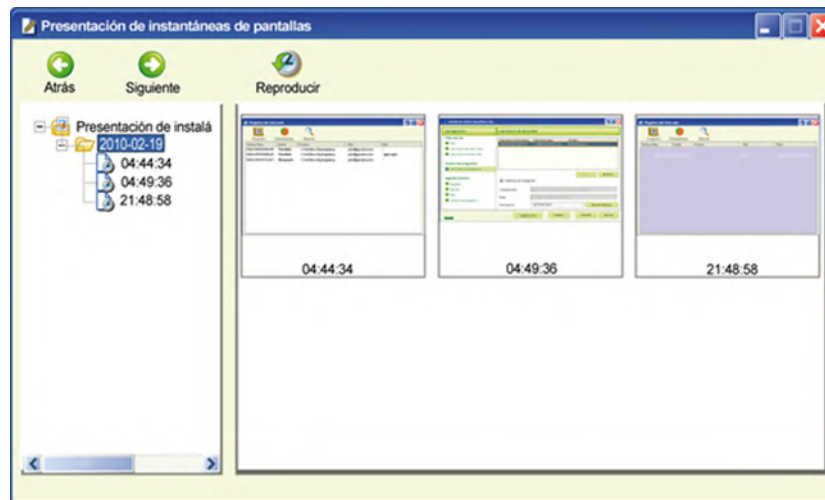
La aplicación Parents Carefree Client puede registrar todos los programas que haya ejecutado el equipo, incluida la hora de inicio, el tiempo de uso, la hora de cierre, el estado, la ruta de acceso y las notas. Puede seleccionar la opción **Estadísticas** en los datos de registro y hacer clic en **Buscar** para buscar información en el registro de programas.

El uso de **Registro de programas** es similar al de la opción **Registro de sitios Web**. Para obtener más información, consulte **Registro de sitios Web**.

**Nota:** Para obtener más información sobre el uso que hacen los alumnos del equipo, consulte los registros de programas. Si un programa no es adecuado para los alumnos (por ejemplo, juegos o programas de chat), podrá agregarlo a la Lista negra de programas.



## Registro de actividad en la computadora



La opción **Presentación de instantáneas** de pantalla registra la imagen de la pantalla automáticamente a intervalos determinados y refleja visualmente la utilización del equipo por parte de los alumnos. Para simular cómo se utiliza el equipo, puede ver las imágenes de pantalla del equipo en una presentación.

Haga clic en el ícono del programa Parents Carefree Client de la bandeja del sistema y seleccione Haga clic en el ícono del programa Parents Carefree Client de la bandeja del sistema y seleccione **Revisión de registro->Presentación de instantáneas de pantalla**. Aparecerá la ventana Presentación de instantáneas de pantalla, en la que podrá ver las instantáneas manualmente o en forma de presentación de diapositivas.. Aparecerá la ventana Presentación de instantáneas de pantalla, en la que podrá ver las instantáneas manualmente o en forma de presentación de diapositivas.

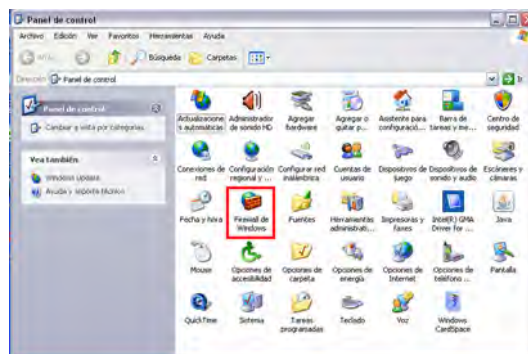


# G. Guía de Software Firewall de Windows

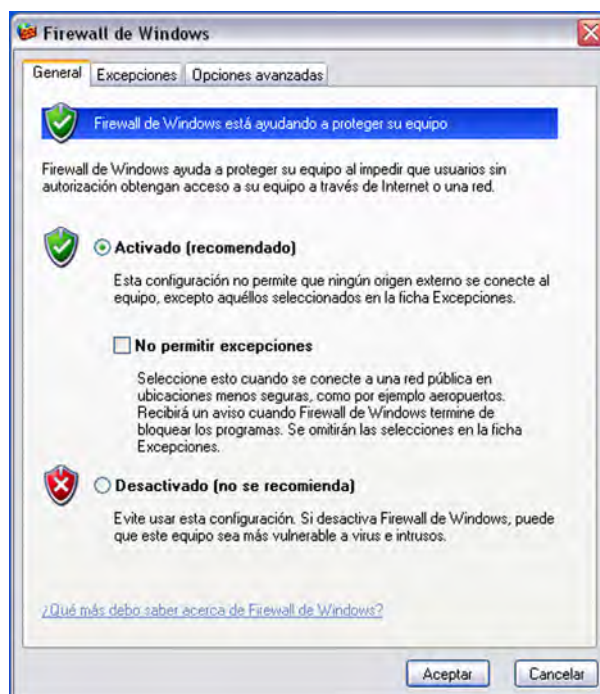
## G.1. Activando el Firewall de Windows

Los siguientes pasos son necesarios para activar el Firewall sobre su equipo:

1. Haga Clic en Inicio -> Panel de Control -> Firewall de Windows.



2. Coloque el Firewall en “Activado (recomendado)” y haga en Clic en **Aceptar**.





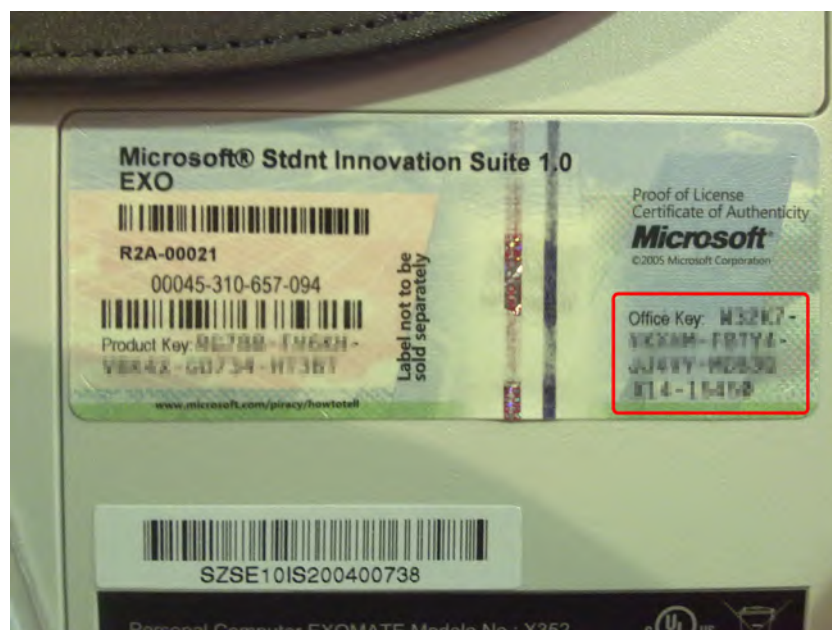
# H. Instructivo de Activación de Microsoft Office y Microsoft Math

El objetivo de este instructivo es detallar los pasos necesarios para activar los productos Microsoft Office 2007 y Microsoft Math 3.0 preinstalados en los equipos MSIS (Microsoft Student Innovation Suite).

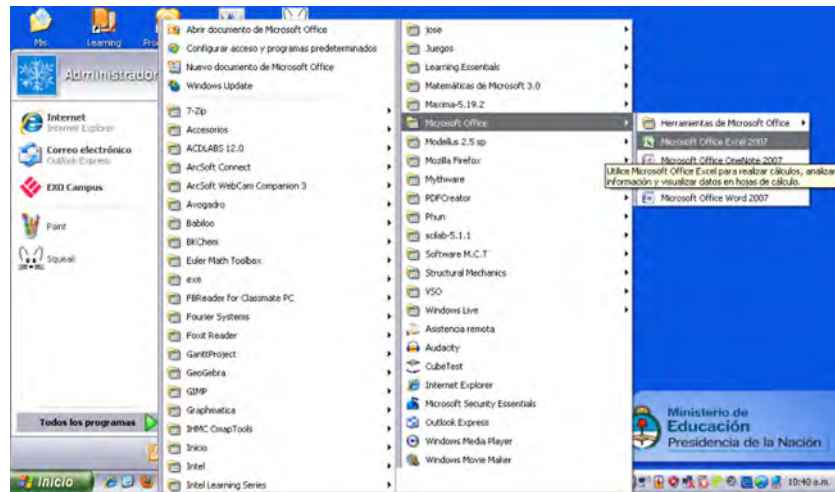
¿Qué ocurre si no se activan? Office permitirá acceder y utilizar las aplicaciones aproximadamente cincuenta veces hasta ingresar en el modo de funcionalidad reducida (por ejemplo, no permitiendo guardar cambios). El mecanismo de activación le asegurara al usuario que su producto es original y que el mismo no conlleva los peligros de un programa adulterado.

## H.1. Activación Microsoft Office 2007

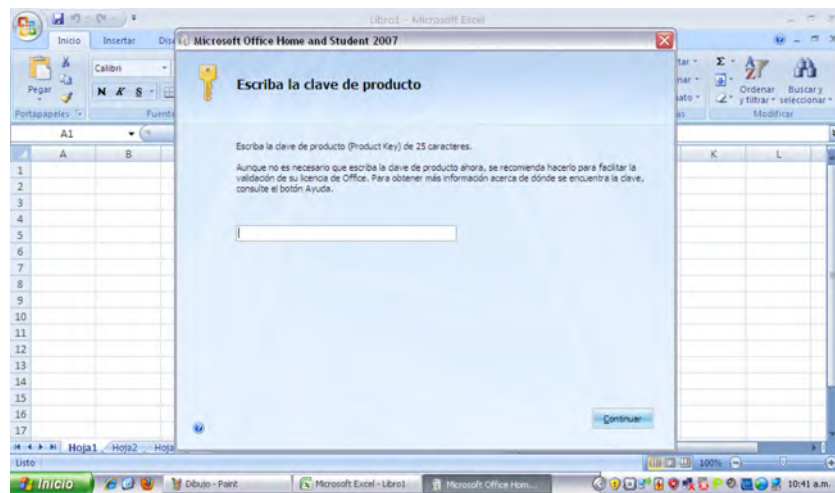
**Requisito previo:** verifique que el código de activación se encuentre adherido a la parte posterior de la Exomate como muestra la foto:



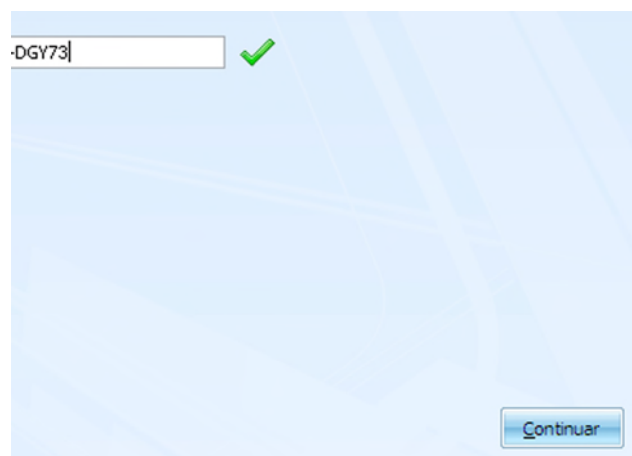
Al iniciar el equipo, será necesario ejecutar alguna aplicación (por ejemplo, Excel) como se muestra en la siguiente pantalla:



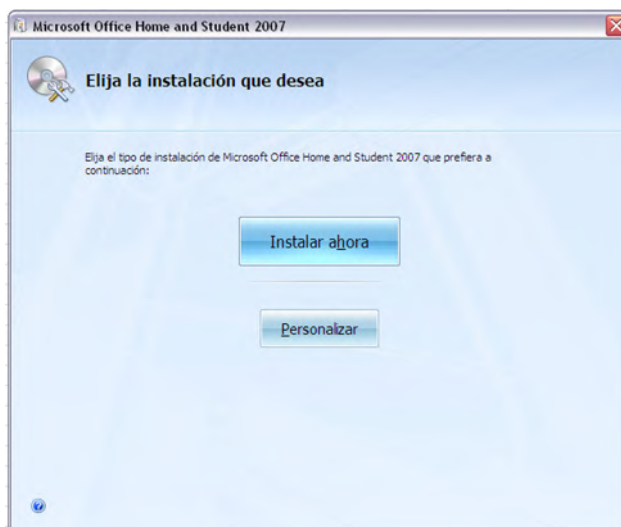
En forma automática, en caso que aún no haya sido activado, Excel solicitará el ingreso de la clave para finalizar la instalación, de la siguiente manera:



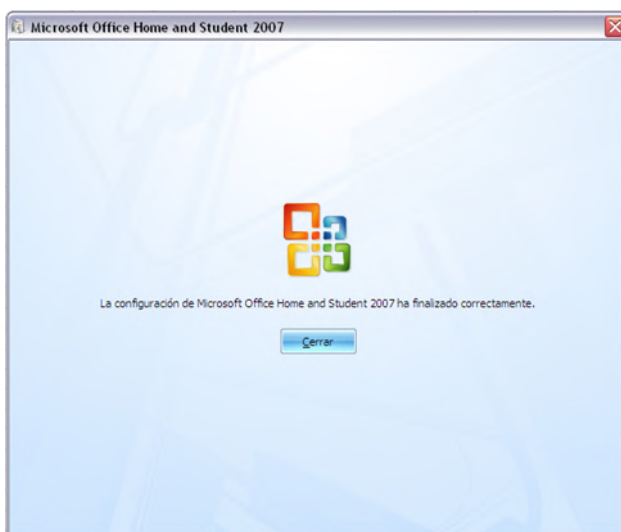
Ingrese la clave del producto que se encuentra en la oblea adjunta a la Exomate. Si la clave es correcta, un tilde verde aparecerá y se iluminará el botón “Continuar”.



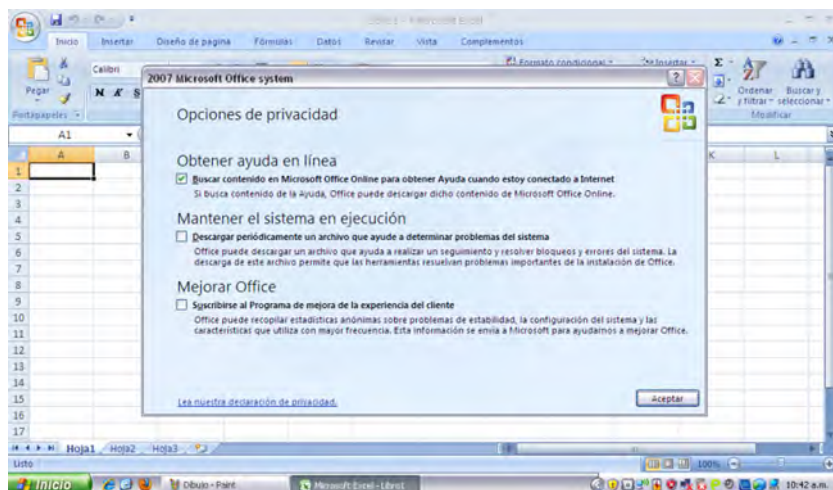
Posteriormente aparecerá una pequeña barra de progreso y luego de esta la pantalla siguiente donde debemos concluir la instalación presionando sobre el botón “Instalar Ahora”.



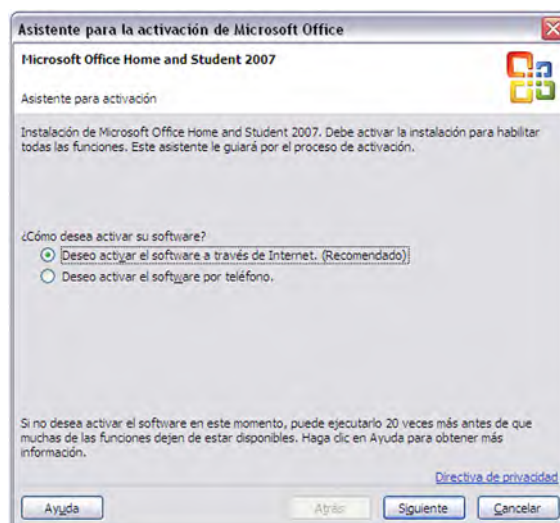
Después de unos segundos de presionado el botón el equipo concluirá la instalación con la siguiente pantalla:



Al presionar “Cerrar” aparecerán por única vez las opciones adicionales para mejorar la experiencia de Office, selecciónelas y luego haga click en “Aceptar”. De esta forma, Microsoft Office finalizara la instalación.

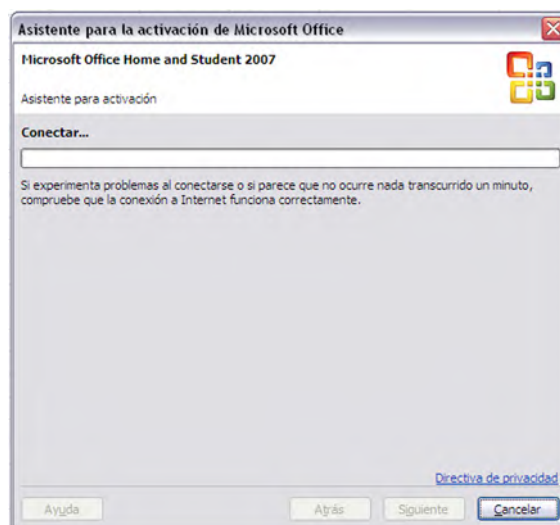


Para poder activar Microsoft Office luego de terminar la instalación debe cerrar el Excel y volverlo a abrir, cuando esto haya sucedido el siguiente mensaje aparecerá!

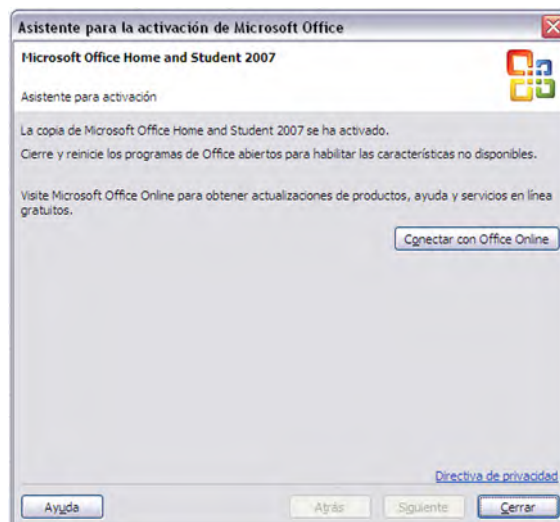


### H.1.1. Activación por Internet

Verifique que haya conexión a Internet y Haga click en siguiente Para que el programa se conecte con los servidores de Activación Microsoft.

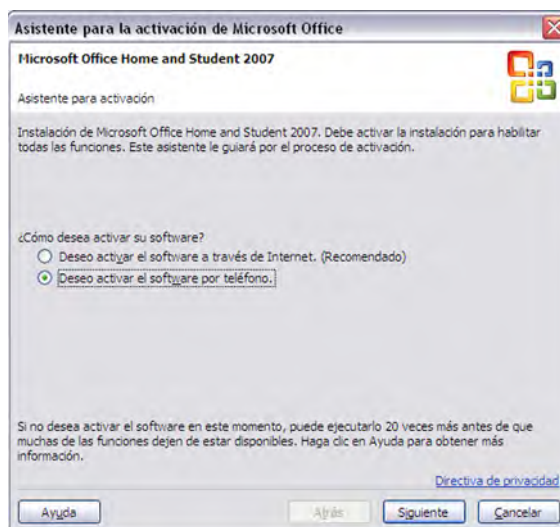


Si el proceso se completa adecuadamente la siguiente pantalla aparecerá y su sistema ya se encontrara Activado y listo para usar.

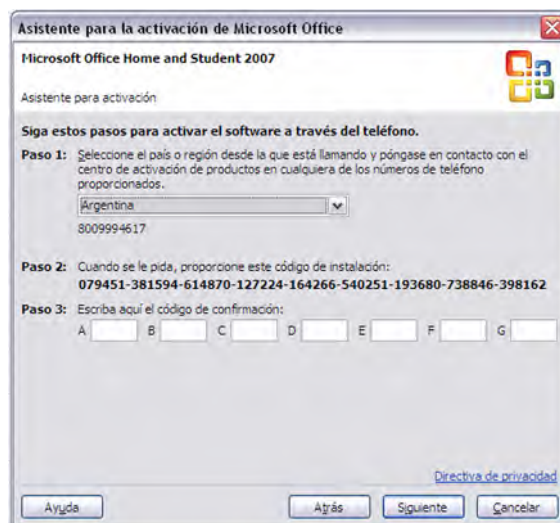


## H.1.2. Activación por teléfono

Para realizar la activación por teléfono seleccione la opción “Deseo activar el software por teléfono” y presione sobre le botón “Siguiente”.



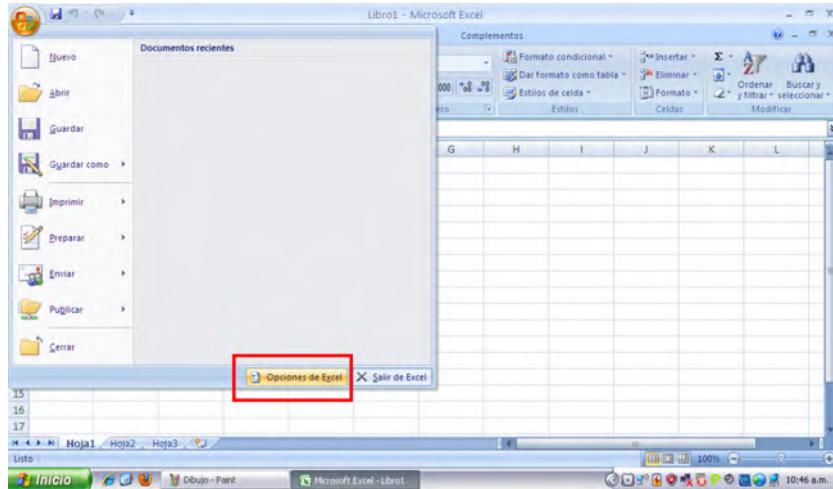
A continuación seleccione el país, cuando lo haga aparecerá el número de teléfono al que debe llamar. Cuando llame, siga las instrucciones del operador del centro de activaciones Microsoft y su sistema quedara activado.



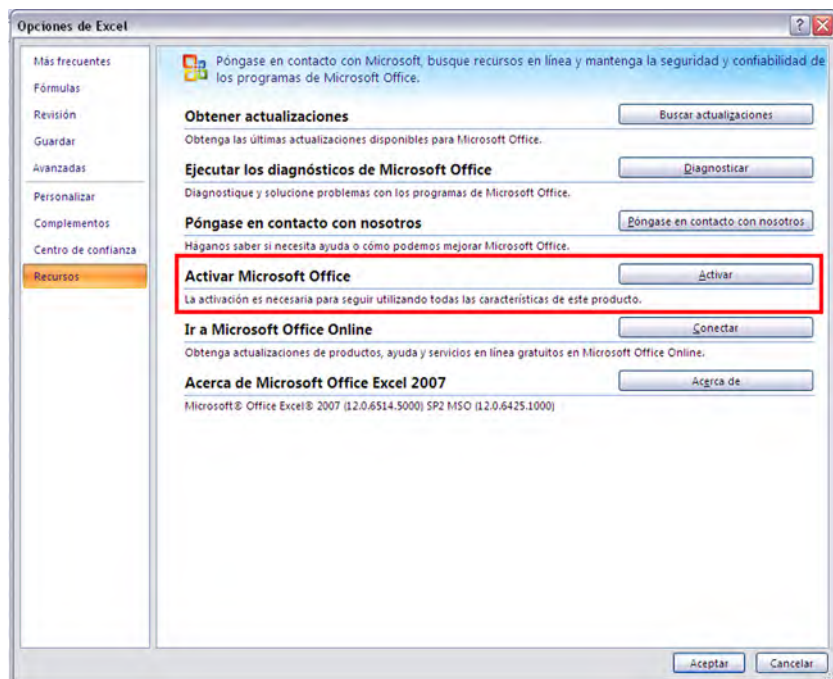
### H.1.3. Activación manual (si no aparece la opción automática)

Si no aparece automáticamente la opción de activación (por ejemplo, si ingreso en el modo de funcionalidad reducida luego de cincuenta usos), debería seguir los siguientes pasos:

- Inicie Excel y haga click en el botón Office (el círculo arriba a la izquierda).
- Luego seleccione “Opciones de Excel” (abajo a la derecha).



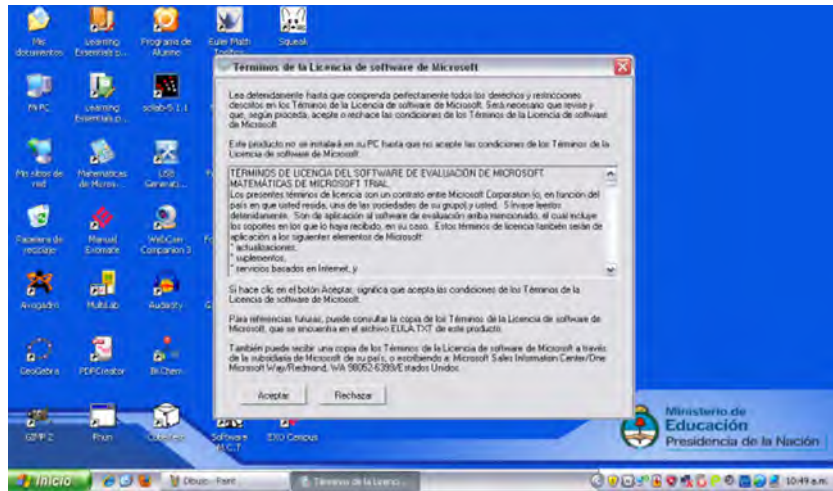
Aparecerá un menú de opciones, una de las cuales le ofrece “Activar Microsoft Office”. Haga click en dicha opción:



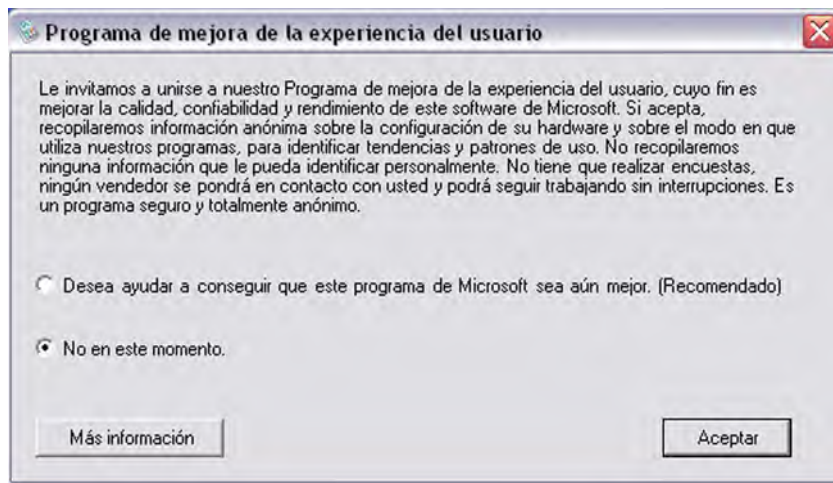




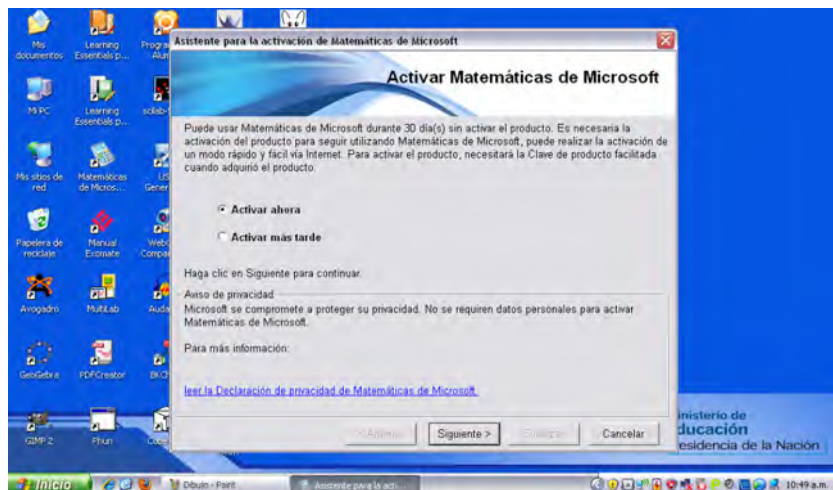
Al iniciar el programa, y previo a cualquier solicitud de ingreso de clave de activación, se le solicitará que acepte los términos y condiciones de uso:



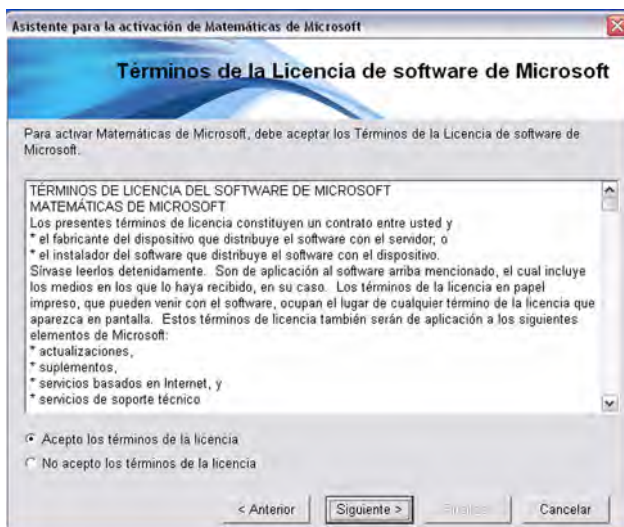
La siguiente pantalla nos preguntara acerca del programa de mejoras de la experiencia del usuario una vez que seleccionemos la opción deseada presionaremos nuevamente “Aceptar”



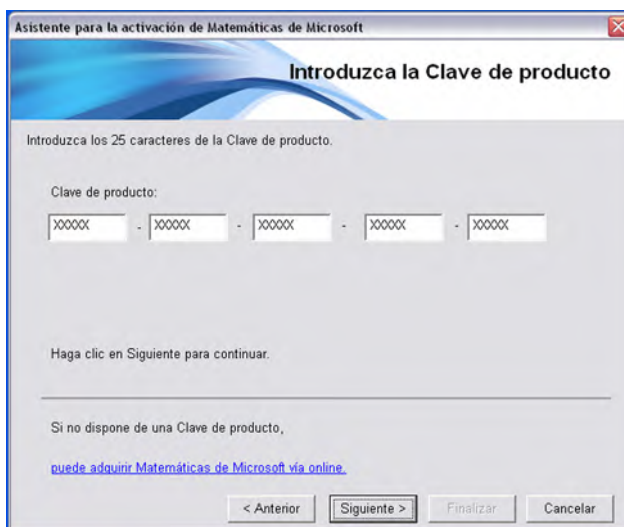
Seleccionaremos desde el tildela opción “Activar ahora” y después presionaremos siguiente:



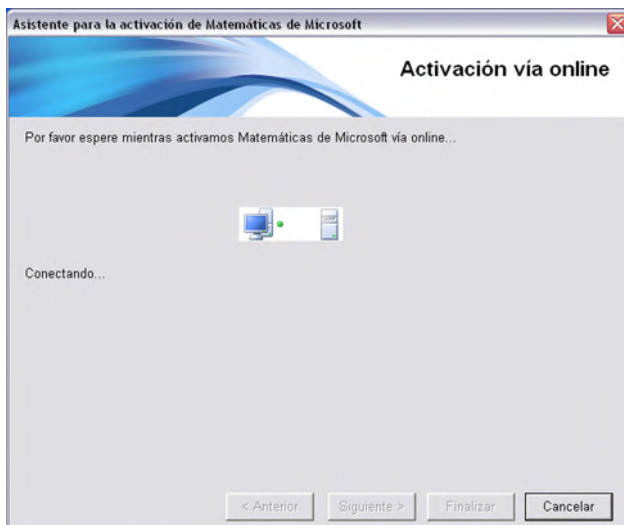
Una vez más aceptaremos los términos de la licencia y presionaremos “Siguiente”



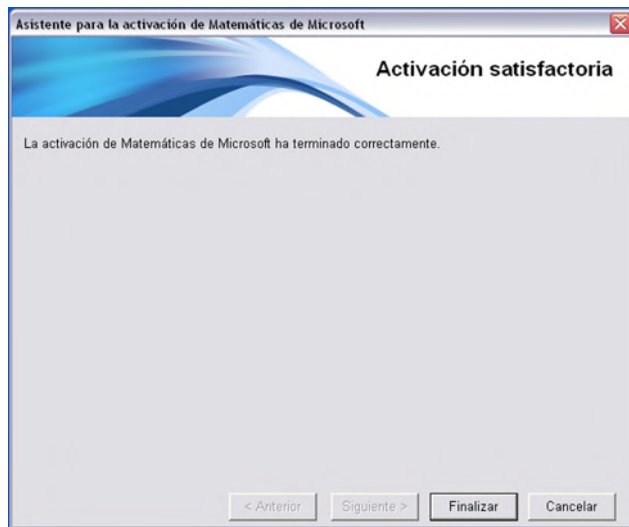
Finalmente, se le solicitará el ingreso de la clave propiamente dicha, al ingresarla haga click en “Siguiente”:



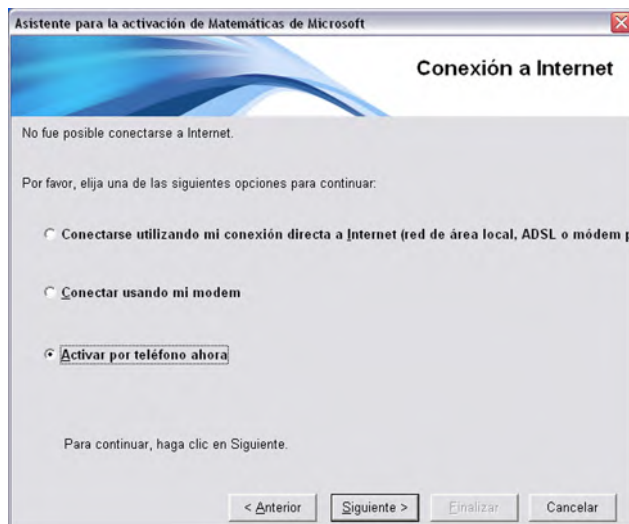
El equipo se conectara a Internet y mostrara la siguiente pantalla.



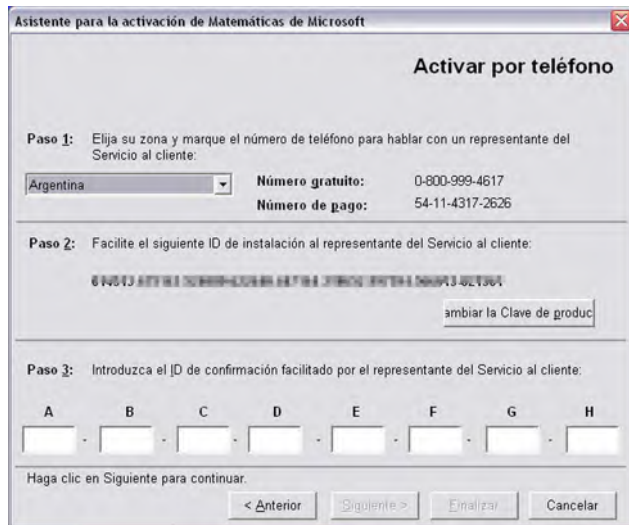
Si el proceso se completa adecuadamente la siguiente pantalla aparecerá y su sistema ya se encontrará Activado y listo para usar.



Si el equipo no logra conectarse a Internet, aparecerá la siguiente pantalla con opciones:



Para activar por teléfono seleccione la opción “Activar por teléfono ahora” y presione siguiente. A continuación seleccione el país, cuando lo haga aparecerá el número de teléfono al que debe llamar. Cuando llame, siga las instrucciones del operador del centro de activaciones Microsoft y su producto quedará activado.



# I. Glosario

Ancho de Banda (Bandwidth)	El ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps).
AP	Un punto de acceso (AP) inalámbrico es un dispositivo que permite que los dispositivos de comunicación inalámbrica se conecten a una red inalámbrica mediante Wi-Fi.
Banda Ancha (Broadband)	Acceso a Internet a un promedio de velocidad alto de datos.
BIOS (Basic Input/Output System)	El BIOS (Sistema Básico de Entrada/Salida) Utilidad de Configuración que ejecuta y mantiene una variedad de funciones del hardware. Contiene el código necesario para controlar los diferentes dispositivos de la PC, como el teclado, la pantalla, las unidades de disco, comunicaciones de serie y otros.
Boot (Arranque)	Arrancar el sistema significa poner en marcha el Sistema Operativo (OS).
Exomate	Exomate.
Conmutador (Switch)	Dispositivo que filtra y reenvía paquetes entre los segmentos de la LAN.
CPU	Unidad Central de Procesamiento (Central Processing Unit). La CPU es donde tienen lugar la mayoría de los cálculos. Conocida como el procesador, es el componente más importante de la computadora.
DSL	Línea de Suscriptor Digital (Digital Subscriber Line), un tipo de acceso a Internet de alta velocidad.
DHCP Server	El servidor DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuración de Anfitrión Dinámico) se utiliza para agregar nuevos dispositivos a la red local de la escuela mediante la asignación de IPs.
DNS	Sistema del Nombre de Dominio (Domain Name System).

---

Router (Enrutador)	Dispositivo que se utiliza para conectar dos o más redes entre sí, y que se utiliza para enviar paquetes de datos a lo largo de las redes.
Firewall (Barrera de protección)	Un sistema diseñado para prevenir el acceso no autorizado a una red privada.
HDD	Unidad de Disco Rígido (Hard Disk Drive).
ILS	Serie de Aprendizaje de Intel (Intel Learning Series).
IP Address (Dirección IP)	Dirección del Protocolo de Internet (IP). Se trata de una dirección lógica y numérica que se asigna a los dispositivos que participan de una red informática.
Listas blancas (White lists)	Una lista de sitios a los que el acceso será permitido.
Listas Negras (Black lists)	Una lista de sitios a los que el acceso estará bloqueado.
LAN	Red de área local (Local Area Network).
Modem	Dispositivo que permite a una computadora transmitir datos a través de líneas telefónicas o de cable.
OS	Sistema Operativo (Operating System). El elemento de software más fundamental. Es responsable de la gestión de todos los aspectos de la computadora y permite que el usuario ejecute e interactúe con todos los demás softwares, incluyendo las aplicaciones.
RF	Radio Frecuencia.
SSID	Identificador de Conjunto de Servicios (Service Set Identifier). Identificador único de 32 caracteres para diferenciar una WLAN de otra, en donde todos los puntos de acceso y dispositivos que intenten conectarse a una WLAN específica deben utilizar el mismo SSID; es conocido por el nombre de red.
Servidor (Server)	Se trata de una computadora o de un dispositivo que gestiona los recursos de red.

---

---

Service Pack(Paquete de Servicios)	Actualización de una versión de software que se descarga o se pide a la empresa. Corrige los problemas existentes, o realiza actualizaciones a las versiones más nuevas de un producto.
TIC	Tecnologías de la Información y Comunicación (Information and Communication Technologies).
Topología de Red (Network Topology)	Se utiliza para referirse a la forma de la LAN o a otro sistema de comunicación.
Wi-Fi	Abreviatura de Wireless Fidelity (Fidelidad Inalámbrica), que es una red de área local que utiliza alta frecuencia de las señales de radio para transmitir y recibir datos a través de distancias de unos pocos cientos de metros con el Protocolo Ethernet.
WiMAX	Interoperabilidad Mundial para Acceso por Microondas. Tecnología de telecomunicaciones que permite la transmisión inalámbrica de datos.
WLAN	Red de Area Local Inalámbrica (Wireless Local Area Network).

---