



Universidad  
Carlos III de Madrid  
[www.uc3m.es](http://www.uc3m.es)

Universidad Carlos III de Madrid

Escuela Politécnica Superior

Departamento de Informática

**Proyecto Fin de carrera de Ingeniería Técnica de  
Informática de Gestión**

*Implantación de un nuevo sistema de autenticación en las aulas  
informáticas del Departamento de informática basado en LDAP*

**Autor: Roberto Fuentes Astorga**

**Tutor: Óscar Pérez Alonso**

Leganés, Octubre de 2012



A mi familia.

“La ciencia no sirve sino para darnos una  
idea de cuan vasta es nuestra ignorancia”  
**Félicité de Lamennais**





# Agradecimientos

En primer lugar quiero agradecer el apoyo de mi familia, que siempre está en los momentos difíciles.

En segundo lugar se lo quiero agradecer a mis compañeros de trabajo, Óscar y Jaime que me han echado una mano siempre que lo he necesitado para ayudarme a depurar fallos en la implantación del proyecto.

En tercer lugar se lo quiero agradecer a Yoshi y Sergi que me ayudaron a construir las bases de mis conocimientos sobre administración de sistemas.

En último lugar, aunque no menos importante, quiero dedicar unos agradecimientos a todos los profesores que me han formado durante la carrera y en especial a todos los integrantes de ARCOS, que me han inculcado interés por los sistemas operativos.



# Tabla de Contenido

Agradecimientos .....	5
Tabla de Contenido.....	7
Índice de Figuras .....	11
Índice de Tablas .....	13
Capítulo 1    Introducción.....	17
1.1.    Motivación.....	17
1.2.    Objetivos .....	18
1.3.    Estructura del documento .....	19
Capítulo 2    Estado del arte .....	21
2.1.    Sistemas de autenticación.....	21
2.1.1.    NIS.....	21
2.1.2.    LDAP .....	23
2.1.3.    Active Directory .....	27
2.2.    Sistemas operativos .....	31
2.2.1.    Microsoft Windows .....	31
2.2.2.    Unix .....	35
2.2.3.    GNU/Linux.....	36
2.2.4.    Otros.....	37
2.3.    Virtualización de Sistemas Operativos .....	38
2.3.1.    VMware .....	39
2.3.2.    KVM.....	41
2.3.3.    Xen .....	42
2.4.    Otros servicios .....	46
2.4.1.    Web .....	46
2.4.2.    DNS .....	47
2.4.3.    DHCP .....	48
2.4.4.    SAMBA .....	48
2.4.5.    Sistema de archivos de red.....	49
Capítulo 3    Análisis.....	51
3.1.    Situación actual del Laboratorio del Departamento de Informática .....	51
3.1.1.    Entorno Linux.....	52

---

3.1.2.	Entorno Windows .....	53
3.1.3.	Apertura de cuentas.....	55
3.1.4.	Administración de cuentas de usuario.....	57
3.2.	Descripción general.....	59
3.2.1.	Funcionalidades .....	59
3.2.2.	Restricciones .....	59
3.2.3.	Características de los usuarios .....	60
3.2.4.	Entorno operacional.....	60
3.3.	Requisitos del sistema.....	61
3.3.1.	Requisitos de capacidad .....	62
3.3.2.	Requisitos de restricción .....	67
3.4.	Casos de uso .....	70
Capítulo 4	Diseño.....	73
4.1.	Establecimiento de requisitos software .....	73
4.1.1.	Requisitos funcionales .....	74
4.1.2.	Requisitos de rendimiento.....	82
4.1.3.	Requisitos de interfaz.....	83
4.1.4.	Requisitos de operación.....	85
4.1.5.	Requisitos de recursos .....	87
4.1.6.	Requisitos de comprobación.....	88
4.1.7.	Requisitos de seguridad.....	88
4.1.8.	Requisitos de fiabilidad .....	89
4.2.	Diseño de la arquitectura de la red.....	90
4.2.1.	Identificación de los subsistemas de diseño .....	91
4.2.2.	Especificación del entorno tecnológico .....	101
4.3.	Diseño arquitectónico de la aplicación web.....	104
4.3.1.	Diagramas de navegación.....	104
4.4.	Matrices de trazabilidad .....	106
4.4.1.	Matriz de trazabilidad entre UR/SR .....	106
4.4.2.	Matriz de trazabilidad entre SR/Comp .....	107
Capítulo 5	Implantación.....	109
5.1.	Instalación del servidor LDAP .....	109
5.1.1.	Instalación de la máquina virtual.....	110
5.1.2.	Instalación del servicio ldap.....	111
5.1.3.	Instalación del servicio Samba .....	113
5.1.4.	Tareas posteriores a la instalación .....	114
5.2.	Instalación del servidor CUENTAS.....	115
5.2.1.	Instalación de la máquina virtual.....	115
5.2.2.	Configuración del cliente ldap.....	115
5.2.3.	Instalación del servicio Samba .....	116
5.2.4.	Ajuste de cuotas de usuario .....	116

---

---

5.3.	Modificaciones realizadas en el servidor CORREO.....	117
5.4.	Modificaciones realizadas en el servidor WEB.....	118
5.4.1.	Creación de las nuevas páginas web.....	118
5.4.2.	Instalación de software y activación de módulos.....	120
5.4.3.	Instalación de Ldap Account Manager.....	121
5.5.	Configuración de los clientes .....	123
5.5.1.	Cliente Linux .....	123
5.5.2.	Cliente Windows.....	124
5.6.	Actualizador de políticas .....	127
5.6.1.	Scripts y ficheros implicados.....	127
5.6.2.	Proceso de actualización .....	128
5.6.3.	Creación de las políticas de grupo.....	131
5.7.	Tareas Programadas.....	134
5.8.	Gestor de políticas y tareas programadas (PolGest).....	136
5.8.1.	Funcionamiento del gestor de políticas .....	136
5.8.2.	Funcionamiento del gestor de tareas programadas.....	140
5.9.	Tareas finales.....	143
5.9.1.	Migración de usuarios .....	143
5.9.2.	Copia de seguridad.....	144
5.9.3.	Script de gestión de usuarios GESTION.....	144
5.9.4.	Preparación del cliente Windows para clonación .....	147
5.9.5.	Creación del perfil de usuario en Windows .....	149
Capítulo 6	Pruebas del sistema .....	151
6.1.	Pruebas del servidor LDAP .....	152
6.1.1.	Prueba del servicio de autenticación .....	152
6.1.2.	Prueba del módulo de creación de cuentas.....	154
6.1.3.	Prueba de la aplicación de gestión de usuarios .....	155
6.1.4.	Prueba de la copia de seguridad .....	158
6.1.5.	Prueba del repositorio de perfiles de usuario.....	159
6.1.6.	Prueba del repositorio de configuración de clientes.....	160
6.2.	Pruebas del servidor CUENTAS .....	161
6.2.1.	Prueba del servicio de datos de usuario .....	161
6.2.2.	Prueba del servicio de autenticación .....	162
6.3.	Prueba del servidor CORREO.....	163
6.4.	Pruebas del servidor WEB .....	164
6.5.	Pruebas del cliente WINDOWS .....	166
6.5.1.	Prueba del módulo tareas .....	166
6.5.2.	Prueba de la política de equipo.....	167
6.5.3.	Prueba de autenticación.....	168
6.6.	Pruebas del cliente LINUX.....	170
6.7.	Pruebas del servidor POLÍTICAS.....	171

---

---

Capítulo 7	Presupuesto y planificación .....	175
7.1.	Estimación.....	175
7.1.1.	Estimación del tamaño.....	177
7.1.2.	Estimación del esfuerzo.....	180
7.2.	Planificación.....	185
7.3.	Presupuesto.....	188
7.3.1.	Costes de personal.....	188
7.3.2.	Costes de material inventariable.....	189
7.3.3.	Costes de software .....	189
7.3.4.	Coste total .....	190
Capítulo 8	Conclusiones y trabajos futuros.....	191
8.1.	Conclusiones.....	191
8.2.	Trabajos futuros.....	193
Capítulo 9	Acrónimos y abreviaturas.....	195
Capítulo 10	Bibliografía y referencias .....	199
Capítulo 11	Apéndice.....	203
11.1.	Ficheros de configuración.....	203
11.1.1.	Servidor LDAP.....	203
11.1.2.	Servidor CUENTAS .....	213
11.1.3.	Servidor CORREO .....	217
11.1.4.	Cliente Linux.....	217
11.2.	Scripts .....	219
11.2.1.	Cuotas de usuario.....	219
11.2.2.	Actualizador de políticas .....	219
11.3.	Páginas web y código php.....	236
11.3.1.	Actualizar Cuenta   Cambiar contraseña.....	236
11.3.2.	Apertura de cuentas .....	237
11.3.3.	Estado de tu cuenta.....	239
11.3.4.	Abrir nueva cuenta.....	241

# Índice de Figuras

Figura 2.1. Arquitectura de Xen.....	43
Figura 3.1. Infraestructura Linux. ....	53
Figura 3.2. Infraestructura Windows.....	54
Figura 3.3. Página web de apertura de cuentas.....	55
Figura 3.4. Pantalla principal de la herramienta GESTION. ....	57
Figura 3.5. Pantalla principal de gestión de usuarios Windows.....	58
Figura 3.6. Diagrama de casos de uso.....	70
Figura 4.1. Estructura del sistema.....	91
Figura 4.2. Diagrama de subsistemas y componentes. ....	92
Figura 4.3. Rack de los servidores físicos perteneciente al ldi.....	102
Figura 4.4. Diagrama de navegación de la página “Apertura de Cuentas”. ....	104
Figura 4.5. Diagrama de navegación de la página “Actualizar cuenta   Cambiar contraseña”.....	105
Figura 5.1. Página inicio de sesión de la administración de la página web. ....	118
Figura 5.2. Página de creación de contenido.....	119
Figura 5.3. Configuración general de la herramienta LAM.....	121
Figura 5.4. Configuración relativa al Perfil del servidor. ....	122
Figura 5.5. Cuadro de diálogo de propiedades del sistema.....	124
Figura 5.6. Cuadro de diálogo “Cambios en el dominio o el nombre del equipo”. .....	125
Figura 5.7. Cuadro de solicitud de credenciales.....	125
Figura 5.8. Mensaje de confirmación de unión al dominio.....	126
Figura 5.9. Ventana de propiedades del sistema.....	126
Figura 5.10. Vista del log que registra el actualizador de políticas.....	129
Figura 5.11. Detalle de un evento del registro de log.....	130
Figura 5.12. Detalle de evento tipo información.....	130
Figura 5.13. Editor de directivas de grupo local.....	131
Figura 5.14. Cuadro de diálogo de búsqueda de objeto de directiva de grupo.....	133
Figura 5.15. Ventana principal del Programador de tareas.....	134
Figura 5.16. Ventana “Crear tarea”.....	135
Figura 5.17. Pantalla principal de la herramienta PolGest.....	136

---

Figura 5.18. Ventana de gestión de políticas de aula.....	137
Figura 5.19. Ventana de gestión de políticas de equipo. ....	138
Figura 5.20. Ventana de políticas existentes en el almacén. ....	139
Figura 5.21. Pantalla principal de la herramienta PolGest.....	140
Figura 5.22. Ventana de gestión de tareas de aula. ....	141
Figura 5.23. Ventana de gestión de tareas programadas de un equipo. ....	142
Figura 5.24. Menú principal. ....	145
Figura 5.25. Menú de gestión de usuario. ....	145
Figura 5.26. Consulta de datos de un usuario.....	146
Figura 5.27. Ventana de propiedades avanzadas del perfil de usuario. ....	150
Figura 5.28. Cuadro de diálogo “Copiar a”.....	150
Figura 7.1. Estructura del sistema.....	175
Figura 7.2. Factores de escala.....	180
Figura 7.3. Factores de escala correspondientes al módulo Web. ....	181
Figura 7.4. Factores de escala correspondientes al módulo Ldap.....	181
Figura 7.5. Factores de escala correspondientes al módulo Cuentas. ....	182
Figura 7.6. Factores de escala correspondientes al módulo Cliente Windows..	182
Figura 7.7. Factores de escala correspondientes al módulo Cliente Linux. ....	183
Figura 7.8. Estimación del esfuerzo del proyecto.....	183
Figura 7.9. Diagrama de Gantt del proyecto. ....	187



# Índice de Tablas

Tabla 2.1. Distribuciones de Linux.....	37
Tabla 3.1. Requisito RC-001.....	62
Tabla 3.2. Requisito RC-002.....	62
Tabla 3.3. Requisito RC-003.....	63
Tabla 3.4. Requisito RC-004.....	63
Tabla 3.5. Requisito RC-005.....	63
Tabla 3.6. Requisito RC-006.....	64
Tabla 3.7. Requisito RC-007.....	64
Tabla 3.8. Requisito RC-008.....	64
Tabla 3.9. Requisito RC-009.....	64
Tabla 3.10. Requisito RC-010.....	65
Tabla 3.11. Requisito RC-011.....	65
Tabla 3.12. Requisito RC-012.....	65
Tabla 3.13. Requisito RC-013.....	65
Tabla 3.14. Requisito RC-014.....	66
Tabla 3.15. Requisito RC-015.....	66
Tabla 3.16. Requisito RC-016.....	66
Tabla 3.17. Requisito RC-017.....	66
Tabla 3.18. Requisito RC-018.....	67
Tabla 3.19. Requisito RR-001.....	67
Tabla 3.20. Requisito RR-002.....	67
Tabla 3.21. Requisito RR-003.....	68
Tabla 3.22. Requisito RR-004.....	68
Tabla 3.23. Requisito RR-005.....	68
Tabla 3.24. Requisito RR-006.....	68
Tabla 3.25. Requisito RR-007.....	69
Tabla 3.26. Requisito RR-008.....	69
Tabla 3.27. CU-01 Abrir cuenta. ....	71
Tabla 3.28. CU-02 Actualizar cuenta. ....	71
Tabla 3.29. CU-03 Cambiar contraseña.....	72
Tabla 3.30. CU-04 Ver estado de la cuenta. ....	72
Tabla 4.1. Requisito RSF-001.....	74

---

Tabla 4.2. Requisito RSF-002.....	74
Tabla 4.3. Requisito RSF-003.....	74
Tabla 4.4. Requisito RSF-004.....	75
Tabla 4.5. Requisito RSF-005.....	75
Tabla 4.6. Requisito RSF-006.....	75
Tabla 4.7. Requisito RSF-007.....	75
Tabla 4.8. Requisito RSF-008.....	76
Tabla 4.9. Requisito RSF-009.....	76
Tabla 4.10. Requisito RSF-010.....	76
Tabla 4.11. Requisito RSF-011.....	76
Tabla 4.12. Requisito RSF-012.....	77
Tabla 4.13. Requisito RSF-013.....	77
Tabla 4.14. Requisito RSF-014.....	77
Tabla 4.15. Requisito RSF-015.....	77
Tabla 4.16. Requisito RSF-016.....	78
Tabla 4.17. Requisito RSF-017.....	78
Tabla 4.18. Requisito RSF-018.....	78
Tabla 4.19. Requisito RSF-019.....	78
Tabla 4.20. Requisito RSF-020.....	79
Tabla 4.21. Requisito RSF-021.....	79
Tabla 4.22. Requisito RSF-022.....	79
Tabla 4.23. Requisito RSF-023.....	80
Tabla 4.24. Requisito RSF-024.....	80
Tabla 4.25. Requisito RSF-025.....	80
Tabla 4.26. Requisito RSF-026.....	80
Tabla 4.27. Requisito RSF-027.....	81
Tabla 4.28. Requisito RSF-028.....	81
Tabla 4.29. Requisito RSF-029.....	81
Tabla 4.30. Requisito RSF-030.....	81
Tabla 4.31. Requisito RSF-031.....	82
Tabla 4.32. Requisito RSR-001.....	82
Tabla 4.33. Requisito RSR-002.....	82
Tabla 4.34. Requisito RSR-003.....	83
Tabla 4.35. Requisito RSI-001.....	83
Tabla 4.36. Requisito RSI-002.....	83
Tabla 4.37. Requisito RSI-003.....	84
Tabla 4.38. Requisito RSI-004.....	84
Tabla 4.39. Requisito RSI-005.....	85
Tabla 4.40. Requisito RSO-001.....	85
Tabla 4.41. Requisito RSO-002.....	85
Tabla 4.42. Requisito RSO-003.....	86

---

---

Tabla 4.43. Requisito RSF-004.....	86
Tabla 4.44. Requisito RSRe-001.....	87
Tabla 4.45. Requisito RSRe-002.....	87
Tabla 4.46. Requisito RSC-001.....	88
Tabla 4.47. Requisito RSS-001.....	88
Tabla 4.48. Requisito RSS-002.....	88
Tabla 4.49. Requisito RSS-003.....	89
Tabla 4.50. Requisito RSS-004.....	89
Tabla 4.51. Requisito RSFi-001.....	89
Tabla 4.52. COML-01 Módulo creación cuentas.....	94
Tabla 4.53. COML-02 Apps gestión usuarios.....	94
Tabla 4.54. COML-03 Config clientes.....	95
Tabla 4.55. COML-04 Perfiles usuario.....	95
Tabla 4.56. COML-05 Servicio autenticación.....	96
Tabla 4.57. COML-06 Backup LDAP.....	96
Tabla 4.58. COMC-01 Servicio autenticación.....	97
Tabla 4.59. COMC-02 Servicio autenticación.....	97
Tabla 4.60. COMCo-01 Servicio de correo.....	98
Tabla 4.61. COMW-01 Aplicación registro.....	98
Tabla 4.62. COMCW-01 Tareas.....	99
Tabla 4.63. COMCW-02 Política equipo.....	99
Tabla 4.64. COMCW-03 Autenticación.....	100
Tabla 4.65. COMCW-01 Autenticación.....	100
Tabla 4.66. COMB-01 Apps gestión políticas/tareas.....	101
Tabla 4.67. Matriz de trazabilidad UR/SR.....	106
Tabla 4.68. Matriz de trazabilidad SR/Comp.....	108
Tabla 6.1. PRU-001 Autenticación de usuario cuenta Linux.....	152
Tabla 6.2. PRU-002 Autenticación de usuario cuenta Windows.....	152
Tabla 6.3. PRU-003 Consulta de cuenta de usuario.....	153
Tabla 6.4. PRU-004 Creación de cuenta de usuario.....	154
Tabla 6.5. PRU-005 Cambio de contraseña de usuario.....	154
Tabla 6.6. PRU-006 Creación de cuenta de usuario.....	155
Tabla 6.7. PRU-007 Consulta de datos personales de usuario.....	155
Tabla 6.8. PRU-008 Cambio de datos personales de usuario.....	156
Tabla 6.9. PRU-009 Generación y envío de contraseña aleatoria.....	156
Tabla 6.10. PRU-010 Bloqueo de cuenta de usuario.....	156
Tabla 6.11. PRU-011 Desbloqueo de cuenta de usuario.....	157
Tabla 6.12. PRU-012 Consulta de usuarios que han excedido la cuota.....	157
Tabla 6.13. PRU-013 Realización y Restauración de copia de seguridad.....	158
Tabla 6.14. PRU-014 Comprobación de accesibilidad al repositorio.....	159
Tabla 6.15. PRU-015 Comprobación de permisos de lectura y escritura.....	159

---

---

Tabla 6.16. PRU-016 Comprobación de accesibilidad al repositorio.....	160
Tabla 6.17. PRU-017 Comprobación de permisos de lectura y escritura. ....	160
Tabla 6.18. PRU-018 Comprobación de accesibilidad a los datos de usuario. .	161
Tabla 6.19. PRU-019 Comprobación de permisos de lectura y escritura. ....	161
Tabla 6.20. PRU-020 Autenticación de usuario cuenta Windows.....	162
Tabla 6.21. PRU-021 Envío de mail desde el servidor LDAP.....	163
Tabla 6.22. PRU-022 Creación de cuenta.....	164
Tabla 6.23. PRU-023 Actualización de cuenta. ....	164
Tabla 6.24. PRU-024 Cambio de contraseña de cuenta.....	165
Tabla 6.25. PRU-025 Consultar existencia de cuenta.....	165
Tabla 6.26. PRU-026 Sincronización de tareas programadas.....	166
Tabla 6.27. PRU-027 Instalación de tarea programada. ....	166
Tabla 6.28. PRU-028 Sincronización y aplicación de política de equipo. ....	167
Tabla 6.29. PRU-029 Autenticación de usuario que no sea tipo asignatura. ...	168
Tabla 6.30. PRU-030 Autenticación de usuario tipo asignatura.....	168
Tabla 6.31. PRU-031 Montaje de home de usuario. ....	169
Tabla 6.32. PRU-032 Sincronización de <i>scripts</i> genéricos.....	169
Tabla 6.33. PRU-033 Autenticación de usuario.....	170
Tabla 6.34. PRU-034 Montaje de home de usuario. ....	170
Tabla 6.35. PRU-035 Comunicación de contraseña cifrada con el servidor. ....	170
Tabla 6.36. PRU-036 Distribución de política a un aula. ....	171
Tabla 6.37. PRU-037 Distribución de política a un equipo.....	171
Tabla 6.38. PRU-038 Consulta de almacén de políticas. ....	172
Tabla 6.39. PRU-039 Distribución de tarea programada a un aula.....	172
Tabla 6.40. PRU-040 Distribución de tarea programada a un equipo. ....	173
Tabla 6.41. PRU-041 Consulta de almacén de tareas programadas.....	173
Tabla 7.1. Resumen de la estimación del tamaño.....	179
Tabla 7.2. Costes de personal.....	188
Tabla 7.3. Costes de material inventariable.....	189
Tabla 7.4. Costes de software.....	190
Tabla 7.5. Coste total.....	190
Tabla 8.1. Comparación de las líneas de código estimadas y reales.....	192

# Capítulo 1

## Introducción

En este capítulo se expone la motivación de la realización del proyecto desarrollando los objetivos que se persiguen, además de describir la estructura de este documento.

### 1.1. Motivación

Este proyecto se ha realizado en el Laboratorio del Departamento de Informática durante el curso académico 2011-2012, en el cual estoy trabajando en calidad de técnico de laboratorio.

La motivación principal del proyecto ha sido la mejora e integración del sistema de sistema de autenticación con el que contaban las aulas informáticas del Laboratorio del Departamento de Informática.

Por un lado, para autenticar usuarios con el sistema operativo GNU/Linux se disponía de un servidor de autenticación basado la tecnología NIS. Por otro lado, para autenticar usuarios con el sistema operativo Microsoft Windows se disponía de un sistema de autenticación propietario denominado *Active Directory*.

Además de tener dos servidores de autenticación para realizar la misma función, otros problemas añadidos eran:

- El retraso en la creación de las cuentas de usuario: se realizaba al principio de las clases y hasta que no se completara el proceso los alumnos no podían acceder a los ordenadores de las aulas.
- No sincronización entre ambos sistemas de autenticación: no se abrían cuenta a los alumnos en ambos sistemas.

## 1.2. Objetivos

El principal objetivo de este proyecto es realizar el análisis, diseño, implementación, implantación y pruebas de un mejor sistema de autenticación para las aulas del Laboratorio del Departamento de Informática.

Los objetivos secundarios que se esperan conseguir del nuevo sistema de autenticación son los siguientes:

- Facilitar la administración de cuentas de usuario.
- Automatizar la creación de cuentas de usuario mediante la página web.
- Integrar el servicio de autenticación para todos los sistemas operativos instalados en las aulas informáticas.
- Mejorar el aprovechamiento de los recursos del laboratorio permitiendo liberar un servidor para utilizarlo en otras tareas.

## 1.3. Estructura del documento

El documento se divide en los siguientes capítulos:

- **Introducción**, en este capítulo se desarrolla la motivación, objetivo y la estructura del documento.
- **Estado del arte**, en este capítulo se expone toda la información relativa a las tecnologías existentes necesarias para desarrollar la solución propuesta.
- **Análisis**, en este capítulo se muestra el análisis del problema planteado.
- **Diseño**, en este capítulo se muestra el diseño de la solución propuesta.
- **Implantación**, en este capítulo se exponen las fases que se han llevado a cabo para la implementación de la solución.
- **Pruebas del Sistema**, en este capítulo se muestran las pruebas de validación realizadas al nuevo sistema.
- **Presupuesto y planificación**, en este capítulo se expone el presupuesto y la planificación realizada para llevar a cabo el proyecto.
- **Conclusiones y trabajos futuros**, en este capítulo se expone las conclusiones extraídas del trabajo realizado y los trabajos futuros para mejorar el sistema.
- **Acrónimos y abreviaturas**, en este capítulo se exponen los acrónimos y abreviaturas encontradas en el documento.
- **Bibliografía y referencias**, en este capítulo se muestra las fuentes externas de información que han sido necesarias para la realización del proyecto.
- **Apéndice**, en este capítulo se muestran los ficheros de configuración y *scripts* utilizados.





# Capítulo 2

## Estado del arte

En este capítulo se analizan las distintas tecnologías disponibles para la realización de la solución propuesta en este proyecto.

### 2.1. Sistemas de autenticación

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización y/o auditoría oportunos.

A continuación se analizarán los sistemas de autenticación de mayor relevancia.

#### 2.1.1. NIS

*Network Information Service*<sup>[1]</sup> (conocido por su acrónimo NIS, que en español significa Sistema de Información de Red), es el nombre de un protocolo de servicios de directorios cliente-servidor desarrollado por Sun Microsystems para el envío de datos de configuración en sistemas distribuidos tales como nombres de usuarios y hosts entre computadoras sobre una red. NIS consta de un servidor, una biblioteca de la parte cliente, y varias herramientas de administración.

### 2.1.1.1. *Historia*

Originalmente NIS se llamaba Páginas Amarillas (*Yellow Pages*), o YP, que todavía se utiliza para referirse a él. Desafortunadamente, ese nombre es una marca registrada de British Telecom, que exigió a Sun abandonar ese nombre. Sin embargo YP permanece como prefijo en los nombres de la mayoría de las órdenes relacionadas con NIS, como ypserv e ypbind.

NIS proporciona prestaciones de acceso a bases de datos genéricas que pueden utilizarse para distribuir, por ejemplo, la información contenida en los ficheros *passwd* y *groups* a todos los nodos de su red. Esto hace que la red parezca un sistema individual, con las mismas cuentas en todos los nodos. De manera similar, se puede usar NIS para distribuir la información de nombres de nodo contenida en */etc/hosts* a todas las máquinas de la red.

### 2.1.1.2. *Implementaciones*

Actualmente NIS está disponible prácticamente en todas las distribuciones de Unix, e incluso existen implementaciones libres. El código de la biblioteca de la parte cliente de esta versión existe en la libc de GNU/Linux desde hace mucho tiempo, y los programas de administración fueron portados a GNU/Linux por Swen Thümmler. Sin embargo, falta un servidor NIS a partir de la implementación de referencia.

Peter Eriksson ha desarrollado una implementación nueva llamada NYS. Soporta tanto NIS básico como la versión mejorada de Sun NIS+ <sup>[2]</sup>. NYS no sólo proporciona una serie de herramientas NIS y un servidor, sino que también añade un completo juego nuevo de funciones de biblioteca que necesita compilar en su libc si quiere utilizarlas. Esto incluye un esquema nuevo de configuración para la resolución de nombres de nodo que sustituye al esquema actual que usa el fichero *host.conf*.

A continuación se enumeran las ventajas y desventajas del sistema de autenticación NIS.

#### **Ventajas:**

- Los administradores no necesitan conocer la estructura interna de los datos de NIS para su correcto funcionamiento.

**Desventajas:**

- No es adecuado para una gran red de máquinas.
- Consume mucho ancho de banda.
- Si un servidor esclavo no está operativo cuando se realiza un cambio del mapa, la copia a dicho servidor no está garantizada una vez esté operativo de nuevo.

**2.1.2. LDAP**

LDAP<sup>[3]</sup> son las siglas de *Lightweight Directory Access Protocol* (en español, Protocolo Ligero de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Un directorio es un conjunto de objetos con atributos organizados de una manera lógica y jerárquica. Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

**2.1.2.1. Origen**

El protocolo fue creado originalmente por Tim Howes (University of Michigan), Steve Kille (Isode Limited), y Wengyik Yeong (Performance Systems International) en el año 1993.

Las compañías de telecomunicaciones introdujeron el concepto de servicios de directorio a tecnologías de información y redes de computadoras culminando sus aportaciones en la especificación X.500, compuesto por un conjunto de protocolos producido por la Unión Internacional de Telecomunicaciones (ITU por sus siglas en inglés) en la década de 1980.

Los servicios de directorio X.500 fueron accedidos tradicionalmente vía DAP (*Directory Access Protocol*), que requería la pila de protocolos OSI (*Open Systems Interconnection*). LDAP fue originalmente dirigido a ser un protocolo alternativo y ligero para acceder a servicios de directorio X.500 a través de la pila de protocolos más simple (y ahora más difundido) TCP/IP.

### 2.1.2.2. *Visión general del protocolo*

Un cliente inicia una sesión de LDAP conectándose a un servidor LDAP, por defecto en el puerto TCP 389. El cliente envía a continuación una petición de operación al servidor, y el servidor le devuelve las respuestas correspondientes. El cliente no necesita esperar una respuesta antes de enviar la siguiente petición, y el servidor puede responder en cualquier orden.

El cliente puede solicitar las siguientes operaciones:

- **Start TLS:** uso de la extensión *Transport Layer Security* (TLS) LDAPv3 para una conexión segura.
- **Bind:** autenticación y especificación de una versión del protocolo LDAP.
- **Search:** búsqueda y obtención de entradas del directorio.
- **Compare:** prueba de la existencia de un atributo en una entrada del directorio.
- **Add:** adición de una nueva entrada.
- **Delete:** eliminación de una entrada.
- **Modify:** modificación de una entrada
- **Abandon:** cancelación de una petición previa
- **Extended Operation:** utilización de una operación genérica usada para definir otras operaciones.
- **Unbind:** cierre de la conexión.

Además, el servidor puede enviar "notificaciones no solicitadas" que no son respuestas a ninguna petición, por ejemplo antes de que se termine el tiempo de conexión.

Un método alternativo común para asegurar las comunicaciones LDAP es usar un túnel SSL. Esto es denotado en las URLs de LDAP usando el esquema de URLs "ldaps". El puerto por defecto para LDAP sobre SSL es 636. El uso de LDAP sobre SSL fue común en LDAP Version 2 (LDAPv2) pero nunca fue estandarizado en una especificación formal. Su uso es considerado obsoleto al igual que LDAPv2, que ha sido retirado oficialmente en 2003.

### 2.1.2.3. Estructura

El protocolo accede a directorios LDAP, que siguen la edición de 1993 del modelo X.500, básicamente las características del modelo son:

- Un directorio es un árbol de entradas de directorio.
- Una entrada consta de un conjunto de atributos.
- Un atributo tiene un nombre (un tipo de atributo o descripción de atributo) y uno o más valores.

Cada entrada tiene un identificador único (*Distinguished Name*, DN) y a su vez éste consta de su *Relative Distinguished Name* (RDN) construido por algunos atributos en la entrada, seguidos del DN de la entrada del padre.

Se debe tener cuidado con el hecho de que un DN puede cambiar en el tiempo de vida de una entrada como, por ejemplo, cuando las entradas son movidas en el árbol. Para hacer más confiables e identificar de manera no ambigua las entradas un UUID podría ser proporcionado en el conjunto de los atributos operacionales de la entrada.

Una entrada puede tener este aspecto cuando es representada en el formato *LDAP Data Interchange Format* (LDIF) (LDAP por sí mismo es un protocolo binario):

```
dn: uid=robfa,dc=example,dc=com
cn: ROBERTO FUENTES ASTORGA
givenName: ROBERTO
sn: FUENTES ASTORGA
telephoneNumber: +34 916249061
mail: robfa@lab.inf.uc3m.es
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

A continuación se desarrolla el significado de cada campo de la entrada:

- “dn” es el nombre de la entrada; no es un atributo ni tampoco parte de la entrada.
- “uid=robfa” es el nombre distinguido relativo (RDN).
- “dc=example,dc=com” es el nombre distinguido (DN) de la entrada del padre, donde se indica el componente de dominio (DC).

- “cn”, “givenName”, “telephoneNumber” y “mail” son atributos de la entrada. Los nombres de atributos son generalmente cadenas mnemotécnicas, como por ejemplo, “cn” para *common name* (nombre común), “dc” para *domain component* (componente de dominio), “mail” para dirección de e-mail y “sn” para *surname* (apellido).

LDAP no define un ordenamiento para los elementos del árbol. El servidor puede devolver los valores de un atributo, los atributos en una entrada y las entradas encontradas por una operación de búsqueda en cualquier orden.

#### 2.1.2.4. Implementaciones

Las implementaciones más relevantes son:

- **OpenLDAP:** Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP. Tiene su propia licencia, la *OpenLDAP Public License*. Al ser un protocolo independiente de la plataforma, varias distribuciones GNU/Linux y BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS.
- **Apple’s Open Directory:** Es la implementación del servicio de directorio LDAP de Apple Inc. En el contexto de Mac OS X Server, Open Directory es un dominio compartido basado en OpenLDAP acompañado de un modelo de autenticación compuesto por Apple Password Server y Kerberos 5.
- **Novell eDirectory:** Novell eDirectory (antes conocido como Servicios de directorio de Novell, a veces referido como Netware Directory Services) es un servicio de directorio X.500 compatible con el software inicialmente lanzado en 1993 por Novell para la gestión centralizada el acceso a los recursos de varios servidores y computadoras dentro de una red determinada.
- **IBM Directory Server:** IBM Tivoli Directory Server (ITDS), conocido formalmente como IBM Directory Server, es una implementación del protocolo ligero de acceso a directorios, y forma parte del paquete software de herramientas de acceso e identificación destinado para las empresas. IBM Tivoli Directory Server cuenta con una infraestructura

LDAP que proporciona una base para el despliegue de aplicaciones integrales de gestión de identidad y arquitecturas de software avanzadas.

- **Sun Java System Directory Server:** Es un servidor de directorio LDAP escalable perteneciente a Sun Microsystems. El servidor Sun Java System Directory Server es un componente del sistema Java Enterprise.
- **Microsoft Active Directory:** Desarrollado ampliamente en el punto 2.1.3.

A continuación se enumeran las ventajas y desventajas del sistema de autenticación LDAP.

#### **Ventajas:**

- Robusto, permite gran cantidad de consultas simultáneas.
- Es multiplataforma y compatible con muchos productos.
- El modelo asegura que las entradas son únicas.
- Permite múltiples directorios independientes.
- Se adapta fácilmente a futuras ampliaciones.

#### **Desventajas:**

- Pobre rendimiento para la realización de escrituras en el árbol.
- La configuración y el mantenimiento del servicio es complicado y requiere de cierta experiencia.

### **2.1.3. Active Directory**

*Active Directory* (AD)<sup>[4]</sup> es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos...).

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

*Active Directory* permite a los administradores establecer políticas a nivel de empresa, desplegar programas en gran cantidad de equipos y aplicar

actualizaciones críticas a una organización entera. Un servidor *Active Directory* almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

### **2.1.3.1. Estructura**

*Active Directory* se basa en una estructura jerárquica de objetos. Los objetos se enmarcan en tres grandes categorías: recursos (p.ej. impresoras), servicios (p.ej. correo electrónico) y usuarios (cuentas, o usuarios y grupos). El AD proporciona información sobre los objetos, los organiza, controla el acceso y establece la seguridad.

Cada objeto representa una entidad individual ya sea un usuario, un equipo, una impresora, una aplicación o una fuente compartida de datos y sus atributos. Un objeto está unívocamente identificado por su nombre y tiene un conjunto de atributos, dichos atributos e información que el objeto puede contener son definidos por el tipo. Los atributos, la estructura básica del objeto, se definen por un esquema, que también determina la clase de objetos que se pueden almacenar en el AD.

Dominios y subdominios se identifican utilizando la misma notación de las zonas DNS, razón por la cual *Active Directory* requiere uno o más servidores DNS que permitan el direccionamiento de los elementos pertenecientes a la red, como por ejemplo el listado de equipos conectados; y los componentes lógicos de la red, como el listado de usuarios.

Un ejemplo de la estructura descendente (o herencia), es que si un usuario pertenece a un dominio, será reconocido en todo el árbol generado a partir de ese dominio, sin necesidad de pertenecer a cada uno de los subdominios.

A su vez, los árboles pueden integrarse en un espacio común denominado bosque (que por lo tanto no comparten el mismo nombre de zona DNS entre ellos) y establecer una relación de confianza entre ellos. De este modo los usuarios y recursos de los distintos árboles serán visibles entre ellos, manteniendo cada estructura de árbol el propio *Active Directory*.



### **2.1.3.2.    *Funcionamiento***

Su funcionamiento es similar a otras estructuras de LDAP (*Lightweight Directory Access Protocol*), ya que este protocolo viene implementado de forma similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación.

A su vez, cada uno de estos objetos tendrá atributos que permiten identificarlos en modo unívoco. Toda esta información queda almacenada en *Active Directory* replicándose de forma automática entre todos los servidores que controlan el acceso al dominio.

De esta forma, es posible crear recursos (como carpetas compartidas, impresoras de red, etc) y conceder acceso a estos recursos a usuarios. *Active Directory* es una implementación de servicio de directorio centralizado en una red distribuida que facilita el control, la administración y la consulta de todos los elementos lógicos de una red (como pueden ser usuarios, equipos y recursos).

### **2.1.3.3.    *Requisitos de instalación***

Para crear un dominio hay que cumplir, por lo menos, con los siguientes requisitos recomendados:

- Tener cualquier versión Server de Windows 2000, 2003 (Server, Advanced Server o Datacenter Server) o Windows 2008, en el caso de 2003 server se debe tener instalado el service pack 1.
- Protocolo TCP/IP instalado y configurado manualmente, es decir, sin contar con una dirección asignada por DHCP,
- Tener un servidor de nombre de DNS, para resolver la dirección de los distintos recursos físicos presentes en la red
- Poseer más de 250 MB en una unidad de disco formateada en el sistema de ficheros NTFS.

A continuación se enumeran las ventajas y desventajas del sistema de autenticación *Active Directory*.

**Ventajas:**

- El usuario dispone de un nombre de usuario y contraseña único para toda la red.
- Mejora la seguridad de la estación de trabajo (cliente).
- Proporciona almacenamiento centralizado a los usuarios.
- Menor coste de mantenimiento ya que no se necesita un profesional con mucha experiencia para realizar la administración.

**Desventajas:**

- *Active Directory* es una base de datos con una estructura plana de ficheros y no escala adecuadamente en ubicaciones distribuidas. Si la red no es lo suficientemente rápida se puede producir fallos en la replicación debido al gran tiempo que lleva realizar dicha operación.
- No cumple plenamente los estándares de LDAP, lo que incrementa el coste de integración de los productos realizados por terceros.
- Es dependiente del sistema operativo y no se puede instalar en cualquier otra plataforma que no sea un servidor de Windows.

## 2.2. Sistemas operativos

Un sistema operativo es un software destinado a permitir la comunicación del usuario con un ordenador y gestionar sus recursos de manera cómoda y eficiente.

En la actualidad, existe multitud de sistemas operativos instalados en una gran variedad de dispositivos. Un ejemplo de los sistemas operativos más populares en la actualidad son los siguientes: Android, iOS, GNU/Linux, Mac OS X, Microsoft Windows y UNIX.

A continuación se analizarán los sistemas operativos más utilizados en el ámbito de ordenadores personales.

### 2.2.1. Microsoft Windows

Microsoft Windows es un sistema operativo con interfaz gráfica propietario de la empresa Microsoft.

Existen varias versiones de dicho sistema operativo, a continuación se desarrollan las versiones más actuales y utilizadas.

#### 2.2.1.1. *Microsoft Windows XP*

Microsoft Windows XP<sup>[5]</sup> es un sistema operativo destinado a ordenadores personales. Se caracteriza por mejorar la experiencia del usuario con el ordenador. De hecho, la interfaz gráfica está rediseñada para ser más amigable que sus anteriores versiones de Microsoft Windows.

Es el primer sistema operativo orientado al usuario construido sobre el núcleo de Windows NT. Los sistemas operativos basados en NT son conocidos por su mejorada estabilidad y eficiencia con respecto a sus predecesores.

Las ediciones más destacadas de Microsoft Windows XP<sup>[6]</sup> son las siguientes:

- **Home:** Esta edición está diseñada para usuarios domésticos y carece de una serie de características que posee la edición Professional.

- **Professional:** Esta edición está diseñada para usuarios avanzados y empresariales. Las características más destacadas que posee frente a la edición Home son las siguientes: posibilidad de formar parte de un dominio de Windows Server, escritorio remoto, cifrado de archivos y el servidor web IIS.
- **Starter:** Esta edición es la de menor coste y se distribuyó solamente en algunos países. Es similar a la edición Home pero destinada a la gama baja de hardware, por lo que tiene restricciones como la ejecución máxima de 3 programas simultáneamente.
- **Media Center:** Esta edición tiene como característica principal la inclusión del Windows Media Center, que proporciona una interfaz accesible remotamente para reproducir contenido multimedia. El resto de características son idénticas a la edición Professional menos la posibilidad de unirse a un dominio ya que el software está destinado a usuarios domésticos.
- **Tablet PC:** Esta edición está especialmente diseñada para los ordenadores portátiles denominados Tablet PC. La característica principal es que esta edición es compatible con una pantalla sensible a un lápiz electrónico. El resto de características son iguales a las ofrecidas por la edición Professional.

### 2.2.1.2. *Microsoft Windows Vista*

Microsoft Windows Vista<sup>[7]</sup> es un sistema operativo destinado a ordenadores personales. Esta versión incluye muchas novedades con respecto a su predecesor, entre las más destacadas está la nueva interfaz gráfica, una nueva y rediseñada función de búsqueda y multitud de herramientas multimedia como, por ejemplo, Windows DVD Maker.

Las ediciones<sup>[8]</sup> destinadas a ordenadores personales de Windows Vista son las siguientes:

- **Starter:** Esta edición es la de menor coste y se distribuyó solamente en algunos países. Es similar a la edición Home Basic pero destinada a la gama baja de hardware, por lo que tiene restricciones como la ejecución máxima de 3 programas simultáneamente.
- **Home Basic:** Esta edición fue concebida para los usuarios que no requieren un soporte avanzado multimedia. Tiene restricciones en la interfaz gráfica y no puede reproducir video de alta definición.

- **Home Premium:** Esta edición es igual que la Home Basic pero sin las restricciones comentadas anteriormente.
- **Business:** Esta edición está destinada al entorno de la pequeña empresa. Dispone de todas las características de la edición Home Premium y además incluye la capacidad de unirse a un dominio de Windows Server, servidor web IIS, escritorio remoto y cifrado del sistema de ficheros entre otros.
- **Enterprise:** Esta edición está destinada al entorno empresarial. Entre las características más destacadas se incluye soporte para aplicaciones Unix.
- **Ultimate:** Esta edición combina las características de las ediciones Home Premium y Enterprise.

### 2.2.1.3. *Microsoft Windows 7*

Microsoft Windows 7<sup>[9]</sup> es la actual versión de Microsoft Windows. De igual manera que Windows Vista y Windows XP está destinado a ordenadores personales. Esta versión incluye multitud de mejoras con respecto a su predecesor, entre las más destacados podemos encontrar las siguientes: mejora del reconocimiento de hardware, mejora del rendimiento en equipos multiprocesador y mejora del arranque.

Las ediciones<sup>[10]</sup> destinadas a ordenadores personales de Microsoft Windows XP son las siguientes:

- **Starter:** Esta edición está destinada principalmente a *netbooks* y es la edición que contiene menos características debido a las restricciones hardware de los equipos.
- **Home Basic:** Esta edición está disponible solamente en algunos países y tiene restringidas muchas características como algunas opciones avanzadas de la interfaz gráfica.
- **Home Premium:** Esta edición contiene características relacionadas con los productos diseñados para el hogar como, por ejemplo, Windows Media Center y soporte multitáctil.
- **Professional:** Esta edición está destinada a pequeños negocios y usuarios avanzados. Entre las características más destacadas se incluye la posibilidad de asociar el equipo a un dominio de Windows Server.
- **Enterprise:** Esta edición está destinada al entorno empresarial. Entre las características más destacadas se incluye soporte para aplicaciones Unix.

- **Ultimate:** Esta edición incluye las mismas características que la edición Enterprise pero está destinada a usuarios domésticos.

#### 2.2.1.4. *Microsoft Windows Server 2008*

Es la actual versión de la familia de sistemas operativos destinada a servidores. Microsoft Windows Server 2008<sup>[1]</sup> está construido sobre el mismo código que Windows Vista. Como novedad este sistema operativo se puede instalar sin la interfaz gráfica característica de los sistemas operativos Windows. Por lo tanto, toda la administración se ha de realizar por línea de comandos.

Las características más relevantes son las siguientes:

- Ampliación de los roles de *Active Directory*.
- Nuevo proceso de reparación de sistemas de ficheros NTFS.
- Mejora en el rendimiento de la virtualización.
- Consola de comandos avanzada *PowerShell*.
- Mejoras en el núcleo del sistema operativo.
- Mejoras en las políticas de grupo.
- Mejoras en el protocolo de autenticación y cifrado.

Las principales ventajas y desventajas de los sistemas operativos comercializados por Microsoft son las siguientes:

##### **Ventajas:**

- Facilidad de uso debido a la interfaz de usuario intuitiva.
- Facilidad de administración en entornos empresariales pequeños en los cuales no se dispone de un administrador experto.

##### **Desventajas:**

- Código fuente no público.
- Consumo de gran cantidad de recursos hardware.
- Poca flexibilidad del sistema operativo.

### 2.2.2. Unix

Unix<sup>[12]</sup> es un sistema operativo multitarea y multiusuario desarrollado originalmente por un grupo de empleados del grupo AT&T. Entre ellos destacan Dennis Ritchie, Brian Kernighan, Douglas McIlroy, Michael Lesk and Joe Ossanna.

La evolución actual de sistemas Unix se divide en varias ramas, desarrollados a lo largo del tiempo por parte de AT&T, así como por varios vendedores comerciales (como la Universidad de California, Berkeley BSD), y organizaciones sin fines de lucro.

Las ramas más significativas de UNIX son las siguientes:

- **AT&T:** tuvo su origen en el UNIX de AT&T. Considerada la familia UNIX “pura” y original. Sus sistemas operativos más significativos son UNIX System III y UNIX System V.
- **BSD:** originada por el otorgamiento de licencia de UNIX a Berkely. BSD se reescribió para no incorporar propiedad intelectual originaria de AT&T en la versión 4. La primera implementación de los protocolos TCP/IP que dieron origen a Internet son la pila (stack) TCP/IP BSD.
- **AIX:** surge por el otorgamiento de licencia de UNIX System III a IBM.
- **Xenix:** deriva de la adquisición de los derechos originales de AT&T. Primero por parte de Microsoft y posteriormente por SCO.
- **GNU/Linux:** En 1983, Richard Stallman anunció el proyecto GNU, un ambicioso esfuerzo para crear un sistema similar a Unix, que pudiese ser distribuido libremente. El software desarrollado por este proyecto -por ejemplo, GNU Emacs y GCC- también han sido parte fundamental de otros sistemas UNIX. En 1991, cuando Linus Torvalds empezó a proponer el núcleo Linux y a reunir colaboradores, las herramientas GNU eran la elección perfecta. Al combinarse ambos elementos, conformaron la base del sistema operativo (basado en POSIX) que hoy se conoce como GNU/Linux. Las distribuciones basadas en el núcleo, el software GNU y otros agregados entre las que se pueden mencionar a Slackware Linux, Red Hat Linux y Debian GNU/Linux se han hecho populares tanto entre los aficionados a la computación como en el mundo empresarial. Obsérvese que Linux tiene un origen independiente, por lo que se considera un 'clónico' de UNIX y no un UNIX en el sentido histórico.

Las principales ventajas y desventajas de los sistemas operativos Unix son las siguientes:

**Ventajas:**

- Es un sistema operativo especialmente robusto. Cuando una aplicación se bloquea, el resto del sistema sigue funcionando correctamente.
- Necesita menos recursos hardware para ofrecer un rendimiento similar a otras plataformas.

**Desventajas:**

- Puede requerir más horas de aprendizaje que el resto de plataformas de sistemas operativos.
- Algunas ramas han sido diseñadas para ser ejecutadas en hardware de una marca específica. Lo que limita la portabilidad del sistema operativo.
- El coste por licencia y mantenimiento suele ser elevado, al tratarse de productos enfocados al mundo empresarial.

### 2.2.3. GNU/Linux

GNU/Linux<sup>[13][14]</sup> es uno de los términos empleados para referirse a la combinación del núcleo o *kernel* libre similar a Unix denominado Linux, que es usado con el sistema operativo GNU.

El nombre GNU, GNU's Not Unix (GNU no es Unix), viene de las herramientas básicas de sistema operativo creadas por el proyecto GNU, iniciado por Richard Stallman en 1983 y mantenido por la FSF. El nombre Linux viene del núcleo Linux, inicialmente escrito por Linus Torvalds en 1991.

A las variantes de esta unión de programas y tecnologías, a las que se les adicionan diversos programas de aplicación de propósitos específicos o generales se las denomina distribuciones. Su objetivo consiste en ofrecer ediciones que cumplan con las necesidades de un determinado grupo de usuarios. Algunas de ellas son especialmente conocidas por su uso en servidores y supercomputadoras.

A continuación se muestra una comparativa entre las distribuciones<sup>[15]</sup> más importantes:



	Kernel	Sistema de Ficheros			Arquitectura	Paquetes
<b>Debian GNU/Linux</b>	2.6.24	ext2, FAT, NTFS, UDF, NFS, ReiserFS	JFS, ISO 9660,	XFS,	x86, x86-64, IA64, PPC, SPARC, SPARC64, Alpha, MIPS, ARM, PARISC, Mac/VME 68k, S/390	23000
<b>Fedora</b>	2.6.25	ext2, FAT, ISO 9660, UDF, NFS	ReiserFS,		x86, x86-64, PowerPC	8000
<b>Ubuntu</b>	2.6.32	ext2, FAT, NTFS, UDF, NFS, ReiserFS	JFS, ISO 9660,	XFS,	x86, x86-64, IA64	23000
<b>Mandriva Linux</b>	2.6.24.4	ext2, FAT, NTFS, UDF, NFS, ReiserFS	JFS, ISO 9660,	XFS,	x86, x86-64, PowerPC	23560
<b>openSUSE</b>	2.6.22.5	ext2, XFS, FAT, NTFS, UDF, NFS, Reiser4	ext3, ISO 9660,	JFS,	x86, x86-64, IA64, PPC, PPC64	22000

Tabla 2.1. Distribuciones de Linux

#### 2.2.4. Otros

Además de los sistemas operativos de la familia Windows, Unix y derivados, existen otros tales como Mac Os X, dirigidos principalmente a máquinas creadas y comercializadas por Apple.

## 2.3. Virtualización de Sistemas Operativos

Una máquina virtual es un software que emula a una computadora y puede ejecutar programas como si fuese una computadora real. Este software en un principio fue definido como “un duplicado eficiente y aislado de una máquina física”. Una característica esencial de una máquina virtual es que el software que se ejecuta en el interior se limita a los recursos y abstracciones proporcionados por la máquina virtual y no puede salir de su entorno virtual.

A continuación se desarrollan los principales tipos de virtualización<sup>[16][17][18]</sup> existentes.

- **Virtualización completa:** Es una técnica de virtualización utilizada para proporcionar un cierto tipo de entorno de máquina virtual, es decir, que es una simulación completa del hardware subyacente. La virtualización completa requiere que cada característica destacada del hardware del equipo físico se refleje en cada máquina virtual, incluyendo el conjunto de instrucciones completo, entrada/salida de las operaciones, las interrupciones, acceso a la memoria, y el resto de elementos que son utilizados por el software que se ejecutaría en la máquina desnuda. En dicho entorno, cualquier software capaz de ejecución en el hardware en bruto se puede ejecutar en la máquina virtual y, en particular, cualquier sistema operativo.
- **Virtualización parcial:** En la virtualización parcial, incluyendo la virtualización del espacio de direcciones, la máquina virtual simula múltiples instancias de la mayor parte de un entorno de hardware subyacente, en particular los espacios de direcciones. Por lo general, esto significa que los sistemas operativos completos, no se pueden ejecutar en la máquina virtual. Una forma fundamental de la virtualización parcial es la virtualización del espacio de direcciones, en el que cada máquina virtual se compone de un espacio de direcciones independiente. Esta capacidad requiere de hardware que reubique las direcciones de memoria.
- **Paravirtualización:** Es una técnica que ofrece una interfaz a las máquinas virtuales que es similar (no idéntica) al hardware de la máquina física. La paravirtualización requiere que el sistema operativo invitado esté modificado para trabajar con dicha api. Un sistema operativo sin dichas modificaciones no se podrá ser ejecutado por una

máquina virtual paravirtualizada. Sin embargo, hay casos que el sistema operativo no puede ser modificado como, por ejemplo, Microsoft Windows para el que existe un proyecto (XenWindowsGplPv) que proporciona un conjunto de drivers que permiten dicha portabilidad como máquina virtual en el *hypervisor* de Xen.

### Razones para utilizar máquinas virtuales

- Se pueden utilizar para consolidar la carga de trabajo de varios servidores. Las ventajas principales son el ahorro de hardware, el coste eléctrico y la administración de la infraestructura.
- A menudo es necesario ejecutar aplicaciones muy antiguas que no funcionarían correctamente en un sistema operativo actual, por lo que se también se utilizan las máquinas virtuales para consolidar aplicaciones de este tipo. De esta manera se logra un mejor aprovechamiento del servidor físico.
- Proporcionan entornos limitados, aislados y seguros para aplicaciones que no son de confianza. Debido a dicho aislamiento se suelen utilizar para realizar pruebas y estudiar el comportamiento del software cuando se le introduce fallos.
- Permiten una administración más sencilla para tareas de migración, copia de seguridad y recuperación.

A continuación se desarrollan las soluciones existentes más utilizadas para realizar máquinas virtuales:

#### 2.3.1. VMware

El software de VMware<sup>[19]</sup> proporciona un completo conjunto de hardware virtualizado al sistema operativo invitado como, por ejemplo, un adaptador de vídeo, un adaptador de red y los adaptadores de disco duro. El anfitrión ofrece conectividad a través de los controladores USB, serie y paralelo a las máquinas invitadas.

VMware cuenta con los siguientes productos:

- **VMware Workstation**<sup>[20]</sup>: Es un software de virtualización para equipos con arquitecturas x86 y x86-64. Permite a los usuarios crear múltiples máquinas virtuales x86 y x86-64 y utilizar uno o más de estas máquinas virtuales simultáneamente con el sistema

operativo huésped. Cada instancia de máquina virtual puede ejecutar su propio sistema operativo invitado, incluyendo Windows, Linux, variantes de BSD, y otros. En términos simples, VMware Workstation permite a una máquina física ejecutar múltiples sistemas operativos simultáneamente.

- **VMware Player**<sup>[21]</sup>: Es un software de virtualización gratuita creado por la empresa VMware, Inc. Puede ejecutar las aplicaciones virtuales y crear sus propias máquinas virtuales que requieren un sistema operativo que se instalará para ser funcional. Utiliza el mismo núcleo de virtualización que VMware Workstation pero solamente está disponible para uso personal no comercial y tiene menos funcionalidad.
- **VMware Fusion**: Es un software de virtualización desarrollado para ordenadores Macintosh con procesadores Intel. VMware Fusion permite a los ‘Macs’ basados en Intel ejecutar máquinas virtuales con arquitecturas x86 y x86-64. Es capaz de virtualizar multitud de sistemas operativos como Microsoft Windows, Linux, NetWare y Solaris.
- **VMware ESX Server**<sup>[22][23]</sup>: Es un software de virtualización a nivel empresarial. ESX es un componente que ofrece mayor capacidad a la infraestructura de virtualización basada en VMware y añade servicios de gestión y fiabilidad en el producto servidor central. VMware ESX es un *hypervisor* tipo *bare-metal*. Dichos hipervisores se ejecutan directamente sobre el hardware del servidor sin necesidad de un sistema operativo.
- **VMware ESXi**<sup>[22][23]</sup>: Es una versión reducida de VMware ESX que no incluye la consola de administración.
- **VMware Server**<sup>[22][23]</sup>: Es un software de virtualización que tiene menos funciones que la versión ESX. Está basado en un modelo cliente-servidor y permite el acceso remoto a las máquinas virtuales mediante interfaz web.

A continuación se enumeran las ventajas y desventajas de la utilización del software VMware.

**Ventajas:**

- Facilidad de uso.
- Buen rendimiento obtenido mediante la técnica de virtualización.

**Desventajas:**

- Aunque se pueden utilizar los productos gratuitos de VMware para ejecutar máquinas virtuales y existen otros productos en el mercado para crearlas, si se quiere tener un rendimiento óptimo es necesaria una licencia para VMware ESX Server.
- La versión VMware ESX Server, que posee el rendimiento más óptimo de todas las soluciones VMware, no es compatible con una gran lista de hardware doméstico.

**2.3.2. KVM**

KVM<sup>[24][25]</sup> o *Kernel-based Virtual Machine* en inglés, es una solución para implementar virtualización completa con Linux. Está formada por un módulo del núcleo y herramientas en el espacio de usuario, siendo en su totalidad software libre. El componente KVM para el núcleo está incluido en Linux desde la versión 2.6.20.

Permite ejecutar máquinas virtuales utilizando imágenes de disco que contienen sistemas operativos sin modificar. Cada máquina virtual tiene su propio hardware virtualizado: una tarjeta de red, discos duros, tarjeta gráfica, etc. Necesita un procesador con arquitectura x86 con soporte *Virtualization Technology* y se puede ejecutar huéspedes GNU/Linux (32 y 64 bits) y Windows (32 bits).

A continuación se enumeran las ventajas y desventajas de la utilización del software KVM.

**Ventajas:**

- Es un software libre y gratuito.
- Facilidad de administración de las máquinas virtuales, ya que cada máquina virtual se ejecuta en el sistema como un proceso.
- No es necesaria la modificación del sistema operativo invitado.

**Desventajas:**

- Compatible únicamente con CPU's que soporten instrucciones de virtualización.

**2.3.3. Xen**

El *hypervisor* Xen<sup>[26]</sup> es una capa de software que se ejecuta directamente en el hardware del equipo sustituyendo al sistema operativo permitiendo que el hardware del equipo ejecute múltiples sistemas operativos invitados al mismo tiempo. Dispone de soporte para arquitecturas x86, x86-64, Itanium, Power PC y procesadores ARM y actualmente soporta Linux, NetBSD, FreeBSD, Solaris, Windows y otros sistemas operativos comunes como invitados.

**2.3.3.1. Historia**

Xen se originó como un proyecto de investigación en la Universidad de Cambridge, dirigido por Ian Pratt, profesor en Cambridge y fundador de XenSource, Inc. se hizo el primer lanzamiento público de Xen en 2003.

Xen ha sido apoyado inicialmente por XenSource Inc., y desde la adquisición de XenSource por Citrix en octubre de 2007. Esta organización apoya el desarrollo del proyecto de software libre y también vende versiones empresariales de software.

El 22 de octubre del 2007, Citrix Systems completó la adquisición de XenSource, y el proyecto Xen se trasladó a <http://www.xen.org/>. Este movimiento había comenzado hace algún tiempo, e hizo pública la existencia de la *Xen Project Advisory Board* (Xen AB), que tenía miembros de Citrix, IBM, Intel, Hewlett-Packard, Novell, Red Hat, Sun Microsystems y Oracle.

La *Xen Project Advisory Board* asesora al líder del proyecto Xen y es responsable de la marca Xen, en la que Citrix concede licencia libre a todos los vendedores y los proyectos que implementan el *hypervisor* Xen.

### 2.3.3.2. *Funcionamiento de Xen*<sup>[27]</sup>

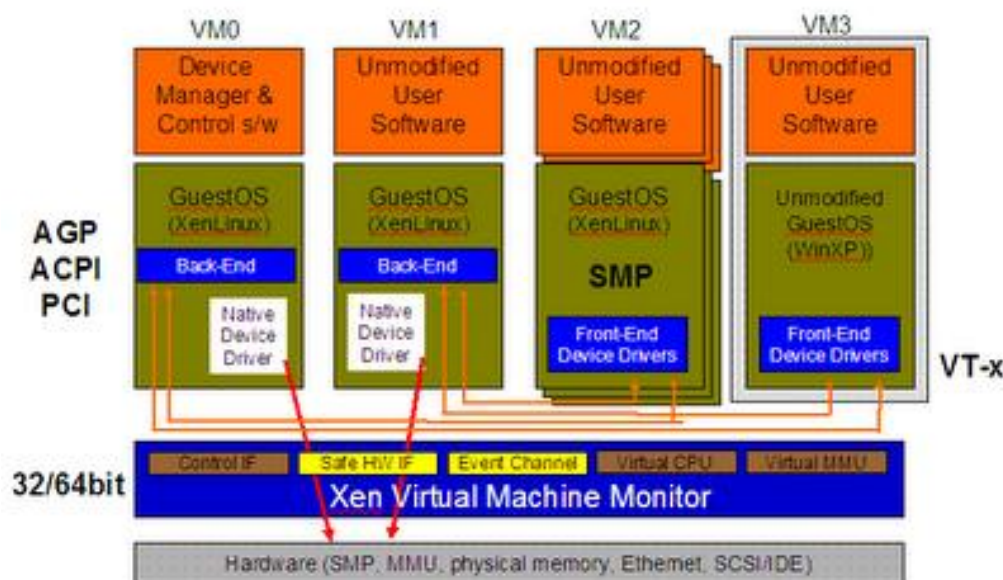


Figura 2.1. Arquitectura de Xen.

Es preciso aclarar la nomenclatura que utiliza Xen para los sistemas ejecutados: la máquina virtual anfitrión VM0 se suele notar como dominio 0 y las demás como dominio U.

En la máquina anfitrión el *kernel* se ejecuta en el nivel del microprocesador 0 así como el monitor o *hypervisor*. El resto de máquinas virtuales se ejecutan en el nivel 1. Las aplicaciones de todas las máquinas virtuales se ejecutan en nivel 3 el nivel con menores privilegios.

En paravirtualización todas las máquinas virtuales usan el procesador directamente haciendo el *hypervisor* de planificador del tiempo de ejecución de tal manera que las máquinas corran de forma nativa.

Cuando las máquinas virtuales acceden a un dispositivo este acceso pasa por el dominio 0 proporcionando el aislamiento necesario. De esta forma los controladores de los dispositivos de las máquinas virtuales no son más que una API que se comunica con el anfitrión, este posee la implementación de los

controladores de los dispositivos virtuales que no son más que unas traducciones hacia los controladores nativos, realiza la operación, accediendo al dispositivo y devuelve el resultado a la máquina invitada.

Uno de los puntos más conflictivos de que se ejecuten las instrucciones de las máquinas virtuales nativamente sobre el procesador son las interrupciones por fallo de página. Para esto el *hypervisor* genera una CPU virtual y una unidad de gestión de memoria (MMU) virtual, pudiendo así correr las máquinas con más o con menos procesadores que los reales.

Las aplicaciones que hacen uso de muchas interrupciones hardware provocan una caída de rendimiento debido a la intercesión del *hypervisor* entre el hardware real y el virtual, así que Xen intenta minimizar al máximo estas actuaciones.

Como también se puede ver en la Figura 2.1, Xen permite la ejecución de sistemas operativos sin modificación, hasta hace poco esto no era posible debido a la necesidad de que el *kernel* de estos se ejecutase a nivel de privilegio del procesador 1 en vez de 0, pero desde la salida de los últimos microprocesadores esto ya es posible por la inclusión de unas nuevas instrucciones al procesador, VT en el caso de Intel y Pacifica en el caso de AMD, que crean un nuevo nivel de privilegios por debajo del nivel 0 denominado *root-mode*, a partir de este nivel ya se pueden ejecutar cualquier sistema operativo sin modificación.

A continuación se enumeran las ventajas y desventajas de la utilización del software Xen.

### **Ventajas:**

- Independencia entre los sistemas virtualizados. Se pueden reiniciar, borrar y crear independientemente.
- Mejor aprovechamiento del hardware de la máquina: balanceo de recursos. Un sistema virtual puede recibir más recursos si los necesita y los demás sistemas no los necesitan.
- Facilidad para realizar copias de seguridad, solo es necesario copiar la máquina virtual permitiendo posteriormente que sea arrancada en un nuevo servidor. Xen incluso permite la migración en caliente, dando flexibilidad y escaso o nulo tiempo de recuperación ante un incidente.



- Se pueden modificar parámetros como la memoria RAM, el número de CPUs, espacio en disco... para ajustarlos a las necesidades de la máquina virtual.
- Se pueden crear máquinas de pruebas similares a las definitivas sin necesidad de adquirir hardware adicional.

**Desventajas:**

- No soporta *drivers* propietarios de algunas tarjetas gráficas en el dom0, aunque se han publicado algunos parches para tener soporte a las distintas versiones del *driver* propietario de nVidia.
- Las versiones de pago son aquellas que implementan interfaces de usuario más intuitivos

## 2.4. Otros servicios

Otros servicios que se necesitarán en la solución propuesta vienen desarrollados a continuación.

### 2.4.1. Web

La función principal de un servidor web<sup>[28]</sup> es ofrecer páginas web sobre la petición de los clientes que utilizan el protocolo de transferencia de hipertexto (HTTP). Esto significa la entrega de los documentos HTML y cualquier contenido adicional que se puede incluir en un documento, como imágenes, hojas de estilo y *scripts*.

Un agente de usuario, normalmente un navegador web o un rastreador web, inicia la comunicación mediante una petición para un recurso específico utilizando HTTP y el servidor responde con el contenido de ese recurso o un mensaje de error si no puede hacerlo.

Las principales implementaciones de servidores web son: Apache e IIS.

#### 2.4.1.1. Apache

El Servidor Apache<sup>[29]</sup> HTTP, comúnmente conocido como Apache es un software de servidor web que destaca por jugar un papel clave en el crecimiento inicial de la *World Wide Web*. En 2009 se convirtió en el primer software de servidor web en superar el hito de servir 100 millones de páginas web.

Apache fue la primera alternativa viable para el servidor de Netscape Communications Corporation (actualmente denominado Oracle iPlanet Web Server), y desde entonces ha evolucionado hasta dominar otros servidores web en términos de funcionalidad y el rendimiento.

Apache soporta gran variedad de características, muchas implementadas como módulos compilados que extienden la funcionalidad básica. Soporta lenguajes como Perl, Python, Tcl, y PHP.

El *hosting* virtual permite que una instalación de Apache sirva muchos sitios web reales diferentes. Por ejemplo, una máquina con una instalación de

Apache simultáneamente podría servir `www.example.com`, `www.example.org`, `test47.test-server.example.edu`, etc...

### 2.4.1.2. IIS

Internet Information Services<sup>[30]</sup> (IIS) es una aplicación de servidor web y un conjunto de módulos de extensión de características creadas por Microsoft para su uso con Microsoft Windows. IIS 7.5 soporta HTTP, HTTPS, FTP, FTPS, SMTP y NNTP.

Es una parte integral de la familia de productos de Windows Server, así como ciertas ediciones de Windows XP, Windows Vista y Windows 7. IIS no está activado de forma predeterminada cuando se instala Windows.

El Administrador de IIS se accede a través de la Consola de administración de Microsoft o de Herramientas administrativas en el Panel de Control.

### 2.4.2. DNS

El sistema de nombres de dominio<sup>[31]</sup> (DNS) es un sistema distribuido de nombres jerárquico para los equipos, servicios o cualquier recurso conectado a Internet en una red privada. Se asocia la información con varios nombres de dominio asignados a cada una de las entidades participantes.

Un servidor DNS resuelve las consultas de estos nombres en direcciones IP con el fin de localizar los servicios informáticos y dispositivos en todo el mundo. Al proporcionar una licencia mundial, distribuida basada en palabras clave de servicio de redirección, el sistema de nombres de dominio es un componente esencial de la funcionalidad de Internet.

Antes de que el DNS se inventara en 1982, cada equipo de la red consultaba un archivo llamado `hosts.txt` desde un ordenador ubicado en el SRI (ahora SRI International). Los archivos *hosts.txt* contienen los nombres asignados a direcciones numéricas. Los archivos de *hosts* todavía se pueden encontrar en la mayoría de los sistemas operativos modernos por defecto y por lo general contiene una asignación de *localhost* a la dirección IP 127.0.0.1.

Muchos sistemas operativos utilizan la lógica de resolución de nombres que permite al administrador configurar las prioridades de selección de los métodos de resolución de nombres disponibles.

El rápido crecimiento de la red requería un mantenimiento centralizado, haciendo que el archivo *hosts.txt* no sea viable. Por lo que era necesario implementar un sistema más escalable, capaz de difundir de forma automática la información necesaria.

### 2.4.3. DHCP

El *Dynamic Host Configuration Protocol* (DHCP)<sup>[32]</sup> es un protocolo de red que se utiliza para configurar los dispositivos de red de modo que puedan comunicarse sobre una red IP. Un cliente DHCP utiliza el protocolo DHCP para obtener información de configuración. Dicha configuración suele ser: la dirección IP, la ruta de salida por defecto y una o más direcciones ip del servidor DNS. El cliente DHCP utiliza esta información para configurar el equipo para comunicarse en internet.

Existen implementaciones de DHCP en dispositivos hardware de red como *routers* o *firewalls*. Por otro lado existen implementaciones propietarias como el servidor DHCP incorporado en los servidores de Microsoft Windows e implementaciones libres como en el caso de Linux.

### 2.4.4. SAMBA

Samba<sup>[33][34]</sup> es un software libre que implementa el protocolo de red SMB/CIFS, originalmente desarrollado por Andrew Tridgell. A partir de la versión 3, Samba proporciona servicios de archivo e impresión para varios clientes de Microsoft Windows y se puede integrar con un dominio de Windows Server, como un controlador de dominio primario (PDC) o como un miembro del dominio.

Samba se ejecuta en la mayoría de los sistemas Unix y similares, tales como GNU/Linux, Solaris, AIX y las variantes BSD, incluyendo Apple Mac OS X Server. Samba es estándar en casi todas las distribuciones de Linux y es comúnmente incluido como un servicio del sistema básico en otros sistemas operativos basados en Unix.

Samba se distribuye bajo la Licencia Pública General GNU.

#### **2.4.4.1. Funcionalidad**

Samba permite compartir archivos e impresoras entre equipos que ejecutan los sistemas operativos Microsoft Windows y Unix.

Es una implementación de varios servicios y protocolos, a continuación se especifican los más destacados:

- NetBIOS sobre TCP/IP (NBT).
- SMB.
- CIFS (una versión mejorada de SMB).
- DCE/RPC o más específicamente, MSRPC, la suite de protocolos de entorno de red.
- Un servidor WINS también conocido como un servidor de nombres NetBIOS (NBNS).
- El conjunto de protocolos del dominio NT, que incluye los inicios de sesión.
- Administrador de cuentas de seguridad (SAM).
- Autoridad de seguridad local (LSA).
- Servicio de impresión compatible con NT (SPOOLSS), NTLM y el inicio de sesión perteneciente a Active Directory que incluye una versión modificada de Kerberos y de LDAP.

Todos estos servicios y protocolos son incorrectamente denominados frecuentemente como NetBIOS o SMB.

#### **2.4.5. Sistema de archivos de red**

Un sistema de archivos de red<sup>[35]</sup> es cualquier sistema de archivos que permite el acceso a los archivos desde múltiples equipos conectados a través de una red informática. Esto hace posible que varios usuarios en varios equipos para compartir archivos y recursos de almacenamiento.

Los equipos cliente no tienen acceso directo al almacenamiento en bloques subyacente sino que interactúan en la red mediante un protocolo. Esto hace que sea posible restringir el acceso al sistema de archivos en función de listas de acceso o capacidades en los servidores y en los clientes, dependiendo de cómo esté diseñado el protocolo.

Una de las soluciones más antiguas y que sigue siendo notable es NFS<sup>[36]</sup> (*Network File System*) que posibilita el acceso a ficheros remotos como si se tratase de locales. Originalmente fue desarrollado en 1984 por Sun Microsystems, con el objetivo de que sea independiente de la máquina, el sistema operativo y el protocolo de transporte, esto fue posible gracias a que está implementado sobre los protocolos XDR (presentación) y ONC RPC (sesión). El protocolo NFS está incluido por defecto en los Sistemas Operativos UNIX y la mayoría de distribuciones Linux.

#### **2.4.5.1. Características**

- El sistema NFS está dividido al menos en dos partes principales: un servidor y uno o más clientes. Los clientes acceden de forma remota a los datos que se encuentran almacenados en el servidor.
- Las estaciones de trabajo locales utilizan menos espacio de disco debido a que los datos se encuentran centralizados en un único lugar pero pueden ser accedidos y modificados por varios usuarios, de tal forma que no es necesario replicar la información.
- Los usuarios no necesitan disponer de un directorio “home” en cada una de las máquinas de la organización. Los directorios “home” pueden crearse en el servidor de NFS para posteriormente poder acceder a ellos desde cualquier máquina a través de la infraestructura de red.
- También se pueden compartir a través de la red dispositivos de almacenamiento como disqueteras, CD-ROM y unidades ZIP. Esto puede reducir la inversión en dichos dispositivos y mejorar el aprovechamiento del hardware existente en la organización.

Todas las operaciones sobre ficheros son síncronas. Esto significa que la operación sólo retorna cuando el servidor ha completado todo el trabajo asociado para esa operación. En caso de una solicitud de escritura, el servidor escribirá físicamente los datos en el disco, y si es necesario, actualizará la estructura de directorios, antes de devolver una respuesta al cliente. Esto garantiza la integridad de los ficheros.

# Capítulo 3

## Análisis

En este capítulo se va a realizar el análisis del proyecto realizado. Para comenzar se describe la situación actual del laboratorio del Departamento de Informática. Seguidamente se definirán las funcionalidades y requisitos que debe cumplir el sistema. Por último se realizará un breve análisis de los casos de uso pertenecientes a la funcionalidad ofrecida por la página web relacionada con la gestión de la cuenta de usuario.

El estándar seguido para la realización del resto del documento ha sido el *ESA software engineering standards to small software projects*<sup>[38]</sup>.

### 3.1. Situación actual del Laboratorio del Departamento de Informática

El laboratorio del Departamento de informática, en adelante “Idi”, cuenta con personal de administración y servicios y becarios para prestar los siguientes servicios a los profesores y alumnos de la Universidad Carlos III de Madrid:

- Acceso a los equipos de las aulas pertenecientes al Departamento de Informática. Dichos equipos cuentan con los sistemas operativos Debian GNU/Linux 6.0 y Microsoft Windows 7.
- Acceso desde el exterior a un equipo denominado Guernika, que permite realizar las prácticas desde casa a los alumnos.
- Correo electrónico.
- Soporte a los alumnos para la realización de las prácticas.
- Soporte a los profesores mediante la instalación del software necesario para impartir las clases.
- Reserva de aulas informáticas mediante la página web.
- Descarga de software de Microsoft para la realización de las prácticas.

El ldi tiene que administrar cinco aulas informáticas, una sala de presentaciones a disposición del Departamento y una sala para profesores asociados. El ldi debe administrar aproximadamente unas 110 máquinas repartidas en las ubicaciones descritas anteriormente.

Cabe destacar que se tienen que gestionar aproximadamente 1300 cuentas de usuario pertenecientes a alumnos y profesores.

A continuación se detalla la configuración inicial del entorno del laboratorio del Departamento de informática.

### 3.1.1. Entorno Linux

Los equipos de las aulas informáticas tienen instalado la versión 6.0 (squeeze) de Debian GNU/Linux. Para poder utilizar este sistema operativo, tanto los alumnos como los profesores deben tener su propia cuenta de usuario. En el apartado 3.1.3. se detalla el proceso de apertura de cuentas de ambos colectivos.

Los equipos necesitan los siguientes servicios para su correcto funcionamiento:

- **Aplicaciones:** Las aplicaciones se ejecutan de manera remota desde los siguientes servidores: squeeze32, squeeze32-2, squeeze32-3 y squeeze32-4.
- **DHCP y DNS:** Los servicios relacionados con la configuración de la interfaz de red y la resolución de nombres de *lab.inf.uc3m.es* son proporcionados por el servidor denominado servicios.
- **Correo:** Cada usuario dispone de cuenta de correo accesible vía web.
- **Web:** Cada usuario dispone de su espacio para realizar su página web accesible mediante la página web del laboratorio.
- **Autenticación:** La autenticación de usuario se realiza mediante NIS y la realiza el servidor cuentas.
- **Datos de usuario:** Los datos almacenados por el usuario son servidos por el servidor cuentas.

A continuación se muestra la infraestructura que da servicio a los equipos cuando están arrancados en el sistema operativo Linux.



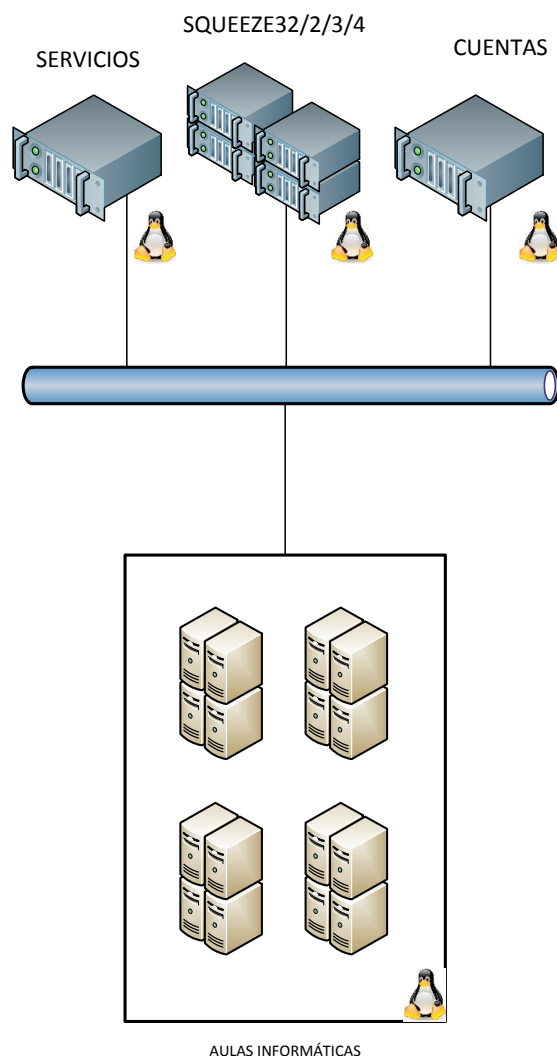


Figura 3.1. Infraestructura Linux.

### 3.1.2. Entorno Windows

Además de Linux, los equipos de las aulas informáticas tienen instalado Microsoft Windows 7 Professional. En este caso, para acceder a los equipos se utilizan cuentas genéricas por asignatura y son utilizadas por los profesores y los alumnos.

A continuación se describen los servicios necesarios por los equipos:

- **Aplicaciones:** Las aplicaciones están instaladas de manera local en cada cliente.
- **DHCP:** El servicio que realiza la configuración de interfaz de red lo proporciona el servidor servicios.

- **DNS:** El servicio de resolución de nombres de *lab.inf.uc3m.es* lo proporciona el controlador de dominio sorolla.
- **Correo:** No se dispone de cuenta de correo.
- **Web:** No se dispone de página web personal.
- **Autenticación:** La autenticación la realiza el controlador de dominio denominado sorolla.
- **Datos de usuario:** Los datos guardados por las cuentas genéricas son almacenados en el servidor sorolla.

A continuación se muestra la infraestructura que da servicio a los equipos cuando están arrancados en el sistema operativo Windows.

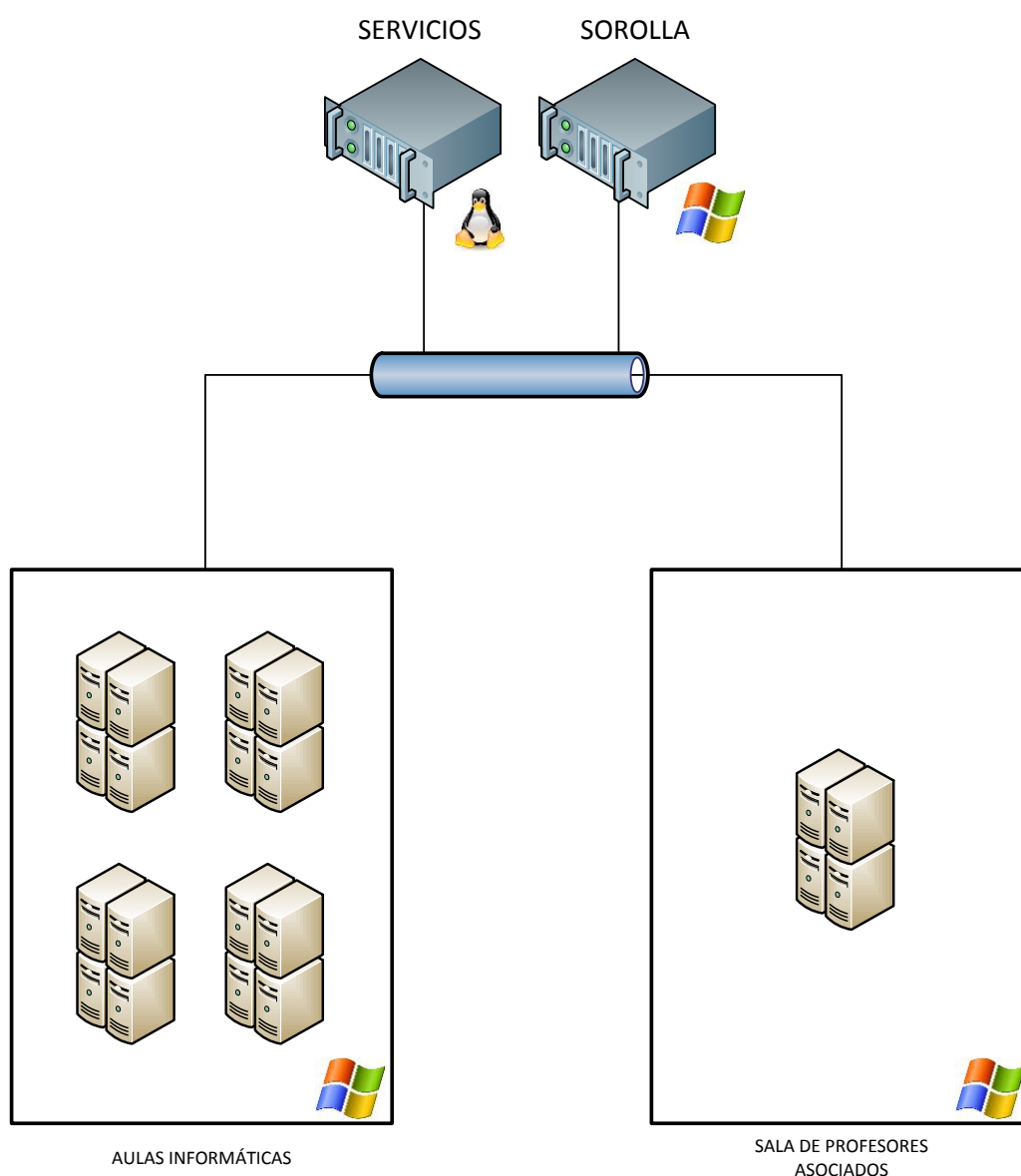


Figura 3.2. Infraestructura Windows.

### 3.1.3. Apertura de cuentas

Para poder acceder a los servicios descritos en el punto 3.1. , los profesores y los alumnos deben tener una cuenta de usuario creada por el ldi. El proceso de apertura de cuenta es diferente en el caso de profesores y alumnos. A continuación se detalla el proceso a seguir para cada colectivo.

#### 3.1.3.1. Alumnos

Para realizar la cuenta de usuario, los alumnos deben rellenar el formulario “Date de Alta” ubicado en la página web (<http://www.lab.inf.uc3m.es>).

**Laboratorio del Departamento de Informática**

Inicio Información Servicios Noticias Mapa Web Buscador Contactar

[Inicio](#) » [Servicios](#) » [Apertura de cuentas](#) Martes, 11 de Septiembre de 2012

### Apertura de cuentas

En esta página podrás abrir una cuenta para poder ser utilizada en las aulas Linux del Departamento de Informática del campus de Leganés (4.0.F16, 4.0.F18, 1.0.A01, 1.0.A02 y 1.0.H02).

Sólo pueden inscribirse alumnos tengan al menos una asignatura que se imparta en dichos laboratorios. Antes de realizar la apertura de la cuenta, se comprobarán las listas oficiales de las asignaturas de cada titulación, para comprobar su veracidad.

Cuidado: una vez introducido, no podrás corregirlo.

#### ¡Última hora!

- Horario de apertura en Agosto (23/07/12)
- Actualiza tu cuenta para utilizar también Windows (04/07/12)
- Clúster kasukabe activo (02/03/12)

#### Date de Alta

Nombre y apellidos:

N.I.A.:

Titulación:

#### Estado de tu cuenta

Aquí podrás ver en que estado se encuentra tu cuenta de linux. Introduce tu NIA y aparecerá un diálogo con el resultado.

N.I.A.:

#### Solicitar nueva contraseña

Aquí podrás solicitar una nueva contraseña para tu cuenta de linux si has olvidado la que tenías. Introduce tu NIA y se te enviará un correo con el que podrás activar una nueva contraseña para tu cuenta

N.I.A.:

[Volver arriba](#)

W3C XHTML 1.0 W3C CSS W3C WAI-AA WCAG 1.0 Laboratorio del Departamento de Informática (LDI) [lab@lab.inf.uc3m.es](mailto:lab@lab.inf.uc3m.es)

Figura 3.3. Página web de apertura de cuentas.

En dicho formulario el alumno tiene que rellenar su nombre y apellidos además del NIA y la titulación que está cursando. Una vez enviado el formulario se crea en el servidor un fichero de texto con los datos introducidos por el usuario, para ser posteriormente tratados por otra herramienta que se describe detalladamente en el punto 3.1.4.1.

Como se puede ver en la Figura 3.1 también se ofrece la posibilidad de consultar si el alumno ya tiene cuenta creada y la solicitud de cambio de contraseña de la cuenta.

### **3.1.3.2. Profesores**

En el caso de los profesores, las cuentas de usuario se realizan de manera manual. Además si necesitan utilizar la sala de profesores asociados, también se les ha de crear otra cuenta en el dominio de Windows para poder utilizar dichos equipos.

Los datos de usuario entre las cuentas del entorno Linux y Windows no son compartidas por lo que se deben copiar primero en otro soporte si se desea mover datos de una cuenta a otra.

Además de los tipos de cuentas descritas en los apartados anteriores, también se pueden solicitar cuentas genéricas temporales, normalmente utilizadas para la realización de una sesión de prácticas.

### **3.1.3.3. Cuentas genéricas**

Se pueden crear cuentas genéricas en el sistema operativo Linux como Windows. Dichas cuentas son independientes y no comparten datos de usuario, debido a que los servidores que autentican y almacenan datos son distintos.

Lo habitual es tener cuentas de usuario genéricas por asignatura en el caso del entorno Windows.

### 3.1.4. Administración de cuentas de usuario

A continuación se describe los recursos que se tienen disponibles para administrar las cuentas de usuario del ldi.

#### 3.1.4.1. Entorno Linux

Para gestionar las cuentas de usuario del entorno Linux se disponía de una herramienta denominada GESTION. Dicha herramienta es un conjunto de *scripts* realizados en el lenguaje *bash* que permitían a los administradores crear y gestionar las cuentas de usuario del entorno Linux.

Las cuentas realizadas desde la página web (apartado 3.1.3.1. ) han de ser creadas desde esta herramienta de manera manual (opción “Script cuentas”).

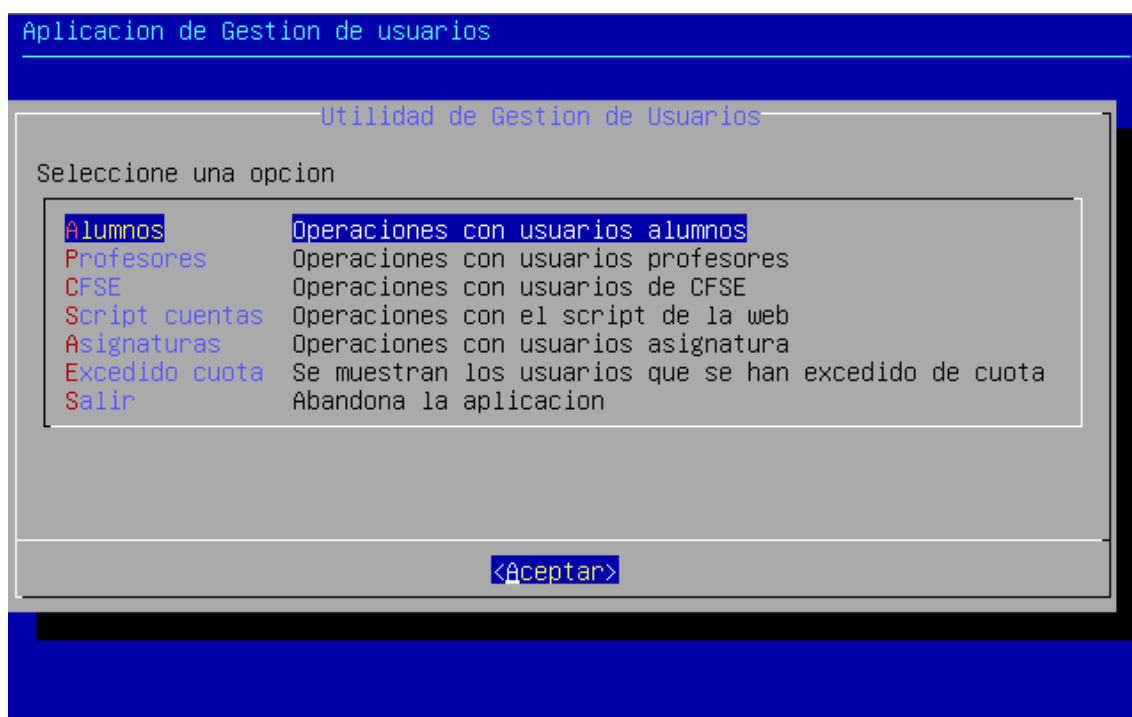


Figura 3.4. Pantalla principal de la herramienta GESTION.

### 3.1.4.2. Entorno Windows

Para gestionar las cuentas de usuario del entorno Windows se dispone de una herramienta incluida en el software servidor Windows 2003 Server denominada *Active Directory*.

*Active Directory* permite a los administradores gestionar de forma centralizada los usuarios y los equipos de la red.

En el entorno Windows solamente se tienen cuentas de usuario genéricas por asignatura y cuentas de profesores asociados que son utilizadas exclusivamente en la sala habilitada para ellos.

A continuación se muestra la pantalla principal de la gestión de usuarios y equipos de *Active Directory*.

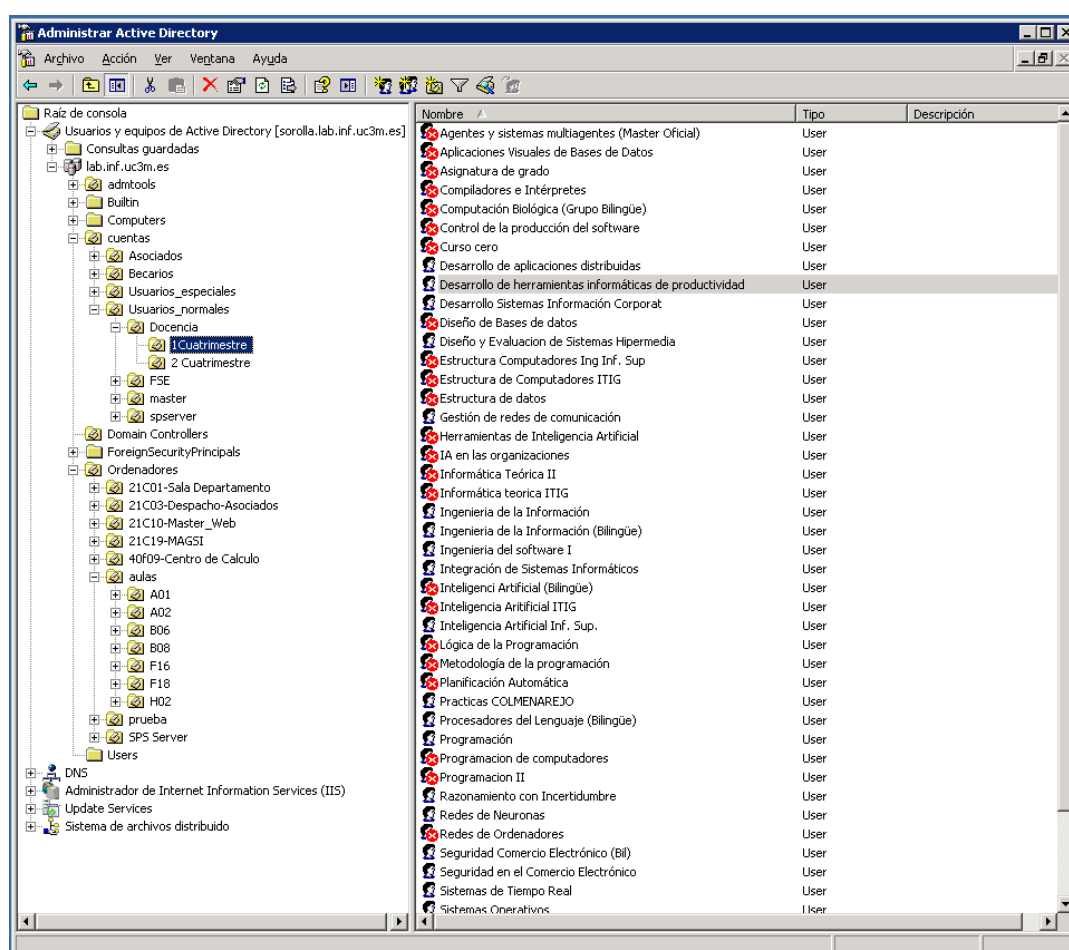


Figura 3.5. Pantalla principal de gestión de usuarios Windows.

## 3.2. Descripción general

A continuación se va a realizar una descripción de las funcionalidades que debe tener el sistema, los sistemas externos que interactúan con él y los perfiles de los usuarios que lo utilizarán.

### 3.2.1. Funcionalidades

Las principales funcionalidades del sistema a desarrollar son las siguientes:

- **Cuenta de usuario única:** El usuario dispondrá solamente de una cuenta de usuario para utilizar cualquier servicio del ldi.
- **Compatibilidad de cuenta:** Los usuarios que ya estaban registrados en el sistema no necesitarán cambiar sus datos de acceso ni perderán los datos ya almacenados en el sistema.
- **Creación de cuenta de usuario:** Los usuarios podrán crear su cuenta de usuario de manera sencilla y sin restricciones de tiempo.
- **Gestión de la contraseña:** El usuario podrá cambiar su contraseña de manera sencilla y en cualquier momento.
- **Administración de cuentas de usuario:** El sistema permitirá a los administradores del ldi una administración sencilla de las cuentas de usuario creadas.
- **Gestión de la configuración de equipos:** Se podrá gestionar remotamente y automáticamente la configuración de los equipos en el entorno Windows.
- **Gestión de tareas programadas:** Se podrá gestionar las tareas programadas que se deseen (entorno Windows) en cada aula ó equipo dependiendo de la configuración aplicada.
- **Copia de seguridad** de la información de autenticación de los usuarios.

### 3.2.2. Restricciones

Las principales restricciones del sistema a implantar son las siguientes:

- **Políticas de regulación:** El sistema manejará datos personales de los usuarios por lo que se deberá cumplir la ley de protección de

datos. (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).

- **Requisitos del lenguaje de alto nivel:** Se utilizará cualquier lenguaje que permita realizar aplicaciones web.
- **Requisitos de fiabilidad:** El sistema debe estar operativo durante 24 horas los 7 días de la semana debido a que un usuario se puede registrar en cualquier momento.
- **Consideraciones de seguridad:** Existe control de acceso al sistema debido a que existen distintos perfiles de usuario que pueden interactuar y con distintos niveles de restricción.

### 3.2.3. Características de los usuarios

Los perfiles de usuarios a los que va dirigido el sistema son muy diversos y con un nivel educativo diferente. A continuación se desarrolla los distintos perfiles de usuarios del sistema.

- **Alumno:** El perfil de usuario alumno tiene acceso a todos los recursos del ldi excepto a los equipos de la sala del Departamento y la sala de profesores asociados.
- **Profesor:** El perfil de usuario profesor tiene acceso a todos los recursos del ldi.
- **Administrador:** El perfil de usuario administrador tiene acceso a todos los recursos del ldi y además puede gestionarlos.

### 3.2.4. Entorno operacional

El sistema desarrollado necesitará realizar consultas al servidor ldap de la universidad para realizar las siguientes tareas:

- Verificar la autenticidad de los usuarios que solicitan la cuenta del ldi.
- Obtener los datos necesarios para crear la cuenta de usuario, en este caso: nombre, apellidos y carrera matriculada (alumno) ó Departamento (profesor).



### 3.3. Requisitos del sistema

La especificación de requisitos que se va a mostrar en este documento, representa los diferentes requerimientos que el sistema debe ser capaz de satisfacer.

Se clasifican en dos grupos: requisitos de capacidad y de restricción:

- Los requisitos de capacidad especifican la funcionalidad que el cliente desea que tenga su sistema.
- Los requisitos de restricción especifican la forma en que se debe construir el sistema y cómo debe el usuario interactuar con él.

Todos los requisitos definidos y especificados en este documento, contendrán los siguientes atributos:

- **Identificador:** los requisitos se nombrarán de manera unívoca con un identificador que tendrá el siguiente formato:

RC-XXX para los Requisitos de Capacidad

RR-XXX para los Requisitos de Restricción

Donde las X serán números comprendidos entre 0 y 9, y se incrementarán en una unidad consecutivamente con cada nuevo requisito, comenzando en el 001.

- **Nombre:** breve descripción del objetivo del requisito.
- **Autor:** indicará el autor del requisito. Podrá ser el cliente o el equipo de desarrollo del proyecto.
- **Descripción:** especificación de la funcionalidad que contemplará el requisito.
- **Prioridad:** define la prioridad con la que debe ser resuelto dicho requisito. Los posibles valores de este campo son:
  - Alta: el requisito se debe diseñar e implementar en primer lugar.
  - Media: el requisito se debe diseñar e implementar tras haber diseñado e implementado los de prioridad alta.
  - Baja: la importancia de estos requisitos permite que sean atendidos en último lugar, tras los de prioridad media.

- **Estabilidad:** define la posibilidad de la modificación o borrado del requisito a lo largo del desarrollo del proyecto. Los posibles valores de este campo son:
  - Estable: tiene una probabilidad baja o nula de ser modificado o borrado.
  - Inestable: se trata de un requisito volátil con altas probabilidades de ser modificado o borrado.
- **Estado:** indica la situación en que se encuentra el requisito. Los posibles valores de este campo son:
  - En construcción: el requisito de está llevando a cabo.
  - Pendiente de Aceptación: la resolución del requisito ha concluido pero aún no ha sido evaluado por el cliente.
  - Aceptado: el requisito ha sido aceptado por el cliente.

### 3.3.1. Requisitos de capacidad

En este apartado se van a especificar los requisitos funcionales que el cliente desea que tenga su sistema.

<b>RC-001</b>	<b>Cuenta de usuario única</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El usuario debe poder utilizar todos los recursos del ldi con una cuenta de usuario personal.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.1. Requisito RC-001.

<b>RC-002</b>	<b>Datos de usuario compartidos</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir acceder a los datos de usuario desde los entornos Linux y Windows.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.2. Requisito RC-002.

---

<b>RC-003</b>	<b>Alta de cuenta de usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe ser capaz de crear nuevos usuarios. Para ello, el usuario debe proporcionar su usuario y contraseña de campus global. Además se necesita introducir la contraseña deseada para la cuenta del ldi.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.3. Requisito RC-003.

---

<b>RC-004</b>	<b>Actualización de cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe ser capaz de modificar una cuenta ya registrada en el sistema para que el usuario pueda usar todos los recursos del ldi. Para ello, el usuario debe proporcionar su usuario y contraseña de campus global. Además se necesita introducir la contraseña deseada para la cuenta del ldi.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.4. Requisito RC-004.

---

<b>RC-005</b>	<b>Consulta de existencia de cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir al usuario realizar una consulta para saber si dispone de cuenta en el sistema. Para ello, el usuario debe proporcionar su usuario y contraseña de campus global.
<b>Prioridad</b>	Media
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.5. Requisito RC-005.

<b>RC-006</b>	<b>Cambiar contraseña</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir al usuario cambiar la contraseña. Para ello, el usuario debe proporcionar su usuario y contraseña de campus global. Además se necesita introducir la nueva contraseña deseada para la cuenta del ldi.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.6. Requisito RC-006.

<b>RC-007</b>	<b>Crear bloques de usuarios para asignatura</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema deber permitir a los administradores realizar varias cuentas de usuario temporales. El nombre de usuario está compuesto por un nombre descriptivo y un número.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.7. Requisito RC-007.

<b>RC-008</b>	<b>Crear cuenta de usuario administrador</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema deber permitir a los administradores realizar una nueva cuenta de usuario con el perfil administrador.
<b>Prioridad</b>	Media
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.8. Requisito RC-008.

<b>RC-009</b>	<b>Consultar usuarios que han excedido de cuota</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir a los administradores realizar la consulta de los usuarios que han excedido la cuota en el sistema.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.9. Requisito RC-009.

---

<b>RC-010</b>	<b>Modificar datos cuenta de usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir a los administradores realizar la modificación de los datos de cualquier cuenta de usuario.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.10. Requisito RC-010.

---

<b>RC-011</b>	<b>Eliminar cuenta de usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir a los administradores eliminar cualquier cuenta de usuario.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.11. Requisito RC-011.

---

<b>RC-012</b>	<b>Reenviar contraseña al usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir a los administradores el envío de una nueva contraseña aleatoria al correo electrónico de los usuarios.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.12. Requisito RC-012.

---

<b>RC-013</b>	<b>Bloquear cuenta de usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir a los administradores el bloqueo de una cuenta de usuario.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.13. Requisito RC-013.

<b>RC-014</b>	<b>Desbloquear cuenta de usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir a los administradores el desbloqueo de una cuenta de usuario.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.14. Requisito RC-014.

<b>RC-015</b>	<b>Consultar datos cuenta de usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir a los administradores la consulta de los datos de cualquier cuenta de usuario.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.15. Requisito RC-015.

<b>RC-016</b>	<b>Distribución de políticas de grupo</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir la distribución de políticas de grupo a los clientes windows de igual manera que un servidor <i>Active Directory</i> .
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.16. Requisito RC-016.

<b>RC-017</b>	<b>Distribución de tareas programadas</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe realizar la distribución de tareas programadas a las aulas y equipos cliente.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

Tabla 3.17. Requisito RC-017.

---

<b>RC-018</b>	<b>Copia de seguridad de la información de los usuarios</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe realizar la copia de seguridad periódica de la información de los usuarios.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.18. Requisito RC-018.

### 3.3.2. Requisitos de restricción

En este apartado se va a especificar la forma en que se va a desarrollar el sistema y la interacción del mismo con el usuario.

---

<b>RR-001</b>	<b>Confidencialidad de datos</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema protegerá los datos de los usuarios del sistema haciendo uso de cifrado.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.19. Requisito RR-001.

---

<b>RR-002</b>	<b>Obtención de datos</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema accederá al servidor LDAP de la Universidad de forma anónima para obtener los datos necesarios para gestionar los usuarios del ldi.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.20. Requisito RR-002.

---

<b>RR-003</b>	<b>Compatibilidad</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema de apertura de cuentas debe visualizarse y funcionar correctamente en cualquier navegador.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.21. Requisito RR-003.

---

<b>RR-004</b>	<b>Tiempo de respuesta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema debe permitir el inicio de sesión del usuario en los equipos en menos de 120s.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.22. Requisito RR-004.

---

<b>RR-005</b>	<b>Fiabilidad</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema deber estar activo el mayor tiempo posible, al menos un 99,8% del tiempo.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.23. Requisito RR-005.

---

<b>RR-006</b>	<b>Usabilidad</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	Hay que simplificar las tareas que impliquen a otras más pequeñas en pequeños pasos guiados para que el usuario en todo momento no se sienta desorientado en la página web.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.24. Requisito RR-006.



---

<b>RR-007</b>	<b>Comunicaciones seguras</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	Las comunicaciones, tanto en el interior del sistema como en el exterior deberán estar cifradas.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.25. Requisito RR-007.

---

<b>RR-008</b>	<b>Acceso a aplicaciones</b>
<b>Autor</b>	Equipo de desarrollo
<b>Descripción</b>	El sistema dispondrá de distintos niveles de restricción para el acceso a las aplicaciones. Dichos niveles son: administrador y usuario.
<b>Prioridad</b>	Alta
<b>Estabilidad</b>	Estable
<b>Estado</b>	Aceptado

---

Tabla 3.26. Requisito RR-008.

### 3.4. Casos de uso

A continuación se desarrollan los casos de uso pertenecientes a la **aplicación web** necesaria para que el usuario gestione su cuenta.

Los casos de uso se identifican con la nomenclatura *CU-XX*, donde las X son valores de 0 a 9.

A los casos de uso se les asigna un nombre que defina claramente su funcionalidad. Para cada caso de uso se indica la siguiente información:

- **Actores:** Agente externo que interactúa con el sistema.
- **Objetivo:** Finalidad del caso de uso.
- **Precondiciones:** Condiciones iniciales que se deben cumplir para realizar el caso de uso.
- **Postcondiciones:** Estado final tras realizar el caso de uso.
- **Descripción:** Explicación del proceso que realiza el caso de uso.
- **Excepción:** Incidencia controlada del caso de uso.

Los casos de uso identificados a partir de los requisitos del cliente son los siguientes:

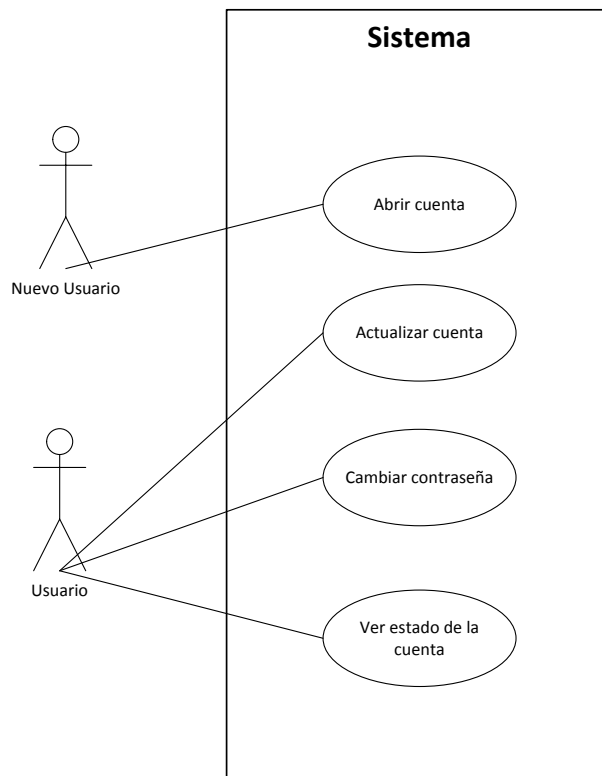


Figura 3.6. Diagrama de casos de uso.

<b>CU-01</b>	<b>Abrir cuenta</b>
<b>Actores</b>	Nuevo Usuario
<b>Objetivo</b>	Crear una nueva cuenta en el sistema.
<b>Precondición</b>	El usuario no existe en el sistema.
<b>Postcondición</b>	Cuenta de usuario creada.
<b>Descripción</b>	<p>En la página web de apertura de cuentas (<a href="https://www.lab.inf.uc3m.es/servicios/apertura_cuentas">https://www.lab.inf.uc3m.es/servicios/apertura_cuentas</a>):</p> <ol style="list-style-type: none"> <li>1. Introducir usuario y contraseña de campus global.</li> <li>2. Introducir la contraseña deseada para la cuenta de usuario en el sistema.</li> <li>3. Pulsar en “Solicitar Cuenta”.</li> <li>4. El usuario recibe un correo de confirmación de solicitud de apertura de cuenta.</li> <li>5. Se notifica al usuario con un correo electrónico cuando la cuenta esté operativa.</li> </ol>
<b>Excepción</b>	<ul style="list-style-type: none"> <li>▪ El identificador de usuario no existe en la base de datos de la universidad.</li> <li>▪ No se cumplen los requisitos de complejidad de contraseña.</li> </ul>

Tabla 3.27. CU-01 Abrir cuenta.

<b>CU-02</b>	<b>Actualizar cuenta</b>
<b>Actores</b>	Usuario
<b>Objetivo</b>	Se actualiza la cuenta en el sistema para que el usuario pueda utilizar todos los sistemas operativos.
<b>Precondición</b>	El usuario debe existir en el sistema.
<b>Postcondición</b>	Cuenta de usuario actualizada.
<b>Descripción</b>	<p>En la página web de actualización de cuenta (<a href="https://www.lab.inf.uc3m.es/servicios/cambiar_pass">https://www.lab.inf.uc3m.es/servicios/cambiar_pass</a>):</p> <ol style="list-style-type: none"> <li>1. Introducir usuario y contraseña de campus global.</li> <li>2. Introducir la contraseña deseada para la cuenta de usuario en el sistema.</li> <li>3. Pulsar en “Enviar”.</li> <li>4. El usuario recibe un correo electrónico cuando la cuenta ha sido actualizada por el sistema.</li> </ol>
<b>Excepción</b>	<ul style="list-style-type: none"> <li>▪ El identificador de usuario no existe en la base de datos de la universidad.</li> <li>▪ No se cumplen los requisitos de complejidad de contraseña.</li> </ul>

Tabla 3.28. CU-02 Actualizar cuenta.

<b>CU-03</b>	<b>Cambiar contraseña</b>
<b>Actores</b>	Usuario
<b>Objetivo</b>	El usuario cambia su contraseña de acceso a los equipos.
<b>Precondición</b>	El usuario debe existir en el sistema.
<b>Postcondición</b>	Contraseña de usuario cambiada.
<b>Descripción</b>	<p>En la página web de actualización de cuenta (<a href="https://www.lab.inf.uc3m.es/servicios/cambiar_pass">https://www.lab.inf.uc3m.es/servicios/cambiar_pass</a>):</p> <ol style="list-style-type: none"> <li>1. Introducir usuario y contraseña de campus global.</li> <li>2. Introducir la contraseña deseada para la cuenta de usuario en el sistema.</li> <li>3. Pulsar en “Enviar”.</li> <li>4. El usuario recibe un correo electrónico cuando la contraseña ha sido cambiada por el sistema.</li> </ol>
<b>Excepción</b>	<ul style="list-style-type: none"> <li>▪ El identificador de usuario no existe en la base de datos de la universidad.</li> <li>▪ No se cumplen los requisitos de complejidad de contraseña.</li> </ul>

Tabla 3.29. CU-03 Cambiar contraseña.

<b>CU-04</b>	<b>Ver estado de la cuenta</b>
<b>Actores</b>	Usuario
<b>Objetivo</b>	Consultar la existencia de la cuenta.
<b>Precondición</b>	Ninguna.
<b>Postcondición</b>	Se muestra el estado de la cuenta.
<b>Descripción</b>	<p>En la página web de apertura de cuentas (<a href="https://www.lab.inf.uc3m.es/servicios/apertura_cuentas">https://www.lab.inf.uc3m.es/servicios/apertura_cuentas</a>):</p> <ol style="list-style-type: none"> <li>1. Introducir usuario y contraseña de campus global.</li> <li>2. Pulsar en “Buscar”.</li> <li>3. La página web muestra el resultado de la operación.</li> </ol>
<b>Excepción</b>	<ul style="list-style-type: none"> <li>▪ El identificador de usuario no existe en la base de datos de la universidad.</li> </ul>

Tabla 3.30. CU-04 Ver estado de la cuenta.

# Capítulo 4

## Diseño

En este capítulo se van a establecer los requisitos software y se expone la arquitectura de red de la solución. Por último se presenta la matriz de trazabilidad entre los requisitos de usuario y los requisitos software y la matriz de trazabilidad entre los requisitos software y los componentes que forman el sistema.

### 4.1. Establecimiento de requisitos software

Los requisitos que se van a definir son los siguientes:

- **Funcionales:** Se identifican por **RSF**.
- **Rendimiento:** Se identifican por **RSR**.
- **Interfaz:** Se identifican por **RSI**.
- **Operación:** Se identifican por **RSO**.
- **Recursos:** Se identifican por **RSRe**.
- **Comprobación:** Se identifican por **RSC**.
- **Seguridad:** Se identifican por **RSS**.
- **Fiabilidad:** Se identifican por **RSFi**.

Los datos necesarios para definir un requisito son los siguientes:

- **Nombre:** Breve identificación del requerimiento.
- **Autor:** Origen del requerimiento, que será el cliente o el Equipo de desarrollo
- **Fuente:** Referencia al requisito de usuario del que proviene.
- **Prioridad:** Puede tomar los valores Alta, Media o Baja, que ayudará al desarrollador a planificar el orden en el que tienen que realizarlos.
- **Descripción:** Explicación del proceso que realiza el requerimiento.

### 4.1.1. Requisitos funcionales

A continuación se describen los requisitos funcionales que debe cumplir el sistema propuesto.

<b>RSF-001</b>	<b>Servidor de autenticación único</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-001
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema tendrá un servidor LDAP que realizará la autenticación de los usuarios que utilicen cualquier servicio de laboratorio.

Tabla 4.1. Requisito RSF-001.

<b>RSF-002</b>	<b>Servidor autenticación para clientes Windows</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-001
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema tendrá un servidor de autenticación (SAMBA) compatible con los clientes Windows. Este servidor trasladará la autenticación realizada por un cliente Windows al servidor LDAP centralizado.

Tabla 4.2. Requisito RSF-002.

<b>RSF-003</b>	<b>Servidor de almacenamiento de ficheros</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-002
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema tendrá un servidor que almacene los datos pertenecientes a los usuarios del ldi.

Tabla 4.3. Requisito RSF-003.

---

<b>RSF-004</b>	<b>Servicio de archivos para clientes Linux</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-002
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema tendrá un servicio compatible con los clientes Linux para que los usuarios puedan utilizar los datos almacenados en la cuenta.

---

Tabla 4.4. Requisito RSF-004.

---

<b>RSF-005</b>	<b>Servicio de archivos para clientes Windows</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-002
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema tendrá un servicio compatible con los clientes Windows para que los usuarios puedan utilizar los datos almacenados en la cuenta.

---

Tabla 4.5. Requisito RSF-005.

---

<b>RSF-006</b>	<b>Página web alta cuenta usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-003
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema tendrá una página web para que cualquier usuario pueda realizar una nueva cuenta en el ldi.

---

Tabla 4.6. Requisito RSF-006.

---

<b>RSF-007</b>	<b>Fichero almacenamiento temporal de cuentas</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-003, RC-004, RC-006
<b>Prioridad</b>	Alta
<b>Descripción</b>	Los datos de los nuevos usuarios estarán almacenados temporalmente en el servidor web antes de proceder a realizar la operación correspondiente (nueva cuenta/cambio de contraseña).

---

Tabla 4.7. Requisito RSF-007.

<b>RSF-008</b>	<b>Script creación de cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-003
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> de creación de cuentas ubicado en el servidor de autenticación centralizado, que se ejecutará cada 5 minutos. Dicho <i>script</i> obtendrá el fichero de usuarios del servidor web y procederá a realizar las nuevas cuentas.

Tabla 4.8. Requisito RSF-008.

<b>RSF-009</b>	<b>Servidor correo electrónico</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-003, RC-004, RC-006
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema necesitará un servidor de correo electrónico para enviar las notificaciones de apertura de cuenta y cambio de contraseña a los usuarios.

Tabla 4.9. Requisito RSF-009.

<b>RSF-010</b>	<b>Página web cambio contraseña cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-004, RC-006
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema tendrá una página web para que cualquier usuario pueda realizar el cambio de contraseña de su cuenta en el ldi.

Tabla 4.10. Requisito RSF-010.

<b>RSF-011</b>	<b>Script cambio contraseña cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-004, RC-006
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> de cambio de contraseñas ubicado en el servidor de autenticación centralizado, que se ejecutará cada 5 minutos. Dicho <i>script</i> obtendrá el fichero de usuarios del servidor web y procederá a realizar los cambios de contraseña oportunos.

Tabla 4.11. Requisito RSF-011.



<b>RSF-012</b>	<b>Página web consulta estado cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-005
<b>Prioridad</b>	Media
<b>Descripción</b>	El sistema tendrá una página web para que cualquier usuario pueda consultar la existencia de su cuenta en el ldi.

Tabla 4.12. Requisito RSF-012.

<b>RSF-013</b>	<b>Script creación bloques de usuarios asignatura</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-007
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi realizar varias cuentas independientes asociadas a una asignatura. Dichas cuentas se distinguirán por un uno o varios dígitos al final del nombre de la cuenta. Un ejemplo formado por 20 cuentas: asig1, asig2 ... asig19, asig20.

Tabla 4.13. Requisito RSF-013.

<b>RSF-014</b>	<b>Script creación cuenta usuario administrador</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-008
<b>Prioridad</b>	Media
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi realizar cuentas con privilegios de administrador.

Tabla 4.14. Requisito RSF-014.

<b>RSF-015</b>	<b>Script consulta cuentas excedidas cuota</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-009
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi consultar las cuentas que se han excedido de cuota en el sistema.

Tabla 4.15. Requisito RSF-015.

<b>RSF-016</b>	<b>Script modificación datos cuenta tipo alumno/profesor/asignatura</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-010
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi modificar los datos de las cuentas pertenecientes a un alumno, profesor o asignatura.

Tabla 4.16. Requisito RSF-016.

<b>RSF-017</b>	<b>Script modificación datos cuenta tipo bdua</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-010
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi modificar los datos de las cuentas pertenecientes a una asignatura.

Tabla 4.17. Requisito RSF-017.

<b>RSF-018</b>	<b>Script eliminar cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-011
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi eliminar una cuenta del sistema.

Tabla 4.18. Requisito RSF-018.

<b>RSF-019</b>	<b>Script reenvío contraseña cuenta alumno</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-012
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi generar una contraseña aleatoria y enviársela a la cuenta de correo de la universidad del alumno.

Tabla 4.19. Requisito RSF-019.

<b>RSF-020</b>	<b>Script reenvío contraseña cuenta usuario tipo profesor/bdua/asignatura</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-012
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi generar una contraseña aleatoria perteneciente a las cuentas de usuario de profesores, bloques de usuarios de asignatura y asignaturas. Dicha contraseña se enviará a la cuenta de correo que especifique el administrador.

Tabla 4.20. Requisito RSF-020.

<b>RSF-021</b>	<b>Script bloqueo cuenta tipo alumno/profesor/asignatura</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-013
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi el bloqueo de cuentas pertenecientes a los alumnos, profesores y asignaturas.

Tabla 4.21. Requisito RSF-021.

<b>RSF-022</b>	<b>Script bloqueo cuenta tipo bdua</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-013
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi el bloqueo de cuentas pertenecientes a los bloques de usuarios de asignatura.

Tabla 4.22. Requisito RSF-022.

<b>RSF-023</b>	<b>Script desbloqueo cuenta tipo alumno/profesor/asignatura</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-014
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi el desbloqueo de cuentas pertenecientes a los alumnos, profesores y asignaturas.

Tabla 4.23. Requisito RSF-023.

<b>RSF-024</b>	<b>Script desbloqueo cuenta tipo bdua</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-014
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi el desbloqueo de cuentas pertenecientes a los bloques de usuarios de asignatura.

Tabla 4.24. Requisito RSF-024.

<b>RSF-025</b>	<b>Script consulta datos cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-015
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que permitirá a los administradores del ldi realizar la consulta de los datos de una cuenta.

Tabla 4.25. Requisito RSF-025.

<b>RSF-026</b>	<b>Servidor almacenamiento políticas/tareas</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-016, RC-017
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema necesitará un servidor que almacene las políticas y las tareas que se aplicarán posteriormente a los equipos/aulas.

Tabla 4.26. Requisito RSF-026.

<b>RSF-027</b>	<b>Script políticas cliente Windows</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-016
<b>Prioridad</b>	Alta
<b>Descripción</b>	El cliente windows contará con un <i>script</i> que obtendrá del servidor “almacén” la política que le corresponde en función del aula ó equipo y posteriormente se la aplicará al sistema.

Tabla 4.27. Requisito RSF-027.

<b>RSF-028</b>	<b>Aplicación gestión distribución políticas</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-016
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con una aplicación para gestionar la distribución de políticas por aula y por equipo.

Tabla 4.28. Requisito RSF-028.

<b>RSF-029</b>	<b>Script tareas cliente Windows</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-017
<b>Prioridad</b>	Alta
<b>Descripción</b>	El cliente windows contará con un <i>script</i> que obtendrá del servidor “almacén” la/s tarea/s que le corresponde en función del aula ó equipo.

Tabla 4.29. Requisito RSF-029.

<b>RSF-030</b>	<b>Aplicación gestión distribución tareas</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-017
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con una aplicación para gestionar la distribución de tareas por aula y por equipo.

Tabla 4.30. Requisito RSF-030.

<b>RSF-031</b>	<b>Script acceso a datos LDAP Universidad</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-002
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema contará con un <i>script</i> que obtendrá, de forma anónima, los datos de los usuarios registrados del servidor ldap de la Universidad. El único dato que se necesitará es el identificador del usuario asignado por la Universidad.

Tabla 4.31. Requisito RSF-031.

#### 4.1.2. Requisitos de rendimiento

A continuación se describen los requisitos de rendimiento que debe cumplir el sistema propuesto.

<b>RSR-001</b>	<b>Tiempo respuesta inicio sesión clientes</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-004
<b>Prioridad</b>	Alta
<b>Descripción</b>	Los clientes, tanto Windows como Linux deben realizar la autenticación del usuario y estar operativos en menos de 120s.

Tabla 4.32. Requisito RSR-001.

<b>RSR-002</b>	<b>Tiempo respuesta creación cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-004
<b>Prioridad</b>	Alta
<b>Descripción</b>	El servidor web no debe tardar más de 5s en procesar la información necesaria para realizar la cuenta de usuario.

Tabla 4.33. Requisito RSR-002.

<b>RSR-003</b>	<b>Capacidad del sistema</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-004
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema debe ser capaz de permitir una media de 100 usuarios simultáneamente con picos de 300 usuarios en la franja de mayor utilización.

Tabla 4.34. Requisito RSR-003.

### 4.1.3. Requisitos de interfaz

A continuación se describen los requisitos de interfaz que debe cumplir el sistema propuesto.

<b>RSI-001</b>	<b>Visualización en navegadores</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-003
<b>Prioridad</b>	Alta
<b>Descripción</b>	Las páginas web deben poder ser visualizadas correctamente desde los siguientes navegadores: <ul style="list-style-type: none"> <li>▪ Internet Explorer.</li> <li>▪ Mozilla Firefox.</li> <li>▪ Safari.</li> <li>▪ Opera.</li> <li>▪ Chrome.</li> </ul>

Tabla 4.35. Requisito RSI-001.

<b>RSI-002</b>	<b>Compatibilidad funcional con navegadores</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-003
<b>Prioridad</b>	Alta
<b>Descripción</b>	La funcionalidad proporcionada por las páginas web deben funcionar correctamente desde los siguientes navegadores: <ul style="list-style-type: none"> <li>▪ Internet Explorer.</li> <li>▪ Mozilla Firefox.</li> <li>▪ Safari.</li> <li>▪ Opera.</li> <li>▪ Chrome.</li> </ul>

Tabla 4.36. Requisito RSI-002.

<b>RSI-003</b>	<b>Desplazamiento en formularios</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-006
<b>Prioridad</b>	Alta
<b>Descripción</b>	<p>Para los formularios contenidos en las páginas web deberá ser posible desplazarse por sus campos usando el tabulador. El orden que se establece para el desplazamiento es:</p> <ul style="list-style-type: none"> <li>▪ Dentro de la misma línea se desplaza a la derecha.</li> <li>▪ Al llegar al final de la línea se desplaza a la siguiente línea y se comienza en el primer campo de la izquierda.</li> <li>▪ Si se ha llegado al final del formulario se vuelve al primer campo.</li> </ul> <p>Se podrá desplazar usando los cursores, desplazándose hacia la dirección indicada en el cursor.</p> <p>Mediante el ratón se activará el campo sobre el que esté el puntero.</p>

Tabla 4.37. Requisito RSI-003.

<b>RSI-004</b>	<b>Usabilidad</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-006
<b>Prioridad</b>	Alta
<b>Descripción</b>	<p>Los procesos complejos se dividirán dentro de la navegación en distintas acciones en función de su complejidad para facilitar la realización del mismo por el usuario.</p>

Tabla 4.38. Requisito RSI-004.



<b>RSI-005</b>	<b>Mensajes de error</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-006
<b>Prioridad</b>	Alta
<b>Descripción</b>	Los errores que se produzcan durante la navegación y el proceso de la información se mostrarán al usuario. La información que se muestre es la siguiente: <ul style="list-style-type: none"> <li>▪ Descripción del error.</li> <li>▪ Posible solución.</li> </ul>

Tabla 4.39. Requisito RSI-005.

#### 4.1.4. Requisitos de operación

A continuación se describen los requisitos de operación que debe cumplir el sistema propuesto.

<b>RSO-001</b>	<b>Control de accesos concurrentes apertura cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-003
<b>Prioridad</b>	Alta
<b>Descripción</b>	Se controlará las escrituras simultáneas del fichero almacenado en el servidor web que contiene los datos de los nuevos usuarios para evitar que se produzcan errores.

Tabla 4.40. Requisito RSO-001.

<b>RSO-002</b>	<b>Perfiles de cuenta</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-008
<b>Prioridad</b>	Alta
<b>Descripción</b>	El sistema servirá dos tipos de perfiles de usuario para el cliente Windows dependiendo del usuario: <ul style="list-style-type: none"> <li>▪ Alumno/Profesor: Este tipo de perfil permitirá guardar la información almacenada en el escritorio y en la carpeta “Mis documentos”.</li> <li>▪ Asignatura/bdua: Este tipo de perfil no permitirá guardar ningún dato cuando se cierre la sesión</li> </ul>

Tabla 4.41. Requisito RSO-002.

---

<b>RSO-003</b>	<b>Grupos de usuario</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-008
<b>Prioridad</b>	Alta
<b>Descripción</b>	<p>El sistema dispondrá de los siguientes grupos de usuarios para controlar el acceso a los recursos:</p> <ul style="list-style-type: none"><li>▪ alumnos</li><li>▪ adm</li><li>▪ asignaturas</li><li>▪ bdua</li><li>▪ profesores</li></ul>

---

Tabla 4.42. Requisito RSO-003.

---

<b>RSO-004</b>	<b>Script copia seguridad datos servidor ldap</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RC-018
<b>Prioridad</b>	Alta
<b>Descripción</b>	<p>El servidor de autenticación realizará una vez por semana una copia de seguridad de los datos de autenticación de las cuentas de usuario del ldi.</p>

---

Tabla 4.43. Requisito RSF-004.

### 4.1.5. Requisitos de recursos

A continuación se describen los requisitos de recursos que debe cumplir el sistema propuesto.

<b>RSRe-001</b>	<b>Especificación de los servidores</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-005
<b>Prioridad</b>	Alta
<b>Descripción</b>	<p>Los servidores empleados para el desarrollo del proyecto tendrán las siguientes características:</p> <ul style="list-style-type: none"> <li>▪ Supermicro H8MR-82</li> <li>▪ 2 CPU Dual-Core AMD Opteron(tm) Processor 2214</li> <li>▪ 8GB DDR2 - 667MHz</li> </ul>

Tabla 4.44. Requisito RSRe-001.

<b>RSRe-002</b>	<b>Especificación de comunicaciones</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-005
<b>Prioridad</b>	Alta
<b>Descripción</b>	<p>Las comunicaciones entre los servidores se realizará a través de una red LAN Ethernet de velocidad 1Gbps. La comunicación entre los clientes y los servidores se realizará a través de una red LAN Ethernet de velocidad 100Mbps.</p>

Tabla 4.45. Requisito RSRe-002.

#### 4.1.6. Requisitos de comprobación

A continuación se describen los requisitos de comprobación que debe cumplir el sistema propuesto.

<b>RSC-001</b>	<b>Verificación datos usuario ldap Universidad</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-002
<b>Prioridad</b>	Alta
<b>Descripción</b>	Cada vez que se obtengan datos del servidor LDAP de la Universidad se realizará una comprobación de compatibilidad con el servidor LDAP del laboratorio antes de proceder a su almacenamiento. Por ejemplo, existen caracteres que deben ser eliminados previamente, como por ejemplo, la letra ñ.

Tabla 4.46. Requisito RSC-001.

#### 4.1.7. Requisitos de seguridad

A continuación se describen los requisitos de seguridad que debe cumplir el sistema propuesto.

<b>RSS-001</b>	<b>Cifrado comunicaciones cliente-servidor ldap</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-007
<b>Prioridad</b>	Alta
<b>Descripción</b>	Las comunicaciones establecidas entre los clientes y el servidor ldap estarán cifradas para proteger la contraseña de acceso de los usuarios.

Tabla 4.47. Requisito RSS-001.

<b>RSS-002</b>	<b>Cifrado comunicaciones servidor web</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-007
<b>Prioridad</b>	Alta
<b>Descripción</b>	Las comunicaciones realizadas con las páginas web de apertura de cuenta, cambio de contraseña y estado de la cuenta estarán cifradas mediante el protocolo seguro https.

Tabla 4.48. Requisito RSS-002.

<b>RSS-003</b>	<b>Almacenamiento contraseña cifrada</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-001
<b>Prioridad</b>	Alta
<b>Descripción</b>	Las contraseñas de acceso se almacenarán cifradas en el servidor ldap.

Tabla 4.49. Requisito RSS-003.

<b>RSS-004</b>	<b>Configuración acceso no anónimo servidor ldap</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-001
<b>Prioridad</b>	Alta
<b>Descripción</b>	Para establecer comunicación con del servidor ldap se requerirá de un usuario y contraseña.

Tabla 4.50. Requisito RSS-004.

#### 4.1.8. Requisitos de fiabilidad

A continuación se describen los requisitos de fiabilidad que debe cumplir el sistema propuesto.

<b>RSFi-001</b>	<b>Distribución carga autenticación</b>
<b>Autor</b>	Equipo de desarrollo
<b>Fuente</b>	RR-005
<b>Prioridad</b>	Alta
<b>Descripción</b>	Para distribuir la carga de autenticación, el sistema contará con un servidor de apoyo destinado a los clientes Windows. Los clientes Linux autenticarán con el servidor ldap directamente.

Tabla 4.51. Requisito RSFi-001.

## 4.2. Diseño de la arquitectura de la red

Una vez realizado el estudio del sistema, se ha decidido implementar la siguiente arquitectura de red formada por los siguientes subsistemas:

- **Servidor Ldap:** Este servidor proporciona la autenticación a todos los clientes y servidores del ldi.
- **Servidor Cuentas:** Este servidor almacena los datos de los usuarios del ldi.
- **Servidor Políticas:** Este servidor alberga las aplicaciones de gestión de políticas de usuario y tareas programas de los clientes Windows.
- **Servidor Correo:** Este servidor se encarga de enviar los correos electrónicos generados por la aplicación web.
- **Servidor Web:** Este servidor alberga la página web del ldi, entre ellas, la aplicación de gestión de cuentas.
- **Cliente Windows:** Este subsistema representa el equipo físico de un aula cuando está ejecutando el sistema operativo Windows.
- **Cliente Linux:** Este subsistema representa el equipo físico de un aula cuando está ejecutando el sistema operativo Linux.

En la Figura 4.1, se muestra los diferentes subsistemas que se han de implementar y las comunicaciones entre ellos. Los subsistemas con fondo gris no son parte de la solución planteada (recurso externo).

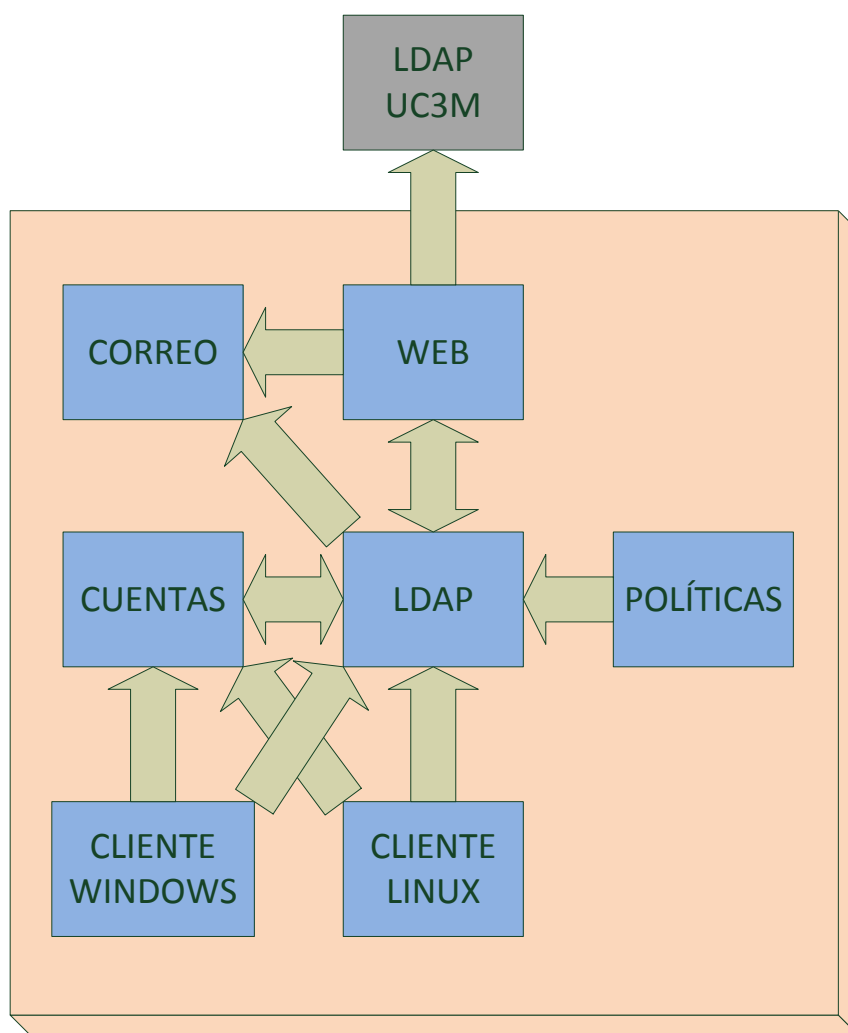


Figura 4.1. Estructura del sistema.

Como se puede observar en la figura anterior, el subsistema ldap es el elemento principal del sistema debido a que casi todos los subsistemas tienen conexión con él. Por otro lado los clientes tienen conexión con ldap y con cuentas debido a que necesitan autenticación y datos de usuario. También se puede observar cómo cuentas y ldap tienen una comunicación bidireccional ya que se necesitan mutuamente para prestar servicio a los clientes de las aulas.

#### 4.2.1. Identificación de los subsistemas de diseño

Como se ha visto en el apartado anterior, el diseño del sistema se divide en siete subsistemas, denominados correo, web, cuentas, ldap, políticas, cliente windows y cliente Linux. A continuación se va a realizar un desglose de componentes atendiendo a su funcionalidad dentro del subsistema.

A continuación se muestra los componentes de cada subsistema identificado en el punto anterior. Los subsistemas con fondo gris no son parte de la solución planteada (recurso externo).

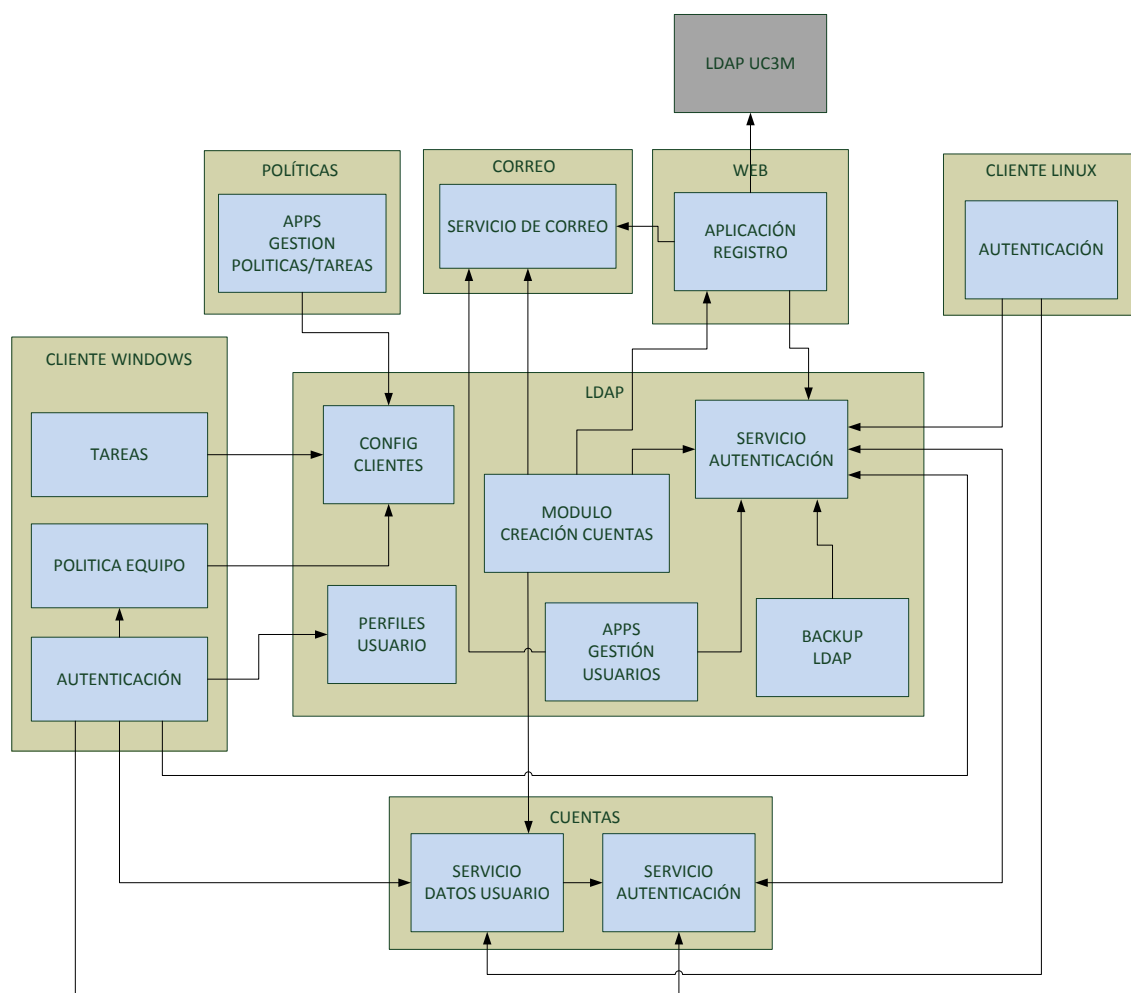


Figura 4.2. Diagrama de subsistemas y componentes.

Como se comentó en el punto 4.2. el subsistema ldap es el elemento principal del sistema y como se puede observar en la Figura 4.2 es el que tiene más componentes. Esto es debido a que dicho subsistema es el que tiene más tareas, entre las destacadas están: gestión de usuarios, creación automática de cuentas, configuración de clientes Windows, servidor de perfiles de usuario y autenticación.



A continuación, se definen los campos que describen los componentes de los subsistemas.

- **Identificador:** este campo identifica de manera unívoca a cada componente. Se seguirá la siguiente nomenclatura: COM[Z]-XX. Donde las X serán números del rango comprendido entre 0 y 9. Se irán incrementar en una unidad consecutivamente con cada nuevo requisito, comenzando en el 01. La Z podrá tomar los valores W (servidor web), C (servidor cuentas), L (servidor ldap), Co (servidor Correo) CW (cliente Windows), CL (cliente Linux) y P (Políticas) identificando al subsistema al que pertenece el componente.
- **Nombre:** denominación del componente
- **Propósito:** Breve descripción del objetivo del componente.
- **Origen:** Requisitos software relacionados con el componente.
- **Procesamiento:** descripción de las funcionalidades del componente.
- **Dependencias:** componentes utilizados por el componente descrito.
- **Recursos:** sistemas externos necesarios para el correcto funcionamiento del componente.
- **Subordinados:** otros componentes que emplean la funcionalidad proporcionada por éste.

#### 4.2.1.1. Componentes del subsistema LDAP

El subsistema LDAP está formado por seis componentes. A continuación se describen dichos componentes:

COML-01	Módulo creación cuentas
<b>Propósito</b>	El módulo de creación de cuentas se encarga de crear las cuentas y modificar las contraseñas de los usuarios que lo solicitan desde la página web del ldi.
<b>Origen</b>	RSF-008, RSF-010, RSF-031, RSRe-001, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Crea cuenta.</li> <li>▪ Modifica contraseña.</li> <li>▪ Actualiza contraseña.</li> </ul>
<b>Dependencias</b>	Servicio de correo, Aplicación registro, Servicio autenticación, Servicio datos usuario.
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Ninguno

Tabla 4.52. COML-01 Módulo creación cuentas.

COML-02	Apps gestión usuarios
<b>Propósito</b>	Este componente gestiona los usuarios del ldi, permite realizar las siguientes tareas sobre las cuentas: crear, eliminar, bloquear, desbloquear, editar datos personales, visualizar datos personales, establecer contraseña aleatoria y listar usuarios que se han sobrepasado la cuota.
<b>Origen</b>	RSF-013, RSF-014, RSF-015, RSF-016, RSF-017, RSF-018, RSF-019, RSF-020, RSF-021, RSF-022, RSF-023, RSF-024, RSF-025, RSF-031, RSRe-001, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Crea cuenta.</li> <li>▪ Elimina cuenta.</li> <li>▪ Bloquea cuenta.</li> <li>▪ Desbloquea cuenta.</li> <li>▪ Editar datos personales cuenta.</li> <li>▪ Visualizar datos personales cuenta.</li> <li>▪ Establecer contraseña aleatoria.</li> <li>▪ Listar usuarios que se han sobrepasado de cuota.</li> </ul>
<b>Dependencias</b>	Servicio autenticación. Servicio de correo.
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Ninguno

Tabla 4.53. COML-02 Apps gestión usuarios.

<b>COML-03</b>	<b>Config clientes</b>
<b>Propósito</b>	Este componente se encarga de almacenar las políticas de grupo (configuraciones) y tareas programadas a los clientes o grupo de clientes (aula).
<b>Origen</b>	RSF-026, RSRe-001, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Exporta por la red una estructura de directorios y ficheros con los clientes Windows.</li> </ul>
<b>Dependencias</b>	Ninguna
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Ninguno

Tabla 4.54. COML-03 Config clientes.

<b>COML-04</b>	<b>Perfiles usuario</b>
<b>Propósito</b>	Este componente alberga los perfiles de los usuarios. Actualmente hay dos tipos de perfiles, el destinado a las cuentas pertenecientes a los alumnos y profesores, y el destinado a las cuentas genéricas (en desuso). La principal diferencia entre ellos es que a los usuarios se les permite guardar los datos de las carpetas escritorio y mis documentos en su cuenta y las cuentas genéricas pierden todos los datos una vez hayan cerrado la sesión.
<b>Origen</b>	RSO-002, RSRe-001, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Exporta por la red una estructura de directorios y ficheros con los clientes Windows.</li> </ul>
<b>Dependencias</b>	Ninguna
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Autenticación (cliente Windows)

Tabla 4.55. COML-04 Perfiles usuario.

<b>COML-05</b>	<b>Servicio autenticación</b>
<b>Propósito</b>	Este componente se encarga de almacenar los datos de los usuarios registrados y procesa las solicitudes de autenticación provenientes de cualquier sistema ó aplicación perteneciente al ldi.
<b>Origen</b>	RSF-001, RSS-001, RSS-003, RSS-004, RSFi-001, RSO-003, RSRe-001, RSRe-002
<b>Procesamiento</b>	▪ Autenticación de usuarios.
<b>Dependencias</b>	Servicio autenticación (cuentas).
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Apps gestión usuarios, Módulo creación cuentas, Aplicación registro, Autenticación (cliente Linux), Autenticación (cliente Windows), Servicio autenticación (cuentas), Backup LDAP.

Tabla 4.56. COML-05 Servicio autenticación.

<b>COML-06</b>	<b>Backup LDAP</b>
<b>Propósito</b>	Este componente se encarga de realizar la copia de seguridad del árbol LDAP una vez por semana. Dicha copia se realizará en formato de fichero ldif y posteriormente será comprimido para ahorrar espacio en disco.
<b>Origen</b>	RSO-004, RSRe-001, RSRe-002
<b>Procesamiento</b>	▪ Copia de seguridad de las cuentas de usuario.
<b>Dependencias</b>	Servicio autenticación (ldap).
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Ninguno

Tabla 4.57. COML-06 Backup LDAP.

#### 4.2.1.2. Componentes del subsistema CUENTAS

El subsistema CUENTAS está formado por dos componentes. A continuación se describen dichos componentes:

COMC-01	Servicio autenticación
<b>Propósito</b>	Este componente se encarga de autenticar los usuarios provenientes de los clientes Windows. Además sirve para distribuir la carga del componente “servicio autenticación” del subsistema LDAP.
<b>Origen</b>	RSF-002, RSS-001, RSFi-001, RSRe-001, RSRe-002
<b>Procesamiento</b>	▪ Autenticación de usuarios (clientes Windows)
<b>Dependencias</b>	Servicio autenticación (ldap)
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Servicio autenticación (ldap), Autenticación (Windows), Servicios datos usuario.

Tabla 4.58. COMC-01 Servicio autenticación.

COMC-02	Servicio datos usuario
<b>Propósito</b>	Este componente sirve los datos de usuario a los clientes Windows y Linux.
<b>Origen</b>	RSF-003, RSF-004, RSF-005, RSRe-001, RSRe-002
<b>Procesamiento</b>	▪ Exportar el árbol de directorios de los datos de usuario.
<b>Dependencias</b>	Servicio autenticación (cuentas)
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Datos usuario (cliente Windows), Módulo creación cuentas, Datos usuario (cliente Linux)

Tabla 4.59. COMC-02 Servicio autenticación.

### 4.2.1.3. Componentes del subsistema CORREO

El subsistema CORREO está formado por un componente. A continuación se describe dicho componente:

<b>COMCo-01</b>	<b>Servicio de correo</b>
<b>Propósito</b>	Este componente se encarga de enviar los correos electrónicos generados por los sistemas y aplicaciones pertenecientes al ldi.
<b>Origen</b>	RSF-009, RSRe-001, RSRe-002
<b>Procesamiento</b>	▪ Envío y recepción de correo.
<b>Dependencias</b>	Ninguna
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Módulo creación cuentas, Apps gestión usuarios.

Tabla 4.60. COMCo-01 Servicio de correo.

### 4.2.1.4. Componentes del subsistema WEB

El subsistema WEB está formado por un componente. A continuación se describe dicho componente:

<b>COMW-01</b>	<b>Aplicación registro</b>
<b>Propósito</b>	Este componente permite a los usuarios crear, consultar estado y cambiar contraseña de su cuenta mediante un navegador web.
<b>Origen</b>	RSF-006, RSF-007, RSF-010, RSF-012, RSF-031, RSR-002, RSI-001, RSI-002, RSI-003, RSI-004, RSI-005, RSO-001, RSS-002, RSRe-001, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Almacena datos de usuario en un fichero cifrado para crear cuenta posteriormente.</li> <li>▪ Almacena datos de usuario en un fichero cifrado para cambiar contraseña posteriormente.</li> <li>▪ Realiza la consulta de existencia de cuenta.</li> </ul>
<b>Dependencias</b>	Servicio autenticación (ldap)
<b>Recursos</b>	LDAP UC3M
<b>Subordinados</b>	Módulo creación cuentas

Tabla 4.61. COMW-01 Aplicación registro.

#### 4.2.1.5. Componentes del subsistema *CLIENTE WINDOWS*

El subsistema CLIENTE WINDOWS está formado por tres componentes. A continuación se describen dichos componentes:

COMCW-01	Tareas
<b>Propósito</b>	Este componente se encarga de obtener la/s tarea/s que le corresponde/n al equipo y las da de alta en el planificador de tareas local.
<b>Origen</b>	RSF-029, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Obtener tareas y copiar localmente.</li> <li>▪ Dar de alta las nuevas tareas en el planificador local.</li> </ul>
<b>Dependencias</b>	Config clientes
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Ninguno

Tabla 4.62. COMCW-01 Tareas.

COMCW-02	Política equipo
<b>Propósito</b>	Este componente se encarga de obtener la política de grupo que le corresponde al equipo y realiza su aplicación inmediata.
<b>Origen</b>	RSF-027, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Obtener política de grupo.</li> <li>▪ Aplicar política de grupo.</li> </ul>
<b>Dependencias</b>	Config clientes
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Autenticación (Cliente Windows)

Tabla 4.63. COMCW-02 Política equipo.

COMCW-03	Autenticación
<b>Propósito</b>	Este componente se encarga de realizar la autenticación con el servidor de los usuarios. Para que se pueda realizar la autenticación se debe consultar si existe alguna restricción proveniente de una política de grupo. Además, todo usuario necesita un perfil que contendrá las configuraciones necesarias para utilizar los programas instalados. Una vez realizada la autenticación, los datos de la cuenta de usuario se podrán acceder desde dicho cliente.
<b>Origen</b>	RSF-001, RSR-001, RSR-003, RSS-001, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Autenticación de usuarios.</li> <li>▪ Consulta de políticas de grupo.</li> <li>▪ Aplicación del perfil correspondiente al usuario.</li> <li>▪ Montaje de los datos del usuario.</li> </ul>
<b>Dependencias</b>	Política equipo, Perfiles usuario, Servicio autenticación (cuentas), Servicio datos usuario (cuentas)
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Ninguno

Tabla 4.64. COMCW-03 Autenticación.

#### 4.2.1.6. Componentes del subsistema *CLIENTE LINUX*

El subsistema CLIENTE LINUX está formado por un componente. A continuación se describe dicho componente:

COMCL-01	Autenticación
<b>Propósito</b>	Este componente se encarga de realizar la autenticación con el servidor de los usuarios. Si la autenticación se realiza correctamente el usuario podrá acceder a los datos de su cuenta.
<b>Origen</b>	RSF-001, RSR-001, RSR-003, RSS-001, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Autenticación de usuarios.</li> <li>▪ Montaje de los datos del usuario.</li> </ul>
<b>Dependencias</b>	Servicio autenticación (ldap), Servicio datos usuario
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Ninguno

Tabla 4.65. COMCW-01 Autenticación.



#### 4.2.1.7. Componentes del subsistema *POLÍTICAS*

El subsistema *POLÍTICAS* está formado por un componente. A continuación se describe dicho componente:

<b>COMP-01</b>	<b>Apps gestión políticas/tareas</b>
<b>Propósito</b>	Este componente se encarga de gestionar de manera gráfica las políticas de grupo y las tareas que se han de aplicar a un aula/cliente.
<b>Origen</b>	RSF-028, RSF-030, RSRe-001, RSRe-002
<b>Procesamiento</b>	<ul style="list-style-type: none"> <li>▪ Asignar política de grupo “equipo” a un aula.</li> <li>▪ Asignar política de grupo “usuario” a un aula.</li> <li>▪ Asignar política de grupo “administrador” a un aula.</li> <li>▪ Asignar política de grupo “equipo” a un cliente.</li> <li>▪ Asignar política de grupo “usuario” a un cliente.</li> <li>▪ Asignar política de grupo “administrador” a un cliente.</li> <li>▪ Asignar tarea a un aula.</li> <li>▪ Asignar tarea a un cliente</li> </ul>
<b>Dependencias</b>	Config clientes
<b>Recursos</b>	Ninguno
<b>Subordinados</b>	Ninguno

Tabla 4.66. COMB-01 Apps gestión políticas/tareas.

### 4.2.2. Especificación del entorno tecnológico

En este apartado se especificará de forma detallada las necesidades tecnológicas del sistema diseñado.

#### 4.2.2.1. Solución hardware clientes

Los clientes que el ldi tiene instalados en las aulas departamentales tienen la siguiente configuración hardware:

- **Fabricante:** Asus y Gigabyte.
- **CPU:** AMD Athlon(tm) 64 X2 Dual Core, 2.2 GHz.
- **RAM:** 4GB DDR2 667Mhz.
- **HDD:** 320GB SATA.

#### 4.2.2.2. *Solución hardware servidores*

Los servidores identificados en los subsistemas expuestos en el punto 4.2. son máquinas virtualizadas mediante el software de virtualización Xen.

Las principales características hardware de dichas máquinas virtuales son:

- **Número de CPU:** 1
- **RAM:** 2GB
- **HDD:** 10GB

Dichas máquinas virtuales se ejecutan sobre máquinas físicas que disponen de un almacenamiento compartido mediante iSCSI con la siguiente configuración hardware:

- **Fabricante:** Supermicro
- **Modelo:** H8DA8 2.0
- **Número de socket CPU:** 2
- **CPU:** Dual-Core AMD Opteron(tm) Processor 2214
- **RAM:** 8GB DDR2 667MHz

A continuación se muestra una imagen del rack en el que están instalados los servidores físicos mencionados en el párrafo anterior.



Figura 4.3. Rack de los servidores físicos perteneciente al ldi.

#### **4.2.2.3. Software a utilizar**

El software necesario para la realización del proyecto se va a desglosar por sistemas operativos y por servicios.

Los sistemas operativos que se van a utilizar son los siguientes:

- **Microsoft Windows 7 Professional:** Este sistema operativo estará destinado a los clientes ubicados en las aulas informáticas.
- **Debian GNU/Linux 6.0 i386:** Este sistema operativo estará destinado a los clientes ubicados en las aulas informáticas.
- **Debian GNU/Linux 6.0 x64:** Este sistema operativo estará destinado a los servidores (físicos y virtuales).
- **Microsoft Windows 2003 Server:** Este sistema operativo estará destinado al servidor que alberga la aplicación que gestiona las políticas y tareas de equipo/aula.

Los servicios que se van a utilizar son los siguientes:

- **Correo:** Para realizar las funciones de servidor de correo se está utilizando actualmente el software Postfix.
- **Web:** Para realizar las tareas de servidor web se está utilizando actualmente el software Apache 2.2.
- **Ldap:** Para realizar las funciones de servidor de autenticación ldap se ha seleccionado el software OpenLDAP.
- **Compartición de datos:** Para realizar la compartición de datos de usuario con los clientes de las aulas informáticas se ha seleccionado el software NFS y SAMBA.

## 4.3. Diseño arquitectónico de la aplicación web

Debido a que la web del ldi ya estaba en producción, y solamente se han modificado algunas funcionalidades de la misma, se va a proceder a describir solamente los diagramas de navegación de las páginas necesarias para que el usuario pueda gestionar su cuenta en el ldi.

### 4.3.1. Diagramas de navegación

En la siguiente figura podemos observar el diagrama de navegación de la página web correspondiente a la apertura de cuentas.

Dicha página constará de dos formularios, uno para poder realizar una cuenta de usuario y otro para poder consultar el estado de la cuenta.

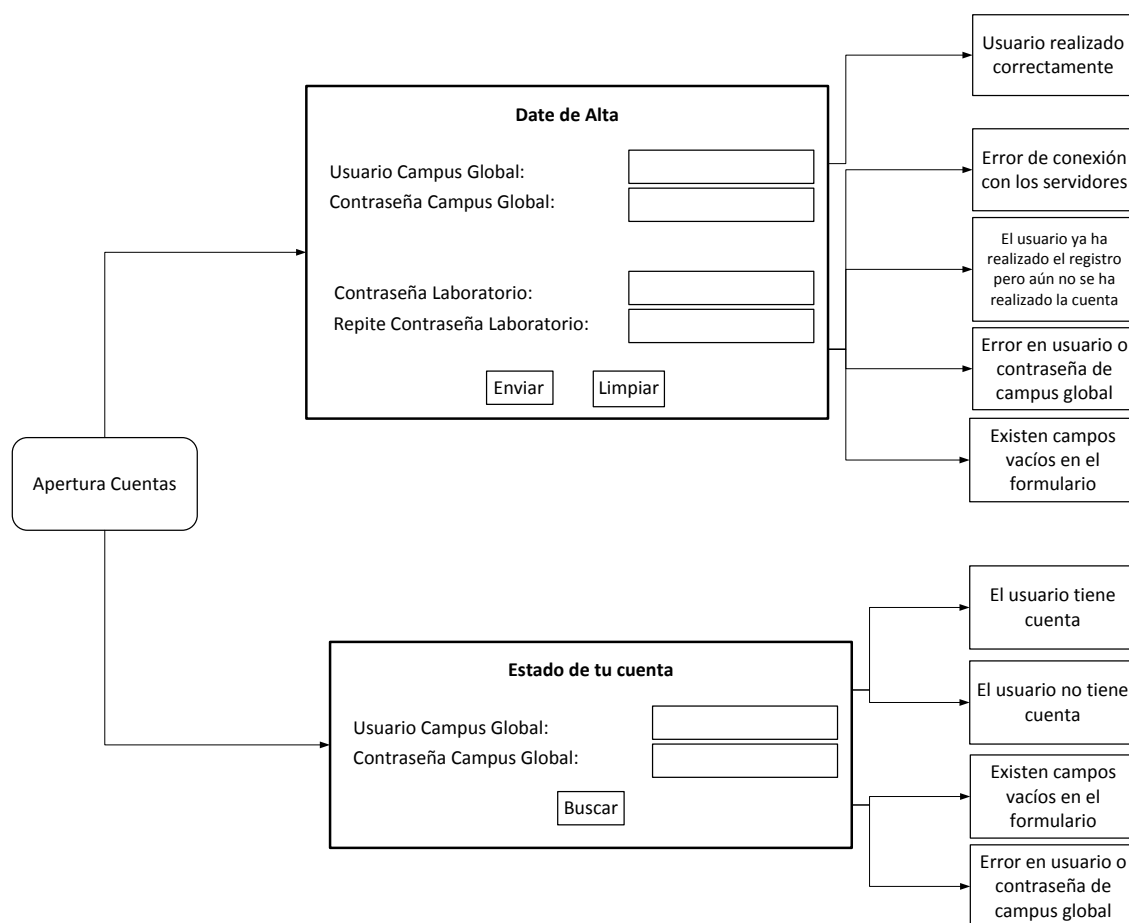


Figura 4.4. Diagrama de navegación de la página "Apertura de Cuentas".

En la siguiente figura podemos observar el diagrama de navegación de la página web correspondiente a la actualización de la cuenta ó cambio de contraseña de la cuenta de usuario.

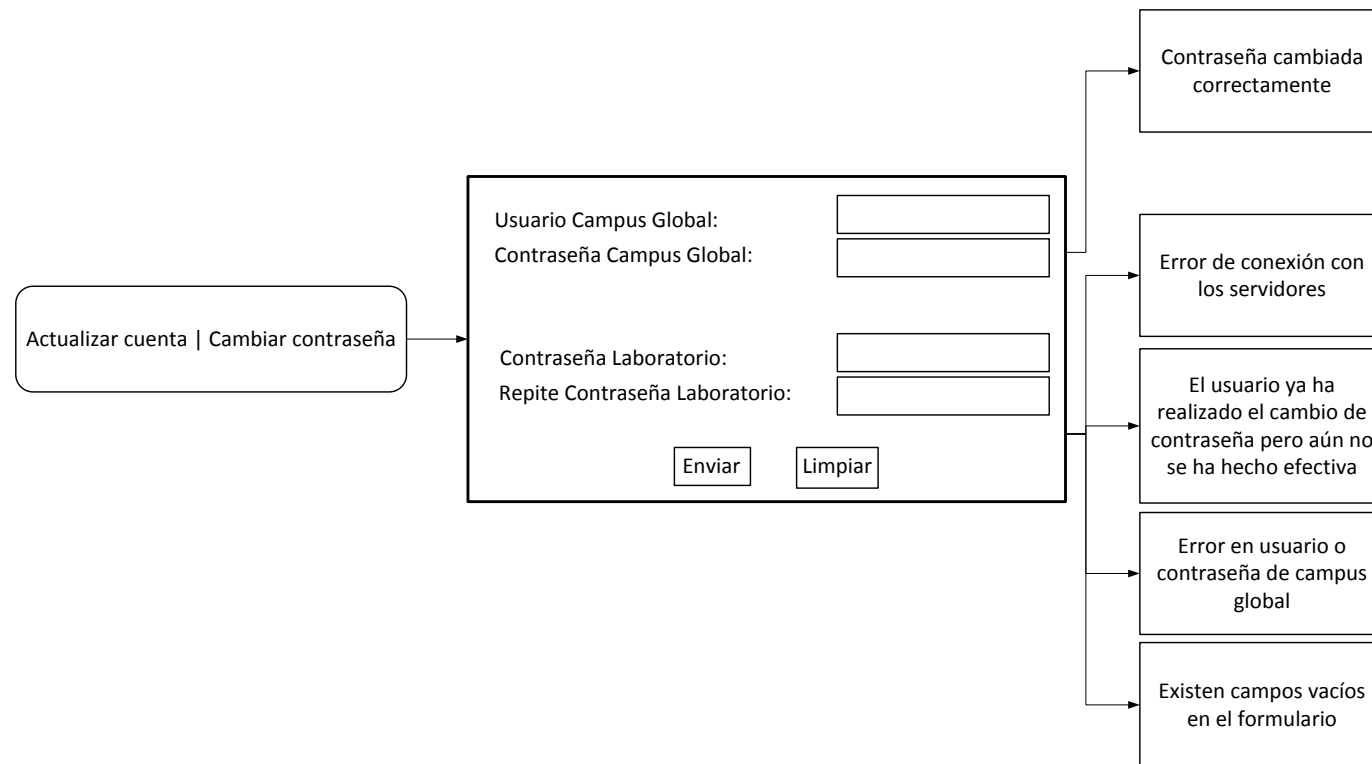


Figura 4.5. Diagrama de navegación de la página “Actualizar cuenta | Cambiar contraseña”.



### 4.4.2. Matriz de trazabilidad entre SR/Comp

	CLIENTE WINDOWS			POLÍTICAS	CORREO	WEB	CLIENTE LINUX	CUENTAS		LDAP					
SR/Comp	COMCW-01	COMCW-02	COMCW-03	COMP-01	COMCo-01	COMW-01	COMCL-01	COMC-01	COMC-02	COML-01	COML-02	COML-03	COML-04	COML-05	COML-06
RSF-001			X				X								X
RSF-002								X							
RSF-003									X						
RSF-004									X						
RSF-005									X						
RSF-006						X									
RSF-007						X									
RSF-008										X					
RSF-009					X										
RSF-010						X				X					
RSF-011															
RSF-012						X									
RSF-013											X				
RSF-014											X				
RSF-015											X				
RSF-016											X				
RSF-017											X				
RSF-018											X				
RSF-019											X				
RSF-020											X				
RSF-021											X				
RSF-022											X				
RSF-023											X				
RSF-024											X				
RSF-025											X				
RSF-026												X			
RSF-027	X														
RSF-028				X											
RSF-029	X														
RSF-030				X											
RSF-031						X				X	X				
RSR-001		X					X								
RSR-002						X									
RSR-003		X					X								

	CLIENTE WINDOWS			POLÍTICAS	CORREO	WEB	CLIENTE LINUX	CUENTAS		LDAP					
SR/Comp	COMCW-01	COMCW-02	COMCW-03	COMP-01	COMCo-01	COMW-01	COMCL-01	COMC-01	COMC-02	COML-01	COML-02	COML-03	COML-04	COML-05	COML-06
RSI-001						X									
RSI-002						X									
RSI-003						X									
RSI-004						X									
RSI-005						X									
RSO-001						X									
RSO-002														X	
RSO-003														X	
RSO-004															X
RSRe-001				X	X	X		X	X	X	X	X	X	X	X
RSRe-002	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
RSC-001															
RSS-001			X				X	X						X	
RSS-002						X									
RSS-003														X	
RSS-004														X	
RSFi-001								X						X	

Tabla 4.68. Matriz de trazabilidad SR/Comp.



# Capítulo 5

## Implantación

En este capítulo se describirá de forma detallada el procedimiento seguido para la instalación, modificación y configuración de los subsistemas que componen la solución propuesta.

Resumiendo, las tareas de implantación realizadas han sido las siguientes:

- Instalación del nuevo servidor ldap.
- Instalación del servidor cuentas.
- Modificaciones al servidor correo.
- Modificaciones al servidor web.
- Configuración de los clientes.
- Actualizador de políticas.
- Tareas programadas.
- Gestor de políticas y tareas (PolGest).
- Tareas finales.

### 5.1. Instalación del servidor LDAP

A continuación se describe el procedimiento seguido para instalar el servidor de autenticación ldap. Como se comentó en el punto 4.2.2. los servicios del ldi se ejecutan en máquinas virtualizadas con el software Xen.

Las tareas realizadas para instalar y configurar el servidor ldap han sido:

- Instalación de la máquina virtual que albergará el servicio de ldap.
- Instalación y configuración del servicio de ldap.
- Instalación del servicio SAMBA (PDC).
- Tareas a realizar después de la instalación.

En primer lugar se explicará detalladamente el procedimiento seguido para realizar la máquina virtual que ejecutará los servicios correspondientes.

### 5.1.1. Instalación de la máquina virtual

El comando a ejecutar para crear la máquina virtual es:

```
# xen-create-image -fs xfs --image sparse \  
--initrd boot/initrd.img-2.6.32-5-xen-amd64 \  
--kernel /boot/vmlinuz-2.6.32-5-xen-amd64 --memory 2048k \  
--size 10240k --swap 1024k --arch i386 --dist squeeze \  
--mirror http://ftp.rediris.es/debian --ip 163.117.142.173 \  
--netmask 255.255.255.0 --gateway 163.117.142.2 \  
--dir /xen-machines --hostname ldap
```

Una vez ejecutado el comando anterior ya tendremos operativa la máquina virtual creada. A continuación se debe realizar una comprobación básica del sistema.

- Se monta el disco duro virtual en un directorio.

```
# mount -o loop disk.img ./montaje
```

- Se comprueba que el nombre de la máquina es el correcto (fichero de configuración en Capítulo 11).

```
# cat ./montaje/etc/hostname
```

- Se comprueba que la configuración de red es la correcta y se añade la tarjeta de red interna que interconecta todos los servidores (fichero de configuración en Capítulo 11).

```
# cat ./montaje/etc/network/interfaces
```

Seguidamente se arrancará la máquina virtual desde la máquina física mediante el siguiente comando (fichero de configuración en Capítulo 11).

```
# umount ./montaje  
# xm create -c /etc/xen/ldap.cfg
```

Una vez arrancada la máquina virtual se realizará la configuración básica del sistema.

- Se instala y configura el servicio ssh (fichero de configuración en Capítulo 11).

```
# apt-get install ssh
```

- Se instala y configura el servicio de correo (fichero de configuración en Capítulo 11).

```
# apt-get install postfix
```

Después de realizar los pasos indicados anteriormente ya se dispone de una máquina totalmente operativa en la que se comenzará a instalar los servicios de autenticación y compartición de ficheros.

### 5.1.2. Instalación del servicio ldap

En este apartado se explicará de forma detallada los pasos para realizar la instalación del servicio ldap.

- Se instala el servidor, librerías y utilidades.

```
# apt-get install slapd libldap-2.4 libdb4.8 ldap-utils
```

- Se procede a borrar el directorio que contiene la configuración ya que deseamos tenerlo en fichero plano en vez de tenerlo integrado en el árbol ldap.

```
# rm -fr /etc/ldap/ldapd.d
```

- Se crea el fichero de texto `/etc/ldap/slapd.conf` (archivo de configuración en Capítulo 11).
- Se genera la contraseña para el administrador (usuario admin) de ldap, la salida del comando se debe copiar en la directiva rootpw del archivo de configuración slapd.conf.

```
# slappasswd -h {SSHA} -s contrasenya  
{SSHA}TKyCVELx7DFN0C3cinwv2eyuFpK3a2+0
```

- Se configura el cliente de ldap para que realice las consultas al propio servidor ldap (fichero de configuración en Capítulo 11).
- Se crea el usuario que tendrá privilegios para realizar las consultas al servidor ldap (fichero en el Capítulo 11).

```
# ldapadd -c -x -D \  
cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es -W -f user.ldif
```

- Se instalan los paquetes necesarios para realizar la autenticación de usuarios con el servidor ldap (ficheros de configuración en Capítulo 11).

```
# apt-get install libpam-ldap libnss-ldap nscd
```

- Se deshabilita la cache de las consultas y contraseñas relativas a las autenticaciones de usuarios (fichero de configuración en Capítulo 11).
- Se modifica el fichero de configuración que contiene la prioridad de búsqueda en las bases de datos de autenticación del sistema para añadir el servidor ldap (fichero de configuración en Capítulo 11).
- Se modifica la configuración del demonio syslog para que almacene los registros del servidor ldap en el fichero */var/log/slapd.conf* (fichero de configuración en Capítulo 11).
- Se configura la rotación del fichero de log del servidor ldap (fichero de configuración en Capítulo 11).
- Se instala las herramientas necesarias para crear el certificado del servidor.

```
# apt-get install openssl
```

- Se procede a generar el certificado del servidor (Importante: Al generar el certificado del servidor rellenar el campo *cn* (*common name*) con el nombre del equipo con el dominio (FQDN)).

```
# mkdir /etc/ldap/ssl  
# cd /etc/ldap/ssl  
# /usr/lib/ssl/misc/CA.sh -newca  
# openssl req -new -nodes -keyout newreq.pem -out  
newreq.pem  
# /usr/lib/ssl/misc/CA.sh -sign  
# cp demoCA/cacert.pem .  
# mv newcert.pem servercrt.pem  
# mv newreq.pem serverkey.pem  
# chmod 640 serverkey.pem  
# chown root:openldap serverkey.pem
```

- Se modifica el fichero */etc/default/slapd* para habilitar la autenticación segura (fichero de configuración en Capítulo 11).
- Se generan los índices de búsqueda del servidor ldap.

```
# /etc/init.d/slaped stop
# slapindex
# chown -R openldap:openldap /var/lib/ldap
# /etc/init.d/slaped start
```

### 5.1.3. Instalación del servicio Samba

En este apartado se explicará de forma detallada los pasos para realizar la instalación del servicio Samba. Este servicio permitirá autenticar los clientes Windows con el servicio ldap y será el servidor PDC (*Primary Domain Master*) de la red Windows.

- Se comienza instalando los paquetes y utilidades relacionados con el servicio (archivo de configuración en Capítulo 11).

```
# apt-get install samba smbclient smbldap-tools
```

- Se introducen las credenciales del usuario admin correspondiente al servicio ldap.

```
# smbldappasswd -w 'contraseña'
```

- Se obtiene el identificador del dominio Windows creado mediante el siguiente comando.

```
# net getlocalsid
```

- Con el resultado obtenido de la ejecución del comando anterior, se procede a modificar el paquete smbldap-tools (fichero de configuración en el Capítulo 11).
- A continuación se configuran las credenciales del usuario admin para las herramientas smbldap-tools modificando el fichero `/etc/smbldap-tools/smbldap_bind.conf` (fichero de configuración en Capítulo 11).
- Seguidamente se creará la estructura necesaria de grupos y usuarios necesarios en el árbol ldap para que los clientes Windows funcionen correctamente.

```
# smbldap-populate
```

- Por último se definirá la contraseña del usuario administrador del dominio.

```
# smbldap-passwd root
```

#### 5.1.4. Tareas posteriores a la instalación

Una vez realizada la instalación del servicio ldap y el servicio Samba se procederá a crear los grupos de usuarios ejecutando los siguientes comandos.

```
# smbldap-groupadd -g 210 alumnos
# smbldap-groupadd -g 220 profes
# smbldap-groupadd -g 230 bdua
# smbldap-groupadd -g 240 asignaturas
# smbldap-groupadd -g 4 adm
```

El paquete smbldap-tools contiene un *script* que permite cambiar la contraseña de los usuarios de forma interactiva (*smbldap-passwd*), pero para los *scripts* automáticos se necesita que la nueva contraseña pueda ser introducida como línea de comandos. Realizando unas modificaciones<sup>[37]</sup> al fichero original se consigue el objetivo deseado, el nuevo fichero se llamará *smbldap-passwd-script* y el fichero original se renombrará como *smbldap-passwd-orig*. Por último se creará un enlace blando con el nombre *smbldap-passwd* que apunte al *script* deseado en ese momento.

## 5.2. Instalación del servidor CUENTAS

A continuación se describe el procedimiento seguido para instalar el servidor cuentas.

Las tareas realizadas para instalar el servidor cuentas han sido:

- Instalación de la máquina virtual cuentas.
- Configuración del cliente ldap.
- Instalación del servicio SAMBA (BDC).
- Ajustes de cuotas de usuario.

### 5.2.1. Instalación de la máquina virtual

El procedimiento para la instalación de la máquina virtual es exactamente el mismo que el descrito en apartado 5.1.1. Solamente cambian los siguientes comandos.

- Comando para crear la máquina virtual.

```
# xen-create-image -fs xfs --image sparse \  
--initrd boot/initrd.img-2.6.32-5-xen-amd64 \  
--kernel /boot/vmlinuz-2.6.32-5-xen-amd64 --memory 2048k \  
--size 10240k --swap 1024k --arch i386 --dist squeeze \  
--mirror http://ftp.rediris.es/debian --ip 163.117.142.230 \  
--netmask 255.255.255.0 --gateway 163.117.142.2 \  
--dir /xen-machines --hostname cuentas
```

- Comando para iniciar la máquina virtual.

```
# xm create -c /etc/xen/cuentas.cfg
```

### 5.2.2. Configuración del cliente ldap

Los pasos necesarios para configurar el cliente ldap son los siguientes.

- Se modifica el fichero de configuración que contiene la dirección del servidor ldap al que realizará las consultas (fichero de configuración en Capítulo 11).

- Se instala los paquetes necesarios para realizar la autenticación de usuarios con el servidor ldap (ficheros de configuración en Capítulo 11).

```
# apt-get install libpam-ldap libnss-ldap nscd
```

- Se modifica el fichero de configuración que contiene la prioridad de búsqueda en las bases de datos de autenticación del sistema para añadir el servidor ldap (fichero de configuración en Capítulo 11).
- Se configura el demonio de cache para que no guarde ningún registro (fichero de configuración en Capítulo 11).
- Se reinicia el servicio de cache de consultas.

```
# /etc/init.d/nscd restart
```

### 5.2.3. Instalación del servicio Samba

El procedimiento a seguir para configurar el servicio Samba es el mismo al seguido en el apartado 5.1.3. pero hay que tener en cuenta que el fichero de configuración `/etc/samba/smb.conf` (se puede consultar en el Capítulo 11) es distinto ya que el rol de este servidor es BDC (*Backup Domain Controller*). Tampoco se han de ejecutar los dos últimos comandos debido a que solamente se han de ejecutar una vez.

Este servidor también autenticará usuarios procedentes de los clientes Windows pero solamente es un apoyo al servidor controlador de dominio (BDC). Además de que el rol es distinto, este servidor se encargará de exportar la cuenta de usuario a los clientes Windows.

### 5.2.4. Ajuste de cuotas de usuario

Debido a la creciente necesidad de espacio provocada por la utilización de la misma cuenta de usuario para ambos sistemas operativos se ha decidido aumentar la cuota de usuario a todas las cuentas de alumno que tiene el ldi. Para realizar dicho cambio se ha realizado un *script* (se puede consultar en el Capítulo 11) que obtiene todas las cuentas de usuario activas y ejecuta el siguiente comando:

```
# /usr/sbin/xfs_quota -xc "limit bsoft=300M bhard=350M $user" /users
```



## 5.3. Modificaciones realizadas en el servidor CORREO

A continuación se describen los pasos realizados para adaptar el servidor de correo al nuevo sistema de autenticación.

- Configuración del cliente ldap para realizar las autenticaciones. El procedimiento es el explicado en el punto 5.5.1.
- Configuración del servicio imap para que sea capaz de autenticar a través de ldap. Se debe modificar el fichero */etc/dovecot/dovecot-ldap.conf* (se puede consultar en el Capítulo 11).

## 5.4. Modificaciones realizadas en el servidor WEB

A continuación se describen los pasos realizados en la página web del ldi para poner en funcionamiento el nuevo sistema de gestión de cuentas de usuario. La página web del ldi es un gestor de contenido llamado Drupal, lo que ha permitido realizar las modificaciones de forma rápida.

Las tareas realizadas para adaptar el servidor web al nuevo sistema de autenticación han sido:

- Creación de las nuevas páginas web.
- Instalación de software adicional y configuración.
- Instalación de una interfaz de administración de ldap: Ldap Account Manager.

### 5.4.1. Creación de las nuevas páginas web

El procedimiento seguido para crear las páginas web ha sido el siguiente:

- Se inicia sesión en la página de administrador del sitio web.

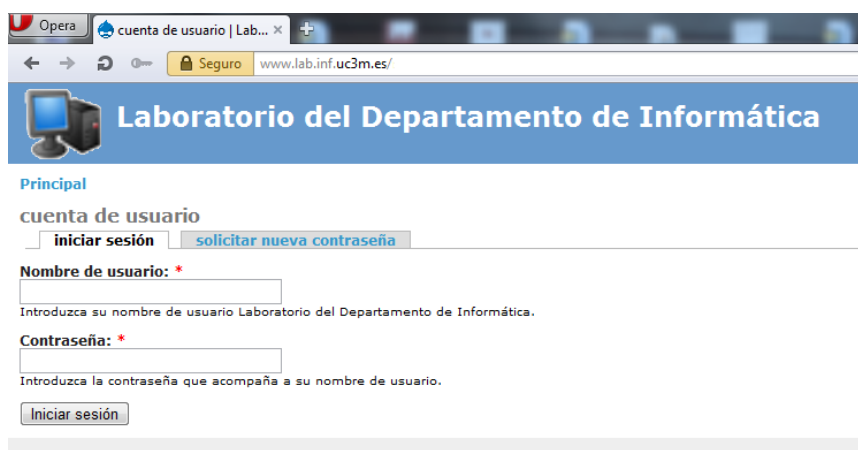


Figura 5.1. Página inicio de sesión de la administración de la página web.

- Seguidamente se despliega la pestaña “crear contenido nuevo” y se selecciona “página”. A continuación se rellenará el contenido necesario para realizar las páginas web.

Opera Enviar página | Laborat... x +

Seguro www.lab.inf.uc3m.es/node/add/page

**Laboratorio del Departamento de Informática**

**Administrador**

- crear contenido nuevo
- aplicación
- aula
- información
- miembro
- noticia
- pregunta frecuente
- página**
- reserva
- servicio
- mi cuenta
- administrar
- cerrar sesión

Principal • crear contenido nuevo

### Enviar página

Título: \*

Categorías:

Soporte usuarios:

- <ninguno>
- Contactar
- Mapa Web
- Noticias
- ¿Quiénes somos?

Servicios:

- <ninguno>
- Apertura de Cuentas
- Abrir nueva cuenta
- Cambio de Contraseña
- Estado de tu cuenta
- Cliente SSH
- Cliente SSH on-line
- Cluster
- Módin

Información:

- <ninguno>
- Equipación Aulas
- Software Linux
- Software Windows
- Horario Aulas
- Información General
- Ocupación Aulas
- Ocupación Actual
- Jueves

Cuerpo: \*

Formato de entrada

Mensaje de registro:

Una explicación de las ediciones o actualizaciones que se han hecho para ayudar a que otros autores entiendan sus motivaciones.

- Opciones de comentarios
- Opciones del menú
- Opciones de ruta URL
- Información de autoría
- Opciones de publicación

Vista previa Enviar

Figura 5.2. Página de creación de contenido.

A continuación se detalla las páginas creadas y su contenido:

- **Actualizar Cuenta | Cambiar contraseña:** Esta página web contiene un formulario para que los usuarios puedan cambiar la contraseña de su cuenta.
- **Apertura de cuentas:** Esta página web contiene dos formularios. Uno para que los usuarios puedan crear su cuenta en el ldi y otro para consultar el estado de la cuenta.
- **Estado de tu cuenta:** Código php necesario para realizar la consulta del estado de la cuenta de usuario. El código se puede consultar en el Capítulo 11.
- **Abrir nueva cuenta:** Código php necesario para realizar la apertura de la nueva cuenta. El código se puede consultar en el Capítulo 11.

#### 5.4.2. Instalación de software y activación de módulos

Para que el servidor web funcione correctamente con el nuevo sistema de autenticación hay que realizar las siguientes modificaciones al sistema.

- Instalación de los siguientes paquetes mediante la ejecución del siguiente comando:

```
# apt-get install libapache2-mod-ldap-userdir php5-mcrypt
```

- Activación de los módulos de apache relacionados con ldap mediante la ejecución de los siguientes comandos:

```
# a2enmod ldap  
# a2enmod ldap_userdir
```

- Configuración del módulo ldap\_userdir añadiendo las siguientes líneas al fichero de configuración /etc/apache2/apache2.conf:

```
LDAPUserDir public_html  
LDAPUserDirDNInfo  
uid=---,dc=lab,dc=inf,dc=uc3m,dc=es PASSWORD  
LDAPUserDirBaseDN ou=People,dc=lab,dc=inf,dc=uc3m,dc=es
```

### 5.4.3. Instalación de Ldap Account Manager

El software “Ldap Account Manager”, en adelante LAM, es una interfaz web que nos permite gestionar de manera gráfica e intuitiva el árbol ldap que contiene toda la información relativa a los usuarios y equipos del ldi.

El paquete disponible en la versión del sistema operativo del servidor (Debian GNU/Linux 6.0) es una versión antigua por lo que se opta por usar la última versión ofrecida por el desarrollador de la herramienta.

Los pasos realizados para la instalación de la herramienta han sido los siguientes:

- Se descarga el paquete LAM 3.4.0 desde <http://www.ldap-account-manager.org/>.
- Se descomprime el fichero en `/var/www/apps.lab.inf.uc3m.es/lam`
- Se procede a configurar la herramienta a través de la interfaz web. La contraseña por defecto es lam. Las pantallas de configuración se muestran a continuación.

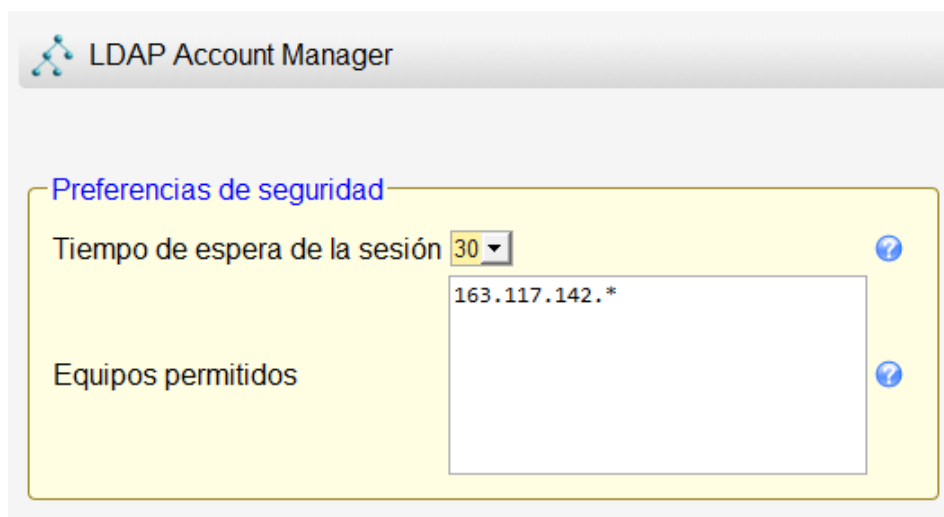


Figura 5.3. Configuración general de la herramienta LAM.

The screenshot displays the 'LDAP Account Manager' configuration window, specifically the 'Configuración general' (General Configuration) tab. The interface is divided into several sections:

- Preferencias del servidor (Server Preferences):**
  - Dirección del servidor: ldap://ldap:389
  - Activar TLS: No
  - Sufijo del árbol: dc=lab,dc=inf,dc=uc3m,dc=es
  - LDAP search limit: -
- Configuración de idioma (Language Configuration):**
  - Idioma por defecto: Español (España)
- Lamdaemon settings:**
  - Lista de servidores: (empty field)
  - Path a script externo: (empty field)
  - Permisos para el directorio principal:
 

	Propietario	Lectura	Escribir	Ejecutar
Grupos	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Otro	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
- Preferencias de seguridad (Security Preferences):**
  - Metodoinicio de sesión: Lista fijada
  - Lista de usuarios validos: cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es
  - Nueva contraseña: (empty field)
  - Vuelva a introducir la contraseña: (empty field)

At the bottom, there are 'Guardar' (Save) and 'Cancelar' (Cancel) buttons.

---

The second screenshot shows the 'Tipos de cuenta' (Account Types) tab in the LDAP Account Manager. It displays the configuration for various account types:

- Habilitar tipos de cuenta (Enable account types):**
  - Alias de email: Alias de correo (e.g. Alias de correo NIS) ☒
  - Asterisk extensions: Asterisk extensions entries ☒
  - DHCP: Administración DHCP ☒
  - NIS grupos de red: NIS entradas de grupo de red ☒
- Tipos de atributos (Account types):**
  - Usuarios (Users):** Cuentas de usuario (e.g. UNIX, Samba y Kolab)
    - Sufijo LDAP: ou=People,dc=lab,dc=inf,dc=uc3m,dc=es
    - Mostrar atributos: #uid; #givenName; #sn; #uidNumber; #gidNumber
    - Eliminar este tipo de cuenta: (button)
  - Grupos (Groups):** Las cuentas de grupo (e.g. Unix y Samba)
    - Sufijo LDAP: ou=Groups,dc=lab,dc=inf,dc=uc3m,dc=es
    - Mostrar atributos: #cn; #gidNumber; #memberUID; #description
    - Eliminar este tipo de cuenta: (button)
  - Hosts:** Cuentas de hosts (e.g. Samba)
    - Sufijo LDAP: ou=Machines,dc=lab,dc=inf,dc=uc3m,dc=es
    - Mostrar atributos: #cn; #description; #uidNumber; #gidNumber
    - Eliminar este tipo de cuenta: (button)
  - Dominios de Samba:** Entradas de al dominio de Samba 3
    - Sufijo LDAP: dc=lab,dc=inf,dc=uc3m,dc=es
    - Mostrar atributos: sambaDomainName:Domain name;sambaS: (truncated)
    - Eliminar este tipo de cuenta: (button)

Figura 5.4. Configuración relativa al Perfil del servidor.

## 5.5. Configuración de los clientes

A continuación se describen los pasos realizados para realizar la configuración a los clientes para que autenticuen con el servidor ldap.

Las tareas realizadas para adaptar los clientes al nuevo sistema de autenticación han sido los siguientes:

- Configuración del cliente Linux.
- Configuración del cliente Windows.

### 5.5.1. Cliente Linux

Aunque todos los servidores (incluido el propio ldap) también son clientes del servidor ldap, se ha decidido incluir este apartado debido a que los clientes de las aulas (a diferencia de los servidores que tienen una red interna) poseen una configuración distinta porque necesitan cifrar las comunicaciones con el servidor.

Los pasos necesarios para configurar el cliente Linux con el nuevo servicio de autenticación basado en ldap son los siguientes.

- Se modifica el fichero de configuración que contiene la dirección del servidor ldap al que realizará las consultas (fichero de configuración en Capítulo 11).
- Se instala los paquetes necesarios para realizar la autenticación de usuarios con el servidor ldap (ficheros de configuración en Capítulo 11).

```
# apt-get install libpam-ldap libnss-ldap nscd
```

- Se modifica el fichero de configuración que contiene la prioridad de búsqueda en las bases de datos de autenticación del sistema para añadir el servidor ldap (fichero de configuración en Capítulo 11).
- Se copia el certificado de la autoridad de certificación almacenado en `/etc/ldap/ssl/cacert.pem` ubicado en el servidor ldap al directorio `/etc/ldap/ssl`
- Se reinicia el servicio de cache de consultas.

```
# /etc/init.d/nscd restart
```

### 5.5.2. Cliente Windows

A continuación se describen los pasos necesarios para añadir un cliente Windows al dominio. Debido a que los clientes Windows no van a trabajar con un servidor *Active Directory* se han de realizar modificaciones en el registro para compatibilizar ambas tecnologías.

- Ejecutar *script* para realizar las modificaciones necesarias en el registro para compatibilizar el cliente con el dominio SAMBA (*script* en el punto Capítulo 11).
- Se abre el cuadro de diálogo de propiedades del sistema abriendo Equipo→propiedades→”Cambiar configuración”.

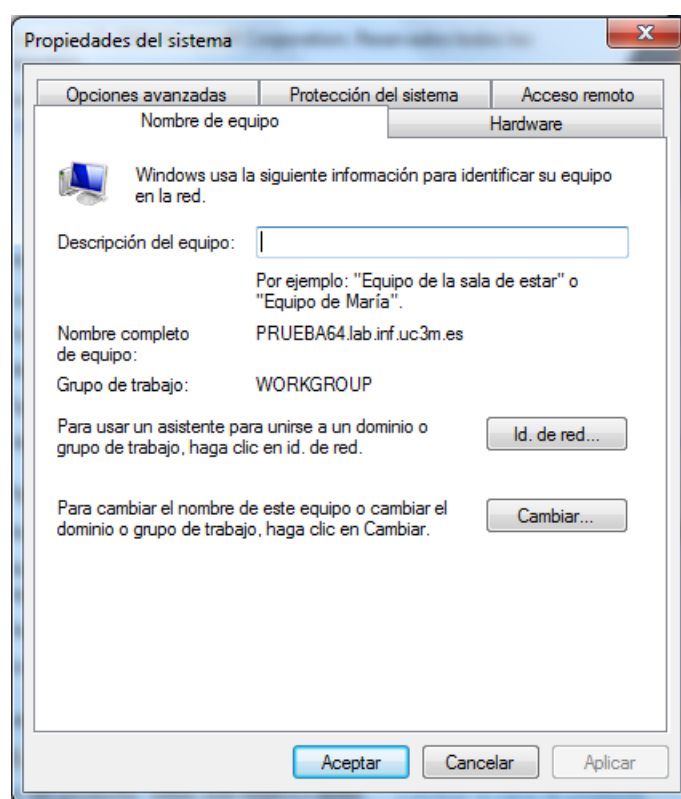


Figura 5.5. Cuadro de diálogo de propiedades del sistema.

- Seguidamente se selecciona el botón “Cambiar” para abrir el cuadro de diálogo “Cambios en el dominio o el nombre del equipo”.



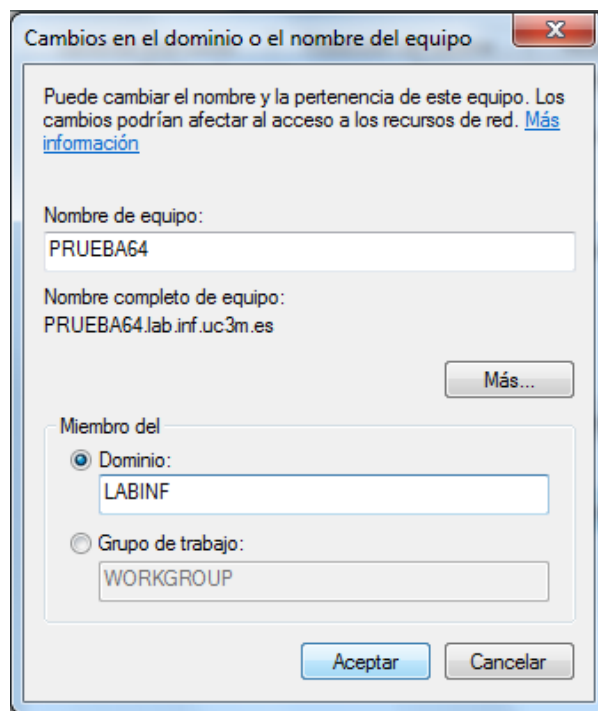


Figura 5.6. Cuadro de diálogo “Cambios en el dominio o el nombre del equipo”.

- A continuación se introducirá el nombre del dominio, en este caso LABINF.
- Aparecerá un cuadro de diálogo en el que se introducirán las credenciales de administrador del dominio.

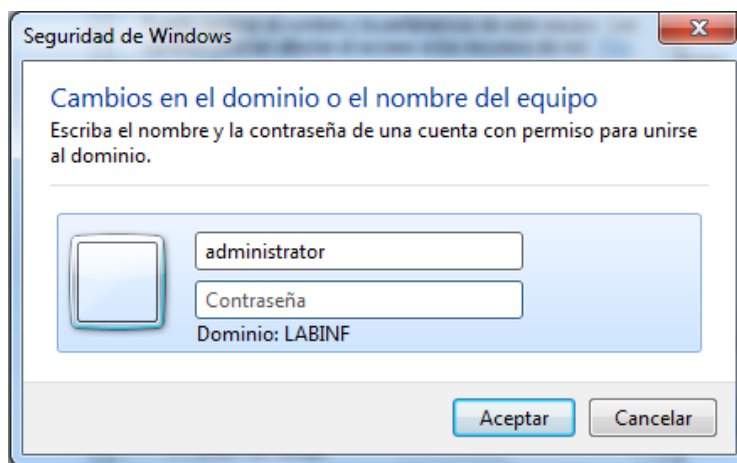


Figura 5.7. Cuadro de solicitud de credenciales.

- Si las credenciales son correctas aparecerá un mensaje informando de que el equipo se ha añadido al dominio correctamente.

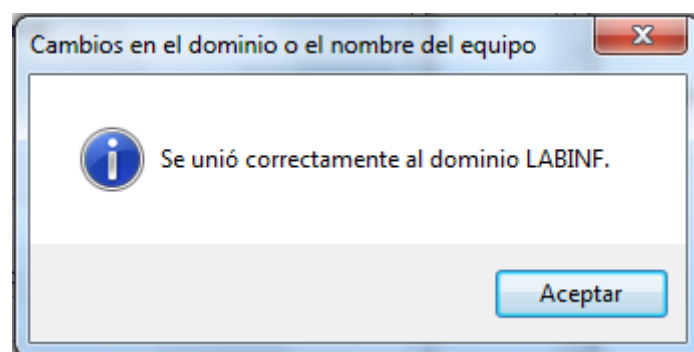


Figura 5.8. Mensaje de confirmación de unión al dominio.

- Después de reiniciar el equipo comprobaremos que se han realizado correctamente los cambios en Equipo→propiedades.

**Sistema**

Evaluación:	La evaluación del sistema no está disponible
Procesador:	AMD Athlon(tm) 64 X2 Dual Core Processor 5200+ 2.70 GHz
Memoria instalada (RAM):	4,00 GB (3,44 GB utilizable)
Tipo de sistema:	Sistema operativo de 32 bits
Lápiz y entrada táctil:	La entrada táctil o manuscrita no está disponible para esta pantalla

**Configuración de nombre, dominio y grupo de trabajo del equipo**

Nombre de equipo:	PRUEBA64	Cambiar configuración
Nombre completo de equipo:	PRUEBA64.lab.inf.uc3m.es	
Descripción del equipo:		
Grupo de trabajo:	LABINF	

Figura 5.9. Ventana de propiedades del sistema.

- Se debe configurar la política de grupo local copiando el contenido de `\\ldap\\sysvol\\policies\\almacen\\computer\\base` en `C:\\Windows\\System32\\GroupPolicy`.
- Para finalizar se aplican los cambios ejecutando `gpupdate /force` desde una consola de comandos. Al reiniciar el equipo se sincronizarán las políticas que le corresponde y se las aplicará al sistema.

## 5.6. Actualizador de políticas

El actualizador de políticas es un conjunto de ficheros y *scripts* que permite a los administradores gestionar las políticas de grupo, de manera centralizada, que se deben aplicar a un equipo o aula concreta.

### 5.6.1. Scripts y ficheros implicados

Para que el sistema funcione correctamente se necesitan *scripts* tanto en el lado del cliente como en el servidor.

A continuación se detallan los *scripts* implicados en el proceso de actualización.

#### 5.6.1.1. Cliente

Los *scripts* ubicados en el cliente y que intervienen en el proceso son los siguientes:

- **C:\scripts\actualizador-scripts.ps1** (contenido en Capítulo 11): Este *script* se encarga de actualizar los *scripts* de encendido y apagado del equipo.
- **C:\scripts\security-template.inf** (contenido en Capítulo 11): Este fichero contiene las configuraciones relativas a la seguridad local de equipo.
- **C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\gpupdate.ps1** (contenido en Capítulo 11): Este *script* se ejecuta siempre que se arranca el equipo.

Su funcionalidad es la siguiente:

- Crea el archivo de log si no existe.
- Crea los directorios que albergan las políticas de usuario y usuario administrador si no existen.
- Realiza la actualización por aula y por equipo.
- Realiza la actualización de tareas programadas por aula y por equipo.
- Aplica la plantilla de seguridad al equipo.
- Actualiza los *scripts* ubicados en *c:\scripts*.
- Lanza la ejecución del *script* *C:\scripts\actualizador-scripts.ps1* para que

actualice los *scripts* de arranque y apagado del equipo.

- **C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown\update-equip.bat (contenido en Capítulo 11):** Este *script* se ejecuta cuando se apaga el equipo y fuerza la actualización de la política del equipo local.

### 5.6.1.2. Servidor

Los servidores tienen varios repositorios de *scripts*. A continuación se detalla la utilidad de cada uno de ellos.

- **\\ldap\netlogon y \\cuentas\netlogon:** Estas ubicaciones contienen los *scripts* y ficheros que se ejecutan cuando un usuario inicia sesión en un equipo.
- **\\ldap\sysvol\scripts:** Esta ubicación contiene los ficheros y *scripts* que se desea que estén presentes en la carpeta C:\scripts de los clientes.
- **\\ldap\sysvol\policies\scripts:** Esta ubicación contiene los *scripts* que se ejecutarán cuando se arranca y apaga un equipo.

## 5.6.2. Proceso de actualización

El proceso que se sigue desde que se arranca el equipo es el siguiente:

- En el proceso de arranque se ejecuta el *script gpupdate.ps1*.
- Se procede a realizar la actualización del equipo por aula si se dispone de políticas.
- Se procede a realizar la actualización del equipo por equipo si se dispone de políticas.
- Se aplica la plantilla de seguridad al equipo.
- Se actualizan los *scripts* ubicados en C:\scripts.
- Se lanza la actualización de los *scripts* de inicio (C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup) y apagado (C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown) del equipo.

### 5.6.2.1. Explicación de los logs

Durante el proceso de actualización, la aplicación registra el resultado de las operaciones realizadas, a continuación se muestra una imagen de los registros de log.

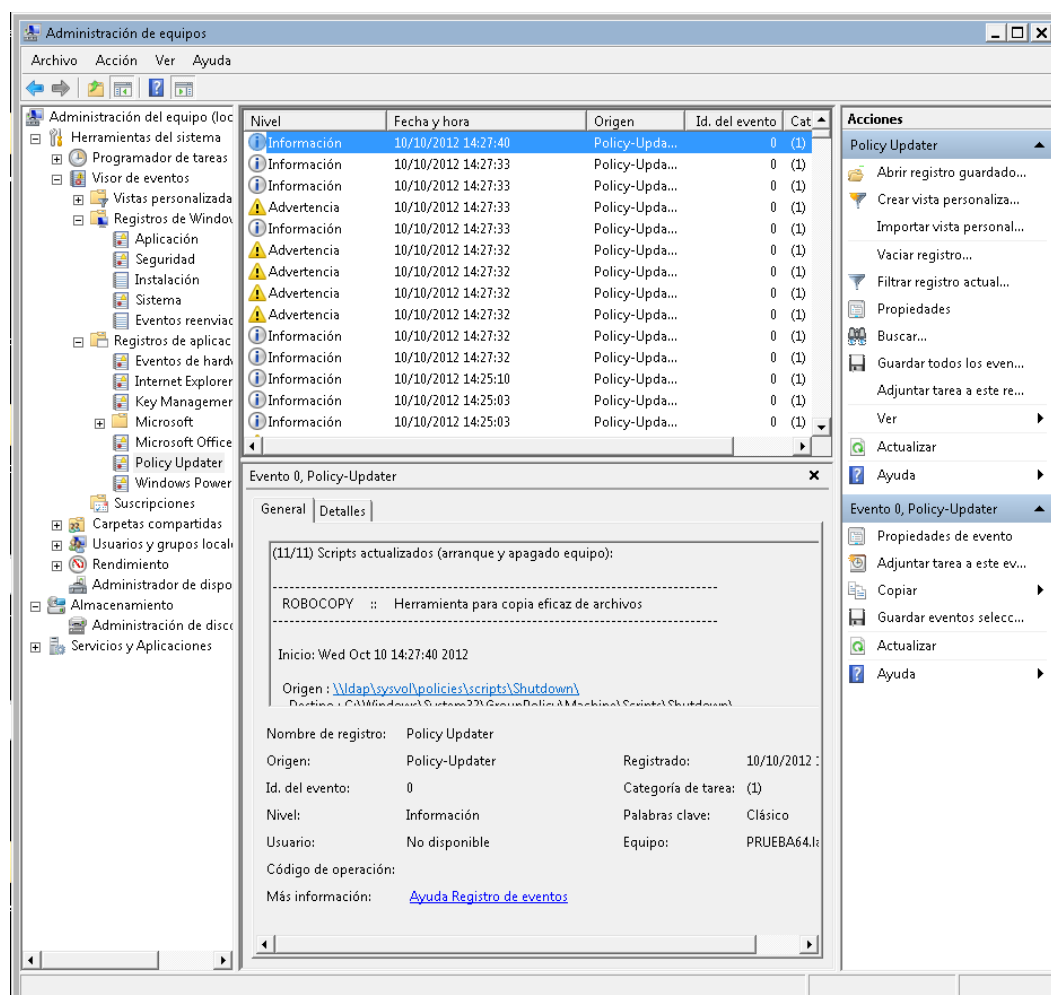


Figura 5.10. Vista del log que registra el actualizador de políticas.

Un ciclo completo de actualización está compuesto por 11 operaciones, en la esquina izquierda de cada registro de log se indica el número de operación realizada. En la siguiente figura se puede observar que la actualización de los *scripts* de arranque y apagado del equipo es la última operación a realizar.

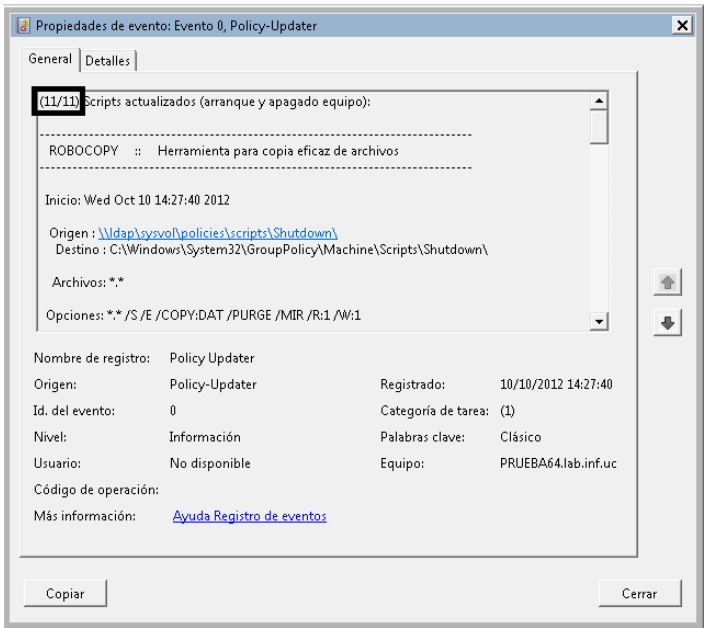


Figura 5.11. Detalle de un evento del registro de log.

Los tipos de eventos que se registran pueden ser de información o de advertencia. Los eventos de tipo información registran la salida de la operación realizada. A continuación se puede ver el detalle de un evento de tipo información.



Figura 5.12. Detalle de evento tipo información.

Los eventos de tipo advertencia se producen porque la política de grupo para el equipo/aula no existe o porque se ha producido un error. Las comprobaciones que se deben realizar para depurar el error son las siguientes:

- Comprobar que el equipo esté agregado al *script* gpupdate.ps1.
- Comprobar que el enlace del contenedor de la política correspondiente existe.
- Comprobar que la ruta del enlace es correcta (se produce un error en la ruta si se crea el enlace con la unidad montada).

### 5.6.3. Creación de las políticas de grupo

Todos los clientes Windows parten de una política de grupo que contiene solamente las directivas necesarias para que los *scripts* realicen la actualización correspondiente en el siguiente reinicio del equipo.

A continuación se describe el proceso seguido para crear la política de grupo perteneciente al equipo y a los usuarios, tanto administradores como no administradores.

#### 5.6.3.1. Creación de la política base (computer)

El proceso a seguir para realizar la política base es descrito a continuación:

- Se abre el editor de directivas de grupo local ejecutando *gpedit.msc* desde la línea de comandos.
- Se despliega la sección “Configuración del equipo→Scripts (Inicio o Apagado).

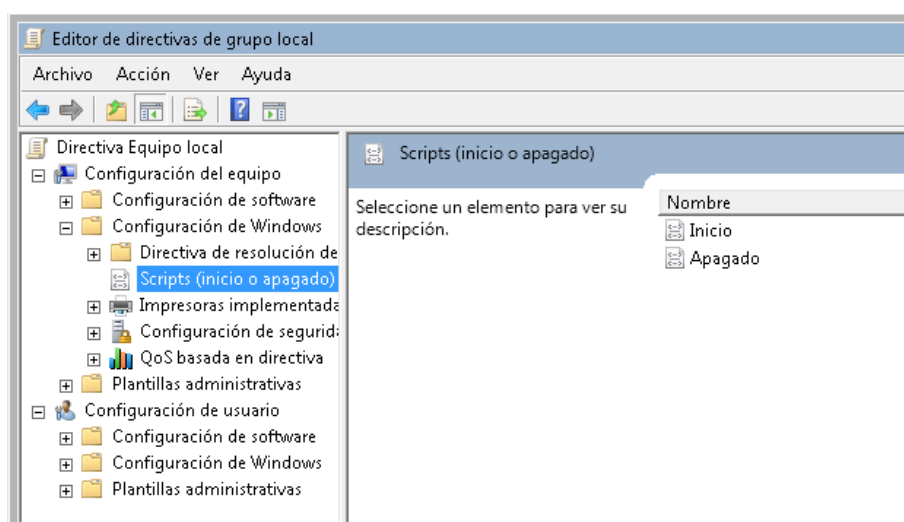


Figura 5.13. Editor de directivas de grupo local.

- En el *script* de Inicio se configura el *script* gpupdate.ps1, dicho *script* se obtendrá de la ubicación `\\ldap\sysvol\policies\scripts\Startup` y se copiará en `C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup`.
- En el *script* de Apagado se configura el *script* update-equipo.bat, dicho *script* se obtendrá de la ubicación de `\\ldap\sysvol\policies\scripts\Shutdown` y se copiará en `C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown`.
- Para finalizar el proceso se cierra el editor y se guarda en el almacén de políticas correspondientes al equipo (`\\ldap\sysvol\policies\almacen\computer`) el directorio local `C:\Windows\System32\GroupPolicy`.

#### 5.6.3.2. Creación de la política relativa a los usuarios (*user* & *useradm*)

El procedimiento para crear nuevas políticas de usuario no administrador y administrador es el siguiente:

- Se abre la consola de administración de Microsoft ejecutando el comando mmc en la línea de comandos.
- Se abre la ventana de complementos en la opción Archivo→Agregar o eliminar complemento.
- Se selecciona el complemento “Editor de objetos de directiva de grupo” finalizando la acción pulsando el botón “Agregar”.
- A continuación aparecerá una ventana que nos permitirá seleccionar un objeto de directiva de grupo. En este caso se selecciona la pestaña “Usuarios” y posteriormente “No administradores”, se confirmará la acción pulsando en el botón “Aceptar”. En la siguiente figura se puede ver la lista de usuarios y grupos disponibles.



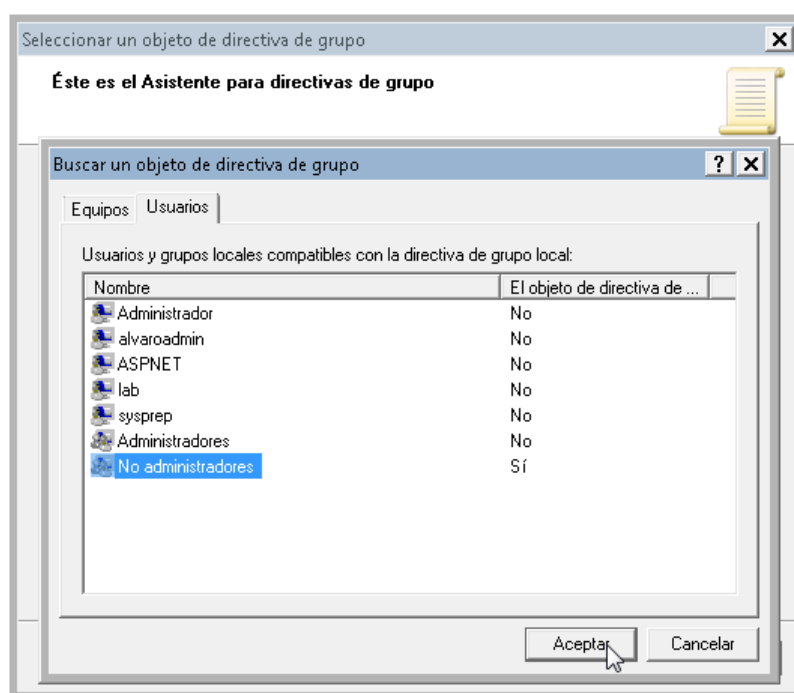


Figura 5.14. Cuadro de diálogo de búsqueda de objeto de directiva de grupo.

- Para finalizar se editará las directivas requeridas y se repetirá el proceso para los usuarios administradores si fuera necesario.
- Para finalizar el proceso se cierra el editor y se guarda en el almacén correspondiente (`\\ldap\\sysvol\\policies\\almacen\\user` para el usuario no administrador y `\\ldap\\sysvol\\policies\\almacen\\useradm` para usuario administrador) el directorio local correspondiente (`C:\\Windows\\System32\\GroupPolicyUsers\\S-1-5-32-545` para usuarios no administradores y `C:\\Windows\\System32\\GroupPolicyUsers\\S-1-5-32-544` para usuarios administradores)

## 5.7. Tareas Programadas

Las tareas programadas son una lista de acciones que el sistema operativo Windows debe de realizar en un momento dado. El periodo en el que el SO realiza cada una de las acciones que tenga asignadas puede variar entre:

- Diariamente
- Semanalmente
- Mensualmente
- Sólo una vez
- Al iniciar el equipo (antes de que un usuario inicie sesión)
- Al iniciar la sesión (sólo después de que el usuario actual inicie sesión)

En el entorno del ldi las tareas programadas se utilizan principalmente para apagar de forma fiable los equipos por la noche. Esto es debido a que en ocasiones los equipos no se apagan debido a que les quitan el cable de red y hace imposible el apagado remoto.

A continuación se describe brevemente los pasos que hay que realizar para crear y configurar para su instalación una tarea programada.

- Abrir el programador de tareas ejecutando el comando *Taskschd.msc* en una ventana de ejecución de comandos. Aparecerá una ventana como la de la siguiente figura.

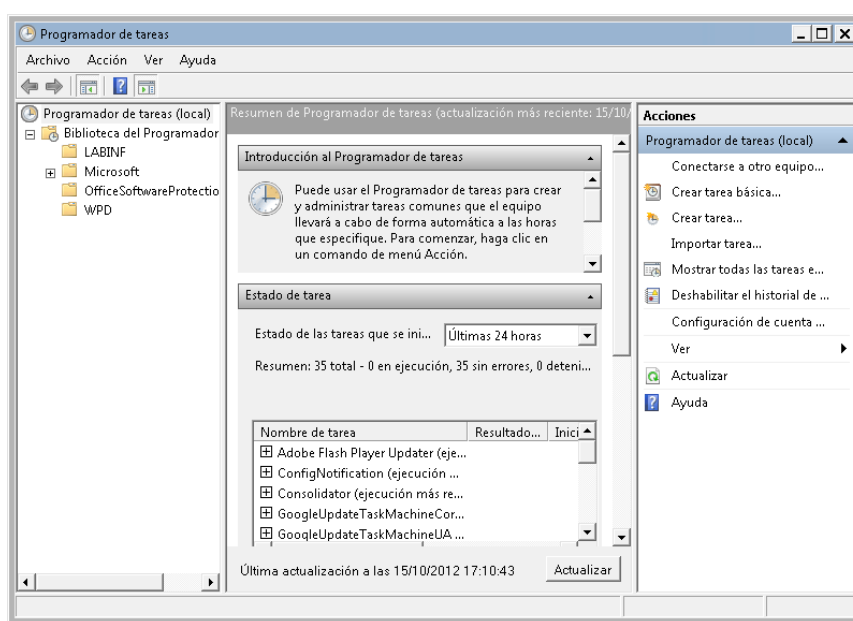


Figura 5.15. Ventana principal del Programador de tareas.

- Comenzar a crear la tarea seleccionando el enlace del menú de la derecha “Crear tarea”. Aparecerá una ventana como la de la siguiente figura para rellenar los datos necesarios para la ejecución de la tarea.

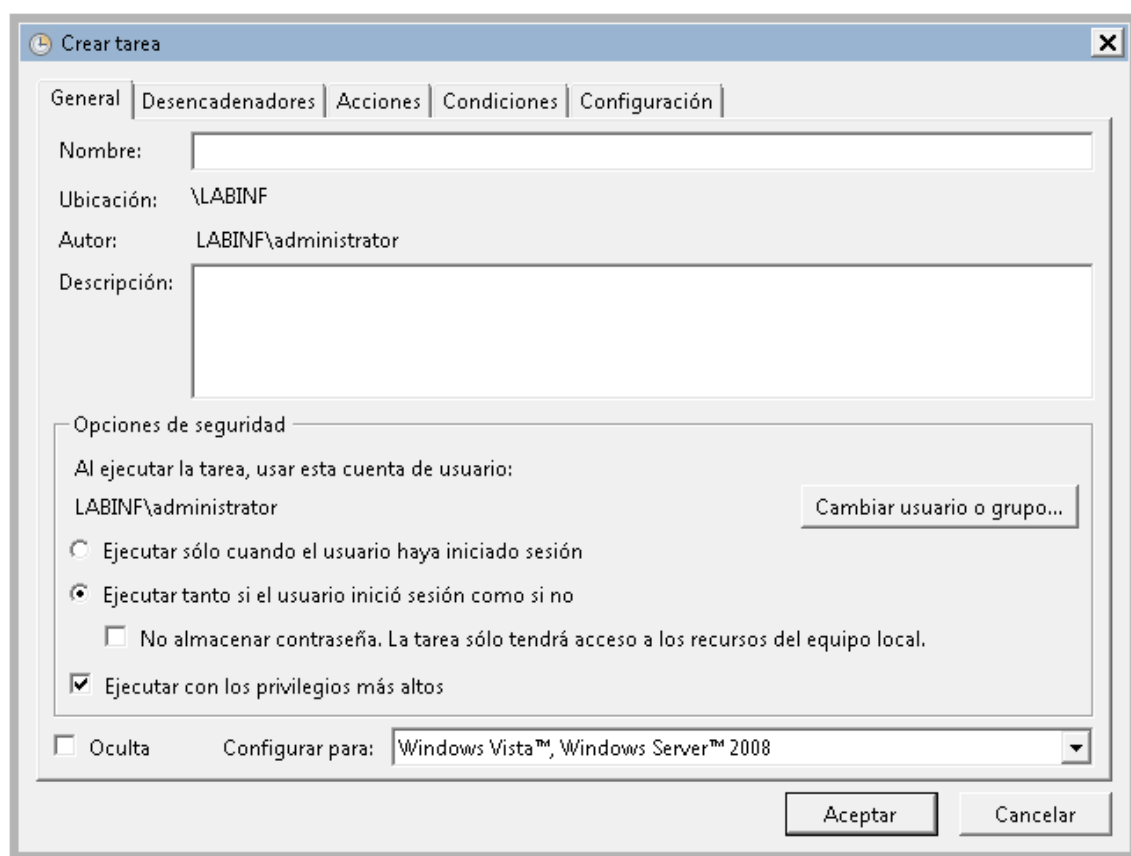


Figura 5.16. Ventana “Crear tarea”.

- A continuación se rellena los campos del Nombre, Descripción y se selecciona el *checkbox* “Ejecutar con los privilegios más altos”.
- En la pestaña “Desencadenadores” se procede a configurar la programación de la tarea.
- En la pestaña “Acciones” se procede a configurar las acciones que debe realizar la tarea.
- A continuación se pulsará el botón Aceptar para finalizar y cerrar la ventana.
- Seguidamente se añade la extensión .xml al archivo creado ubicado en *C:\Windows\System32\Tasks* y se copia el fichero en el almacén de tareas ubicado en *\\ldap\sysvol\Tasks\almacen*.
- Por último se configura la tarea en las aulas o equipos que se necesite con la herramienta PolGest.

## 5.8. Gestor de políticas y tareas programadas (PolGest)

“PolGest” es una herramienta creada por un becario del ldi que simplifica la tarea de gestión de políticas de grupo y tareas programadas. Dispone de una interfaz gráfica que permite consultar y modificar las políticas de grupo y las tareas programadas, correspondientes a un equipo o aula de forma sencilla e intuitiva.

### 5.8.1. Funcionamiento del gestor de políticas

Una vez iniciado el archivo ejecutable, se muestra una pantalla en la que se presenta un menú en la parte superior donde se encuentran todas las aulas del ldi. Por defecto, la herramienta se inicia con la pestaña del aula 1.0.A01 abierta.

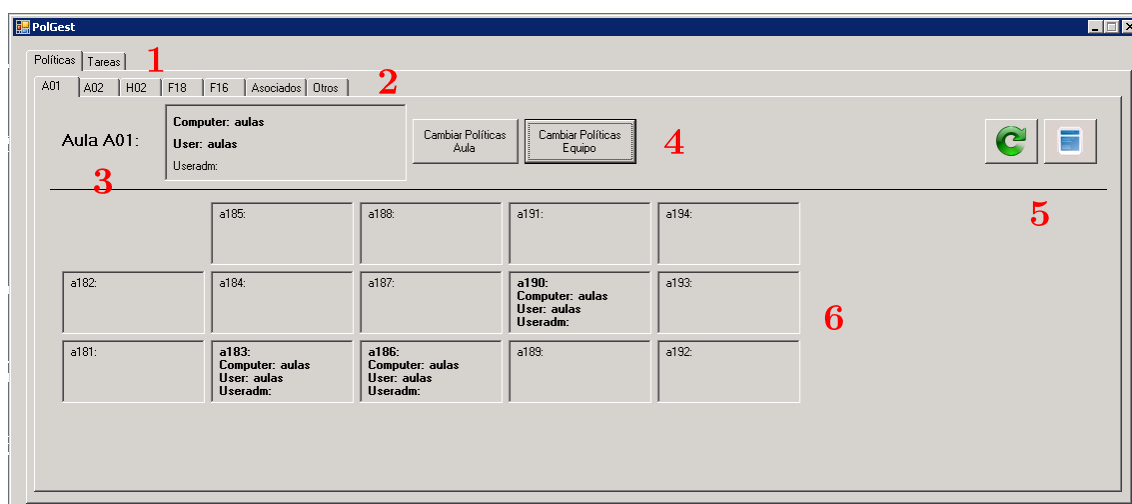


Figura 5.17. Pantalla principal de la herramienta PolGest.

A continuación se describe los elementos que componen la interfaz de la herramienta:

1. Pestañas para seleccionar la gestión de políticas o tareas programadas.
2. Pestañas para seleccionar el aula informática en la que se han de realizar cambios.
3. Ventana que muestra las políticas aplicadas actualmente al aula.

4. Botones para realizar cambios en las políticas del aula seleccionada y equipo.
5. Botón para consultar las políticas almacenadas en el servidor y botón para refrescar el contenido de las políticas asignadas al aula y equipos.
6. Equipos pertenecientes al aula informática seleccionada con las políticas asignadas a cada uno.

#### 5.8.1.1. *Cambiar políticas de un aula*

Al pulsar el botón “Cambiar Políticas Aula” se abre la ventana de la Figura 5.18.

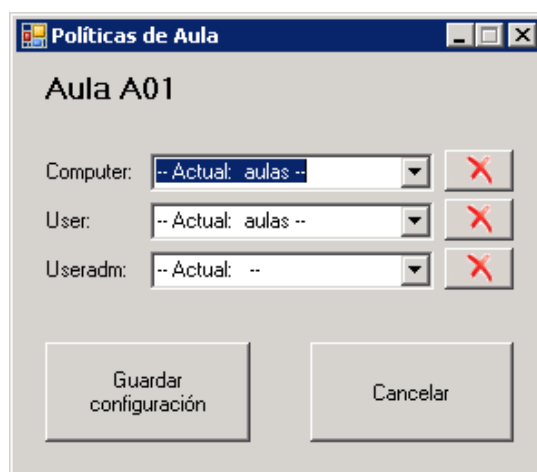


Figura 5.18. Ventana de gestión de políticas de aula.

En el centro de la ventana aparecen tres desplegables para poder configurar la política al objeto apropiado (equipo, usuario y usuario administrador). Una vez seleccionadas las políticas deseadas se pulsa en el botón “Guardar configuración” para salvar los cambios realizados.

Si se desea eliminar la política asignada a un objeto se ha de pulsar en los botones con forma de aspa en la parte derecha del desplegable.

### 5.8.1.2. Cambiar políticas de un equipo

Al pulsar el botón “Cambiar Políticas Equipo” se abre la ventana de la Figura 5.19.

La política prioritaria siempre es la configurada en el equipo, por lo que si un equipo tiene configurada una política distinta al del aula, siempre se aplicará la política asignada al equipo. En el caso de la Figura 5.17 los equipos a183, a186 y a190 tienen políticas prioritarias asignadas.

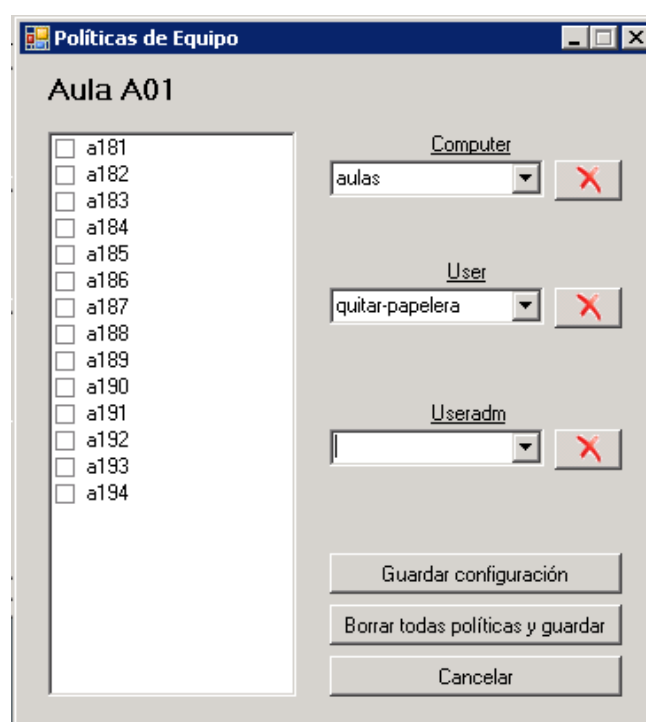


Figura 5.19. Ventana de gestión de políticas de equipo.

El procedimiento es similar al explicado en el apartado 5.8.1.1. Lo único que se debe tener en cuenta es que se puede seleccionar más de un equipo para asignar una misma política a un objeto o varios. Además también se puede borrar todas las políticas de usuario configuradas pulsando en el botón “Borrar todas políticas y guardar”.

### 5.8.1.3. Consultar políticas del almacén

Para consultar las políticas disponibles en el almacén se ha de pulsar en el botón de la derecha del elemento número cuatro de la Figura 5.17. Seguidamente aparecerá una ventana como la de la siguiente figura que nos listará las políticas disponibles clasificadas por objetos.



Figura 5.20. Ventana de políticas existentes en el almacén.

### 5.8.2. Funcionamiento del gestor de tareas programadas

Una vez iniciado el archivo ejecutable, se muestra una pantalla en la que se presenta un menú en la parte superior donde se encuentran todas las aulas del IIdi. Por defecto, la herramienta se inicia con la pestaña del aula 1.0.A01 abierta.

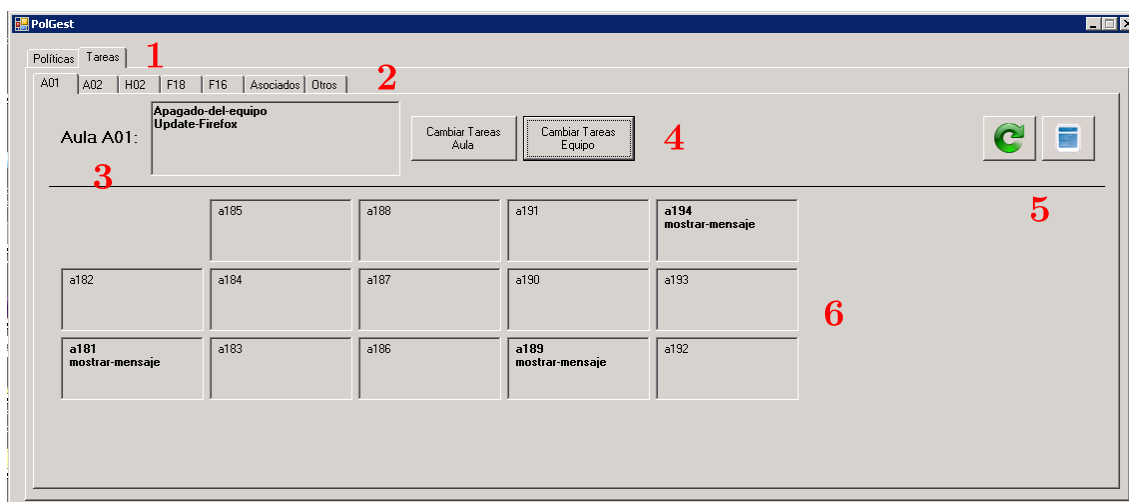


Figura 5.21. Pantalla principal de la herramienta PolGest.

A continuación se describe los elementos que componen la interfaz de la herramienta:

1. Pestañas para seleccionar la gestión de políticas o tareas programadas.
2. Pestañas para seleccionar el aula informática en la que se han de realizar cambios.
3. Ventana que muestra las tareas programadas aplicadas actualmente al aula.
4. Botones para realizar cambios en las tareas del aula seleccionada y equipo.
5. Botón para consultar las tareas programadas almacenadas en el servidor y botón para refrescar el contenido de las tareas programadas asignadas al aula y equipos.
6. Equipos pertenecientes al aula informática seleccionada con las tareas programadas asignadas a cada uno.



### 5.8.2.1. *Cambiar tareas programadas de un aula*

Al pulsar el botón “Cambiar Tareas Aula” se abre la ventana de la Figura 5.22.

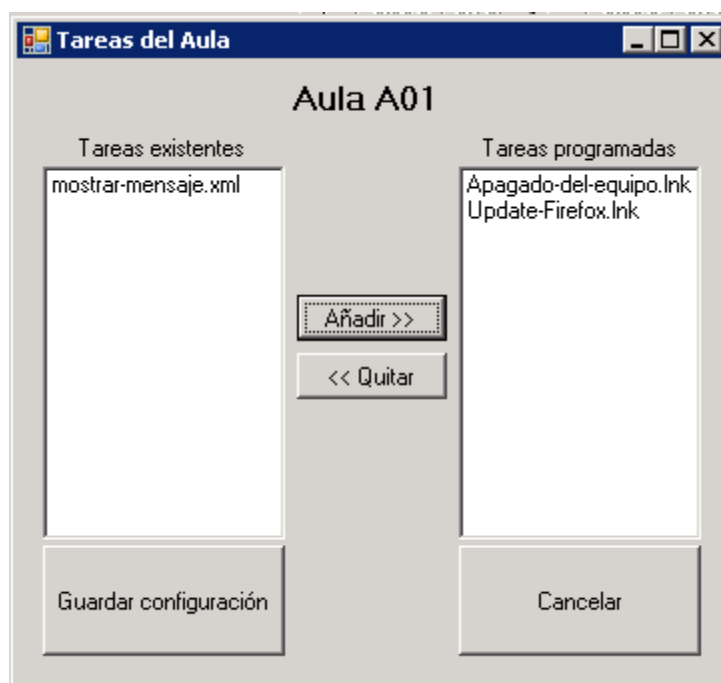


Figura 5.22. Ventana de gestión de tareas de aula.

A la izquierda aparece una ventana con las tareas programadas disponibles en el almacén. A la derecha se tiene una ventana con las tareas programadas asignadas actualmente al aula. Para añadir una tarea se tiene que seleccionar el texto de la ventana de la izquierda y se pulsará en el botón Añadir. Para eliminar una tarea programada se selecciona un texto de la ventana de la derecha y se pulsará en el botón Quitar. Una vez seleccionadas las tareas programadas deseadas se pulsa en el botón “Guardar configuración” para salvar los cambios realizados.

### 5.8.2.2. *Cambiar tareas programadas de un equipo*

Al pulsar el botón “Cambiar Tareas Equipo” se abre la ventana de la Figura 5.23.

La tarea programada prioritaria siempre es la configurada en el equipo, por lo que si un equipo tiene configurada una tarea programada distinta al del aula, siempre se aplicará la tarea programada asignada al equipo. En el caso de la Figura 5.21 los equipos a181, a189 y a194 tienen tareas programadas prioritarias asignadas.

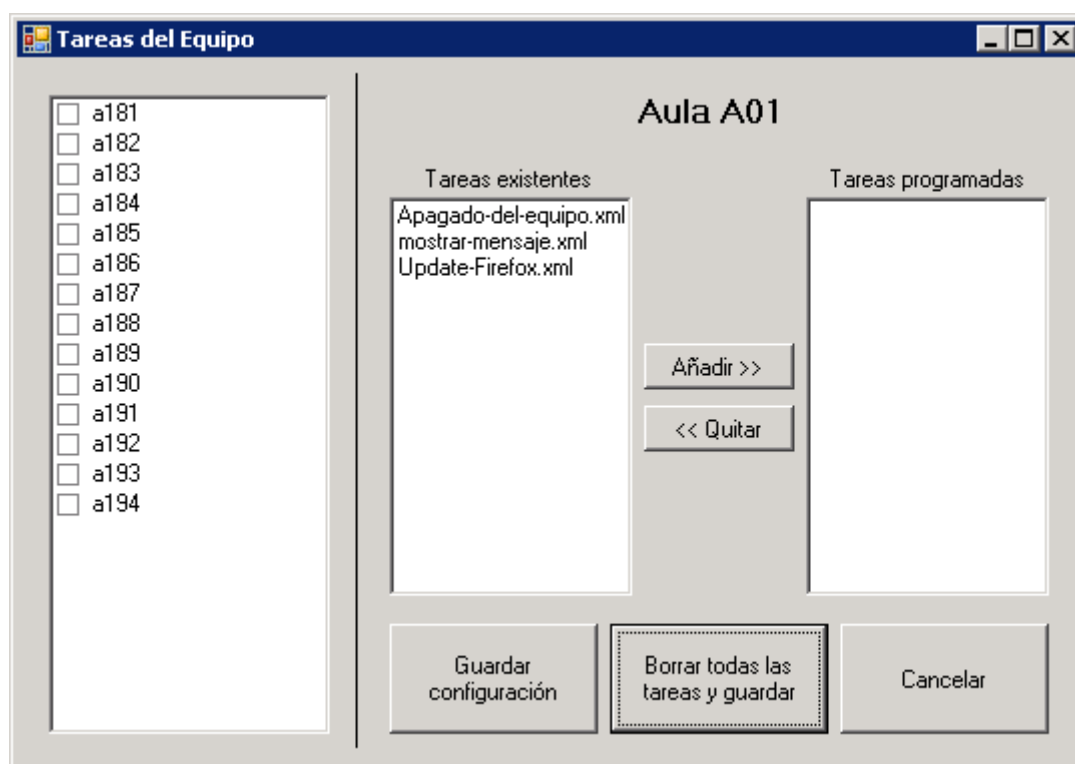


Figura 5.23. Ventana de gestión de tareas programadas de un equipo.

El procedimiento es similar al explicado en el apartado 5.8.2.1. Lo único que se debe tener en cuenta es que se puede seleccionar más de un equipo para asignar una misma tarea programada. Además también se puede borrar todas las tareas programadas pulsando en el botón “Borrar todas las tareas y guardar”.

## 5.9. Tareas finales

A continuación se describen todas las tareas realizadas después de instalar y configurar los servicios descritos en los puntos anteriores.

### 5.9.1. Migración de usuarios

Una vez instalados los servicios se procede a migrar las cuentas de usuario del anterior sistema.

Las cuentas (fichero *passwd*) y contraseñas (fichero *shadow*) del anterior sistema (NIS) se encuentran almacenadas en ficheros de texto por lo que se ha realizado un *script* (se puede consultar en Capítulo 11) que realiza las siguientes operaciones para migrar dichas cuentas al nuevo sistema.

1. Obtiene el identificador del fichero *passwd*.
2. Realiza la consulta en el ldap de la universidad del nombre, apellidos y carrera cursada (alumno) o Departamento (profesor).
3. Si el usuario está en el ldap de la universidad se procede a realizar la cuenta de usuario sin contraseña.
4. Si el usuario no está en el ldap de la universidad se guarda la línea obtenida en un fichero de log para tratarlo posteriormente de manera manual.
5. Una vez finalizada la creación de cuentas se procede con la asignación de contraseñas, para ello se abre el fichero de contraseñas y se asignan a los usuarios creados anteriormente.

Hay que tener en cuenta que la contraseña migrada solamente es válida para iniciar sesión en los clientes Linux. Esto es debido que se debe generar otra contraseña (que es la misma para los dos sistemas operativos pero con distinto cifrado) para iniciar sesión en los clientes Windows. Para realizar dicha actualización de contraseña es necesario cumplimentar el formulario de la página web del ldi con url [https://www.lab.inf.uc3m.es/servicios/cambiar\\_pass](https://www.lab.inf.uc3m.es/servicios/cambiar_pass).

### 5.9.2. Copia de seguridad

Aunque el ldi realice una copia de seguridad periódica de las máquinas virtuales que prestan los servicios a las aulas informáticas se ha considerado oportuno realizar una copia de seguridad adicional del árbol del directorio ldap.

El *script* (se puede consultar en el Capítulo 11) que realiza la copia de seguridad utiliza un comando que nos ofrece el paquete que contiene el servidor y nos permite salvar los registros aunque el servidor esté en funcionamiento. Una vez guardados los registros en un fichero, el *script* le asigna una fecha y lo guarda en un histórico por si fuera necesario en caso de pérdida de datos.

### 5.9.3. Script de gestión de usuarios GESTION

Para gestionar los usuarios pertenecientes al ldi, el personal dispone de una aplicación compuesta por varios *scripts*. Dicha herramienta se denomina GESTION y se ha tenido que modificar para adaptarse al nuevo sistema de autenticación de usuarios.

A continuación se realiza una descripción de la funcionalidad de la herramienta.

La herramienta GESTION se debe ejecutar desde el servidor ldap, debido a que es único servidor permitido para realizar operaciones de escritura en el árbol ldap.

En la siguiente figura se puede observar el menú principal de la herramienta. En ella se muestra las distintas cuentas con las que el administrador puede operar. Los tipos de cuenta que se pueden administrar son: alumno, profesor, BDUA (bloques de usuario asignatura), asignatura y personal.

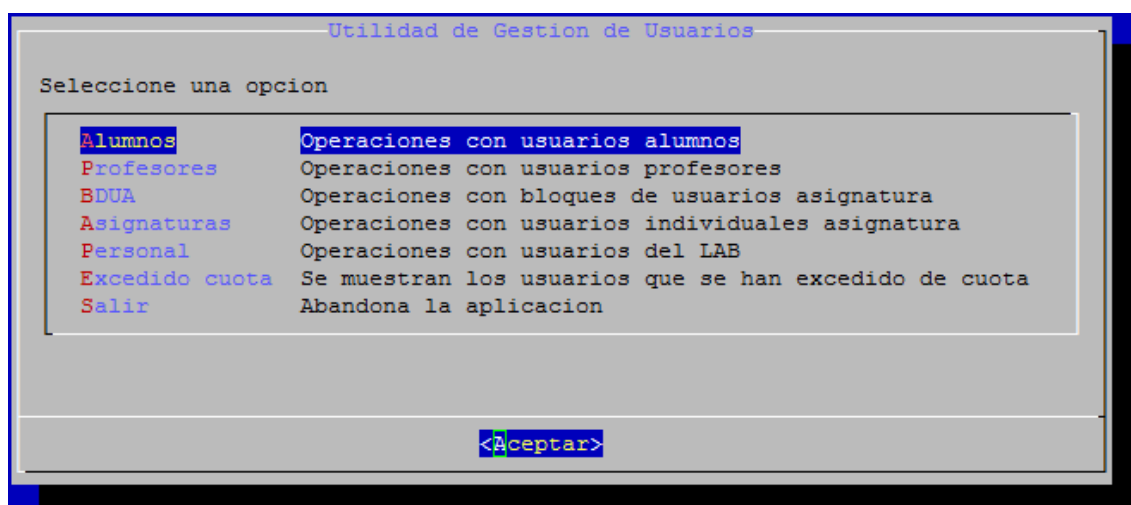


Figura 5.24. Menú principal.

Cuando se selecciona el tipo de cuenta que se desea administrar se solicita el nombre o número de cuenta de usuario. Una vez introducido dicho valor aparece un menú similar al de la siguiente figura.

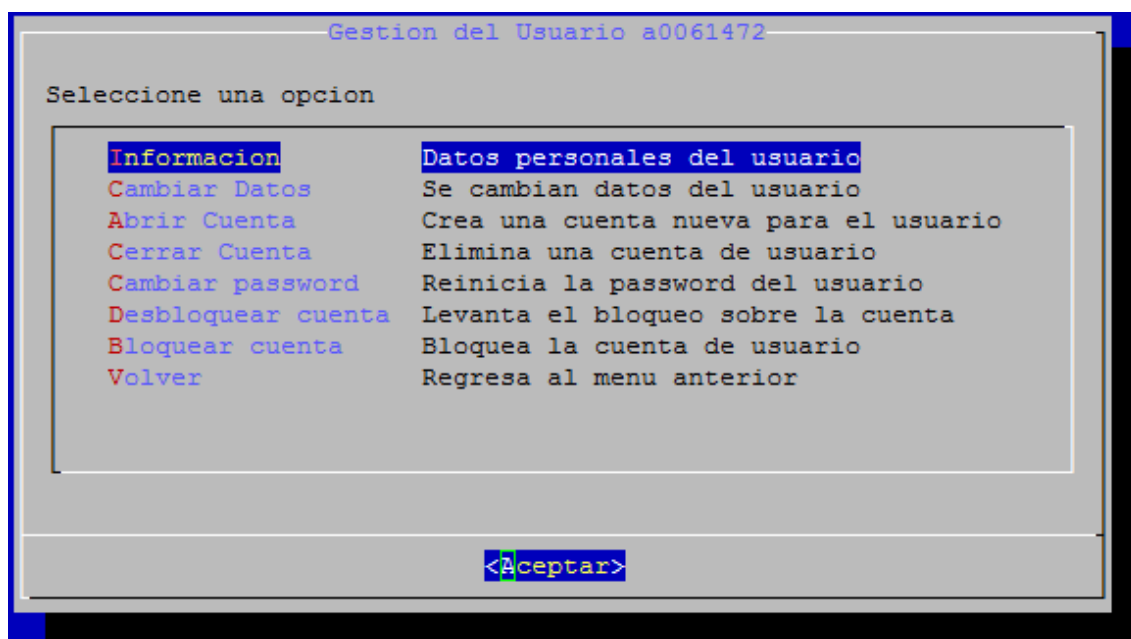


Figura 5.25. Menú de gestión de usuario.

En dicho menú se puede observar las diversas operaciones que se pueden realizar sobre una cuenta de usuario.

La funcionalidad de cada operación es:

- **Información:** Seleccionando esta opción se muestra toda la información almacenada en el ldap relativa al usuario. En la siguiente figura se puede ver un ejemplo de los datos mostrados.

The screenshot shows a terminal window titled "Gestion de Usuarios". It displays the LDAP entry for user "a0061472". Below the entry, it shows disk quotas for the user.

```

Informacion del usuario a0061472:
dn: uid=a0061472,ou=People,dc=lab,dc=inf,dc=uc3m,dc=es
objectClass:
top,person,organizationalPerson,inetOrgPerson,posixAccount,shadowAccount,sambaSamAccount,inetLocalMailRecipient
cn: ROBERTO FUENTES ASTORGA
sn: FUENTES ASTORGA
givenName: ROBERTO
uid: a0061472
gidNumber: 210
loginShell: /bin/bash
gecos: ROBERTO FUENTES ASTORGA,INGENIERIA TECNICA EN INFORMATICA DE GESTION,,,
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
displayName: ROBERTO FUENTES ASTORGA
sambaPrimaryGroupSID: S-1-5-21-686392925-4218348329-2259797951-1421
mailLocalAddress: a0061472
mail: a0061472@lab.inf.uc3m.es
sambaSID: S-1-5-21-686392925-4218348329-2259797951-12008
uidNumber: 5504
homeDirectory: /users/alumnos-05-06/a0061472
sambaProfilePath: \\ldap\profiles\perfil_comun_w7
sambaLMPassword:
sambaNTPassword:
sambaPwdMustChange: 9988755302
userPassword:
shadowLastChange: 15611
shadowMax: 99999
sambaAcctFlags: [UX]
sambaPwdLastSet: 1348841703

User ID      Used    Soft    Hard    Warn/Grace
-----
Disk quotas for User a0061472 (5504)
Filesystem  Blocks  Quota   Limit Warn/Time   Mounted on
/dev/xvdb1  804,1M    2G      2G    00 [-----] /users
Disk quotas for User a0061472 (5504)
Filesystem  Blocks  Quota   Limit Warn/Time   Mounted on
/dev/xvdb1  804,1M    2G      2G    00 [-----] /users
  
```

At the bottom of the window, there is a button labeled "<Aceptar>".

Figura 5.26. Consulta de datos de un usuario.

- **Cambiar datos:** Esta opción permite realizar la modificación del nombre, apellidos y curso/despacho de un usuario.
- **Abrir cuenta:** Esta opción permite la creación de una cuenta.
- **Cerrar cuenta:** Seleccionando esta opción se eliminará la cuenta y los datos del usuario seleccionado.
- **Cambiar contraseña:** Esta opción permitirá al administrador enviar al usuario una nueva contraseña aleatoria.

- **Desbloquear cuenta:** Seleccionando esta opción se bloqueará la cuenta de usuario y no permitirá el uso de la cuenta en ningún servicio del ldi.
- **Bloquear cuenta:** Esta opción permite desbloquear la cuenta de usuario para que se pueda usar los servicios prestados por el ldi.

#### 5.9.4. Preparación del cliente Windows para clonación

Para realizar la instalación de los sistemas operativos de los equipos cliente el ldi cuenta con una herramienta de creación propia, denominada Ghost, que realiza dicha tarea de forma remota y simultánea en un aula informática.

Debido a que los equipos de las aulas informáticas no tienen el mismo hardware, la configuración de los clientes Windows no es la misma y pueden surgir problemas al instalar la imagen del sistema operativo si dicha imagen no está preparada primero.

Microsoft pone a disposición de sus usuarios una herramienta denominada Sysprep que permite solucionar los problemas de configuración inicial de los clientes Windows. A continuación se realiza una breve descripción de la herramienta Sysprep.

##### 5.9.4.1. *Sysprep*

La Herramienta de preparación del sistema, *Sysprep.exe*, se usa para preparar una instalación de Windows para la creación de imágenes o la entrega a un cliente.

Sysprep.exe es el programa principal que llama a otros archivos ejecutables que preparan la instalación de Windows. Sysprep.exe se encuentra en el directorio `%WINDIR%\system32\sysprep` de todas las instalaciones. Siempre se debe ejecutar desde el directorio `%WINDIR%\system32\sysprep` y debe ejecutarse en la versión de Windows con la que se ha instalado.

Las ventajas de usar Sysprep son las siguientes:

- **Quita de Windows datos específicos del sistema:** Sysprep puede quitar toda la información específica del sistema de una imagen de Windows instalada, incluido el identificador de

seguridad (SID) del equipo. Esto permite capturar la instalación de Windows e instalarla en toda la organización.

- **Configura Windows para arrancar el modo auditoría:** Este modo permite instalar controladores de dispositivo y aplicaciones de terceros, así como probar la funcionalidad del sistema.
- **Configura Windows para arrancar la Bienvenida de Windows:** Configura una instalación de Windows para arrancar la Bienvenida de Windows la próxima vez que se inicie el sistema. En general, configura un sistema para arrancar la Bienvenida de Windows inmediatamente antes de entregar el equipo a un cliente.
- **Restablece la activación de productos de Windows:** Sysprep puede restablecer tres veces la activación de productos de Windows.

Cuando se ejecuta Sysprep, se realiza el siguiente proceso:

- Comprueba que se puede ejecutar Sysprep. Sólo un administrador puede ejecutar Sysprep y sólo se puede ejecutar una sesión de Sysprep a la vez. Además, Sysprep debe ejecutarse en la versión de Windows con la que se ha instalado.
- Inicializa el registro.
- Analiza los argumentos de la línea de comandos.
- Si no se han incluido argumentos de la línea de comandos, aparece la ventana de Sysprep, que permite a los usuarios especificar acciones de Sysprep.
- Procesa las acciones de Sysprep, llama a los archivos .dll y ejecutables apropiados y agrega acciones al archivo de registro.
- Comprueba que todos los archivos .dll han procesado todas sus tareas y, a continuación, apaga el sistema, lo reinicia o sale de Sysprep.

El ldi utiliza esta herramienta para configurar las siguientes configuraciones de los clientes Windows:

- Resolución de la pantalla.
- Asignación de clave temporal al equipo.
- Rellenar información del propietario del equipo.
- Configuración de los servidores DNS de la tarjeta de red.
- Activación del administrador local del equipo.



- Configuración del inicio de sesión automático como usuario administrador durante 3 reinicios (necesarios para configurar el equipo automáticamente mediante un *script*).
- Configuración del nombre del equipo.
- Lenguaje del sistema.

### 5.9.5. Creación del perfil de usuario en Windows

En la familia de sistemas operativos Microsoft Windows los usuarios pueden personalizar su cuenta de usuario para que tenga una distribución y apariencia personalizada.

Esta característica se ha utilizado en el ldi para dar un aspecto homogéneo a todos los usuarios que utilicen el servicio. Además dicho perfil es temporal y de sólo lectura, por lo que los cambios realizados no se propagarán al servidor que lo contiene.

A continuación se detalla el proceso de creación del perfil de usuario para utilizar los clientes Windows.

1. Configurar los aspectos visuales del usuario con el que estamos realizando la imagen del sistema (Es importante que solamente exista un usuario registrado en el sistema).
2. Se ejecuta Sysprep para que el sistema realice la copia del perfil modificado al usuario `c:\users\default`.
3. Cuando sysprep realice todas las tareas requeridas se debe arrancar de nuevo el equipo para obtener el perfil de usuario.
4. Se debe preparar una ubicación de red para guardar el perfil de usuario, en nuestro caso `\\ldap\profiles`.
5. En el equipo cliente se procede a montar y asignar letra a la dirección de red del punto anterior.
6. Se abre la administración de perfiles locales siguiendo los pasos Inicio → Panel de control → Cuentas de usuario → Cuentas de usuario → Configurar las propiedades avanzadas del perfil de usuario.

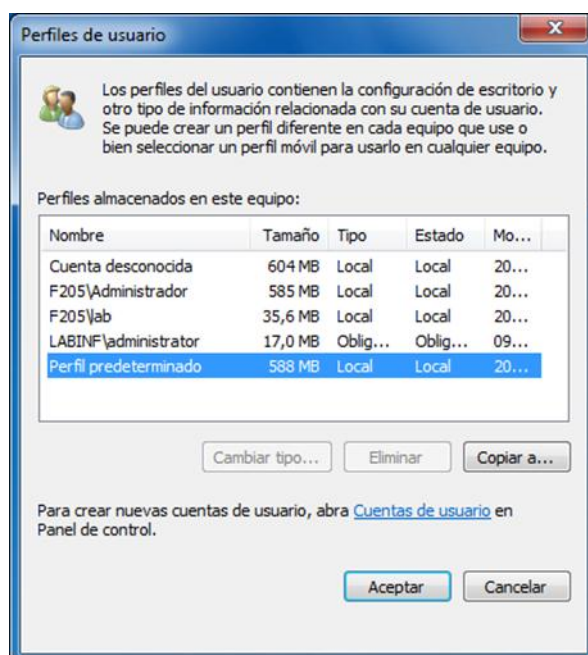


Figura 5.27. Ventana de propiedades avanzadas del perfil de usuario.

- Se debe seleccionar la opción “Perfil predeterminado” y seguidamente se pulsa en el botón “Copiar a” para introducir la ubicación de destino del perfil (Importante: la carpeta de destino debe acabar en .v2).

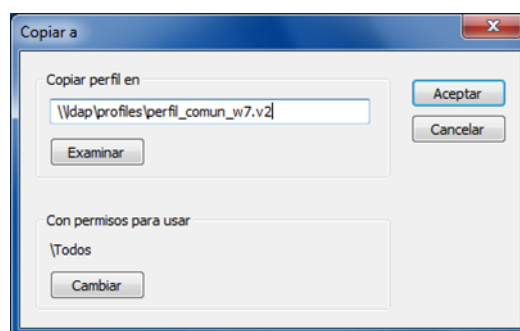


Figura 5.28. Cuadro de diálogo “Copiar a”.

- Para que todos los usuarios puedan leer el perfil se debe cambiar los permisos para usar a “Todos”.
- Para que el perfil no se pueda modificar se cambia la extensión del fichero NTUSER.DAT por NTUSER.MAN.
- Por último se eliminará los datos del perfil poco relevantes para que ocupe el mínimo espacio posible. Hay que tener en cuenta que cuando un usuario inicia sesión el equipo debe realizar una copia del perfil en el disco duro para poder aplicárselo al usuario.

# Capítulo 6

## Pruebas del sistema

En este capítulo se van a describir todas las pruebas realizadas al sistema para comprobar y validar su funcionamiento.

Para cada prueba se realiza una tabla que contendrá la siguiente información:

- **Identificador:** Identifica una prueba de manera unívoca. La nomenclatura que se seguirá es la siguiente: PRU-XXX, siendo X un número entero comprendido entre 0 y 9.
- **Descripción:** Descripción de la prueba de sistema.
- **Entrada:** Datos de entrada que se usarán en la prueba para analizar su comportamiento.
- **Salida:** Resultado obtenido o esperado de la prueba.
- **Secuencia:** Pasos que debe realizar el cliente para realizar la prueba.
- **Precondiciones:** Condiciones que deben cumplirse para que se pueda realizar la prueba.

## 6.1. Pruebas del servidor LDAP

A continuación se describe las pruebas realizadas a los componentes del servidor ldap para validar su funcionamiento.

### 6.1.1. Prueba del servicio de autenticación

A continuación se describe las pruebas realizadas al componente “Servicio Autenticación” perteneciente al subsistema LDAP.

<b>PRU-001</b>	<b>Autenticación de usuario cuenta Linux</b>
<b>Descripción</b>	Comprobación de autenticación de usuario en el servidor utilizando el sistema operativo Linux.
<b>Entrada</b>	Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Autenticación correcta del usuario.
<b>Secuencia</b>	1. Ejecutar el siguiente comando en el servidor: # su <id-usuario> 2. Introducir la contraseña del usuario.
<b>Precondiciones</b>	La cuenta debe existir en el sistema.

Tabla 6.1. PRU-001 Autenticación de usuario cuenta Linux.

<b>PRU-002</b>	<b>Autenticación de usuario cuenta Windows</b>
<b>Descripción</b>	Comprobación de autenticación de usuario en el servidor utilizando el sistema operativo Windows.
<b>Entrada</b>	Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Listado de los servicios disponibles en el servidor.
<b>Secuencia</b>	1. Ejecutar el siguiente comando en el servidor: # smbclient -L //ldap -U <id-usuario> 2. Introducir la contraseña del usuario.
<b>Precondiciones</b>	La cuenta debe existir en el sistema.

Tabla 6.2. PRU-002 Autenticación de usuario cuenta Windows.

---

<b>PRU-003</b>	<b>Consulta de cuenta de usuario</b>
<b>Descripción</b>	Comprobación de la función de búsqueda en el árbol ldap para obtener datos de un usuario.
<b>Entrada</b>	Identificador del usuario.
<b>Salida</b>	Datos del usuario.
<b>Secuencia</b>	1. Ejecutar el siguiente comando en el servidor: # smbldap-usershow <id-usuario>
<b>Precondiciones</b>	El usuario debe existir en el sistema.

---

Tabla 6.3. PRU-003 Consulta de cuenta de usuario.

### 6.1.2. Prueba del módulo de creación de cuentas

A continuación se describe las pruebas realizadas al componente “Módulo Creación Cuentas” perteneciente al subsistema LDAP.

<b>PRU-004</b>	<b>Creación de cuenta de usuario</b>
<b>Descripción</b>	Comprobación de creación de cuenta de usuario.
<b>Entrada</b>	Fichero de altas de usuario.
<b>Salida</b>	La cuenta de usuario creada correctamente.
<b>Secuencia</b>	1. Ejecución del siguiente comando en el servidor: # /etc/ldap/scripts/crea_usuario.pl
<b>Precondiciones</b>	La cuenta de usuario no debe existir en el sistema.

Tabla 6.4. PRU-004 Creación de cuenta de usuario.

<b>PRU-005</b>	<b>Cambio de contraseña de usuario</b>
<b>Descripción</b>	Comprobación de cambio de contraseña de usuario.
<b>Entrada</b>	Fichero de cambios de contraseña de usuario.
<b>Salida</b>	El cambio de contraseña realizado correctamente.
<b>Secuencia</b>	1. Ejecución del siguiente comando en el servidor: # /etc/ldap/scripts/crea_usuario.pl
<b>Precondiciones</b>	La cuenta de usuario debe existir en el sistema.

Tabla 6.5. PRU-005 Cambio de contraseña de usuario.

### 6.1.3. Prueba de la aplicación de gestión de usuarios

A continuación se describe las pruebas realizadas al componente “Apps Gestión Usuarios” perteneciente al subsistema LDAP.

<b>PRU-006</b>	<b>Creación de cuenta de usuario</b>
<b>Descripción</b>	Comprobación de creación de cuenta de usuario.
<b>Entrada</b>	Identificador del usuario.
<b>Salida</b>	Cuenta de usuario creada correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # GESTION</li> <li>2. Seleccionar la opción <i>Alumnos</i>.</li> <li>3. Introducir los 6 últimos dígitos del NIA del alumno.</li> <li>4. Seleccionar la opción <i>Abrir Cuenta</i>.</li> <li>5. Comprobar que los datos mostrados del usuario son correctos y pulsar en <i>Aceptar</i>.</li> </ol>
<b>Precondiciones</b>	La cuenta de usuario no debe existir en el sistema.

Tabla 6.6. PRU-006 Creación de cuenta de usuario.

<b>PRU-007</b>	<b>Consulta de datos personales de usuario</b>
<b>Descripción</b>	Comprobación de la realización de una consulta de los datos personales de un usuario.
<b>Entrada</b>	Identificador del usuario.
<b>Salida</b>	Datos del usuario.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # GESTION</li> <li>2. Seleccionar la opción <i>Alumnos</i>.</li> <li>3. Introducir los 6 últimos dígitos del NIA del alumno.</li> <li>4. Seleccionar la opción <i>Información</i>.</li> </ol>
<b>Precondiciones</b>	La cuenta de usuario debe existir en el sistema.

Tabla 6.7. PRU-007 Consulta de datos personales de usuario.

<b>PRU-008</b>	<b>Cambio de datos personales de usuario</b>
<b>Descripción</b>	Comprobación de cambio de datos personales del usuario.
<b>Entrada</b>	Identificador del usuario. Nuevos datos personales.
<b>Salida</b>	Datos de usuario cambiados correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # GESTION</li> <li>2. Seleccionar la opción <i>Alumnos</i>.</li> <li>3. Introducir los 6 últimos dígitos del NIA del alumno.</li> <li>4. Seleccionar la opción <i>Cambiar Datos</i>.</li> <li>5. Introducir los nuevos datos y pulsar <i>Aceptar</i>.</li> </ol>
<b>Precondiciones</b>	La cuenta de usuario debe existir en el sistema.

Tabla 6.8. PRU-008 Cambio de datos personales de usuario.

<b>PRU-009</b>	<b>Generación y envío de contraseña aleatoria</b>
<b>Descripción</b>	Comprobación del cambio aleatorio de contraseña y posterior envío al usuario mediante correo electrónico.
<b>Entrada</b>	Identificador del usuario.
<b>Salida</b>	Cambio de contraseña efectuada correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # GESTION</li> <li>2. Seleccionar la opción <i>Alumnos</i>.</li> <li>3. Introducir los 6 últimos dígitos del NIA del alumno.</li> <li>4. Seleccionar la opción <i>Cambiar password</i>.</li> </ol>
<b>Precondiciones</b>	La cuenta de usuario debe existir en el sistema.

Tabla 6.9. PRU-009 Generación y envío de contraseña aleatoria.

<b>PRU-010</b>	<b>Bloqueo de cuenta de usuario</b>
<b>Descripción</b>	Comprobación del bloqueo de la cuenta de usuario.
<b>Entrada</b>	Identificador del usuario.
<b>Salida</b>	Cuenta de usuario bloqueada para el uso de todos los sistemas operativos.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # GESTION</li> <li>2. Seleccionar la opción <i>Alumnos</i>.</li> <li>3. Introducir los 6 últimos dígitos del NIA del alumno.</li> <li>4. Seleccionar la opción <i>Bloquear cuenta</i>.</li> </ol>
<b>Precondiciones</b>	La cuenta de usuario debe existir en el sistema.

Tabla 6.10. PRU-010 Bloqueo de cuenta de usuario.



<b>PRU-011</b>	<b>Desbloqueo de cuenta de usuario</b>
<b>Descripción</b>	Comprobación del desbloqueo de la cuenta de usuario.
<b>Entrada</b>	Identificador del usuario.
<b>Salida</b>	Cuenta de usuario desbloqueada para el uso de todos los sistemas operativos.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # GESTION</li> <li>2. Seleccionar la opción <i>Alumnos</i>.</li> <li>3. Introducir los 6 últimos dígitos del NIA del alumno.</li> <li>4. Seleccionar la opción <i>Desbloquear cuenta</i>.</li> </ol>
<b>Precondiciones</b>	La cuenta de usuario debe existir en el sistema.

Tabla 6.11. PRU-011 Desbloqueo de cuenta de usuario.

<b>PRU-012</b>	<b>Consulta de usuarios que han excedido la cuota</b>
<b>Descripción</b>	Comprobación de la realización de una consulta de los usuarios que han excedido la cuota en el sistema.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Listado de los usuarios que han excedido la cuota con el tamaño de datos que tienen almacenado en la cuenta.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # GESTION</li> <li>2. Seleccionar la opción <i>Excedido cuota</i>.</li> </ol>
<b>Precondiciones</b>	Ninguna.

Tabla 6.12. PRU-012 Consulta de usuarios que han excedido la cuota.

#### 6.1.4. Prueba de la copia de seguridad

A continuación se describe las pruebas realizadas al componente “Backup Ldap” perteneciente al subsistema LDAP.

<b>PRU-013</b>	<b>Realización y Restauración de copia de seguridad</b>
<b>Descripción</b>	Comprobación de la realización y restauración de la copia de seguridad de los datos de ldap.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Copia de seguridad realizada y restaurada con éxito.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Realización de la copia de seguridad ejecutando el siguiente comando en el servidor: # /users.local/backup/ldap-backup.sh</li> <li>2. Restauración de la copia de seguridad ejecutando el siguiente comando en el servidor: # /users.local/backup/restaurar.sh</li> </ol>
<b>Precondiciones</b>	Ninguna.

Tabla 6.13. PRU-013 Realización y Restauración de copia de seguridad.

### 6.1.5. Prueba del repositorio de perfiles de usuario

A continuación se describe las pruebas realizadas al componente “Perfiles Usuario” perteneciente al subsistema LDAP.

<b>PRU-014</b>	<b>Comprobación de accesibilidad al repositorio</b>
<b>Descripción</b>	Comprobación de acceso al repositorio que contiene los perfiles de usuario.
<b>Entrada</b>	Dirección de red del repositorio. Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Listado de los archivos del repositorio.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor:  <pre>#      smbclient      -U      &lt;id-usuario&gt; //ldap/profiles</pre> </li> <li>2. Introducir la contraseña del usuario.</li> <li>3. Ejecutar el siguiente comando en el servidor:  <pre>smb: \&gt; dir</pre> </li> </ol>
<b>Precondiciones</b>	Ninguna.

Tabla 6.14. PRU-014 Comprobación de accesibilidad al repositorio.

<b>PRU-015</b>	<b>Comprobación de permisos de escritura</b>
<b>Descripción</b>	Comprobación de la configuración de permisos de escritura del repositorio de perfiles de usuario.
<b>Entrada</b>	Dirección de red del repositorio. Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	No debe permitir la escritura en la unidad.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor:  <pre>#      smbclient      -U      &lt;id-usuario&gt; //ldap/profiles</pre> </li> <li>2. Introducir la contraseña del usuario.</li> <li>3. Ejecutar el siguiente comando en el servidor:  <pre>smb: \&gt; mkdir</pre> </li> </ol>
<b>Precondiciones</b>	El usuario no debe ser administrador del sistema.

Tabla 6.15. PRU-015 Comprobación de permisos de lectura y escritura.

### 6.1.6. Prueba del repositorio de configuración de clientes

A continuación se describe las pruebas realizadas al componente “Config Clientes” perteneciente al subsistema LDAP.

PRU-016	Comprobación de accesibilidad al repositorio
<b>Descripción</b>	Comprobación de acceso al repositorio que contiene la configuración de los clientes.
<b>Entrada</b>	Dirección de red del repositorio. Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Repositorio accesible.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # smbclient -U &lt;id-usuario&gt; //ldap/sysvol</li> <li>2. Introducir la contraseña del usuario.</li> <li>3. Ejecutar el siguiente comando en el servidor: smb: \&gt; dir</li> </ol>
<b>Precondiciones</b>	Ninguna.

Tabla 6.16. PRU-016 Comprobación de accesibilidad al repositorio.

PRU-017	Comprobación de permisos de lectura y escritura
<b>Descripción</b>	Comprobación de la configuración de permisos de lectura y escritura del repositorio de configuración de los clientes.
<b>Entrada</b>	Dirección de red del repositorio. Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	No debe permitir la escritura en la unidad.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecutar el siguiente comando en el servidor: # smbclient -U &lt;id-usuario&gt; //ldap/sysvol</li> <li>2. Introducir la contraseña del usuario.</li> <li>3. Ejecutar el siguiente comando en el servidor: smb: \&gt; mkdir</li> </ol>
<b>Precondiciones</b>	El usuario no debe ser administrador del sistema.

Tabla 6.17. PRU-017 Comprobación de permisos de lectura y escritura.

## 6.2. Pruebas del servidor CUENTAS

A continuación se describen las pruebas realizadas a los componentes del servidor cuentas para validar su funcionamiento.

### 6.2.1. Prueba del servicio de datos de usuario

A continuación se describe las pruebas realizadas al componente “Servicio Datos Usuario” perteneciente al subsistema CUENTAS.

<b>PRU-018</b>	<b>Comprobación de accesibilidad a los datos de usuario</b>
<b>Descripción</b>	Comprobación de acceso al repositorio que contiene los datos de usuario.
<b>Entrada</b>	Dirección de red del repositorio. Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Repositorio accesible.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>Ejecutar el siguiente comando en el servidor:  <pre>#      smbclient      -U      &lt;id-usuario&gt; //cuentas/&lt;id-usuario&gt;</pre> </li> <li>Introducir la contraseña del usuario.</li> <li>Ejecutar los siguientes comandos en el servidor:  <pre>smb: \&gt; dir</pre> </li> </ol>
<b>Precondiciones</b>	Ninguna.

Tabla 6.18. PRU-018 Comprobación de accesibilidad a los datos de usuario.

<b>PRU-019</b>	<b>Comprobación de permisos de lectura y escritura</b>
<b>Descripción</b>	Comprobación de la configuración de permisos de lectura y escritura del repositorio.
<b>Entrada</b>	Dirección de red del repositorio. Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Debe permitir la lectura y escritura en la unidad.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>Ejecutar el siguiente comando en el servidor:  <pre>#      smbclient      -U      &lt;id-usuario&gt; //cuentas/&lt;id-usuario&gt;</pre> </li> <li>Introducir la contraseña del usuario.</li> <li>Ejecutar los siguientes comandos en el servidor:  <pre>smb: \&gt; mkdir prueba smb: \&gt; dir prueba</pre> </li> </ol>
<b>Precondiciones</b>	El usuario no debe ser administrador del sistema.

Tabla 6.19. PRU-019 Comprobación de permisos de lectura y escritura.

### 6.2.2. Prueba del servicio de autenticación

A continuación se describe las pruebas realizadas al componente “Servicio Autenticación” perteneciente al subsistema CUENTAS.

<b>PRU-020</b>	<b>Autenticación de usuario cuenta Windows</b>
<b>Descripción</b>	Comprobación de autenticación
<b>Entrada</b>	Dirección de red del repositorio. Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Autenticación correcta del usuario.
<b>Secuencia</b>	7. Ejecutar el siguiente comando en el servidor: # smbclient -U <id-usuario> //cuentas/<id-usuario> 8. Introducir la contraseña del usuario.
<b>Precondiciones</b>	Ninguna.

Tabla 6.20. PRU-020 Autenticación de usuario cuenta Windows.

## 6.3. Prueba del servidor CORREO

A continuación se describen las pruebas realizadas al servidor de correo para validar su funcionamiento.

<b>PRU-021</b>	<b>Envío de mail desde el servidor LDAP</b>
<b>Descripción</b>	Comprobación de envío de email desde el servidor ldap.
<b>Entrada</b>	Identificador del usuario.
<b>Salida</b>	Correo electrónico recibido correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"><li>1. Ejecutar el siguiente comando en el servidor: # mail -s prueba roberto.fuentes@uc3m.es</li><li>2. Escribir texto mensaje con un punto al final. Pulsar la tecla Enter.</li></ol>
<b>Precondiciones</b>	Ninguna.

Tabla 6.21. PRU-021 Envío de mail desde el servidor LDAP.

## 6.4. Pruebas del servidor WEB

A continuación se describen las pruebas realizadas al servidor web para validar su funcionamiento.

<b>PRU-022</b>	<b>Creación de cuenta</b>
<b>Descripción</b>	Comprobación de creación de cuenta de usuario desde la página web del ldi.
<b>Entrada</b>	Formulario de alta.
<b>Salida</b>	Usuario creado correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Acceder a la página web con url: <a href="https://www.lab.inf.uc3m.es/servicios/apertura_cuentas">https://www.lab.inf.uc3m.es/servicios/apertura_cuentas</a></li> <li>2. Introducir usuario de campus global.</li> <li>3. Introducir la contraseña de campus global.</li> <li>4. Introducir por duplicado la contraseña deseada para el ldi.</li> <li>5. Pulsar en el botón <i>Solicitar cuenta</i>.</li> </ol>
<b>Precondiciones</b>	El usuario debe tener cuenta en el ldap de la Universidad. El usuario no debe tener cuenta en el ldap del ldi.

Tabla 6.22. PRU-022 Creación de cuenta.

<b>PRU-023</b>	<b>Actualización de cuenta</b>
<b>Descripción</b>	Comprobación de actualización de una cuenta que ha sido migrada el sistema anterior.
<b>Entrada</b>	Formulario de actualización de cuenta.
<b>Salida</b>	Usuario actualizado correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Acceder a la página web con url: <a href="https://www.lab.inf.uc3m.es/servicios/cambiar_pass">https://www.lab.inf.uc3m.es/servicios/cambiar_pass</a></li> <li>2. Introducir usuario de campus global.</li> <li>3. Introducir la contraseña de campus global.</li> <li>4. Introducir por duplicado la contraseña deseada para el ldi.</li> <li>5. Pulsar en el botón <i>Enviar</i>.</li> <li>6. El resultado de realizar la prueba con identificador PRU-029 debe ser satisfactorio.</li> </ol>
<b>Precondiciones</b>	El usuario debe tener cuenta en el ldap de la Universidad. El usuario debe tener cuenta en el ldap del ldi.

Tabla 6.23. PRU-023 Actualización de cuenta.



<b>PRU-024</b>	<b>Cambio de contraseña de cuenta</b>
<b>Descripción</b>	Comprobación de cambio de contraseña de la cuenta de usuario.
<b>Entrada</b>	Formulario de cambio de contraseña.
<b>Salida</b>	Contraseña cambiada correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Acceder a la página web con url: <a href="https://www.lab.inf.uc3m.es/servicios/cambiar_pass">https://www.lab.inf.uc3m.es/servicios/cambiar_pass</a></li> <li>2. Introducir usuario de campus global.</li> <li>3. Introducir la contraseña de campus global.</li> <li>4. Introducir por duplicado la contraseña deseada para el ldi.</li> <li>5. Pulsar en el botón <i>Enviar</i>.</li> <li>6. El resultado de realizar las pruebas con identificador PRU-029 y PRU-033 debe ser satisfactorio.</li> </ol>
<b>Precondiciones</b>	<p>El usuario debe tener cuenta en el ldap de la Universidad.</p> <p>El usuario debe tener cuenta en el ldap del ldi.</p>

Tabla 6.24. PRU-024 Cambio de contraseña de cuenta.

<b>PRU-025</b>	<b>Consultar existencia de cuenta</b>
<b>Descripción</b>	Comprobación de existencia de cuenta de usuario en el ldi.
<b>Entrada</b>	Formulario de estado de cuenta.
<b>Salida</b>	Consulta realizada correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Acceder a la página web con url: <a href="https://www.lab.inf.uc3m.es/servicios/apertura_cuentas">https://www.lab.inf.uc3m.es/servicios/apertura_cuentas</a></li> <li>2. Introducir usuario de campus global.</li> <li>3. Introducir la contraseña de campus global.</li> <li>4. Pulsar en el botón <i>Buscar</i>.</li> </ol>
<b>Precondiciones</b>	El usuario debe tener cuenta en el ldap de la Universidad.

Tabla 6.25. PRU-025 Consultar existencia de cuenta.

## 6.5. Pruebas del cliente WINDOWS

A continuación se describen las pruebas realizadas a los componentes del cliente Windows para validar su funcionamiento.

### 6.5.1. Prueba del módulo tareas

A continuación se describe las pruebas realizadas al componente “Tareas” perteneciente al subsistema CLIENTE WINDOWS.

<b>PRU-026</b>	<b>Sincronización de tareas programadas</b>
<b>Descripción</b>	Comprobación de la sincronización de tareas programadas en un equipo.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Tareas programadas asignadas sincronizadas correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Asignación de tarea programada al equipo mediante programa PolGest.</li> <li>2. Ejecución del <i>script</i> C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\gpupdate.ps1</li> <li>3. Abrir la ubicación C:\Windows\System32\Tasks con el explorador de archivos.</li> </ol>
<b>Precondicio nes</b>	El equipo o el aula que lo contiene deben tener, al menos, una tarea programada asignada.

Tabla 6.26. PRU-026 Sincronización de tareas programadas.

<b>PRU-027</b>	<b>Instalación de tarea programada</b>
<b>Descripción</b>	Comprobación de la instalación en el programador de tareas del equipo de las tareas programadas asignadas.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Tareas programadas instaladas correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Realización satisfactoria de la prueba PRU-026.</li> <li>2. Abrir el programador de tareas ejecutando el comando: Task sched.msc</li> <li>3. Seleccionar la Biblioteca del Programador de tareas para confirmar la instalación de las tareas programadas asignadas.</li> </ol>
<b>Precondiciones</b>	El equipo o el aula que lo contiene deben tener, al menos, una tarea programada asignada.

Tabla 6.27. PRU-027 Instalación de tarea programada.

### 6.5.2. Prueba de la política de equipo

A continuación se describe las pruebas realizadas al componente “Política Equipo” perteneciente al subsistema CLIENTE WINDOWS.

<b>PRU-028</b>	<b>Sincronización y aplicación de política de equipo</b>
<b>Descripción</b>	Comprobación de la sincronización y aplicación de la política de equipo ubicada en el servidor.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Realización de la sincronización y aplicación de la política en el equipo satisfactoriamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Asignación de política al equipo mediante programa PolGest.</li> <li>2. Ejecución del <i>script</i> C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\gpupdate.ps1</li> <li>3. Ejecutar en una ventana de línea de comandos el comando gpedit.msc.</li> <li>4. Seleccionar la opción <i>Todos los valores</i> que se encuentra en el menú del lado izquierdo de la ventana.</li> <li>5. Realizar orden de la lista por el valor <i>Estado</i> y comprobar que las directivas configuradas son correctas.</li> </ol>
<b>Precondicio- nes</b>	El equipo o el aula que lo contiene deben tener, al menos, una política asignada.

Tabla 6.28. PRU-028 Sincronización y aplicación de política de equipo.

### 6.5.3. Prueba de autenticación

A continuación se describe las pruebas realizadas al componente “Autenticación” perteneciente al subsistema CLIENTE WINDOWS.

<b>PRU-029</b>	<b>Autenticación de usuario que no sea tipo asignatura</b>
<b>Descripción</b>	Comprobación de la autenticación de un usuario que no sea del tipo asignatura.
<b>Entrada</b>	Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Autenticación correcta y perfil de usuario genérico cargado correctamente.
<b>Secuencia</b>	1. Inicio de sesión en cliente Windows. 2. Comprobación de los colores de ventanas y mensaje de bienvenida.
<b>Precondiciones</b>	El usuario debe existir en el sistema. El tipo de usuario no debe ser asignatura.

Tabla 6.29. PRU-029 Autenticación de usuario que no sea tipo asignatura.

<b>PRU-030</b>	<b>Autenticación de usuario tipo asignatura</b>
<b>Descripción</b>	Comprobación de la autenticación de un usuario de tipo asignatura.
<b>Entrada</b>	Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Autenticación correcta y perfil de usuario tipo asignatura cargado correctamente.
<b>Secuencia</b>	1. Inicio de sesión en cliente Windows. 2. Comprobación de los colores de ventanas y mensaje de bienvenida.
<b>Precondiciones</b>	El usuario debe existir en el sistema. El tipo de usuario debe ser asignatura.

Tabla 6.30. PRU-030 Autenticación de usuario tipo asignatura.

<b>PRU-031</b>	<b>Montaje de home de usuario</b>
<b>Descripción</b>	Comprobación de montaje de unidad Z:\ con los datos del usuario.
<b>Entrada</b>	Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Montaje de unidad Z:\ realizado correctamente
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecución satisfactoria de la prueba PRU-029 o PRU-030.</li> <li>2. Abrir el explorador de Windows e intentar acceder a la unidad Z:\</li> </ol>
<b>Precondiciones</b>	El usuario debe existir en el sistema.

Tabla 6.31. PRU-031 Montaje de home de usuario.

<b>PRU-032</b>	<b>Sincronización de scripts genéricos</b>
<b>Descripción</b>	Comprobación de la sincronización de los <i>script</i> genéricos en el cliente Windows.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	<i>Scripts</i> genéricos sincronizados correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecución del <i>script</i> C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\gpupdate.ps1</li> <li>2. Comprobación de los ficheros en la ubicación C:\<i>scripts</i>. El origen (\\ldap\sysvol\scripts) debe tener el mismo contenido.</li> </ol>
<b>Precondiciones</b>	El servidor debe tener <i>scripts</i> almacenados previamente.

Tabla 6.32. PRU-032 Sincronización de *scripts* genéricos.

## 6.6. Pruebas del cliente LINUX

A continuación se describen las pruebas realizadas al cliente Linux para validar su funcionamiento.

<b>PRU-033</b>	<b>Autenticación de usuario</b>
<b>Descripción</b>	Comprobación de la autenticación de un usuario.
<b>Entrada</b>	Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Autenticación correcta.
<b>Secuencia</b>	1. Inicio de sesión en el cliente Linux.
<b>Precondiciones</b>	El usuario debe existir en el sistema.

Tabla 6.33. PRU-033 Autenticación de usuario.

<b>PRU-034</b>	<b>Montaje de home de usuario</b>
<b>Descripción</b>	Comprobación del montaje de los datos de usuario.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Montaje de datos de usuario realizado correctamente.
<b>Secuencia</b>	1. Realización satisfactoria de la prueba PRU-033. 2. Ejecución del siguiente comando para listar los ficheros que contiene la cuenta de usuario. # <code>ls -als</code>
<b>Precondiciones</b>	El usuario debe existir en el sistema.

Tabla 6.34. PRU-034 Montaje de home de usuario.

<b>PRU-035</b>	<b>Comunicación de contraseña cifrada con el servidor</b>
<b>Descripción</b>	Comprobación de comunicación segura con el servidor a la hora de autenticar un usuario.
<b>Entrada</b>	Identificador del usuario. Contraseña del usuario.
<b>Salida</b>	Captura de paquetes cifrados correctamente.
<b>Secuencia</b>	1. Preparación de la captura de paquetes con el software wireshark en el lado del cliente o en el lado del servidor. 2. Ejecución de la prueba PRU-033. 3. Comprobación de comunicación segura al autenticar con el servidor.
<b>Precondiciones</b>	El usuario debe existir en el sistema.

Tabla 6.35. PRU-035 Comunicación de contraseña cifrada con el servidor.

## 6.7. Pruebas del servidor POLÍTICAS

A continuación se describen las pruebas realizadas al servidor de políticas para validar su funcionamiento.

PRU-036	Distribución de política a un aula
<b>Descripción</b>	Comprobación de la distribución de una política a un aula mediante la herramienta PolGest.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Distribución de una política a un aula realizada correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecución de PolGest en el servidor políticas.</li> <li>2. Selección de aula H02.</li> <li>3. Pulsar botón <i>Cambiar Políticas Aula</i>.</li> <li>4. Seleccionar una política para cada objeto.</li> <li>5. Comprobar que en la dirección de red \\ldap\sysvol\policies\aulas\H02 se han creado los accesos directos (computer, user y useradm) a la política configurada.</li> </ol>
<b>Precondiciones</b>	Debe existir, al menos, una política en el almacén.

Tabla 6.36. PRU-036 Distribución de política a un aula.

PRU-037	Distribución de política a un equipo
<b>Descripción</b>	Comprobación de la distribución de una política a un equipo mediante la herramienta PolGest.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Distribución de una política a un equipo realizada correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecución de PolGest en el servidor políticas.</li> <li>2. Selección de aula H02.</li> <li>3. Pulsar botón <i>Cambiar Políticas Equipo</i>.</li> <li>4. Seleccionar el equipo h50 y configurar una política para cada objeto.</li> <li>5. Comprobar que en la dirección de red \\ldap\sysvol\policies\equipos\H02\h50 se han creado los accesos directos (computer, user y useradm) a la política configurada.</li> </ol>
<b>Precondiciones</b>	Debe existir, al menos, una política en el almacén.

Tabla 6.37. PRU-037 Distribución de política a un equipo.

<b>PRU-038</b>	<b>Consulta de almacén de políticas</b>
<b>Descripción</b>	Comprobación de la consulta de las políticas almacenadas en el servidor.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Listado de las políticas almacenadas en el servidor.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecución de PolGest en el servidor políticas.</li> <li>2. Selección del botón ubicado a derecha con un icono azul.</li> </ol>
<b>Precondiciones</b>	Debe existir, al menos, una política en el almacén.

Tabla 6.38. PRU-038 Consulta de almacén de políticas.

<b>PRU-039</b>	<b>Distribución de tarea programada a un aula</b>
<b>Descripción</b>	Comprobación de la distribución de una tarea programada a un aula mediante la herramienta PolGest.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Distribución de una tarea programada a un aula realizada correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecución de PolGest en el servidor políticas.</li> <li>2. Selección de la pestaña <i>Tareas</i>.</li> <li>3. Selección de aula H02.</li> <li>4. Pulsar botón <i>Cambiar Tareas Aula</i>.</li> <li>5. Seleccionar una tarea programada de la lista.</li> <li>6. Comprobar que en la dirección de red \\ldap\sysvol\Tasks\aulas\H02 se han creado los accesos directos a la tarea programada configurada.</li> </ol>
<b>Precondiciones</b>	Debe existir, al menos, una tarea programada en el almacén.

Tabla 6.39. PRU-039 Distribución de tarea programada a un aula.



<b>PRU-040</b>	<b>Distribución de tarea programada a un equipo</b>
<b>Descripción</b>	Comprobación de la distribución de una tarea programada a un equipo mediante la herramienta PolGest.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Distribución de una tarea programada a un equipo realizada correctamente.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecución de PolGest en el servidor políticas.</li> <li>2. Selección de la pestaña <i>Tareas</i>.</li> <li>3. Selección de aula H02.</li> <li>4. Pulsar botón <i>Cambiar Tareas Equipo</i>.</li> <li>5. Seleccionar el equipo h50 y configurar una tarea programada de la lista.</li> </ol> <p>Comprobar que en la dirección de red \\ldap\sysvol\Tasks\equipos\H02\h50 se han creado los accesos directos a la tarea programada configurada.</p>
<b>Precondiciones</b>	Debe existir, al menos, una tarea programada en el almacén.

Tabla 6.40. PRU-040 Distribución de tarea programada a un equipo.

<b>PRU-041</b>	<b>Consulta de almacén de tareas programadas</b>
<b>Descripción</b>	Comprobación de la consulta de las tareas programadas almacenadas en el servidor.
<b>Entrada</b>	Ninguna.
<b>Salida</b>	Listado de las tareas programadas almacenadas en el servidor.
<b>Secuencia</b>	<ol style="list-style-type: none"> <li>1. Ejecución de PolGest en el servidor políticas.</li> <li>2. Selección de la pestaña <i>Tareas</i>.</li> <li>3. Selección del botón ubicado a derecha con un icono azul.</li> </ol>
<b>Precondiciones</b>	Debe existir, al menos, una tarea programada en el almacén.

Tabla 6.41. PRU-041 Consulta de almacén de tareas programadas.



# Capítulo 7

## Presupuesto y planificación

En este capítulo se va a incluir la estimación, planificación detallada y presupuesto del proyecto realizado.

### 7.1. Estimación

A continuación se va a proceder a realizar la estimación del software del proyecto. Esta estimación se va a realizar fundamentalmente en dos fases:

- Una primera fase en la cual se estimen los puntos de función del proyecto en base al diseño de arquitectura de la red del apartado 4.2.1.
- Una segunda fase utilizando el modelo COCOMOII<sup>[40]</sup> para estimar el esfuerzo necesario relativo a estos puntos de función calculados.

Por lo tanto se parte del siguiente diseño arquitectónico de red para realizar la estimación:

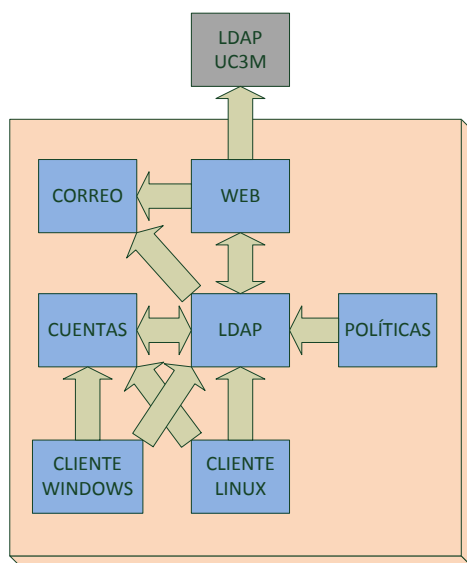


Figura 7.1. Estructura del sistema.

Hay que tener en cuenta que no todos los subsistemas especificados en el diseño van a contar con un esfuerzo o líneas de código estimadas. Se evaluará únicamente los subsistemas que serán modificados sustancialmente, despreciando el esfuerzo invertido en la configuración de los subsistemas menos importantes.

Por lo que se estimará sobre los siguientes subsistemas:

- **WEB:** Aplicaciones de gestión de cuenta de usuario.
- **LDAP:** Servidor central de autenticación.
- **CUENTAS:** Servidor central de datos.
- **CLIENTE WINDOWS:** Cliente de las aulas con sistema operativo Windows.
- **CLIENTE LINUX:** Cliente de las aulas con sistema operativo Linux.

Se ha despreciado también la estimación del subsistema POLÍTICAS ya que se trata de una aplicación existente que ha sido integrada en el sistema total. Nótese que tampoco se tiene en cuenta el subsistema LDAP UC3M ya que se trata de un elemento externo.

Es importante también señalar que se ha aplicado, como se puede ver, un método de estimación de software a un proyecto que tiene el desarrollo de un conjunto de *scripts* como elemento secundario. Sin embargo la estimación ha sido realizada de tal modo que se tiene en cuenta también la instalación y puesta en marcha de los servicios.

### 7.1.1. Estimación del tamaño

Como se ha comentado, esta primera parte se hará con la estimación por puntos de función<sup>[39]</sup> sobre estos cinco subsistemas a evaluar. Los resultados obtenidos han sido los siguientes:

- **WEB:** Aplicaciones de gestión de cuentas de usuario.
  - Internal Logical Files:
    - 2 Ficheros de complejidad baja que guardan los datos de usuario y las contraseñas para la gestión de usuarios.
  - External Interface Files:
    - 1 Fichero de complejidad alta con muchos campos de datos de usuario que se consultará del subsistema externo LDAP UC3M.
  - External Input:
    - 3 Entradas en forma de formularios de complejidad baja (Alta de usuario, modificación de contraseña y estado de la cuenta).
  - External Output:
    - 1 Salida de complejidad media debido al envío de un correo al usuario.
    - 3 Salidas por pantalla de resultado de operaciones de usuario
  - External Inquiry:
    - 1 Consulta externa a LDAP UC3M para saber los datos de usuario.
    - 1 Consulta externa a LDAP para saber si el usuario existe.
- **LDAP:** Servidor central de autenticación.
  - Internal Logical Files:
    - 1 Fichero interno de complejidad alta correspondiente a los datos internos LDAP.
    - 1 Fichero de complejidad alta correspondiente al backup de datos.
    - 1 Fichero de complejidad media con las configuraciones de clientes Windows.
  - External Interface Files
    - 2 ficheros de complejidad baja que consulta del subsistema WEB.

- External Input:
    - 1 Entrada de complejidad baja desde el subsistema WEB.
    - 1 Entrada de complejidad baja desde el subsistema POLÍTICAS.
    - 2 Entradas de complejidad baja que incluyen perfiles y configuración de clientes.
    - 1 Entrada de complejidad baja desde el CLIENTE LINUX.
  - External Output:
    - 1 Salida de complejidad baja que crea los datos iniciales de usuario en el subsistema CUENTAS.
    - 1 Salida de complejidad media para la creación de cuentas desde el subsistema WEB.
  - External Inquiry: Ninguna.
- **CUENTAS:** Servidor central de datos.
    - Internal Logical Files: Ninguno
    - External Interface Files:
      - 1 Fichero de complejidad alta que consulta del subsistema LDAP.
    - External Input:
      - 1 Entrada de complejidad baja que crea el espacio de usuario desde el subsistema LDAP.
      - 2 Entradas de complejidad baja de autenticación de CLIENTE WINDOWS y LINUX.
    - External Output: Ninguna.
    - External Inquiry
      - 1 Consulta de complejidad baja para autenticar usuario en el subsistema LDAP.
  - **CLIENTE WINDOWS:** Cliente de las aulas con sistema operativo Windows.
    - Internal Logical Files:
      - 1 Fichero de complejidad media correspondiente a la planificación de tareas del cliente.
      - 1 Fichero de complejidad alta correspondiente a las políticas del equipo.
    - External Interface Files:
      - 1 Fichero de complejidad alta que consulta del subsistema LDAP.

- 1 Fichero de complejidad media con las configuraciones de clientes Windows.
- External Input: Ninguna.
- External Output: Ninguna.
- External Inquiry:
  - 3 Consultas de complejidad baja correspondientes a autenticación, perfiles y políticas de usuario.
- **CLIENTE LINUX:** Cliente de las aulas con sistema operativo Linux.
  - Internal Logical Files: Ninguno.
  - External Interface Files:
    - 1 Fichero de complejidad alta que consulta del subsistema LDAP.
  - External Input: Ninguna.
  - External Output: Ninguna.
  - External Inquiry:
    - 2 Consultas de complejidad baja correspondientes a autenticación y datos de usuario.

Finalmente se contará por lo tanto con los siguientes puntos de función y líneas de código asociadas:

Módulo	Puntos de función	Líneas de código	Lenguaje de programación
<b>Web</b>	56	1176	Perl
<b>Ldap</b>	74	1554	Shell Script
<b>Cuentas</b>	22	462	Shell Script
<b>C.Windows</b>	51	1479	Visual Basic
<b>C.Linux</b>	16	336	Shell Script
<b>TOTAL</b>	<b>219</b>	<b>5007</b>	

Tabla 7.1. Resumen de la estimación del tamaño.

Los puntos de función se han calculado con la herramienta COCOMOII introduciendo la información del sistema. Debido a que la herramienta COCOMOII no dispone de todos los lenguajes de programación existentes en la actualidad, los lenguajes de programación asignados a cada módulo se han basado en la complejidad del lenguaje de programación utilizado en el desarrollo.

### 7.1.2. Estimación del esfuerzo

Una vez hallado el tamaño de los subsistemas a realizar, se va a utilizar COCOMOII para estimar el esfuerzo necesario para la realización del proyecto.

El modelo de COCOMOII que más se aproxima al proyecto realizado es *Early Design*, que tiene en cuenta cinco factores de escala y siete multiplicadores de esfuerzo por cada módulo.

Los factores de escala han sido fijados del siguiente modo:

- **Precedentes:** Se considera este valor como alto ya que se ha trabajado durante bastante tiempo sobre sistemas similares.
- **Flexibilidad de desarrollo:** Al tratarse de un trabajo interno del laboratorio se considera que se cuenta con una alta flexibilidad de desarrollo.
- **Cohesión del equipo:** Se considera que el equipo del laboratorio va a aportar facilidades en el desarrollo del proyecto, por lo que se fija este valor a alto.

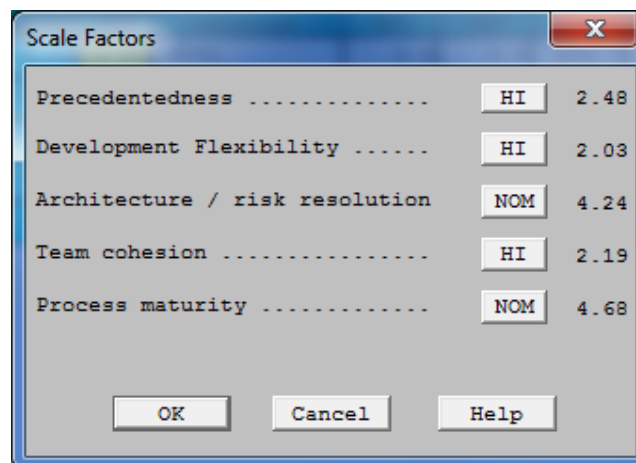


Figura 7.2. Factores de escala.



Los multiplicadores de esfuerzo de cada módulo son los siguientes:

▪ **WEB:**

- Complejidad: Se considera un módulo con complejidad muy baja.
- Reusabilidad: No se contempla reusabilidad en el código.
- Capacidad del personal de desarrollo: Se considera que la capacidad del personal de desarrollo debe ser muy alta.

The screenshot shows a dialog box titled "EAF - Web". It contains a table of effort factors for various categories. The formula "base + incr % = rating" is displayed at the top. The categories and their values are:

	RCPX	RUSE	PDIF	PERS	PREX	FCIL	USR1	USR2
base	VLO	LO	NOM	VHI	NOM	NOM	NOM	NOM
Incr%	0%	0%	0%	0%	0%	0%	0%	0%

Below the table, it states "EAF is also affected by Schedule". The calculated EAF value is shown as 0.36. At the bottom, there are buttons for "OK", "Cancel", and "Help".

Figura 7.3. Factores de escala correspondientes al módulo Web.

▪ **LDAP:**

- Complejidad: Se considera un módulo con complejidad alta.
- Experiencia del personal: Se considera que se requiere una alta experiencia del personal.

The screenshot shows a dialog box titled "EAF - ldap". It contains a table of effort factors for various categories. The formula "base + incr % = rating" is displayed at the top. The categories and their values are:

	RCPX	RUSE	PDIF	PERS	PREX	FCIL	USR1	USR2
base	HI	NOM	NOM	NOM	HI	NOM	NOM	NOM
Incr%	0%	0%	0%	0%	0%	0%	0%	0%

Below the table, it states "EAF is also affected by Schedule". The calculated EAF value is shown as 1.16. At the bottom, there are buttons for "OK", "Cancel", and "Help".

Figura 7.4. Factores de escala correspondientes al módulo Ldap.

▪ **CUENTAS:**

- Dificultad de uso de la plataforma: Se considera que el uso de la plataforma es bajo.
- Facilidades de desarrollo: Se considera que las facilidades de desarrollo es alto.

base + incr % = rating

	RCPX	RUSE	PDIF	PERS	PREX	FCIL	USR1	USR2
base	NOM	NOM	LO	NOM	NOM	HI	NOM	NOM
Incr%	0%	0%	0%	0%	0%	0%	0%	0%

EAF is also affected by Schedule

EAF: 0.76

OK Cancel Help

Figura 7.5. Factores de escala correspondientes al módulo Cuentas.

▪ **CLIENTE WINDOWS:**

- Capacidad del personal: Se considera que la capacidad del personal debe ser muy alta.
- Experiencia del personal: Se considera que la experiencia del personal debe ser muy alta.

base + incr % = rating

	RCPX	RUSE	PDIF	PERS	PREX	FCIL	USR1	USR2
base	NOM	NOM	NOM	VHI	VHI	NOM	NOM	NOM
Incr%	0%	0%	0%	0%	0%	0%	0%	0%

EAF is also affected by Schedule

EAF: 0.47

OK Cancel Help

Figura 7.6. Factores de escala correspondientes al módulo Cliente Windows.

- **CLIENTE LINUX:**
  - Capacidad del personal: Se considera que la capacidad del personal debe ser muy alta.
  - Experiencia del personal: Se considera que la experiencia del personal debe ser muy alta.

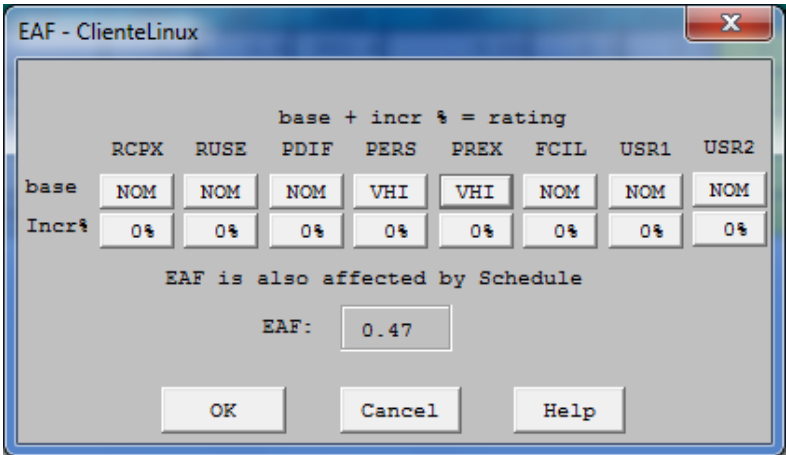


Figura 7.7. Factores de escala correspondientes al módulo Cliente Linux.

El resultado de la introducción de todos los datos mencionados anteriormente en la herramienta COCOMOII se puede observar en la siguiente figura.

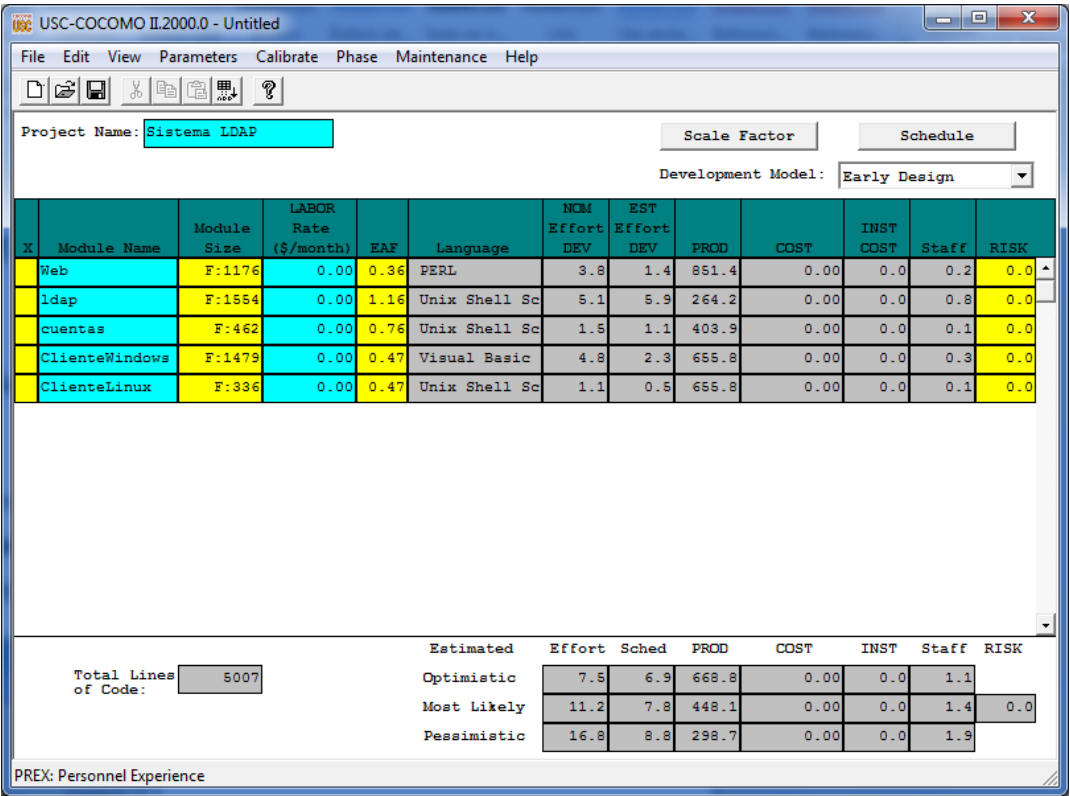


Figura 7.8. Estimación del esfuerzo del proyecto.

---

Como se puede observar el resultado más optimista en la estimación realizada es que el trabajo podría ser realizado por una persona en aproximadamente 7 meses. En el caso de este proyecto, como se podrá ver en las conclusiones, los resultados pueden considerarse similares. También se destaca que las líneas de código implementadas estimadas serán 5000 aproximadamente, este dato también será contrastado en las conclusiones.

## 7.2. Planificación

La planificación llevada a cabo durante el desarrollo del proyecto se va a mostrar siguiendo primero una lista de tareas llevadas a cabo, y posteriormente un diagrama de Gantt más explicativo:

La duración del proyecto ha sido de aproximadamente 15 meses. El comienzo del mismo ha sido en Junio de 2011 y la finalización en Septiembre de 2012. A continuación se muestran las tareas realizadas junto con el tiempo llevado a cabo y el periodo que ha comprendido:

- **Propuesta del proyecto:** Tarea de análisis de la viabilidad del proyecto y refinamiento de los objetivos del mismo.
- **Análisis:** Tareas de estudio y desglose de todos los aspectos a considerar sobre el proyecto, y definición de las características y requisitos del proyecto.
  - Definición del problema.
  - Definición de características generales.
  - Definición de requisitos.
- **Diseño:** Tareas relativas a la creación del diseño de la arquitectura de red del nuevo sistema de autenticación.
- **Implantación:** Tareas de puesta en producción del sistema de autenticación.
  - Fase I: Las cuentas de tipo asignatura (Windows) utilizan el nuevo sistema de autenticación (SAMBA-LDAP) y las cuentas de usuario (Linux) utilizan el antiguo sistema de autenticación (NIS).
  - Fase II: Las cuentas de tipo asignatura (Windows) utilizan el nuevo sistema de autenticación (SAMBA-LDAP) y las cuentas de usuario (Linux) utilizan el nuevo sistema de autenticación (LDAP).
  - Fase III: Se eliminan las cuentas de tipo asignatura. Todos los usuarios deben tener cuenta propia. Todos los clientes (Linux y Windows) utilizan el nuevo sistema de autenticación (SAMBA-LDAP).

- 
- **Pruebas del sistema:** Tareas de validación del sistema completo.
  - **Documentación:** Tarea de documentación del proyecto.

A continuación se muestra el diagrama de Gantt que muestra de manera gráfica las tareas descritas anteriormente.

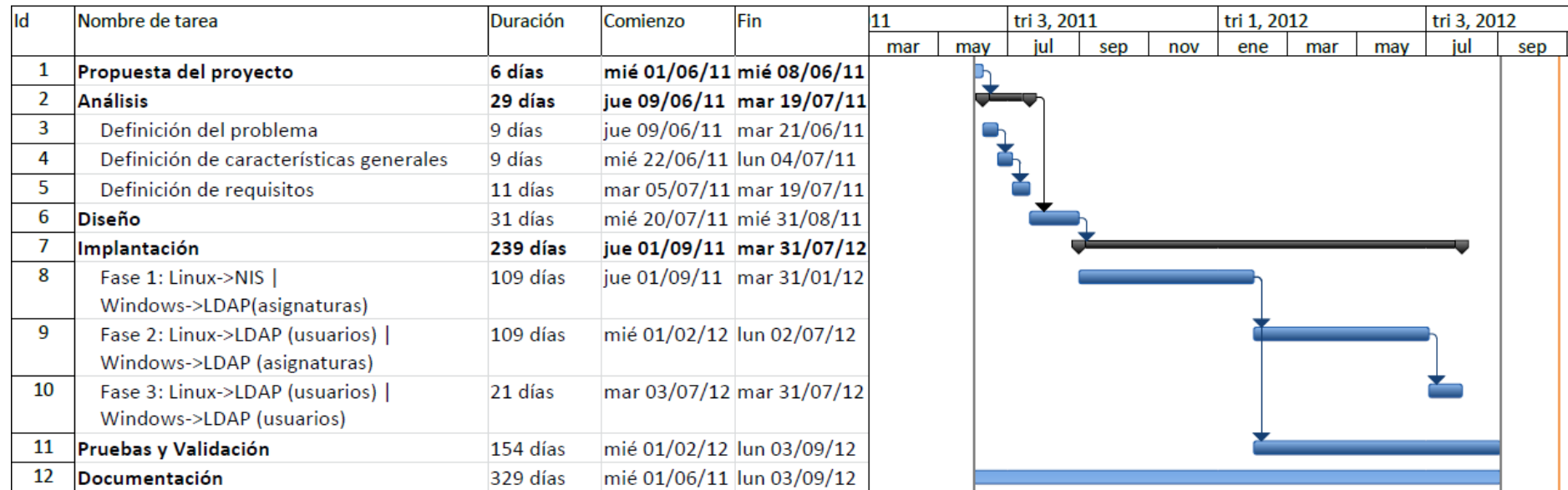


Figura 7.9. Diagrama de Gantt del proyecto.

## 7.3. Presupuesto

En este apartado se va a realizar una estimación de los gastos que han supuesto la realización de este proyecto. El desglose del presupuesto se realiza en distintas categorías, con el objetivo de conseguir el mayor detalle posible en el mismo. Es importante destacar que todos los precios incluidos en el desglose no incluyen el IVA, siendo éste calculado con IVA al final en los costes totales del proyecto.

El desglose del presupuesto del proyecto es el siguiente:

- Costes de personal.
- Costes de material inventariable.
- Costes de software.

### 7.3.1. Costes de personal

En el proyecto sólo ha participado un ingeniero senior durante los 15 meses de duración del proyecto. Se han trabajado un total de 329 días como se puede apreciar en el diagrama de Gantt realizado en la planificación, y se ha estimado que se han trabajado durante 4 horas por día laborable.

El precio estimado por hora para cada nivel de retribución involucrada en el proyecto es de 60 €/hora. Este valor se ha estimado calculando la media de precios de contratación existentes para un ingeniero senior en la actualidad.

El coste asociado al personal es el siguiente:

Concepto	Salario/hora	Días laborables	Horas trabajadas al día	Total
Ingeniero Senior	60,00€/hora	329 días	4 horas/día	78.960,00€
<b>TOTAL</b>				<b>78.960,00€</b>

Tabla 7.2. Costes de personal.



### 7.3.2. Costes de material inventariable

En este apartado se incluye el material utilizado de carácter inventariable. En el coste de este tipo de material se tendrá en cuenta la amortización que hay que aplicarle.

El coste de los servidores no está incluido en este apartado debido a que dicho material ya está amortizado.

Nombre	Precio unitario	Unidades	Amortización unidad/mes <sup>1</sup>	Meses	Total
<b>PC Sobremesa 8GB RAM/ HDD 1TB</b>	600€	1	12,5€	15	187,50€
<b>Impresora HP 2420</b>	300€	1	6,25€	15	93,75€
<b>TOTAL</b>					<b>281,25€</b>

Tabla 7.3. Costes de material inventariable

### 7.3.3. Costes de software

En este apartado se va a reflejar el coste relacionado con las licencias de software utilizadas. Debido a que el Departamento de informática tiene un acuerdo con Microsoft, el coste de las licencias utilizadas es cero euros. Aun así, se ha calculado el coste de las licencias en el hipotético caso de que el proyecto no hubiera sido en un entorno académico.

Concepto	Cantidad	Coste/unidad	Total
<b>Microsoft Windows 7 Professional</b>	97	309,99€	30.069,03€
<b>Microsoft Office 2010 Professional</b>	1	499,00€	499,00€
<b>Microsoft Project 2010 Professional</b>	1	1067,00€	1067,00€

<sup>1</sup> La amortización aplicada a los equipos informáticos es de 4 años.

<b>Debian GNU/Linux 6.0</b>	120	0€	0€
<b>Apache Web Server</b>	1	0€	0€
<b>Microsoft Windows 2003 Server Enterprise Edition</b>	1	793,02€	793,02€
<b>TOTAL</b>			<b>32.428,05€</b>

Tabla 7.4. Costes de software.

### 7.3.4. Coste total

Finalmente, se realiza la suma de todas las categorías, y se agrega un porcentaje para cubrir los riesgos que puedan surgir en el proyecto, y un porcentaje en concepto de beneficio. El presupuesto final es por tanto, el siguiente.

Concepto	Total
Costes de personal	78.960,00€
Costes de material inventariable	281,25€
Costes de software	32.428,05€
<b>Subtotal</b>	<b>111.669,30€</b>
<b>Riesgo (20%)</b>	<b>22.333,86€</b>
<b>Beneficio (25%)</b>	<b>27.917,33€</b>
<b>Total</b>	<b>161.920,49€</b>
<b>IVA (21%)</b>	<b>34.003,30€</b>
<b>TOTAL con IVA</b>	<b><u>195.923,79€</u></b>

Tabla 7.5. Coste total.

El presupuesto total de ejecución de este proyecto asciende a la cantidad de **CIENTO SESENTA Y UN MIL NOVECIENTOS VEINTE CON CUARENTA Y NUEVE EUROS** sin incluir el impuesto sobre el valor añadido.

Incluyendo el IVA vigente al 21%, el coste total es de **CIENTO NOVENTA Y CINCO MIL NOVECIENTOS VEINTITRÉS CON SETENTA Y NUEVE EUROS**.

# Capítulo 8

## Conclusiones y trabajos futuros

En este apartado se resumen las conclusiones e ideas que se han obtenido en la realización de este proyecto, y posteriormente son analizadas las líneas de investigación futuras, con las cuales podríamos continuar, mejorar y avanzar este proyecto.

Para comenzar se va a observar desde un punto de vista técnico, donde se ve si se han logrado alcanzar las metas del proyecto, y posteriormente se va a observar desde un punto de vista personal.

### 8.1. Conclusiones

La principal conclusión que se puede obtener de este proyecto es que se ha conseguido desplegar con éxito un nuevo sistema de autenticación que facilita la gestión de la cuenta al usuario y la administración al personal del ldi.

Además se ha conseguido mejorar la seguridad completa del sistema gracias a la identificación del usuario en el servidor del ldap de la universidad. Otro objetivo muy importante que se ha cumplido es que se ha conseguido facilitar la gestión de su cuenta al usuario gracias a la integración de las aplicaciones web con el sistema de autenticación.

En relación con el nuevo dominio de Windows, se ha conseguido paliar en gran medida las carencias de la falta de un servidor con *Active Directory*. Gracias al conjunto de *scripts* realizados, se puede distribuir de forma automática y transparente nuevas políticas de grupo a los clientes seleccionados de las aulas informáticas. De la misma manera se pueden añadir y eliminar tareas programas a cualquier equipo de las aulas informáticas.

En relación a la estimación del proyecto, se muestra a continuación una tabla con las diferencias entre las líneas de código estimadas y reales.

Módulo	Líneas de código estimadas	Líneas de código reales	Desviación (%)
<b>Web</b>	1176	1407	19,64
<b>Ldap</b>	1554	2094	34,74
<b>Cuentas</b>	462	0	100
<b>C.Windows</b>	1479	759	51,31
<b>C. Linux</b>	336	0	100
<b>TOTAL</b>	<b>5007</b>	<b>4260</b>	<b>17,53</b>

Tabla 8.1. Comparación de las líneas de código estimadas y reales.

De los datos mostrados en la tabla anterior se puede concluir lo siguiente:

- Los módulos cuentas y cliente Linux no tiene ninguna línea de código real debido a que no se ha desarrollado ningún software.
- La estimación de los módulos web y ldap han sido ligeramente optimista comparada con la realidad.

Si se observa las líneas de código totales, la estimación se aproxima mucho a la realidad y se puede dar por buena teniendo en cuenta que en esta comparación no se ha incluido el esfuerzo necesario para la instalación y configuración de dichos módulos. En relación al esfuerzo y tiempo necesario para completarlo, también se aproxima mucho a la realidad debido a que la estimación era de 7 meses x 1 persona a tiempo completo y en realidad ha sido 15 meses x 1 persona a media jornada.

En resumen, este proyecto fin de carrera ha conseguido crear un entorno de autenticación completo y centralizado fácil de gestionar y válido para varios sistemas operativos.

En cuanto a las conclusiones personales, este proyecto me ha parecido muy completo ya que he podido aplicar la mayoría de los conocimientos adquiridos en la carrera, desde la aplicación de la ingeniería del software para la realización de este documento hasta la aplicación de los sistemas operativos.

Por otro lado considero que el nuevo sistema de autenticación ha contribuido a mejorar el procedimiento de creación y gestión de la cuenta de usuario. Desde que el sistema está en producción se ha podido observar que los

alumnos han agradecido que se pueda acceder a los datos de su cuenta desde el sistema operativo Windows y que se haya unificado las credenciales de acceso a su cuenta.

## 8.2. Trabajos futuros

Los trabajos futuros que se plantean para mejorar el sistema de autenticación instalado son los siguientes:

- **Instalación de servidor ldap esclavo:** Se propone la instalación de otro servidor ldap de apoyo al principal para balancear la carga. Dicho servidor puede ser necesario en el caso de que aumente el número de equipos y servicios ofrecidos por el ldi.
- **Instalación de Samba 4:** Se propone la instalación, cuando sea estable y esté suficiente probada, de la versión 4 del software Samba. Dicho software permitirá simplificar el sistema debido a la integración de las políticas de grupo.
- **Escalabilidad de los scripts de políticas y tareas:** Se propone una generalización de los *scripts* de políticas y tareas para que sean útiles para cualquier cambio de distribución de las aulas informáticas.
- **Control de acceso:** Se propone añadir un registro centralizado de control de acceso de los usuarios a los clientes de las aulas informáticas. De esta manera se podrá saber el/los usuario/s que han utilizado cada cliente de las aulas informáticas en todo momento. Dicha información también puede ser útil para realizar un mantenimiento más exhaustivo a los equipos que más horas de uso han tenido.
- **Integración del software Ifolder con el sistema de autenticación:** Se propone la integración del software Ifolder con el nuevo sistema de autenticación debido a que el actualmente está configurado de manera manual con usuarios y contraseñas independientes del resto del sistema de autenticación del ldi.

- **Integración de un servicio de autenticación para la red inalámbrica del ldi:** Se propone la integración de un servicio de autenticación para la red inalámbrica del ldi. Actualmente dicho servicio está configurado con una clave compartida. La instalación de dicho servicio mejoraría sustancialmente la seguridad de la red.
- **Creación de scripts genéricos para gestión masiva de usuarios:** Se propone la creación de *scripts* genéricos de gestión masiva de usuarios. Dichos scripts serían útiles para realizar modificaciones en los datos de los usuarios o realizar consultas de los mismos para el desarrollo de informes.
- **Realización de encuestas de satisfacción de usuario:** Se propone la realización de encuestas a los usuarios del ldi para conocer el nivel de satisfacción de los usuarios con las nuevas funcionalidades ofrecidas por el nuevo sistema de autenticación y en qué aspectos es mejorable el sistema.
- **Autenticación en máquinas virtuales instaladas en los clientes:** Se propone la integración de la autenticación en las máquinas virtuales instaladas en los clientes de las aulas informáticas para la elaboración de informes de uso. De esta manera se puede optimizar el espacio ocupado en los clientes debido a que se espera que los informes ayuden a conocer de manera precisa las máquinas virtuales que realmente son utilizadas y los periodos de tiempo.
- **Integración de la autenticación en otro tipo de clientes:** Se propone la realización de un estudio de la integración del sistema de autenticación en otro tipo de clientes, como por ejemplo, dispositivos móviles.

# Capítulo 9

## Acrónimos y abreviaturas

- **NIS:** Network Information Service.
- **YP:** Yellow Pages.
- **GNU:** GNU is Not Unix.
- **NYS:** NIS/YP with Switches.
- **LDAP:** Lightweight Directory Access Protocol.
- **ITU:** Unión Internacional de Telecomunicaciones.
- **DAP:** Directory Access Protocol.
- **OSI:** Open Systems Interconnection.
- **TCP:** Transmission Control Protocol.
- **IP:** Internet Protocol.
- **TLS:** Transport Layer Security.
- **URL:** Uniform Resource Locator.
- **SSL:** Secure Sockets Layer.
- **DN:** Distinguished Name.
- **RDN:** Relative Distinguished Name.
- **UUID:** Universally Unique Identifier
- **LDIF:** LDAP Data Interchange Format.
- **CN:** Common Name.
- **SN:** Surname.
- **DC:** Domain Component.
- **UID:** Unique Identification Number.
- **BSD:** Berkeley Software Distribution.
- **AIX:** Advanced Interactive eXecutive.
- **OS:** Operating System.
- **HP-UX:** Hewlett-Packard UniX.
- **ITDS:** IBM Tivoli Directory Server.
- **AD:** Active Directory.
- **DNS:** Domain Name System.
- **DHCP:** Dynamic Host Configuration Protocol.
- **NTFS:** New Technology File System.

- **NT**: New Technology.
- **PC**: Personal Computer.
- **IIS**: Internet Information Services.
- **DVD**: Digital Versatile Disc.
- **AT&T**: American Telephone and Telegraph.
- **GCC**: GNU Compiler Collection.
- **POSIX**: Portable Operating System Interface.
- **FSF**: Free Software Foundation.
- **FAT**: file allocation table.
- **JFS**: Journaling File System.
- **UDF**: Universal Disk Format.
- **ISO**: International Organization for Standardization.
- **PPC**: PowerPC.
- **USB**: Universal Serial Bus.
- **KVM**: Kernel-based Virtual Machine.
- **VT**: Virtualization Technology.
- **CPU**: Central Processing Unit.
- **ARM**: Advanced RISC Machine.
- **MIPS**: Microprocessor without Interlocked Pipeline Stages.
- **SPARC**: Scalable Processor ARChitecture.
- **IBM**: International Business Machines.
- **API**: Application Programming Interface.
- **MMU**: Memory Management Unit.
- **AMD**: Advanced Micro Devices.
- **TLB**: Translation Lookaside Buffer.
- **MB**: MegaByte.
- **LVM**: Logical Volume Manager.
- **RAM**: Random-Access Memory
- **HTML**: HyperText Markup Language.
- **HTTP**: Hypertext Transfer Protocol.
- **FTP**: File Transfer Protocol.
- **HTTPS**: Hyper Text Transfer Protocol Secure.
- **FTPS**: FTP Secure.
- **SMTP**: Simple Mail Transfer Protocol.
- **NNTP**: Network News Transport Protocol.
- **SMB**: Server Message Block.
- **CIFS**: Common Internet File System.
- **PDC**: Primary Domain Controller.
- **BDC**: Backup Domain Controller.
- **MSRPC**: Microsoft Remote Procedure Call.



- **RCP:** Remote Procedure Call.
- **DCE:** Remote Procedure Call.
- **NBNS:** NetBIOS.
- **WINS:** Windows Internet Naming Service.
- **SAM:** Security Accounts Manager.
- **LSA:** Local Security Authority.
- **LAN:** Local Area Network.
- **NTLM:** NT LAN Manager.
- **XDR:** eXternal Data Representation.
- **NFS:** Network File System.
- **CD-ROM:** Compact Disc - Read Only Memory.
- **LDI:** Laboratorio del Departamento de Informática.
- **NIA:** Número de Identificación de Alumnado.
- **CU:** Caso de Uso.
- **RSF:** Requisitos Software Funcionales.
- **RSR:** Requisitos Software de Rendimiento.
- **RSI:** Requisitos Software de Interfaz.
- **RSO:** Requisitos Software de Operación.
- **RSRe:** Requisitos Software de Recursos.
- **RSC:** Requisitos Software de Comprobación.
- **RSS:** Requisitos Software de Seguridad.
- **RSFi:** Requisitos Software de Fiabilidad.
- **HDD:** Hard Disk Drive.



# Capítulo 10

## Bibliografía y referencias

- [1] Enciclopedia sobre Network Information Service (Español). 2012. Disponible:  
[http://es.wikipedia.org/wiki/Network\\_Information\\_Service](http://es.wikipedia.org/wiki/Network_Information_Service)
- [2] ONC+ Developer's Guide (Inglés). 2002. Disponible:  
<http://docs.oracle.com/cd/E19683-01/816-1435/816-1435.pdf>
- [3] Enciclopedia sobre Lightweight Directory Access Protocol (Español). 2012. Disponible:  
<http://es.wikipedia.org/wiki/LDAP>
- [4] Enciclopedia sobre *Active Directory* (Español). 2012. Disponible:  
[http://es.wikipedia.org/wiki/Active\\_Directory](http://es.wikipedia.org/wiki/Active_Directory)
- [5] Enciclopedia sobre Windows XP (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Windows\\_XP](http://en.wikipedia.org/wiki/Windows_XP)
- [6] Enciclopedia sobre Ediciones de Windows XP (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Windows\\_XP\\_editions](http://en.wikipedia.org/wiki/Windows_XP_editions)
- [7] Enciclopedia sobre Windows Vista (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Windows\\_Vista](http://en.wikipedia.org/wiki/Windows_Vista)
- [8] Enciclopedia sobre versiones de Windows Vista (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Windows\\_Vista\\_editions](http://en.wikipedia.org/wiki/Windows_Vista_editions)
- [9] Enciclopedia sobre Windows 7 (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Windows\\_7](http://en.wikipedia.org/wiki/Windows_7)
- [10] Enciclopedia sobre ediciones de Windows 7 (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Windows\\_7\\_editions](http://en.wikipedia.org/wiki/Windows_7_editions)
- [11] Enciclopedia sobre Windows Server 2008 (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Windows\\_Server\\_2008](http://en.wikipedia.org/wiki/Windows_Server_2008)
- [12] Enciclopedia sobre Unix (Inglés). 2012. Disponible:  
<http://en.wikipedia.org/wiki/Unix>
- [13] Enciclopedia sobre Linux (Inglés). 2012. Disponible:  
<http://en.wikipedia.org/wiki/Linux>

- 
- [14] Enciclopedia sobre Linux (Español). 2012. Disponible:  
<http://es.wikipedia.org/wiki/GNU/Linux>
  - [15] Enciclopedia sobre comparaciones de distribuciones Linux (Español). 2012. Disponible:  
[http://es.wikipedia.org/wiki/Anexo:Comparación\\_de\\_distribuciones\\_Linux](http://es.wikipedia.org/wiki/Anexo:Comparación_de_distribuciones_Linux)
  - [16] Enciclopedia sobre virtualización hardware (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Hardware\\_virtualization](http://en.wikipedia.org/wiki/Hardware_virtualization)
  - [17] Enciclopedia sobre virtualización (Inglés). 2012. Disponible:  
<http://en.wikipedia.org/wiki/Virtualization>
  - [18] Introducción a la virtualización (Inglés). 2004. Disponible  
<http://www.kernelthread.com/publications/virtualization/>
  - [19] Enciclopedia sobre VMware (Inglés). 2012. Disponible.  
<http://en.wikipedia.org/wiki/VMware>
  - [20] Enciclopedia sobre VMware Workstation (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/VMware\\_Workstation](http://en.wikipedia.org/wiki/VMware_Workstation)
  - [21] Enciclopedia sobre VMware Player (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/VMware\\_Player](http://en.wikipedia.org/wiki/VMware_Player)
  - [22] Enciclopedia sobre VMware Server (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/VMware\\_Server](http://en.wikipedia.org/wiki/VMware_Server)
  - [23] Enciclopedia sobre VMware ESX (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/VMware\\_ESX](http://en.wikipedia.org/wiki/VMware_ESX)
  - [24] Virtualización con KVM (Inglés). 2008. Disponible:  
<http://www.linuxjournal.com/article/9764>
  - [25] Rendimiento de la virtualización en Linux usando KVM (Inglés). 2012. Disponible:  
<http://www.phoronix.com/scan.php?page=article&item=623&num=4>
  - [26] Enciclopedia sobre Xen (Inglés). 2012. Disponible:  
<http://en.wikipedia.org/wiki/Xen>
  - [27] Funcionamiento de Xen (Español). 2007. Disponible:  
<http://pepssss.blogspot.com.es/2007/04/arquitectura-de-xen-antes-de-empezar.html>
  - [28] Enciclopedia sobre servidor web (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Web\\_server](http://en.wikipedia.org/wiki/Web_server)
  - [29] Enciclopedia sobre servidor http de Apache (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Apache\\_HTTP\\_Server](http://en.wikipedia.org/wiki/Apache_HTTP_Server)
  - [30] Enciclopedia sobre Internet Information Services (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Internet\\_Information\\_Services](http://en.wikipedia.org/wiki/Internet_Information_Services)
  - [31] Enciclopedia sobre Domain Name System (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Domain\\_Name\\_System](http://en.wikipedia.org/wiki/Domain_Name_System)
-

- 
- [32] Enciclopedia sobre Dynamic Host Configuration Protocol (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)
  - [33] Página oficial de los desarrolladores de SAMBA (Inglés). 2012. Disponible:  
<http://www.samba.org>
  - [34] Enciclopedia sobre SAMBA (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Samba\\_\(software\)](http://en.wikipedia.org/wiki/Samba_(software))
  - [35] Enciclopedia sobre Distributed file system (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Distributed\\_file\\_system](http://en.wikipedia.org/wiki/Distributed_file_system)
  - [36] Enciclopedia sobre Network File System (Inglés). 2012. Disponible:  
[http://en.wikipedia.org/wiki/Network\\_File\\_System](http://en.wikipedia.org/wiki/Network_File_System)
  - [37] Parches para los scripts smbldap-tools (Español). 2005. Disponible:  
<http://osl.ull.es/node/48>
  - [38] Estándar ESA (Inglés). 2012. Disponible:  
[http://www.esa.int/SPECIALS/Space\\_Engineering/SEMXXCR0P0WF\\_0.html](http://www.esa.int/SPECIALS/Space_Engineering/SEMXXCR0P0WF_0.html)
  - [39] Puntos de función (Español). 2012. Disponible:  
<http://www.upv.es/~jmontesa/eog/eog00at4.ppt>
  - [40] Página web COCOMOII (Inglés). 2012. Disponible:  
[http://sunset.usc.edu/csse/research/COCOMOII/cocomo\\_main.html](http://sunset.usc.edu/csse/research/COCOMOII/cocomo_main.html)



# Capítulo 11

## Apéndice

En este capítulo se recoge toda la información que se desea anexar al documento.

### 11.1. Ficheros de configuración

A continuación se anexan los ficheros de configuración referenciados en el documento.

#### 11.1.1. Servidor LDAP

Los archivos de configuración relevantes del servidor LDAP son los siguientes:

##### 11.1.1.1. */etc/hostname*

```
ldap
```

##### 11.1.1.2. */etc/network/interfaces*

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 163.117.142.173
gateway 163.117.142.2
netmask 255.255.255.0

auto eth1
iface eth1 inet static
address 10.0.142.173
netmask 255.255.255.0
```

**11.1.1.3. */etc/xen/ldap.cfg***

```

kernel      = '/boot/vmlinuz-2.6.32-5-xen-amd64'
ramdisk     = '/boot/initrd.img-2.6.32-5-xen-amd64'
memory      = 1024
extra       = 'TERM=xterm'
console     = 'hvc0'

root        = '/dev/xvda2 ro'
disk        = [
    'file:/xen-
machines/domains/ldap/swap.img,xvda1,w',
    'file:/xen-
machines/domains/ldap/disk.img,xvda2,w',
    'file:/xen-
machines/domains/ldap/disk2.img,xvda3,w',
]

name        = 'ldap'

vif         = [
    'mac=00:16:3E:1E:FC:AA, bridge=xenbr1,
ip=163.117.142.173',
    'mac=00:16:3E:1E:FD:AA,
bridge=xenbr0, ip=10.0.142.173' ]

on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash     = 'restart'

```

**11.1.1.4. */etc/ssh/sshd\_config***

```

Port 22

ListenAddress 10.0.142.229
Protocol 2

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key

UsePrivilegeSeparation yes

KeyRegenerationInterval 3600
ServerKeyBits 768

SyslogFacility AUTH
LogLevel INFO

LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes

```



```

IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no

PermitEmptyPasswords no

ChallengeResponseAuthentication no

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes

AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

UsePAM yes

```

#### 11.1.1.5. */etc/postfix/main.cf*

```

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no

append_dot_mydomain = no

readme_directory = no

smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database =
btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database =
btree:${data_directory}/smtp_scache

myhostname = lab.inf.uc3m.es
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = ldap, localhost.localdomain, localhost
relayhost = 10.0.142.245
mynetworks = 127.0.0.0/8
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = 10.0.142.173

```

#### 11.1.1.6. */etc/ldap/slapd.conf*

```

include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
include      /etc/ldap/schema/nis.schema
include      /etc/ldap/schema/misc.schema

```

---

```

include      /etc/ldap/schema/inetorgperson.schema
include      /etc/ldap/schema/samba.schema

pidfile      /var/run/slapd/slapd.pid
argsfile     /var/run/slapd/slapd.args
logfile      /var/log/slapd.log
loglevel     512

modulepath   /usr/lib/ldap
moduleload   back_hdb

sizelimit 50
tool-threads 1

TLSCACertificateFile /etc/ldap/ssl/cacert.pem
TLSCertificateKeyFile /etc/ldap/ssl/serverkey.pem
TLSCertificateFile /etc/ldap/ssl/servercert.pem
TLSVerifyClient never

backend      hdb

database     hdb
suffix       "dc=lab,dc=inf,dc=uc3m,dc=es"
rootdn       "cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es"
rootpw       -----

directory    "/var/lib/ldap"

dbconfig set_cachesize 0 2097152 0
dbconfig set_lk_max_objects 1500
dbconfig set_lk_max_locks 1500
dbconfig set_lk_max_lockers 1500

index objectClass eq
index                                     cn
pres,sub,eq
index                                     sn
pres,sub,eq
index                                     uid
pres,sub,eq
index displayname
pres,sub,eq
index default sub
index uidNumber eq
index gidNumber eq
index mail,givenName
eq,subinitial
index dc eq
index memberUid,uniqueMember eq
index sambaSID,sambaGroupType,sambaSIDList eq
index sambaPrimaryGroupSID,sambaDomainName eq

limits dn.exact="uid---,dc=lab,dc=inf,dc=uc3m,dc=es"
size=5000

```

---

```

lastmod      on
checkpoint   512 30

access to attrs=shadowLastChange
            by self write
            by * read
access to attrs=sambaLMPassword
            by self write
            by * auth
access to attrs=sambaNTPassword
            by self write
            by * auth
access to attrs=userPassword
            by self write
            by * auth
access to attrs=gecos
            by                                          dn="uid=---
,dc=lab,dc=inf,dc=uc3m,dc=es" read
            by self write
            by * auth
access to dn.base=""
            by self write
            by self read
            by * auth

access to *
            by                                          dn="uid=---
,dc=lab,dc=inf,dc=uc3m,dc=es" read
            by
dn="cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es" write
            by self read
            by * auth

```

#### 11.1.1.7. */etc/ldap/ldap.conf*

```

BASE      dc=lab,dc=inf,dc=uc3m,dc=es
URI        ldap://localhost

SIZELIMIT 50
TIMELIMIT 60
DEREF      always
TLS_REQCERT never

```

#### 11.1.1.8. *Fichero de creación de usuario ldap para realizar consultas*

```

dn: uid=---,dc=lab,dc=inf,dc=uc3m,dc=es
uid: ---
uidNumber: ---
gidNumber: ---
cn: ---
sn: ---
objectClass: top

```

```
objectClass: person
objectClass: shadowAccount
objectClass: posixAccount
homeDirectory: /home/---
```

#### 11.1.1.9. */etc/pam\_ldap.conf y /etc/libnss-ldap*

```
base dc=lab,dc=inf,dc=uc3m,dc=es
uri ldap://localhost
ldap_version 3
binddn uid=---,dc=lab,dc=inf,dc=uc3m,dc=es
bindpw contraseña
```

#### 11.1.1.10. */etc/nscd.conf*

debug-level	0		
paranoia	no		
enable-cache	passwd		no
positive-time-to-live	passwd		600
negative-time-to-live	passwd		20
suggested-size	passwd		211
check-files	passwd		yes
persistent	passwd		yes
shared	passwd		yes
max-db-size	passwd		33554432
auto-propagate	passwd		yes
enable-cache	group		no
positive-time-to-live	group		3600
negative-time-to-live	group		60
suggested-size	group		211
check-files	group		yes
persistent	group		yes
shared	group		yes
max-db-size	group		33554432
auto-propagate	group		yes
enable-cache	hosts		no
positive-time-to-live	hosts		3600
negative-time-to-live	hosts		20
suggested-size	hosts		211
check-files	hosts		yes
persistent	hosts		yes
shared	hosts		yes
max-db-size	hosts		33554432
enable-cache	services		no
positive-time-to-live	services		28800
negative-time-to-live	services		20
suggested-size	services		211
check-files	services		yes
persistent	services		yes

---

shared	services	yes
max-db-size	services	33554432

**11.1.1.11. /etc/nsswitch.conf**

```
passwd:      compat ldap
group:       compat ldap
shadow:      compat ldap

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

**11.1.1.12. /etc/rsyslog.conf**

```
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022

$IncludeConfig /etc/rsyslog.d/*.conf

local4.* -
/var/log/slapd.log
auth,authpriv.*
/var/log/auth.log
*.*;auth,authpriv.none;local4.none -
/var/log/syslog
daemon.* -
/var/log/daemon.log
kern.* -
/var/log/kern.log
lpr.* -
/var/log/lpr.log
mail.* -
/var/log/mail.log
user.* -
/var/log/user.log

mail.info -/var/log/mail.info
mail.warn -/var/log/mail.warn
mail.err /var/log/mail.err

news.crit /var/log/news/news.crit
```

---

```

news.err                /var/log/news/news.err
news.notice             -/var/log/news/news.notice

*.=debug;\
    auth,authpriv.none;\
    news.none;mail.none;local4.none      -
/var/log/debug
*.=info;*.=notice;*.=warn;\
    auth,authpriv.none;\
    cron,daemon.none;\
    mail,news.none                -/var/log/messages

*.emerg                  *

daemon.*;mail.*;\
    news.err;\
    *.=debug;*.=info;\
    *.=notice;*.=warn            |/dev/xconsole

```

#### 11.1.1.13. */etc/logrotate.d/slapd*

```

/var/log/slapd.log {
    rotate 35
    size 8192k
    create 0660 root root
    compress
}

```

#### 11.1.1.14. */etc/default/slapd*

```

SLAPD_CONF=
SLAPD_USER="openldap"
SLAPD_GROUP="openldap"
SLAPD_PIDFILE=
SLAPD_SERVICES="ldap:// ldaps://"
SLAPD_SENTINEL_FILE=/etc/ldap/noslapd
SLAPD_OPTIONS=""

```

#### 11.1.1.15. */etc/samba/smb.conf*

```

[global]
workgroup = LABINF
netbios name = LDAP
passdb backend = ldapsam:ldap://localhost
username map = /etc/samba/smbusers

add user script = /usr/sbin/smbldap-useradd -m '%u'
delete user script = /usr/sbin/smbldap-userdel %u
add group script = /usr/sbin/smbldap-groupadd -p '%g'
delete group script = /usr/sbin/smbldap-groupdel '%g'
add user to group script = /usr/sbin/smbldap-groupmod -m
'%u' '%g'

```

```
delete user from group script = /usr/sbin/smbldap-groupmod
-x '%u' '%g'
set primary group script = /usr/sbin/smbldap-usermod -g
'%g' '%u'
add machine script = /usr/sbin/smbldap-useradd -w '%u'

logon script = inicio-users.vbs
logon path = \\CUENTAS\\%U\\profile
logon drive = Z:
logon home = \\CUENTAS\\%U

interfaces      =      163.117.142.173/24      10.0.142.173/24
127.0.0.1/8
bind interfaces only = Yes

domain logons = Yes
preferred master = Yes
domain master = Yes
wins support = Yes
dns proxy = Yes
name resolve order = bcast host lmhosts wins

admin users= @"Domain Admins"
enable privileges = yes
security = user
encrypt passwords = true
kernel oplocks = no

ldap suffix = dc=lab,dc=inf,dc=uc3m,dc=es
ldap machine suffix = ou=Machines
ldap user suffix = ou=People
ldap group suffix = ou=groups
ldap idmap suffix = ou=idmap
ldap admin dn = cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es
ldap ssl = no
ldap passwd sync = Yes
idmap uid = 15000-20000
idmap gid = 15000-20000

load printers = no

; to maintain capital letters in shortcuts in any of the
profile folders:
preserve case = yes
short preserve case = yes
case sensitive = no
use spnego = yes
hosts allow = 163.117.142.0/24 10.0.142.0/24 127.0.0.1

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
Dos charset = 850
Unix charset = ISO8859-15

[netlogon]
```

```

        path = /users/windows/netlogon
        browseable = No
        write list = @"Domain Admins"
        guest ok = yes

[sysvol]
        path = /users/windows/sysvol
        browseable = No
        write list = @"Domain Admins"
        read only = yes
        guest ok = yes
        invalid users = @"alumnos", @"asignaturas",
@"profes", @"bdua", @"bscw"

[profiles]
        path = /users/windows/perfiles
        guest ok = yes
        read only = yes
        write list = @"Domain Admins"
        profile acls = Yes
        hide files =
        /desktop.ini/outlook*.lnk/*Briefcase*/*$RECYCLE.BIN*/

[asociados]
        path = /users/profes
        valid users = @"Domain Admins"
        write list = @"Domain Admins"

```

#### 11.1.1.16. /etc/smbldap-tools/smbldap.conf

```

SID="---"

sambaDomain="LABINF"
slaveLDAP="localhost"
slavePort="389"
masterLDAP="localhost"
masterPort="389"

ldapTLS="0"
verify=""
cafile=""
clientcert=""
clientkey=""

suffix="dc=lab,dc=inf,dc=uc3m,dc=es"
usersdn="ou=people,${suffix}"
computersdn="ou=machines,${suffix}"
groupsdn="ou=groups,${suffix}"
idmapdn="ou=idmap,${suffix}"
sambaUnixIdPoolIdn="sambaDomainName=LABINF,${suffix}"
scope="sub"

hash_encrypt="SSHA"
crypt_salt_format=""

```



```

userLoginShell="/bin/bash"
userHome="/homes/alumnos/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="210"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="99999"

userProfile="//ldap/profiles/perfil_comun_w7"

mailDomain="lab.inf.uc3m.es"
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"

```

#### **11.1.1.17. */etc/smbldap-tools/smbldap\_\_bind.conf***

```

slaveDN="cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es"
slavePw="contraseña"
masterDN="cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es"
masterPw="contraseña"

```

### **11.1.2. Servidor CUENTAS**

Los archivos de configuración relevantes del servidor CUENTAS son los siguientes:

#### **11.1.2.1. */etc/pam\_ldap.conf* y */etc/libnss-ldap***

```

base dc=lab,dc=inf,dc=uc3m,dc=es
uri ldap://ldap
ldap_version 3
binddn uid=---,dc=lab,dc=inf,dc=uc3m,dc=es
bindpw contraseña

```

#### **11.1.2.2. */etc/samba/smb.conf***

```

[global]
workgroup = LABINF
netbios name = CUENTAS
passdb backend = ldapsam:ldap://ldap
username map = /etc/samba/smbusers

add user script = /usr/sbin/smbldap-useradd -m '%u'
delete user script = /usr/sbin/smbldap-userdel %u
add group script = /usr/sbin/smbldap-groupadd -p '%g'
delete group script = /usr/sbin/smbldap-groupdel '%g'
add user to group script = /usr/sbin/smbldap-groupmod -m '%u' '%g'

```

```

delete user from group script = /usr/sbin/smbldap-groupmod
-x '%u' '%g'
set primary group script = /usr/sbin/smbldap-usermod -g
'%g' '%u'
add machine script = /usr/sbin/smbldap-useradd -w '%u'

logon script = inicio-users.vbs
logon path = \\CUENTAS%U\profile
logon drive = Z:
logon home = \\CUENTAS%U

interfaces      =      163.117.142.230/24      10.0.142.230/24
127.0.0.1/8
bind interfaces only = Yes

domain logons = Yes
preferred master = No
domain master = No
wins support = No
dns proxy = No
wins server = 10.0.142.173 163.117.142.173
name resolve order = bcast host lmhosts wins

admin users= @"Domain Admins"

ldap suffix = dc=lab,dc=inf,dc=uc3m,dc=es
ldap machine suffix = ou=Machines
ldap user suffix = ou=People
ldap group suffix = ou=groups
ldap idmap suffix = ou=idmap
ldap admin dn = cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es
ldap ssl = no
ldap passwd sync = Yes
idmap uid = 15000-20000
idmap gid = 15000-20000

load printers = no

; to maintain capital letters in shortcuts in any of the
profile folders:
preserve case = yes
short preserve case = yes
case sensitive = no
use spnego = yes
hosts allow = 163.117.142.0/24 10.0.142.0/24 127.0.0.1

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
Dos charset = 850
Unix charset = ISO8859-15

[netlogon]
path = /users/windows/netlogon
browseable = No
write list = @"Domain Admins"

```

```

        guest ok = yes

[homes]
    comment = Directorio HOME de %U, %u
    read only = No
    create mask = 0600
    directory mask = 0700
    force directory mode = 0700
    browseable = No
    writable = yes
    force user = %U
    valid users = %U, "@Domain Admins"
    hide                                files =
    /desktop.ini/outlook*.lnk/*Briefcase*/*$RECYCLE.BIN*/

```

### 11.1.2.3. */etc/smbldap-tools/smbldap.conf*

```

SID="---"
sambaDomain="LABINF"

slaveLDAP="ldap"
slavePort="389"
masterLDAP="ldap"
masterPort="389"

ldapTLS="0"
verify=""
cafile=""
clientcert=""
clientkey=""

suffix="dc=lab,dc=inf,dc=uc3m,dc=es"
usersdn="ou=people,${suffix}"
computersdn="ou=machines,${suffix}"
groupsdn="ou=groups,${suffix}"
idmapdn="ou=idmap,${suffix}"
sambaUnixIdPool="sambaDomainName=LABINF,${suffix}"
scope="sub"

hash_encrypt="SSHA"
crypt_salt_format=""

userLoginShell="/bin/bash"
userHome="/homes/alumnos/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="210"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="99999"

userProfile="//ldap/profiles/perfil_comun_w7"

```

```
mailDomain="lab.inf.uc3m.es"

with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
```

#### 11.1.2.4. */etc/smbldap-tools/smbldap\_\_bind.conf*

```
slaveDN="cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es"
slavePw="contraseña"
masterDN="cn=admin,dc=lab,dc=inf,dc=uc3m,dc=es"
masterPw="contraseña"
```

#### 11.1.2.5. */etc/nscd.conf*

debug-level	0		
paranoia	no		
enable-cache	passwd		yes
positive-time-to-live	passwd		600
negative-time-to-live	passwd		20
suggested-size	passwd		211
check-files	passwd		yes
persistent	passwd		yes
shared	passwd		yes
max-db-size	passwd		33554432
auto-propagate	passwd		yes
enable-cache	group		yes
positive-time-to-live	group		3600
negative-time-to-live	group		60
suggested-size	group		211
check-files	group		yes
persistent	group		yes
shared	group		yes
max-db-size	group		33554432
auto-propagate	group		yes
enable-cache	hosts		no
positive-time-to-live	hosts		3600
negative-time-to-live	hosts		20
suggested-size	hosts		211
check-files	hosts		yes
persistent	hosts		yes
shared	hosts		yes
max-db-size	hosts		33554432
enable-cache	services		yes
positive-time-to-live	services		28800
negative-time-to-live	services		20
suggested-size	services		211

---

check-files	services	yes
persistent	services	yes
shared	services	yes
max-db-size	services	33554432

### 11.1.3. Servidor CORREO

Los archivos de configuración relevantes del servidor CORREO son los siguientes:

#### 11.1.3.1. */etc/dovecot/dovecot-ldap.conf*

```
hosts = ldap:389

dn = uid=---,dc=lab,dc=inf,dc=uc3m,dc=es
dnpass = password
auth_bind = yes
ldap_version = 3

base = ou=People,dc=lab,dc=inf,dc=uc3m,dc=es
deref = never
scope = subtree
user_attrs =
homeDirectory=home,uidNumber=uid,gidNumber=gid
user_filter = (&(objectClass=posixAccount)(uid=%u))
pass_attrs = mail,userPassword
pass_filter = (&(objectClass=posixAccount)(uid=%u))
```

### 11.1.4. Cliente Linux

Los archivos de configuración relevantes del cliente Linux son los siguientes:

#### 11.1.4.1. */etc/pam\_ldap.conf* y */etc/libnss-ldap*

```
host ldap.lab.inf.uc3m.es
base dc=lab,dc=inf,dc=uc3m,dc=es
uri ldaps://ldap.lab.inf.uc3m.es

ldap_version 3

binddn uid=---,dc=lab,dc=inf,dc=uc3m,dc=es
bindpw contraseña

pam_password crypt

ssl start_tls
ssl on
tls_cacertfile /etc/ldap/ssl/cacert.pem
```

#### 11.1.4.2. */etc/nsswitch.conf*

```
passwd:      compat ldap
group:       compat ldap
shadow:      compat ldap

hosts:       files mdns4_minimal [NOTFOUND=return] dns
mdns4
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

#### 11.1.4.3. */etc/ldap/ldap.conf*

```
BASE    dc=lab,dc=inf,dc=uc3m,dc=es
URI      ldaps://ldap.lab.inf.uc3m.es

SIZELIMIT    50
TIMELIMIT    60
DEREF        always

TLS_CACERT    /etc/ldap/ssl/cacert.pem
TLS_REQCERT   never
```

## 11.2. Scripts

A continuación se anexan los scripts utilizados por el sistema, los utilizados durante la implementación y cuando el sistema está en producción.

### 11.2.1. Cuotas de usuario

Los scripts relevantes relacionados con las cuotas de usuario es el siguiente:

#### 11.2.1.1. *Script de modificación masiva de cuotas de usuario*

```
#!/bin/bash

ls -w 1 /users/alumnos-* | grep -v alumnos > ./users.txt
rm ./users-limpio.txt

for I in $(cat ./users.txt); do
    echo $I | grep "a0" >> users-limpio.txt
done

for I in $(cat ./users-limpio.txt); do
    /usr/sbin/xfs_quota -xc "limit bsoft=300M bhard=350M $I" /users
    echo "cambiando quota alumno" $I
done
```

### 11.2.2. Actualizador de políticas

Los scripts relevantes relacionados con el actualizador de políticas son los siguientes:

### 11.2.2.1. *c:\scripts\actualizador-scripts.ps1*

```
# Servidor de Políticas
$server = "ldap"
$ruta_scripts_policy = "\sysvol\policies\scripts\"

function sincronizar_scripts_maquina {
    $comando_base = "robocopy"
    $opciones = "/E /R:1 /W:1 /MIR"
    $destino1 = "C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown"
    $destino2 = "C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup"
    $origen1 = "\\\"+$server+$ruta_scripts_policy+"Shutdown"
    $origen2 = "\\\"+$server+$ruta_scripts_policy+"Startup"

    $comando = $comando_base+" "+$origen1+" "+$destino1+" "+$opciones
    $salida1 = Invoke-Expression $comando
    $convertido1 = convert_array_to_string $salida1
    $comando = $comando_base+" "+$origen2+" "+$destino2+" "+$opciones
    $salida2 = Invoke-Expression $comando
    $convertido2 = convert_array_to_string $salida2

    return $convertido1+$convertido2
}

function convert_array_to_string ($array) {
    $str = ""
    for ($i=0; $i -lt $array.length; $i++){
        $str = $str + $array[$i] + "`n"
    }
    return $str
}
```



```
function escribir_log ($evento, $tipo) {
    Write-Eventlog -logname 'Policy Updater' -Source 'Policy-Updater' -Message $evento -EntryType
$tipo -id 0
    #remove-eventlog "Policy Updater"
    #get-eventlog -list
}
```

```
#####
##### PROGRAMA PRINCIPAL #####
#####
```

```
Start-Sleep -s 5
$output = sincronizar_scripts_maquina
$mensaje = "(11/11) Scripts actualizados (arranque y apagado equipo):`n"+$output
escribir_log $mensaje "Information"
```

#### 11.2.2.2. *c:\scripts\security-template.inf*

```
[System Access]
MinimumPasswordLength = 8
[Version]
signature="$CHICAGO$"
Revision=1
[Privilege Rights]
SeNetworkLogonRight = *S-1-5-21-686392925-4218348329-2259797951-1441,*S-1-5-21-686392925-4218348329-
2259797951-512,*S-1-5-21-686392925-4218348329-2259797951-1009
SeMachineAccountPrivilege = *S-1-5-21-686392925-4218348329-2259797951-512
SeLoadDriverPrivilege = *S-1-5-21-686392925-4218348329-2259797951-1441,*S-1-5-32-544
SeServiceLogonRight = *S-1-5-18,*S-1-5-19,*S-1-5-21-686392925-4218348329-2259797951-512
SeSystemEnvironmentPrivilege = *S-1-5-21-686392925-4218348329-2259797951-1441,*S-1-5-32-544
```

```
SeRemoteInteractiveLogonRight    =    *S-1-5-21-686392925-4218348329-2259797951-512,*S-1-5-21-686392925-4218348329-2259797951-1009
SeCreateSymbolicLinkPrivilege = *S-1-5-11,*S-1-5-32-544
[Registry Values]
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DontDisplayLastUserName=4,1
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon=4,1
```

### 11.2.2.3. *c:\Windows\System32\GroupPolicy\Machine\Scripts\Startup\gpupdate.ps1*

```
#Variables globales
#servidor que contiene las políticas
$server = "ldap"
#ubicación en el servidor de las politicas de las aulas
$ruta_aulas = "\\\"+$server+"\sysvol\policies\aulas"
#ubicación en el servidor de las politicas de los equipos
$ruta_equipos = "\\\"+$server+"\sysvol\policies\equipos"
#ubicación en el cliente de los scripts genéricos
$destino_scripts_genericos = "C:\scripts"
#ubicación en el servidor de los scripts genéricos
$ruta_origen_scripts_genericos = "\\\"+$server+"\sysvol\scripts"
#ubicación en el servidor de las tareas programadas para las aulas
$ruta_aulas_tasks = "\\\"+$server+"\sysvol\Tasks\aulas"
#ubicación en el servidor de las tareas programadas para los equipos
$ruta_equipos_tasks = "\\\"+$server+"\sysvol\Tasks\equipos"
#ubicación en el cliente de las tareas programadas
$ruta_destino_scheduled_tasks = "C:\Windows\System32\Tasks\LABINF"

#AULAS
$aulas = @("A01","A02","F16","F18","H02","ASO","otros")
$A01
@("A181","A182","A183","A184","A185","A186","A187","A188","A189","A190","A191","A192","A193","A194")
```

```

$A02
@("A151","A152","A153","A154","A155","A156","A157","A158","A159","A160","A161","A162","A163","A164","A165","A166","A167","A168","A169","A170","A171")
$H02
@("H50","H51","H52","H53","H54","H55","H56","H57","H58","H59","H60","H61","H62","H63","H64","H65","H66","H67","H68","H69","H70")
$F16
@("F101","F102","F103","F104","F105","F106","F107","F108","F109","F110","F111","F112","F113","F114","F115","F116","F117","F118","F119","F120")
$F18
@("F201","F202","F203","F204","F205","F206","F207","F208","F209","F210","F211","F212","F213","F214","F215","F216","F217","F218","F219","F220")
$ASO = @("H71","H72","H73","H74","H75","H76","H77")
$otros = @("PRUEBA64","MWEB","CLIENTE")

function obtener_ruta_shortcut ($ruta) {

    #Definimos objeto del acceso directo
    $WshShell = New-Object -ComObject WScript.Shell;
    #Obtenemos los datos del acceso directo
    $link = $WshShell.CreateShortcut($ruta)
    #Obtenemos solamente el parámetro que nos interesa (TargetPath)
    $link = $link.TargetPath
    return $link
}

function obtener_aula_equipo {
    $hostname = hostname
    $return = 0
    foreach ($aula in $aulas){
        switch ($aula){
            "A01" { if ($A01 -contains $hostname) {$return = $aula} }
            "A02" { if ($A02 -contains $hostname) {$return = $aula} }
        }
    }
}

```

```

        "H02" { if ($H02 -contains $hostname) {$return = $aula} }
        "F16" { if ($F16 -contains $hostname) {$return = $aula} }
        "F18" { if ($F18 -contains $hostname) {$return = $aula} }
        "ASO" { if ($ASO -contains $hostname) {$return = $aula} }
        "otros" { if ($otros -contains $hostname) {$return = $aula} }
    }
}
return $return
}

function obtener_ruta_policy ($tipo, $gp) {
    if ($tipo -like "aula") {
        if (obtener_aula_equipo){
            switch ($gp) {
                "computer" { $ruta = $ruta_aulas+"\\"+(obtener_aula_equipo)+"\\"+"computer.lnk" }
                "user" { $ruta = $ruta_aulas+"\\"+(obtener_aula_equipo)+"\\"+"user.lnk" }
                "useradm" { $ruta = $ruta_aulas+"\\"+(obtener_aula_equipo)+"\\"+"useradm.lnk" }
            }
            if ($(obtener_ruta_shortcut $ruta) -like ""){
                return 1
            }else{
                return obtener_ruta_shortcut $ruta
            }
        }
    }
    elseif ($tipo -like "equipo") {
        if (obtener_aula_equipo){
            switch ($gp) {
                "computer" {
                    $ruta = $ruta_equipos+"\\"+(obtener_aula_equipo)+"\\"+(hostname)+"\\"+"computer.lnk" }
                "user" {
                    $ruta = $ruta_equipos+"\\"+(obtener_aula_equipo)+"\\"+(hostname)+"\\"+"user.lnk" }
            }
        }
    }
}

```

```

        "useradm" { $ruta
$ruta_equipos+"\\"+$(obtener_aula_equipo)+"\\"+$(hostname)+"\\"+"useradm.lnk" }
        }
        if ($(obtener_ruta_shortcut $ruta) -like ""){
            return 1
        }else{
            return obtener_ruta_shortcut $ruta
        }
    }
}
return 0
}

function obtener_lista_tasks ($tipo) {

    [array] $lista_tasks=''

    if ($tipo -like "aula") {
        if (obtener_aula_equipo){
            $ruta = $ruta_aulas_tasks+"\\"+$(obtener_aula_equipo)+"\\"

            #listar todas los accesos directos del directorio de destino y meterlas en un array
            $accesos_directos = Get-ChildItem -Path $ruta

            foreach ($acceso_directo in $accesos_directos)
            {
                if ($acceso_directo.Attributes -eq "Archive") {
                    $ruta_task = obtener_ruta_shortcut ($ruta+"\\"+$acceso_directo)
                    $lista_tasks += $ruta_task
                }
            }

            if ($lista_tasks.length -gt 1){

```

```
        return $lista_tasks
    }else{
        return 1
    }
}
}
elseif ($tipo -like "equipo") {
    if (obtener_aula_equipo){
        $ruta = $ruta_equipos_tasks+"\${obtener_aula_equipo)+"\${hostname)+"\"

        #listar todas los accesos directos del directorio de destino y meterlas en un array
        $accesos_directos = Get-ChildItem -Path $ruta

        foreach ($acceso_directo in $accesos_directos)
        {
            if ($acceso_directo.Attributes -eq "Archive") {
                $ruta_task = obtener_ruta_shortcut ($ruta+"\${acceso_directo)
                $lista_tasks += $ruta_task
            }
        }

        if ($lista_tasks.length -gt 1){
            return $lista_tasks
        }else{
            return 1
        }
    }
}
return 0
}

function sincronizar_gp ($ruta, $gp){
    $comando_base = "robocopy"
```

```
$opciones = "/E /R:1 /W:1 /MIR /XF gpupdate.ps1 update-equipo.bat"
$destino_computer = "C:\Windows\System32\GroupPolicy"
$destino_useradm = "C:\Windows\System32\GroupPolicyUsers\S-1-5-32-544"
$destino_user = "C:\Windows\System32\GroupPolicyUsers\S-1-5-32-545"
switch ($gp){
    "computer" {
        $comando = $comando_base+" "+$ruta+" "+$destino_computer+" "+$opciones
        $salida = Invoke-Expression $comando
        return $salida
    }
    "user" {
        $comando = $comando_base+" "+$ruta+" "+$destino_user+" "+$opciones
        $salida = Invoke-Expression $comando
        return $salida
    }
    "useradm" {
        $comando = $comando_base+" "+$ruta+" "+$destino_useradm+" "+$opciones
        $salida = Invoke-Expression $comando
        return $salida
    }
}

function crear_log {
    $estado = Get-Eventlog -list | findstr "Policy Updater"
    if ($estado -like ""){
        New-Eventlog -logname 'Policy Updater' -Source 'Policy-Updater'
        Limit-Eventlog -overflowaction OverwriteOlder -logname 'Policy Updater' -MaximumSize 10240KB
    }
}

function escribir_log ($evento, $tipo) {
```

```
        Write-Eventlog -logname 'Policy Updater' -Source 'Policy-Updater' -Message $evento -EntryType
$tipo -id 0
        #remove-eventlog "Policy Updater"
        #get-eventlog -list
    }

function asignar_permisos {

    $dir ="C:\Windows\System32\GroupPolicyUsers\S-1-5-32-544"
    $acl = Get-Item $dir |get-acl
    # Eliminamos itinerancia con la carpeta superior
    $acl.SetAccessRuleProtection($true,$true)
    $acl |Set-Acl

    # Creamos objeto acl
    $colRights
=[System.Security.AccessControl.FileSystemRights]"Write,AppendData,ChangePermissions,CreateDirectories,
CreateFiles,Delete,DeleteSubdirectoriesAndFiles,ExecuteFile,FullControl,ListDirectory,Modify,Read,ReadA
ndExecute,ReadAttributes,ReadData,ReadExtendedAttributes,ReadPermissions,Synchronize,TakeOwnership,Trav
erse,WriteAttributes,WriteData,WriteExtendedAttributes"
    $InheritanceFlag = [System.Security.AccessControl.InheritanceFlags]::None
    $PropagationFlag = [System.Security.AccessControl.PropagationFlags]::None
    $objType =[System.Security.AccessControl.AccessControlType]::Allow
    $objUser = New-Object System.Security.Principal.NTAccount("NT AUTHORITY\Usuarios autenticados")
    $objACE = New-Object System.Security.AccessControl.FileSystemAccessRule ($objUser, $colRights,
$InheritanceFlag, $PropagationFlag, $objType)
    $objACL = Get-ACL "C:\Windows\System32\GroupPolicyUsers\S-1-5-32-544"

    # Eliminamos objeto acl
    $objACL.RemoveAccessRuleAll($objACE)
    Set-ACL "C:\Windows\System32\GroupPolicyUsers\S-1-5-32-544" $objACL

}
```



```
function convert_array_to_string ($array) {
    $str = ""
    for ($i=0; $i -lt $array.length; $i++){
        $str = $str + $array[$i] + "`n"
    }
    return $str
}

function lanzar_actualizador_scripts {
    Start-Process powershell.exe c:\scripts\actualizador-scripts.ps1
}

function actualizar_scripts_genericos {
    $comando_base = "robocopy"
    $opciones = "/E /R:1 /W:1 /MIR"

    $comando = $comando_base+" "+$ruta_origen_scripts_genericos+" "+$destino_scripts_genericos+"
"+$opciones

    $salida = Invoke-Expression $comando
    return $salida
}

function sincronizar_tasks ($lista_tasks){

    $salida=''

    $comando_base_copiar = "xcopy"
    $opciones_copiar = "/Y"
    $comando_base_importar = "schtasks /create /F /TN \LABINF\"
    $opciones_importar = "/XML "
```

---

```

    #Comprobamos que el directorio existe
    if(!(test-path $ruta_destino_scheduled_tasks -pathtype container)){
        new-item $ruta_destino_scheduled_tasks -type directory
    }

    foreach ($tarea in $lista_tasks)
    {
        if ($tarea -notlike ''){
            #recorrer el array e importar las tareas al scheduler
            $comando_copiar = $comando_base_copiar+" "+$tarea+" "+$ruta_destino_scheduled_tasks+"
"+$opciones_copiar
            $fichero = obtener_nombre_fichero $tarea

            $salida += "`n`nCopiando "+$fichero+"`n"
            $salida += Invoke-Expression $comando_copiar

            $comando_importar = $comando_base_importar+$fichero+"
"+$opciones_importar+$ruta_destino_scheduled_tasks+"\ "+$fichero
            $salida += "`n`nImportando "+$fichero+"`n"
            $salida += Invoke-Expression $comando_importar
        }
    }
    return $salida
}

function obtener_nombre_fichero ($ruta){
    $partes=$ruta.split("\")
    $numero_partes=$partes.Count
    $fichero=$partes[$numero_partes-1]
    return $fichero
}

function borrar_tasks {

```

---

```

        $ruta_borrar = $ruta_destino_scheduled_tasks+"\*"
        Remove-Item $ruta_borrar
    }

#####
#####          PROGRAMAPRINCIPAL          #####
#####

#creamos el log si no existe
crear_log

#creamos los directorios de politicas de user y user_adm en el equipo
if(!(test-path "C:\Windows\System32\GroupPolicyUsers\S-1-5-32-544" -pathtype container)){
    new-item "C:\Windows\System32\GroupPolicyUsers\S-1-5-32-544" -type directory
    #configuramos seguridad en carpeta S-1-5-32-544
    asignar_permisos
}
if(!(test-path "C:\Windows\System32\GroupPolicyUsers\S-1-5-32-545" -pathtype container)){new-item
"C:\Windows\System32\GroupPolicyUsers\S-1-5-32-545" -type directory}

#Sincronizamos las políticas de usuario/administradores/equipo
#Actualizamos las políticas por aula
write-host ACTUALIZAMOS AULA.....
$path_aula_computer = obtener_ruta_policy aula computer
if ( ($path_aula_computer -ne 0) -and ($path_aula_computer -ne 1) ){
    $salida = sincronizar_gp $path_aula_computer computer
    $convertido = convert_array_to_string $salida
    $mensaje = "(1/11) Realizada actualización por aula (Políticas de equipo)`n"+$convertido
    escribir_log $mensaje "Information"
}else{
    $mensaje = "(1/11) No se ha realizado la actualización por aula (Políticas de equipo):`n`n    La
política no existe o se ha producido un error.`n`n    Las posibles causas son las siguientes:`n    *.-

```

```

Comprobar que el equipo esta debidamente agregado en el script.`n      *.- Comprobar que el enlace del
contenedor correspondiente existe.`n      *.- Comprobar que la ruta del enlace es correcta (se produce un
error en la ruta si se crea el enlace con la unidad montada y asignada con una letra).`n"
    escribir_log $mensaje "Warning"
}
$path_aula_user = obtener_ruta_policy aula user
if ( ($path_aula_user -ne 0) -and ($path_aula_user -ne 1) ){
    $salida = sincronizar_gp $path_aula_user user
    $convertido = convert_array_to_string $salida
    $mensaje = "(2/11) Realizada actualización por aula (Políticas de user)`n"+$convertido
    escribir_log $mensaje "Information"

}else{
    $mensaje = "(2/11) No se ha realizado la actualización por aula (Políticas de user):`n`n      La
política no existe o se ha producido un error.`n`n      Las posibles causas son las siguientes:`n      *.-
Comprobar que el equipo esta debidamente agregado en el script.`n      *.- Comprobar que el enlace del
contenedor correspondiente existe.`n      *.- Comprobar que la ruta del enlace es correcta (se produce un
error en la ruta si se crea el enlace con la unidad montada y asignada con una letra).`n"
    escribir_log $mensaje "Warning"
}
$path_aula_useradm = obtener_ruta_policy aula useradm
if ( ($path_aula_useradm -ne 0) -and ($path_aula_useradm -ne 1) ){
    $salida = sincronizar_gp $path_aula_useradm useradm
    $convertido = convert_array_to_string $salida
    $mensaje = "(3/11) Realizada actualización por aula (Políticas de useradm)`n"+$convertido
    escribir_log $mensaje "Information"

}else{
    $mensaje = "(3/11) No se ha realizado la actualización por aula (Políticas de useradm):`n`n      La
política no existe o se ha producido un error.`n`n      Las posibles causas son las siguientes:`n      *.-
Comprobar que el equipo esta debidamente agregado en el script.`n      *.- Comprobar que el enlace del
contenedor correspondiente existe.`n      *.- Comprobar que la ruta del enlace es correcta (se produce un
error en la ruta si se crea el enlace con la unidad montada y asignada con una letra).`n"

```

```
        escribir_log $mensaje "Warning"
    }

    #Actualizamos las políticas por equipo
    write-host ACTUALIZAMOS EQUIPO.....
    $path_equipo_computer = obtener_ruta_policy equipo computer
    if ( ($path_equipo_computer -ne 0) -and ($path_equipo_computer -ne 1) ){
        $salida = sincronizar_gp $path_equipo_computer computer
        $convertido = convert_array_to_string $salida
        $mensaje = "(4/11) Realizada actualización por equipo (Políticas de equipo)`n"+$convertido
        escribir_log $mensaje "Information"
    }else{
        $mensaje = "(4/11) No se ha realizado la actualización por equipo (Políticas de equipo):`n`n La
política no existe o se ha producido un error.`n`n Las posibles causas son las siguientes:`n      *.-
Comprobar que el equipo esta debidamente agregado en el script.`n      *.- Comprobar que el enlace del
contenedor correspondiente existe.`n      *.- Comprobar que la ruta del enlace es correcta (se produce un
error en la ruta si se crea el enlace con la unidad montada y asignada con una letra).`n"
        escribir_log $mensaje "Warning"
    }
    $path_equipo_user = obtener_ruta_policy equipo user
    if ( ($path_equipo_user -ne 0) -and ($path_equipo_user -ne 1) ){
        $salida = sincronizar_gp $path_equipo_user user
        $convertido = convert_array_to_string $salida
        $mensaje = "(5/11) Realizada actualización por equipo (Políticas de user)`n"+$convertido
        escribir_log $mensaje "Information"
    }else{
        $mensaje = "(5/11) No se ha realizado la actualización por equipo (Políticas de user):`n`n La
política no existe o se ha producido un error.`n`n Las posibles causas son las siguientes:`n      *.-
Comprobar que el equipo esta debidamente agregado en el script.`n      *.- Comprobar que el enlace del
contenedor correspondiente existe.`n      *.- Comprobar que la ruta del enlace es correcta (se produce un
error en la ruta si se crea el enlace con la unidad montada y asignada con una letra).`n"
        escribir_log $mensaje "Warning"
    }
}
```

```
$path_equipo_useradm = obtener_ruta_policy equipo useradm
if ( ($path_equipo_useradm -ne 0) -and ($path_equipo_useradm -ne 1) ){
    $salida = sincronizar_gp $path_equipo_useradm useradm
    $convertido = convert_array_to_string $salida
    $mensaje = "(6/11) Realizada actualización por equipo (Políticas de useradm)`n"+$convertido
    escribir_log $mensaje "Information"
}else{
    $mensaje = "(6/11) No se ha realizado la actualización por equipo (Políticas de useradm):`n`n La
política no existe o se ha producido un error.`n`n Las posibles causas son las siguientes:`n      *.-
Comprobar que el equipo esta debidamente agregado en el script.`n      *.- Comprobar que el enlace del
contenedor correspondiente existe.`n      *.- Comprobar que la ruta del enlace es correcta (se produce un
error en la ruta si se crea el enlace con la unidad montada y asignada con una letra).`n"
    escribir_log $mensaje "Warning"
}

#Sincronizamos las tareas programadas
#Actualizamos tareas por aula
borrar_tasks
write-host ACTUALIZAMOS TASKS AULA.....
$tareas_aula = obtener_lista_tasks aula
if ( ($tareas_aula -ne 0) -and ($tareas_aula -ne 1) ){
    $salida = sincronizar_tasks $tareas_aula
    #$convertido = convert_array_to_string $salida
    $mensaje = "(7/11) Realizada actualización de tareas por aula `n"+$salida
    escribir_log $mensaje "Information"
}else{
    $mensaje = "(7/11) No se ha realizado la actualización de tareas por aula:`n`n No existen
tareas para este aula o se ha producido un error.`n`n Las posibles causas son las siguientes:`n
      *.- Comprobar que el equipo esta debidamente agregado en el script.`n      *.- Comprobar que el enlace
del contenedor correspondiente existe.`n      *.- Comprobar que la ruta del enlace es correcta (se produce un
error en la ruta si se crea el enlace con la unidad montada y asignada con una letra).`n"
    escribir_log $mensaje "Warning"
}
```

```
#Actualizamos tareas por equipo
write-host ACTUALIZAMOS TASKS EQUIPO.....
$tareas_equipo = obtener_lista_tasks equipo
if ( ($tareas_equipo -ne 0) -and ($tareas_equipo -ne 1) ){
    borrar_tasks
    $salida = sincronizar_tasks $tareas_equipo
    $mensaje = "(8/11) Realizada actualización de tareas por equipo `n"+$salida
    escribir_log $mensaje "Information"
}else{
    $mensaje = "(8/11) No se ha realizado la actualización de tareas por equipo:`n`n No existen
tareas para este equipo o se ha producido un error.`n`n Las posibles causas son las siguientes:`n
    *.- Comprobar que el equipo esta debidamente agregado en el script.`n *.- Comprobar que el enlace
del contenedor correspondiente existe.`n *.- Comprobar que la ruta del enlace es correcta (se produce un
error en la ruta si se crea el enlace con la unidad montada y asignada con una letra).`n"
    escribir_log $mensaje "Warning"
}

#Aplicamos configuración de seguridad en el equipo (mediante archivo .inf)
$comando = "c:\windows\system32\secedit.exe /configure /db secedit.sdb /cfg c:\scripts\security-
template.inf"
$salida = Invoke-Expression $comando
$mensaje = [string]"(9/11) Aplicada plantilla de seguridad:`n`n"+$salida
escribir_log $mensaje "Information"

#Actualizamos scripts genéricos de c:\scripts
$output = actualizar_scripts_genericos
$convertido = convert_array_to_string $output
$mensaje = [string]"(10/11) Actualizados scripts genéricos (c:\scripts):`n"+$convertido
escribir_log $mensaje "Information"

#Actualizamos scripts de arranque de apagado (gpupdate.ps1 y apagar-equipo.bat)
lanzar_actualizador_scripts
```

#### 11.2.2.4. *c:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown\update-equipo.bat*

*c:\windows\system32\gpupdate.exe /Force /target:computer*

## 11.3. Páginas web y código php

Los scripts relevantes relacionados con las páginas web son los siguientes:

### 11.3.1. Actualizar Cuenta | Cambiar contraseña

```
<div id="titulosecundario">
<ul>
<li class="aperturacuentas"><h2>Actualizar cuenta | Cambiar contraseña</h2></li>
</ul>
</div>
<div id="descripciones">
<p>En esta página podrás actualizar tu actual cuenta de Linux para poder utilizar Linux y Windows con el mismo usuario.</p>
<p>También puedes realizar el cambio de contraseña de tu cuenta.</p>
</div>

<div class="apertura_cuentas">
<form method="post" action="/servicios/apertura_cuentas/abrir_cuenta">

<table id="apertura-cuentas-tabla">
<tr><td class="izq"><label for="user">Usuario Campus Global: </label></td><td class="izq"><input
type="text" size="25" maxlength="15" name="user" id="apertura-cuentas-input" /></td></tr>
<tr><td class="izq"><label for="pass">Contraseña Campus Global: </label></td><td class="izq"><input
type="password" size="25" maxlength="20" name="pass" id="apertura-cuentas-input"/></td></tr>
</table>
```



```

<p></p>
<p align="justify"><b>Nota:</b> La contraseña del laboratorio debe tener, al menos, 8 caracteres y de 1
a 3 deben ser numéricos.</p>

<table id="apertura-cuentas-tabla">
<tr><td class="izq"><label for="pass_lab">Contraseña Laboratorio: </label></td><td class="izq"><input
type="password" size="25" maxlength="20" name="pass_lab" id="apertura-cuentas-input"/></td></tr>
<tr><td class="izq"><label for="pass_lab_1">Repite Contraseña Laboratorio: </label></td><td
class="izq"><input type="password" size="25" maxlength="20" name="pass_lab_1" id="apertura-cuentas-
input"/></td></tr>
<tr><td colspan="2" class="centro"><input type="submit" value="Enviar"/>&nbsp;<input type="reset"
value="Limpiar"/></td></tr>
</table>
</form>
</div>

```

### 11.3.2. Apertura de cuentas

```

<div id="titulosecundario">
<ul>
<li class="aperturacuentas"><h2>Apertura de cuentas</h2></li>
</ul>
</div>
<div id="descripciones">
<p>En esta página podrás abrir una cuenta para poder ser utilizada en las aulas del
Departamento de Informática del <strong>campus de Leganes</strong> (4.0.F16, 4.0.F18,
1.0.A01, 1.0.A02 y 1.0.H02).</p>
<p>Se lo pueden inscribir alumnos y profesores que tengan al menos una asignatura que se
imparta en dichos laboratorios. Antes de realizar la apertura de la cuenta, se comprobarán las
listas oficiales de las asignaturas de cada titulación, para comprobar su veracidad.</p>
</div>

```

```

<div class="apertura_cuentas">
<h3 class="centrar">Date de Alta</h3>
<form method="post" action="/servicios/apertura_cuentas/abrir_cuenta">

<table id="apertura-cuentas-tabla">
<tr><td class="izq"><label for="user">Usuario Campus Global: </label></td><td class="izq"><input
type="text" size="25" maxlength="15" name="user" id="apertura-cuentas-input" /></td></tr>
<tr><td class="izq"><label for="pass">Contraseña Campus Global: </label></td><td class="izq"><input
type="password" size="25" maxlength="20" name="pass" id="apertura-cuentas-input"/></td></tr>
</table>

<p></p>
<p align="justify"><b>Nota:</b> La contraseña del laboratorio debe tener, al menos, 8 caracteres y de 1
a 3 deben ser numéricos.</p>

<table id="apertura-cuentas-tabla">
<tr><td class="izq"><label for="pass_lab">Contraseña Laboratorio: </label></td><td class="izq"><input
type="password" size="25" maxlength="20" name="pass_lab" id="apertura-cuentas-input"/></td></tr>
<tr><td class="izq"><label for="pass_lab_1">Repite Contraseña Laboratorio: </label></td><td
class="izq"><input type="password" size="25" maxlength="20" name="pass_lab_1" id="apertura-cuentas-
input"/></td></tr>
<tr><td colspan="2" class="centro"><input type="submit" value="Solicitar cuenta"/>&nbsp;<input
type="reset" value="Limpiar"/></td></tr>
</table>
</form>
</div>

<div class="apertura_cuentas">
<h3 class="centrar">Estado de tu cuenta</h3>
<p>Aquí podrás ver en que estado se encuentra tu cuenta. Introduce tu NIA y
aparecerá un diálogo con el resultado.</p>
<form method="post" action="/servicios/apertura_cuentas/estado_cuenta">

```

```

<table id="apertura-cuentas-tabla">
<tr><td class="izq"><label for="usuario">Usuario Campus Global: </label></td><td class="izq"><input
type="text" size="25" maxlength="15" name="user" id="apertura-cuentas-input" /></td></tr>
<tr><td class="izq"><label for="pass">Contraseña Campus Global: </label></td><td class="izq"><input
type="password" size="25" maxlength="20" name="pass" id="apertura-cuentas-input"/></td></tr>
<tr><td colspan="2" class="centro"><input type="submit" value="Buscar"/></td></tr>
</table>
</form>
</div>

```

### 11.3.3. Estado de tu cuenta

```

<?php
include ("/var/www/www.lab.inf.uc3m.es/cuentas/funciones_aux/func_aux.php");

$config= array();
$ruta_gestion_cfg='/root/shared/aplicaciones/GESTION/gestion.cfg.ldap';

    $user= $_POST["user"];
    $pass= $_POST["pass"];
    $resultado=3;
    $form_completo=1;

    // Leemos la configuración
    $config=get_config_gestion ($ruta_gestion_cfg);
    $lab_ldap_server=$config['LDAP_SERVER_MASTER'];
    $pass_consultas=$config['CLAVE_CONSULTAS_LDAP'];

    # Se verifica si se han completado los campos del formulario
    if (!$user || !$pass) {
        $form_completo=0;
    }

```

```
if ($form_completo){
    # Comprobamos si es alumno o profesor
    $tipo = comprobarTipoUsuario($user);
    # Se llama a la funcion de LDAP ($tipo = 0 alumno, $tipo = 1 profesor)
    $resultado = validar_ldap($user, $pass, $tipo, $mail, $registro_user);

    switch ($resultado) {
        //Usuario validado correctamente
        case 0:
            if (existe_usuario_ldap ($user, $lab_ldap_server, $pass_consultas)){
                $nia_lab=obtener_nia_lab($user);
                $mensaje="<p>El usuario ".$nia_lab." ya existe en el laboratorio, puede
cambiar la contraseña <a href=\"/servicios/apertura_cuentas\">aquí</a>.</p></div>";
                echo "        <div                id=\"miguitas\"><a                class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
                echo $mensaje;
            }else{
                echo "        <div                id=\"miguitas\"><a                class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
                echo "<p>El usuario no existe en el laboratorio, puede crear una cuenta <a
href=\"/servicios/apertura_cuentas\">aquí</a>.</p></div>";
            }
            break;
        //Error en el servidor
        case 1:
            echo "<div id=\"miguitas\"><a class=\"volver\" href=\"javascript:history.go(-
1)\">Volver</a></br></br></br>";
            echo "<p>No se puede contactar con el servidor, por favor, inténtelo de nuevo
más tarde</p></div>";
            break;
        //Usuario no encontrado
        default:
```

```

        echo "<div id=\"miguitas\"><a class=\"volver\" href=\"javascript:history.go(-
1)\">Volver</a></br></br></br>";
        echo "<p>Usuario o contraseña incorrectos. Inténtelo de nuevo</p></div>";
    }
}
}
else{
    echo "<div id=\"miguitas\"><a class=\"volver\" href=\"javascript:history.go(-
1)\">Volver</a></br></br></br>";
    echo "<p>Faltan datos por rellenar en el formulario</p></div>";
}

?>

```

#### 11.3.4. Abrir nueva cuenta

```

<?php

include ("/var/www/www.lab.inf.uc3m.es/cuentas/funciones_aux/func_aux.php");

$config= array();
$ruta_gestion_cfg='/root/shared/aplicaciones/GESTION/gestion.cfg.ldap';

//COMPROBAR EXISTENCIA DE GESTION.....EN CASO CONTRARIO NO ESTARIA MONTADO EL ROOT
if (file_exists($ruta_gestion_cfg)){

    // Leemos la configuración
    $config=get_config_gestion ($ruta_gestion_cfg);

    $home_alumnos=$config['PATH_ALUMNOS'];
    $home_profes=$config['PATH_PROFESORES'];
    $GID_ALUMNOS=$config['GID_ALUMNOS'];
    $GID_PROFESORES=$config['GID_PROFES'];
    $lab_ldap_server=$config['LDAP_SERVER_MASTER'];
}

```

```
$sambaProfilePath=$config['SMB_PROFILE_PATH'];
$archivo_bloqueo=$config['FILE_BLOQUEO'];
$tipo_hash=$config['TIPO_HASH'];
$fichero_nuevos_usuarios_web=$config['WEB_USERS_FILE'];
$fichero_nuevas_pass_web=$config['WEB_PASS_FILE'];
$pass_consultas=$config['CLAVE_CONSULTAS_LDAP'];
$pass_cifrar=$config['CLAVE_CIFRADO_PASS'];

$user= $_POST["user"];
$pass= $_POST["pass"];
$pass_lab= $_POST["pass_lab"];
$pass_lab_1= $_POST["pass_lab_1"];
$resultado=3;
$form_completo=1;

# Se verifica si se han completado los campos del formulario
if (!$user || !$pass || !$pass_lab || !$pass_lab_1) {
    $form_completo=0;
}

if ($form_completo){
    $salida=comprobar_validez_password($pass_lab, $pass_lab_1);
    if ($salida!=0){
        # la contraseña no cumple los requisitos
        if ($salida==1){
            echo "<div id=\"miguitas\"><a class=\"volver\" href=\"javascript:history.go(-1)\">Volver</a></div>";
            echo "<p>La contraseña no cumple los requisitos</p></div>";
        }else{
            # la contraseña no coincide en los campos del formulario
            echo "<div id=\"miguitas\"><a class=\"volver\" href=\"javascript:history.go(-1)\">Volver</a></div>";
            echo "<p>La contraseña no coincide en los campos del formulario</p></div>";
        }
    }
}
```

```

    }
} else {

    # Comprobamos si es alumno o profesor
    $tipo = comprobarTipoUsuario($user);

    # Se llama a la funcion de LDAP ($tipo = 0 alumno, $tipo = 1 profesor)
    $resultado = validar_ldap($user, $pass, $tipo, $mail, $registro_user);

    switch ($resultado) {
        //Usuario validado correctamente
        case 0:
            if (!existe_usuario_ldap ($user, $lab_ldap_server, $pass_consultas)){
                // waiting until file will be locked for writing (20 seconds as
timeout)

                if ($fp = fopen($archivo_bloqueo, 'a')) {
                    $startTime = microtime();
                    do {
                        $scanWrite = flock($fp, LOCK_EX);
                        // If lock not obtained sleep for 0 - 100 milliseconds,
to avoid collision and CPU load

                        if (!$scanWrite) usleep(1000000);
                    } while ((!$scanWrite)and((microtime()-$startTime) < 20000));
                    //file was locked so now we can store information
                    if ($scanWrite) {
                        $salida=escribir_nuevo_usuario_file($user, $tipo,
$registro_user, $pass_lab, $lab_ldap_server, $tipo_hash, $fichero_nuevos_usuarios_web, $pass_consultas,
$pass_cifrar);
                    }
                    fclose($fp);
                }
            }
            switch ($salida) {
                case 0:

```

```

//todo ok
enviar_mail($user, $mail, $tipo);
echo "<div id=\"miguitas\"><a class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
echo "<p>El usuario se ha creado correctamente. Le
llegará un correo cuando la cuenta esté disponible.</p><p>Dicho proceso puede tardar hasta 5
minutos.</p></div>";

break;
case 1:
//error con los servidores ldap

echo "<div id=\"miguitas\"><a class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
echo "<p>Error con los servidores ldap</p></div>";
break;
case 2:
//el usuario ya existe en el labo
echo "<div id=\"miguitas\"><a class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
echo "<p>El usuario ya existe en el
laboratorio</p></div>";

break;
case 3:
//el usuario ya está en el fichero de web
echo "<div id=\"miguitas\"><a class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
echo "<p>Su cuenta se creará en breve, puede tardar hasta
5 minutos.</p></div>";

break;
}
}else{
//cambiamos contraseña porque el usuario ya existe.....

```



```

                                $salida=cambiar_contraseña($user,
                                $pass_lab,
                                $fichero_nuevas_pass_web, $pass_cifrar);
                                switch ($salida) {
                                    case 0:
                                        //todo ok
                                        echo "<div id=\"miguitas\"><a class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
                                        echo "<p>Se ha cambiado la contraseña correctamente. Le
llegará un correo cuando la nueva contraseña sea efectiva.</p><p>Dicho proceso puede tardar hasta 5
minutos.</p></div>";
                                        break;
                                    case 1:
                                        //error
                                        echo "<div id=\"miguitas\"><a class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
                                        echo "<p>Ya has solicitado un cambio de contraseña y no
se ha realizado el cambio aún. Puede tardar hasta 5 minutos.</p></div>";
                                        break;
                                }
                                }
                                break;
                                //Error en el servidor
                                case 1:
                                    echo "<div id=\"miguitas\"><a class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
                                    echo "<p>Error en el servidor de la UC3M</p></div>";
                                    break;
                                default:
                                    echo "<div id=\"miguitas\"><a class=\"volver\"
href=\"javascript:history.go(-1)\">Volver</a></br></br></br>";
                                    echo "<p>Error en el usuario o en la contraseña</p></div>";
                                }
                            }
    }

```

```
        }else{
            if (!$form_completo){
                echo " <div id=\"miguitas\"><a class=\"volver\" href=\"javascript:history.go(-
1)\">Volver</a></br></br></br>";
                echo "<p>Faltan campos por rellenar en el formulario</p></div>";
            }
        }
    }else{
        //ENVIAR MAIL DE ERROR AL LAB
        echo "ERROR no se encuentra el fichero de configuración";
    }
}

?>
```