



UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERIA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES E INFORMATICOS

Tema:

**SISTEMA DE AUTENTICACIÓN UNIFICADA PARA LA CORRECTA TRANSMISIÓN DE
INFORMACIÓN EN EL CENTRO DE EDUCACIÓN "SAGRADA FAMILIA" DE
LA CIUDAD DE AMBATO**

Trabajo de Graduación, Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

AUTOR: Adriana Cumandá. Salinas Pérez.

TUTOR: Ing. René Francisco Terán Rodríguez.

Ambato – Ecuador

Octubre -2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: **“SISTEMA DE AUTENTICACIÓN UNIFICADA PARA LA CORRECTA TRANSMISIÓN DE INFORMACIÓN EN EL CENTRO DE EDUCACIÓN “SAGRADA FAMILIA” DE LA CIUDAD DE AMBATO**, presentado por la Srta. Adriana Cumanda Salinas Pérez, estudiante del a carrera de Ingeniería en Sistemas Computacionales e Informáticos de la facultad de Ingeniería en Sistemas Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato.

Ambato, Octubre 18 del 2012

EL TUTOR

Ing. René F. Terán R.

AUTORÍA

El presente trabajo de investigación titulado, **“SISTEMA DE AUTENTICACIÓN UNIFICADA PARA LA CORRECTA TRANSMISIÓN DE INFORMACIÓN EN EL CENTRO DE EDUCACIÓN “SAGRADA FAMILIA”**”, es absolutamente original, autentico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Octubre 18 del 2012

Adriana Cumanda Salinas Pérez

C.I 1804255923

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión calificadora del presente trabajo ,conformada por los Señores docentes: Ing. M.Sc Franklin Oswaldo Mayorga Mayorga e Ing. M.Sc Teresa Milena Freire Aillón, revisó y aprobó el informe Final del trabajo de graduación titulado, **SISTEMA DE AUTENTICACIÓN UNIFICADA PARA LA CORRECTA TRANSMISIÓN DE INFORMACIÓN EN EL CENTRO DE EDUCACIÓN “SAGRADA FAMILIA”**, presentado por la Srta. Adriana Cumanda Salinas Pérez de acuerdo al Art 18 del Reglamento de Graduación para obtener el título Terminal del tercer nivel de la Universidad Técnica de Ambato.

Ing. M.Sc. Oswaldo E. Paredes O.

PRESIDENTE DEL TRIBUNAL

Ing. M.Sc. Teresa M. Freire A.

DOCENTE CALIFICADOR

Ing. M.Sc. Franklin O. Mayorga M.

DOCENTE CALIFICADOR

DEDICATORIA

A mis padres José Salinas y María Pérez por apoyarme día a día brindándome su comprensión y amor a lo largo de mi vida personal y estudiantil.

A mis hermanos Robert Salinas y Catherine Salinas por ser mi fuente de sabiduría y motivación.

A todas aquellas personas quienes confiaron en mí, y compartieron mi camino a lo largo de los años hasta llegar al culmino de mi carrera.

AGRADECIMIENTO

Agradezco a la Facultad de Ingeniería en Sistemas y a sus docentes quienes aportaron sus conocimientos dentro de mi ciclo Universitario.

A la Escuela Sagrada Familia en especial a su director, Hno. Daniel Zúñiga, por abrirme las puertas de su institución y brindarme toda su colaboración.

A mi tutor de tesis Ing. Rene Terán, por su amplia guía en el desarrollo de este proyecto.

A mis Padres y hermanos por el apoyo moral y económico para llegar al cumplimiento de uno de mis objetivos.

ÍNDICE DE CONTENIDOS

PRELIMINARES	II
APROBACIÓN DEL TUTOR	ii
AUTORÍA	iii
APROBACIÓN DE LA COMISIÓN CALIFICADORA	iv
DEDICATORIA	v
AGRADECIMIENTO	vi
ÍNDICE DE CONTENIDOS	vii
ÍNDICE DE FIGURAS (ESTFIGURAS)	xiv
RESUMEN EJECUTIVO	xxi
INTRODUCCIÓN	xxii
CAPITULO I	1
1.1 TEMA:	1
1.2 PLANTEAMIENTO DEL PROBLEMA	1
1.2.1 CONTEXTUALIZACIÓN	1
1.2.2 ANÁLISIS CRÍTICO	2
1.2.3 PROGNOSIS	3
1.2.4 FORMULACIÓN DEL PROBLEMA	3
1.2.5 PREGUNTAS DIRECTRICES	3
1.2.6 DELIMITACIÓN DEL PROBLEMA	4
1.3 JUSTIFICACIÓN	4
1.4 OBJETIVOS	5
1.4.1 OBJETIVO GENERAL	5
1.4.2 OBJETIVOS ESPECÍFICOS	5
2 CAPITULO II	6
2.1 ANTECEDENTES INVESTIGATIVOS	6
2.2 FUNDAMENTACIÓN LEGAL	7
2.3 CATEGORÍAS FUNDAMENTALES	9
2.4 FUNDAMENTACIÓN TEÓRICA	9
2.4.1 RED DE COMPUTADORES	9
2.4.1.1 PROTOCOLOS DE RED	13
2.4.1.2 DISPOSITIVOS PARA CONECTIVIDAD	14
2.4.1.3 REQUERIMIENTOS DE RED	15
2.4.2 SERVIDORES	15

2.4.2.1	TIPOS DE SERVIDORES	15
2.4.2.2	SISTEMAS OPERATIVOS DE RED	18
2.4.2.3	CLIENTE – SERVIDOR	20
2.4.3	SEGURIDAD	20
2.4.3.1	POLÍTICAS O NORMATIVAS	21
2.4.3.2	SEGURIDAD EN TECNOLOGÍAS DE RED INALÁMBRICA	22
2.4.3.3	RESPALDOS	24
2.4.3.4	PROTECCIÓN DE DATOS	25
2.4.3.5	MODELOS DE SEGURIDAD	25
2.4.3.6	RECUPERACIÓN FRENTE A CATÁSTROFES	25
2.4.3.7	VIRUS INFORMÁTICOS	26
2.4.4	FIREWALL	28
2.4.4.1	POLÍTICAS DEL CORTAFUEGOS	29
2.4.4.2	TIPOS DE FIREWALL	30
2.4.4.3	BENEFICIOS DE UN FIREWALL EN INTERNET	32
2.4.5	PROXY	33
2.4.5.1	PROXY DE WEB / PROXY CACHE DE WEB	33
2.4.6	SISTEMA DE AUTENTICACIÓN	35
2.4.6.1	INTEROPERABILIDAD	37
2.4.7	LABORATORIO INFORMÁTICO	37
2.4.7.1	CARACTERÍSTICAS	38
2.4.7.2	REQUERIMIENTOS	38
2.4.8	INTRANET	38
2.4.8.1	DHCP	39
2.4.8.2	DNS	39
2.4.9	TRATAMIENTO DE LA INFORMACIÓN	41
2.4.9.1	TRATAMIENTO MANUAL	41
2.4.9.2	TRATAMIENTO AUTOMÁTICO	41
2.4.10	E-LEARNING	41
2.4.10.1	AULA VIRTUAL	42
2.4.10.2	EL AULA VIRTUAL EN FORMATO SINCRÓNICO	43
2.4.10.3	EL AULA VIRTUAL EN FORMATO ASINCRÓNICO	43
2.5	HIPÓTESIS	44
2.6	DETERMINACIÓN DE VARIABLES DE LA HIPÓTESIS	44
3	CAPITULO III	45
3.1	ENFOQUE	45
3.2	MODALIDAD BÁSICA DE LA INVESTIGACIÓN	45

3.2.1	INVESTIGACIÓN DE CAMPO	45
3.2.2	INVESTIGACIÓN BIBLIOGRÁFICA – DOCUMENTAL	45
3.3	NIVEL O TIPO DE INVESTIGACIÓN	46
3.3.1	EXPLORATORIO	46
3.3.2	DESCRIPTIVO	46
3.3.3	ASOCIACIÓN DE VARIABLES	46
3.4	POBLACIÓN Y MUESTRA	46
3.4.1	POBLACIÓN	46
3.4.2	MUESTRA	47
3.5	OPERACIONALIZACIÓN DE VARIABLES	48
3.5.1	VARIABLE INDEPENDIENTE	48
3.5.2	VARIABLE DEPENDIENTE	49
3.6	RECOLECCIÓN DE LA INFORMACIÓN	50
3.6.1	PLAN DE RECOLECCIÓN DE INFORMACIÓN	50
3.7	PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN	50
3.7.1	PLAN QUE SE EMPLEARÁ PARA PROCESAR LA INFORMACIÓN RECOGIDA	50
3.7.2	PLAN DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS	51
4	CAPITULO IV	52
4.1	RECOPIACIÓN DE LA INFORMACIÓN	52
4.2	ANÁLISIS E INTERPRETACIÓN DE LA INFORMACIÓN RECOLECTADA	52
4.3	VERIFICACIÓN DE LA HIPÓTESIS	62
4.3.1	COMBINACIÓN DE FRECUENCIAS (FRECUENCIA OBSERVADA)	63
4.3.2	FRECUENCIA ESPERADA	64
4.3.3	MODELO LÓGICO	65
4.3.4	NIVEL DE SIGNIFICANCIA Y REGLA DE DECISIÓN	65
4.3.4.1	GRADO DE LIBERTAD	65
4.3.4.2	GRADO DE SIGNIFICANCIA	65
4.3.5	CALCULO DEL CHI CUADRADO	67
5	CAPITULO V	70
5.1	CONCLUSIONES	70
5.2	RECOMENDACIONES	71
6	CAPITULO VI	72
6.1	DATOS INFORMATIVOS	72
6.2	ANTECEDENTES DE LA PROPUESTA	73
6.3	JUSTIFICACIÓN	73
6.4	OBJETIVOS	74
6.4.1	OBJETIVO GENERAL	74

6.4.2	OBJETIVOS ESPECÍFICOS	74
6.5	ANÁLISIS DE FACTIBILIDAD	75
6.5.1	FACTIBILIDAD OPERATIVA	75
6.5.2	FACTIBILIDAD ECONÓMICA	75
6.5.3	FACTIBILIDAD TÉCNICA	75
6.6	FUNDAMENTACIÓN	77
6.6.1	DISTRIBUCIONES LINUX	77
6.6.1.1	FEDORA	77
6.6.1.2	UBUNTU	78
6.6.1.3	CENTOS	78
6.6.2	SERVICIOS DE INTRANET	79
6.6.2.1	SERVICIO DE NOMBRES DE DOMINIO (DNS)	79
6.6.2.1.1	DNSMASQ	80
6.6.2.1.2	BIND	80
6.6.2.2	PROXY - SQUID	81
6.6.2.2.1	LISTAS DE CONTROL DE ACCESO (ACLs)	83
6.6.2.2.2	AUTENTICACIÓN SQUID	84
6.6.3	PLATAFORMAS EDUCATIVAS LIBRES	86
6.6.3.1	CLAROLINE	86
6.6.3.2	MOODLE	87
6.6.3.2.1	ESPECIFICACIONES TÉCNICAS	88
6.6.3.2.2	ADMINISTRACIÓN DE LOS USUARIOS - AUTENTICACIÓN	88
6.6.3.2.3	ADMINISTRACIÓN DE CURSOS	89
6.6.3.2.4	MÓDULOS PRINCIPALES	90
6.6.4	SERVICIOS DE DIRECTORIO	93
6.6.4.1	CENTOS DIRECTORY SERVER	93
6.6.4.2	OPENLDAP	94
6.6.5	SOFTWARE PARA RESPALDO LINUX	95
6.7	METODOLOGÍA	96
6.8	MODELO OPERATIVO	97
6.8.1	ANÁLISIS DEL SISTEMA	97
6.8.1.1	ANÁLISIS DE LA SITUACIÓN ACTUAL	97
6.8.1.2	ANÁLISIS DE REQUERIMIENTOS	98
6.8.2	DISEÑO DEL SISTEMA	99
6.8.2.1	ESTRUCTURA FÍSICA PROPUESTA	99
6.8.2.2	SISTEMA OPERATIVO	100
6.8.2.3	AUTENTICACIÓN	100

6.8.2.4	PROXY	101
6.8.2.5	DNS	102
6.8.2.6	AMBIENTE EDUCATIVO VIRTUAL	102
6.8.3	DESARROLLO E IMPLANTACIÓN	102
6.8.3.1	INSTALACIÓN DE LA DISTRIBUCIÓN CENTOS 6.0	102
6.8.3.2	DIRECCIONAMIENTO IP	103
6.8.3.3	ENRUTAMIENTO	104
6.8.3.4	CONFIGURACIÓN DNS – BIND	106
6.8.3.5	CONFIGURACIÓN OPENLDAP	112
6.8.3.5.1	CONFIGURACIÓN DE CENTOS PARA UTILIZAR AUTENTICACIÓN LDAP	121
6.8.3.6	CONFIGURACIÓN PROXY - SQUID	124
6.8.3.7	CONFIGURACIÓN PLATAFORMA EDUCATIVA – MOODLE	130
6.8.3.7.1	CONFIGURACIÓN DE MOODLE	133
6.8.3.7.2	AUTENTICACIÓN MOODLE CONTRA LDAP	142
6.8.3.7.3	PERSONALIZACIÓN- MOODLE	148
6.8.4	PRUEBAS DE FUNCIONAMIENTO	154
6.8.4.1	COMPROBACIÓN – BIND	154
6.8.4.2	COMPROBACIÓN – OPENLDAP	157
6.8.4.3	COMPROBACIÓN SQUID	160
6.8.4.4	COMPROBACIÓN – MOODLE	162
6.8.5	PLAN DE CONTINGENCIA	166
6.9	CONCLUSIONES Y RECOMENDACIONES	168
6.9.1	CONCLUSIONES	168
6.9.2	RECOMENDACIONES	169
BIBLIOGRAFÍA		170
GLOSARIO		173
ANEXOS		175
ANEXO A: ESTRUCTURA DEL CUESTIONARIO		176
ANEXO B : DETALLE DE LA INSTALACIÓN DE CENTOS		178
ANEXO C: DECRETO PRESIDENCIAL DEL USO DE SOFTWARE LIBRE EN LA REPUBLICA DEL ECUADOR		186
ANEXO D: DISPOSITIVOS DE LA INSTITUCIÓN		188
ANEXO E: MANUAL DE POLÍTICAS DE USO DE SERVICIOS		189

ÍNDICE DE TABLAS

TABLA 2.2 POBLACIÓN	46
TABLA 3.1 OPERACIONALIZACIÓN DE VARIABLES – SISTEMA DE AUTENTICACIÓN UNIFICADA	48
TABLA 3.2 OPERACIONALIZACIÓN DE VARIABLES – TRATAMIENTO DE LA INFORMACIÓN	49
TABLA 4.3 DATOS DE CONFORMIDAD CON EL MANEJO Y TRANSMISIÓN DE INFORMACIÓN	53
TABLA 4.4 DATOS DE CONFORMIDAD CON ATAQUES INFORMÁTICOS A LA INSTITUCIÓN	54
TABLA 4.5 DATOS DE CONFORMIDAD CON PÉRDIDAS DE INFORMACIÓN	55
TABLA 4.6 DATOS DE CONFORMIDAD CON LA RED INALÁMBRICA	56
TABLA 4.7 DATOS DE CONFORMIDAD CON LOS INCONVENIENTES DE LA INSTITUCIÓN	57
TABLA 4.8 DATOS DE CONFORMIDAD CON EL MANEJO DE AULAS VIRTUALES	58
TABLA 4.9 DATOS DE CONFORMIDAD CON LA AUTENTICACIÓN AL INTERNET	59
TABLA 4.10 DATOS DE CONFORMIDAD CON LA RED ALÁMBRICA	60
TABLA 4.11 DATOS DE CONFORMIDAD CON LA RESTRICCIÓN DE PÁGINAS WEB	61
TABLA 4.12 COMBINACIÓN DE FRECUENCIA	63
TABLA 4.13 FRECUENCIAS ESPERADAS	64
TABLA 4.14 VALORES CRÍTICOS DEL CHI CUADRADO	66
TABLA 4.15 DIFERENCIA DE FRECUENCIAS	67
TABLA 4.16 CUADRADO DE LA DIFERENCIA DE FRECUENCIAS	68
TABLA 4.17 CUADRADO DE LA DIFERENCIA DE FRECUENCIAS DIVIDIDO PARA DOS	68
TABLA 6.1 CARACTERÍSTICAS DE HARDWARE DEL SERVIDOR	76
TABLA 6.2 EQUIPOS CLIENTES DE LA RED INALÁMBRICA	76
TABLA 6.3 CARACTERÍSTICAS DE LOS DISPOSITIVOS DE LA INSTITUCIÓN	77
TABLA 6.4 MODULO DE AUTENTICACIÓN DE USUARIOS SQUID	86
TABLA 6.5 DIRECCIONAMIENTO IP	103
TABLA 6.6 DATOS DE CONFIGURACION - SQUID	125
TABLA 6.7 REGLAS DE ACCESO - SQUID	126
TABLA 6.8 CONTROL DE ACCESO - SQUID	127

TABLA 6.9 DATOS LDAP - MOODLE	147
TABLA 6.10 ESTUDIANTES QUINTO AÑO ROJO	158

ÍNDICE DE FIGURAS

FIGURA 2.1 CLASIFICACIÓN DE LAS REDES POR EXTENSIÓN	10
FIGURA 2.2 RED CLIENTE SERVIDOR	10
FIGURA 2.3 RED PEER TO PEER	11
FIGURA 2.4 TOPOLOGÍA DE ANILLO	11
FIGURA 2.5 TOPOLOGÍA DE BUS	12
FIGURA 2.6 TOPOLOGÍA EN ESTRELLA	12
FIGURA 2.7 TOPOLOGÍA DE MALLA	13
FIGURA 2.8 INTRANET EXTRANET	13
FIGURA 2.9 ROUTER INALÁMBRICO	14
FIGURA 2.10 SERVIDOR DE ARCHIVOS	16
FIGURA 2.11 SERVIDOR DE IMPRESION	16
FIGURA 2.12 SERVIDOR DE APLICACIÓN	17
FIGURA 2.13 SERVIDOR DE CORREO	17
FIGURA 2.14 DIAGRAMA CLIENTE SERVIDOR	20
FIGURA 2.15 AUTENTICACIÓN	22
FIGURA 2.16 SEGURIDAD EN TECNOLOGÍAS INALÁMBRICAS	23
FIGURA 2.17 TIPOS DE VIRUS INFORMÁTICOS	27
FIGURA 2.18 FIREWALL	28
FIGURA 2.19 FIREWALL A NIVEL DE RED	30
FIGURA 2.20 FIREWALL A NIVEL DE APLICACIÓN	32
FIGURA 2.21 PROXY	33
FIGURA 2.22 PROXY DE CACHE WEB	34
FIGURA 2.23 SERVIDOR DHCP	39
FIGURA 2.24 FUNCIONAMIENTO SERVIDOR DNS	40
FIGURA 4.3 RESULTADOS SOBRE EL MANEJO Y TRANSMISIÓN DE INFORMACIÓN	53
FIGURA 4.4 RESULTADOS SOBRE CON ATAQUES INFORMÁTICOS A LA INSTITUCIÓN	54

FIGURA 4.5 RESULTADOS SOBRE CON PÉRDIDAS DE INFORMACIÓN	55
FIGURA 4.6 RESULTADOS SOBRE LA RED INALÁMBRICA	56
FIGURA 4.7 RESULTADOS SOBRE LOS INCONVENIENTES DE LA INSTITUCIÓN	57
FIGURA 4.8 RESULTADOS SOBRE EL MANEJO DE AULAS VIRTUALES	58
FIGURA 4.9 RESULTADOS SOBRE LOS INCONVENIENTES DE LA INSTITUCIÓN	59
FIGURA 4.10 RESULTADOS SOBRE LA RED ALÁMBRICA	60
FIGURA 4.11 RESULTADOS SOBRE LA RESTRICCIÓN DE PÁGINAS WEB	61
FIGURA 6.1 FUNCIONAMIENTO DNS	80
FIGURA 6.2 FUNCIONAMIENTO PROXY	81
FIGURA 6.3 ESTRUCTURA FÍSICA ACTUAL	97
FIGURA 6.4 ESTRUCTURA FÍSICA PROPUESTA	99
FIGURA 6.5 AUTENTICACIÓN OPENLDAP	101
FIGURA 6.6 DIRECCIONAMIENTO IP	103
FIGURA 6.7 HABILITACIÓN ENRUTAMIENTO IP	104
FIGURA 6.8 INICIANDO CENTOS	104
FIGURA 6.9 CONFIGURACIÓN FIREWALL PARA ENRUTAMIENTO IP	105
FIGURA 6.10 GUARDANDO CONFIGURACIÓN EN FIREWALL	105
FIGURA 6.11 REINICIANDO CONFIGURACIÓN EN FIREWALL	105
FIGURA 6.12 COMANDO DE APERTURA ARCHIVO ETC/HOSTS	106
FIGURA 6.13 ARCHIVO ETC/HOSTS	106
FIGURA 6.14 INSTALACIÓN DE BIND	107
FIGURA 6.15 APERTURA DEL PUERTO 53 - CORTAFUEGOS	107
FIGURA 6.16 CREACIÓN DE ARCHIVOS DE CONFIGURACIÓN - BIND	108
FIGURA 6.17 CREACIÓN DEL ARCHIVO NAMED- BIND	108
FIGURA 6.18 ARCHIVO NAMED - BIND	109
FIGURA 6.19 CREACIÓN DE LA ZONA DIRECTA - BIND	110
FIGURA 6.20 ARCHIVO DE ZONA DIRECTA - BIND	110
FIGURA 6.21 CREACIÓN DE ZONA INVERSA - BIND	111

FIGURA 6.22 CONTENIDO ZONA INVERSA- BIND	111
FIGURA 6.23 REINICIO DEL SERVICIO NAMED	112
FIGURA 6.24 CONFIGURACIÓN DEL ARCHIVO ETC/RESOLV.CONF	112
FIGURA 6.25 INSTALACION DE OPENLDAP	112
FIGURA 6.26 VERIFICACIÓN DE PERMISOS Y GESTIÓN DB_CONFIG	113
FIGURA 6.27 CREACIÓN DE CONTRASEÑA	113
FIGURA 6.28 CONFIGURACIÓN DEL ARCHIVO OLCDATABASE\={2}\BDB.LDIF	114
FIGURA 6.29 CONTENIDO DEL ARCHIVO OLCDATABASE\={2}\BDB.LDIF	115
FIGURA 6.30 CONFIGURACIÓN DEL ARCHIVO OLCDATABASE\={1}\BDB.LDIF	115
FIGURA 6.31 ARCHIVO OLCDATABASE\={1}\BDB.LDIF	116
FIGURA 6.32 COMPROBACIÓN DE LA CONFIGURACION	116
FIGURA 6.33 INICIO DEL SERVICIO SLAPD	117
FIGURA 6.34 CREACIÓN DE ENTRADAS EN LA BDD - OPENLDAP	117
FIGURA 6.35 IMPORTACIÓN DEL ARCHIVO SAFA.LDIF	118
FIGURA 6.36 COMPROBACION DE INFORMACION EN BDD - OPENLDAP	118
FIGURA 6.37 REVISIÓN DE LA INSTALACIÓN DE OPENSLL	119
FIGURA 6.38 GENERACIÓN DE LLAVE Y CERTIFICADO OPENSLL	119
FIGURA 6.39 COMANDO DE APERTURA ARCHIVO CN=\CONFIG.LDIF	120
FIGURA 6.40 CONFIGURACIÓN DEL ARCHIVO CN=\CONFIG.LDIF	120
FIGURA 6.41 INSTALACIÓN DE NSS-PAM-LDAP	121
FIGURA 6.42 EJECUCIÓN DEL COMANDO AUTHCONFIG-TUI	121
FIGURA 6.43 CONFIGURACIÓN DE AUTENTICACIÓN	121
FIGURA 6.44 CREACIÓN DEL ARCHIVO WEBMIN.REPO	122
FIGURA 6.45 ARCHIVO WEBMIN.REPO	122
FIGURA 6.46 IMPORTACIÓN DE CLAVES	122
FIGURA 6.47 INSTALACIÓN DE WEBMIN	123
FIGURA 6.48 PORTADA WEBMIN	123
FIGURA 6.49 INSTALACIÓN DE SQUID	124

FIGURA 6.50 ARCHIVO SQUID.CONF	128
FIGURA 6.51 ARCHIVO FILTRAR	129
FIGURA 6.52 ARCHIVO SOCIALES	129
FIGURA 6.53 ARCHIVO DESCARGAS	130
FIGURA 6.54 INSTALACIÓN DE MYSQL	131
FIGURA 6.55 INSTALACION DE PHP	131
FIGURA 6.56 INCIO DE SERVICIOS PHP Y MYSQL	132
FIGURA 6.57 COMPROBACIÓN FUNCIONAMIENTO APACHE	132
FIGURA 6.58 COMPROBACIÓN FUNCIONAMIENTO MYSQL	133
FIGURA 6.59 PAGINA DE DESCARGA MOODLE	133
FIGURA 6.60 MOVIENDO ARCHIVO DESCARGADO A DIRECCION WWW/HTML	134
FIGURA 6.61 DESCOMPRESIÓN DEL ARCHIVO MOODLE.TGZ	134
FIGURA 6.62 ASIGNACIÓN DE PERMISOS A LA CARPETA MOODLE	134
FIGURA 6.63 CREACIÓN DE LA BASE DE DATOS MOODLEDB	135
FIGURA 6.64 CREACIÓN DEL USUARIO ADMINMOODLE	135
FIGURA 6.65 ASIGNACIÓN DE PERMISOS AL USUARIO ADMINMOODLE	136
FIGURA 6.66 CREACIÓN DEL DIRECTORIO MOODLEDATA	136
FIGURA 6.67 INSTALACIÓN MOODLE - SELECCIÓN DE IDIOMA	137
FIGURA 6.68 INSTALACIÓN MOODLE – SELECCIÓN DE CONTROLADOR BDD	137
FIGURA 6.69 INSTALACIÓN MOODLE – CONFIGURACIÓN DE BDD	138
FIGURA 6.70 INSTALACIÓN MOODLE – INFORME DE CONFIGURACIÓN	138
FIGURA 6.71 CREACIÓN DEL ARCHIVO CONFIG.PHP	139
FIGURA 6.72 CONTENIDO DEL ARCHIVO CONFIG.PHP	139
FIGURA 6.73 INSTALACIÓN MOODLE – TÉRMINOS Y CONDICIONES	140
FIGURA 6.74 INSTALACIÓN MOODLE - INFORME DE REQUISITOS MÍNIMOS	140
FIGURA 6.75 INSTALACIÓN MOODLE – INFORME DE INSTALACIÓN	141
FIGURA 6.76 INSTALACIÓN MOODLE – CREACIÓN DEL USUARIO ADMINISTRADOR	141
FIGURA 6.77 ACCESO A LA PLATAFORMA MOODLE	142

FIGURA 6.78 GESTIONAR IDENTIFICACION - MOODLE	143
FIGURA 6.79 ACTIVACIÓN USO DE LDAP - MOODLE	143
FIGURA 6.80 CONFIGURACIÓN DE LDAP - MOODLE	146
FIGURA 6.81 PANEL DE ADMINISTRACIÓN DEL SITIO - MOODLE	148
FIGURA 6.82 CONFIRMACIÓN POR EMAIL - MOODLE	148
FIGURA 6.83 AGREGAR EDITAR CURSOS - MOODLE	149
FIGURA 6.84 EDICIÓN CONFIGURACIÓN DEL CURSO - MOODLE	149
FIGURA 6.85 ETIQUETAS - MOODLE	150
FIGURA 6.86 ARCHIVOS - MOODLE	150
FIGURA 6.87 FORO - MOODLE	151
FIGURA 6.88 TAREA - MOODLE	151
FIGURA 6.89 URL - MOODLE	152
FIGURA 6.90 CONSULTA - MOODLE	152
FIGURA 6.91 TAREA - MOODLE	153
FIGURA 6.92 CUESTIONARIO - MOODLE	153
FIGURA 6.93 AGREGAR PREGUNTAS A CUESTIONARIO - MOODLE	154
FIGURA 6.94 TIPOS DE PREGUNTAS CUESTIONARIO - MOODLE	154
FIGURA 6.95 COMPROBACION DIG - DNS	155
FIGURA 6.96 COMPROBACIÓN NSLOOKUP - DNS	156
FIGURA 6.97 COMPROBACIÓN DOMINIOS - DNS	156
FIGURA 6.98 COMPROBACIÓN DOMINIO MOODLE - DNS	157
FIGURA 6.99 PÁGINA INICIAL WEBMIN	159
FIGURA 6.100 USUARIOS CREADOS WEBMIN	159
FIGURA 6.101 CONSULTA BDD LDAP	160
FIGURA 6.102 ACCESO POR CONTRASEÑA - SQUID	160
FIGURA 6.103 INGRESO DE USUARIO - SQUID	161
FIGURA 6.104 ACCESO A INTERNET - SQUID	161
FIGURA 6.105 BÚSQUEDA PAGINAS NO DESEADAS - SQUID	161

FIGURA 6.106 INFORME DE RESTRICCIÓN - SQUID	162
FIGURA 6.107 PÁGINA INICIAL - DNS	162
FIGURA 6.108 PÁGINA INICIAL - MOODLE	163
FIGURA 6.109 DATOS ERRÓNEOS - MOODLE	163
FIGURA 6.110 ACTUALIZACIÓN DE INFORMACIÓN - MOODLE	164
FIGURA 6.111 AUTENTICACIÓN - MOODLE	164
FIGURA 6.112 RESUMEN ESTUDIANTE AUTENTICADO - MOODLE	165
FIGURA 6.113 MATRICULACIÓN - MOODLE	165
FIGURA 6.114 PAGINA INICIAL CURSO VALORES HUMANOS - MOODLE	166
FIGURA B1 PAGINA INICIAL INSTALACIÓN CENTOS	178
FIGURA B2 LEVANTANDO SERVIDOR	178
FIGURA B3 PROBAR DISCO DE INSTALACION	179
FIGURA B4 CORRIENDO ANACONDA	179
FIGURA B5 CORRIENDO DE INSTALACIÓN	179
FIGURA B6 SELECCIÓN DEL IDIOMA DEL TECLADO	180
FIGURA B7 SELECCIÓN DEL IDIOMA DE INSTALACIÓN	180
FIGURA B8 SELECCIÓN TIPO DE DISPOSITIVOS	181
FIGURA B9 EXAMINANDO DISPOSITIVOS	181
FIGURA B10 ASIGNACIÓN NOMBRE AL SERVIDOR	181
FIGURA B11 UBICACIÓN ACTUAL DEL SERVIDOR	182
FIGURA B12 ASIGNACIÓN DE CONTRASEÑA	182
FIGURA B13 SELECCIÓN TIPO DE INSTALACIÓN	182
FIGURA B14 AVISO DE ESCRITURA	183
FIGURA B15 SELECCIÓN DE SERVICIOS DE INSTALACION	183
FIGURA B16 PROGRESO DE LA INSTALACION	184
FIGURA B17 AVISO INSTALACIÓN COMPLETA	184
FIGURA B18 INICIANDO CENTOS	184
FIGURA B19 ESCRITORIO DE CENTOS	185

FIGURA D1 LABORATORIO DE COMPUTACIÓN VISIÓN LATERAL	188
FIGURA D2 LABORATORIO DE COMPUTACIÓN VISIÓN FRONTAL	188
FIGURA D3 ROUTER DLINK	188

RESUMEN EJECUTIVO

La implementación del Sistema de Autenticación Unificada para la correcta transmisión de información en el centro de educación “Sagrada Familia” pretende optimizar recursos informáticos llevando una adecuada autenticación y control de acceso tanto al internet como a las herramientas didácticas presentes, mejorando la calidad de la información adquirida mediante estos medios de investigación, además de incursionar hacia las aulas virtuales mediante la aplicación de la plataforma moodle dentro de la institución.

Siendo una institución educativa, con el inconveniente de no contar con una red de comunicación de datos, lo cual obstaculiza el desarrollo tecnológico a nivel institucional, se ha visto la necesidad de diseñar e implementar una red inalámbrica con un servidor de datos basado en el sistema operativo Linux que proporcione servicios como enrutamiento dinámico, acceso a aulas virtuales, seguridad de firewall, filtrado a páginas web, proxy squid, entre otros.

El presente trabajo investigativo destaca las siguientes etapas:

La determinación de los requerimientos, en la que se detalla las demandas y exigencias con las que se debe cumplir en la red, los aspectos relativos para el desarrollo de la red wireless, así como las características de los dispositivos necesarios para cumplir con todos los requerimientos que proporcionen un correcto funcionamiento y desempeño de la red.

Un análisis detallado de los servicios y funcionalidades necesarias que debe poseer el servidor de datos para una adecuada funcionalidad de la intranet de la institución, como también las seguridades necesarias a implementarse dentro del mismo.

Aplicación de plataformas educativas que permitan fomentar el auto aprendizaje al estudiantado.

INTRODUCCIÓN

Los avances tecnológicos a lo largo del tiempo permiten proporcionar variedad de servicios a las instituciones educativas, como: la capacidad de compartir recursos informáticos, servicios de almacenamiento de información, implementación de Aulas virtuales las cuales abren nuevas puertas hacia el futuro, una de ellas es la adquisición de información de tipo educativo, logrando así una captación sobre temas más completos y comprensibles para el estudiante.

Una red de computadoras permite compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones

En la institución educativa “Sagrada Familia” la falta de comunicación lógica digital mediante una red de datos como también el inadecuado control y autenticación hacia el internet, acarrea consecuencias tales como la optimización de recursos, velocidad de transmisión de la información, inseguridad en la comunicación, Por lo que el presente proyecto de investigación logrará optimizar los recursos informáticos, agilizar la velocidad de comunicación entre equipos así como de acceso al internet ampliando el ámbito de investigación de los estudiantes y proporcionando seguridad de firewall para evitar posibles ataques informáticos, como también controlar el acceso al internet mediante una autenticación adecuada, además de actualizar a la institución mediante la aplicación de plataformas educativas.

El presente trabajo de graduación se encuentra desarrollado mediante la siguiente distribución y organización de capítulos:

CAPÍTULO I

Se Identifica, contextualiza y analiza críticamente el problema de investigación, además se plantea la justificación y delimitación del problema, lo cual será de gran utilidad para llevar una adecuada organización en el desarrollo de la investigación.

CAPÍTULO II

Contiene el respaldo teórico necesario para empezar la investigación, en donde se abordan temas como: Tipos de Servidores, Autenticación (métodos y beneficios), Aulas Virtuales, Firewall, Proxy, con la finalidad de llegar a comprender el fenómeno y buscar una solución apropiada.

CAPÍTULO III

Se determina la metodología de investigación a utilizar, el enfoque obtenido luego del proceso de investigación en la población, describiendo todas sus técnicas e instrumentos, el tipo de investigación y procesamiento de la información para posteriores análisis.

CAPÍTULO IV

Muestra el análisis e interpretación de resultados, de las encuestas realizadas a los docentes y administrativos que laboran en la institución, para asegurar y confirmar las necesidades de los mismos.

CAPÍTULO V

Contiene las conclusiones elaboradas a partir del análisis de resultados, además de recomendaciones del trabajo desarrollado.

CAPÍTULO VI

Parte fundamental del presente trabajo de investigación ya que presenta el desarrollo de la propuesta, detallando explícitamente el diseño, elaboración e implantación del sistema de autenticación desarrollado para la escuela Sagrada Familia de la ciudad de Ambato.

CAPITULO I

EL PROBLEMA

1.1 TEMA:

“**SISTEMA DE AUTENTICACIÓN UNIFICADA PARA LA CORRECTA TRANSMISIÓN DE INFORMACIÓN EN LA ESCUELA SAGRADA FAMILIA DE LA CIUDAD DE AMBATO**”

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 CONTEXTUALIZACIÓN

Los rápidos progresos de las nuevas tecnologías de la información y la comunicación, han modificado aspectos políticos, económicos, culturales y formativos, siendo así que las entidades educativas se han visto en la necesidad de actualizarse tecnológicamente implantando redes de datos, las cuales posibilitan la conexión mutua de dispositivos permitiendo: intercambiar información, compartir servicios, ofrecer recursos, convirtiéndose en una necesidad al momento de interactuar eficientemente con la información.

En el Ecuador los profundos cambios que se han producido en los últimos años exigen el impulso al desarrollo, formación y capacitación de excelencia de tal manera que el continuo desarrollo de las herramientas informáticas escolares han propiciado la implementación de redes de computadores en las instituciones

educativas para proporcionar flexibilidad y escalabilidad, sin embargo, son pocas las que disponen de una estructura de red adecuada.

El Centro Educativo “Sagrada Familia” ubicado en la ciudad de Ambato, tiene un gran interés por ir a la par con los cambios tecnológicos por lo mismo ofrece al alumnado un laboratorio con equipos informáticos actualizados, sin embargo no posee conexión de red alguna que permita compartir recursos, como tampoco adecuados métodos de control del internet.

1.2.2 ANÁLISIS CRITICO

En el Centro Educativo “Sagrada Familia”, no existe una interconexión de red como tampoco una adecuada configuración de equipos informáticos, los dispositivos obtenidos con anterioridad para el centro no se encuentran correctamente configurados para un apto funcionamiento, lo cual genera la subutilización de los recursos informáticos, además de tornarse imposible el trabajar con software educativo orientado a una red.

E servicio de internet proporcionado a la institución se torna relativamente lento, el manejo del mismo por los niños es prácticamente imposible debido a la calidad del mismo, lo cual es provocado principalmente por la actual ineficiente topología de red y falta de control del mismo, además de que no existe ningún tipo de filtrado de contenidos, provocando a que los escolares tengan acceso a páginas exclusivamente para adultos.

En el área de Sistemas claramente se observa la necesidad de optimizar el uso del internet ampliando el ámbito de investigación y aprendizaje por parte de los estudiantes, sin embargo este debe ser bien llevado mediante un control de acceso, además de un filtrado de páginas web, y no solo proveer protección a los infantes de páginas obscenas y peligrosas que rodean al internet sino también mejorar el control de la información interna de la institución.

Adicionalmente la implementación de plataformas educativas que permitan motivar de mejor manera al estudiante hacia las distintas asignaturas impartidas, gracias a interactivos métodos de enseñanza dentro de este entorno, y así propiciar un estímulo hacia la innovación y el crecimiento institucional.

1.2.3 PROGNOSIS

De continuar la situación actual y no realizarse el presente proyecto de investigación, la institución podría manifestar complicaciones en la transmisión y recepción de información, mayor lentitud del servicio de internet, subutilización de recursos tanto informáticos como humanos, constantes mantenimientos correctivos a sus equipos entre otros.

Al no actualizarse tecnológicamente, mediante aulas virtuales que proporcionen mayor flexibilidad en el aprendizaje, como tampoco una intranet eficiente que permita, compartir recursos, instaurar software educativo en red y minimizar problemas de seguridad. La institución se estaría estancando y aislando del avance tecnológico actual.

Es muy importante la elaboración del presente proyecto ya que se brindará un mayor campo de investigación a los niños dentro de la institución, además se proveerá de los respectivos filtrados de seguridad mediante el servidor permitiendo llevar un adecuado control de autenticación y acceso al internet.

1.2.4 FORMULACIÓN DEL PROBLEMA

¿Qué incidencia tiene la Subutilización de recursos informáticos para la transmisión de información en el centro educativo “Sagrada Familia”?

1.2.5 PREGUNTAS DIRECTRICES

- ¿Cuáles serían los resultados y beneficios que prestaría una red informática para la escuela “Sagrada Familia”?
- ¿Cuál S.O es el más adecuado para una adecuada transmisión de la información?
- ¿Cuál son las funcionalidades de un Sistema de Control y Autenticación?

1.2.6 DELIMITACIÓN DEL PROBLEMA

El presente proyecto se desarrollara en la escuela “Sagrada Familia” ubicada en el Cantón Ambato en la Provincia del Tungurahua, País Ecuador, en un periodo de seis meses a partir de la aprobación por parte del Honorable Consejo Directivo.

1.3 JUSTIFICACIÓN

El mundo de la informática ha venido evolucionando a través de las redes informáticas para mejorar su conectividad y comunicación. En particular se ha planteado la necesidad de enfocar el área de sistemas, mediante la realización de la interconectividad de red e instauración de una intranet que permita controlar y autenticar el acceso al internet, implantando las respectivas medidas de seguridad.

El Centro de Educación “Sagrada Familia”, actualmente no cuenta con una interconexión entre computadores como tampoco lleva un control de virus spyware, acceso de internet y compartimiento de archivos e impresoras, siendo este un factor negativo para la rápida elaboración de las actividades diarias por parte de niños y docentes.

Se ha optado por realizar este estudio, con el objeto de dotar a la institución de adecuadas herramientas que permitan beneficiarse de soluciones de alto rendimiento.

Los beneficios que alcanzara la escuela con este proyecto es el crecimiento tecnológico de la institución con lo cual el servicio educativo que se oferta será sobresaliente ya que tanto estudiantes como maestros tendrán una mejor herramienta y un mayor campo de investigación.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

- Implantar un Sistema de Autenticación Unificada para la correcta transmisión de información en la Escuela “Sagrada Familia”

1.4.2 OBJETIVOS ESPECÍFICOS

- Realizar un estudio y análisis sobre el software necesario a ser utilizado en la institución
- Analizar la red para optimizar los recursos de la institución
- Desarrollar una propuesta que permita una correcta transmisión de la información a través de un Sistema de Autenticación Unificado

CAPITULO II

MARCO TEORICO

2.1 ANTECEDENTES INVESTIGATIVOS

Revisados los archivos de la facultad de Ingeniería en Sistemas Electrónica e Industrial se encontraron los trabajos siguientes:

- a) “DISEÑO, IMPLANTACION Y CONFIGURACION LOGICA DE UNA RED PARA LA IMPLEMENTACION DE UNA INTRANET INFORMATIVA BAJO EL SISTEMA OPERATIVO LINUX PARA EL CENTRO EDUCATIVO NUEVO MUNDO”. Elaborado por el Ingeniero Geovanny Mauricio Iturralde Ruiz cuyas conclusiones dicen lo siguiente “ La labor realizada se lo ha hecho según las posibilidades de la institución, tanto en la parte lógica como física, por ende se puede decir que la red informática que necesitan los estudiantes del Nuevo Mundo debe ser implantada por completo lo más antes posible y se ha escogido una buena herramienta como servidor CENTOS, ya que este ha prestado las sub herramientas para la buena administración del red”.
- b) “DISEÑO DEL CABLEADO ESTRUCTURADO Y DE LA RED WIRELESS LAN PARA LA COOPERATIVA DE AHORRO Y CRÉDITO EDUCADORES DE TUNGURAHUA LTDA.” Elaborado por la Ingeniera Sonia Guadalupe Carrera Valle cuyas conclusiones dicen lo siguiente “Un diseño económico y eficiente depende de la recolección de toda la información necesaria y suficiente, cuidando de efectuar todas las investigaciones preliminares, ya que una buena construcción que sirva para un largo plazo será consecuencia de un buen diseño.

- c) “DISEÑO E IMPLANTACIÓN DE UNA RED INALÁMBRICA CON ACCESO A INTERNET EN EL CENTRO COMERCIAL CARACOL A TRAVÉS DE COMPUIDEAS” Elaborado por el Ingeniero Alirio Vidal Freire Sánchez cuyas conclusiones dicen lo siguiente “Se ha establecido y elaborado una intranet inalámbrica para este servicio con lo cual todos los usuarios accederán a un mismo servidor de Internet el cual es el único que estará enlazado vía cable y centralizado en un solo lugar para su mejor administración”

2.2 FUNDAMENTACIÓN LEGAL

El Centro Educativo “Sagrada Familia” se inicia con la comunidad de la Sagrada Familia, la cual es una congregación de hermanos religiosos católicos, que a nivel mundial tienen muchas obras de carácter educativo. Llevan su obra espiritual desde hace 32 años, poco a poco se insertaron en el ámbito educativo a través de la administración de instituciones de los vicariatos, como en Lago Agrio, Puyo y Guaranda.

En Ambato la oferta educativa inició en el año escolar 2009 – 2010, donde se dio inicio con los primeros años de Educación Básica, primero, segundo y tercero, siendo una gran ventaja la edificación propia perteneciente a la institución, en los próximos años se proponen ampliar la oferta académica para completar la educación básica, y al ser una unidad educativa aspira posteriormente extenderse hacia el bachillerato y preparar jóvenes para su ingreso a la universidad.

Misión

Estaremos atentos y abiertos a la realidad socio-cultural y religiosa en que se encuentra situado nuestro centro para que los servicios que ofrece desde la identidad que le es propia, correspondan a las necesidades reales.

Como centro educativo estamos abiertos a cuantos elijan este proyecto y nos proponemos formar a las personas en todas sus dimensiones, para ello eliminaremos toda discriminación:

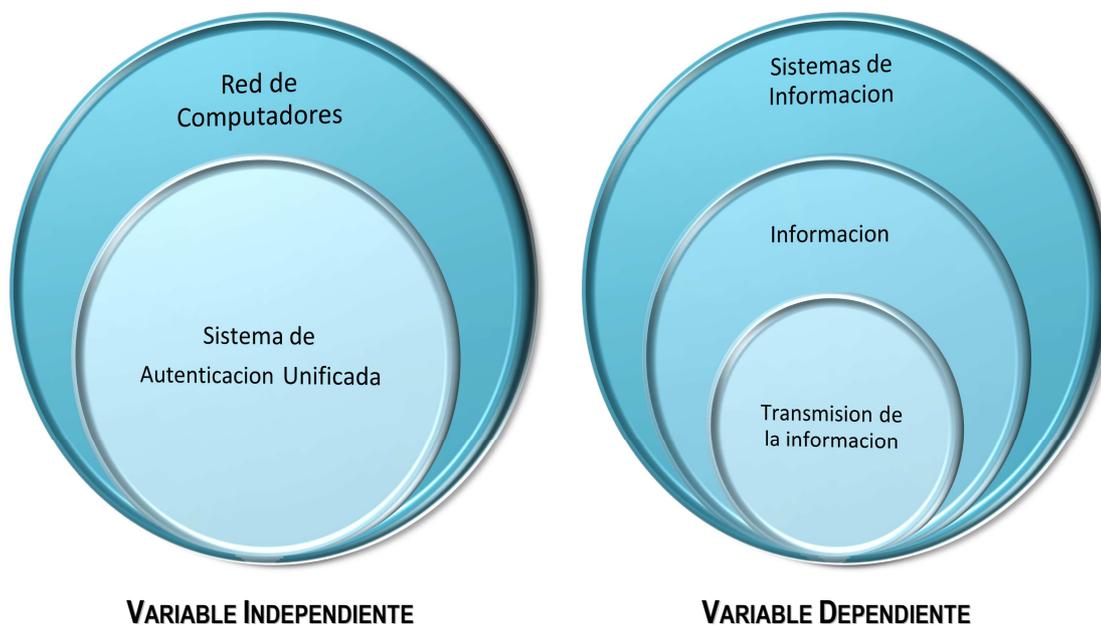
En el orden religioso formando alumnos cristianos y acogiendo también a los alumnos de otras religiones e incluso no creyentes.

- En el orden cultural, dando a todos una sólida formación cultural y atendiendo en lo posible a los problemas más álgidos que se vayan presentando en los educandos a través de los diferentes departamentos que la institución tenga que implementar.
- En el orden social, no admitiendo discriminaciones por sexo, raza, condición social o física.
- En el orden económico, enseñando valientemente las exigencias de la justicia y tratando de hacerlas operativas en la propia comunidad escolar. Gestionaremos el financiamiento de los costos de la educación de nuestro centro para que, en la medida de nuestras posibilidades, nadie sea discriminado por su condición económica.
- Fomentar una educación de calidad y excelencia, a través de una enseñanza participativa, reflexiva, creativa, orientadora, técnica, científica y axiológica; desarrollando aptitudes, habilidades y destrezas con el apoyo de toda la comunidad educativa.

Visión

Ser un establecimiento educativo que brinde a la juventud de Ambato y la Provincia de Tungurahua una Co-educación Integral, Científica y Humanística; que forme ciudadanos creativos, solidarios, profundamente comprometidos con el cambio social; que reconozcan y se sientan orgullosos de su identidad nacional, pluricultural y pluriétnica, que desarrollen y fortalezcan sus valores espirituales, éticos y morales, ayudando así a la consolidación de la democracia en la cual impere la equidad entre géneros y la justicia social.

2.3 CATEGORÍAS FUNDAMENTALES



2.4 FUNDAMENTACIÓN TEÓRICA

2.4.1 RED DE COMPUTADORES

“Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos, que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios. Este término también engloba aquellos medios técnicos que permiten compartir la información.

La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la

información, aumentar la velocidad de transmisión de los datos y reducir el coste general de estas acciones.”¹

“Por extensión las redes pueden ser:

- Área de red local (LAN)
- Área de red metropolitana (MAN)
- Área de red amplia (WAN)
- Área de red personal (PAN)

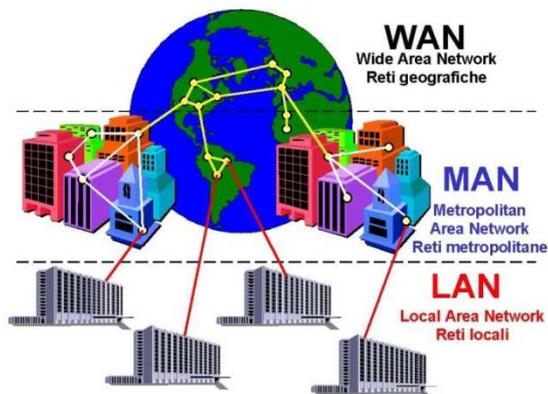


FIGURA 2.1 CLASIFICACIÓN DE LAS REDES POR EXTENSIÓN

Fuente: <http://omarpartida.blogspot.com/2010/04/clasificacion-de-las-redes.html>

Por relación funcional:

- Cliente/Servidor



FIGURA 2.2 RED CLIENTE SERVIDOR

Fuente: <http://1136110050.blogspot.com/>

- igual-a-igual (P2P)

¹ <http://www.innovacionate.com/servicios/consultorias-en-redes.html> Hace referencia a las características y clasificación de las redes



FIGURA 2.3 RED PEER TO PEER
Fuente: <http://1136110050.blogspot.com/>

Por topología:

- Red de anillo

Cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación del anillo.

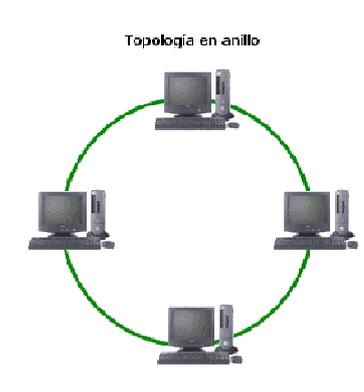


FIGURA 2.4 TOPOLOGÍA DE ANILLO
Fuente: <http://www.monografias.com/trabajos53/topologias-red/topologias-red.shtml>

- Red de bus

Una red en bus es multipunto. Un cable largo actúa como una red troncal que conecta todos los dispositivos en la red. Los nodos se conectan al bus mediante cables de conexión (latiguillos) y sondas.

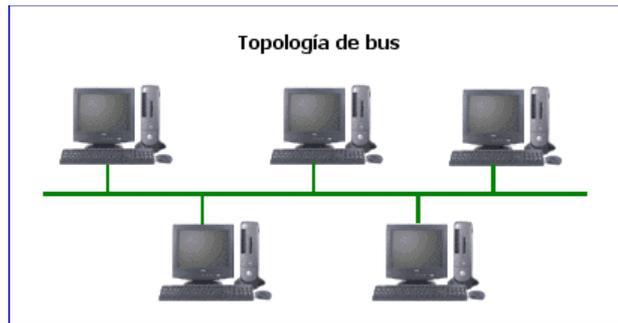


FIGURA 2.5 TOPOLOGÍA DE BUS

Fuente: http://usuaris.tinet.cat/acl/html_web/redes/topologia/topologia_2.html

- Red de estrella

En la red en estrella cada dispositivo solamente tiene un enlace punto a punto dedicado con el controlador central, habitualmente llamado concentrador.

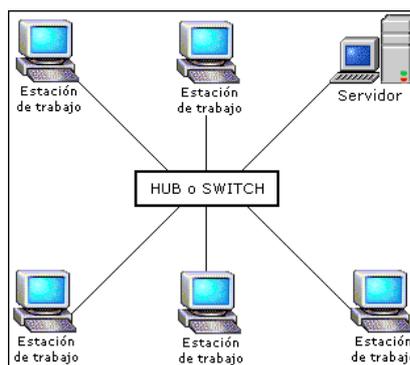


FIGURA 2.6 TOPOLOGÍA EN ESTRELLA

Fuente: http://usuaris.tinet.cat/acl/html_web/redes/topologia/topologia_2.html

- Red Mesh

En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo".²

² <http://elblogdelasredes.blogspot.com/p/redes-por-topologia-red-inalambrica-una.html> Se refiere a la clasificación de las redes



FIGURA 2.7 TOPOLOGÍA DE MALLA

Fuente: http://usuaris.tinet.cat/acl/html_web/redes/topologia/topologia_2.html

Puede ser una intranet o extranet.

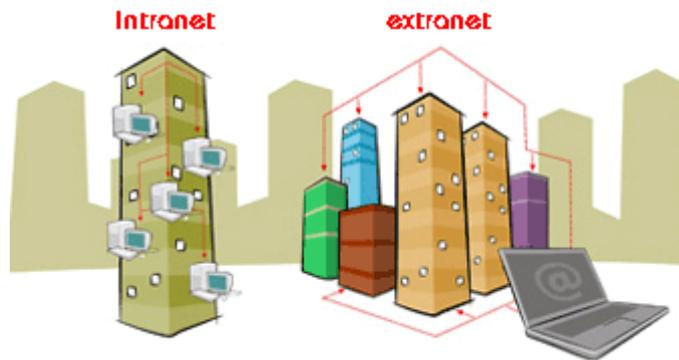


FIGURA 2.8 INTRANET EXTRANET

Fuente: <http://www.redecom.es/Desarrollo-Web-Intranet-Extranet.aspx>

2.4.1.1 PROTOCOLOS DE RED

Podemos definir un protocolo como el conjunto de normas que regulan la comunicación (establecimiento, mantenimiento y cancelación) entre los distintos componentes de una red informática.

Los protocolos de red proporcionan lo que se denominan «servicios de enlace». Estos protocolos gestionan información sobre direccionamiento y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es Ethernet o Token Ring.

- ▶ **IP:** El protocolo de TCP/IP para el encaminamiento de paquetes.

- ▶ **IPX:** El protocolo de Novell para el encaminamiento de paquetes.
- ▶ **NWLink:** La implementación de Microsoft del protocolo IPX/SPX.
- ▶ **NetBEUI:** Un protocolo de transporte que proporciona servicios de transporte de datos para sesiones y aplicaciones NetBIOS.
- ▶ **DDP (Protocolo de entrega de datagramas):** Un protocolo de Apple Talk para el transporte de datos.

2.4.1.2 DISPOSITIVOS PARA CONECTIVIDAD

El dispositivo de comunicación más básico de conectividad entre redes es el módem. Los módems se han convertido en dispositivos habituales y constituyen el equipamiento estándar en la mayoría de los equipos que se venden hoy en día. Además de los módems, también se utilizan otros dispositivos para conectar pequeñas LAN en una gran red de área extensa (WAN). Cada uno de estos dispositivos tiene su propia funcionalidad junto con algunas limitaciones. Simplemente, se pueden utilizar para extender la longitud del medio de red o para proporcionar acceso a una red mundial en Internet.

Los dispositivos utilizados para extender las Redes LAN incluyen repetidores, bridges (puentes), routers (encaminadores), brouters (b-encaminadores) y gateways (pasarelas).



FIGURA 2.9 ROUTER INALÁMBRICO

Fuente: http://yamiidussau.blogspot.com/2011_05_01_archive.html

Los Routers inalámbricos, como su nombre lo expresa, son **tecnología wireless**, es decir libre de cables, lo que no sólo redundará en la calidad de la conexión a Internet sino que definitivamente ayuda a la estética del sitio en donde este sistema de transmisión de ondas este implementado. Los distintos modelos y características de routers inalámbricos se adecuan específicamente a la cantidad de equipos que pueden generar una central de

conexión, como se le conoce popularmente a los espacios que agrupan a más de un computador que necesitan de una transmisión para complementar sus opciones de manejo.

2.4.1.3 REQUERIMIENTOS DE RED

A tomar en cuenta:

- Tamaño de las instalaciones (localizadas en una planta o varias plantas)
- Número de usuarios.
- Si la LAN se va a extender a varios edificios.
- El entorno (oficinas, fabricación, exteriores).
- Conocimientos técnicos de los usuarios.
- Nivel de tráfico de la red (actual y prevista para un futuro).
- Nivel de seguridad.

2.4.2 SERVIDORES

“Computadores que proporcionan servicios a las estaciones de trabajo de la red tales como almacenamiento en discos, acceso a las impresoras, unidades para respaldo de archivos, acceso a otras redes o computadores centrales.

Sirve información a los ordenadores que se conecten a él. Cuando los usuarios se conectan a este pueden acceder a programas, archivos y otra información del servidor.

2.4.2.1 TIPOS DE SERVIDORES

Servidores de archivos: Permite crear una especie de biblioteca de documentos, cuando un usuario necesita un archivo, lo busca en el servidor de archivos, trabaja con él localmente en su escritorio y después lo devuelve.

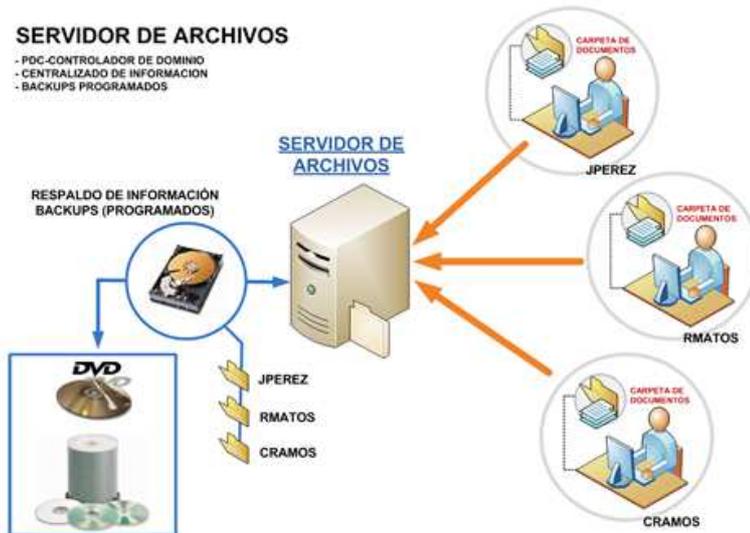


FIGURA 2.10 SERVIDOR DE ARCHIVOS

Fuente: <http://www.soportelinux.com.pe/servicios/serv-instserver.php>

Servidores de impresión: Permite el acceso a una o varias impresoras, en ocasiones, el mismo servidor funciona como servidor de archivos y de impresión.

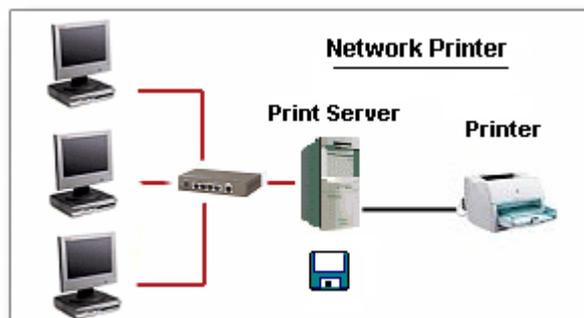


FIGURA 2.11 SERVIDOR DE IMPRESIÓN

Fuente: <http://vazquezilla.blogspot.com/2010/05/elementos-de-red.html>

Servidores de aplicación: Es un repositorio de información. Puede almacenar bases de datos, puede procesar información para proporcionar únicamente los datos que el usuario o cliente solicita específicamente.



FIGURA 2.12 SERVIDOR DE APLICACIÓN
Fuente: <http://sistdist01.blogspot.com/>

Servidores de correo: Funciona como una oficina postal de red para la administración y el almacenamiento de mensajes; entrega el correo electrónico a los PC cliente o lo aloja para que los usuarios remotos tengan acceso a sus mensajes cuando consideren oportuno.”³

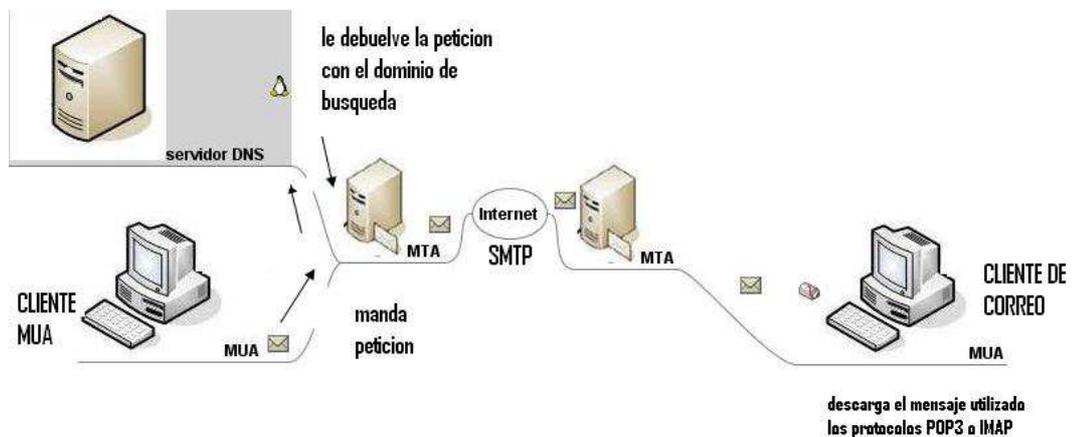


FIGURA 2.13 SERVIDOR DE CORREO
Fuente: <http://redjorge.wordpress.com/2010/06/18/diagrama-basico-de-servidor-de-correo/>

³ <http://pilarinformatico.blogspot.com/p/servidores.html> Hace referencia a los tipos de servidores

2.4.2.2 SISTEMAS OPERATIVOS DE RED

“Son aquellos sistemas que mantienen a dos o más equipos unidos a través de algún medio de comunicación (físico o no), con el objetivo primordial de poder compartir los diferentes recursos hardware y software. Los sistemas operativos de red más ampliamente usados son: Novell Netware, LAN Manager, Windows Server, UNIX, Linux, LANtastic, Li, etc. Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. Si no se dispone de ningún equipo que monte un sistema operativo de red, no existirá una gestión centralizada de recursos, por lo que la red se convertirá en lo que se ha denominado grupo de trabajo. Si existe un sistema operativo en red, los recursos de la red se gestionarán siempre a través del ordenador principal de forma centralizada.

SISTEMAS OPERATIVOS EN RED – LINUX

Linux es un sistema operativo de propósito general, multiusuario y multitarea. Normalmente, un sistema UNIX/Linux está constituido por un equipo central y múltiples terminales para los usuarios. Este sistema operativo incluye las prestaciones de red, diseñado específicamente para grandes redes, pero también presenta algunas aplicaciones para equipos personales, trabaja bien sobre un equipo autónomo y, como consecuencia de sus posibilidades de multitarea, también lo hace perfectamente en un entorno de red.

A diferencia de los sistemas operativos Microsoft, Linux en cualquiera de sus versiones puede funcionar como cliente o como servidor.

SISTEMAS OPERATIVOS EN RED - WINDOWS

Windows Server es un S.O diseñado para entorno de servidores que trabaja sobre un modelo denominado dominio. Un dominio es una colección de equipos (clientes y servidores) que comparten una política de seguridad y una base de datos común. Cada dominio tiene un nombre único.

Los servicios más habituales que ofrece este tipo de S.O para la gestión de la red son los siguientes:

- Servicios de compartición de recursos. Este servicio es con el que se puede poner a disposición de los usuarios de la red archivos, carpetas, impresoras, o cualquier otro recurso, de forma centralizada y con un nivel de seguridad determinando.
- Seguridad. Al igual que los sistemas operativos de red más importantes, Windows Server proporciona seguridad para cualquier recurso de la red. El servidor de red Windows mantiene todos los registros de las cuentas de usuario y gestiona los permisos y derechos de usuario. Para acceder a cualquier recurso de la red, el usuario debe tener los derechos necesarios para realizar la tarea y los permisos adecuados para utilizar el recurso.
- Servicios de impresión. En una red Windows Server, cualquier servidor o cliente puede funcionar como servidor de impresión. La diferencia es que si el servicio de impresión está montado en un cliente, el administrador de la red no tendrá control total sobre el mismo. Lo normal es instalar estos servicios en el servidor y gestionarlos desde este equipo.
- Servicios de red. Windows Server proporciona diferentes servicios de red que ayudan a la gestión global de un entorno de red. Algunos de estos servicios son:
 - Servicio de mensajería. Monitoriza la red y recibe mensajes emergentes para el usuario.
 - Servicio de alarma. Envía las notificaciones recibidas por el servicio de mensajería.
 - Servicio de exploración. Proporciona una lista de servidores disponibles en los dominios y en los grupos de trabajo.
 - Servicio de estación. Se ejecuta sobre una estación de trabajo y es responsable de las conexiones con el servidor.
 - Servicio de servidor. Proporciona acceso de red a los recursos de un equipo
- Interoperabilidad. Los diferentes protocolos y servicios de red que gestiona un sistema Windows Server sirven para configurar un entorno de red mixto o fácilmente interoperable. Como ejemplo se incorpora el protocolo de red NWLink

diseñado para que Windows Server sea compatible con otros servidores no Windows, como Novell NetWare.”⁴

2.4.2.3 CLIENTE – SERVIDOR

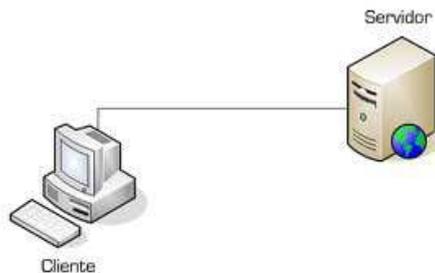


FIGURA 2.14 DIAGRAMA CLIENTE SERVIDOR

El término «cliente/servidor» se refiere a un modelo en el que el procesamiento de datos es compartido entre el equipo cliente y el equipo servidor.

El enfoque cliente/servidor puede beneficiar a cualquier organización en la que muchas personas necesiten acceder continuamente a grandes cantidades de datos.

La red cliente/servidor es la forma más eficaz de ofrecer:

- Acceso y gestión de bases de datos para aplicaciones tales como hojas de cálculo, contabilidad, comunicaciones y gestión de documentos.
- Gestión de la red.
- Almacenamiento centralizado de archivos.

2.4.3 SEGURIDAD

La seguridad, protección de los equipos conectados en red y de los datos que almacenan y comparten, es un hecho muy importante en la interconexión de equipos. Cuanto más grande sea una empresa, más importante será la necesidad de seguridad en la red.

⁴ <http://albeiro1.blogspot.com/> Se refiere a los sistemas operativos en ambientes distribuidos

La seguridad es más que evitar el acceso no autorizado a equipos y a sus datos. Incluye el mantenimiento del entorno físico apropiado que permita un funcionamiento correcto de la red.

2.4.3.1 POLÍTICAS O NORMATIVAS

Generar la seguridad en una red requiere establecer un conjunto de reglas, regulaciones y políticas que no dejan nada al azar. El primer paso para garantizar la seguridad de los datos es implementar las políticas que establecen los matices de la seguridad y ayudan al administrador y a los usuarios a actuar cuando se producen modificaciones, esperadas como no planificadas, en el desarrollo de la red.

Prevención

La mejor forma de diseñar las políticas de seguridad de los datos es optar por una perspectiva preventiva. Los datos se mantienen seguros cuando se evita el acceso no autorizado. Un sistema basado en la prevención requiere que el administrador conozca todas las herramientas y métodos disponibles que permiten mantener la seguridad de los datos.

Autenticación

Para acceder a la red, un usuario debe introducir un nombre de usuario y una contraseña válida. Dado que las contraseñas se vinculan a las cuentas de usuario, un sistema de autenticación de contraseñas constituye la primera línea de defensa frente a usuarios no autorizados.

Es importante no permitir un exceso de confianza en este proceso de autenticación engañándonos con una falsa idea de seguridad. Por ejemplo, en una red de peer-to-peer, casi todos los usuarios pueden entrar en el sistema con un nombre y contraseña única. Esto sólo puede proporcionar a un usuario acceso completo a la red, de forma que cualquier cosa que se comparta está disponible para este usuario. La autenticación funciona sólo en una red basada en servidor, donde el nombre y contraseña de usuario debe ser autenticada utilizando para ello la base de datos de seguridad.

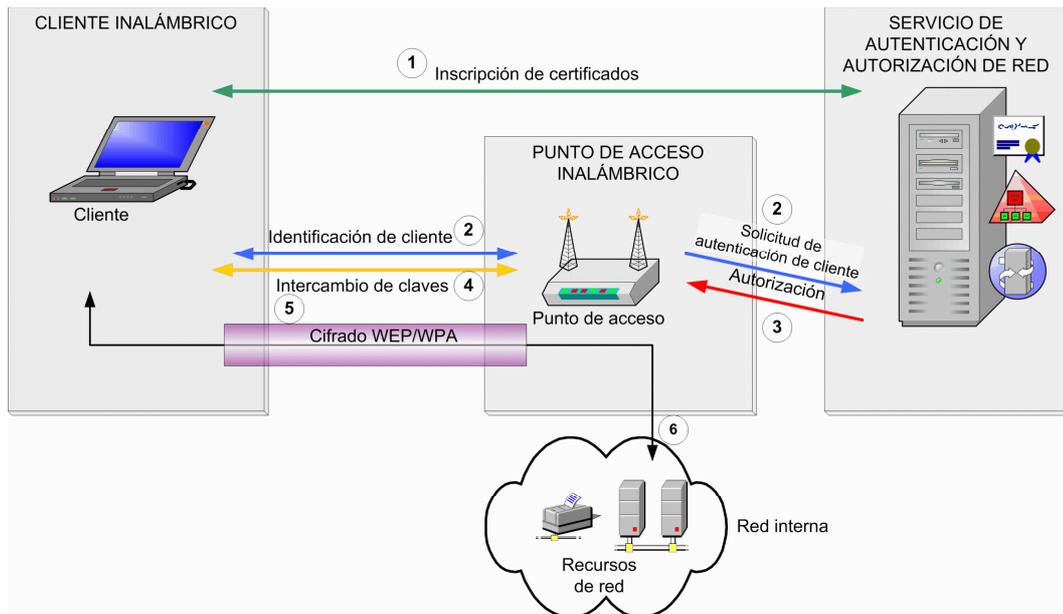


FIGURA 2.15 AUTENTICACIÓN

Fuente: <http://technet.microsoft.com/es-es/library/dd458733.aspx>

2.4.3.2 SEGURIDAD EN TECNOLOGÍAS DE RED INALÁMBRICA

“En redes inalámbricas con infraestructura se utiliza un punto de acceso (wireless access point, WAP o simplemente AP) para interconectar todos los dispositivos inalámbricos de la red. Usualmente un AP se conecta también a una red cableada, transmitiendo datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

La seguridad es un tema importante en las redes inalámbricas porque, al contrario que en una red cableada a la que sólo tienen acceso las personas que físicamente pueden conectarse, cualquier persona de la calle o pisos o edificios vecinos pueden conectarse a una red inalámbrica o ver el contenido de los paquetes que circulan por ella si ésta no está convenientemente protegida.

Algunos de los principales protocolos estándar para proporcionar seguridad en redes inalámbricas IEEE 802.11 son:

WPA (Wi-Fi Protected Access) fue creado para corregir los múltiples fallos detectados en el protocolo WEP. WPA fue diseñado por el consorcio Wi-Fi Alliance basándose en un borrador del estándar 802.11i (es un subconjunto del mismo), y utiliza TKIP (Temporal Key

Integrity Protocol) como protocolo de cifrado que sustituye a WEP sin necesidad de modificar el hardware existente (podría funcionar actualizando el firmware).

En concreto, WPA sigue usando RC4 como algoritmo de cifrado con claves de 128 bits, pero usa TKIP para cambiar dinámicamente estas claves.

WPA fue diseñado para ser usado junto a un servidor AAA, de manera que se le asignan claves distintas a cada uno de los posibles usuarios. Sin embargo, para entornos domésticos o pequeñas oficinas también se puede usar, de forma menos segura, con una única clave compartida (pre-shared key, PSK). En este caso se habla de WPA-PSK.

WPA2 se basa en el nuevo estándar 802.11i, y el cambio más significativo respecto a WPA es que usa el protocolo de cifrado AES en lugar de RC4. Mientras que WAP puede ejecutarse en el hardware que soporte WEP (tras actualizar el firmware), WPA2 necesita un hardware más nuevo (posterior al 2004). Sin embargo, se sabe que WAP también terminará siendo comprometido a medio plazo y por tanto sólo se recomienda como transición a WPA2.”⁵

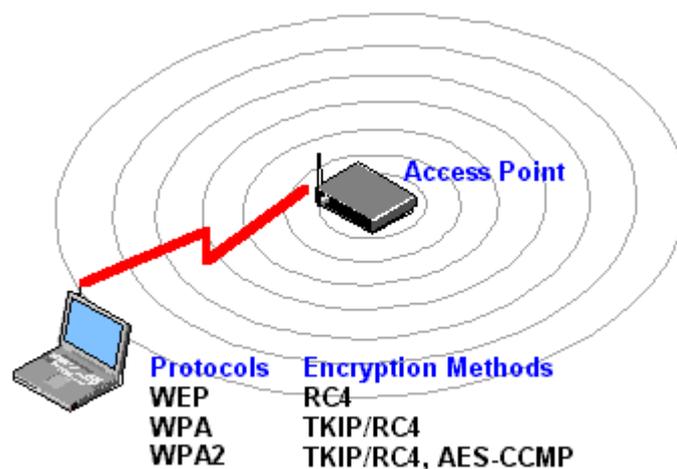


FIGURA 2.16 SEGURIDAD EN TECNOLOGÍAS INALÁMBRICAS

Fuente: <http://francorebolledo.blogspot.com/>

⁵ <http://www.uv.es/~montanan/ampliacion/trabajos/SeguridadWireless.pdf> Se refiere a la seguridad en redes inalámbricas

2.4.3.3 RESPALDOS

“Una backup (su nombre en inglés), en tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos.

Fundamentalmente son útiles para:

- ▶ Recuperarse de una catástrofe informática,
- ▶ Recuperar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente o corrompido.

La pérdida de datos es muy común: El 66% de los usuarios de internet han sufrido una seria pérdida de datos. La organización del espacio de almacenamiento y la administración del proceso de efectuar la copia de seguridad son tareas complicadas. Para brindar una estructura de almacenamiento es conveniente utilizar un modelo de almacenaje de datos, existen muchos tipos diferentes de dispositivos para almacenar datos que son útiles para hacer copias de seguridad, cada uno con sus ventajas y desventajas a tener en cuenta para elegirlos, como duplicidad, seguridad en los datos y facilidad de traslado.

Se han desarrollado muchas técnicas diferentes para optimizar el procedimiento de efectuar los backups. Estos procedimientos incluyen optimizaciones para trabajar con archivos abiertos y fuentes de datos en uso y también procesos de compresión, cifrado, y procesos de duplicación, entendiéndose por esto último a una forma específica de compresión donde los datos superfluos son eliminados. Muchas organizaciones e individuos tratan de asegurarse que el proceso de backup se efectúe de la manera esperada y trabajan en la evaluación y la validación de las técnicas utilizadas, las copias de seguridad garantizan dos objetivos: integridad y disponibilidad”⁶

⁶ http://es.wikipedia.org/wiki/Copia_de_seguridad Se refiere a las copias de seguridad

2.4.3.4 PROTECCIÓN DE DATOS

“La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (sólo se copian los ficheros creados o modificados desde el último backup). Es vital para las empresas elaborar un plan de backup en función del volumen de información generada y la cantidad de equipos críticos.”⁷

2.4.3.5 MODELOS DE SEGURIDAD

“Un Modelo de Seguridad de la Información es un diseño formal que promueve consistentes y efectivos mecanismos para la definición e implementación de controles.

Los componentes deben estar dirigidos a identificar los niveles de riesgo presentes y las acciones que se deben implementar para reducirlos.

Un adecuado modelo de seguridad debe incluir políticas, procedimientos y estándares definidos de acuerdo con las características del negocio.

Se debe contar con un plan de concientización adecuadamente estructurado para la creación de la cultura de seguridad en la organización. La seguridad de la información es tan buena como el nivel de entendimiento y capacitación que el personal tenga de los riesgos reales y las formas de protección.

Utilizar los recursos tecnológicos necesarios como soporte para un adecuado respaldo de las políticas.

Las mejores herramientas de seguridad son vulnerables si no existen políticas adecuadas que definan claramente su utilización.”⁸

2.4.3.6 RECUPERACIÓN FRENTE A CATÁSTROFES

“No todas las catástrofes se pueden evitar. Cada jurisdicción tiene un plan de contingencia frente a catástrofes y se gastan muchas horas cada año en la preparación de este plan. Dado que cada comunidad es diferente, los planes de recuperación tendrán en cuenta

⁷ http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica Se refiere a la seguridad Informática

⁸ <http://www.slideshare.net/luisrobles17/modelos-de-seguridad-de-la-informacin> Se refiere a los modelos de seguridad de la información

distintos factores. Si, por ejemplo, vive en una zona de inundaciones, debería tener un plan para proteger la red frente a niveles muy altos de concentración de agua.

Cuando se considera la protección frente a las catástrofes, necesitará un plan para el hardware, software y datos. Se pueden reemplazar las aplicaciones software y hardware y los sistemas operativos. Pero para realizar esto, es necesario, primero, conocer exactamente los recursos que se disponen.

Los componentes físicos de una red se pueden reemplazar fácilmente y, normalmente, están cubiertos por algún tipo de seguro, pero el problema se plantea con los datos que son altamente vulnerables a las catástrofes. En caso de incendio, puede reemplazar todos los equipos y hardware, pero no los archivos, diseños y especificaciones para un proyecto multimillonario que ha preparado la organización durante el último año.

Para conseguir una recuperación total frente a cualquier catástrofe, se necesita:

- ▶ Realizar un plan de recuperación.
- ▶ Implementar el plan.
- ▶ Comprobar el plan.”⁹

2.4.3.7 VIRUS INFORMÁTICOS

Los virus son bits de programación de equipos o código, que se ocultan en los programas de equipos o en el sector de arranque de los dispositivos de almacenamiento, como unidades de disco duro o unidades de disco. El principal propósito de un virus es reproducirse, así mismo, con tanta asiduidad como sea posible y, finalmente, destruir el funcionamiento del equipo o programa infectado. Una vez activado, un virus puede ser un simple anuncio o completamente catastrófico en su efecto. Los virus son desarrollados por gente que tiene la intención de hacer daño.

Los virus se clasifican en dos categorías, en función de su manera de propagarse

El primer tipo, denominado «virus del sector de arranque», reside en el primer sector de una unidad de disco o disco duro, el virus se ejecuta cuando arranca el equipo. Se trata de un método habitual de transmisión de virus de un medio de almacenamiento a otro. Cada vez que se inserta y se accede a un nuevo disco, el virus se reproduce en la nueva unidad.

⁹ <http://es.scribd.com/doc/52469203/Concepto-de-Red-Local-215>

El segundo tipo de virus se conoce como un «contaminador de archivos». Estos virus se unen a un archivo o programa y se activan en el momento en que se utiliza el archivo. Existen muchas subcategorías de contaminadores de archivos.

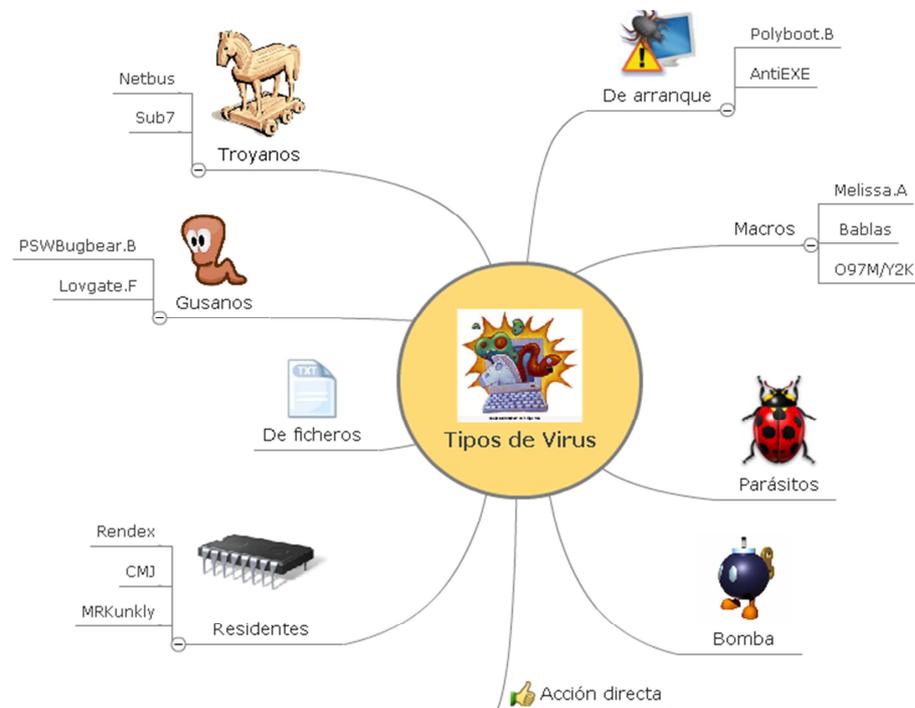


FIGURA 2.17 TIPOS DE VIRUS INFORMÁTICOS

Fuente: <http://ticinformativ.blogspot.com/2012/04/clasificacion-de-virus-informaticos.html>

Algunos de los contaminadores de archivos más habituales, son:

- ▶ Virus acompañante. Se denomina de esta forma debido a que utiliza el nombre de un programa real, su compañero. Un virus acompañante se activa utilizando una extensión de archivo diferente de su compañero. Por ejemplo, supongamos que decidimos ejecutar un programa denominado «procesadortextos.exe». Cuando se utiliza el comando para ejecutar la aplicación se ejecutará en su lugar, un virus denominado «procesadortextos.com». Esto es posible porque el archivo .com tiene prioridad sobre un archivo .exe.
- ▶ Virus de macro. Un virus de macro es difícil de detectar y se han hecho muy populares. Se denominan de esta forma porque se escriben como una macro para una aplicación específica. Los objetivos de estos virus son las aplicaciones más

utilizadas, como Microsoft Word. Cuando el usuario abre un archivo que contiene el virus, éste se une a la aplicación y, a continuación, infecta cualquier otro archivo que utilice la aplicación.

- ▶ Virus polimórficos. Un virus polimórfico se denomina de esta forma debido a que modifica su apariencia cada vez que se reproduce. Esto hace que sea más difícil de detectar puesto que no tenemos dos virus exactamente iguales.
- ▶ Virus camuflable. Un virus camuflable se denomina así debido a que intenta por todos los medios evitar que lo detecten. Cuando el programa antivirus intenta localizarlo, el virus camuflable intenta interceptar el análisis y devuelve información falsa indicando que no existe el citado virus.¹⁰

2.4.4 FIREWALL

“Es una parte de un sistema o una red que está diseñada para bloquear o denegar el acceso a personas no autorizadas a una pc, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

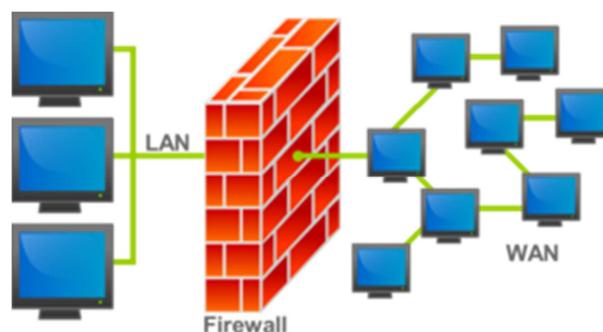


FIGURA 2.18 FIREWALL

Fuente: <http://infoaprende.web44.net/infoaprende/firewall-o-cortafuegos/>

¹⁰ <http://www4.uji.es/~al053184/main.html> Hace referencia a los virus informáticos

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección”¹¹

2.4.4.1 POLÍTICAS DEL CORTAFUEGOS

“Hay dos políticas básicas en la configuración de un cortafuego que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

- **Política restrictiva:** Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.
- **Política permisiva:** Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.”¹²

¹¹ <http://infoaprende.web44.net/infoaprende/firewall-o-cortafuegos/>

¹² http://iscseguridad.blogspot.com/2012/05/unidad-4-seguridad-en-la-comunicacion_30.html

2.4.4.2 TIPOS DE FIREWALL

“Conceptualmente, se pueden distinguir dos tipos diferentes de firewalls:

- ▶ Nivel de red.
- ▶ Nivel de aplicación.

FIREWALLS DEL NIVEL DE RED

Toman decisiones según la dirección de procedencia, dirección de destino y puerto de cada uno de los paquetes IP. Un simple router es un ejemplo de firewall de nivel de red, con la deficiencia de que no pueden tomar decisiones sofisticadas. Los actuales cortafuegos de nivel de red permiten mayor complejidad a la hora de decidir; mantienen información interna acerca del estado de las conexiones que pasan por él.

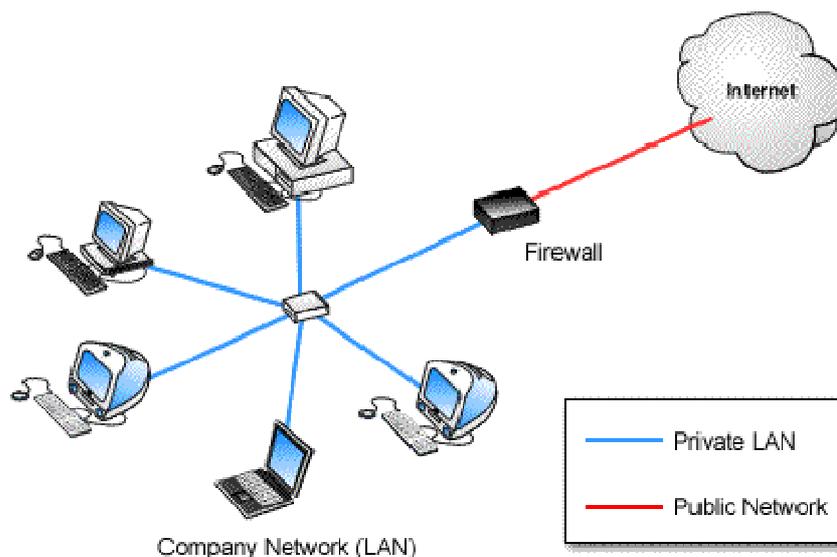


FIGURA 2.19 FIREWALL A NIVEL DE RED

Fuente: <http://www.desarrollandosoftware.com/posts/IPCop-Primera-Parte.html>

“Un firewall a nivel de red suele ser un encaminador de pantalla o un ordenador especial que examina las direcciones de los paquetes para determinar si el paquete debe pasar a la red local o se debe impedir el acceso.

En este tipo de firewalls se elaboran una especie de lista negra con las direcciones IP cuyo acceso desea impedir, además puede especificar los servicios que desea restringir su uso. Por ejemplo, puede permitir que los usuarios de Internet accedan a las páginas web de su red privada pero impedir que accedan mediante telnet o al servidor FTP. O bien hacer que se pueda acceder al servidor FTP y descarguen archivos desde él, para impedir que puedan transferir archivos a su servidor FTP.

Parámetros para diseñar un firewall a nivel de red:

- ▶ La dirección de origen de la que provienen los datos.
- ▶ La dirección de destino de los datos.
- ▶ El protocolo de sesión de los datos; TCP, UDP, ICMP.
- ▶ El puerto de aplicación de origen y destino del servicio deseado.
- ▶ Si el paquete es el inicio de una petición de conexión.

Un firewall a nivel de red correctamente configurado será transparente a los usuarios de su red, a no ser que intenten realizar una acción no permitida, como enviar información a una máquina que se encuentra en la lista negra. Además todos los usuarios externos incluidos en la lista negra, no podrán enviar ni recibir paquetes a y desde su red.”¹³

FIREWALLS DE NIVEL DE APLICACIÓN

Un firewall a nivel de aplicación suelen ser ordenadores que ejecutan software de servidor proxy, con lo que los administradores de red suelen referirse a estos firewalls simplemente como servidor proxy. Los servidores proxy se comunican con los servidores de internet en nombre de los usuarios. Los usuarios de una red que se conectan a Internet a través de un proxy aparecen para los ordenadores de internet con la dirección IP del servidor proxy (lo cual es muy apropiado para enmascarar las direcciones IP de la LAN).

Los servidores proxy se pueden configurar para los diferentes protocolos, puede permitir que se acceda a su servidor FTP para descargar archivos pero impedir que se envíen archivos a su servidor FTP. Existen servidores proxy para diferentes servicios; HTTP, FTP, Telnet. Al implementar servidores proxy es necesario cerciorarse que las

¹³ http://docente.ucol.mx/ychavezt/public_html/FIREWALL.htm

aplicaciones cliente soportan el proxy instalado. Con los servidores proxy se puede controlar fácilmente el tráfico que pasa por ellos.

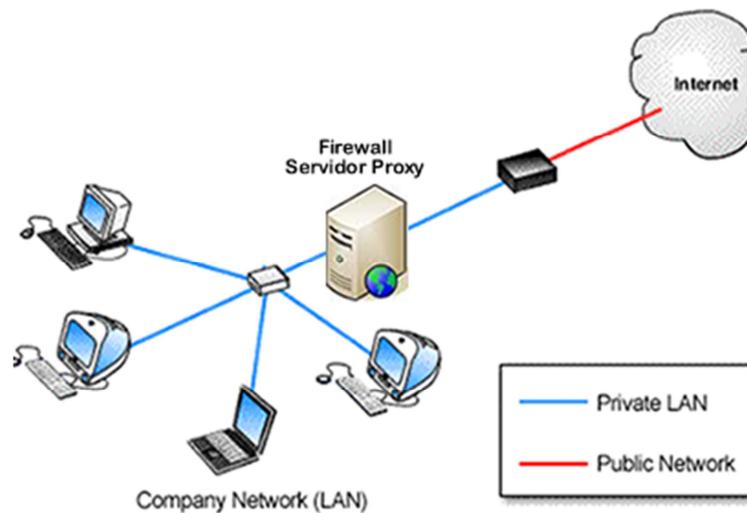
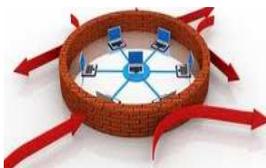


FIGURA 2.20 FIREWALL A NIVEL DE APLICACIÓN

2.4.4.3 BENEFICIOS DE UN FIREWALL EN INTERNET

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, los servidores propios del sistema están expuestos al ataque de otros servidores en el Internet.



El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no autorizados (tal, como., hackers, crackers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran la red privada. El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos.

2.4.5 PROXY

Un proxy, en una red informática, realiza una acción en representación de otro, esto es, si una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B; C entonces no sabrá que la petición procedió originalmente de A. Su finalidad más habitual es la de servidor proxy, que sirve para interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

Realiza una tarea como es el acceso a Internet en lugar de otro ordenador. Un proxy es un punto intermedio entre un ordenador conectado a Internet y el servidor al que está accediendo. Cuando se navega a través de un proxy, en realidad no se está accediendo directamente al servidor, sino que se realiza una solicitud sobre el proxy y es éste quien se conecta con el servidor que se necesita acceder y devuelve el resultado de la solicitud.¹⁴

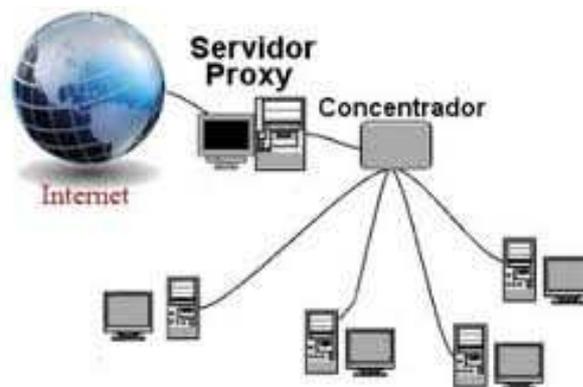


FIGURA 2.21 PROXY

2.4.5.1 PROXY DE WEB / PROXY CACHE DE WEB

Se trata de un proxy para una aplicación específica; el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con una mejora en los

¹⁴ <http://es.wikipedia.org/wiki/Proxy> Hace referencia a Proxy

tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

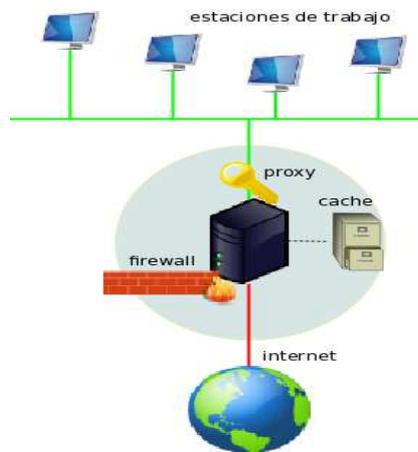


FIGURA 2.22 PROXY DE CACHE WEB

FUNCIONAMIENTO

1. El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
2. Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargó en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones.

Un cliente de un ISP manda una petición a Google la cual llega en un inicio al servidor Proxy que tiene este ISP, no va directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta en mucho menor tiempo. Cuando el usuario crea una búsqueda en Google el servidor Proxy ya no es utilizado; el ISP envía su petición y el cliente recibe su respuesta ahora sí desde Google.

2.4.6 SISTEMA DE AUTENTICACIÓN

Autenticación, en términos de seguridad de redes de datos, se puede considerar uno de los tres pasos fundamentales (AAA). Cada uno de ellos es, de forma ordenada:

- ▶ **Autenticación** *En la seguridad de ordenador* es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. *En un web de confianza*, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que son.
- ▶ **Autorización** Proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.
- ▶ **Auditoría** Mediante la cual la red o sistemas asociados registran todos y cada uno de los accesos a los recursos que realiza el usuario autorizados o no.

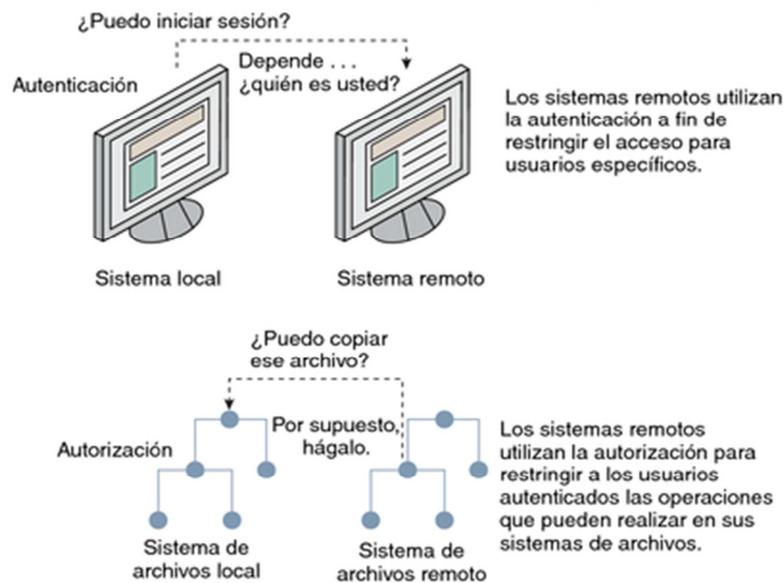


FIGURA 2.23 PROTOCOLO AAA

Fuente: http://docs.oracle.com/cd/E26921_01/html/E25886/concept-4.html

El uso más exacto describe la autenticación como el proceso de verificar la identidad de una persona, mientras la autorización es el proceso de verificación que una persona conocida tenga la autoridad para realizar una cierta operación. La autenticación, por lo tanto, debe preceder la autorización.

Autenticación hace referencia al proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y unos credenciales por parte del usuario que demanda acceso.

Un tipo habitual de credencial es el uso de una contraseña (password) que junto al nombre de usuario permite acceder a determinados recursos. El nombre de usuario es la identidad de una persona, que puede ser públicamente conocida, mientras que la contraseña se mantiene en secreto, y sirve para que nadie suplante dicha identidad.

Existen muchos métodos concretos que implementan el proceso de la autenticación como por ejemplo:

- **AUTENTICACIÓN DE SISTEMA (SYSTEM AUTHENTICATION)**.- típica en un sistema Unix, normalmente realizada mediante el uso del fichero `/etc/passwd`;
- **PROCOLOS PAP** (Password Authentication Protocol), y su versión segura CHAP (Challenge Handshake Authentication Protocol), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP.
- **LDAP** (Lightweight Directory Access Protocol), un protocolo a nivel de aplicación (sobre TCP/IP) que implementa un servicio de directorio ordenado, y muy empleado como base de datos para contener nombres de usuarios y sus contraseñas;
- **KERBEROS**, el famoso método de autenticación diseñado por el MIT.
- **EAP** (Extensible Authentication Protocol), que no es un método concreto sino un entorno universal de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto.

AUTORIZACIÓN

Se refiere a conceder servicios específicos (entre los que se incluye la “negación de servicio”) a un determinado usuario, basándose para ellos en su propia autenticación, los servicios que está solicitando, y el estado actual del sistema. Es posible configurar restricciones a la autorización de determinados servicios en función de aspectos como,

por ejemplo, la hora del día, la localización del usuario, o incluso la posibilidad o imposibilidad de realizar múltiples “logins” de un mismo usuario.

El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

No se debe confundir los términos autenticación con autorización. Mientras que la autenticación es el proceso de verificar un derecho reclamado por un individuo (persona o incluso ordenador), la autorización es el proceso de verificar que una persona ya autenticada tiene la autoridad para efectuar una determinada operación.

2.4.6.1 INTEROPERABILIDAD

Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

2.4.7 LABORATORIO INFORMÁTICO

Un laboratorio informático debe estar en capacidad de:

- 1.- Guiar y orientar a los alumnos en el uso de la información, entiéndase, enciclopedias, bibliotecas digitales, software, y programas de herramientas Informáticas, aplicaciones de red, así como proporcionar acceso a los alumnos para usar sus propios recursos.
- 2.- Potenciar que los alumnos se vuelvan activos en el proceso de aprendizaje auto dirigido, en el marco de acciones de aprendizaje abierto.
- 3.- Asesorar y gestionar el ambiente de aprendizaje en el que los alumnos están utilizando los recursos de aprendizaje. Tienen que ser capaces de guiar a los alumnos en el desarrollo de experiencias cooperativas, monitorear el progreso del estudiante; proporcionar feedback de apoyo al trabajo del estudiante; y ofrecer oportunidades reales para la difusión del trabajo del estudiante.

2.4.7.1 CARACTERÍSTICAS

Un laboratorio de Informática no puede ser solo un conjunto de ordenadores conectados entre sí que les dan la posibilidad a los usuarios de explotar el ordenador y los servicios que puede brindar la red institucional y/o Internet. El laboratorio debe ser un centro potencial de aprendizajes, de búsqueda y tratamiento de información precisa, útil y viable.

La consideración de estos nuevos escenarios de entornos tecnológicos, donde el laboratorio de Informática juega un importante papel, coloca a los docentes, ante la disyuntiva, principalmente pedagógica y no tecnológica, del empleo de las Tecnologías de la Información y las Comunicaciones (TIC) en aras de hacer más eficiente el Proceso de Enseñanza – Aprendizaje.

2.4.7.2 REQUERIMIENTOS

Un laboratorio de informática requiere concepciones del proceso de enseñanza y aprendizaje en las que se acentúa la participación activa del alumno en su propio proceso de aprendizaje; la preparación de los niños para asumir responsabilidades en un mundo en rápido y constante cambio.

La masificación de las redes informáticas en los institutos de enseñanza, ha contribuido a permitir que el maestro se dedique al rol de facilitador, logrando mayor independencia y flexibilidad de los estudiantes.

2.4.8 INTRANET

Una Intranet es una red o un conjunto de redes informáticas interconectadas pertenecientes a una misma institución. Como en todas las redes informáticas, el propósito fundamental de la Intranet es compartir información y recursos entre los distintos usuarios de la misma, lo que distingue a una Intranet de otros tipos de redes es el protocolo usado para la comunicación entre los ordenadores, que es el TCP/IP, el mismo que se utiliza en Internet. Con lo cual una Intranet puede ser considerada como una Internet a pequeña escala.

2.4.8.1 DHCP

DHCP (sigla en inglés de Dynamic Host Configuration Protocol- Protocolo de configuración dinámica de host) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

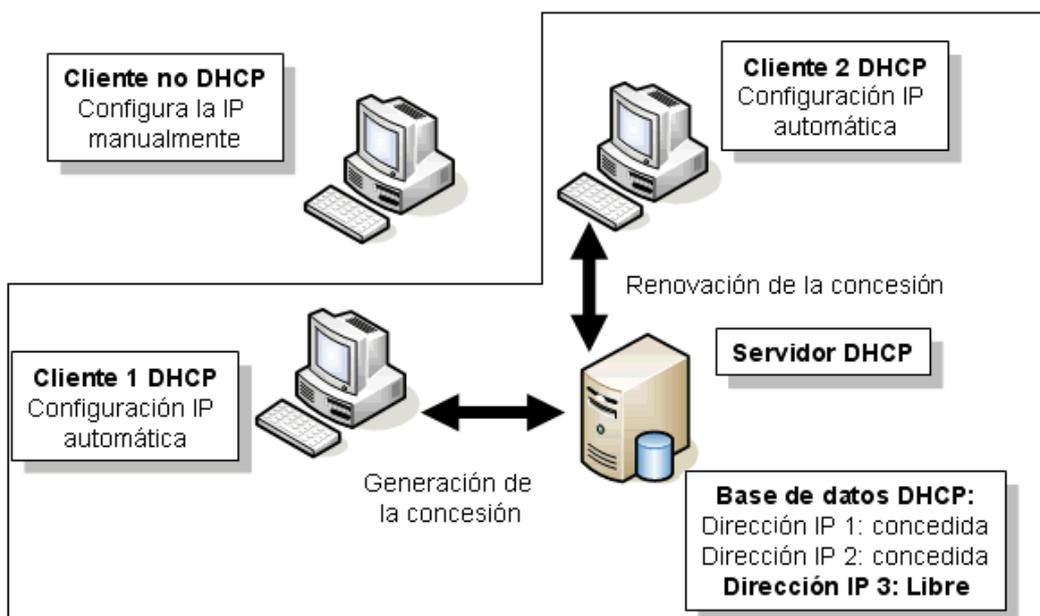


FIGURA 2.24 SERVIDOR DHCP - FUNCIONAMIENTO

Fuente: <http://www.adrformacion.com/cursos/exchange10/leccion2/tutorial2.html>

2.4.8.2 DNS

Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

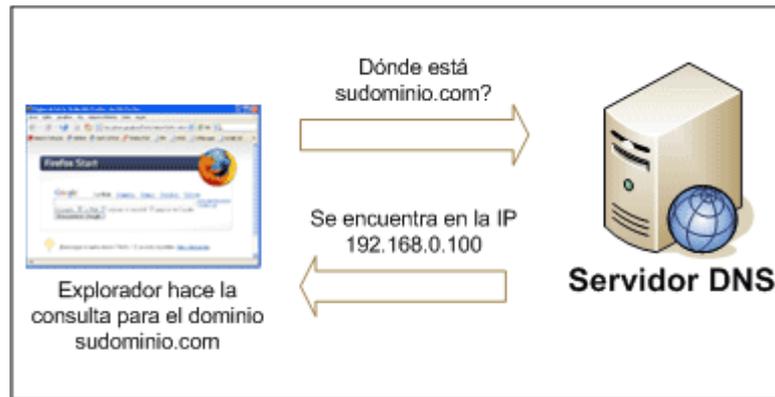


FIGURA 2.25 FUNCIONAMIENTO SERVIDOR DNS

Fuente: <http://culturacion.com/2011/01/como-funcionan-los-servidores-dns/>

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.mx es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.mx y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre.

DNS DE CACHEO (CACHING ONLY NAMESERVER)

Un servidor DNS CACHE sirve para "cachar" las peticiones que los clientes de una red le hacen a un servidor de nombres de dominio (DNS SERVER) que en la mayoría de los casos esta fuera de la propia LAN y que proporciona el proveedor de Internet (ISP - Internet Service Provider), posteriormente el Cache server conserva esa IP y el siguiente usuario que solicite la página, el mismo servidor local Linux lo resolverá, sin necesidad de hacer el viaje hasta el proveedor, reduciendo enormemente los tiempos de consulta.

Los servidores de cacheo no requieren administración experta, una oficina satélite es el único requisito para tener un DNS administrativo funcionado.¹⁵

2.4.9 TRATAMIENTO DE LA INFORMACIÓN

Se entiende por tratamiento de la información a las operaciones que las personas ejecutan con la información. Estas operaciones pueden ser muy variadas, por ejemplo:

- Lectura, escritura, copia, traducción, transmisión
- Ordenación, clasificación, comparación, archivo
- Cálculo, análisis, síntesis

2.4.9.1 TRATAMIENTO MANUAL

Tratamiento que realiza una persona de forma directa. A menudo se utiliza herramientas simples (lápiz, ábaco, máquina de escribir...)

2.4.9.2 TRATAMIENTO AUTOMÁTICO

Se realiza a través de dispositivos que generan procesos automáticos siguiendo las instrucciones de un programa.

2.4.10 E-LEARNING



El e-learning consiste en la educación y capacitación a través de Internet. Este tipo de enseñanza online permite la interacción del usuario con el material mediante la utilización de diversas herramientas informáticas.

Este nuevo concepto educativo es una revolucionaria modalidad de capacitación que hoy se posiciona como la forma de capacitación predominante en el futuro. Este sistema ha

¹⁵ http://es.wikipedia.org/wiki/Domain_Name_System Se refiere a Servicios de Nombres de dominio

transformado la educación, abriendo puertas al aprendizaje individual y organizacional. Es por ello que hoy en día está ocupando un lugar cada vez más destacado y reconocido dentro de las organizaciones empresariales y educativas.

El término "e-learning" es la simplificación de Electronic Learning. El mismo reúne a las diferentes tecnologías, y a los aspectos pedagógicos de la enseñanza y el aprendizaje.

El e-learning comprende fundamentalmente los siguientes aspectos:

- ▶ El pedagógico, referido a la Tecnología Educativa como disciplina de las ciencias de la educación, vinculada a los medios tecnológicos, la psicología educativa y la didáctica.
- ▶ El tecnológico, referido a la Tecnología de la Información y la Comunicación, mediante la selección, diseño, personalización, implementación, alojamiento y mantenimiento de soluciones en donde se integran tecnologías propietarias y de código abierto (Open Source).

2.4.10.1 AULA VIRTUAL



Permite promover la comunicación fuera de los límites áulicos entre los alumnos y el docente, o para los alumnos entre sí. Este sistema permite que los alumnos se familiaricen con el uso de las tecnologías, les da acceso a los materiales de clase desde cualquier computadora conectado a la red, les permite mantener la clase actualizada con últimas publicaciones de buenas fuentes, y especialmente en los casos de clases numerosas, los alumnos logran comunicarse aun fuera del horario de clase sin tener que concurrir a clases de consulta, pueden compartir puntos de vista con compañeros de clase, y llevar a cabo trabajos en grupo. También permite limitar el uso fotocopias ya que los alumnos deciden si van a guardar las lecturas y contenidos de la clase en un usb para leer de la pantalla, o si van a imprimirlo, según los estilos de aprendizaje de cada uno.

2.4.10.2 EL AULA VIRTUAL EN FORMATO SINCRÓNICO

Estos servicios son aquellos en que el emisor y receptor del mensaje en el proceso de comunicación operan en el mismo marco temporal, es decir para que se pueda transmitir dicho mensaje, es necesario que las dos personas estén presentes en el mismo momento.

Para este tipo de servicio, se requiere mayor cantidad de recursos tecnológicos, así como disponibilidad horaria por parte de quienes efectúan las tareas de tutores o maestros, ya que este tipo de relación es 1 a 1 en línea. Este tipo de formato está pensado por ejemplo, para casos en los cuales el público al que va dirigido se encuentra en una región geográfica de difícil acceso o en el caso de alumnos que se encuentren realizando trabajo de campo con supervisión de sus maestros.

2.4.10.3 EL AULA VIRTUAL EN FORMATO ASINCRÓNICO

Este formato de Aula Virtual, constituye uno de los recursos más valiosos para su utilización en la modalidad de educación a distancia, ya que el acceso en forma diferida en el tiempo de la información, se hace absolutamente necesaria por las características especiales que presentan los estudiantes (limitación de tiempo, cuestiones familiares y laborales, etc.).

Generalmente, en la mayoría de los casos será el formato a preferir por las facilidades que presenta a la hora de darle al estudiante varias de las ventajas mencionadas en el párrafo anterior, con la consecuente ventaja que esto representa tanto para el alumno como para la institución educativa.

2.5 HIPÓTESIS

La implementación de un sistema de autenticación unificada influye en la transmisión de la información dentro de la Escuela Sagrada Familia

2.6 DETERMINACIÓN DE VARIABLES DE LA HIPÓTESIS

VARIABLE INDEPENDIENTE

Sistema de Autenticación Unificada

VARIABLE DEPENDIENTE

Transmisión de la Información

CAPITULO III

MARCO METODOLOGICO

3.1 ENFOQUE

La presente investigación estará enmarcada dentro del paradigma crítico propositivo por lo tanto tendrá un enfoque cuali-cuantitativo porque se realizará una investigación de todas las causas y factores referentes al tema del proyecto y la información proporcionada servirá de referencia para interpretarla con el sustento científico y profesional así como el tratamiento estadístico de los datos con lo que se pretende solucionar el problema.

3.2 MODALIDAD BÁSICA DE LA INVESTIGACIÓN

3.2.1 INVESTIGACIÓN DE CAMPO

Se realizará una investigación de campo con el fin de recolectar información real desde el lugar donde surge el problema de investigación en este caso la escuela “Sagrada Familia”.

3.2.2 INVESTIGACIÓN BIBLIOGRÁFICA – DOCUMENTAL

Se realizará una investigación bibliográfica - documental para poder obtener información más profunda con respecto a problemas similares, de esta manera se recopilará información valiosa que servirá como sustento científico del proyecto.

3.3 NIVEL O TIPO DE INVESTIGACIÓN

3.3.1 EXPLORATORIO

La investigación es de nivel exploratorio debido a la necesidad de conocer el ambiente de la Institución e indagar las causas del problema. Se detectará las características del problema y determinará si es factible o no de solucionarse.

3.3.2 DESCRIPTIVO

El proceso investigativo tendrá un nivel descriptivo porque se analizará el problema, estableciendo sus causas y consecuencias así como las dificultades por las que está atravesando.

3.3.3 ASOCIACIÓN DE VARIABLES

Se llegará a establecer la relación de una variable con la otra y la incidencia que tiene en la solución del problema.

3.4 POBLACIÓN Y MUESTRA

3.4.1 POBLACIÓN

Los beneficiarios del proyecto dentro de la institución son estudiantes, maestros y administrativos sin embargo los estudiantes por ser un grupo de niños de muy corta edad no se los ha tomado en cuenta para el desarrollo de la presente investigación, de tal forma que la población está conformada por 12 personas entre Administrativos y Docentes, como se detalla en la tabla 2.2

Población	Total	Frecuencia
Administrativos	2	17%
Docentes	10	83%
Total	12	100%

TABLA 2.2 POBLACIÓN
Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

3.4.2 MUESTRA

Para definir la muestra a investigarse, se utilizó el método estadístico “Modus Ponendo Ponens”, el cuál establece entre dos enunciados una relación de causa-efecto. La regla ‘ponendo ponens’ significa, “afirmando afirmo” y en un condicional establece, que si el antecedente (primer término, en este caso p) se afirma, necesariamente se afirma el consecuente (segundo término, en este caso q).

$p \rightarrow q$ “Si la población es reducida, entonces la muestra es igual a la población” **premisa**

p “La población es reducida” **premisa**

q “La muestra es igual a la población” **Conclusión**

La conclusión fue que “la población es igual a la muestra”, por lo tanto todos los integrantes de la población en este caso, docentes y administrativos de la institución, pasan a ser la muestra.

3.5 OPERACIONALIZACIÓN DE VARIABLES

3.5.1 VARIABLE INDEPENDIENTE

CONCEPTUALIZACIONES	DIMENSIONES	INDICADORES	ÍTEMS
<p>SISTEMA DE AUTENTICACIÓN UNIFICADA</p> <p>Proceso de <u>verificar</u> la <u>identidad digital</u> de un <u>usuario</u> para <u>autorizar el acceso</u> a una entidad</p>	Verificación de la identidad	Intranet	¿Qué utilidades ofrece una intranet?
		Seguridad	¿Qué herramientas informáticas se utiliza en una intranet?
	Autorización de Acceso	Servidor	¿Cuáles son los métodos de seguridad más indicados para asegurar una intranet?
		Controles	¿Cuáles son las técnicas de control de acceso más adecuadas para una institución?
			Que autorizaciones de acceso se pueden implantar en un servidor?

TABLA 3.1 OPERACIONALIZACIÓN DE VARIABLES – SISTEMA DE AUTENTICACIÓN UNIFICADA

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

3.5.2 VARIABLE DEPENDIENTE

CONCEPTUALIZACIONES	DIMENSIONES	INDICADORES	ÍTEMS
TRATAMIENTO DE LA INFORMACIÓN <u>Operaciones</u> que las personas <u>ejecutan</u> con la <u>información</u>	Operación ejecutadas	Beneficios	¿Qué operaciones son ejecutadas comúnmente por los usuarios?
		Riesgos	¿Qué riesgos se contraen con la transmisión de la información? ¿Qué beneficios conlleva el tratar la información con precaución?
	Manipulación de la Información	Manual	¿Cómo manipulan la información los usuarios?
		Automática	Que ocurrencias manuales no deben ser cometidas con la información? Cuáles son las formas automáticas de manipular la información?

TABLA 3.2 OPERACIONALIZACIÓN DE VARIABLES – TRATAMIENTO DE LA INFORMACIÓN

Fuente. Encuesta personal docente

Elaborado por: Adriana Salinas

3.6 RECOLECCIÓN DE LA INFORMACIÓN

3.6.1 PLAN DE RECOLECCIÓN DE INFORMACIÓN

La recolección de información se realizará mediante la aplicación de encuestas (Anexo A), las mismas que estarán dirigidas a los docentes y personal administrativo de la institución educativa “Sagrada Familia” de la ciudad de Ambato.

Se seleccionó la encuesta como método de recolección de información por ser una herramienta que permite comparar y cuantificar el peso de las distintas opiniones expresadas, ofreciendo la ventaja de permitir el tratamiento estadístico de la información de forma clara, rápida y eficaz.

La encuesta se orientó hacia las necesidades e inconvenientes resididas dentro de la institución, con respecto al departamento informático, específicamente al tratamiento de la información, autenticación y aulas virtuales.

3.7 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

3.7.1 PLAN QUE SE EMPLEARÁ PARA PROCESAR LA INFORMACIÓN RECOGIDA

El procesamiento de la información se realizará, luego de aplicar la encuesta a los docentes y administrativos de la institución, mediante el siguiente orden:

- Recopilación y Revisión crítica de la información
- Realización de tabulaciones
- Organización de la información
- Elaboración de gráficos
- Registro de la información

3.7.2 PLAN DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

El análisis de resultados se realizará mediante la utilización del gráfico circular o pastel, el cuál utiliza radios para dividir el círculo en sectores, de manera que las áreas de los sectores son proporcionales a las cantidades representadas, lo cual permitirá representar porcentajes y proporciones, que muestren el número de veces que se cita una opción de respuesta, de forma clara y de fácil interpretación.

Finalmente se podrá llegar a comprobar la hipótesis planteada y además establecer conclusiones y recomendaciones que servirán de apoyo para realizar de manera eficiente el diseño del Sistema de Autenticación Unificada dentro de la institución.

CAPITULO IV

ANALISIS E INTERPRETACION DE RESULTADOS

4.1 RECOPIACIÓN DE LA INFORMACIÓN

Los datos obtenidos en el presente trabajo de investigación fueron tabulados según la encuesta realizada al personal Administrativo y Docente de la escuela “Sagrada Familia”, éstos datos fueron analizados de forma sistemática e interpretada estadísticamente para obtener conclusiones válidas. Se ha utilizado la herramienta Microsoft Office Excel, para realizar los respectivos gráficos, en los cuales se detalla el porcentaje de cada ítem en relación a las respuestas.

Al final de cada uno de los gráficos, se encuentra explícito el análisis e interpretación respectivo de acuerdo a los resultados obtenidos, de ésta forma se exterioriza la problemática investigada.

Se trabajó con una población integrada por 12 personas, que comprenden todo el Universo a investigarse, quienes facilitaron los datos obtenidos.

4.2 ANÁLISIS E INTERPRETACIÓN DE LA INFORMACIÓN RECOLECTADA

Una vez realizada la encuesta al personal docente y administrativo de la escuela Sagrada Familia se obtuvieron los siguientes resultados, lo que servirá de base para comenzar a realizar el presente proyecto.

1. ¿SE SIENTE CONFORME CON EL ACTUAL MANEJO Y TRANSMISIÓN DE INFORMACIÓN DENTRO LA INSTITUCIÓN?

RESPUESTAS	CANTIDAD	PORCENTAJE
SI	6	50%
NO	6	50%
TOTAL	12	100%

TABLA 4.3 DATOS DE CONFORMIDAD CON EL MANEJO Y TRANSMISIÓN DE INFORMACIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

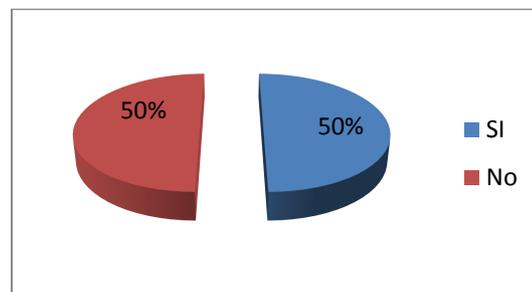


FIGURA 4.3 RESULTADOS SOBRE EL MANEJO Y TRANSMISIÓN DE INFORMACIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

El gráfico, ilustra que un 50% de la población está conforme con el manejo de la información actual, mientras que el otro 50% está en desacuerdo con la transmisión de los datos.

INTERPRETACIÓN

Se interpretó que las personas investigadas se sienten en parte conformes con el manejo de la información sin embargo necesitan mejoras y alternativas de actualización.

2. ¿ESTA CONSCIENTE DE LOS ATAQUES DE TERCEROS QUE PUEDE SUFRIR LA INSTITUCIÓN?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	9	75%
NO	3	25%
TOTAL	12	100%

TABLA 4.4 DATOS DE CONFORMIDAD CON ATAQUES INFORMÁTICOS A LA INSTITUCIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

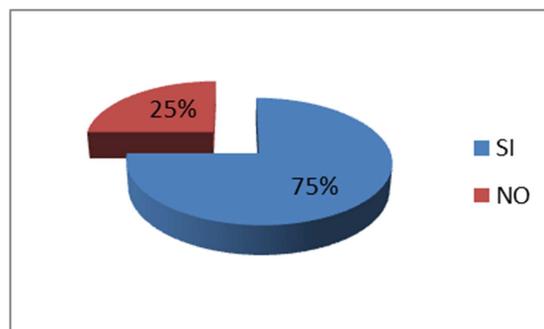


FIGURA 4.4 RESULTADOS SOBRE CON ATAQUES INFORMÁTICOS A LA INSTITUCIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

La grafica indica que el 75% de los encuestados está consciente de los posibles ataques de terceros que puede sufrir la institución mientras que tan solo un 25% no conoce o no siente que le conciernen los ataques maliciosos que se pueden suscitar.

INTERPRETACIÓN

Se concluyó que la gran mayoría de docentes y administrativos entiende que la información es invaluable y necesita protección.

3. ¿HA SUFRIDO PÉRDIDAS DE INFORMACIÓN EN LOS COMPUTADORES DEL INSTITUTO?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	3	25%
NO	9	75%
TOTAL	12	100%

TABLA 4.5 DATOS DE CONFORMIDAD CON PÉRDIDAS DE INFORMACIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

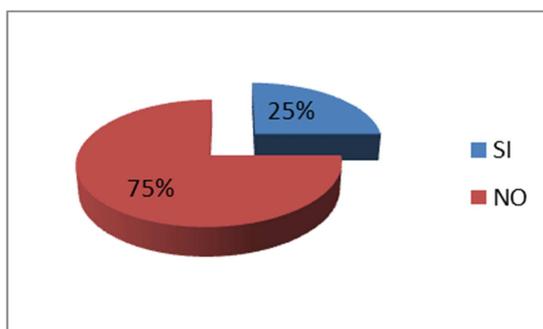


FIGURA 4.5 RESULTADOS SOBRE CON PÉRDIDAS DE INFORMACIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

De acuerdo al gráfico ilustrado se el 75% de los encuestados no ha tenido pérdidas de la información dentro de la institución, mientras que un 25% si los ha sufrido.

INTERPRETACIÓN

Se determinó que dentro del establecimiento educativo generalmente no se pierde la información, sin embargo a considerar por el $\frac{1}{4}$ de encuestados que respondió lo contrario se concluye que es necesaria una mejora en el control de la información.

4. ¿OPINA UD. QUE UNA RED INALÁMBRICA PERMITIRÁ UNA GESTIÓN Y EXPLOTACIÓN MUCHO MÁS EFICAZ DE LOS RECURSOS INFORMÁTICOS?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	11	92%
NO	1	8%
TOTAL	12	100%

TABLA 4.6 DATOS DE CONFORMIDAD CON LA RED INALÁMBRICA

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

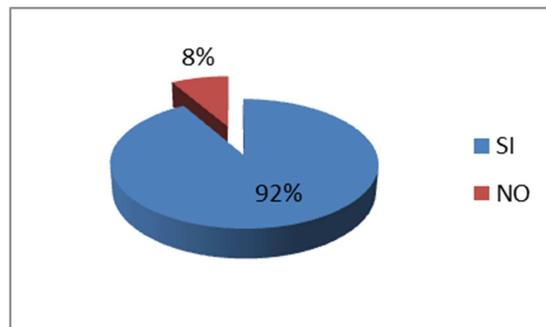


FIGURA 4.6 RESULTADOS SOBRE LA RED INALÁMBRICA

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

El gráfico muestra que el 92% de los encuestados opina que una red inalámbrica permitirá gestionar de mejor manera los recursos informáticos mientras que tan solo un 8% opina lo contrario.

INTERPRETACIÓN

Se concluyó que en su mayoría los encuestados, están de acuerdo en que una red inalámbrica permitirá una gestión y explotación mucho más eficaz de los recursos informáticos, y aprueban las redes inalámbricas, además de que les parece una buena opción la implantación de las mismas dentro de la institución.

5. ¿ESTÁ COMPLETAMENTE CONFORME CON LA VELOCIDAD DEL INTERNET DENTRO LA INSTITUCIÓN?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	5	42%
NO	7	58%
TOTAL	12	100%

TABLA 4.7 DATOS DE CONFORMIDAD CON LOS INCONVENIENTES DE LA INSTITUCIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

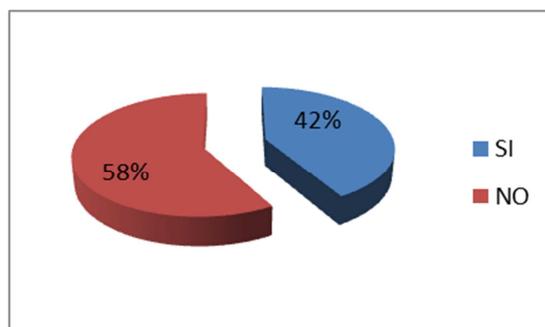


FIGURA 4.7 RESULTADOS SOBRE LOS INCONVENIENTES DE LA INSTITUCIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

De acuerdo a la gráfica el 58% de los encuestados no está conforme con el internet brindado en la institución y el 42% a diferencia de ese grupo se encuentra conforme con la velocidad del mismo.

INTERPRETACIÓN

Se dedujo que la mayoría de los encuestados encuentra inconvenientes en la velocidad del internet, lo cual indica que es necesario aplicar medidas que modifiquen y mejoren la eficiencia del internet.

6. ¿LE PARECE IMPORTANTE EL MANEJO DE AULAS VIRTUALES DENTRO DE LA ESCUELA?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	12	100%
NO	0	0%
TOTAL	12	100%

TABLA 4.8 DATOS DE CONFORMIDAD CON EL MANEJO DE AULAS VIRTUALES

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

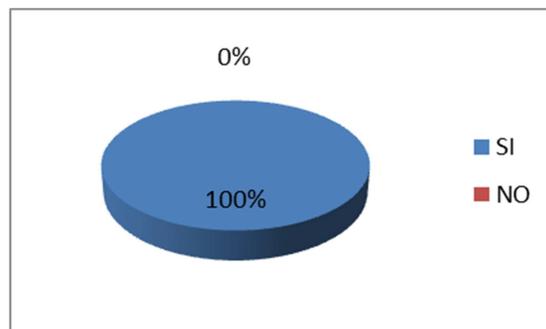


FIGURA 4.8 RESULTADOS SOBRE EL MANEJO DE AULAS VIRTUALES

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

Según el diagrama estadístico el 100% de los encuestados opina que las aulas virtuales son importantes para el buen desempeño de la institución.

INTERPRETACIÓN

Se interpretó que todos los docentes y administrativos están conscientes de los beneficios que se puede concebir mediante la implantación de las aulas virtuales.

7. ¿CONSIDERA NECESARIA UNA AUTENTICACIÓN DE ACCESO AL INTERNET EN CADA COMPUTADOR DENTRO DEL LABORATORIO DE COMPUTACIÓN?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	11	92%
NO	1	8%
TOTAL	12	100%

TABLA 4.9 DATOS DE CONFORMIDAD CON LA AUTENTICACIÓN AL INTERNET

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

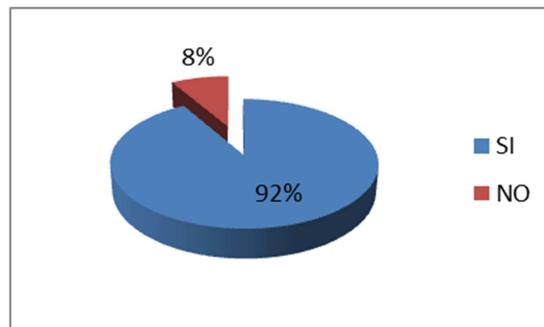


FIGURA 4.9 RESULTADOS SOBRE LOS INCONVENIENTES DE LA INSTITUCIÓN

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

El 92% de los encuestados está de acuerdo en que se implante un sistema de autenticación en la institución, de tal forma que en el laboratorio de computación se requiera el ingreso de usuario y contraseña para su utilización, mientras que tan solo el 8% estará en desacuerdo con esta noción.

INTERPRETACIÓN

Se concluyó que la gran mayoría está de acuerdo en que es necesaria la implantación de un sistema de autenticación para el acceso al internet entre otros servicios dentro de la institución.

8. ¿CREE Ud. QUE UNA RED ALÁMBRICA ESTRUCTURADA OPTIMIZARA LA VELOCIDAD DE COMUNICACIÓN?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	11	92%
NO	1	8%
TOTAL	12	100%

TABLA 4.10 DATOS DE CONFORMIDAD CON LA RED ALÁMBRICA

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

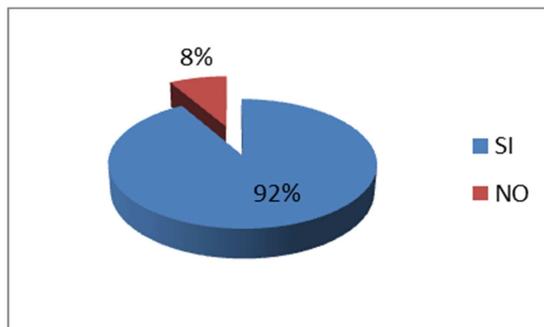


FIGURA 4.10 RESULTADOS SOBRE LA RED ALÁMBRICA

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

La gráfica indica que el 92% de los encuestados considera que una red alámbrica podría mejorar la velocidad de la comunicación y tan solo el 8% indica que no optimizaría la transmisión de la información.

INTERPRETACIÓN

Se concluyó que los docentes y administrativos en su gran mayoría aceptarían con agrado una conexión alámbrica para beneficio de la comunicación.

9. ¿CONSIDERA. QUE ES NECESARIO RESTRINGIR DETERMINADAS PÁGINAS WEB A LAS QUE SE TIENE ACCESO DENTRO DE LA ESCUELA?

RESPUESTA	CANTIDAD	PORCENTAJE
SI	9	75%
NO	3	25%
TOTAL	12	100%

TABLA 4.11 DATOS DE CONFORMIDAD CON LA RESTRICCIÓN DE PÁGINAS WEB

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

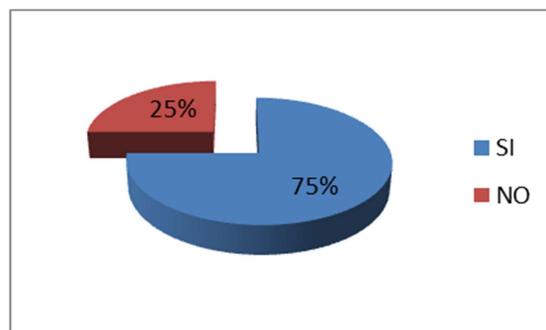


FIGURA 4.11 RESULTADOS SOBRE LA RESTRICCIÓN DE PÁGINAS WEB

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

ANÁLISIS

El 75% de los encuestados está de acuerdo en que se deben restringir determinadas páginas web dentro de la institución mientras que tan solo el 25% opina lo contrario

INTERPRETACIÓN

Se concluyó que a la gran mayoría de los encuestados no le importaría tener acceso restringido a páginas web de distracción personal entre otras.

4.3 VERIFICACIÓN DE LA HIPÓTESIS

Una vez tabuladas las encuestas, se procede a la comprobación de la hipótesis mediante el método estadístico: Chi-Cuadrado.

Formula:
$$x^2 = \sum \left(\frac{(O-E)^2}{E} \right)$$

Dónde:

x^2 = Chi Cuadrado

\sum = Sumatoria

O = Frecuencia Observada

E = Frecuencia técnica esperada

4.3.1 COMBINACIÓN DE FRECUENCIAS (FRECUENCIA OBSERVADA)

N°	Pregunta	Si	No	Total
1	¿Se siente Conforme con el actual manejo y transmisión de información dentro la institución?	6	6	12
2	¿Esta consiente de los ataques de terceros que puede sufrir la institución?	9	3	12
3	¿Ha sufrido pérdidas de información en los computadores del instituto?	3	9	12
4	¿Opina Ud. que una red inalámbrica permitirá una gestión y explotación mucho más eficaz de los recursos informáticos?	11	1	12
5	¿Está completamente conforme con la velocidad del internet dentro la institución?	5	7	12
6	¿Le parece importante el manejo de aulas virtuales dentro de la escuela?	12	0	12
7	¿Considera necesaria Una autenticación de acceso al internet en cada computador dentro del laboratorio de computación?	11	1	12
8	¿Cree Ud. que una red alámbrica estructurada optimizara la velocidad de comunicación?	11	1	12
9	¿Considera que es necesario restringir determinadas páginas web a las que se tiene acceso dentro de la escuela?	9	3	12
TOTAL		77	31	108

TABLA 4.12 COMBINACIÓN DE FRECUENCIA

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

4.3.2 FRECUENCIA ESPERADA

$$f_{e1} = (77 * 12)/108$$

$$f_{e2} = (31 * 12)/108$$

N°	Pregunta	Si	No	Total
1	¿Se siente Conforme con el actual manejo y transmisión de información dentro la institución?	8,55	3,44	12
2	¿Esta consiente de los ataques de terceros que puede sufrir la institución?	8,55	3,44	12
3	¿Ha sufrido pérdidas de información en los computadores del instituto?	8,55	3,44	12
4	¿Opina Ud. que una red inalámbrica permitirá una gestión y explotación mucho más eficaz de los recursos informáticos?	8,55	3,44	12
5	¿Está completamente conforme con la velocidad del internet dentro la institución?	8,55	3,44	12
6	¿Le parece importante el manejo de aulas virtuales dentro de la escuela?	8,55	3,44	12
7	¿Considera necesaria Una autenticación de acceso al internet en cada computador dentro del laboratorio de computación?	8,55	3,44	12
8	¿Cree Ud. que una red alámbrica estructurada optimizara la velocidad de comunicación?	8,55	3,44	12
9	¿Considera que es necesario restringir determinadas páginas web a las que se tiene acceso dentro de la escuela?	8,55	3,44	12
TOTAL		77	31	108

TABLA 4.13 FRECUENCIAS ESPERADAS

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

4.3.3 MODELO LÓGICO

Hipótesis Alternativa (H_a) = Hipótesis si

Hipótesis Nula (H_0) = Hipótesis no

4.3.4 NIVEL DE SIGNIFICANCIA Y REGLA DE DECISIÓN

4.3.4.1 GRADO DE LIBERTAD

Formula: $GL = (c-1)*(f-1)$

Siendo c el número de columnas y f el número de filas, el producto del número de celdas menos uno, por el número de filas menos uno

$$GL = (c-1)*(f-1)$$

$$GL = (9-1)*(2-1)$$

$$GL = (8)*(1)$$

$$GL = 8$$

4.3.4.2 GRADO DE SIGNIFICANCIA

Nivel de significación (P): Denominado nivel de confianza, se refiere a la probabilidad de que los resultados observados se deban al azar.

Este valor es fijado por el investigador, usualmente es el 5% o 10%. Lo que indica que si se toma $P=0.05$, se está significando que solo en un 5% de las veces en que se realice la medición, el resultado obtenido podría deberse al azar.

De lo contrario sería decir que existe un nivel de confianza del 95% que el resultado es real y no debido a la casualidad.

Nivel de confiabilidad = 95%

El grado de significancia será 0.05

VALORES CRÍTICOS DEL CHI CUADRADO

La tabla muestra valores χ^2 que corresponden a un área específica de la extremidad de la derecha y a un número determinado de grados de libertad.

<i>PROBABILIDAD DE UN VALOR SUPERIOR - ALFA (A)</i>					
GRADOS LIBERTAD	0,1	0,05	0,025	0,01	0,005
1	2,71	3,84	5,02	6,63	7,88
2	4,61	5,99	7,38	9,21	10,6
3	6,25	7,81	9,35	11,34	12,84
4	7,78	9,49	11,14	13,28	14,86
5	9,24	11,07	12,83	15,09	16,75
6	10,64	12,59	14,45	16,81	18,55
7	12,02	14,07	16,01	18,48	20,28
8	13,36	15,51	17,53	20,09	21,95
9	14,68	16,92	19,02	21,67	23,59
10	15,99	18,31	20,48	23,21	25,19
11	17,28	19,68	21,92	24,73	26,76
12	18,55	21,03	23,34	26,22	28,3
13	19,81	22,36	24,74	27,69	29,82
14	21,06	23,68	26,12	29,14	31,32
15	22,31	25	27,49	30,58	32,8
16	23,54	26,3	28,85	32	34,27

TABLA 4.14 VALORES CRÍTICOS DEL CHI CUADRADO

Se ubica en la tabla los grados de libertad y los grados de significancia, los grados de libertad son 8 y los de significancia son 0,05

$$X_{t^2}(c - 1) * (t - 1) = 15,51$$

4.3.5 CALCULO DEL CHI CUADRADO

$$x^2 = \sum \left(\frac{(O-E)^2}{E} \right)$$

(**O** – **E**) = Frecuencia Observada menos Frecuencia Esperada

-2,55	2,56
0,45	-0,44
-5,55	5,56
2,45	-2,44
-3,55	3,56
3,45	-3,44
2,45	-2,44
2,45	-2,44
0,45	-0,44

TABLA 4.15 DIFERENCIA DE FRECUENCIAS

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

$(O - E)^2$ = Cuadrado de la F. Observada menos la F. Esperada

6,50	6,55
0,20	0,19
30,80	30,91
6,00	5,95
12,60	12,67
11,90	11,83
6,00	5,95
6,00	5,95
0,20	0,19

TABLA 4.16 CUADRADO DE LA DIFERENCIA DE FRECUENCIAS

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

$\frac{(O-E)^2}{E}$ = Cuadrado de la Diferencia entre F. Observada y F. Esperada dividido para las F. Esperadas

0,76	1,91
0,02	0,06
3,60	8,99
0,70	1,73
1,47	3,68
1,39	3,44
0,70	1,73
0,70	1,73
0,02	0,06

TABLA 4.17 CUADRADO DE LA DIFERENCIA DE FRECUENCIAS DIVIDIDO PARA DOS

Fuente. Encuesta personal docente
Elaborado por: Adriana Salinas

La sumatoria de estos términos (todas las celdas del cuadro anterior) es 32,70

$$x^2 = 77,1$$

$$X_{t^2}(c - 1) * (t - 1) = 15,51$$

CRITERIO DE DECISIÓN:

$$X_2 < X_{t^2}(C - 1) * (f - 1) \quad \text{ACEPTA } H_0$$

VALORES DE DECISIÓN:

$$32,70 > 15,51 \quad \text{RECHAZA } H_0$$

Debido a que X_2 es mayor a $X_2 < X_{t^2}(C - 1) * (f - 1)$ se rechaza H_0 y se acepta H_a .

Por lo tanto el diseño configuración e implementación del Sistema de autenticación unificada para la correcta transmisión de la información en la escuela Sagrada Familia es factible.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

De acuerdo a lo observado anteriormente y según los datos obtenidos se pueden determinar las siguientes conclusiones:

- Los inconvenientes de la institución radican esencialmente en la velocidad de comunicación la cual se manifiesta principalmente en el uso del internet, el mismo que podría optimizarse mediante un adecuado control.
- La red inalámbrica es muy importante para el mejoramiento del actual manejo de la información interna de la institución, lo cual posibilitará la disminución mayor de errores de comunicación.
- Docentes y directivos apoyan completamente a la actualización tecnológica, de tal forma que la implementación de una plataforma educativa facilitará el trabajo dentro de la institución.
- Es necesaria una autenticación de acceso al internet con el fin de controlar el acceso de los niños a determinados sitios dañinos y obscenos.

5.2 RECOMENDACIONES

- Realizar mayor control sobre el servicio de internet dentro de la institución, tanto en horarios como en ancho de banda.
- Capacitar de mejor manera a los docentes sobre las nuevas tecnologías de la información y la comunicación
- Analizar las seguridades que serán necesarias dentro de la institución para evitar ataques de intrusos que podrían in-estabilizar el correcto funcionamiento del establecimiento.
- Tomar medidas de control con la finalidad de restringir sitios web que atenten contra la seguridad de la escuela además de organizar todo el tráfico que origina el internet dentro del plantel educativo.
- Generar una medida de control de autenticación para los servicios ofertados en la institución.

CAPITULO VI

LA PROPUESTA

6.1 DATOS INFORMATIVOS

Tema de la Propuesta: Implantación de un Sistema de Autenticación Unificada para mejorar y controlar el modo actual de transmisión de información en el Centro Educativo “Sagrada Familia” de la ciudad de Ambato

Grupo Objetivo: Elaborado para docentes y estudiantes que utilizan el servicio de internet, la intranet y la red inalámbrica del Centro Educativo “Sagrada Familia”

Ubicación: Av. de las Américas 4-74 y Brasil (Ex-Seminario Pío XII)

Tutor: Ing. Rene Terán

Autor: Adriana Cumandá Salinas Pérez

6.2 ANTECEDENTES DE LA PROPUESTA

Después de recolectar información y revisar los antecedentes del problema investigado, se concluyó que los usuarios del internet y de la red inalámbrica de la Institución, no están completamente satisfechos con el servicio de internet proporcionado a la institución siendo visible la necesidad de optimización del tráfico hacia el internet, autenticación, y restricción de acceso a determinados sitios web.

Concluida la investigación, una de las alternativas de solución al problema planteado es elaborar un Sistema de Autenticación Unificada para mejorar y controlar el modo actual de transmisión de información proveniente del internet donde éste forma parte de un importante recurso investigativo para estudiantes como también para docentes.

Este sistema presenta una excelente oportunidad para aprovechar los recursos de la institución, además de optimizar el servicio de internet el mismo que abrirá puertas de investigación a sus usuarios.

La Autenticación es un instrumento de control muy eficaz que al ser adecuadamente instaurado, previo al análisis de los requerimientos de la red permitirá llevar estructurada y organizadamente el servicio de internet.

6.3 JUSTIFICACIÓN

En la actualidad un factor importante en la revolución tecnológica ha sido la masificación del internet, su crecimiento y desarrollo han marcado una nueva era en el mundo actual, una era que abre puertas al desarrollo investigativo donde la información es encontrada de forma rápida y eficiente gracias a servidores ubicados en todo el mundo proporcionando información las 24 horas del día los 365 días del año.

Otro factor importante al avance del internet son los métodos de control y acceso a entornos de apoyo a la enseñanza como las aulas virtuales, ya que la información que se proporciona en estos medios debe ser bien llevada evitando caer en redes maliciosas.

Con los antecedentes expuestos anteriormente se pretende presentar como argumentos permisivos para el desarrollo de esta propuesta a los beneficios que conlleva el adecuado

control e inspección del uso del internet, ya que se minimizan los riesgos de ataques tanto de virus como de personas malintencionadas que puedan perjudicar a la institución mediante el mal uso de la información residente en la misma.

El filtrado de páginas web que socorre a la necesidad de proteger a los niños de sitios no deseados, como también el bloqueo de sitios no provechosos en horarios de clase forman parte de un factor importante para el desarrollo de esta propuesta, además de la optimización del ancho de banda proporcionado dentro de la institución mediante efectivos métodos de control de descargas promoviendo de esta manera la investigación y aprendizaje de los estudiantes.

En definitiva un sistema de autenticación optimizará los recursos de la institución mejorando y controlando adecuadamente los servicios de red proporcionados.

6.4 OBJETIVOS

6.4.1 OBJETIVO GENERAL

Implantar un Sistema de Autenticación Unificada que permita gestionar el acceso al internet y el aula virtual de la institución optimizando el flujo de información en la intranet del Centro Educativo “Sagrada Familia”

6.4.2 OBJETIVOS ESPECÍFICOS

- Analizar las características y estructura física actual de los recursos informáticos.
- Diseñar una estructura de red que permita a sus usuarios acceder servicios de intranet (Plataforma educativa, Controles de acceso)
- Diseñar un Sistema de Autenticación y Control de acceso al internet, como también a la plataforma educativa de la institución.
- Implementar un Sistema de Autenticación y control de acceso al internet y al aula virtual.
- Verificar mediante las pruebas necesarias el correcto funcionamiento del Sistema de Autenticación.

6.5 ANÁLISIS DE FACTIBILIDAD

6.5.1 FACTIBILIDAD OPERATIVA

En la escuela Sagrada Familia tanto docentes como personal administrativo muestran una amplia apertura a la innovación y utilización de nuevas tecnologías, esto se lo ha podido comprobar en el transcurso de elaboración del presente proyecto.

Sin embargo no se requiere una capacitación extensa, debido a que todo quedará centralizado en el servidor, siendo necesarias únicamente posibles actualizaciones técnicas de las que se encargará el Director de la institución.

6.5.2 FACTIBILIDAD ECONÓMICA

El presente proyecto es factible económicamente, ya que para la implementación del sistema, se utilizará herramientas de software libre, como el Sistema Operativo Linux “Centos”, que no tiene costo de soporte.

Además la institución cuenta con todos los dispositivos de comunicación necesarios para la implementación del presente trabajo.

6.5.3 FACTIBILIDAD TÉCNICA

SOFTWARE

Para la configuración del Servidor se utilizará el Sistema Operativo CentOS, una distribución de Linux basada en Red Hat GNU/Linux, que concentra sus objetivos en la restricción de uso, lanzamientos regulares y facilidad de instalación.

Para el diseño e implementación de la plataforma educativa se utilizará una herramienta denominada “Moodle”, la cual es un Sistema de Gestión de Cursos basados en internet, por ser una aplicación web gratuita utilizada en la creación de sitios de aprendizaje en línea.

Los equipos inalámbricos utilizarán el sistema predeterminado que viene instalado, tal es el caso de los routers inalámbricos que en su configuración necesitan su propio software.

HARDWARE

Se cuenta con equipos de las siguientes características para ser parte del presente proyecto

Servidor:

Procesador:	Intel® Core Duo
Ram	2GB
Bits	32
Disco Duro:	300Gb

TABLA 6.1 CARACTERÍSTICAS DE HARDWARE DEL SERVIDOR

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Equipos que se conectaran a la red inalámbrica y serán beneficiarios del sistema de autenticación:

PROCESADOR	CARACTERÍSTICAS	
Intel® Core™2 Duo	Ram	2GB
	Bits	32
	Disco Duro:	100GB
	Número de Equipos	11
Intel® Dual Core	Ram	2GB
	Bits	32
	Disco Duro:	100Gb
	Número de Equipos	15

TABLA 6.2 EQUIPOS CLIENTES DE LA RED INALÁMBRICA

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Dispositivos inalámbricos:

DISPOSITIVO	CARACTERÍSTICAS
<u>Wireless Router</u> <u>DIR-635</u>	Marca D-link Firmware Version 2.32ww Hardware version B3
<u>Wireless Router</u> <u>TEW-652BRP</u>	Marca Trendnet
<u>Modem ADSL</u> <u>THOMPSON ST546</u>	Nombre ST546 Version del Software 7.4.4.7

TABLA 6.3 CARACTERÍSTICAS DE LOS DISPOSITIVOS DE LA INSTITUCIÓN

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

6.6 FUNDAMENTACIÓN

La fundamentación teórica en la que se va a sustentar la propuesta se compondrá de un análisis que abarcará:

Distribuciones Linux que podrían ser utilizados en el servidor sus características y funcionalidades, además de la configuración de los servicios necesarios para el buen funcionamiento del mismo, como también los requisitos para una autenticación unificada, y finalmente la correcta implementación de un Sistema de Aprendizaje

6.6.1 DISTRIBUCIONES LINUX

6.6.1.1 FEDORA



“Es una distribución Linux para propósitos generales basada en RPM, que se caracteriza por ser un sistema estable, la cual es mantenida gracias a una comunidad internacional de ingenieros, diseñadores gráficos y usuarios que informan de fallos y prueban nuevas tecnologías.

Los desarrolladores de Fedora prefieren hacer cambios en las fuentes originales en lugar de aplicar los parches específicos en su distribución, de esta forma se asegura que las actualizaciones estén disponibles para todas las variantes de GNU/Linux.

Durante sus primeras 6 versiones se llamó Fedora Core, debido a que solo incluía los paquetes más importantes del sistema operativo. La última versión es Fedora 17, puesta a disposición del público el 29 de Mayo del 2012.”¹⁶

6.6.1.2 UBUNTU



“Ubuntu es un sistema operativo mantenido por Canonical y la comunidad de desarrolladores. Utiliza un núcleo Linux, y su origen está basado en Debian. Está compuesto de múltiple software normalmente distribuido bajo una licencia libre o de código abierto. Estadísticas web sugieren que el porcentaje de mercado de Ubuntu dentro de "distribuciones linux" es de aproximadamente 49%,y con una tendencia a subir como servidor web.

Ubuntu posee una gran gama de aplicaciones para llevar a cabo tareas cotidianas, entretenimiento, desarrollo y aplicaciones para la configuración de todo el sistema. La interfaz predeterminada de Ubuntu es Unity y utiliza en conjunto las aplicaciones de GNOME. Existen otras versiones extraoficiales mantenidas por la comunidad, con diferentes escritorios, y pueden ser instalados independientemente del instalado por defecto en Ubuntu.”¹⁷

6.6.1.3 CENTOS



CentOS (Community ENTerprise Operating System) es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente liberado por Red Hat.

¹⁶ [http://es.wikipedia.org/wiki/Fedora_\(distribuci%C3%B3n_Linux\)](http://es.wikipedia.org/wiki/Fedora_(distribuci%C3%B3n_Linux)) Se refiere a la distribución Linux fedora

¹⁷ <http://es.wikipedia.org/wiki/Ubuntu> Se refiere a la distribución Linux Ubuntu

Red Hat Enterprise Linux se compone de software libre y código abierto, pero se publica en formato binario usable (CD-ROM o DVD-ROM) solamente a suscriptores pagados. Como es requerido, Red Hat libera todo el código fuente del producto de forma pública bajo los términos de la Licencia pública general de GNU y otras licencias. Existen otras distribuciones también derivadas de los fuentes de Red Hat, usa yum para bajar e instalar las actualizaciones.

CentOS en su mayoría orientado a servidores, ofrece todos los servicios necesarios por los ISPs y hosts web como: servidor web Apache (SSL-capaz), servidor de correo (Postfix con SMTP-AUTH y TLS), Servidor DNS (BIND), servidor FTP, servidor MySQL, Dovecot POP3/IMAP, Quota, Firewall, etc.

Diseñado para personas que necesitan un sistema operativo de clase empresarial sin el coste o el apoyo del destacado proveedor.¹⁸

6.6.2 SERVICIOS DE INTRANET

6.6.2.1 SERVICIO DE NOMBRES DE DOMINIO (DNS)

DNS es un sistema para asignar nombres a equipos y servicios de red que se organiza en una jerarquía de dominios. La asignación de nombres DNS se utiliza en las redes TCP/IP, como Internet, para localizar equipos y servicios con nombres descriptivos. Cuando un usuario escribe un nombre DNS en una aplicación, los servicios DNS podrán traducir el nombre a otra información asociada con el mismo, como una dirección IP, los sistemas de nombres como DNS proporcionan una forma de asignar nombres descriptivos de los equipos o servicios a sus direcciones numéricas.

La siguiente ilustración muestra un uso básico de DNS, consistente en la búsqueda de la dirección IP de un equipo basada en su nombre.

¹⁸ <http://www.centos.org/> Se refiere a la distribución Linux Centos

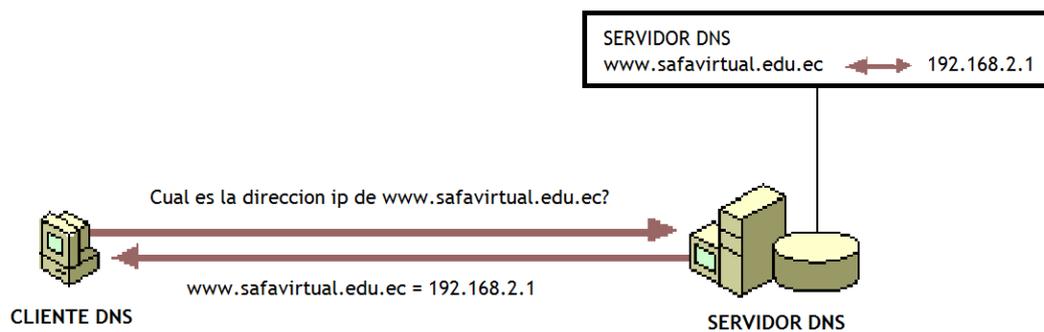


FIGURA 6.1 FUNCIONAMIENTO DNS
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

6.6.2.1.1 DNSMASQ

Dnsmasq es un servidor (DNS, DHCP) muy ligero que tiene un efecto colateral; además de funcionar como servidor DNS para la red local (gracias a que lee el archivo `/etc/hosts`) y resolver los nombres asignados a los equipos, también hace de servidor DNS caché, es decir almacena las IPs consultadas para no tener que repetir la consulta cuando vuelven a pedirse.

El resultado es que el acceso a las páginas de Internet es más rápido, antes de visualizar su contenido, debe resolverse el nombre del equipo al que se envía la petición a través de una compleja red de servidores, que se inicia en el (o los) que se han definido en `/etc/resolv.conf`

6.6.2.1.2 BIND

BIND (Berkeley Internet Name Domain) es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, entrega dos tipos de servicios DNS

caching only nameserver, que se limita a guardar en una caché las IPs de los nombres de máquina más solicitados, obteniéndolas de servidores externos, es lo básico si se requiere navegar por INTERNET con un servidor DNS propio, el archivo de configuración para este servicio es `/var/named/named.cache` y por lo general sólo se debe actualizar por lo menos una vez al mes.

El otro servicio es el de entregar la configuración de un determinado dominio, necesario para nuestra red como puede ser nuestra propia página web o en este caso aula virtual

6.6.2.2 PROXY - SQUID

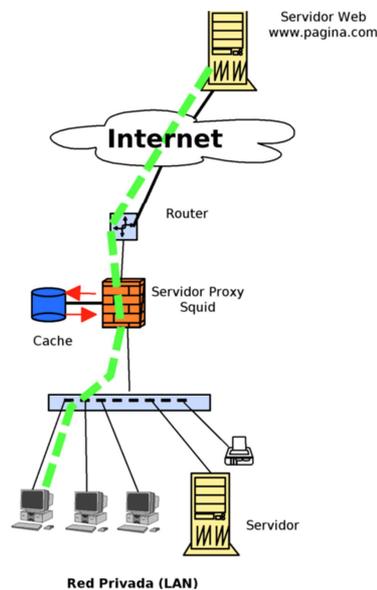


FIGURA 6.2 FUNCIONAMIENTO PROXY

Fuente:http://tuxjm.net/docs/Manual_de_Instalacion_de_Servidor_Proxy_Web_con_Ubuntu_Server_y_Squid/html-onechunk

Sistema informático cuya misión es hacer de intermediario entre un sistema y otro a través de Internet. Entre las misiones de un proxy están acelerar el acceso a Internet, filtrar los contenidos a los que se ha accedido y proteger los sistemas evitando su comunicación directa.

Su finalidad más habitual consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.

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

Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto.

- ▶ Proporciona un servicio de Proxy que soporta peticiones HTTP, HTTPS y FTP a equipos que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentra fuera de la red interna.
- ▶ Ofrece la posibilidad de establecer reglas de control de acceso. Esto permite establecer políticas de acceso en forma centralizada, simplificando la administración de una red.

Squid incorpora un sistema de control de acceso bastante flexible y potente basado en Listas de Control de Acceso o ACLs. Los controles de acceso en Squid están formados por dos componentes principales: los elementos de ACL y las listas de acceso.

Los elementos de una ACL definen el origen o destino de la petición realizada por el cliente, hay diferentes tipos de elementos de ACL,

Los tipos de elementos de ACL de tipo origen pueden ser:

- Dirección IP del cliente
- Nombre del usuario
- Grupo de usuarios
- Navegador

Los tipos de elementos de ACL de tipo destino pueden ser:

- Puerto
- Dominio DNS
- URL
- Tipo MIME

Además hay otros tipos de elementos de ACL como:

- Protocolo
- Método usado en la petición, GET, POST, CONNECT

6.6.2.2.1 LISTAS DE CONTROL DE ACCESO (ACLs)

Un ACL es una definición de control de acceso, que permite denegar el paso a ciertos tipos de extensiones de archivo, permite hacer un uso más racional del ancho de banda con el que se dispone, además permite designar qué máquinas o redes tienen permitido, o no, acceder al servidor.

El funcionamiento es verdaderamente simple, y consiste en denegar el acceso a ciertos tipos de extensiones que coincidan con lo establecido en una *Lista de Control de Acceso* que en Squid se especifica mediante el parámetro `acl` según la siguiente sintaxis:

```
acl nombre_acl tipo_acl descripción
```

```
acl nombre_acl tipo_acl "fichero_de_descripciones"
```

TIPOS DE ELEMENTOS DE ACL

Para crear controles de acceso basados en el origen de la petición del cliente se puede usar los siguientes tipos de elementos de ACL:

- ▶ **Src** Dirección IP del cliente, puede ser una sola dirección lista o rango de direcciones IP, soporta el uso de máscaras de subred en formato CIDR
- ▶ **proxy_auth** Autenticación de usuarios vía procesos externos
- ▶ **browser** User-agent del navegador web que realiza la petición

Para crear controles de acceso basados en el destino de la petición se encuentran los siguientes tipos de elementos de ACL:

- ▶ **Dstdomain** Este tipo define uno o más dominios destino solicitados por el cliente
- ▶ **url_regex** Tipo con soporte de expresiones regulares para el URL solicitado por el cliente
- ▶ **urlpath_regex** URL-path regular expression pattern matching, leaves out the protocol and hostname

- ▶ **port** Este tipo define uno o más números de puerto destino solicitados por el cliente
- ▶ **method** Este tipo define el método usado por el cliente para la petición HTTP (get, post, etc)

Para crear controles de acceso basados en el tipo MIME de la solicitud o respuesta de la petición se puede usar los siguientes tipos de elementos de ACL:

- ▶ **req_mime_type** regular expression pattern matching on the request content-type header
- ▶ **rep_mime_type** regular expression pattern matching on the reply (downloaded content) content-type header.

Además es posible crear controles de acceso basados en el tiempo en el que se realiza la petición, y usando procesos externos, por ejemplo para realizar autenticación basada en grupos, las ACLs que se puede utilizar son:

- ▶ **Time** hora del día, y día de la semana
- ▶ **External** lookup via external acl helper defined by `external_acl_type`¹⁹

6.6.2.2 AUTENTICACIÓN SQUID

SQUID permite realizar autenticación mediante diferentes métodos como: Basic, Digest y NTLM, provee varios módulos de autenticación (helpers) que serán los encargados de realizar la validación (NCSA, PAM, SASL, YP y SMB).

Es muy útil el poder establecer un sistema de autenticación para poder acceder hacia Internet, pues esto permite controlar quienes sí y quienes no accederán a Internet sin importar desde que máquina de la red local lo hagan. De modo que se tiene un doble control, primero por dirección IP y segundo por nombre de usuario y contraseña.

¹⁹

http://tuxjm.net/docs/Manual_de_Instalacion_de_Servidor_Proxy_Web_con_Ubuntu_Server_y_Squid/html-multiples/configuracion-de-los-esquemas-de-control-de-acceso-en-squid.html#id554188 Se refiere a las listas de contro de Acceso

AUTENTICACIÓN DE USUARIOS EN SQUID

Cuando se configura un servidor Proxy con soporte de autenticación los navegadores web envían las credenciales codificadas del usuario en la petición usando la cabecera *Authorization*, si el proxy recibe una petición con la cabecera *Authorization* el proxy descodifica el nombre de usuario y la contraseña para validar el usuario.

La negociación de la autenticación la realiza el programa auxiliar de acuerdo al protocolo soportado, en su mayoría la autenticación es de tipo básico como NCSA, LDAP y otros basados en negociación como NTLM o Kerberos.

Algunos esquemas requieren de la previa configuración de un sistema como PAM, LDAP, Samba, Kerberos y otros, sin embargo, Squid soporta el esquema de autenticación básica basada en NCSA el cual usa un archivo en el cual mantiene una lista de usuarios y contraseñas codificadas, este es el método más simple de usar, aunque no el más flexible y seguro.²⁰

ESQUEMAS DE AUTENTICACIÓN DE USUARIOS EN SQUID

Cuando se trabaja con Proxy resulta muy útil el poder establecer un sistema de autenticación para poder acceder hacia Internet, pues esto permite controlar quienes sí y quienes no accederán a Internet sin importar desde que máquina de la red local lo hagan.

Squid permite usar diferentes protocolos de autenticación o esquemas de autenticación desde los más simples hasta los más seguros, a continuación se listan los esquemas de autenticación más usuales:

²⁰ <http://es.scribd.com/doc/94412942/Resumen-Squid>

Se refiere a Autenticación Squid

MODULO	DESCRIPCIÓN
NCSA	USA UN ARCHIVO DE USUARIOS Y CONTRASEÑAS AL ESTILO NCSA
LDAP	USA EL PROTOCOLO LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
MSNT	USA UN DOMINIO DE AUTENTICACIÓN WINDOWS NT
PAM	USA LOS MÓDULOS DE AUTENTICACIÓN PAM
SMB	USA UN SERVIDOR SMB COMO WINDOWS NT O SAMBA
GETPWAM	USA EL VIEJO ARCHIVO DE CONTRASEÑAS UNIX
SASL	USA LAS BIBLIOTECAS DE AUTENTICACIÓN SASL
NTLM	USA LA AUTENTICACIÓN Y NEGOCIACIÓN DE AUTENTICACIÓN

TABLA 6.4 MODULO DE AUTENTICACIÓN DE USUARIOS SQUID

6.6.3 PLATAFORMAS EDUCATIVAS LIBRES

“Surgidas como una alternativa para economizar un proyecto de formación en línea, las herramientas también llamadas “Open Source”, son generalmente desarrolladas por instituciones educativas o por personas que están vinculadas al sector educativo.

Es amplia la gama de funcionalidades que traen cada una de ellas, hay algunas que pueden equipararse a las comerciales mientras que otras solo cuentan con funcionalidades básicas. Entre las más usadas están: Atutor, Dokeos, Claroline, dotLRN, Moodle etc.

6.6.3.1 CLAROLINE



Claroline es una plataforma de aprendizaje que permite a los formadores construir cursos online y gestionar las actividades de aprendizaje y colaboración en la Web. Está traducido a 35 idiomas y tiene una gran comunidad de desarrolladores y usuarios en todo el mundo.

Se basa en un modelo educativo flexible, donde la información se convierte en conocimiento a través de las actividades y producciones de los alumnos en un sistema impulsado por la motivación y la interacción. La amplia gama de herramientas a disposición de los usuarios permite a cualquier profesor o estudiante para establecer u operar un dispositivo educativo para el aprendizaje. Los instrumentos genéricos (calendario, documentos, foros) pueden utilizar la plataforma en diferentes contextos, es una plataforma estable, abierta a todos, lo que permite un fácil uso del espacio para la formación y la colaboración. Su funcionamiento no requiere conocimientos técnicos especiales.²¹

6.6.3.2 MOODLE



Moodle es un Ambiente Educativo Virtual, sistema de gestión de cursos, de distribución libre, que ayuda a los educadores a crear comunidades de aprendizaje en línea. Este tipo de plataformas tecnológicas también se conoce como LMS (Learning Management System).

Moodle fue creado por Martin Dougiamas, quien fue administrador de WebCT en la Universidad Tecnológica de Curtin. Basó su diseño en las ideas del constructivismo en pedagogía que afirman que el conocimiento se construye en la mente del estudiante en lugar de ser transmitido sin cambios a partir de libros o enseñanzas y en el aprendizaje colaborativo.

Un profesor que opera desde este punto de vista crea un ambiente centrado en el estudiante que le ayuda a construir ese conocimiento con base en sus habilidades y conocimientos propios en lugar de simplemente publicar y transmitir la información que se considera que los estudiantes deben conocer.²²

²¹ <http://jornadaie.unvm.edu.ar/ponencia12.pdf> Se refiere a la plataforma educativa Claroline

²² <http://es.wikipedia.org/wiki/Moodle> Se refiere a Moodle

6.6.3.2.1 ESPECIFICACIONES TÉCNICAS

SERVIDOR

En términos de arquitectura, Moodle es una aplicación web que se ejecuta sin modificaciones en GNU/Linux, y sistemas que soportan PHP, incluyendo la mayoría de proveedores de alojamiento web.

Los datos se almacenan en una base de datos SQL. Los sistemas de gestión de bases de datos soportados son: MySQL, PostgreSQL, MSSQL, Oracle, SQLite. 2

CLIENTE

Al ser una aplicación web el cliente puede ser casi cualquier navegador web moderno. Se debe contar con las extensiones necesarias para visualizar los vídeos, audio y demás material multimedia que un curso pueda contener.

6.6.3.2.2 ADMINISTRACIÓN DE LOS USUARIOS - AUTENTICACIÓN

Moodle soporta un rango de mecanismos de autenticación a través de módulos, que permiten una integración sencilla con los sistemas existentes.

Las características principales incluyen:

- Método estándar de alta por correo electrónico: los estudiantes pueden crear sus propias cuentas de acceso. La dirección de correo electrónico se verifica mediante confirmación.
- Método LDAP: las cuentas de acceso pueden verificarse en un servidor LDAP. El administrador puede especificar qué campos usar.
- IMAP, POP3, NNTP: las cuentas de acceso se verifican contra un servidor de correo o de noticias (news). Soporta los certificados SSL y TLS.
- Base de datos externa: Cualquier base de datos que contenga al menos dos campos puede usarse como fuente externa de autenticación.

Cada persona necesita sólo una cuenta para todo el servidor. Por otra parte, cada cuenta puede tener diferentes tipos de acceso. Con una cuenta de administrador que controla la creación de cursos y determina los profesores, asignando usuarios a los cursos.

- Seguridad: los profesores pueden añadir una "clave de acceso" para sus cursos, con el fin de impedir el acceso de quienes no sean sus estudiantes. Pueden transmitir esta clave personalmente o a través del correo electrónico personal, etc. Los profesores pueden dar de baja a los estudiantes manualmente si lo desean, aunque también existe una forma automática de dar de baja a los estudiantes que permanezcan inactivos durante un determinado período de tiempo (establecido por el administrador).

6.6.3.2.3 ADMINISTRACIÓN DE CURSOS

El profesor tiene control total sobre todas las opciones de un curso. Se puede elegir entre varios formatos de curso tales como semanal, por temas o el formato social, basado en debates.

En general Moodle ofrece una serie flexible de actividades para los cursos: foros, diarios, cuestionarios, materiales, consultas, encuestas y tareas. En la página principal del curso se pueden presentar los cambios ocurridos desde la última vez que el usuario entró en el curso, lo que ayuda a crear una sensación de comunidad.

La mayoría de las áreas para introducir texto (materiales, envío de mensajes a un foro, entradas en el diario, etc.) pueden editarse usando un editor HTML WYSIWYG integrado.

Todas las calificaciones para los foros, diarios, cuestionarios y tareas pueden verse en una única página (y descargarse como un archivo con formato de hoja de cálculo). Además, se dispone de informes de actividad de cada estudiante, con gráficos y detalles sobre su paso por cada módulo (último acceso, número de veces que lo ha leído), así como también de una detallada "historia" de la participación de cada estudiante, incluyendo mensajes enviados, entradas en el diario, etc. en una sola página.

Pueden enviarse por correo electrónico copias de los mensajes enviados a un foro, los comentarios de los profesores, etc. en formato HTML o de texto.

6.6.3.2.4 MÓDULOS PRINCIPALES

MÓDULO DE TAREAS

- Puede especificarse la fecha final de entrega de una tarea y la calificación máxima que se le podrá asignar.
- Los estudiantes pueden subir sus tareas (en cualquier formato de archivo) al servidor. Se registra la fecha en que se han subido.
- Se permite enviar tareas fuera de tiempo, pero el profesor puede ver claramente el tiempo de retraso.
- Para cada tarea en particular, puede evaluarse a la clase entera (calificaciones y comentarios) en una única página con un único formulario.
- Las observaciones del profesor se adjuntan a la página de la tarea de cada estudiante y se le envía un mensaje de notificación.
- El profesor tiene la posibilidad de permitir el reenvío de una tarea tras su calificación.

MÓDULO DE CONSULTA

Es como una votación. Puede usarse para votar sobre algo o para recibir una respuesta de cada estudiante (por ejemplo, para pedir su consentimiento para algo).

- El profesor puede ver una tabla que presenta de forma intuitiva la información sobre quién ha elegido qué.
- Se puede permitir que los estudiantes vean un gráfico actualizado de los resultados.

MÓDULO FORO

Hay diferentes tipos de foros disponibles: exclusivos para los profesores, de noticias del curso y abiertos a todos.

- Todos los mensajes llevan adjunta la foto del autor.
- Las discusiones pueden verse anidadas por rama, o presentar los mensajes más antiguos o los más nuevos primero.

- El profesor puede obligar la suscripción de todos a un foro o permitir que cada persona elija a qué foros suscribirse de manera que se le envíe una copia de los mensajes por correo electrónico.
- El profesor puede elegir que no se permitan respuestas en un foro (por ejemplo, para crear un foro dedicado a anuncios).
- El profesor puede mover fácilmente los temas de discusión entre distintos foros.

MÓDULO DIARIO

Los diarios constituyen información privada entre el estudiante y el profesor.

- Cada entrada en el diario puede estar motivada por una pregunta abierta.
- La clase entera puede ser evaluada en una página con un único formulario, por cada entrada particular de diario.
- Los comentarios del profesor se adjuntan a la página de entrada del diario y se envía por correo la notificación.

MÓDULO CUESTIONARIO

- Los profesores pueden definir una base de datos de preguntas que podrán ser reutilizadas en diferentes cuestionarios.
- Las preguntas pueden ser almacenadas en categorías de fácil acceso, y estas categorías pueden ser "publicadas" para hacerlas accesibles desde cualquier curso del sitio.
- Los cuestionarios se califican automáticamente, y pueden ser recalificados si se modifican las preguntas.
- Los cuestionarios pueden tener un límite de tiempo a partir del cual no estarán disponibles.
- El profesor puede determinar si los cuestionarios pueden ser resueltos varias veces y si se mostrarán o no las respuestas correctas y los comentarios
- Las preguntas y las respuestas de los cuestionarios pueden ser mezcladas (aleatoriamente) para disminuir las copias entre los alumnos.
- Las preguntas pueden crearse en HTML y con imágenes.

- Las preguntas pueden importarse desde archivos de texto externos.
- Las preguntas pueden tener diferentes métricas y tipos de captura.

MÓDULO RECURSO

- Admite la presentación de un importante número de contenido digital, Word, Powerpoint, Excel, Flash, vídeo, sonidos, etc.
- Los archivos pueden subirse y manejarse en el servidor, o pueden ser creados sobre la marcha usando formularios web (de texto o HTML).
- Pueden enlazarse aplicaciones web para transferir datos.

MÓDULO ENCUESTA

- Se proporcionan encuestas ya preparadas (COLLES, ATTLS) y contrastadas como instrumentos para el análisis de las clases en línea.
- Se pueden generar informes de las encuestas los cuales incluyen gráficos. Los datos pueden descargarse con formato de hoja de cálculo Excel o como archivo de texto CSV.
- La interfaz de las encuestas impide la posibilidad de que sean respondidas sólo parcialmente.
- A cada estudiante se le informa sobre sus resultados comparados con la media de la clase.

MÓDULO WIKI

- El profesor puede crear este módulo para que los alumnos trabajen en grupo en un mismo documento.
- Todos los alumnos podrán modificar el contenido incluido por el resto de compañeros.
- De este modo cada alumno puede modificar el wiki del grupo al que pertenece, pero podrá consultar todos los wikis.

6.6.4 SERVICIOS DE DIRECTORIO

Un servicio de directorio (SD) es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores, sobre recursos de red, y permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. Además, los servicios de directorio actúan como una capa de abstracción entre los usuarios y los recursos compartidos.

Permite a los usuarios trabajar desde cualquier puesto, accediendo con la misma contraseña y viendo el mismo entorno de trabajo en todos ellos con las consiguientes ventajas:

- Aumento de la productividad y posibilidad de trabajo en grupo
- Interfaz y paradigma conocidos (carpetas+ficheros)
- No dependencia de un puesto de hardware

La interfaz del servicio de directorio es la encargada de gestionar la autenticación de los accesos al servicio de forma segura, actuando como autoridad central para el acceso a los recursos de sistema que manejan los datos del directorio.

Existen numerosas formas de implementación de servicios de directorio de diferentes compañías. Algunos de estos ejemplos son: eDirectory, CentOS Directory Server, Active Directory, OpenLdap, Servidor de directorio de Red Hat entre otros.²³

6.6.4.1 CENTOS DIRECTORY SERVER



Centos Directory Server permite a los administradores crear un registro basado en la red que las aplicaciones pueden utilizar para almacenar información compartida, tal como la información de usuarios, grupos y preferencias.

²³ http://es.wikipedia.org/wiki/Servicio_de_directorio Se refiere a los Servicios de Directorio

Mediante el Servidor de Directorio, las aplicaciones pueden lograr independencia del lugar al almacenar y recuperar preferencias en el directorio en lugar de leer distintos archivos en las computadoras de escritorio de los usuarios, esto permite a los usuarios trabajar prácticamente en cualquier computadora como si lo hicieran en la propia.²⁴

6.6.4.2 OPENLDAP



OpenLDAP es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP. Está liberada bajo su propia licencia OpenLDAP Public License. LDAP es un protocolo de comunicación independiente de la plataforma. Muchas distribuciones GNU/Linux incluyen el software OpenLDAP para el soporte LDAP. Este software también corre en plataformas BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows (NT y derivados, incluyendo 2000, XP, Vista), y z/OS.

Básicamente, OpenLDAP posee tres componentes principales:

- slapd - Dominio de servidor y herramientas.
- Bibliotecas que implementan el protocolo LDAP.
- Programas cliente: Idapsearch, Idapadd, Idapdelete.

Adicionalmente, el proyecto OpenLDAP es anfitrión de los subproyectos:

- JLDAP - biblioteca de clases LDAP para Java.
- JDBC-LDAP - controlador Java JDBC - LDAP.
- Idapc++ - biblioteca de clases LDAP para C++.

Históricamente la arquitectura del servidor OpenLDAP (slapd, Standalone LDAP Daemon) fue dividida entre una sección frontal que maneja las conexiones de redes y el procesamiento del protocolo, y una base de datos dorsal o de segundo plano (backend) que trata únicamente con el almacenamiento de datos. La arquitectura es modular y una variedad de backends está disponible para interactuar con otras tecnologías, no sólo bases de datos tradicionales.²⁵

²⁴ http://www.latam.redhat.com/pdf/Red_Hat_Directory_Server.pdf Se refiere a Red Hat Directory Server

²⁵ <http://es.wikipedia.org/wiki/OpenLDAP> Se refiere a Openldap

La información que se suele guardar en un directorio está formada por entradas. Cada entrada es un conjunto de atributos (información) que se identifica a través de un nombre distinguido, DN, Distished name en inglés. Cada uno de estos atributos es de un tipo concreto y puede tener uno o varios valores. Estos atributos suelen ser nemónicos como por ejemplo cn (common name) o mail que indicaría el nombre o email de una entrada en el directorio.

La información se almacena en el directorio en forma de árbol jerarquico.

LDAP posee un atributo, objectClass, que permite definir que datos van a ser obligatorios y cuales opcionales a través de los esquemas (schemas). O sea, los esquemas van a ser como definiciones de los datos que va a contener el directorio. OpenLDAP incluye varios esquemas, pero se puede añadir o modificar los ya existentes.

El acceso a la información del directorio, se hace a través de los nombres distinguidos, DN, y de los RND, nombres distinguidos relativos. Estos se construyen a partir de una entrada, concatenandole el DN de todos sus padres.

OpenLDAP permite, además, definir ACL (access control lists) para el acceso a los datos, aparte de que permite transmitir los datos sobre una capa segura como OpenSSL. Así mismo, OpenLDAP permite la replicación de los datos entre varios servidores OpenLDAP para descongestionar los servidores.

Hay una serie de ventajas respecto a otros sistemas de directorio que hacen que OpenLDAP sea el sistema más flexible y escalable como por ejemplo está optimizado en lectura de registros, la posibilidad de múltiples directorios independientes, la mayoría de aplicaciones y sistemas operativos disponen de soporte para LDAP, realizar criterios de búsqueda complejos, permitir la réplica de la base de datos a otro servidor.

6.6.5 SOFTWARE PARA RESPALDO LINUX

Existe variedad de Software de Backup de manera Comercial y OpenSource para realizar respaldos de servidores. Un ejemplo es CloneZilla el cual permite a los usuarios clonar una máquina individual, partición o disco para ser reproducido en otro medio. La clonación puede ser guardada como un archivo de imagen o como una copia exacta de datos. Los

datos pueden ser guardados localmente, en un servidor SSH, servidor Samba o un recurso compartido de archivos NFS y luego restaurarlos en una fecha posterior. El software se puede ejecutar ya sea desde un arranque de unidad flash USB o cd/dvd.

6.7 METODOLOGÍA

Para la elaboración del presente proyecto se utilizará como base el modelo en cascada el mismo que indica el ciclo de vida del software siendo las etapas base para su desarrollo las siguientes:

ANÁLISIS

En este ciclo se analizarán todos los requerimientos y necesidades de la institución para determinar los límites del trabajo. En esta fase se debe consensuar todo lo que requiere el sistema y será aquello lo que seguirá en las siguientes etapas, no pudiéndose requerir nuevos resultados a la mitad del proceso de elaboración del proyecto.

DISEÑO

Tras establecer los requerimientos de la institución se procederá a estructurar adecuadamente la red mediante un diagrama de la arquitectura necesaria, además de determinar las herramientas que se utilizarán para el desarrollo de la propuesta.

DESARROLLO E IMPLEMENTACIÓN

Una vez estipuladas las herramientas a utilizarse y preparados todos los dispositivos necesarios para el desarrollo del proyecto se procederá a realizar la implantación, en donde se instalará y configurará adecuadamente el servidor, permitiendo la autenticación de sus usuarios al internet, y se creará el aula virtual con gestión de autenticación.

PRUEBAS

En la etapa de pruebas se verificará la funcionalidad y eficacia del sistema, desde cada máquina usuaria dentro del establecimiento.

6.8 MODELO OPERATIVO

6.8.1 ANÁLISIS DEL SISTEMA

6.8.1.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

Actualmente en el Centro Educativo Sagrada Familia, la red manejada no es controlada ni administrada mediante adecuadas medidas de control, el siguiente diagrama muestra la conexión de red utilizada actualmente dentro de la institución.

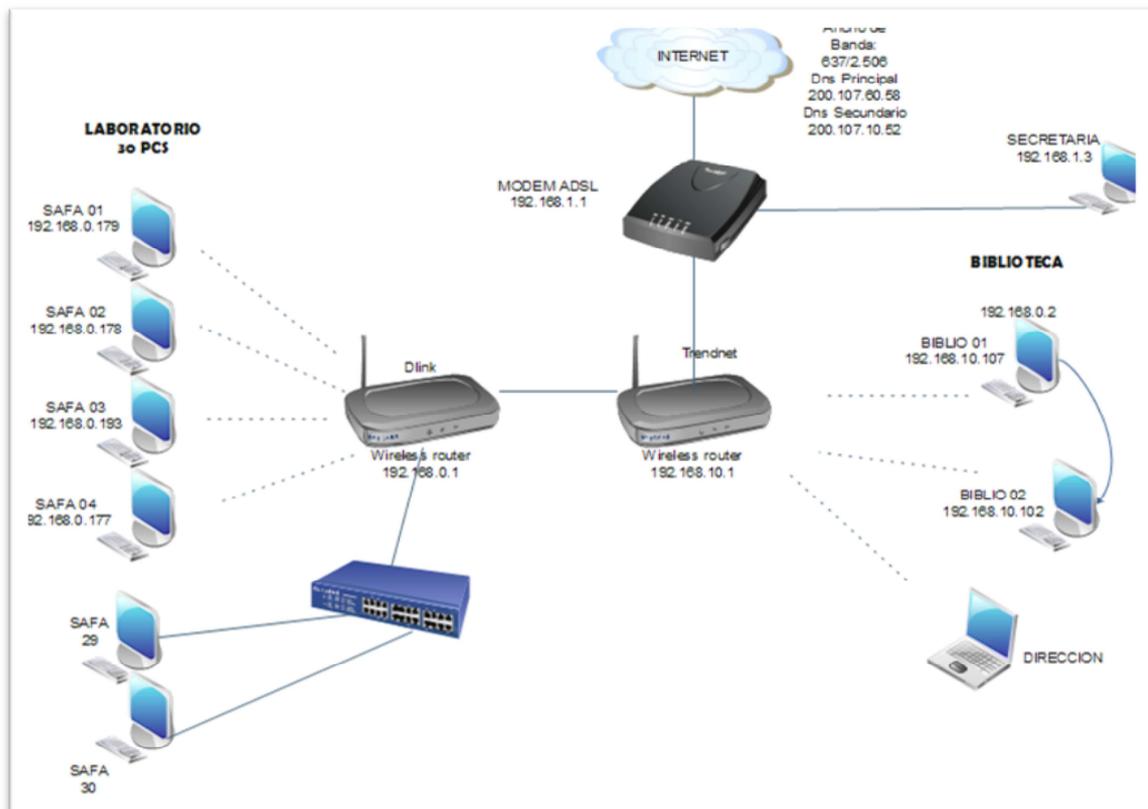


FIGURA 6.3 ESTRUCTURA FÍSICA ACTUAL

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Como se observa en la ilustración, la institución dispone de un laboratorio de computación que contiene 30 computadores, de los cuales 28 se conectan inalámbricamente a un Access point cuyo SSID es Dlink, 2 computadores se interconectan mediante cable a un switch mismo que a su vez se interconecta nuevamente al router con SSID Dlink.

El router inalámbrico denominado Dlink se interconecta mediante cable a otro router inalámbrico cuyo SSID es Trendnet, el cual se comunica directamente con el modem Adsl que proporciona el internet a la institución

Los computadores de la biblioteca y de la dirección del plantel se comunican inalámbricamente hacia el router cuyo SSID es Trendnet.

6.8.1.2 ANÁLISIS DE REQUERIMIENTOS

Luego de haber analizado el estado actual de la institución y contemplado las solicitudes por parte de la misma, se ha obtenido los siguientes requerimientos:

- ▶ Estructuración adecuada de la interconexión física de los dispositivos informáticos.
- ▶ Implantación de un servidor que proporcione servicios básicos de internet.
- ▶ Control del Internet con el fin de permitir el acceso únicamente a personas autorizadas.
- ▶ Restricción de determinados sitios web.
- ▶ Control de la información externa que ingresa al centro educativo evitando ataques maliciosos.
- ▶ Implementación de una plataforma educativa con funcionalidades de :
 - Autenticación de Acceso
 - Descarga de archivos
 - Foros
 - Comunicación en tiempo real
 - Publicación de Cuestionarios
 - Disponibilidad de Información sobre el curso dictado

6.8.2 DISEÑO DEL SISTEMA

6.8.2.1 ESTRUCTURA FÍSICA PROPUESTA

Para el desarrollo del Sistema de Autenticación se ha propuesto un modelo de conexión basado en la arquitectura cliente-servidor en donde el servidor dispondrá de dos tarjetas de red, la una para interconectarse hacia la red LAN de la escuela, y la otra para servir de puente con el modem ADSL, el cual provee de internet a la institución.

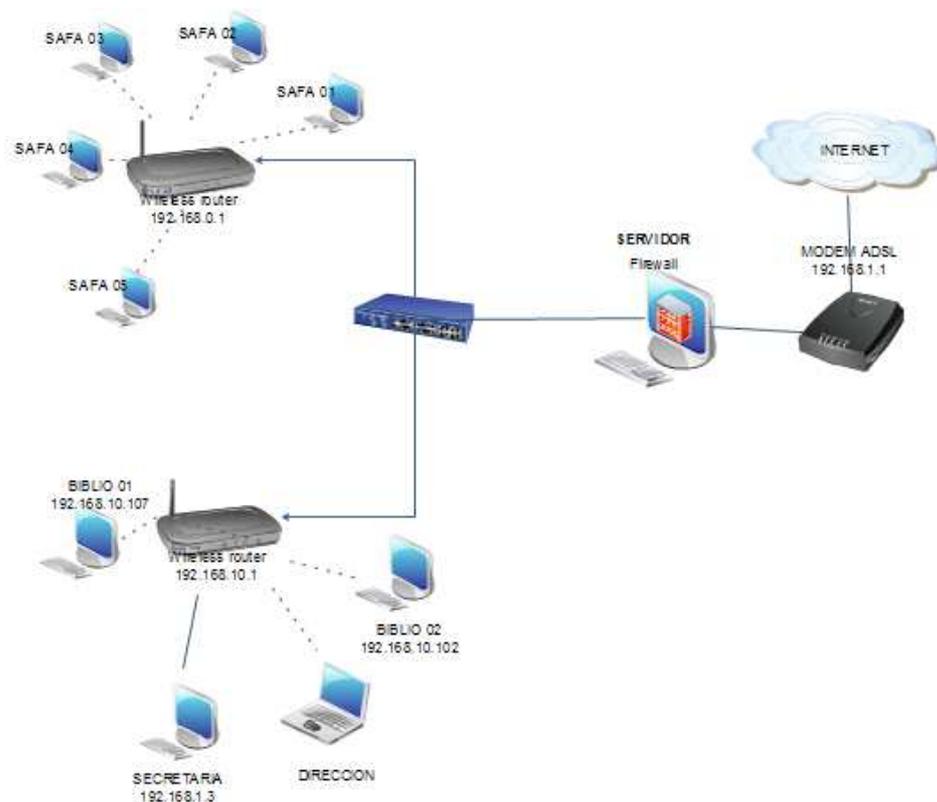


FIGURA 6.4 ESTRUCTURA FÍSICA PROPUESTA

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

La figura 6.4 ilustra la Estructura Propuesta, con la existencia de dos subredes conectadas mediante un switch, el cual a su vez se conecta con el servidor, la una subred estará conformada por los equipos del laboratorio de computación, haciendo uso del ruteador dlink con SSID Dlink y la otra por los computadores de la biblioteca mediante el ruteador con SSID Trendnet.

Mediante ésta arquitectura se logrará integrar la información relevante a nivel global, y distribuir los procesos en forma más eficiente, con el objetivo de reducir notablemente el tráfico de red y agilizar el tiempo empleado en realizar tareas.

Éste diseño de red ofrece amplias mejoras en relación a la estructura utilizada actualmente, entre ellas la centralización de contenidos, debido a que el servidor será el centro de la red administrando los recursos comunes a todos los usuarios, lo cual permitirá la implantación de nuevas tecnologías educativas entre ellas las plataformas virtuales, notándose que con la estructura de red actual no se podrían realizar estas implantaciones.

La seguridad se verá agudizada, puesto que toda la información proveniente desde el exterior de la institución, necesariamente pasará por el servidor antes de llegar a la red local, logrando así un mayor control de la información y cerrando vías de ataque externo.

6.8.2.2 SISTEMA OPERATIVO

Para la selección del Sistema Operativo a utilizar en el servidor, se consideraron como posibles opciones: Fedora, Ubuntu y CentOS, se optó por utilizar “CentOS” debido a que tiene claras ventajas frente a las otras distribuciones Linux analizadas.

Se escogió CentOS ya que es un Sistema Operativo orientado a servidores, el mismo que se encuentra en constante actualización con nuevos parches de seguridad, notándose que el tiempo necesario para parchar este Sistema Operativo es menor al tiempo requerido para los parches de cualquier otro S.O, adicionalmente posee una activa y creciente comunidad de usuarios de soporte y rápidas actualizaciones de seguridad.

6.8.2.3 AUTENTICACIÓN

La Autenticación en la institución se la realizará mediante servicios de directorio, que permiten gestionar de una manera concreta a usuarios de una intranet, tras haber analizado OpenLdap y Centos Directory Server como opciones de servicios de directorio, se eligió OpenLdap, para ser implementado dentro de la institución, debido a que es libre no tiene costo alguno y además proporciona un alto rendimiento, al ser el encargado de

gestionar la autenticación de acceso a los servicios de internet de forma segura, actuando como autoridad central para el acceso a los recursos.

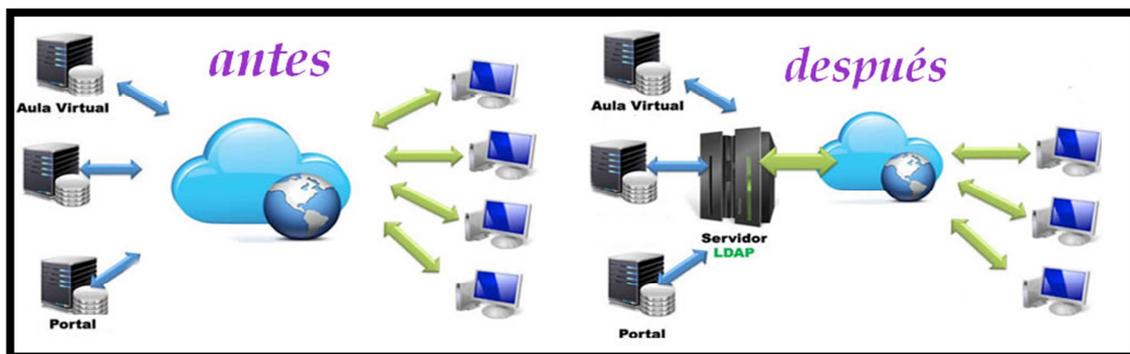


FIGURA 6.5 AUTENTICACIÓN OPENLDAP

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

6.8.2.4 PROXY

El servidor proxy a emplearse para el desarrollo de la presente propuesta es Squid por ser muy completo y robusto, además de facilitar la implementación de reglas de control para restringir o permitir el acceso a páginas web dentro de la institución en base a las políticas de uso del internet.

Las políticas de uso del internet dentro de la institución se llevarán a cabo mediante el servidor proxy y se detallan a continuación:

- ▶ Está restringido el acceso a páginas de pornografía, sexo, necrofilia
- ▶ Todos los usuarios de la institución tienen acceso a internet, tanto estudiantes como docentes.
- ▶ No está permitido ingresar a sitios web de farándula, entretenimiento, redes sociales en horario de clases.
- ▶ Los equipos utilizados para la conexión de la intranet, contarán con una clave de acceso debiendo autenticarse para su ingreso.
- ▶ A partir de las 2 de la tarde el acceso a internet se ofrece sin restricciones

6.8.2.5 Dns

Luego haber realizado un análisis entre dnsmasq y bind. El servicio de dominio seleccionado para la resolución de nombres fue “Bind”, puesto que ofrece un servicio de cacheo el cual permitirá hacer más rápido el acceso al internet, además de permitir la resolución de dominios propios, con lo cual se puede otorgar un dominio interno a la institución, facilitando el acceso a la plataforma virtual que va a ser implementada.

El dominio escogido para ser accesible dentro de escuela fue www.safavirtual.edu.ec estando compuesto por la unión de las palabras “safa” y “virtual”, Safa en representación de Sagrada Familia y Virtual que indica el proporcionar un medio virtual a la institución.

6.8.2.6 AMBIENTE EDUCATIVO VIRTUAL

Existen alternativas gratuitas (opensource), disponibles para crear variados entornos virtuales como son: ATutor, Chamilo, Claroline, Dokeos entre otros, para el desarrollo de este proyecto se ha escogido la Plataforma Moodle puesto que es una plataforma completa, tiene las herramientas adecuadas para planificar, organizar y desarrollar cursos. Es también la plataforma más utilizada en centros educativos lo que trae como beneficio la facilidad de intercambio de cursos.

Adicionalmente por proveer continuamente actualizaciones de este entorno educativo como también el soporte que provee a sus usuarios por parte de los desarrolladores de esta herramienta.

6.8.3 DESARROLLO E IMPLANTACIÓN

6.8.3.1 INSTALACIÓN DE LA DISTRIBUCIÓN CENTOS 6.0

Antes de proceder con la instalación del S.O escogido en el servidor de la institución, se instaló adecuadamente los dispositivos físicos necesarios, a partir de allí la instalación fue realizada siguiendo los pasos: 1. Encendido, 2. Configuración de bios con finalidad de que arranque inicialmente el computador desde el CD-ROM, 3. Reinicio del mismo, 4. Instalación. *Detalle de la instalación ver Anexo B*

6.8.3.2 DIRECCIONAMIENTO IP

La siguiente tabla ilustra el direccionamiento ip que se configuró dentro de la institución.

DISPOSITIVO	IP LAN	IP-WAN	GATEWAY-WAN
 Modem ADSL	192.168.1.1	190.152.169.238	
 Servidor	192.168.2.1/30	192.168.1.2	192.168.1.1
 Router Dlink	192.168.0.1/30	192.168.2.2	192.168.2.1
 Router Trendnet	192.168.10.1/30	192.168.2.3	192.168.2.1

TABLA 6.5 DIRECCIONAMIENTO IP
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

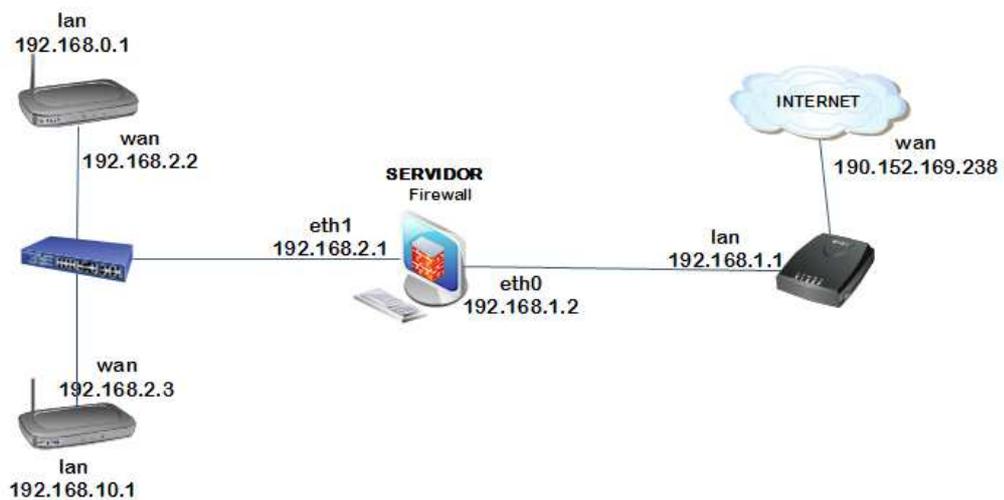
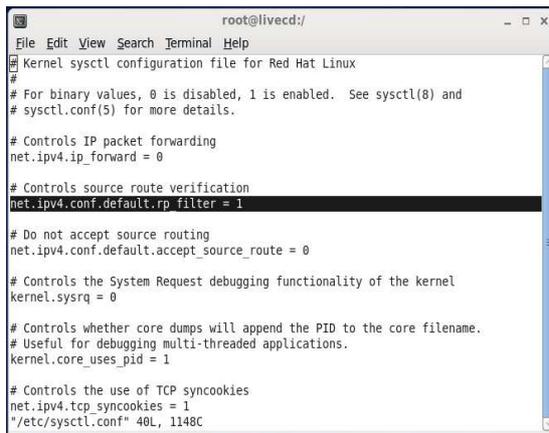


FIGURA 6.6 DIRECCIONAMIENTO IP
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

6.8.3.3 ENRUTAMIENTO

El servidor debe actuar como router para poder distribuir el internet hacia la red Lan, para lo cual se activó el enrutamiento de paquetes modificando el archivo `/etc/sysctl.conf` y cambiando la línea `net.ipv4.conf.default.forward = 1`.

Siguiendo los siguientes pasos:



```
root@livecd:/
File Edit View Search Terminal Help
Kernel sysctl configuration file for Red Hat Linux
#
# For binary values, 0 is disabled, 1 is enabled. See sysctl(8) and
# sysctl.conf(5) for more details.
#
# Controls IP packet forwarding
net.ipv4.ip_forward = 0
#
# Controls source route verification
net.ipv4.conf.default.rp_filter = 1
#
# Do not accept source routing
net.ipv4.conf.default.accept_source_route = 0
#
# Controls the System Request debugging functionality of the kernel
kernel.sysrq = 0
#
# Controls whether core dumps will append the PID to the core filename.
# Useful for debugging multi-threaded applications.
kernel.core_uses_pid = 1
#
# Controls the use of TCP syncookies
net.ipv4.tcp_syncookies = 1
"/etc/sysctl.conf" 40L, 1148C
```

1. Configuración del archivo

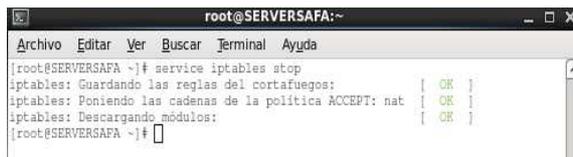
`/etc/sysctl.conf`

FIGURA 6.7 HABILITACIÓN ENRUTAMIENTO IP

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Service iptables stop



```
root@SERVERSAFA:~
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA ~]# service iptables stop
iptables: Guardando las reglas del cortafuegos: [ OK ]
iptables: Poniendo las cadenas de la política ACCEPT: nat [ OK ]
iptables: Descargando módulos: [ OK ]
[root@SERVERSAFA ~]#
```

2. Reinicio del servicio iptables o del firewall.

FIGURA 6.8 DETENCIÓN IPTABLES

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE



FIGURA 6.9 CONFIGURACIÓN FIREWALL PARA ENRUTAMIENTO IP
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

3. Configuración del iptables para que todos los paquetes que llegan al servidor salgan por la interfaz eth0 hacia el modem adsl es decir que puedan salir hacia el internet

Service iptables save



FIGURA 6.10 GUARDANDO CONFIGURACIÓN EN FIREWALL
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

4. Guardado de cambios

Service iptables restart

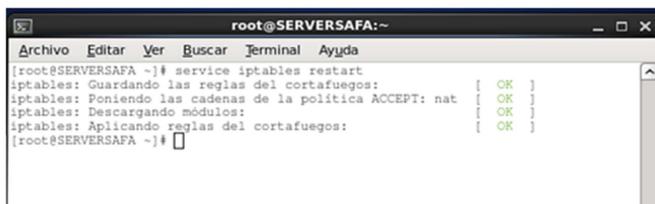


FIGURA 6.11 REINICIANDO CONFIGURACIÓN EN FIREWALL
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

5. Reinicio del servicio para que tomen efecto los cambios realizados en el cortafuego.

De esta forma los clientes Windows estarán recibiendo el internet proporcionado por el servidor "SERVERSAFA" evitando el tráfico innecesario que puede transcurrir por la red.

6.8.3.4 CONFIGURACIÓN DNS – BIND

La institución requiere de un servidor de dominio DNS entre otras funciones importantes para resolver el nombre del aula virtual que se empleará, como servidor de dns de cacheo y agilizar las búsquedas en el internet, los pasos para la configuración del mismo fueron:

1. EDICIÓN EL ARCHIVO ETC/HOSTS

Este fichero es utilizado para obtener una relación entre un nombre de máquina y una dirección IP: en cada línea de /etc/hosts se especifica una dirección IP y los nombres de máquina que le corresponden, de forma que un usuario no tenga que recordar direcciones sino nombres de hosts. Este archivo se lo utilizó para darle el nombre www.safavirtual.edu.ec al servidor.



FIGURA 6.12 COMANDO DE APERTURA ARCHIVO ETC/HOSTS
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Utilización del editor de texto vi para abrir el fichero etc/hosts.



FIGURA 6.13 ARCHIVO ETC/HOSTS
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Añadidura de la línea:
192.168.2.1 www.safavirtual.edu.ec
SERVERSAFA

dentro del archivo etc/hosts.

2. INSTALACIÓN DE BIND , CHROOT



```
root@SERVERSAFA:~  
Archivo Editar Ver Buscar Terminal Ayuda  
[root@SERVERSAFA ~]# yum -y install bind bind-chroot
```

FIGURA 6.14 INSTALACIÓN DE BIND
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Utilización del comando

`yum -y install bind chroot`

para instalar el paquete dns bind

3. APERTURA DEL PUERTO 53

Con la finalidad de que los clientes de la red de área local puedan hacer uso del servidor DNS en Internet, se abrió puerto 53 (dns), por TCP y UDP.



```
root@SERVERSAFA:~  
Archivo Editar Ver Buscar Terminal Ayuda  
[root@SERVERSAFA ~]# iptables -I INPUT -p udp --dport 53 -j ACCEPT  
[root@SERVERSAFA ~]# iptables -I INPUT -p tcp --dport 53 -j ACCEPT  
[root@SERVERSAFA ~]# service iptables save  
iptables: Guardando las reglas del cortafuegos en /etc/sysc[ OK ]tables:  
[root@SERVERSAFA ~]# service iptables restart  
iptables: Guardando las reglas del cortafuegos: [ OK ]  
iptables: Poniendo las cadenas de la política ACCEPT: nat f[ OK ]  
iptables: Descargando módulos: [ OK ]  
iptables: Aplicando reglas del cortafuegos: [ OK ]  
[root@SERVERSAFA ~]#
```

Manejo de los comandos:

`iptables -I Input -p udp -dport 53 -j ACCEPT`
`iptables -I Input -p tcp -dport 53 -j ACCEPT`

para abrir el del puerto 53 del
cortafuego

FIGURA 6.15 APERTURA DEL PUERTO 53 - CORTAFUEGOS

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

4. CREACIÓN DE LOS ARCHIVOS NECESARIOS PARA LA CONFIGURACIÓN DE BIND

Para la configuración del servidor de dominios (DNS) se requirieron ciertos archivos que fueron creados mediante los siguientes comandos:

```
# cp -R /usr/share/doc/bind-9.7.3/sample/var/named/* /var/named/chroot/var/named/  
# touch /var/named/chroot/var/named/data/cache_dump.db  
# touch /var/named/chroot/var/named/data/named_stats.txt  
# touch /var/named/chroot/var/named/data/named_mem_stats.txt  
# touch /var/named/chroot/var/named/data/named.run
```

```
# mkdir /var/named/chroot/var/named/dynamic
# touch /var/named/chroot/var/named/dynamic/managed-keys.bind
# chmod -R 777 /var/named/chroot/var/named/data
# chmod -R 777 /var/named/chroot/var/named/dynamic
```

```
root@SERVERSAFA:~
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA ~]# cp -R /usr/share/doc/bind-9.7.3/sample/var/named/* /var/named/chroot/var/named/
[root@SERVERSAFA ~]# touch /var/named/chroot/var/named/data/cache_dump.db
[root@SERVERSAFA ~]# touch /var/named/chroot/var/named/data/named_stats.txt
[root@SERVERSAFA ~]# touch /var/named/chroot/var/named/data/named_mem_stats.txt
[root@SERVERSAFA ~]# touch /var/named/chroot/var/named/data/named.run
root@SERVERSAFA ~]# mkdir /var/named/chroot/var/named/dynamic
root@SERVERSAFA ~]# touch /var/named/chroot/var/named/dynamic/managed-keys.bind
root@SERVERSAFA ~]# chmod -R 777 /var/named/chroot/var/named/data
root@SERVERSAFA ~]# chmod -R 777 /var/named/chroot/var/named/dynamic
root@SERVERSAFA ~]#
```

Creación de archivos de configuración de Bind y otorgación de permisos

FIGURA 6.16 CREACIÓN DE ARCHIVOS DE CONFIGURACIÓN - BIND

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

5. CONFIGURACIÓN DEL ARCHIVO /VAR/NAMED/CHROOT/ETC/NAMED.CONF

Para la configuración del archivo named se necesitó copiar la clave de RNDC la cual fue obtenida mediante el comando

```
# cat /etc/mdc.key
```

Posteriormente se escribió la configuración necesaria dentro del archivo named.conf

```
root@SERVERSAFA:~
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA ~]# touch /var/named/chroot/etc/named.conf
[root@SERVERSAFA ~]# vim /var/named/chroot/etc/named.conf
[root@SERVERSAFA ~]#
```

Creación del archivo named.conf en la dirección /var/named/chroot/etc

FIGURA 6.17 CREACIÓN DEL ARCHIVO NAMED- BIND

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

```
root@SERVERSIFA:/var/named/chroot/etc
Archivo Editar Ver Buscar Terminal Ayuda
key "rndc-key" {
    algorithm hmac-md5;
    secret "u68PuwWuYrWaveh5I3Ss2w==";
};

controls {
    inet 127.0.0.1 allow { 127.0.0.1; } keys { rndc-key; };
    inet 192.168.2.1 allow { 192.168.2.0/24; } keys { rndc-key; };
};

options {
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    pid-file "/var/run/named/named.pid";
    memstatistics-file "var/named/data/named_mem_stats.txt";

    recursion yes;

    bindkeys-file "/etc/named.iscdlv.key";

    allow-recursion {
        localhost;
        127.0.0.1;
        192.168.2.0/24;
    };

    forwarders {
        200.107.60.58;
        200.107.10.52;
    };

    listen-on {
        localhost;
        127.0.0.1;
        192.168.2.1;
    };

    query-source address * port 53;

    version "REFUSED";

    allow-query {
        localhost;
        127.0.0.1;
        192.168.2.0/24;
    };

    server 192.168.2.0 {
        keys { rndc-key; };
    };

    zone "." IN {
        type hint;
        file "named.ca";
    };

    include "/etc/named.rfc1912.zones";

    //forward zone
    zone "safavirtual.edu.ec" IN {
        type master;
        file "safavirtual.edu.ec.zone";
        allow-transfer { 192.168.2.2; };
        notify yes;
        also-notify { 192.168.2.2; };
    };

    //reservezone
    zone "2.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.2.zone";
        allow-transfer { 192.168.2.2; };
        notify yes;
        also-notify { 192.168.2.2; };
    };
};
```

*Archivo named.conf
configurado, mismo que
contiene la ubicación de la
zona directa e inversa.*

FIGURA 6.18 ARCHIVO NAMED - BIND
*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

6. CONFIGURACIÓN DE LA ZONA DE BÚSQUEDA DIRECTA

Para su configuración se requirió la creación del archivo `safavirtual.edu.ec.zone`, la información más relevante añadida dentro de éste es la siguiente:

`safavirtual.edu.ec IN NS ns.safavirtual.edu.ec` - Relaciona el nombre de subdominio `safavirtual.edu.ec` con el servidor de nombres responsable de la zona en este caso `ns.safavirtual.edu.ec`

`ns.safavirtual.com IN A 192.168.2.1` - Traduce el nombre del servidor a la dirección IP del mismo

`www.safavirtual.edu.ec IN CNAME ns.safavirtual.edu.ec` - Asigna como alias `ns.safavirtual.com` al nombre de la máquina.

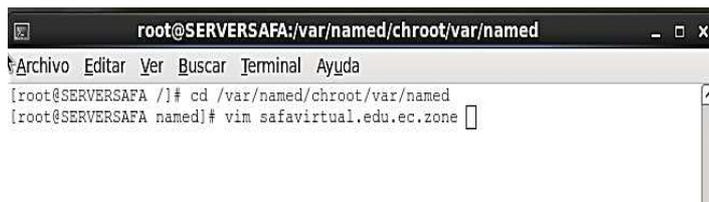


FIGURA 6.19 CREACIÓN DE LA ZONA DIRECTA - BIND
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Utilización del
comando

`vim safavirtual.edu.ec.zone`
para crear y abrir el
archivo de zona directa

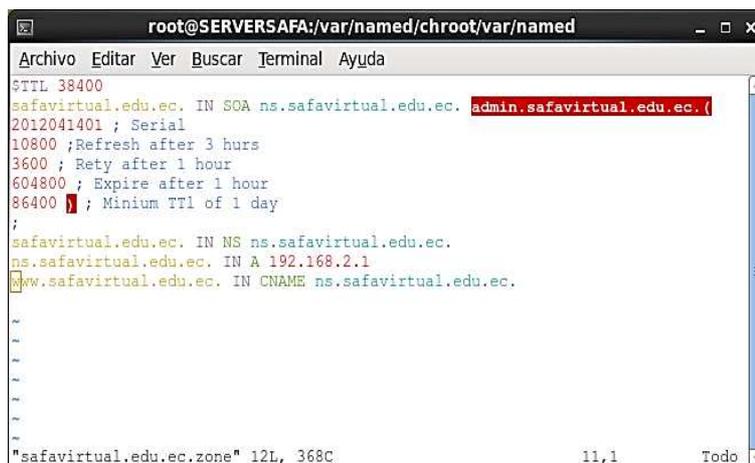


FIGURA 6.20 ARCHIVO DE ZONA DIRECTA - BIND
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Contenido del archivo
de zona directa
llamado
`safavirtual.edu.ec.zone`

8. REINICIO DEL SERVICIO Y CONFIGURACIÓN PARA QUE SE LEVANTE AL INICIAR EL SERVIDOR



```
root@SERVERSAFA:~  
[root@SERVERSAFA ~]# /etc/rc.d/init.d/named restart  
Deteniendo named: [ OK ]  
Iniciando named: [ OK ]  
[root@SERVERSAFA ~]#
```

Reinició el servicio mediante el comando `restart` y configuración del levantamiento automático del servicio mediante el comando `chkconfig`

FIGURA 6.23 REINICIO DEL SERVICIO NAMED

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

9. EDICIÓN DEL ARCHIVO /ETC/RESOLV.CONF Y REINICIO DE LA RED



```
root@SERVERSAFA:~  
# Generated by NetworkManager  
domain www.safavirtual.edu.ec  
search www.safavirtual.edu.ec  
  
nameserver 192.168.2.1  
nameserver 192.168.10.1  
-  
-
```

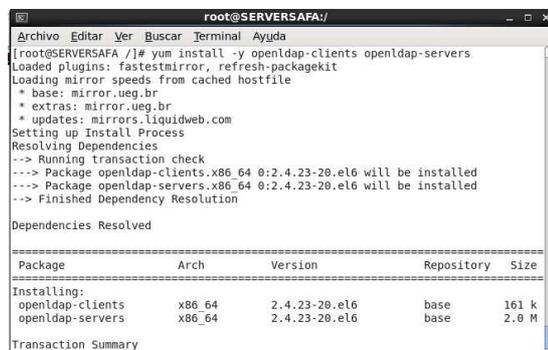
Es necesario configurar correctamente el archivo `/etc/resolv.conf` para que se pueda resolver los nombres de los servidores en Internet.

FIGURA 6.24 CONFIGURACIÓN DEL ARCHIVO ETC/RESOLV.CONF

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

6.8.3.5 CONFIGURACIÓN OPENLDAP

OPENLDAP es comúnmente usado para administrar usuarios y grupos con propósitos de autenticación. Para su configuración se siguieron los siguientes pasos:



```
root@SERVERSAFA:~  
[root@SERVERSAFA /]# yum install -y openldap-clients openldap-servers  
Loaded plugins: fastestmirror, refresh-packagekit  
Loading mirror speeds from cached hostfile  
* base: mirror.ueg.br  
* extras: mirror.ueg.br  
* updates: mirrors.liquidweb.com  
Setting up Install Process  
Resolving Dependencies  
--> Running transaction check  
--> Package openldap-clients.x86_64 0:2.4.23-20.el6 will be installed  
--> Package openldap-servers.x86_64 0:2.4.23-20.el6 will be installed  
--> Finished Dependency Resolution  
  
Dependencies Resolved  
  
=====
```

Package	Arch	Version	Repository	Size
Installing:				
openldap-clients	x86_64	2.4.23-20.el6	base	161 k
openldap-servers	x86_64	2.4.23-20.el6	base	2.0 M

```
Transaction Summary  
-----
```

Instalación openldap mediante el comando:
`yum install openldap openldap-clients openldap-servers`

FIGURA 6.25 INSTALACION DE OPENLDAP

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

OpenLdap necesita un archivo de parámetros para iniciar una nueva base de datos, este archivo debe ser copiado al directorio de base datos de Ldap.

Además verificar que el directorio `var/lib/ldap` le pertenezca al usuario `ldap`:



```
root@SERVERSAFA:/var/named/chroot/var/named
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA named]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
[root@SERVERSAFA named]# chown -R ldap:ldap /var/lib/ldap
[root@SERVERSAFA named]#
```

FIGURA 6.26 VERIFICACIÓN DE PERMISOS Y GESTIÓN DB_CONFIG

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Aplicación del comando:

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

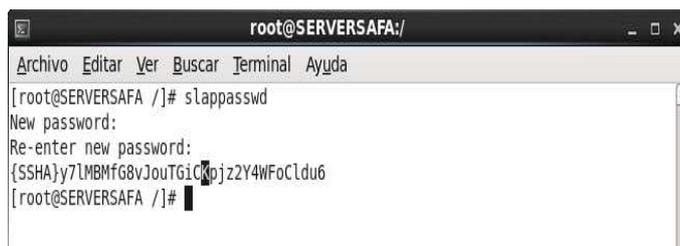
para copiar el archivo `DB_CONFIG.example` a la dirección de configuración de `ldap`

y del comando

```
chown -R ldap:ldap /var/lib/ldap
```

para que el directorio `var/lib/ldap` le pertenezca al usuario `ldap`

Las opciones de configuración se encuentran en el directorio `/etc/openldap/slap.p`



```
root@SERVERSAFA:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# slappasswd
New password:
Re-enter new password:
{SSHA}y7lMBMfG8vJouT6iCp0jz2Y4WfoCldu6
[root@SERVERSAFA /]#
```

FIGURA 6.27 CREACIÓN DE CONTRASEÑA

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Obtención de una clave de administrador para la utilización de servicio de directorio, mediante el comando:
`slappasswd`

Tras obtener la clave de administrador se solicita que se ingrese la clave para el servidor de directorio, al escribir la clave devuelve la misma clave pero esta a su vez encriptada, la cual se requiere copiar ya que será utilizada posteriormente.



```
root@SERVERSAFA:/etc/openldap/slapd.d/cn=config
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# cd /etc/openldap/slapd.d/cn=config
[root@SERVERSAFA cn=config]# vi olcDatabase={2}bdb.ldif
```

Edición el archivo cn=config ubicado en el directorio /etc/openldap/slapd.d mediante los comandos:

```
cd /etc/openldap/slapd.d/cn=config
vi olcDatabase={2}bdb.ldif
```

**FIGURA 6.28 CONFIGURACIÓN DEL ARCHIVO
OLCDATABASE={2}BDB.LDIF**
*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

Dentro de este archivo se busca la línea **olcSuffix: dc=my-domain,dc=com** y en su lugar se escribe **olcSuffix: dc=safa,dc=com**

En la línea: **olcRoot:cn=Manager,dc=my-domain,dc=com** se especifica el usuario administrador de la base de datos de openldap , donde se modificó de la siguiente manera: **olcRoot:cn=Manager,dc=safa,dc=com**

Adicionalmente se añadió la siguiente línea debajo de **olcRootDn: <clave encriptada>** en este caso: **olcRootPw:{SSHA}x6QZR4yae4kAUdof2dNKUFseqgVtzt9**

El código escrito junto a **olc:RootPW:** es la clave encriptada que fue copiada anteriormente al ejecutar slappasswd.

```

AdminSafa@SERVERSAFA:/etc/openldap/slapd.d/cn=config
Archivo Editar Ver Buscar Terminal Ayuda
dn: olcDatabase={2}bdb
objectClass: olcDatabaseConfig
objectClass: olcBdbConfig
olcDatabase: {2}bdb
olcSuffix: dc=safa,dc=com
olcAddContentAcl: FALSE
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcReadOnly: FALSE
olcRootDN: cn=Manager,dc=safa,dc=com
olcRootPW: {SSHA}xGQZR4yae4kAUdof2dNKUFseggVtzt9
olcSyncUsSubentry: FALSE
olcMonitoring: TRUE
-- INSERTAR --
12,10 Comienzo

```

FIGURA 6.29 CONTENIDO DEL ARCHIVO `olcDatabase={2}bdb.ldif`

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Posteriormente se realizó la edición el archivo `olcDatabase={1}monitor.ldif` mediante los comandos:

```

cd /etc/openldap/slapd.d/cn=config
vi olcDatabase={1}bdb.ldif

```

```

root@SERVERSAFA:/etc/openldap/slapd.d/cn=config
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# cd /etc/openldap/slapd.d/cn=config
[root@SERVERSAFA cn=config]# vi olcDatabase={1}bdb.ldif

```

FIGURA 6.30 CONFIGURACIÓN DEL ARCHIVO `olcDatabase={1}bdb.ldif`

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Reemplazo de las líneas:

```

olcAccess:{0} to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by
dn.base="cn=Manager,dc=my-domain,dc=com" read by *none

```

por las siguientes:

```

olcAccess:{0} to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read by
dn.base="cn=Manager,dc=safa,dc=com" read by *none

```



```

AdminSafa@SERVERSAFA:/etc/openldap/slapd.d/cn=config
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA cn=config]# service slapd start
Iniciando slapd: [ OK ]
[root@SERVERSAFA cn=config]# chkconfig slapd on
[root@SERVERSAFA cn=config]# █

```

FIGURA 6.33 INICIO DEL SERVICIO SLAPD
Fuente: Escuela Sagrada Familia
Elaborado por: Adriana Salinas

CREACIÓN DE ENTRADAS EN LA BASE DE DATOS

Para poder utilizar el directorio de LDAP se necesita importar algunas entradas de base de datos, para hacer esto se requirió la creación de un archivo llamado **safa.ldif** con los siguientes contenidos:

```

root@SERVERSAFA:/etc/openldap
Archivo Editar Ver Buscar Terminal Ayuda
dn: dc=safa,dc=com
dc: safa
objectClass: top
objectClass: domain

dn: ou=people,dc=safa,dc=com
ou: people
objectClass: top
objectClass: organizationalUnit

dn: ou=groups,dc=safa,dc=com
ou: groups
objectClass: top
objectClass: organizationalUnit

"safa.ldif" 14L, 245C 1,1 Todo

```

FIGURA 6.34 CREACIÓN DE ENTRADAS EN LA BDD - OPENLDAP
Fuente: Escuela Sagrada Familia
Elaborado por: Adriana Salinas

```

dn: dc=safa,dc=com
dc:safa
objectClass:top
objectClass:domain

```

```

dn:
ou=people,dc=safa,dc=com
ou:people

```

```

objectClass:top
objectClass:organization
alUnit

```

```

dn:
ou=groups,dc=safa,dc=com
ou:groups
objectClass:top
objectClass:organization
alUnit

```

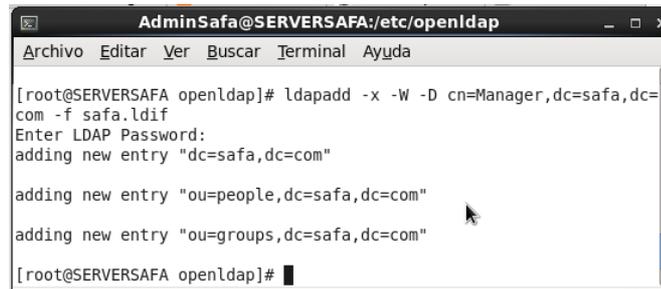
EL siguiente paso fué importar el archivo **safa.ldif** a la base de datos de LDAP mediante el comando:

```

ldapadd -x -W -D cn=Manager,dc=safa,dc=com -f safa.ldif

```

Solicitó la clave de acceso LDAP que fue creada anteriormente mediante slappasswd y mostró las entradas que están siendo añadidas.



```
AdminSafa@SERVERSAFA:/etc/openldap
Archivo Editar Ver Buscar Terminal Ayuda

[root@SERVERSAFA openldap]# ldapadd -x -W -D cn=Manager,dc=safa,dc=com -f safa.ldif
Enter LDAP Password:
adding new entry "dc=safa,dc=com"

adding new entry "ou=people,dc=safa,dc=com"

adding new entry "ou=groups,dc=safa,dc=com"

[root@SERVERSAFA openldap]#
```

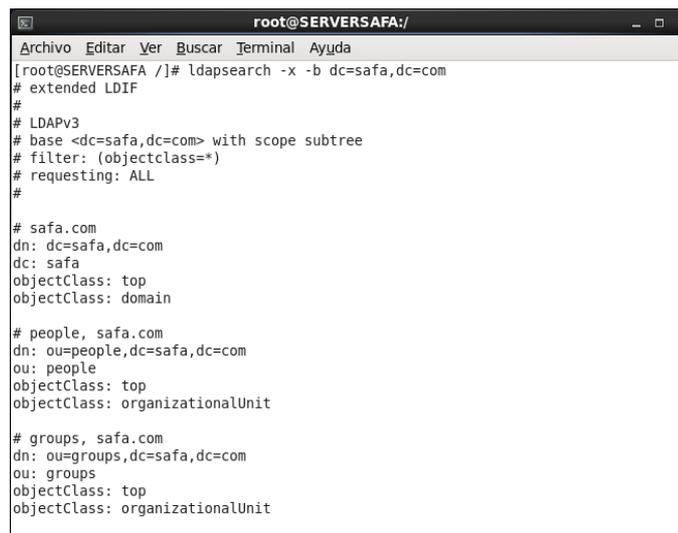
FIGURA 6.35 IMPORTACIÓN DEL ARCHIVO SAFA.LDIF

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Para comprobar la información almacenada en la base se ejecutó el siguiente comando:

ldapsearch -x -b dc=safa,dc=com



```
root@SERVERSAFA:/
Archivo Editar Ver Buscar Terminal Ayuda

[root@SERVERSAFA /]# ldapsearch -x -b dc=safa,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=safa,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# safa.com
dn: dc=safa,dc=com
dc: safa
objectClass: top
objectClass: domain

# people, safa.com
dn: ou=people,dc=safa,dc=com
ou: people
objectClass: top
objectClass: organizationalUnit

# groups, safa.com
dn: ou=groups,dc=safa,dc=com
ou: groups
objectClass: top
objectClass: organizationalUnit
```

FIGURA 6.36 COMPROBACION DE INFORMACION EN BDD - OPENLDAP

Fuente. Escuela Sagrada Familia

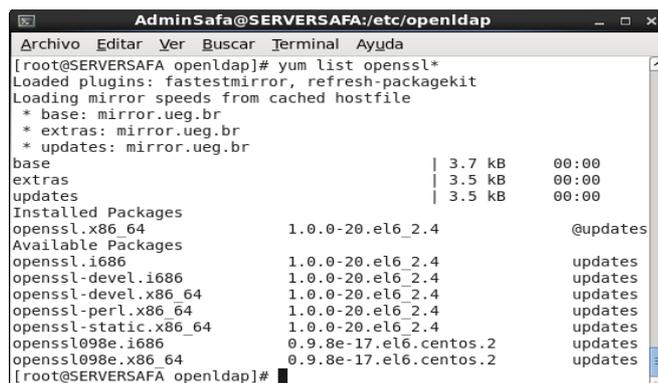
Elaborado por: Adriana Salinas

GENERACIÓN DE UN CERTIFICADO PARA EL SERVIDOR LDAP

Para realizar esta acción se utilizó openssl,

Revisión de instalación mediante:

```
yum list openssl*
```



```
AdminSafa@SERVERSAFA:/etc/openldap
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA openldap]# yum list openssl*
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.ueg.br
 * extras: mirror.ueg.br
 * updates: mirror.ueg.br
base                               | 3.7 kB    00:00
extras                             | 3.5 kB    00:00
updates                            | 3.5 kB    00:00
Installed Packages
openssl.x86_64                     1.0.0-20.el6_2.4      @updates
Available Packages
openssl.i686                       1.0.0-20.el6_2.4      updates
openssl-devel.i686                 1.0.0-20.el6_2.4      updates
openssl-devel.x86_64               1.0.0-20.el6_2.4      updates
openssl-perl.x86_64                1.0.0-20.el6_2.4      updates
openssl-static.x86_64              1.0.0-20.el6_2.4      updates
openssl098e.i686                   0.9.8e-17.el6.centos.2 updates
openssl098e.x86_64                 0.9.8e-17.el6.centos.2 updates
[root@SERVERSAFA openldap]#
```

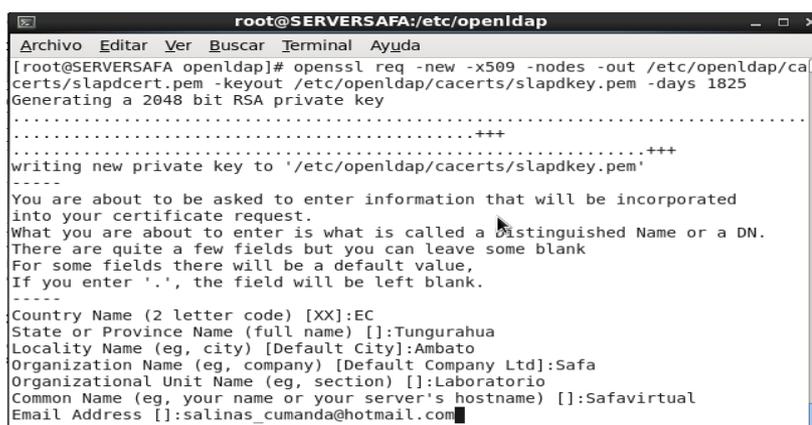
FIGURA 6.37 REVISIÓN DE LA INSTALACIÓN DE OPENSLL

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Generación de llave y certificado mediante el siguiente comando:

```
Openssl req -new -x509 -nodes -out /etc/openldap/cacerts/slapdcert.pem -
keyout /etc/openldap/cacert/slapdkey.pem -days 1825
```



```
root@SERVERSAFA:/etc/openldap
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA openldap]# openssl req -new -x509 -nodes -out /etc/openldap/ca
certs/slapdcert.pem -keyout /etc/openldap/cacert/slapdkey.pem -days 1825
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/openldap/cacerts/slapdkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:EC
State or Province Name (full name) []:Tungurahua
Locality Name (eg, city) [Default City]:Ambato
Organization Name (eg, company) [Default Company Ltd]:Safa
Organizational Unit Name (eg, section) []:Laboratorio
Common Name (eg, your name or your server's hostname) []:Safavirtual
Email Address []:salinas_cumanda@hotmail.com
```

FIGURA 6.38 GENERACIÓN DE LLAVE Y CERTIFICADO OPENSLL

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

La llave y certificado se crearon en el directorio /etc/openldap/cacerts, el hostname que se utilizó en este certificado debe coincidir con la configuración de authconfig-tui que se realizará en el siguiente paso. Notar que -days 1825 indica que el certificado tendrá una duración de 5 años.

La llave y certificado necesita entradas en la configuración del servidor LDAP lo cual se realizó mediante el comando:

```
vi etc/openldap/slapd.d/cn=config.ldif
```



FIGURA 6.39 COMANDO DE APERTURA ARCHIVO CN=CONFIG.LDIF

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

Se añadió las líneas:

```
olcTLSCertificateFile:/etc/openldap/cacerts/slapdcert.pem  
olcTLSCertificateKeyFile:/etc/openldap/cacerts/slapdkey.pem
```

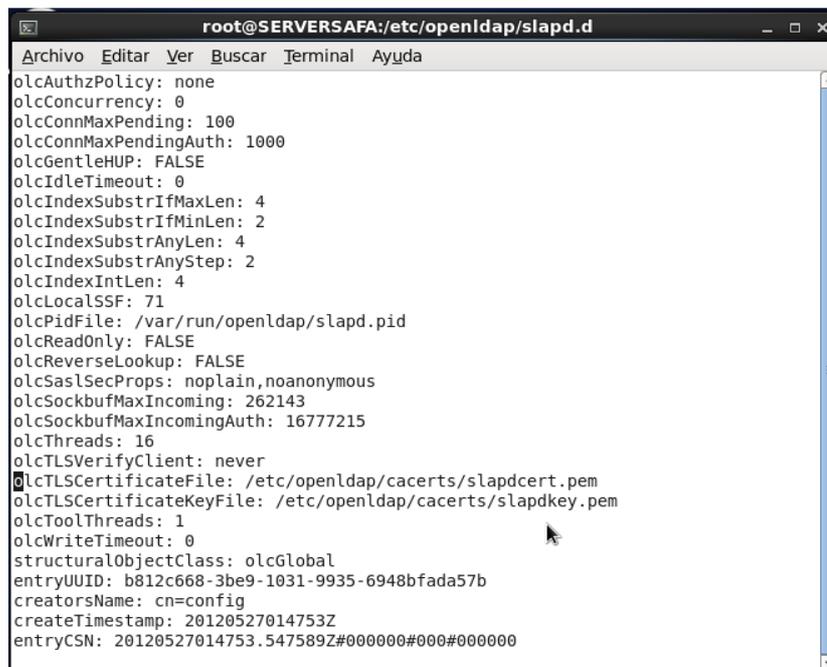


FIGURA 6.40 CONFIGURACIÓN DEL ARCHIVO CN=CONFIG.LDIF

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

6.8.3.5.1 CONFIGURACIÓN DE CENTOS PARA UTILIZAR AUTENTICACIÓN LDAP

Comprobación de la instalación nss-pam-ldapd

Yum install nss-pam-ldapd



```
root@SERVERSAFA:/  
Archivo Editar Ver Buscar Terminal Ayuda  
[root@SERVERSAFA /]# yum install nss-pam-ldapd  
Loaded plugins: fastestmirror, refresh-packagekit  
Loading mirror speeds from cached hostfile  
* Webmin: download.webmin.com  
* base: centos-mirror.hostdime.com.br  
* extras: centos-mirror.hostdime.com.br  
* updates: centos-mirror.hostdime.com.br
```

FIGURA 6.41 INSTALACIÓN DE NSS-PAM-LDAP

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Configuración de autenticación

Authconfig-tui

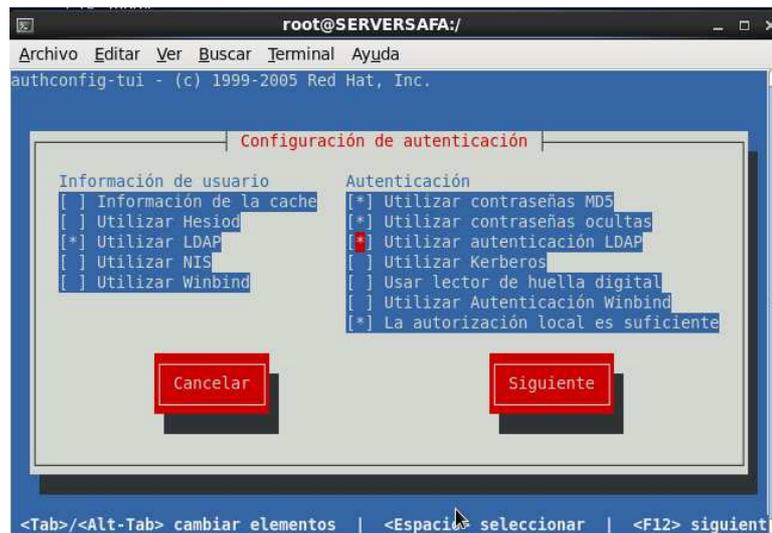


```
AdminSafa@SERVERSAFA:/etc/openldap  
Archivo Editar Ver Buscar Terminal Ayuda  
[root@SERVERSAFA openldap]# authconfig-tui
```

FIGURA 6.42 EJECUCIÓN DEL COMANDO AUTHCONFIG-TUI

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Selección “Utilizar LDAP”:



```
root@SERVERSAFA:/  
Archivo Editar Ver Buscar Terminal Ayuda  
authconfig-tui - (c) 1999-2005 Red Hat, Inc.  
Configuración de autenticación  
Información de usuario  
[ ] Información de la cache  
[ ] Utilizar Hesiod  
[*] Utilizar LDAP  
[ ] Utilizar NIS  
[ ] Utilizar Winbind  
Autenticación  
[*] Utilizar contraseñas MD5  
[*] Utilizar contraseñas ocultas  
[*] Utilizar autenticación LDAP  
[ ] Utilizar Kerberos  
[ ] Usar lector de huella digital  
[ ] Utilizar Autenticación Winbind  
[*] La autorización local es suficiente  
Cancelar Siguiete  
<Tab>/<Alt-Tab> cambiar elementos | <Espacio> seleccionar | <F12> siguiete
```

FIGURA 6.43 CONFIGURACIÓN DE AUTENTICACIÓN

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

AÑADIR USUARIOS Y GRUPOS

Con el objetivo de hacer más fácil el añadir usuarios y grupos se utilizó la herramienta *Webmin LDAP Usuarios y grupos*.

Para poder instalar webmin desde los repositorios de Centos es necesario crear el archivo *webmin.repo* en la ubicación *etc/yum.repos.d* mediante el comando:

```
vim /etc/yum.repos.d/webmin.repo
```



FIGURA 6.44 CREACIÓN DEL ARCHIVO WEBMIN.REPO

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Configuración del archivo webmin.repo.

```
[Webmin]
Name=Webmin Distribution Neutral
#baseurl=http://download.webmin.com/download/yum
mirrorlist=http://download.webmin.com/download/yum/mirrorlist
enabled=1
```



FIGURA 6.45 ARCHIVO WEBMIN.REPO

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Importación de claves:

```
wget http://www.webmin.com/jcameron-key.asc
rpm --import jcameron-key.asc
```



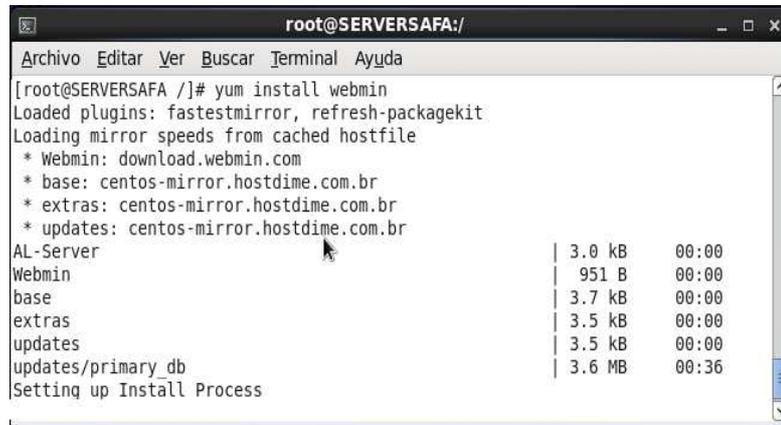
FIGURA 6.46 IMPORTACIÓN DE CLAVES

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Instalación webmin desde los repositorios mediante el comando:

`yum install webmin`



```
root@SERVERSAFA: /
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# yum install webmin
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * Webmin: download.webmin.com
 * base: centos-mirror.hostdime.com.br
 * extras: centos-mirror.hostdime.com.br
 * updates: centos-mirror.hostdime.com.br
AL-Server | 3.0 kB | 00:00
Webmin | 951 B | 00:00
base | 3.7 kB | 00:00
extras | 3.5 kB | 00:00
updates | 3.5 kB | 00:00
updates/primary_db | 3.6 MB | 00:36
Setting up Install Process
```

FIGURA 6.47 INSTALACIÓN DE WEBMIN

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Para poder utilizar Webmin en el explorador se requiere escribir “dirección ip : 10000” en este caso 192.168.2.1:1000

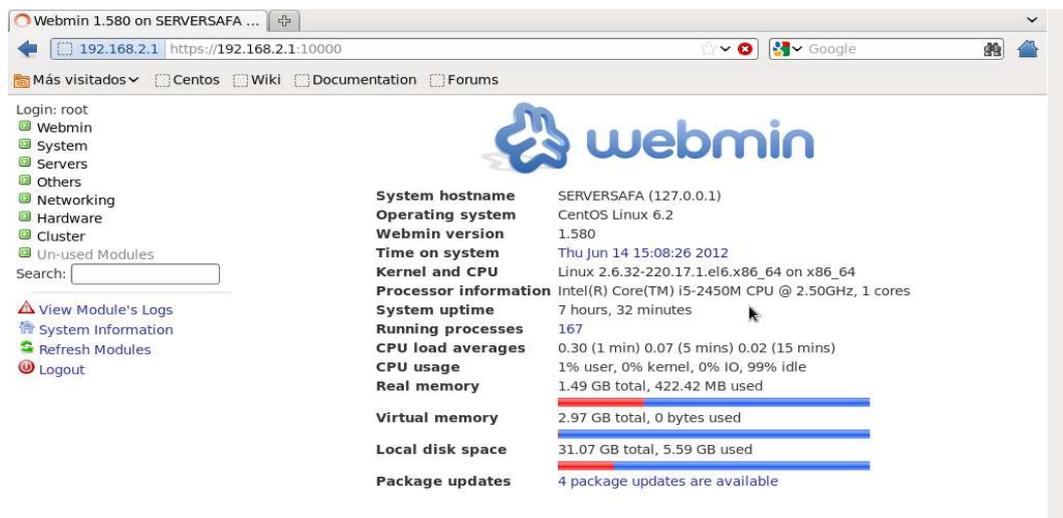


FIGURA 6.48 PORTADA WEBMIN

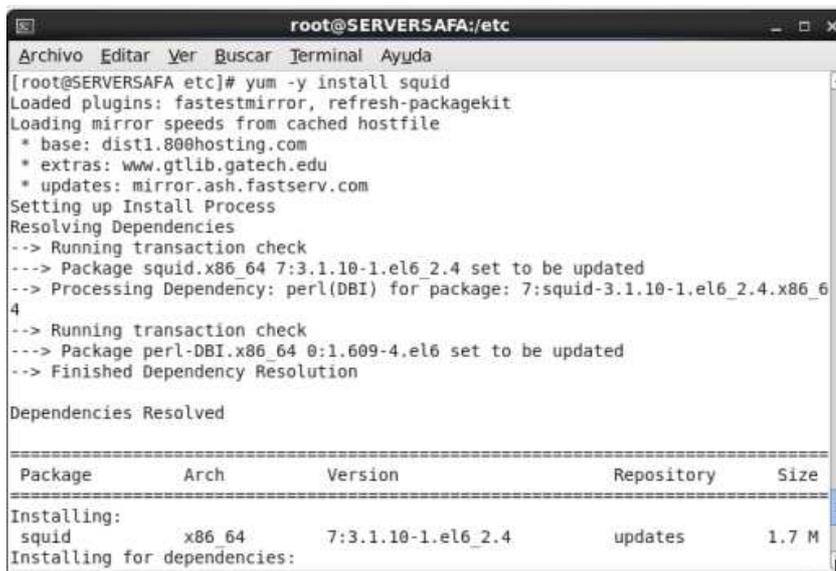
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

6.8.3.6 CONFIGURACIÓN PROXY - SQUID

El término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP

Los pasos a seguir para su funcionamiento son:

- **INSTALACIÓN DE SQUID MEDIANTE EL COMANDO `yum -y install squid`**



```
root@SERVERSAFA:/etc
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA etc]# yum -y install squid
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: dist1.800hosting.com
 * extras: www.gtlib.gatech.edu
 * updates: mirror.ash.fastserv.com
Setting up Install Process
Resolving Dependencies
--> Running transaction check
--> Package squid.x86_64 7:3.1.10-1.el6_2.4 set to be updated
--> Processing Dependency: perl(DBI) for package: 7:squid-3.1.10-1.el6_2.4.x86_64
--> Running transaction check
--> Package perl-DBI.x86_64 0:1.609-4.el6 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Installing:
 squid x86_64 7:3.1.10-1.el6_2.4 updates 1.7 M
Installing for dependencies:
```

FIGURA 6.49 INSTALACIÓN DE SQUID
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

- **ARCHIVOS DE CONFIGURACIÓN DEL SQUID**

Los archivos de configuración de squid se encuentran en la ruta ***etc/squid*** el más importante de ellos es ***squid.conf*** el cual se encarga de la configuración del servicio.

Por recomendación antes de editar un archivo de configuración de algún servicio, siempre se debe hacer una copia de respaldo original del mismo.

- **CONFIGURACIÓN DE SQUID - PARAMETROS**

En el archivo de configuración squid.conf ubicado en la ruta /etc/squid/ se harán las siguientes modificaciones:

PARÁMETRO	DESCRIPCIÓN
<i>http_port 3128</i>	<i>Establece el puerto de escucha para squid ,por defecto puerto 3128</i>
<i>access_log /var/log/squid/access.log squid</i>	<i>Especifica en que directorio se realizara el registro de accesos al squid.</i>
<i>cache_dir ufs /var/spool/squid 700 16 256</i>	<i>Con este parámetro se establece el tamaño deseado para la cache en el disco</i>

TABLA 6.6 DATOS DE CONFIGURACION - SQUID

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

➤ CONFIGURACIÓN DE SQUID - REGLAS ACL

Una ACL es una definición de control de acceso, existen varios tipos de reglas ACL como: src, time, dts, srcdomain, dstdomain, time, url_regex, urlpath_regex, req_mime, Para la configuración del servidor Proxy se hizo uso de algunas de ellas, la tabla siguiente muestra las reglas que se han aplicado con una descripción de las mismas.

PARÁMETRO	REGLA APLICADA	DESCRIPCIÓN
Acl [Nombre] src [Contenido]	<i>acl laboratorio src 192.168.0.0/24</i>	El nombre de la regla es llamada laboratorio y tiene asignado el segmento de red 192.168.0.0 mascara 255.255.255.0
	<i>acl routers src 192.168.2.1 – 192.168.2.4</i>	Esta regla se denomina routers comprendiendo las ip desde la 192.168.2.1 hasta la 192.168.2.4
Acl [Nombre] url_regex “Path”	<i>Acl filtrar url_regex “etc/squid/filtrar”</i>	Esta regla se llama filtrar la cual manda a llamar a un archivo llamado filtrar ubicado en la ruta etc/squid.
	<i>acl sociales url_regex “etc/squid/sociales”</i>	Esta regla se llama sociales la cual manda a llamar a un archivo llamado sociales ubicado en la ruta etc/squid.
	<i>acl descargas url_path regex “etc/squid/descargas”</i>	Esta regla se llama descargas la cual manda a llamar a un archivo llamado descargas ubicado en la ruta etc/squid.
	<i>acl horario time MTWTFH 07:00 – 14:00</i>	La regla horario establece que está habilitada los días Lunes a Viernes de 07:00 a 14:00
	<i>acl password proxy auth required</i>	Habilita la regla para la autenticación de usuarios.

TABLA 6.7 REGLAS DE ACCESO - SQUID

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

➤ **CONFIGURACIÓN DE SQUID – CONTROL DE ACCESO**

Las reglas de control de acceso especifican si se permite o deniega el acceso a las reglas creadas con anterioridad, su nomenclatura es:

http_access allow/deny regla

Acceso a Regla	Descripción
http_access allow routers !horario	Permite la navegación a las ips especificadas en la regla routers (192.168.2.1 - 192.168.2.4) sin ninguna restricción, fuera del horario que se especifica en la regla llamada horario
http_access allow horario routers !sociales !filtrar !descargas password	<p>Establece el requerimiento de contraseña para el acceso al internet, y además especifica que están bloqueadas las páginas que se indiquen en los archivos correspondientes a las reglas sociales, filtrar y descargas</p> <p>Todo en el horario especificado por la regla horario (07:00 – 14:00)</p>

TABLA 6.8 CONTROL DE ACCESO - SQUID

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

➤ CONFIGURACIÓN DE SQUID – AUTENTICACIÓN LDAP

Considerando que se ha configurado exitosamente OpenLDAP como servidor de autenticación, sólo se necesita definir el directorio (o subdirectorio) y el servidor LDAP a utilizar.

Para lo cual se añaden las siguientes líneas al archivo de configuración de squid.

```
auth_param basic program /usr/lib64/squid/squid_ldap_auth -b  
"dc=safavirtual,dc=com" -f "uid=%s" -h 192.168.2.1
```

Con esto estará terminada la configuración del servidor proxy squid, la siguiente imagen muestra el archivo squid.conf

FIGURA 6.50 ARCHIVO SQUID.CONF
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

128

La imagen 6.51 detalla una parte del contenido del archivo **filtrar** ubicada en la dirección etc/squid que sirve de base para la regla de tipo url_regex creada anteriormente.

```
root@SERVERSAFA:/etc/squid
Archivo Editar Ver Buscar Terminal Ayuda
130.94.139.201/porno
130.94.139.201/pornotour
130.94.141.202/karls-cum-tent
130.94.141.207/hlg
130.94.141.214/pips-all-fun-tranny-show
130.94.141.52/1
130.94.142.168/lez
130.94.142.168/teen
130.94.143.171/www/parx/gp02
130.94.143.171/www/pikachu
130.94.143.171/www/pornxaction
130.94.143.195/www/hot/sex
130.94.143.242/www/sexxx
130.94.143.242/www/xxx
130.94.143.95/doggy/touch/hole8
130.94.143.95/kitty/please/lip8
130.94.143.95/luck/sand/ali8
130.94.143.95/pool/lesbo
130.94.143.95/rudy/kossa7
133.130.3.7/~gogo77
133.130.3.7/~shy
13370.com/gallerys/mza2
133.wizardtech.net/patricia-ford
1352.dial-messenger.com/gay
136479.com/cum
137.165.37.207/orgs/peerh/sex
140.99.107.25/babes
140.99.107.25/latinamateur
1438.dial-messenger.com/sexy
146.164.44.62/instalado
147.210.18.149/~lebrusq/girl
150.254.5.54/~giga/4boys
151.196.206.42/kc
151.196.213.3/fetishes
151.196.214.69/sjaynethumbs
151.196.220.72/fetishes
152.7.7.42/movies
157.238.200.197/personal/giggs/gogo15
157.238.200.34/www/busty
157.238.200.34/www/fred/111/69w
157.238.200.34/www/fred/111/70r
157.238.200.34/www/fuck/snt2/hrdn301
157.238.200.34/www/mystickyspot/lesbian1126
```

FIGURA 6.51 ARCHIVO FILTRAR
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

La imagen 6.52 detalla el archivo **sociales** ubicada en la dirección etc/squid que sirve de base para la regla de tipo url_regex creada anteriormente

```
root@SERVERSAFA:/etc/squid
Archivo Editar Ver Buscar Terminal Ayuda
facebook.com
www.facebook.com
hi5.com
www.hi5.com
badoo.com
www.badoo.com
myspace.com
www.myspace.com
twitter.com
www.twitter.com
www.youtube.com
~
~
```

FIGURA 6.52 ARCHIVO SOCIALES
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

La imagen 6.53 detalla una parte del contenido del archivo **descargas** ubicada en la dirección etc/squid que sirve de base para la regla de tipo url_regex creada anteriormente



FIGURA 6.53 ARCHIVO DESCARGAS
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

6.8.3.7 CONFIGURACIÓN PLATAFORMA EDUCATIVA – MOODLE

Moodle es un Sistema de Gestión de Cursos de Código Abierto, conocido también como Sistema de Gestión del Aprendizaje. Es una aplicación web gratuita que los educadores pueden utilizar para crear sitios de aprendizaje efectivo en línea.

Para su instalación y configuración es necesario tener instalado php y mysql, lo cual se instaló mediante los repositorios de centos:

yum install mysql-server mysql-devel

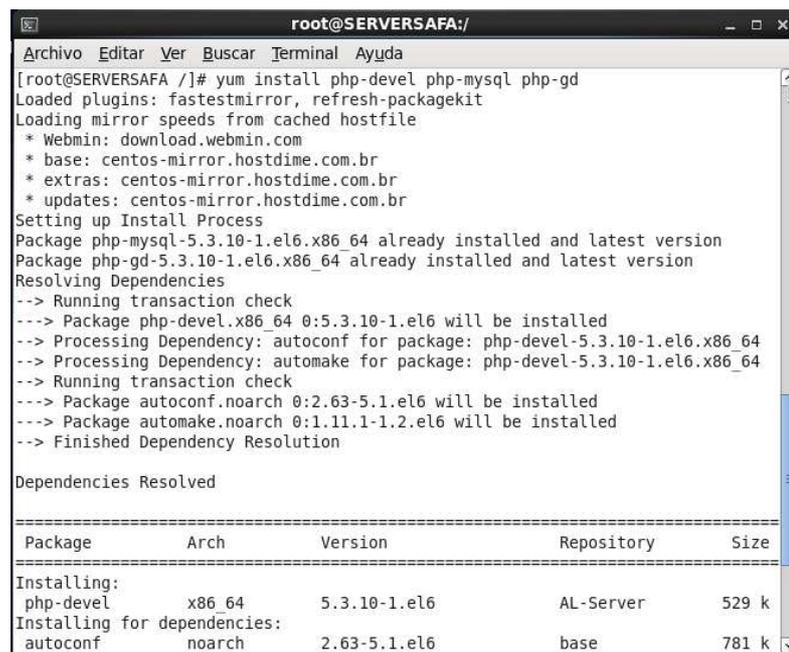


```
root@SERVERSAFA: /
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# yum install mysql-server mysql-devel
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
* Webmin: download.webmin.com
* base: centos-mirror.hostdime.com.br
* extras: centos-mirror.hostdime.com.br
* updates: centos-mirror.hostdime.com.br
Setting up Install Process
```

FIGURA 6.54 INSTALACIÓN DE MYSQL
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Una vez instalado mysql se procede a instalar php mediante:

yum install php-devel php-mysql php-gd



```
root@SERVERSAFA: /
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# yum install php-devel php-mysql php-gd
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
* Webmin: download.webmin.com
* base: centos-mirror.hostdime.com.br
* extras: centos-mirror.hostdime.com.br
* updates: centos-mirror.hostdime.com.br
Setting up Install Process
Package php-mysql-5.3.10-1.el6.x86_64 already installed and latest version
Package php-gd-5.3.10-1.el6.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
--> Package php-devel.x86_64 0:5.3.10-1.el6 will be installed
--> Processing Dependency: autoconf for package: php-devel-5.3.10-1.el6.x86_64
--> Processing Dependency: automake for package: php-devel-5.3.10-1.el6.x86_64
--> Running transaction check
--> Package autoconf.noarch 0:2.63-5.1.el6 will be installed
--> Package automake.noarch 0:1.11.1-1.2.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Installing:
php-devel x86_64 5.3.10-1.el6 AL-Server 529 k
Installing for dependencies:
autoconf noarch 2.63-5.1.el6 base 781 k
=====
```

FIGURA 6.55 INSTALACION DE PHP
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Luego de instalar php y mysql se reinician los servicios httpd y mysqld , además se establece que se inicie el servicio automáticamente al encender el servidor mediante :

service httpd restart
service mysqld restart

chkconfig httpd on
chkconfig mysqld on



```
root@SERVERSAFA:/  
Archivo Editar Ver Buscar Terminal Ayuda  
[root@SERVERSAFA /]# service httpd restart  
Parando httpd: [ OK ]  
Iniciando httpd: [ OK ]  
[root@SERVERSAFA /]# service mysqld restart  
Parando mysqld: [ OK ]  
Iniciando mysqld: [ OK ]  
[root@SERVERSAFA /]# chkconfig httpd on  
[root@SERVERSAFA /]# chkconfig mysqld on  
[root@SERVERSAFA /]# █
```

FIGURA 6.56 INICIO DE SERVICIOS PHP Y MYSQL
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Para comprobar que realmente funciona apache, se abre el navegador y se escribe en el navegador `http://192.168.2.1/` donde debe aparecer la página de prueba de apache

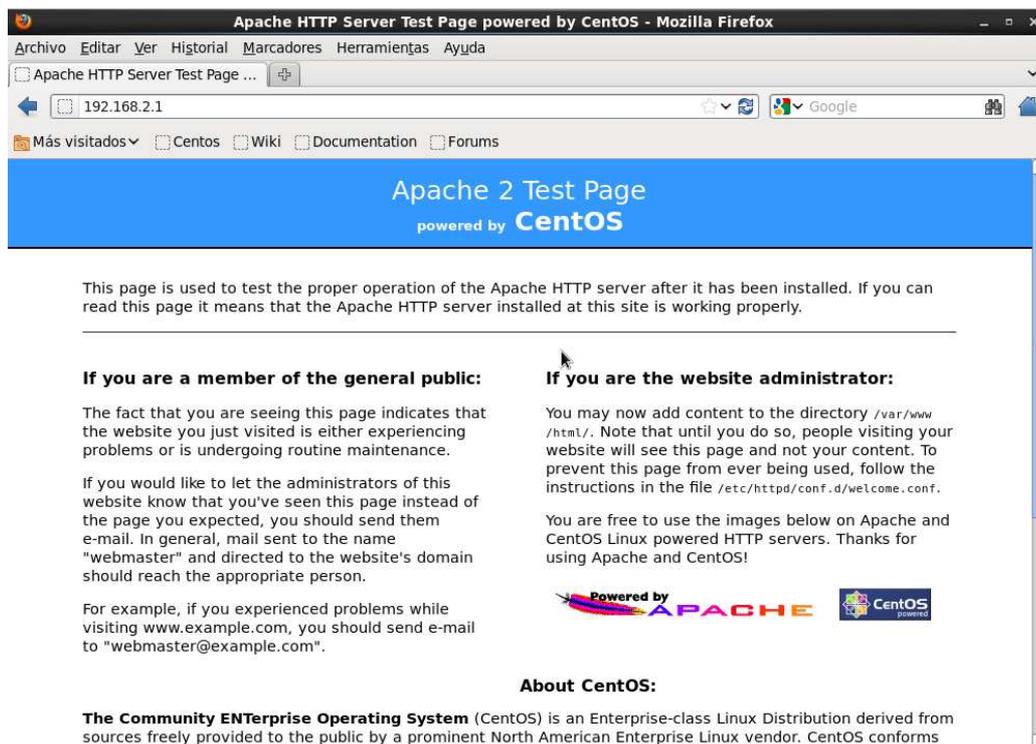
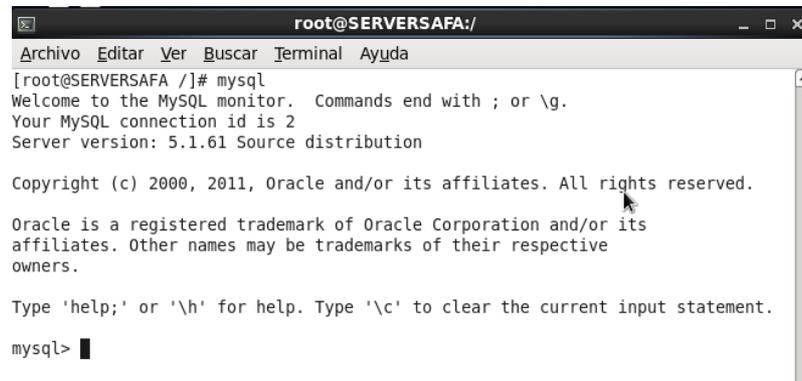


FIGURA 6.57 COMPROBACIÓN FUNCIONAMIENTO APACHE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Para comprobar que mysql funciona en un terminal se escribe **mysql** donde debe permitir ingresar comandos



```
root@SERVERSAFA:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.1.61 Source distribution

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

FIGURA 6.58 COMPROBACIÓN FUNCIONAMIENTO MYSQL
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

6.8.3.7.1 CONFIGURACIÓN DE MOODLE

El paso siguiente luego de comprobar que estén correctamente instalados y funcionando tanto php como mysql es descargar de la página de moodle la última versión estable del mismo en este caso es: Moodle 2.2.3

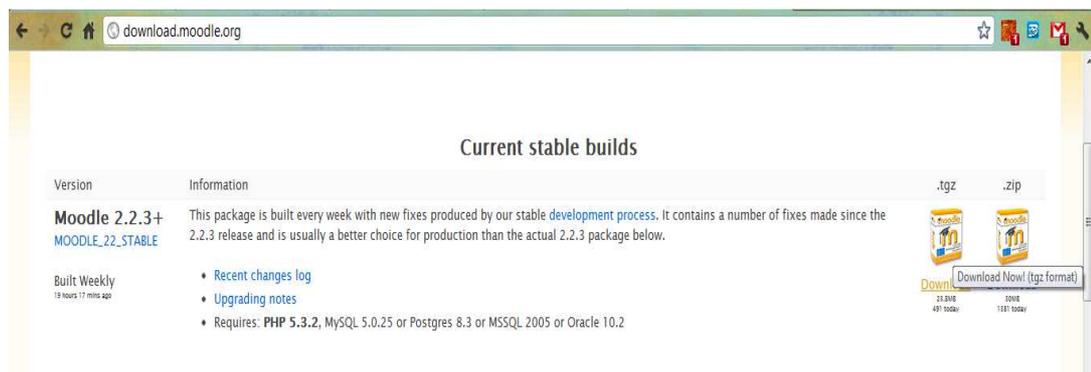
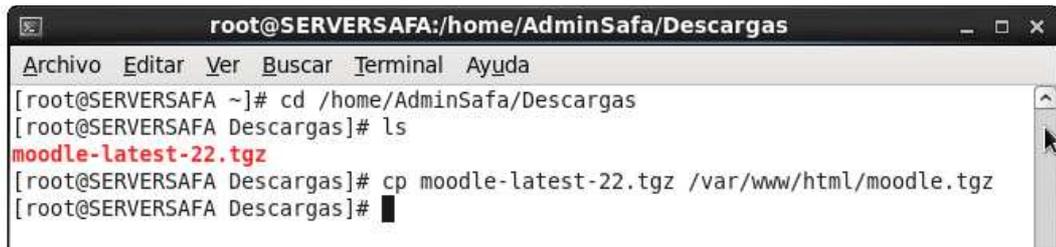


FIGURA 6.59 PAGINA DE DESCARGA MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Se descarga comprimido con .tgz, (en este caso se descargó en la ubicación /home/AdminSafa/Descargas, se lo traslada a la ubicación /var/www/html y posteriormente se lo descomprime)



```
root@SERVERSAFA:/home/AdminSafa/Descargas
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA ~]# cd /home/AdminSafa/Descargas
[root@SERVERSAFA Descargas]# ls
moodle-latest-22.tgz
[root@SERVERSAFA Descargas]# cp moodle-latest-22.tgz /var/www/html/moodle.tgz
[root@SERVERSAFA Descargas]#
```

FIGURA 6.60 MOVIENDO ARCHIVO DESCARGADO A DIRECCION WWW/HTML

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas



```
root@SERVERSAFA:/var/www/html
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA html]# ls
moodle moodledata moodle.tgz
[root@SERVERSAFA html]# tar xvzf moodle.tgz
```

FIGURA 6.61 DESCOMPRESIÓN DEL ARCHIVO MOODLE.TGZ

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Emisión de permisos de lectura y escritura mediante:

Chmod 755 moodle



```
root@SERVERSAFA:/var/www/html
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA html]# chmod 755 moodle
```

FIGURA 6.62 ASIGNACIÓN DE PERMISOS A LA CARPETA MOODLE

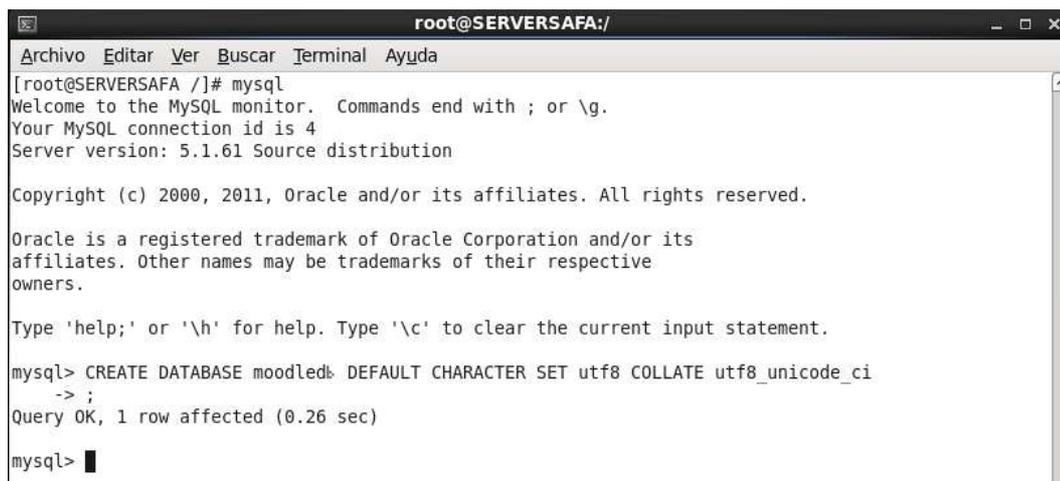
Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Para que Moodle funcione adecuadamente se requiere de una base de datos la cual fue creada y configurada desde la terminal ejecutando:

mysql

```
CREATE DATABASE moodledb DEFAULT CHARACTER SET utf8 COLLATE
utf8_unicode_ci;
```



```
root@SERVERSAFA:/  
Archivo Editar Ver Buscar Terminal Ayuda  
[root@SERVERSAFA /]# mysql  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 4  
Server version: 5.1.61 Source distribution  
  
Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> CREATE DATABASE moodledb DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci  
-> ;  
Query OK, 1 row affected (0.26 sec)  
  
mysql> █
```

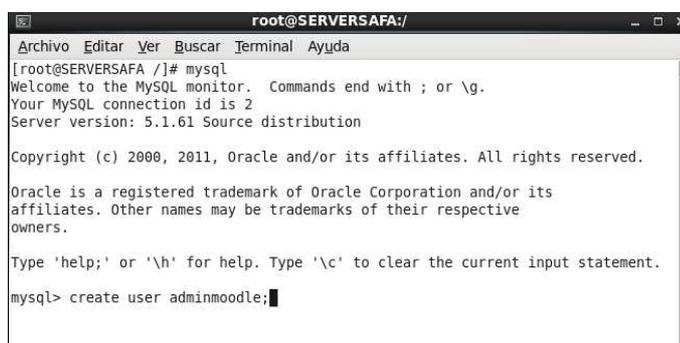
FIGURA 6.63 CREACIÓN DE LA BASE DE DATOS MOODLEDB

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Además se creó un usuario de base de datos con permisos de selección inserción actualización y eliminación

Create user adminmoodle:



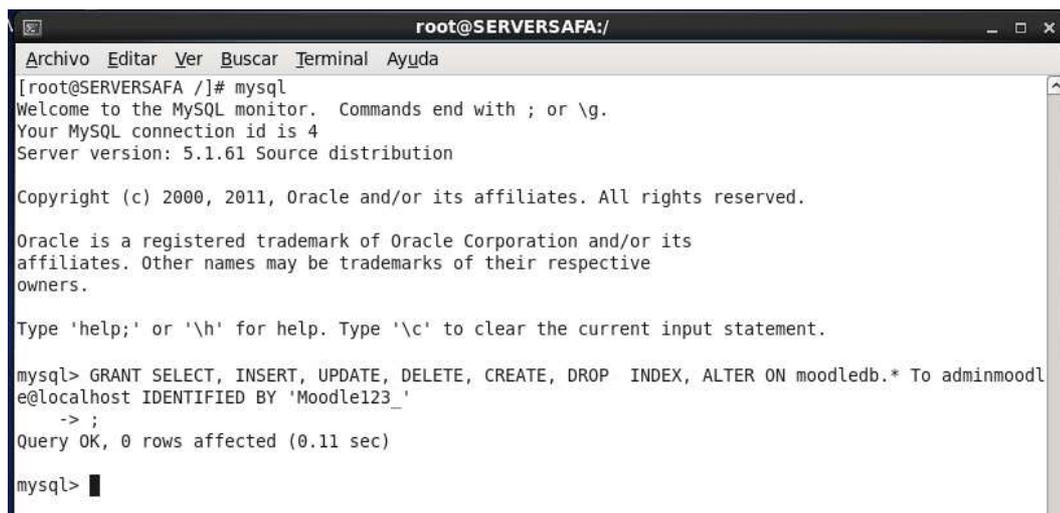
```
root@SERVERSAFA:/  
Archivo Editar Ver Buscar Terminal Ayuda  
[root@SERVERSAFA /]# mysql  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 2  
Server version: 5.1.61 Source distribution  
  
Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> create user adminmoodle; █
```

FIGURA 6.64 CREACIÓN DEL USUARIO ADMINMOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

**GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP,
INDEX,ALTER ON moodledb.* TO adminmoodle@localhost IDENTIFIED BY 'Moodle123_';**



```
root@SERVERSAFA:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.1.61 Source distribution

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP INDEX, ALTER ON moodledb.* To adminmoodle@localhost IDENTIFIED BY 'Moodle123_'
-> ;
Query OK, 0 rows affected (0.11 sec)

mysql> █
```

FIGURA 6.65 ASIGNACIÓN DE PERMISOS AL USUARIO ADMINMOODLE

Fuente. Escuela Sagrada Familia

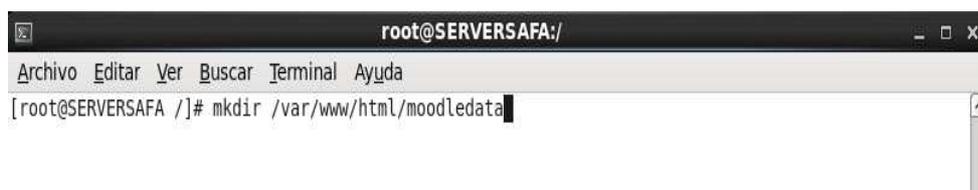
Elaborado por: Adriana Salinas

Este usuario y clave es el que se utilizará para poder acceder a moodle en las futuras conexiones como administrador.

Hasta este momento, se encuentra creada la carpeta moodle con permisos de root en /var/www/html/moodle/ y también creada la base de datos con un usuario y contraseña.

Adicional se requiere la creación de otra carpeta para que se guarden todos los datos de Moodle. Por defecto Moodle solicita que la carpeta se llame “moodledata”.

La carpeta debe de estar en la siguiente ruta: /var/www/html/



```
root@SERVERSAFA:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# mkdir /var/www/html/moodledata █
```

FIGURA 6.66 CREACIÓN DEL DIRECTORIO MOODLEDATA

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Finalmente se inició con la instalación de Moodle para lo cual se abrió un navegador y en la barra de direcciones se escribió: <http://www.safavirtual.edu.ec/moode> .

En la primera página solicita que se seleccione el lenguaje a utilizar a lo largo de la instalación, en donde fue seleccionado español

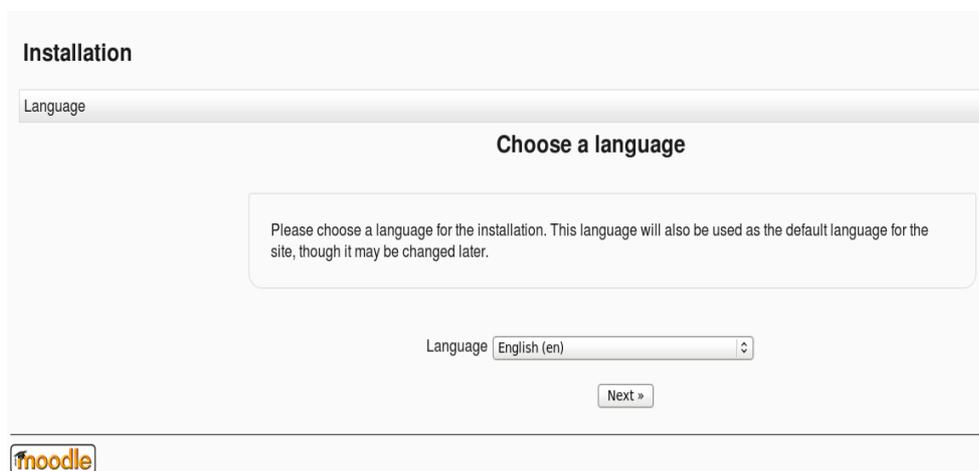


FIGURA 6.67 INSTALACIÓN MOODLE - SELECCIÓN DE IDIOMA

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

La siguiente pantalla solicita que se seleccione el controlador de la base de datos, en donde se seleccionó My SQL



FIGURA 6.68 INSTALACIÓN MOODLE – SELECCIÓN DE CONTROLADOR BDD

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Posteriormente solicita que se ingrese la información sobre el usuario de la base de datos que fue creado con anterioridad en este caso se indicó que la base de datos se llama moodledb y el usuario de la misma es adminmoodle con clave Moodle123_

Database settings

Improved MySQL (native/mysqli)

Now you need to configure the database where most Moodle data will be stored. Database may be created if database user has needed permissions, username and password must already exist. Table prefix is optional.

Database host

Database name

Database user

Database password

Tables prefix

Unix socket



FIGURA 6.69 INSTALACIÓN MOODLE – CONFIGURACIÓN DE BDD

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Al dar clic en el botón siguiente aparece la página que indica que la configuración está completa sin embargo no se puede crear el archivo config.php, por lo cual solicita su creación, indicando que se debe copiar y pegar dentro del archivo a config.php la información que indica en el mensaje

Installation

config.php

Configuration completed

Moodle made an attempt to save your configuration in a file in the root of your Moodle installation. The installer script was not able to automatically create a config.php file containing your chosen settings, probably because the Moodle directory is not writeable. You can manually copy the following code into a file named config.php within the root directory of Moodle.

```

<?php // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype      = 'mysql';
$CFG->dblibrary   = 'native';
$CFG->dbhost      = 'localhost';
$CFG->dbname      = 'moodledb';
$CFG->dbuser      = 'adminmoodle';
$CFG->dbpass      = 'Moodle123_';
$CFG->prefix      = 'mdl_';

```

Installation - Moodle 2.0.0

FIGURA 6.70 INSTALACIÓN MOODLE – INFORME DE CONFIGURACIÓN

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Para lo cual se procede a copiar los datos que devolvió en el mensaje y crear el archivo config.php en la ruta /var/www/html/moodle



```
root@SERVERSAFA:/var/www/html/moodle
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# cd var/www/html/moodle
[root@SERVERSAFA moodle]# vim config.php
[root@SERVERSAFA moodle]#
```

FIGURA 6.71 CREACIÓN DEL ARCHIVO CONFIG.PHP

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Dentro de este archivo fueron adheridos los datos copiados.



```
root@SERVERSAFA:/var/www/html/moodle
Archivo Editar Ver Buscar Terminal Ayuda
<?php // Moodle configuration file
unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype      = 'mysqli';
$CFG->dblibrary   = 'native';
$CFG->dbhost      = 'localhost';
$CFG->dbname      = 'moodledb';
$CFG->dbuser      = 'adminmoodle';
$CFG->dbpass      = 'Moodle123_';
$CFG->prefix      = 'mdl_';
$CFG->dboptions   = array (
    'dbpersist' => 0,
    'dbsocket'  => 0,
);

$CFG->wwwroot     = 'http://192.168.2.1/moodle';
$CFG->dataroot    = '/var/www/moodledata';
$CFG->admin       = 'admin';

$CFG->directorypermissions = 0777;

-- INSERTAR --
```

FIGURA 6.72 CONTENIDO DEL ARCHIVO CONFIG.PHP

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

El siguiente paso es aceptar las condiciones de uso de moodle

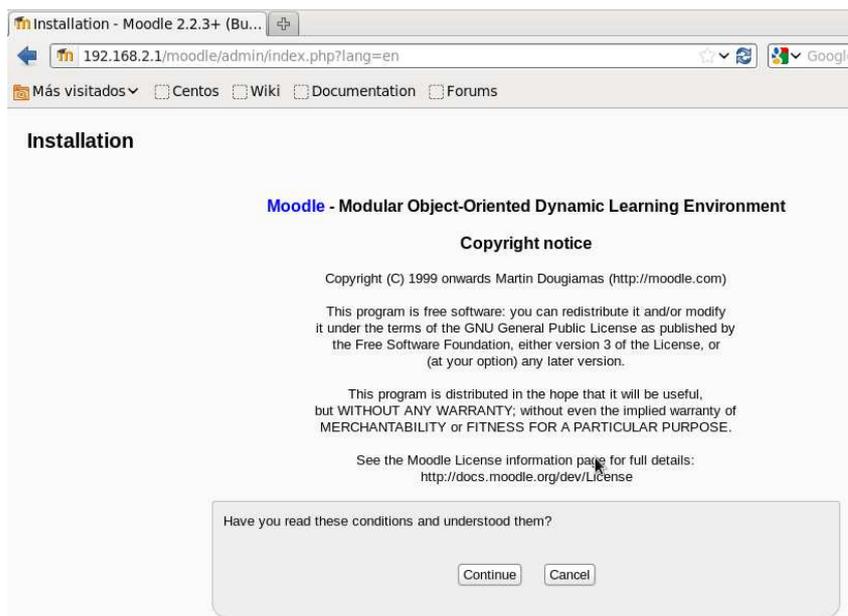


FIGURA 6.73 INSTALACIÓN MOODLE – TÉRMINOS Y CONDICIONES
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

AL no existir errores y estar listos todos los requisitos previos para la utilización de moodle aparece la siguiente pantalla.

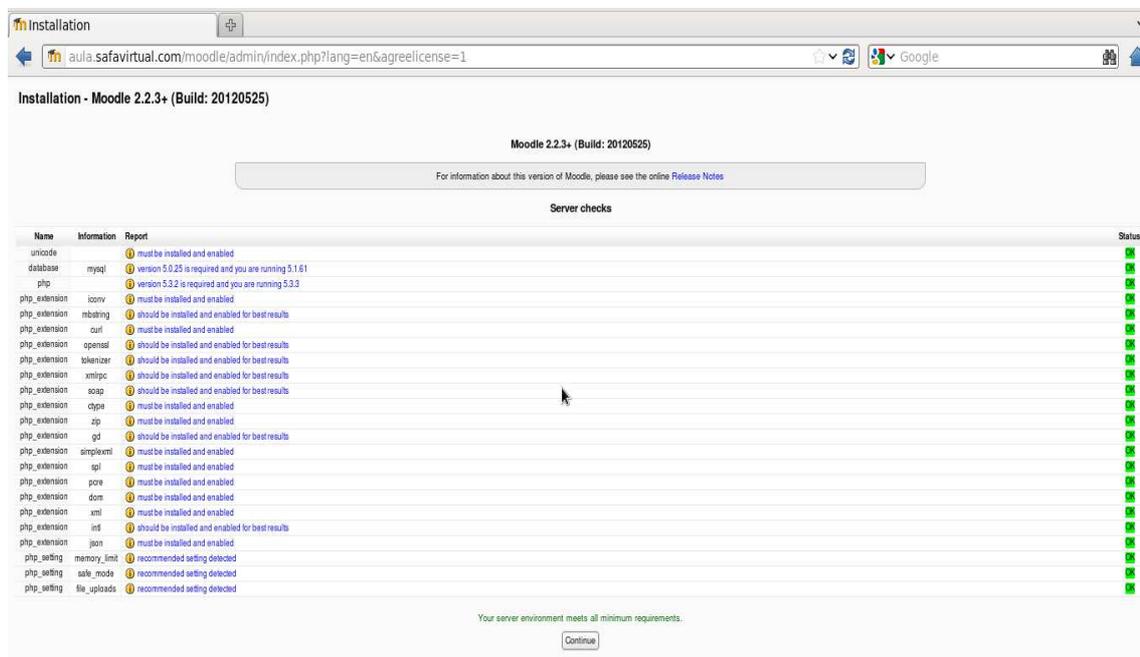


FIGURA 6.74 INSTALACIÓN MOODLE - INFORME DE REQUISITOS MÍNIMOS
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Al dar clic en continuar requirió volcar las tablas a la base de datos de nombre moodledb.

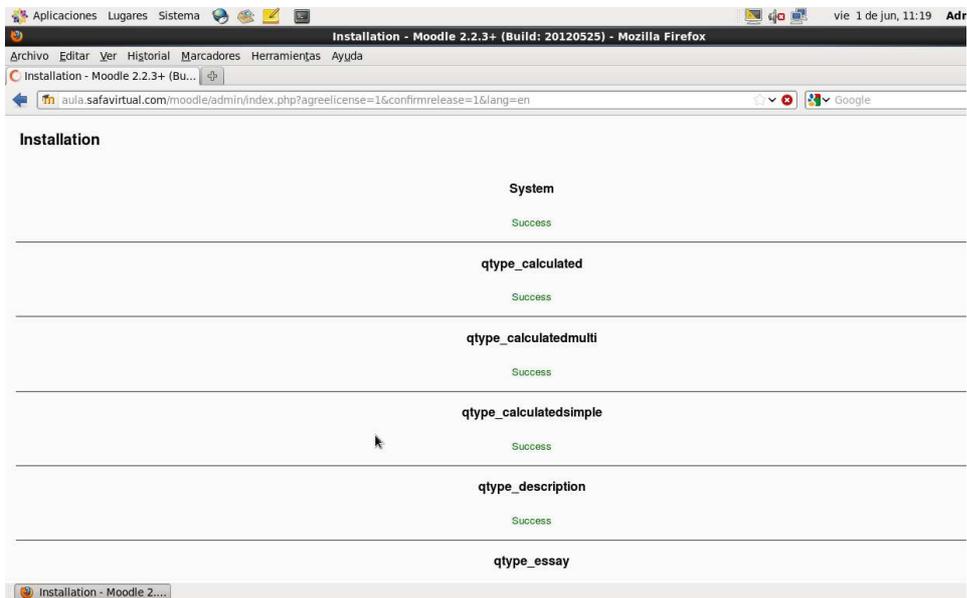


FIGURA 6.75 INSTALACIÓN MOODLE – INFORME DE INSTALACIÓN

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

Se procedió con la creación de la cuenta del usuario administrador, con este usuario será con el cual se podrán crear nuevos cursos y estudiantes.

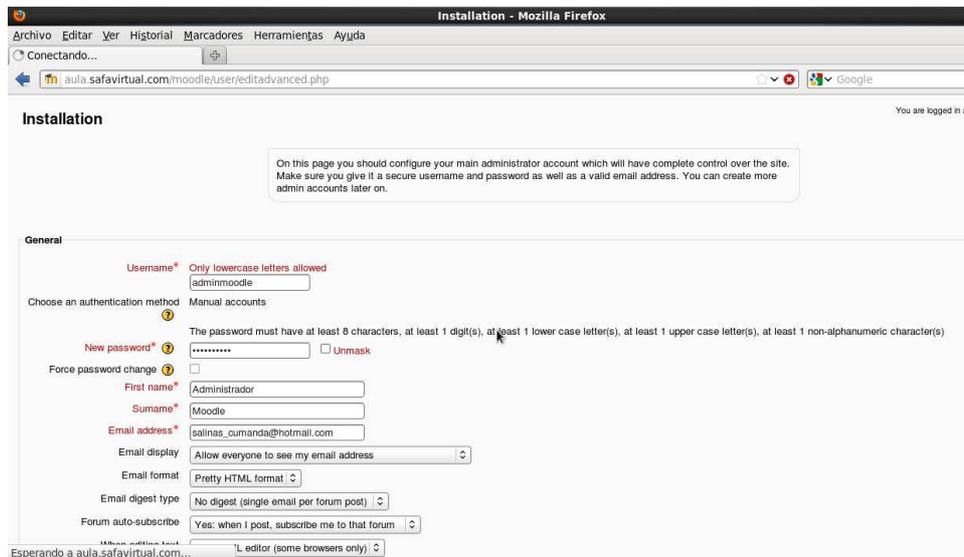


FIGURA 6.76 INSTALACIÓN MOODLE – CREACIÓN DEL USUARIO ADMINISTRADOR

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

6.8.3.7.2 AUTENTICACIÓN MOODLE CONTRA LDAP

Moodle como método eficaz para el control de estudiantes implementa un protocolo de comunicación y autenticación a través del servicio de directorios Ldap, lo cual facilita el manejo de los alumnos, puesto que usuarios de otros servicios pueden utilizar el mismo nombre de usuario y contraseña para ingresar a específicos cursos dictados dentro de la institución, para su configuración se siguieron los siguientes pasos:

Accesar a la plataforma como usuario administrador en este caso con usuario *adminmoodle*

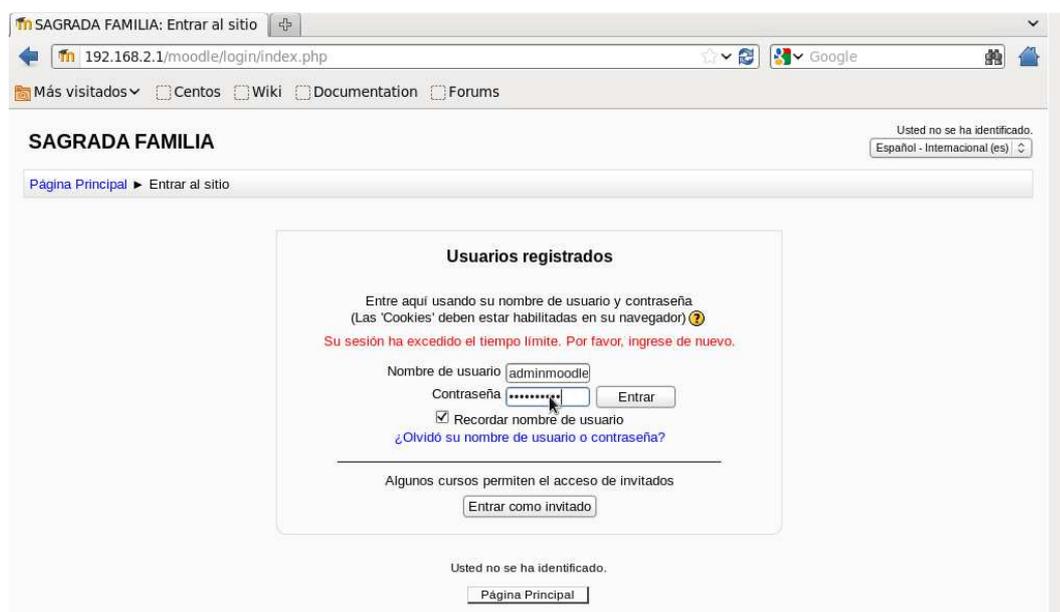


FIGURA 6.77 ACCESO A LA PLATAFORMA MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Posteriormente se necesita la ubicación del enlace Gestionar Identificación en parte lateral izquierda en el menú

- *Administración del Sitio*
 - *Extensiones*
 - *Identificación*
 - *Gestionar Identificación*

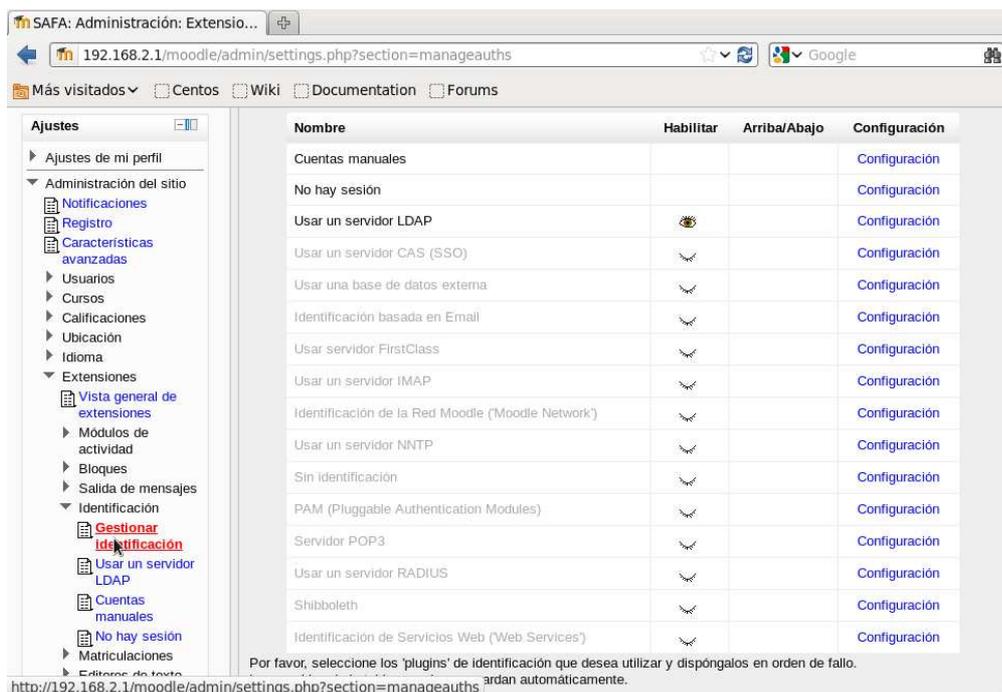


FIGURA 6.78 GESTIONAR IDENTIFICACION - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Gestionar identificación permitirá seleccionar la forma en que los alumnos del aula virtual se autenticaran o conectaran a el servidor Moodle, muestra la pantalla de selección de servicios en donde se selecciona “Usar un servidor ldap” el ojo que se muestra allí debe estar abierto.

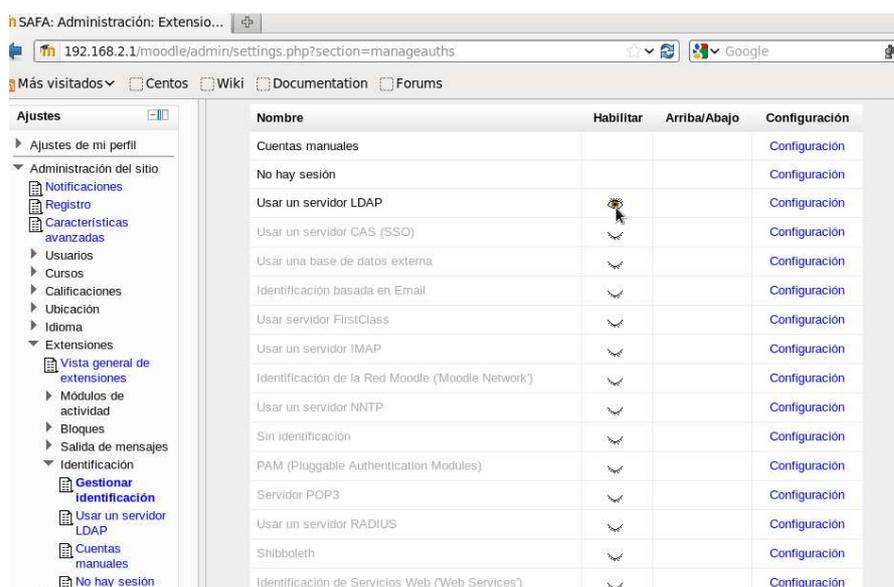


FIGURA 6.79 ACTIVACIÓN USO DE LDAP - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

De esa manera se activó la conexión mediante el servidor ldap. Para poder establecer su conexión se requiere abrir la página de configuración, la cual muestra y solicita la información referente al servidor ldap.

Usar un servidor LDAP

Este método proporciona identificación contra un servidor LDAP externo. Si el nombre de usuario y contraseña facilitados son válidos, Moodle crea una nueva entrada para el usuario en su base de datos. Este módulo puede leer atributos de usuario desde LDAP y prerellenar los campos requeridos en Moodle. Para las entradas sucesivas solo se comprueba el usuario y la contraseña.

Ajustes de servidor LDAP

URL del host	<input type="text" value="192.168.2.1"/>	Especificar el host LDAP en forma de URL como 'ldap://ldap.myorg.com/' o 'ldaps://ldap.myorg.com/'
Versión	<input type="text" value="3"/>	La versión del protocolo LDAP que su servidor está utilizando.
Codificación LDAP	<input type="text" value="utf-8"/>	Especifique la codificación usada por el servidor LDAP. Muy probablemente utf-8. MS AD v2 utiliza codificación de plataforma por defecto como cp1252, cp1250, etc.

Fijar ajustes

Ocultar contraseñas	<input type="text" value="Si"/>	Seleccione 'si' para evitar que las contraseñas se almacenen en la base de datos de Moodle.
Nombre distinguido	<input type="text" value="cn=Manager,dc=safa,dc=com"/>	Si quiere usar 'bind-user' para buscar usuarios, especifíquelo aquí. Algo como 'cn=ldapuser,ou=public,o=org'
Contraseña	<input type="password" value="*****"/>	Contraseña para bind-user.

Ajustes de búsqueda de usuario

Tipo de usuario	<input type="text" value="posixAccount (rfc2307)"/>	Seleccione cómo se almacenarán los usuarios en LDAP. Este ajuste también especifica cómo funcionarán la
-----------------	---	---

Contextos	<input type="text" value="ou=people,dc=safa,dc=com"/>	Lista de contextos donde están localizados los usuarios. Separe contextos diferentes con ','. Por ejemplo: 'ou=usuarios,o=org; ou=otros,o=org'
Buscar subcontextos	<input type="text" value="Si"/>	Ponga el valor <> 0 si quiere buscar usuarios desde subcontextos.
Dereferenciar los alias	<input type="text" value="No"/>	Determina cómo se manejan los alias durante la búsqueda. Seleccione uno de los siguientes valores: "No" (LDAP_DEREF_NEVER) o "Si" (LDAP_DEREF_ALWAYS)
Atributo de usuario	<input type="text" value="uid"/>	El atributo usado para nombrar/buscar usuarios. Normalmente 'cn'.
Atributo de miembro	<input type="text" value="member"/>	Especificar el atributo para nombre de usuario, cuando los usuarios se integran en un grupo. Normalmente 'miembro'
Atributos de miembro utilizan dn	<input type="text"/>	Opcional: Anula el manejo de valores de atributos de los miembros, es 0 ó 1
Clase de objetos	<input type="text" value="posixAccount"/>	Filtro usado para usuarios name/search. Normalmente deberá ajustarlo a algo parecido a objectClass=posixAccount. Valores por defecto para objectClass=* que devolverán todos los objetos desde LDAP.

Forzar cambio de contraseña

Forzar cambio de contraseña	<input type="text" value="No"/>	Forzar a los usuarios a cambiar la contraseña la primera vez que accedan a Moodle.
-----------------------------	---------------------------------	--

<p>Utilizar Página de cambio de contraseña estándar <input type="button" value="No"/></p> <p>Formato de contraseña <input type="button" value="Texto plano"/></p> <p>URL para cambio de contraseña <input type="text"/></p> <p>Ajustes de caducidad de la contraseña LDAP.</p> <p>Expiración <input type="button" value="no"/></p> <p>Advertencia de expiración <input type="text" value="10"/></p> <p>Atributo de expiración <input type="text"/></p> <p>Entradas libres <input type="button" value="No"/></p>	<p>Si el sistema de identificación externa permite cambios de contraseña en Moodle, seleccione Sí. Este ajuste pasa por alto 'Cambiar contraseña URL'.</p> <p>NOTA: Se recomienda que utilice LDAP sobre un túnel encriptado SSL (ldaps://) si el servidor LDAP es remoto.</p> <p>Especifique el formato de las contraseñas nuevas o cambiadas en el servidor LDAP</p> <p>Aquí puede especificar dónde pueden sus usuarios recuperar o cambiar su nombre de usuario/contraseña si lo han olvidado. Para ello, aparecerá un botón en la página de entrada. Si deja esto en blanco, este botón no se mostrará.</p> <p>Seleccione No para deshabilitar comprobar si la contraseña ha caducado, o LDAP para leer el tiempo de caducidad de la contraseña directamente de LDAP.</p> <p>Número de días antes de que aparezca la advertencia de caducidad de la contraseña.</p> <p>Opcional: anula el atributo ldap que almacena el tiempo de caducidad de la contraseña PasswordExpirationTime</p> <p>Activar el soporte de entrada libre LDAP. Una vez que la contraseña ha caducado, el usuario puede entrar hasta que la cuenta de acceso libre llega a cero. Si se activa esta opción se mostrará un mensaje de acceso libre en el caso de que la contraseña haya caducado.</p>
--	---

<p>Atributo de entrada libre <input type="text"/></p> <p>Habilitar creación por parte del usuario</p> <p>Crear usuarios externamente <input type="button" value="Sí"/></p> <p>Contexto para nuevos usuarios <input type="text"/></p> <p>Creador de curso</p> <p>Creadores <input type="text"/></p> <p>Script de sincronización del Cron</p> <p>Usuario externo eliminado <input type="button" value="Mantener interna"/></p> <p>NTLM SSO</p> <p>Habilitar <input type="button" value="No"/></p>	<p>Opcional: Anula el atributo gracelogin</p> <p>Los nuevos usuarios (anónimos) pueden crear cuentas de usuario sobre el código externo de identificación y confirmar vía correo electrónico. Si usted habilita esto, recuerde también configurar las opciones del módulo específico para la creación de usuario.</p> <p>Si habilita la creación de usuario con confirmación por medio de correo electrónico, especifique el contexto en el que se crean los usuarios. Este contexto debe ser diferente de otros usuarios para prevenir problemas de seguridad. No es necesario añadir este contexto a ldap_context-variable, Moodle buscará automáticamente los usuarios de este contexto.</p> <p>Lista de grupos cuyos miembros están autorizados para crear nuevos cursos. Pueden separarse varios grupos con ";". Normalmente así: 'cn=teachers,ou=staff,o=myorg'</p> <p>Especifique qué hacer con una cuenta de usuario interna durante sincronización masiva cuando el usuario fue eliminado de la fuente externa. Únicamente los usuarios suspendidos son automáticamente revividos si ellos reaparecen en una fuente externa.</p> <p>Seleccione Sí para intentar Single Sign On con el dominio NTLM. Nota: esto requiere un ajuste adicional en el</p>
---	---

<p>Sub-red <input type="text"/></p> <p>¿Ruta rápida MS IE? <input type="button" value="No"/></p> <p>Tipo de identificación <input type="button" value="NTLM"/></p> <p>Mapeado de datos</p> <p>Nombre <input type="text"/></p> <p style="text-align: right;">Actualizar datos locales <input type="button" value="Al crearse"/></p> <p>Actualizar datos externos <input type="button" value="Nunca"/></p> <p style="text-align: right;">Bloquear valor <input type="button" value="Desbloqueado"/></p> <p>Apellido <input type="text"/></p> <p style="text-align: right;">Actualizar datos locales <input type="button" value="Al crearse"/></p> <p>Actualizar datos externos <input type="button" value="Nunca"/></p> <p style="text-align: right;">Bloquear valor <input type="button" value="Desbloqueado"/></p>	<p>Si se selecciona, sólo intentará el SSO con clientes de esta sub-red. Formato: xxx.xxx.xxx.xxx/bitmask. Separe varias sub-redes con "," (coma).</p> <p>Establezca en "Sí" para habilitar la ruta NTLM SSO rápida (se salta algunos pasos y solo trabaja si el explorador es MS Internet Explorer).</p> <p>El método de autenticación configurado en el servidor Web para autenticar a los usuarios (en caso de duda, elija NTLM)</p> <p>Estos campos son opcionales. Usted puede elegir pre-rellenar algunos campos de usuario en Moodle con información de los campos LDAP que especifique aquí. Si deja estos campos en blanco, entonces no se transferirá nada desde LDAP y se usará el sistema predeterminado en Moodle.</p> <p>En ambos casos, los usuarios podrán editar todos estos campos después de entrar.</p> <p>Actualizar datos locales: Si está activado, el campo debe ser actualizado (con identificación externa) cada vez que el usuario entra o se produce una sincronización de usuarios. Los campos a actualizar localmente deberían ser bloqueados.</p> <p>Bloquear valor: Si se activa, los usuarios y administradores de Moodle no podrán editar directamente</p>
---	---

Dirección de correo

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

Ciudad

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

País

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

Idioma

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

administradores de Moodle no podrán editar directamente el campo. Utilice esta opción si mantiene estos datos en el sistema de identificación externo.

Actualizar datos externos: Si está activado, la identificación externa será actualizada cuando se actualice el registro del usuario. Los campos deberían estar desbloqueados para poder editarlos.

Note: La actualización de datos LDAP externos requiere que usted ajuste los valores 'binddn' y 'bindpw' a un usuario con privilegios de edición de todos los registros de usuario. Por el momento, esto no preserva los atributos multi-valor, y eliminará los valores extra durante la actualización.

Página web

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

Número de ID

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

Institución

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

Departamento

Actualizar datos locales ↕

Teléfono 1

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

Teléfono 2

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

Dirección

Actualizar datos locales ↕

Actualizar datos externos ↕

Bloquear valor ↕

FIGURA 6.80 CONFIGURACIÓN DE LDAP - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Campo	Información	Valor de Configuración
<u>Url del host</u>	Dirección ip del servidor donde se encuentran alojadas las bases de datos de ldap	192.168.2.1
<u>Version</u>	Version del protocolo Ldap utilizado	3
<u>Nombre distinguido</u>	Nombre con el que se conectara al servidor ldap y realizar las consultas referentes a usuarios	cn=Manager,dc=safa,dc=com
<u>Atributo de usuario</u>	Permite nombrar y buscar a los usuarios en el árbol LDAP.	uid
<u>Atributo de miembro</u>	Utilizado para listar todos los miembros de un grupo.	member
<u>Clase de objetos</u>	El tipo de objeto LDAP utilizado para buscar usuarios.	posixAccount

TABLA 6.9 DATOS LDAP - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

El siguiente paso y uno de los más importantes fue desactivar la ratificación de cuentas vía email, con el objetivo de que los estudiantes no tengan que confirmar sus cuentas en la plataforma mediante correo electrónico y de esta manera ahorrar tiempo.

Para lo cual se requiere acceder al menú:

- *Administración del Sitio*
 - *Seguridad*
 - *Políticas del Sitio*



FIGURA 6.81 PANEL DE ADMINISTRACIÓN DEL SITIO - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Dentro de la página de políticas del sitio se requiere quitar la selección del combo que indica la aceptación la confirmación de cuentas mediante e-mail

Desactivar imágenes en el perfil del usuario <small>disableuserimages</small>	<input type="checkbox"/> Valor por defecto: No	Desactiva la posibilidad de que los usuarios cambien las imágenes de sus perfiles.
Confirmación de cambio de email <small>emailchangeconfirmation</small>	<input type="checkbox"/> Valor por defecto: Si	Cuando los usuarios cambien su dirección de correo electrónico en sus perfiles de usuario, se requerirá confirmación del correo electrónico.
Recordar nombre de usuario <small>rememberusername</small>	<input type="text" value="opcional"/> Valor por defecto: opcional	Activar si desea almacenar las cookies permanentes con nombres de usuario durante el inicio de sesión. Las cookies permanentes se deben tratar como un asunto de privacidad si se utilizan sin consentimiento.
Validación estricta de campos obligatorios <small>strictformrequired</small>	<input type="checkbox"/> Valor por defecto: No	Si está activado, se impide a los usuarios introducir un espacio en blanco o un salto de línea en los campos obligatorios de los formularios.

FIGURA 6.82 CONFIRMACIÓN POR EMAIL - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

6.8.3.7.3 PERSONALIZACIÓN- MOODLE

➤ CREACIÓN DEL CURSO

Se Implementó un curso de valores humanos orientado hacia los niños de entre 8 a 10 años de la institución, para lo cual se hizo uso de la paleta derecha de moodle.

Administración del sitio – Cursos – Agregar Editar Cursos



FIGURA 6.83 AGREGAR EDITAR CURSOS - MOODLE

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

A continuación se seleccionó nuevo curso el cual dio a lugar la página de edición donde se personalizó con información relevante, en el formato del curso se seleccionó “Temas” lo cual indica que el curso estará basara en el número de temas a tratar en este caso se asignaron 3 temas.

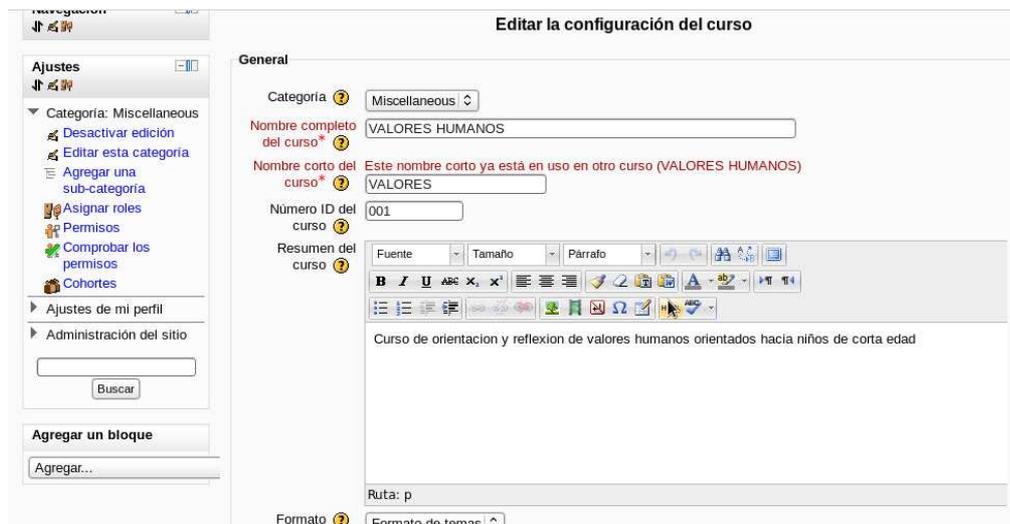


FIGURA 6.84 EDICIÓN CONFIGURACIÓN DEL CURSO - MOODLE

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

➤ EXPOSICIÓN DE ETIQUETAS

Las etiquetas permiten añadir texto HTML y pequeños gráficos en los bloques de contenido, Este texto sirve para identificar las partes del curso y dar una estructura lógica a la página

Para agregar una etiqueta a el curso se selecciona el combo box que titula “agregar recurso” a continuación se selecciona etiqueta.

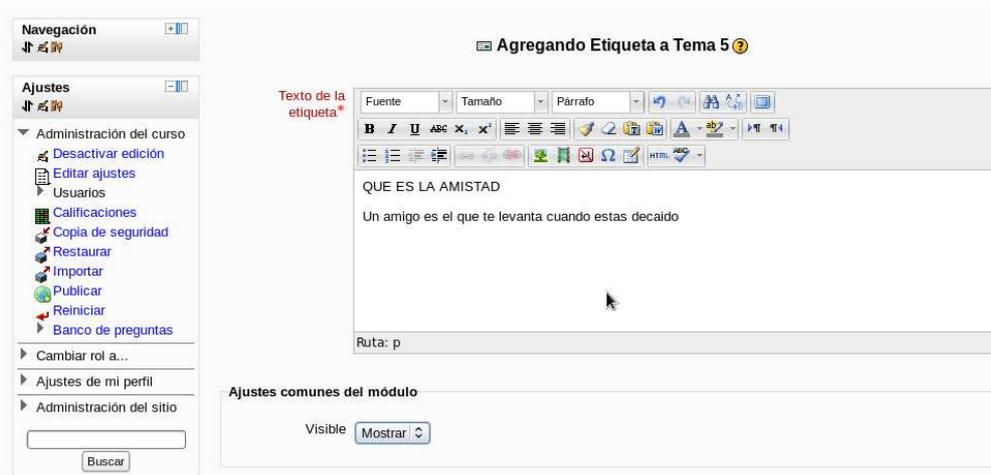


FIGURA 6.85 ETIQUETAS - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

➤ UTILIZACIÓN DE RECURSOS

Un recurso es un objeto que un profesor puede usar para asistir el aprendizaje.

Para el tema uno, se hizo uso de recursos como los archivos de texto, se subió un documento con un texto educativo referente al contenido a tratar.

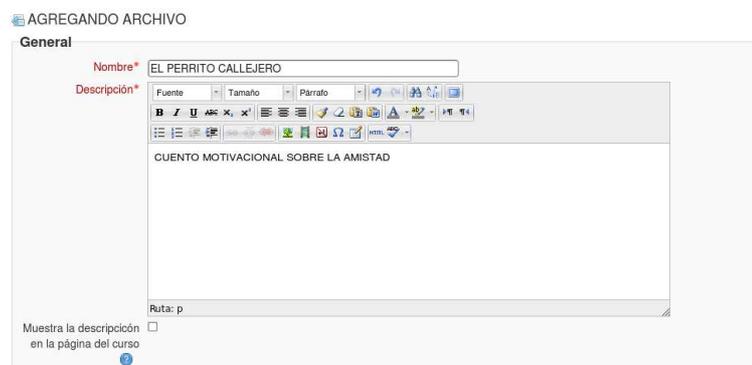


FIGURA 6.86 ARCHIVOS - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

➤ UTILIZACIÓN DE ACTIVIDADES

El bloque de Actividades lista todas las categorías de actividades disponibles en el curso (foros, consultas, tareas, etc.).

Para el desarrollo de este curso se utilizó un foro el cual fue agregado seleccionándolo desde el combobox de actividades.

The screenshot shows the 'Agregarando Foro' (Adding Forum) form in Moodle. The form is titled 'General' and includes the following fields and options:

- Nombre del foro***: Discussion Importancia de la Amistad
- Tipo de foro**: Foro para uso general
- Introducción***: A rich text editor with a toolbar and the text: "Es necesaria la amistad para las personas? por que?"
- Ruta:** p
- Muestra la descripción en la página del curso**:
- Modalidad de suscripción**: Suscripción opcional
- ¿Leer rastro de**: Opcional

FIGURA 6.87 FORO - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

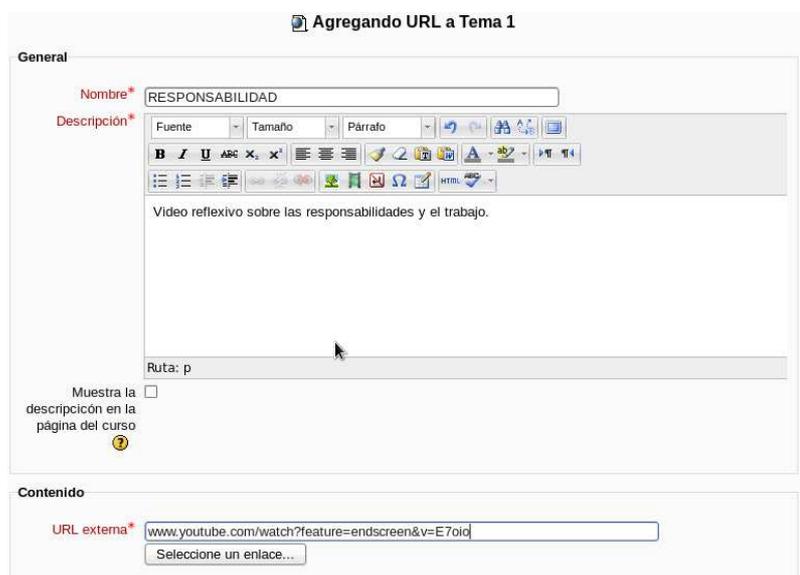
Adicionalmente se utilizó la herramienta tarea mediante al cual se solicita que suban un archivo de texto a la plataforma la cual será calificada.

The screenshot shows the 'Agregarando Tarea' (Adding Task) form in Moodle. The form includes the following fields and options:

- Nombre de la tarea**: ANECDOTA
- Descripción***: A rich text editor with a toolbar and the text: "Subir una historia o anecdotas personal que refleje la importancia de tener amigos y ser amable con los de"
- Ruta:** p
- Muestra la descripción en la página del curso**:
- Disponible desde**: 12 junio 2012 00:55 Habilitar
- Fecha de entrega**: 19 junio 2012 00:55 Habilitar
- Impedir envíos retrasados**: No
- Calificación**: 20

FIGURA 6.88 TAREA - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

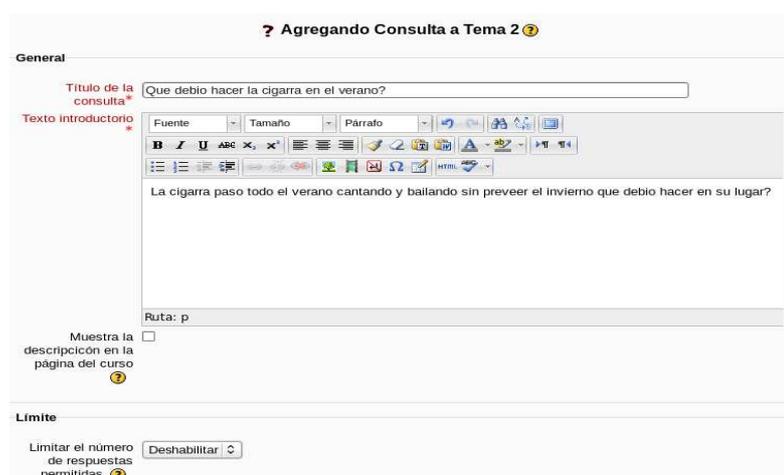
También se puede utilizar la inserción de enlaces hacia ciertos sitios web o videos alojados en el internet.



The screenshot shows the Moodle interface for adding a URL to a topic. The title is "Agregar URL a Tema 1". Under the "General" section, the "Nombre*" field contains "RESPONSABILIDAD". The "Descripción*" field has a rich text editor with the text "Video reflexivo sobre las responsabilidades y el trabajo." and a "Ruta: p" field below it. There is a checkbox for "Muestra la descripción en la página del curso" which is unchecked. The "Contenido" section has a "URL externa*" field containing "www.youtube.com/watch?feature=endscreen&v=E7oid" and a "Seleccione un enlace..." button.

FIGURA 6.89 URL - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

La consulta es una actividad muy sencilla, consistente en una pregunta y una serie de respuestas entre las cuales deben elegir los alumnos, muy útil para realizar encuestas rápidas para estimular la reflexión sobre un asunto, para permitir que el grupo decida sobre cualquier tema, o para recabar el consentimiento para realizar una investigación.



The screenshot shows the Moodle interface for adding a quiz question. The title is "Agregar Consulta a Tema 2". Under the "General" section, the "Titulo de la consulta*" field contains "Que debio hacer la cigarra en el verano?". The "Texto introductorio*" field has a rich text editor with the text "La cigarra paso todo el verano cantando y bailando sin preveer el invierno que debio hacer en su lugar?" and a "Ruta: p" field below it. There is a checkbox for "Muestra la descripción en la página del curso" which is unchecked. The "Limite" section has a "Limitar el número de respuestas permitidas" field set to "Deshabilitar".

FIGURA 6.90 CONSULTA - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

La tarea texto en línea ayudara a que los alumnos reflexionen sobre un tema en mayor profundidad y a nivel personal, y crear un canal más de comunicación entre el profesor y sus alumnos.

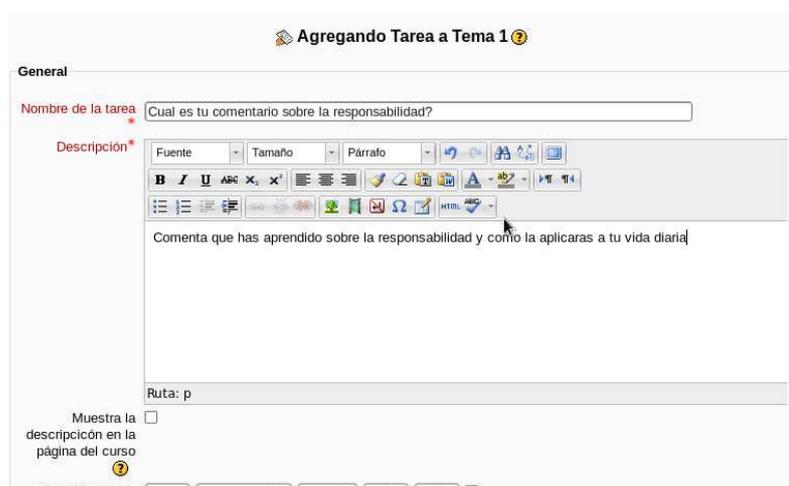


FIGURA 6.91 TAREA - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Los cuestionarios permiten diseñar y aplicar cuestionarios.

Existe una amplia variedad de Tipos de preguntas (opción múltiple, verdadero/falso, respuestas cortas,...). Las preguntas se organizan por categorías en un Banco de Preguntas y pueden utilizarse en el mismo curso o en otros cursos.

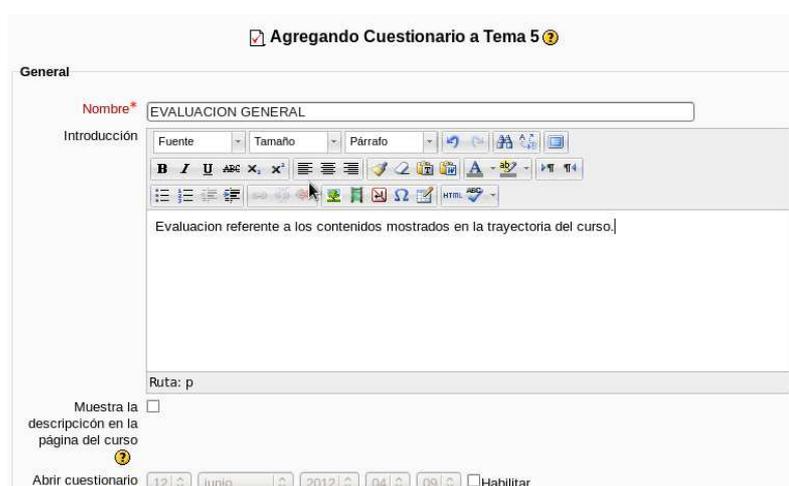


FIGURA 6.92 CUESTIONARIO - MOODLE
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Posteriormente proporciona la opción de ingresar las preguntas convenientes para el cuestionario.

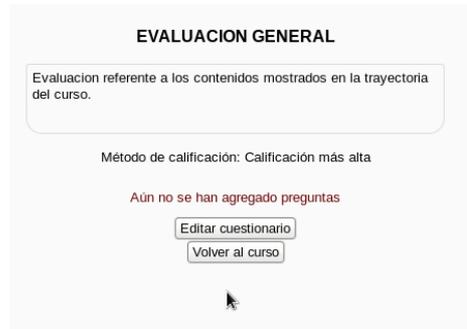


FIGURA 6.93 AGREGAR PREGUNTAS A CUESTIONARIO - MOODLE

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

Permitiendo escoger de varios tipos de preguntas

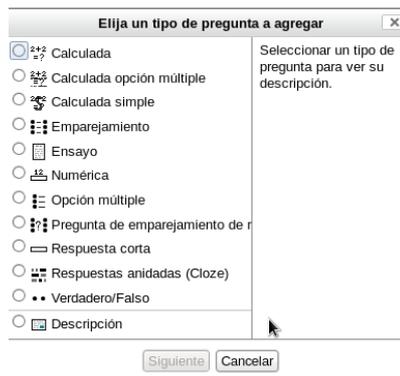


FIGURA 6.94 TIPOS DE PREGUNTAS CUESTIONARIO - MOODLE

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

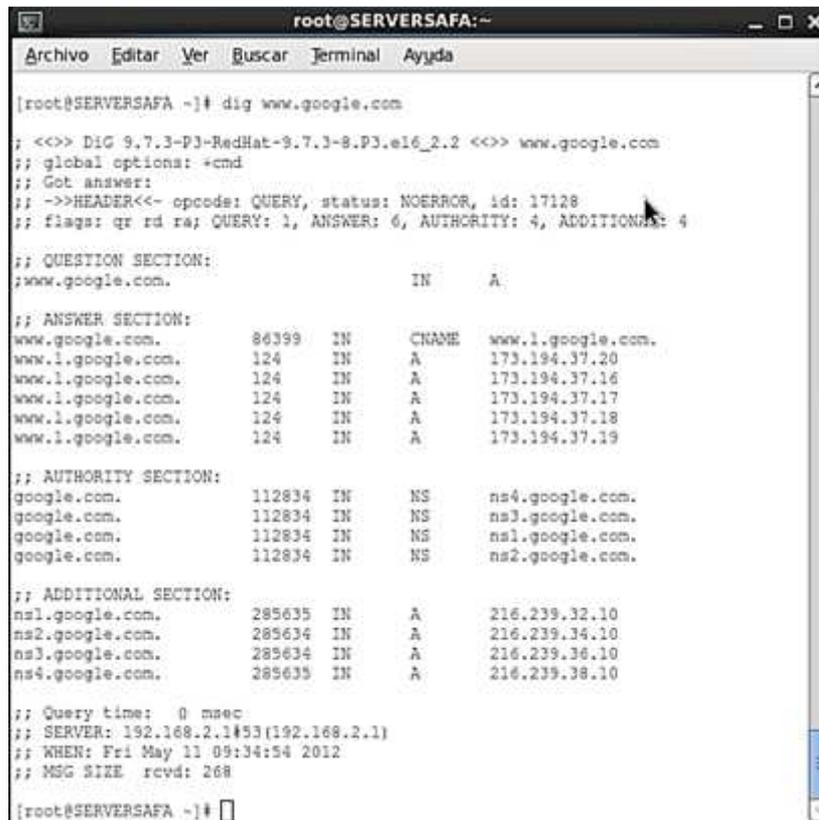
6.8.4 PRUEBAS DE FUNCIONAMIENTO

6.8.4.1 COMPROBACIÓN – BIND

Para comprobar que nuestro servidor dns bind esté funcionando correctamente tanto como servidor de cacheo como también resolviendo las direcciones locales dentro de la

institución se utilizó del comando dig y esperando obtener respuesta desde la dirección 192.168.2.1 en donde está alojado el servicio de nombres de dominio.

`dig www.google.com`



```
[root@SERVERSAFA ~]# dig www.google.com

;<<> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.e16_2.2 <<> www.google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 17128
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;www.google.com.                IN      A

;; ANSWER SECTION:
www.google.com.                86399  IN      CNAME   www.l.google.com.
www.l.google.com.             124    IN      A       173.194.37.20
www.l.google.com.             124    IN      A       173.194.37.16
www.l.google.com.             124    IN      A       173.194.37.17
www.l.google.com.             124    IN      A       173.194.37.18
www.l.google.com.             124    IN      A       173.194.37.19

;; AUTHORITY SECTION:
google.com.                    112834 IN      NS      ns4.google.com.
google.com.                    112834 IN      NS      ns3.google.com.
google.com.                    112834 IN      NS      ns1.google.com.
google.com.                    112834 IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.                285635 IN      A       216.239.32.10
ns2.google.com.                285634 IN      A       216.239.34.10
ns3.google.com.                285634 IN      A       216.239.36.10
ns4.google.com.                285635 IN      A       216.239.38.10

;; Query time: 0 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Fri May 11 09:34:54 2012
;; MSG SIZE rcvd: 268

[root@SERVERSAFA ~]#
```

FIGURA 6.95 COMPROBACION DIG - DNS

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

La imagen indica que el servidor dns devuelve como ip de google la ip 74.194.37.20 en un tiempo de consulta de 0 milisegundos, con lo que se comprueba que el servidor dns de cacheo funciona correctamente

Para comprobar que resuelva la dirección ip local www.safavirtual.edu.ec con la cual está alojada en nuestro propio servidor se utilizó el comando

`nslookup www.safavirtual.edu.ec`

```
root@SERVERSAFA:/
Archivo Editar Ver Buscar Terminal Ayuda
[root@SERVERSAFA /]# nslookup www.safavirtual.edu.ec
Server:      192.168.2.1
Address:     192.168.2.1#53

www.safavirtual.edu.ec canonical name = ns.safavirtual.edu.ec.
Name:   ns.safavirtual.edu.ec
Address: 192.168.2.1

[root@SERVERSAFA /]#
```

FIGURA 6.96 COMPROBACIÓN NSLOOKUP - DNS

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

La consulta devuelve que el nombre de dominio www.safavirtual.edu.ec está ubicado en la dirección 192.168.2.1 lo cual es correcto.

En el navegador del host “Safa 12”, se escribió www.safavirtual.edu.ec, seguidamente apareció la pantalla de bienvenida, demostrándose que efectivamente funciona el direccionamiento hacia la ip 192.168.2.1 en los equipos clientes.



FIGURA 6.97 COMPROBACIÓN DOMINIOS - DNS

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Al digitar en la barra de direcciones www.safavirtual.edu.ec/moodle, traslada al cliente hacia el aula virtual creada mediante moodle y alojada en el servidor.



FIGURA 6.98 COMPROBACIÓN DOMINIO MOODLE - DNS

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Con esto se ha comprobado que el servidor de domino DNS-BIND está activo y funcionando.

6.8.4.2 COMPROBACIÓN – OPENLDAP

Para comprobar que el servidor de directorios funciona se hizo uso de una herramienta de configuración de sistemas accesible vía web, **Webmin**, la misma que fué instalada anteriormente en el servidor, y se procedió a ingresar los estudiantes correspondientes al quinto año rojo con usuario y contraseña siguientes:

NOMBRE	USUARIO	CONTRASEÑA
ALULEMA ORTIZ ESTEFANO JAVIER	EAlulema1	xxxxx
ARROYO VASQUEZ ALEJANDRO SEBASTIAN	AArroyo2	xxxxx
CARRILLO NUÑEZ JUAN FERNANDO	JCarrillo3	xxxxx
CASTILLO JACOME JOSEPH ALEJANDRO	JCastillo4	xxxxx
HINOJOSA OÑATE DANNA PAOLA	DHinojosa5	xxxxx
JURADO MARCILLO ADRIAN ELIAS	AJurado6	xxxxx
MAZAQUIZA SANCHEZ ABRAHAN JOEL	AMazaquiza7	xxxxx
MERA RODRIGUEZ JUAN SEBASTIAN	JMera8	xxxxx
MOLINA RAMOS URIEL DAVID	UMolina9	xxxxx
MORA VILLACIS MARIA SOL	MMora10	xxxxx
ORTIZ VILLACIS DANIEL LEONARDO	DOrtiz11	xxxxx
PAZ JIMENEZ JUAN ESTEBAN	JPaz12	xxxxx
PAZMIÑO CAMPOVERDE DOMENICA AYN0HA	DPazmiño13	xxxxx
PEREZ TIRADO DOMENICA PATRICIA	DPerez14	xxxxx
SALAS BONILLA NICOLE ESTEFANIA	NSalas15	xxxxx
SOLIS IÑIGUEZ LORENA ELIZABETH	LSolis16	xxxxx
VACA SANCHEZ ANTONIO SEBASTIAN	AVaca17	xxxxx
VERA COCHA REINA ESTEFANIA	RVera18	xxxxx
VILLACIS PORTERO CHRISTOPHER JAIR	CVillacis19	xxxxx
ZURITA GOMEZ ANGELES NAYELI	AZurita20	xxxxx

TABLA 6.10 ESTUDIANTES QUINTO AÑO ROJO
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

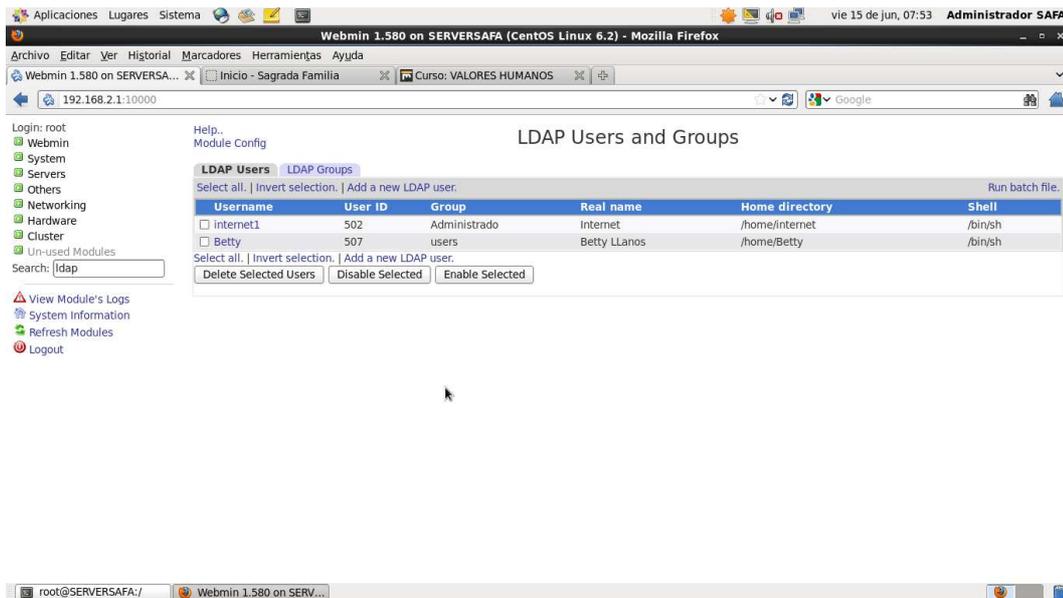


FIGURA 6.99 PÁGINA INICIAL WEBMIN
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

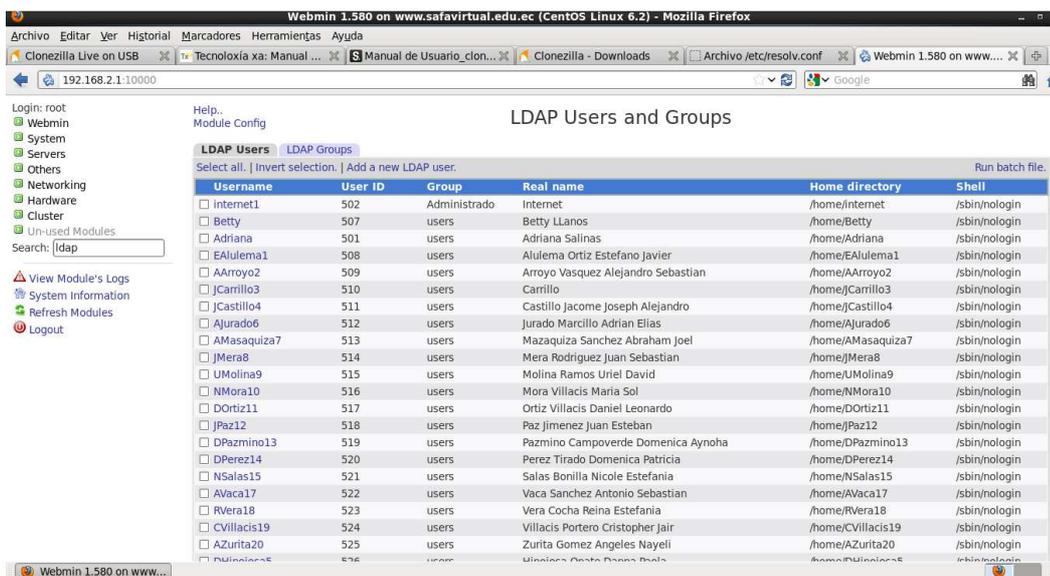


FIGURA 6.100 USUARIOS CREADOS WEBMIN
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Tras ingresar los datos, se revisó que efectivamente se encuentran almacenados en la base de datos de ldap mediante el comando:

`ldapsearch -x -b dc=safavirtual,dc=com`

```
root@SERVERSIFA:/
Archivo Editar Ver Buscar Terminal Ayuda
# EAlulemal, people, safavirtual.com
dn: uid=EAlulemal,ou=people,dc=safavirtual,dc=com
cn: Alulema Ortiz Estefano Javier
uid: EAlulemal
uidNumber: 508
loginShell: /bin/sh
homeDirectory: /home/EAlulemal
gidNumber: 100
userPassword:: e2NyeXB0fVJVbWswUkvMud1Q0E=
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
shadowLastChange: 15506
gecos: Alulema Ortiz Estefano Javier
sn: Alulema Ortiz Estefano Javier

# AArroyo2, people, safavirtual.com
dn: uid=AArroyo2,ou=people,dc=safavirtual,dc=com
cn: Arroyo Vasquez Alejandro Sebastian
uid: AArroyo2
uidNumber: 509
loginShell: /bin/sh
homeDirectory: /home/AArroyo2
gidNumber: 100
userPassword:: e2NyeXB0fVFGWnQwd0lycjIucEO=
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
shadowLastChange: 15506
gecos: Arroyo Vasquez Alejandro Sebastian
sn: Arroyo Vasquez Alejandro Sebastian

# JCarrillo3, people, safavirtual.com
dn: uid=JCarrillo3,ou=people,dc=safavirtual,dc=com
cn: Carrillo
uid: JCarrillo3
uidNumber: 510
loginShell: /bin/sh
homeDirectory: /home/JCarrillo3
gidNumber: 100
userPassword:: e2NyeXB0fUJaOTI3TE8weXhNQVE=
objectClass: posixAccount
objectClass: shadowAccount
```

FIGURA 6.101 CONSULTA BDD LDAP
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

En la imagen se observa que la información correspondiente a los estudiantes del quinto año rojo se encuentran en la bdd con lo cual se comprueba que el servidor Ldap está funcionando.

6.8.4.3 COMPROBACIÓN SQUID

Para comprobar que el proxy squid se encuentra funcionando adecuadamente mediante autenticación LDAP se abrió un navegador, automáticamente apareció la página de acceso por contraseña.

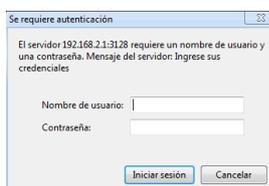


FIGURA 6.102 ACCESO POR CONTRASEÑA - SQUID
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

Solicitó ingreso de usuario y contraseña, donde se requiere la autenticación por medio de uno de los usuarios ingresados en la bdd de ldap para este caso se utilizó el usuario EAlulema1 contraseña Alulema



FIGURA 6.103 INGRESO DE USUARIO - SQUID

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Al dar clic en aceptar permitió acceder al internet, lo cual confirmó que la autenticación mediante el servicio de directorio Openldap funciona,

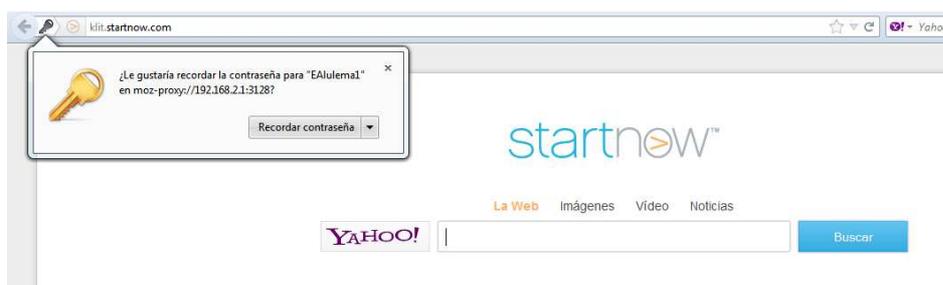


FIGURA 6.104 ACCESO A INTERNET - SQUID

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Seguidamente se comprobó la restricción de las páginas solicitadas como por ejemplo páginas de pornografía para lo cual se escribió en el buscador la palabra "pedofilia"



FIGURA 6.105 BÚSQUEDA PAGINAS NO DESEADAS - SQUID

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Se obtuvo como respuesta una notificación de que la página está bloqueada por políticas de la institución



FIGURA 6.106 INFORME DE RESTRICCIÓN - SQUID

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Mediante lo cual se comprobó que el proxy squid está funcionando y ejecutándose en las máquinas de la institución.

6.8.4.4 COMPROBACIÓN – MOODLE

Para comprobar el funcionamiento de moodle, se abrió la plataforma virtual en una maquina cliente en este caso se utilizó la maquina Safa05

En el navegador se escribió www.safavirtual.edu.ec y seguidamente apareció la página inicial de la institución, desde la cual se puede acceder al aula virtual mediante uno de sus enlaces.



FIGURA 6.107 PÁGINA INICIAL - DNS

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Al hacer clic sobre el enlace AulaVirtual se redirigió a la plataforma moodle, donde se observa los cursos disponibles, en este caso el curso de Valores Humanos



FIGURA 6.108 PÁGINA INICIAL - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Al pulsar en acceder al curso este solicitó autenticación de usuario y contraseña.

Se ingresaron datos de un usuario no existente en la base de datos de ldap y se obtuvo como respuesta **“Datos erróneos Inténtelo otra vez”**



FIGURA 6.109 DATOS ERRÓNEOS - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Posteriormente en el cuadro de autenticación se ingresó un usuario existente en la bdd de ldap en este caso de prueba el usuario EAlulema1 y contraseña Alulema, devuelvió como

resultado el ingreso exitoso a la plataforma en la página de edición de información, donde el usuario debe ingresar sus datos personales.

The screenshot shows the Moodle 'Edit profile' page. On the left, there is a 'NAVIGATION' menu with 'Home', 'My home', 'Site pages', 'My profile', and 'Courses'. Below it is a 'SETTINGS' menu with 'My profile settings', 'Edit profile', 'Messaging', and 'Blogs'. The main content area is titled 'General' and contains the following fields:

- First name* (empty)
- Surname* (empty)
- Email address* (empty)
- Email display: Allow only other course members to see my email address
- Email format: Pretty HTML format
- Email digest type: No digest (single email per forum post)
- Forum auto-subscribe: Yes: when I post, subscribe me to that forum
- Forum tracking: No: don't keep track of posts I have seen
- When editing text: Use HTML editor (some browsers only)
- AJAX and Javascript: Yes: use advanced web features
- Screen reader: No
- City/town* (empty)
- Select a country* (empty)
- Timezone: Server's local time
- Preferred language: English (en)

Below the 'General' section is the 'User picture' section, which shows 'Current picture: None' and a 'New picture' button with a 'Choose a file...' link and a note 'Maximum size for new files: 2MB'.

FIGURA 6.110 ACTUALIZACIÓN DE INFORMACIÓN - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Allí se ingresaron los datos referentes al estudiante y se autenticó el usuario dentro de la plataforma educativa.

The screenshot shows the Moodle 'Edit profile' page with the 'General' section filled out. The fields are:

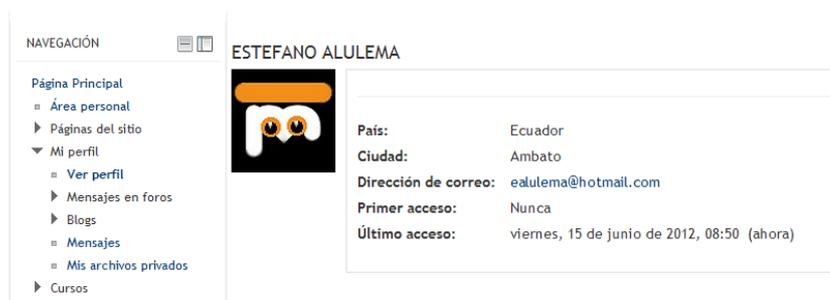
- First name*: Estefano
- Surname*: Alulema
- Email address*: ealulema@hotmail.com
- Email display: Allow only other course members to see my email address
- Email format: Pretty HTML format
- Email digest type: No digest (single email per forum post)
- Forum auto-subscribe: Yes: when I post, subscribe me to that forum
- Forum tracking: No: don't keep track of posts I have seen
- When editing text: Use HTML editor (some browsers only)
- AJAX and Javascript: Yes: use advanced web features
- Screen reader: No
- City/town*: Ambato
- Select a country*: Ecuador
- Timezone: Server's local time
- Preferred language: Español - Internacional (es)

FIGURA 6.111 AUTENTICACIÓN - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Finalmente apareció un resumen referente a la información ingresada del estudiante Estefano Alulema



The screenshot shows the Moodle user profile for Estefano Alulema. On the left is a navigation menu with options like 'Página Principal', 'Área personal', 'Páginas del sitio', 'Mi perfil', 'Ver perfil', 'Mensajes en foros', 'Blogs', 'Mensajes', 'Mis archivos privados', and 'Cursos'. The main content area displays the user's name 'ESTEFANO ALULEMA' with a profile picture of a stylized face. To the right, a table lists personal information: País: Ecuador, Ciudad: Ambato, Dirección de correo: ealulema@hotmail.com, Primer acceso: Nunca, and Último acceso: viernes, 15 de junio de 2012, 08:50 (ahora).

FIGURA 6.112 RESUMEN ESTUDIANTE AUTENTICADO - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Posteriormente se matriculó al alumno en el curso de Valores Humanos, ingresando la clave de matriculación estipulada por el administrador en fue la palabra **valores**



The screenshot shows the Moodle course enrollment page for 'VALORES'. The top navigation bar includes the Moodle logo, the user name 'Estefano Alulema', and a profile icon. Below the navigation bar, a breadcrumb trail reads 'PÁGINA PRINCIPAL > CURSOS > VALORES > MATRICULARME EN ESTE CURSO > OPCIONES DE...'. The main content area is titled 'OPCIONES DE MATRICULACIÓN' and features a section for 'Auto-matriculación (Estudiante)'. This section contains a text input field for 'Clave de matriculación' and a 'Matricularme' button.

FIGURA 6.113 MATRICULACIÓN - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Finalmente se pudo acceder a el curso y ver sus temas.

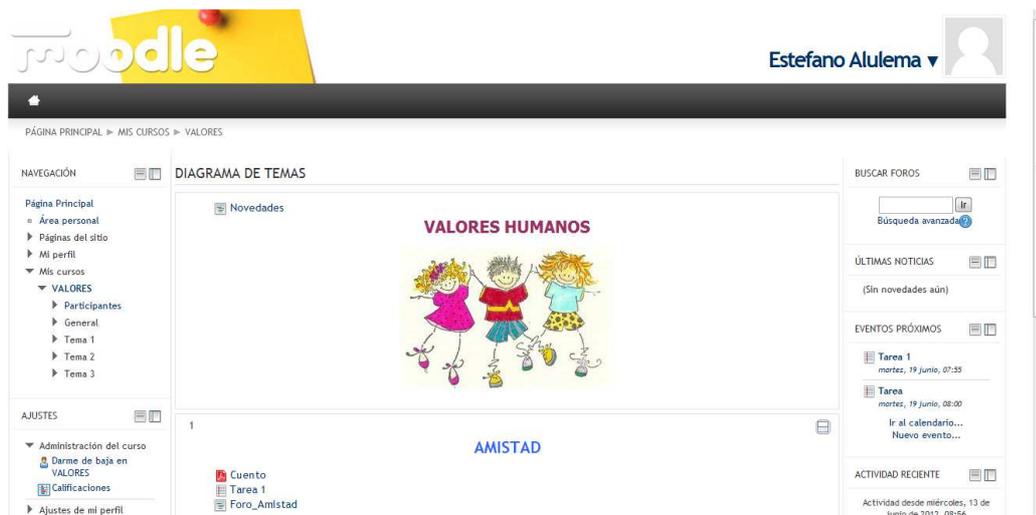


FIGURA 6.114 PAGINA INICIAL CURSO VALORES HUMANOS - MOODLE

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Mediante lo cual se comprobó el funcionamiento de la plataforma educativa moodle, creación de cursos, autenticación, matriculación y acceso a los datos del curso.

6.8.5 PLAN DE CONTINGENCIA

El plan de contingencia contiene las medidas técnicas necesarias para garantizar la continuidad del sistema y las operaciones de la intranet.

En este caso se ha realizado una imagen del disco del servidor en otro computador de la institución como respaldo de los servicios y demás implantaciones realizadas en el servidor de manera que en el caso de que se suscite algún inconveniente se pueda levantar el respaldo y se continúe normalmente con la utilización de las funcionalidades del sistema.

Para esto se utilizó el software CloneZilla, la cual es una potente herramienta Open Source liberada bajo la licencia GPLv2, gratuita y basada en el kernel de Linux, con la cual se pueden realizar imágenes de disco y restaurarlas de manera fácil y rápida, las imágenes del disco pueden ser almacenadas en lugares como:

- ▶ Partición de disco duro.
- ▶ Unidad de disco duro interna
- ▶ Dispositivos USB
- ▶ Servidor SSH
- ▶ Disco Duro conectado a un equipo remoto en una red interna. (Configurable mediante Samba)

Funciona como livecd o puede bootear desde flash USB.

El programa puede ser descargado directamente desde la página oficial del proyecto en la dirección www.clonezilla.org

6.9 CONCLUSIONES Y RECOMENDACIONES

6.9.1 CONCLUSIONES

- El software libre abre cada vez más oportunidades de innovación y facilidad de uso para instituciones públicas y privadas que quieran incursionar en el medio.
- La Implementación de un sistema de Autenticación Unificada en la escuela Sagrada Familia resulto de gran aporte para la institución puesto que se pudo optimizar sus recursos como también desarrollar indicios para una mejora académica.
- El Autenticar los estudiantes de la institución tanto a la plataforma Moodle como al servicio de internet provee un gran aporte de seguridad y reducción de tiempo al momento de gestionar usuarios.
- Las políticas de acceso y restricción de uso del internet pudieron ser plasmadas dentro del centro educativo con las ventajas de que los infantes no tendrán acceso a páginas inapropiadas para su edad.
- La plataforma Moodle como herramienta tecnológica de docencia provee un gran apoyo a quienes la implementan mediante soporte brindado directamente por sus desarrolladores.

6.9.2 RECOMENDACIONES

- Realizar una capacitación al personal Docente acerca de la utilización de plataformas virtuales con el fin de facilitar el uso de la misma.
- Analizar detenidamente el funcionamiento del Sistema de Autenticación dentro de la institución para que posteriormente puedan ir actualizando sus políticas de uso del internet.
- Ubicar los dispositivos electrónicos y de comunicación en un sitio adecuado y evitar el desprendimiento de cables por causa el continuo tráfico de estudiantes, como la manipulación no adecuada de los mismos.
- Realizar la reposición de los cables de conexión en mal estado.
- Analizar el uso del Webmin para facilitar la creación y edición de usuarios para el acceso al internet como para la plataforma educativa moodle.
- Preservar el plan de contingencia y respaldo instaurado en la institución.

BIBLIOGRAFÍA

REFERENCIAS BIBLIOGRÁFICAS DEL INTERNET

- [1] Portillo, E. (2011) Redes Informáticas, [En línea]. El Salvador. Disponible en:
<http://www.innovacionate.com/servicios/consultorias-en-redes.html>
- [2] Jae, J (2011). Topología de Redes, [En línea]. Disponible en:
<http://elblogdelasredes.blogspot.com/p/redes-por-topologia-red-inalambrica-una.html>.
- [3] Alzate, G (2011). El pilar informatico [En línea]. Disponible en:
<http://pilarinformatico.blogspot.com/p/servidores.html>
- [4] Axel (2012). Sistemas Operativos en Ambientes Distribuidos, [En línea]. Disponible en: <http://albeiro1.blogspot.com/>
- [5] Alapont, V (2012). Seguridad en redes inalámbricas, [En línea]. Valencia, Disponible en:
<http://www.uv.es/~montanan/ampliacion/trabajos/SeguridadWireless.pdf>
- [6] Wikipedia (2011), Copia de Seguridad [En línea]. Disponible en:
http://es.wikipedia.org/wiki/Copia_de_seguridad
- [7] Wikipedia (2011), Seguridad Informática [En línea]. Disponible en:
http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- [8] Robles,L (2011), Modelos de Seguridad de la Información España [En línea]. Disponible en: <http://www.slideshare.net/luisrobles17/modelos-de-seguridad-de-la-informacin>
- [9] Ruiz, C (2012), Red Local [En línea]. Disponible en:
<http://es.scribd.com/doc/52469203/Concepto-de-Red-Local-215>
- [10] Anónimo (2011), Virus Informáticos, España, [En línea]. Disponible en:
<http://www4.uji.es/~al053184/main.html>

- [11] Anónimo (2011), Firewall o Cortafuegos [En línea]. Disponible en:
<http://infoaprende.web44.net/infoaprende/firewall-o-cortafuegos/>
- [12] Anónimo (2012), Seguridad en Redes, [En línea]. Disponible en:
http://iscseguridad.blogspot.com/2012/05/unidad-4-seguridad-en-la-comunicacion_30.html
- [13] Anónimo (2011), Firewalls, [En línea]. Disponible en:
http://docente.ucol.mx/ychave/public_html/FIREWALL.htm
- [14] Wikipedia,(2012), Proxy, [En línea]. Disponible en: [http: es.wikipedia.org/wiki/Proxy](http://es.wikipedia.org/wiki/Proxy)
- [15] Wikipedia (2012), Domain Name System, [En línea]. Disponible en:
http://es.wikipedia.org/wiki/Domain_Name_System
- [16] Wikipedia, (2012), Fedora (Distribución Linux), [En línea]. Disponible en:
[http://es.wikipedia.org/wiki/Fedora_\(distribuci%C3%B3n_Linux\)](http://es.wikipedia.org/wiki/Fedora_(distribuci%C3%B3n_Linux))
- [17] Wikipedia, (2012), Ubuntu, [En línea]. Disponible en:
<http://es.wikipedia.org/wiki/Ubuntu>
- [18] Medina,J (2011), Configuración de los esquemas de control de acceso en squid [En línea]. Disponible en:
http://tuxjm.net/docs/Manual_de_Instalacion_de_Servidor_Proxy_Web_con_Ubuntu_Server_y_Squid/html-multiples/configuracion-de-los-esquemas-de-control-de-acceso-en-squid.html#id554188
- [19] Anónimo,(2012) Squid, [En línea]. Disponible en:
<http://usuarios.multimania.es/ogmeo/squid.pdf>
- [20] Anónimo, (2012), [En línea], Resumen Squid, Disponible en:
<http://es.scribd.com/doc/94412942/Resumen-Squid>
- [21] Carletto,A Claroline, una herramienta libre como apoyo a la docencia presencia, [En línea]. Disponible en: <http://jornadaie.unvm.edu.ar/ponencia12.pdf>

- [22] Wikipedia, (2011), Moodle, [En línea]. Disponible en:
<http://es.wikipedia.org/wiki/Moodle>
- [23] Wikipedia (2012), Servicio de Directorio, [En línea]. Disponible en:
http://es.wikipedia.org/wiki/Servicio_de_directorio
- [24] Red Hat Directory Server, [En línea]. Disponible en:
http://www.latam.redhat.com/pdf/Red_Hat_Directory_Server.pdf
- [25] Wikipedia, (2011), [En línea]. Disponible en:
<http://es.wikipedia.org/wiki/OpenLDAP>
- Evolution, F.(2012) Servidor Proxy , [En línea].México. Disponible en:
<http://www.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base+de+Conocimiento/Servidor+Proxy#section-Servidor+Proxy-Archivos+de+configuración+del+squid>
- Kenangan, C,C (2012) Setup DNS Server Bind chroot Centos 6.2, [En línea].Indonésia. Disponible en:
<http://bachem.wordpress.com/2012/04/14/setup-dns-server-bind-chroot-centos-6-2/>
- C,G,A (2009) Configuración de Moodle con usuarios LDAP, [En línea]. Andalucía. Disponible en:
http://www.juntadeandalucia.es/averroes/cga/IMG/pdf/configuracion_de_moodle_con_usuarios_de_ldap.pdf
- Ducea,M (2006) How to enable IP Forwarding in Linux, [En línea]. California. Disponible en: <http://www.ducea.com/2006/08/01/how-to-enable-ip-forwarding-in-linux/>

GLOSARIO

SOFTWARE LIBRE.- Programas o aplicaciones informáticas que pueden ser usadas, adquiridas, copiadas y distribuidas de manera libre.

DOMINIO.- Es un nombre base que agrupa a un conjunto de equipos o dispositivos y que permite proporcionar nombres de equipo más fácilmente recordables en lugar de una dirección ip numérica.

DNS.- Servicio de nombres de dominio

PROTOCOLO.- Estándar que controla o permite la conexión comunicación y transferencia de datos entre dos puntos finales

UNIX.- Es un sistema operativo, portable, multitarea y multiusuario desarrollado en principio en 1969

MURO CORTAFUEGOS.- Es una parte de un sistema o de una red que está diseñada para bloquear el acceso no autorizado permitiendo al mismo tiempo comunicaciones autorizadas.

www: World Wide Web.

BASE DE DATOS: Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella.

CLAVE DE ACCESO: Password Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

CLIENTE - SERVIDOR: Se denomina así al binomio consistente en un programa cliente que consigue datos de otro llamado servidor sin tener que estar obligatoriamente ubicados en el mismo ordenador.

APACHE: Sitio web de distribución libre. Fue desarrollado en 1995 y ha llegado a ser el más usado de Internet.

BACKUP: Copia de seguridad. Se hace para prevenir una posible pérdida de información

CACHÉ: en un navegador, el caché guarda copias de documentos de acceso frecuente, para que en el futuro aparezcan más rápidamente.

DOWNLOAD: Descargar, bajar. Transferencia de información desde Internet a una computadora.

USUARIO: Cualquier individuo que interactúa con la computadora a nivel de aplicación. Los programadores, operadores y otro personal técnico no son considerados usuarios cuando trabajan con la computadora a nivel profesional.

ENCRIPTAR: proteger archivos expresando su contenido en un lenguaje cifrado. Los lenguajes cifrados simples consisten, por ejemplo, en la sustitución de letras por números.

ANEXOS

ANEXO A: ESTRUCTURA DEL CUESTIONARIO

UNIVERSIDAD TECNICA DE AMBATO
FACULTAD DE INGENIERIA EN SISTEMAS ELECTRONICA E INDUSTRIAL
CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES E INFORMATICOS

ENCUESTA DIRIGIDA AL PERSONAL ADMINISTRATIVO Y DOCENTES DE LA ESCUELA "SAGRADA FAMILIA"

OBJETIVO:

Determinar el requerimiento de un Sistema de Autenticación Unificada para un correcto control y manejo de la información dentro de una red de datos.

INSTRUCCIONES:

Marque en el espacio en blanco la respuesta de acuerdo con las necesidades que usted crea conveniente

FECHA: _____

1. ¿SE SIENTE CONFORME CON EL ACTUAL MANEJO Y TRANSMISIÓN DE INFORMACIÓN DENTRO LA INSTITUCIÓN?

SI () NO ()

2. ¿ESTA CONSIENTE DE LOS ATAQUES DE TERCEROS QUE PUEDE SUFRIR LA INSTITUCIÓN?

SI () NO ()

3. ¿HA SUFRIDO PÉRDIDAS DE INFORMACIÓN EN LOS COMPUTADORES DEL INSTITUTO?

SI () NO ()

4. ¿OPINA UD. QUE UNA RED INALÁMBRICA PERMITIRÁ UNA GESTIÓN Y EXPLOTACIÓN MUCHO MÁS EFICAZ DE LOS RECURSOS INFORMÁTICOS?

SI () NO ()

5. ¿ESTÁ COMPLETAMENTE CONFORME CON LA VELOCIDAD DEL INTERNET DENTRO LA INSTITUCIÓN?

SI () NO ()

6. ¿LE PARECE IMPORTANTE EL MANEJO DE AULAS VIRTUALES DENTRO DE LA ESCUELA?

SI () NO ()

7. ¿CONSIDERA NECESARIA UNA AUTENTICACIÓN DE ACCESO AL INTERNET EN CADA COMPUTADOR DENTRO DEL LABORATORIO DE COMPUTACIÓN?

SI () NO ()

8. ¿CREE UD. QUE UNA RED ALÁMBRICA ESTRUCTURADA OPTIMIZARA LA VELOCIDAD DE COMUNICACIÓN?

SI () NO ()

9. ¿CONSIDERA. QUE ES NECESARIO RESTRINGIR DETERMINADAS PÁGINAS WEB A LAS QUE SE TIENE ACCESO DENTRO DE LA ESCUELA?

SI () NO ()

GRACIAS POR SU COLABORACIÓN

ANEXO B : DETALLE DE LA INSTALACIÓN DE CENTOS



Selección de la primera opción la cual indica que instalará el sistema operativo en modo grafico

FIGURA B1 PAGINA INICIAL INSTALACIÓN CENTOS

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

```
input: ImEXPS/2 Generic Explorer Mouse as /devices/platform/i8042/serio1/input/
input4
usbhid: v2.6:USB HID core driver
TCP cubic registered
Initializing XFRM netlink socket
NET: Registered protocol family 17
registered taskstats version 1
IMB: No TPM chip found, activating TPM-bypass!
rtc_cmos rtc_cmos: setting system clock to 2012-04-27 04:39:10 UTC (1335501550)
Initializing network drop monitor service
Freeing unused kernel memory: 1220k freed
Write protecting the kernel read-only data: 7176k

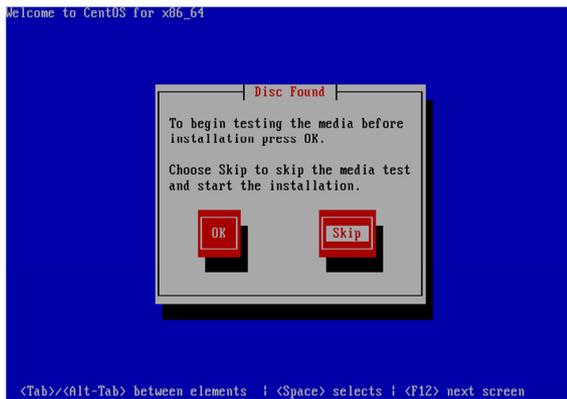
Greetings.
anaconda installer init version 13.21.02 starting
mounting /proc filesystem... done
creating /dev filesystem... done
starting udev...done
mounting /dev/pts (unix98 pts) filesystem... done
mounting /sys filesystem... done
trying to remount root filesystem read write... done
mounting /tmp as tmpfs... done
running install...
running /sbin/loader
```

Mostrara información de la configuración necesaria para levantar el instalador.

FIGURA B2 LEVANTANDO SERVIDOR

Fuente. Escuela Sagrada Familia

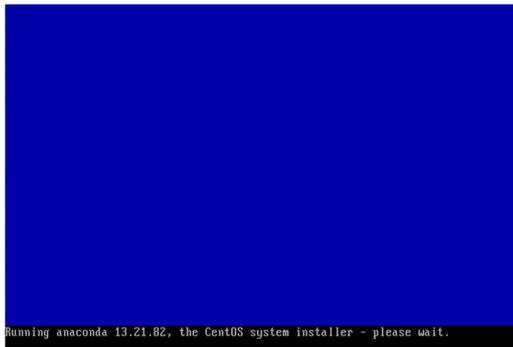
Elaborado por: Adriana Salinas



Pregunta si se desea probar el disco de instalación antes de continuar, en este caso se presionó skip indicando que no testee el disco y avance

FIGURA B3 PROBAR DISCO DE INSTALACION

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*



Seguidamente indica que está corriendo anaconda el cual es el instalador de Red Hat

FIGURA B4 CORRIENDO ANACONDA

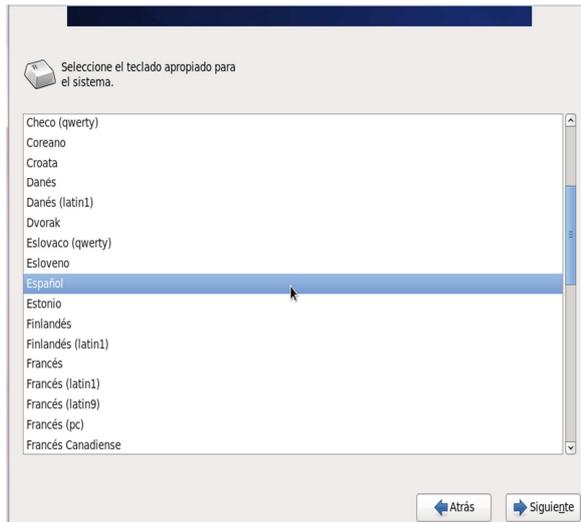
*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*



La siguiente pantalla muestra que la instalación del S.O ha iniciado indicándo que se instalara Centos 6.0

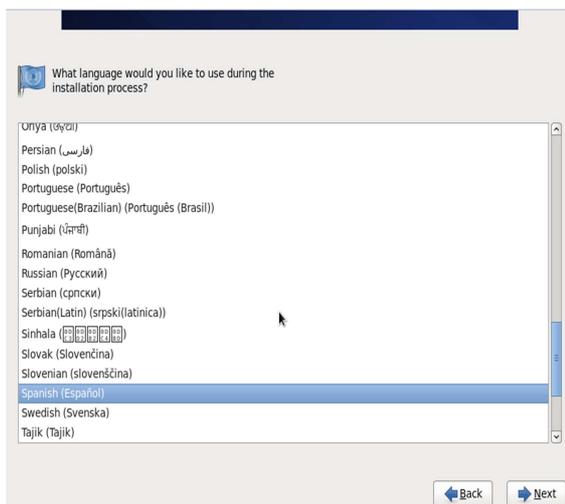
FIGURA B5 CORRIENDO DE INSTALACIÓN

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*



El paso siguiente es seleccionar el idioma del teclado si el teclado contiene la letra ñ es español caso contrario es inglés, en esta ocasión se seleccionó español

FIGURA B6 SELECCIÓN DEL IDIOMA DEL TECLADO
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas



Se Indicó el lenguaje a utilizar durante la instalación de Centos, español

FIGURA B7 SELECCIÓN DEL IDIOMA DE INSTALACIÓN
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas



FIGURA B8 SELECCIÓN TIPO DE DISPOSITIVOS

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Solicita que se indique el tipo de dispositivos involucra la instalación, se seleccionó dispositivos de almacenamiento básico



FIGURA B9 EXAMINANDO DISPOSITIVOS

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Esta pantalla muestra que el instalador está examinando los dispositivos presentes en el servidor



FIGURA B10 ASIGNACIÓN NOMBRE AL SERVIDOR

Fuente. Escuela Sagrada Familia

Elaborado por: Adriana Salinas

Luego de examinar los dispositivos solicita un nombre para el servidor, en este caso por ser el servidor de la escuela sagrada familia se lo llamo SERVERSAFA



Posteriormente se indicó la ubicación actual del servidor en el mapa, la más cercana fue Guayaquil puesto que no apareció Ambato

FIGURA B11 UBICACIÓN ACTUAL DEL SERVIDOR

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas



Solicita el ingreso de la contraseña de root o administrador se ingresó una contraseña general para facilitar su manejo.

FIGURA B12 ASIGNACIÓN DE CONTRASEÑA

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas



Pregunta el tipo de instalación deseada, en esta ocasión como es una nueva instalación se seleccionó la opción utilizar todo el espacio

FIGURA B13 SELECCIÓN TIPO DE INSTALACIÓN

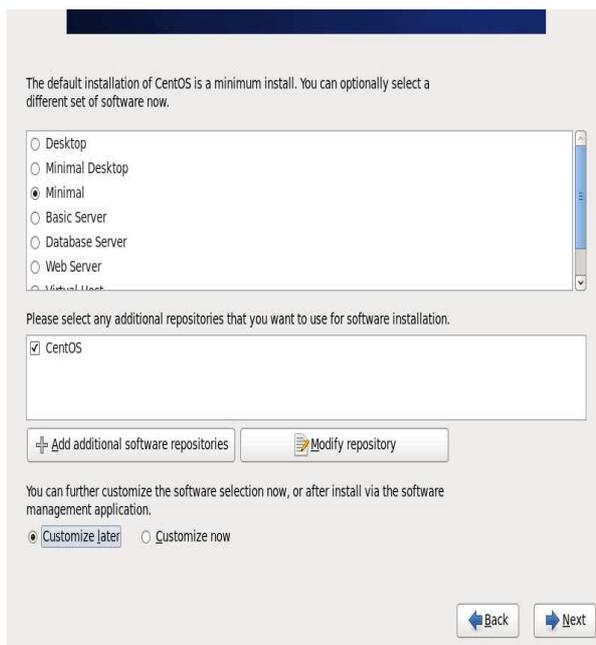
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas



Mediante esta pantalla indica que todas la opciones seleccionadas servirán para la escritura en el disco duro

FIGURA B14 AVISO DE ESCRITURA

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas



Esta sección es muy importante puesto que pide la elección de los servicios que se instalaran, seleccionare mínima la cual es ideal para servidores sin embargo más adelante se puede añadir más características.

FIGURA B15 SELECCIÓN DE SERVICIOS DE INSTALACION

Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas



Indica el progreso de la instalación

FIGURA B16 PROGRESO DE LA INSTALACION

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*



Esta pantalla indica que finalmente se completó la instalación de Centos en el computador

FIGURA B17 AVISO INSTALACIÓN COMPLETA

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*



Esta pantalla muestra que Centos se está iniciando

FIGURA B18 INICIANDO CENTOS

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*



FIGURA B19 ESCRITORIO DE CENTOS
Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas

En ese caso el servidor será utilizado y administrado por el personal de la institución por lo cual se necesita un servidor amigable al usuario por lo mismo se instaló el escritorio de Centos mediante el comando: ***Yum groupinstall Desktop***

**ANEXO C: DECRETO PRESIDENCIAL DEL USO DE SOFTWARE LIBRE EN LA
REPUBLICA DEL ECUADOR**

ARTÍCULO 1.- Establecer como política pública para las Entidades de la Administración Pública Central la utilización de Software Libre en sus sistemas y equipamientos informáticos.

ARTÍCULO 2.- Se entiende por Software Libre, a los programas de computación que se pueden utilizar y distribuir sin restricción alguna, que permitan su acceso a los códigos fuentes y que sus aplicaciones, puedan ser mejoradas. Estos programas de computación tienen las siguientes libertades:

- a) Utilización del programa con cualquier propósito de uso común.
- b) Distribución de copias sin restricción alguna.
- c) Estudio y modificación del programa (Requisito: código fuente disponible).
- d) Publicación del programa mejorado (Requisito: código fuente disponible).

ARTÍCULO 3.- Las entidades de la Administración Pública Central previa a la instalación del software libre en sus equipos, deberán verificar la existencia de capacidad técnica que brinde el soporte necesario para el uso de éste tipo de software.

ARTÍCULO 4.- Se faculta la utilización de software propietario (no libre) únicamente cuando no exista una solución de Software Libre que supla las necesidades requeridas, o cuando esté en riesgo la seguridad nacional, o cuando el proyecto informático se encuentre en un punto de no retorno.

En este caso, se concibe como seguridad nacional, las garantías para la supervivencia de la colectividad y la defensa del patrimonio nacional.

Para efectos de este decreto se entiende por un punto de no retorno, cuando el sistema o proyecto informático se encuentre en cualquiera de estas condiciones:

- a) Sistema en producción funcionando satisfactoriamente y que un análisis de costo – beneficio muestre que no es razonable ni conveniente una migración a Software Libre.

b) Proyecto en estado de desarrollo y que un análisis de costo – beneficio muestre que no es conveniente modificar el proyecto y utilizar Software Libre.

Periódicamente se evaluarán los sistemas informáticos que utilizan software propietario con la finalidad de migrarlos a Software Libre.

ARTÍCULO 5.- Tanto para software libre como software propietario, siempre y cuando se satisfagan los requerimientos, se debe preferir las soluciones en este orden:

a) Nacionales que permitan autonomía y soberanía tecnológica.

b) Regionales con componente nacional.

c) Regionales con proveedores nacionales.

d) Internacionales con componente nacional.

e) Internacionales con proveedores nacionales.

f) Internacionales.

ARTÍCULO 6.- La Subsecretaría de Informática como órgano regulador y ejecutor de las políticas y proyectos informáticos en las entidades del Gobierno Central deberá realizar el control y seguimiento de éste Decreto.

Para todas las evaluaciones constantes en este decreto la Subsecretaría de Informática establecerá los parámetros y metodologías obligatorias.

ARTÍCULO 7.- Encárguese de la ejecución de este decreto a los señores Ministros Coordinadores y el señor Secretario General de la Administración Pública y Comunicación. 162

Dado en el Palacio Nacional en la ciudad de San Francisco de Quito, Distrito Metropolitano, el día de hoy 10 de abril del 2008.

RAFAEL CORREA DELGADO
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

ANEXO D: DISPOSITIVOS DE LA INSTITUCIÓN



FIGURA D1 LABORATORIO DE COMPUTACIÓN VISIÓN LATERAL

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*



FIGURA D2 LABORATORIO DE COMPUTACIÓN VISIÓN FRONTAL

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*



FIGURA D3 ROUTER DLINK

*Fuente. Escuela Sagrada Familia
Elaborado por: Adriana Salinas*

ANEXO E: MANUAL DE POLÍTICAS DE USO DE SERVICIOS

POLÍTICAS DE USO RESPONSABLE DE LOS SERVICIOS IMPLANTADOS PARA LA ESCUELA SAGRADA FAMILIA

PROPÓSITO

El propósito de este documento es definir las políticas institucionales respecto al uso responsable de los servicios implantados en la escuela “Sagrada Familia”. Entendiéndose por uso responsable al seguimiento de normas políticas y buenas prácticas que salvaguarden la seguridad de la información y recursos tecnológicos institucionales asegurando el buen funcionamiento de los mismos.

ALCANCE

Estas políticas se aplicarán a todos los estudiantes, docentes, administrativos y cualquier otra persona que tenga acceso a los sistemas de información de la institución.

TÉRMINOS / DEFINICIONES

Para propósitos de estas políticas se aplicarán las siguientes definiciones:

- ▶ Material no permitido: Incluye transmisión, distribución o almacenamiento de todo material que viole cualquier ley aplicable. Se incluye sin limitación, material protegido por derechos de reproducción, marca comercial. Secreto comercial, u otro derecho sobre la propiedad intelectual utilizada sin la debida autorización y material que resulte obsceno, difamatorio o ilegal bajo las leyes nacionales.
- ▶ Redes: Incluye cualquier sistema de cableado o equipos físicos como enrutadores, switches, además de varios sistemas electrónicos como redes de video, datos, voz y dispositivos de almacenamiento.
- ▶ Sistemas de Información: Incluye cualquier sistema o aplicación de software que sea administrado por la institución y de los cuales ella es responsable, como Moodle, Webmin, aplicaciones de servidor y escritorio, sistemas operativos y aplicaciones de internet.

- ▶ Usuarios: Incluye toda aquella persona no necesariamente vinculada con la institución, a quién se le conceda los medios y niveles de autorización y acceso necesarios para hacer uso de los servicios o sistemas de información de la escuela (personal administrativo, docentes, estudiantes, directivos, etc.).
- ▶ Webmin: Herramienta de configuración de sistemas accesible vía web. Con él se pueden configurar aspectos internos, como usuarios.

GENERALIDADES

La Escuela Sagrada Familia “SAFA” facilita el acceso al personal administrativo, estudiantes, docentes y directivos, a fuentes de información nacional e internacional y por proveer un ambiente que fomente la difusión en línea del conocimiento, en el marco de la misión educativa.

El acceso a los servicios son un privilegio no un derecho, y debe ser tratado de esta manera por todos los usuarios, quienes deben actuar honesta y responsablemente. Cada usuario es responsable por la integridad de estos servicios y tiene el deber de respetar los derechos de otros usuarios, la integridad de las instalaciones físicas y sus métodos de control. Debiendo actuar de acuerdo con esos lineamientos y las leyes nacionales pertinentes.

USO DE LA RED INSTITUCIONAL

- ▶ Las identificaciones y claves de acceso a la red institucional, la intranet o cualquier otro sistema de información son propiedad de la institución. Estas identificaciones y claves son para uso estrictamente personal y la responsabilidad de su uso debido recae exclusivamente en el usuario al que se le asignen.
- ▶ El acceso no autorizado a los sistemas de información e la institución está prohibido. Nadie debe usar identificación, identidad o contraseña de otro usuario, y de la misma manera ningún usuario debe dar a conocer su contraseña o identificación a otro, excepto en casos que faciliten la reparación o el mantenimiento de algún servicio o equipo.

- ▶ El usuario no deberá sin permiso de la institución hacer modificaciones de la red institucional, la intranet o a sus recursos. No se permitirá ningún intento de vulnerar o de atentar contra los sistemas de protección o de seguridad de la red.
- ▶ En la red institucional en horarios de clases matutinas no está permitida la operación de software para la descarga y distribución de archivos de música, videos y similares impropios de las asignaturas escolares.
- ▶ Está prohibido intentar instalar u operar puntos de acceso inalámbricos (Access point) conectados a la red cableada de la "SAFA" sin autorización de la dirección de la institución
- ▶ Los usuarios no deben intentar modificar, reubicar o sustraer del lugar donde han sido instalados o configurados, equipos de cómputo, software, información o periféricos sin la debida autorización.
- ▶ No se permite interferir sin autorización el acceso de otros usuarios a los recursos de los sistemas de información de la institución.
- ▶ Está prohibido transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- ▶ No se consiente permiso de uso de las comunicaciones electrónicas para acosar o amenazar a los usuarios de la institución o externos, de alguna manera que sin razón interfiera con la educación.
- ▶ Está prohibido utilizar los servicios ofertados por la institución para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material obsceno.

USO DEL INTERNET

- ▶ Los privilegios de uso del internet serán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada usuario.

- ▶ Cada usuario recibirá un código de identificación y una contraseña única. Sin importar la circunstancia, está prohibido compartir o revelar la contraseña a otros usuarios.
- ▶ El usuario no debe entrar a páginas web con contenido pornográfico.
- ▶ No se permitirá el uso del internet para descargar de videos, programas, software en horario de clases.
- ▶ El usuario no debe instalar ningún programa para escuchar MP3, RA, WAV o emisoras de radio vía internet.
- ▶ Se prohíbe cualquier tipo de transmisión vía internet (escuchar música y ver videos).
- ▶ Está restringido el acceso a páginas de pornografía, sexo, necrofilia
- ▶ No está permitido ingresar a sitios web de farándula, entretenimiento, redes sociales en horario de clases.
- ▶ A partir de las 2 de la tarde el acceso a internet se ofrece sin restricciones

USO Y ADMINISTRACIÓN DE LA HERRAMIENTA WEBMIN

- ▶ La gestión y creación de usuarios que serán de utilidad para el acceso de los mismos a los servicios de internet y educación virtual serán realizados por el Director de la institución y la docente de la asignatura de computación.

USO Y ADMINISTRACIÓN DEL AMBIENTE EDUCATIVO VIRTUAL (MOODLE)

- ▶ La herramienta moodle está considerada para el uso de docentes y estudiantes.

- ▶ La Administración de la plataforma educativa es ejecutada directamente por el Director de la institución y la docente de la asignatura de computación.
- ▶ Para su desempeño los Administradores de la plataforma serán los encargados de la creación de cursos.
- ▶ El nombre del usuario del profesor será el otorgado por uno de los administradores de la plataforma, así mismo sus alumnos deberán usar el usuario y clave única utilizado para el acceso a los demás servicios de la institución.
- ▶ Los datos del perfil del catedrático o instructor deben estar completos, verídicos y actualizados (incluyendo la imagen la cual deberá ser del rostro, individual, nítida y reciente).
- ▶ Los instructores son responsables de la información contenida en el curso y de los derechos reservados sobre las obras (documentos, imágenes, programas, etc.) utilizadas dentro del curso.
- ▶ El profesor es responsable de la configuración de seguridad de su curso así como el respaldo de la información del mismo; y por ningún motivo deberá proporcionar su clave a otra persona.
- ▶ El profesor deberá notificar cualquier falla, anomalía o problema que detecte durante el uso de la herramienta, al administrador de la plataforma.