

UNIVERSIDAD TÉCNICA DEL NORTE



FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA ELECTRÓNICA Y REDES DE COMUNICACIÓN

**“SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
(SGSI) EN EL COMANDO PROVINCIAL DE POLICÍA IMBABURA**

Nro. 12”

**PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN
ELECTRÓNICA Y REDES DE COMUNICACIÓN**

PAOLA ALEXANDRA DÍAZ PARCO

DIRECTOR: ING. JAIME MICHILENA

Ibarra, Febrero 2013



UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de Identidad	1002938056
Apellidos y Nombres	Díaz Parco Paola Alexandra
Dirección	Río Chinchipe 1-14 y Río Daule
Email	pao_lucho@hotmail.com
Teléfono Móvil	0989719176

DATOS DE LA OBRA	
Título	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL COMANDO PROVINCIAL DE POLICÍA "IMBABURA Nro. 12"
Autor	Díaz Parco Paola Alexandra
Fecha	06 de Febrero de 2013
Programa	Pregrado
Título por el que se aspira	Ingeniera en Electrónica y Redes de Comunicación
Director	Ing. Jaime Michilena

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Paola Alexandra Díaz Parco, con cédula de identidad Nro. 1002938056, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.



UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **Paola Alexandra Díaz Parco**, con cédula de identidad Nro. 1002938056, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, Artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado **“SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL COMANDO PROVINCIAL DE POLICÍA IMBABURA Nro. 12”**, que ha sido desarrollado para optar por el título de **Ingeniera en Electrónica y Redes de Comunicación**, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en el formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

A handwritten signature in blue ink that reads 'Paola Díaz'. The signature is written in a cursive style with a large initial 'P'.

Firma

Nombre: Paola Alexandra Díaz Parco

Cédula: 1002938056

CERTIFICACIÓN

Certifico que el presente trabajo de grado titulado: "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN EL COMANDO PROVINCIAL DE POLICÍA IMBABURA Nro. 12", fue desarrollado por la estudiante: **PAOLA ALEXANDRA DÍAZ PARCO**, bajo mi supervisión.

A handwritten signature in blue ink on a light-colored background. The signature is stylized and appears to read 'Jaime Michilena'.

Ing. Jaime Michilena
DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Quiero hacer extensivos mis más sinceros agradecimientos;

En primer lugar a Dios, por permitirme cumplir con una de mis metas propuestas y por poner en mi camino a personas de excelente calidad humana con las que he compartido momentos inolvidables.

A mis padres, Soledad y Ramiro, por el inmesurable amor que me brindan y por apoyarme siempre en todo momento. Gracias por darme un buen ejemplo y por sus valiosas enseñanzas.

A mis hermanos Bryan y Javier, mi hermana Nathaly (+), con quienes he compartido maravillosos momentos y siempre están presentes para apoyarme.

A mi director de tesis, Ing. Jaime Michilena, por todo su apoyo, tiempo y paciencia en la realización de mi tesis. Gracias por todos sus consejos que me sirvieron para culminar satisfactoriamente mi proyecto.

Al Comando Provincial de Policía "Imbabura" No. 12, de manera especial al Cbop. Ing. Ángel Núñez por abrirme las puertas de la institución y brindarme incondicionalmente su ayuda.

Paola

DEDICATORIA

Quiero dedicar este trabajo a mi familia porque ellos son el pilar fundamental y una bendición en mi vida y de manera especial a mi hermana Nathaly (+) quien fue mi ejemplo a seguir y quien a pesar de ya no estar a mi lado, por siempre se mantendrá viva en mi corazón.

A mi novio Luis Carlos, por ser un apoyo fundamental en mi vida, por estar a mi lado en cada momento, por enseñarme el verdadero sentido del amor y la felicidad y por ser una persona inigualable.

A mis amigas, porque con ellas he compartido hermosos momentos y cada una tiene un lugar en mi corazón.

A todas las personas que de una u otra manera hicieron posible que yo pueda llegar hasta el final y cumplir con mi objetivo.

Paola

TABLA DE CONTENIDOS

CERTIFICACIÓN	v
AGRADECIMIENTOS	vi
DEDICATORIA.....	vii
TABLA DE CONTENIDOS	viii
RESUMEN	xxiii
ABSTRACT	xxiv
PRESENTACIÓN	xxv
CAPÍTULO I	1
FUNDAMENTO TEÓRICO.....	1
1.1 NORMA ISO/IEC 27000.....	1
1.1.1 TÉRMINOS Y DEFINICIONES.....	3
1.2 ESTÁNDAR INTERNACIONAL ISO/IEC 27001.....	5
1.2.1 ENFOQUE DEL PROCESO	6
1.2.2 ALCANCE DEL ESTÁNDAR	9
1.2.3 REFERENCIAS NORMATIVAS.....	9
1.2.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	9
1.2.4.1. Requerimientos generales	10
1.2.4.2. Establecer y manejar el SGSI	10
1.2.4.3. Requerimientos de documentación.....	14
1.2.5 RESPONSABILIDAD DE LA GERENCIA.....	15
1.2.6 AUDITORÍAS INTERNAS SGSI	15
1.2.7 MEJORAMIENTO DEL SGSI	16
1.2.8 OBJETIVOS DE CONTROL Y CONTROLES.....	16
1.3 ESTÁNDAR INTERNACIONAL ISO/IEC 27002.....	17
1.3.1 ALCANCE DEL ESTÁNDAR	18
1.3.2 CLÁUSULAS.....	18
1.3.2.1. Política de seguridad	19
1.3.2.2. Organización de la Seguridad de la Información.....	19
1.3.2.3. Gestión de Activos.....	20
1.3.2.4. Seguridad de Recursos Humanos.....	20

1.3.2.5.	Seguridad Física y Ambiental (Entorno físico).....	20
1.3.2.6.	Gestión de Comunicaciones y Operaciones	20
1.3.2.7.	Control de Acceso.....	20
1.3.2.8.	Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.....	21
1.3.2.9.	Gestión de Incidentes de Seguridad de la Información	21
1.3.2.10.	Gestión de la Continuidad Comercial.....	21
1.3.2.11.	Cumplimiento.....	21
CAPÍTULO II		22
SITUACIÓN ACTUAL DE LA RED DE DATOS.....		22
2.1	ANÁLISIS DEL ESTADO ACTUAL DE LA ENTIDAD.....	22
2.2	TOPOLOGÍA FÍSICA DE LA RED INTERNA	23
2.2.1	DIRECCIONAMIENTO IP.....	26
2.3	DESCRIPCIÓN DE LOS EQUIPOS DE RED	27
2.4	DESCRIPCIÓN DE LOS DEPARTAMENTOS DEL CP-12.....	33
2.4.1	COMANDANCIA	33
2.4.2	PREVENCIÓN	34
2.4.3	JEFATURA FINANCIERA.....	35
2.4.4	COMPRAS PÚBLICAS.....	36
2.4.5	OPERACIONES.....	36
2.4.6	ASUNTOS INTERNOS.....	37
2.4.7	RELACIONES PÚBLICAS	38
2.4.8	POLICÍA COMUNITARIA.....	39
2.4.9	REGIÓN NORTE.....	40
2.4.10	RECURSOS HUMANOS.....	40
2.4.11	RECURSOS LOGÍSTICOS	41
2.4.12	ASESORÍA JURÍDICA	42
2.4.13	RASTRILLO	42
2.4.14	INTELIGENCIA	43
2.4.15	SISTEMAS.....	44
2.5	SITUACIÓN ACTUAL.....	44
CAPÍTULO III		57
ANÁLISIS Y EVALUACIÓN DE RIESGOS.....		57

3.1	METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS	57
3.2	ADMINISTRACIÓN DE RIESGOS	58
3.3	ANÁLISIS DE RIESGOS	59
3.3.1	CONTROL DE ACTIVOS.....	59
3.3.1.1	Identificación de activos del CP-12	61
3.3.1.2	Valoración de activos del CP-12	65
3.3.2	CONTROL DE AMENAZAS	66
3.3.2.1	Cálculo del riesgo inicial del CP-12	69
3.3.3	DETERMINACIÓN DEL IMPACTO	72
3.3.3.1	Impacto acumulado.....	72
3.3.3.2	Impacto repercutido.....	74
3.3.4	DETERMINACIÓN DEL RIESGO.....	75
3.3.4.1	Riesgo acumulado	77
3.3.4.2	Riesgo repercutido	78
3.3.5	SALVAGUARDAS	80
CAPÍTULO IV		81
DISEÑO E IMPLEMENTACIÓN DEL SGSI.....		81
4.1	DISEÑO DEL SGSI	81
4.1.1.	POLÍTICAS DE SEGURIDAD BASADAS EN OBJETIVOS DE CONTROL.....	81
4.1.1.1.	Política de Seguridad.....	82
4.1.1.2.	Organización de la seguridad de la información	84
4.1.1.3.	Gestión de activos	86
4.1.1.4.	Seguridad de los recursos humanos.....	88
4.1.1.5.	Seguridad física y ambiental (Entorno físico de los activos)	90
4.1.1.6.	Gestión de las comunicaciones y operaciones.....	91
4.1.1.7.	Control de acceso	93
4.1.1.8.	Adquisición, desarrollo y mantenimiento de los sistemas de información	96
4.1.1.9.	Gestión de incidentes en la seguridad de la información	97
4.1.1.10.	Gestión de la continuidad comercial.....	99
4.1.1.11.	Cumplimiento	101
4.2.	ARQUITECTURA DE RED IMPLEMENTADA	103
4.2.1.	REDISTRIBUCIÓN DE DIRECCIONAMIENTO IP	104
4.3.	IMPLEMENTACIÓN DE HERRAMIENTAS	105

4.3.1.	HERRAMIENTAS USADAS EN EL SGSI.....	106
4.3.2.	DESCRIPCIÓN DE HERRAMIENTAS.....	107
4.3.2.1.	Generador de contraseñas RPG	107
4.3.2.2.	Controlador de dominio con Samba 4	108
4.3.2.3.	iTALC.....	110
4.3.2.4.	Nagios3-NCONF	112
4.3.2.5.	OCS Inventory.....	113
4.3.2.6.	OTRS	114
4.3.2.7.	Servidor de archivos con samba 3.....	116
4.3.2.8.	Cobian Backup	117
4.3.2.9.	Truecrypt	118
4.3.2.10.	UTM	119
4.3.2.11.	Puertos utilizados por los servicios implementados	124
4.3.2.12.	Direccionamiento IP utilizado	125
CAPÍTULO V		126
REVISIÓN DEL SGSI.....		126
5.1	POLÍTICAS DE SEGURIDAD IMPLEMENTADAS.....	126
5.2	VERIFICACIÓN DEL FUNCIONAMIENTO DEL CONTROLADOR DE DOMINIO.....	127
5.3	VERIFICACIÓN DEL FUNCIONAMIENTO DE iTALC.....	130
5.4	VERIFICACIÓN DEL FUNCIONAMIENTO DE NAGIOS.....	131
5.5	VERIFICACIÓN DEL FUNCIONAMIENTO DE OCS INVENTORY	131
5.6	VERIFICACIÓN DEL FUNCIONAMIENTO DE OTRS	133
5.7	VERIFICACIÓN DEL FUNCIONAMIENTO DE MRTG.....	135
5.8	VERIFICACIÓN DEL FUNCIONAMIENTO DE COBIAN BACKUP Y TRUECRYPT	137
5.9	VERIFICACIÓN DEL FUNCIONAMIENTO DELUTM	138
CAPÍTULO VI		142
MANUALES DE OPERACIÓN		142
6.1.	CONTROLADOR DE DOMINIO	142
6.2.	iTALC.....	157
6.3.	NAGIOS3-NCONF	166
6.4.	OCS INVENTORY	201
6.5.	OTRS	218

6.6.	SERVIDOR DE ARCHIVOS CON SAMBA 3	240
6.7.	COBIAN	241
6.8.	TRUE CRYPT	247
6.9.	FIREWALL.....	255
6.10.	PROXY	261
6.11.	NTOP.....	267
6.12.	MRTG.....	269
6.13.	IDS/IPS	271
CAPÍTULO VII		274
CONCLUSIONES Y RECOMENDACIONES		274
7.1.	CONCLUSIONES	274
7.2.	RECOMENDACIONES	275
REFERENCIAS BIBLIOGRÁFICAS		277
GLOSARIO DE TÉRMINOS.....		279
ANEXOS		281

ÍNDICE DE FIGURAS

Figura 1. Modelo de desarrollo PDCA	7
Figura 2. Procedimiento del establecimiento del SGSI	11
Figura 3. Procedimiento de implementación y operación del SGSI	12
Figura 4. Procedimiento de monitoreo y revisión del SGSI	13
Figura 5. Procedimiento para mantener y mejorar el SGSI	13
Figura 6. Documentos requeridos por el estándar ISO/IEC 27001	14
Figura 7. Esquema de distribución de subredes por disposición física	24
Figura 8. Topología física de la red del Comando Provincial	25
Figura 9. Mapa distributivo departamental por subredes	26
Figura 10. Gráfico estadístico del indicador Confidencialidad de la Información	48
Figura 11. Gráfico estadístico del indicador Integridad de la Información	49
Figura 12. Gráfico estadístico del indicador Políticas de Seguridad	50
Figura 13. Gráfico estadístico del indicador Clasificación y Control de Valores	51
Figura 14. Gráfico estadístico del indicador Aspectos organizativos para la seguridad	53
Figura 15. Gráfico estadístico del indicador Seguridad Física	55
Figura 16. Esquema base para administración de riesgos	58
Figura 17. Requisitos de desarrollo para objetivos de control	81
Figura 18. Arquitectura de red implementada en el CP-12	103
Figura 19. Generador de claves RPG	107
Figura 20. Circular informativa	127
Figura 21. Políticas del controlador de dominio	128
Figura 22. Selección de política de restricción del panel de control	128
Figura 23. Habilidad de la política de restricción	129
Figura 24. Mensaje de restricción de acceso al panel de control	129
Figura 25. Panel principal del administrador de iTALC	130
Figura 26. Monitoreo de servicios mediante Nagios	131
Figura 27. Recopilación de datos de equipos mediante OCS Inventory	132
Figura 28. Información del equipo UPCFERROCARRIL	132
Figura 29. Información de la red a la que pertenece el equipo	132
Figura 30. Información de Software del equipo	133
Figura 31. Ingreso de datos del usuario de prueba	134
Figura 32. Apertura de ticket de usuario	134
Figura 33. Ticket generado por el usuario	135
Figura 34. Pantalla principal de monitoreo de MRTG	135
Figura 35. Tráfico de entrada y salida de la eth0	136
Figura 36. Respaldo realizado de la carpeta Prueba	137
Figura 37. Reporte de respaldo de Cobian	137
Figura 38. Acceso denegado a páginas restringidas	138
Figura 39. Reporte de navegación del proxy	138
Figura 40. Reporte de navegación generado por Sarg	139
Figura 41. Escaneo de puertos	139

Figura 42. Alerta generada por el IDS	140
Figura 43. Bloqueo realizado por el IPS.....	140
Figura 44. Monitoreo de la red mediante NTOP.....	141
Figura 45. Ventana de configuración de equipo con Windows 7	142
Figura 46. Ingreso de nombre de usuario y clave para administración.	143
Figura 47. Asociación del equipo al dominio	143
Figura 48. Inicio de sesión del usuario administrador	144
Figura 49. Opción: Administración de directivas de grupo	144
Figura 50. Ventana de administración de directivas.....	145
Figura 51. Ventana de ingreso de nombre de equipo y dominio en Windows XP	145
Figura 52. Inicio de sesión de administrador desde Windows XP.....	146
Figura 53. Ejecución del comando dsa.msc.....	146
Figura 54. Ventana de administración de herramientas de AD en Windows XP	146
Figura 55. Ventana principal de Active Directory	147
Figura 56. Menú superior	147
Figura 57. Menú lateral izquierdo	148
Figura 58. Creación de una Unidad Organizativa.....	149
Figura 59. Ingreso de nombre de la Unidad Organizativa.....	150
Figura 60. Unidad Organizativa creada	150
Figura 61. Creación de un usuario.....	151
Figura 62. Ingreso de datos para el nuevo usuario	151
Figura 63. Asignación de contraseña para el nuevo usuario	152
Figura 64. Información de usuario creado	152
Figura 65. Ingreso del nombre del nuevo grupo.....	153
Figura 66. Grupo creado dentro de una unidad organizativa	153
Figura 67. Administración de directivas de grupo	154
Figura 68. Creación de GPO para la Unidad organizativa	154
Figura 69. Ingreso de nombre de la directiva	155
Figura 70. Edición de la directiva creada.....	155
Figura 71. Directivas de grupos.....	155
Figura 72. Selección de directivas	156
Figura 73. Habilitación de directiva.....	156
Figura 74. Logo de la aplicación	157
Figura 75. Pantalla principal de iTALC.....	157
Figura 76. Barra de menú superior	158
Figura 77. Ventana de ingreso de nombre de grupos	161
Figura 78. Ingreso de datos del nuevo ordenador	161
Figura 79. Ventana de capturas de pantalla	162
Figura 80. Ventana de configuración de Italc.....	163
Figura 81. Ventana para ingresar mensajes de texto	164
Figura 82. Ventana para confirmación de acción	164
Figura 83. Ventana de acceso remoto	165
Figura 84. Ventana de soporte técnico	166
Figura 85. Ventana de Autenticación.....	166

Figura 86. Pantalla principal de nagios3.....	167
Figura 87. Información del estado actual de la red.....	168
Figura 88. Funciones de Monitoreo	169
Figura 89. Detalle de Servicios	171
Figura 90. Detalle del estado de host.....	172
Figura 91. Resumen general de grupos de host.....	172
Figura 92. Resumen de estado de grupos de host	173
Figura 93. Estado de la red por grupos de host	174
Figura 94. Información general por grupos de servicios.....	174
Figura 95. Resumen general por grupos de servicios	175
Figura 96. Estado de la red por grupos de servicios.....	175
Figura 97. Mapa de estado.....	176
Figura 98. Nota descriptiva del host	176
Figura 99. Detalle de servicios activos en un host	177
Figura 100.Descarga de archivo para mapa 3D.....	177
Figura 101. Detalle de servicios con problemas.....	178
Figura 102. Detalle de host con problemas	179
Figura 103. Caídas de servicio en la red	179
Figura 104. Búsqueda rápida de host o grupo de host	179
Figura 105. Ingreso de comentarios.....	180
Figura 106.Programación de tiempos de inactividad	181
Figura 107.Programación de tiempos de inactividad en un host	181
Figura 108.Información de procesos de Nagios.....	182
Figura 109.Información del rendimiento de host y servicios.....	183
Figura 110. Paso 1, para crear reportes de estado	184
Figura 111. Paso 2, para crear reportes de estado	184
Figura 112. Paso 3, para crear reportes de estado	184
Figura 113. Paso 1, para crear reportes de disponibilidad	185
Figura 114. Paso 2, para crear reportes de disponibilidad	185
Figura 115. Paso 3, para crear reportes de disponibilidad	186
Figura 116. Reporte de disponibilidad del grupo de host.....	188
Figura 117. Paso 1, para crear histogramas de alertas	189
Figura 118. Paso 2, para crear histogramas de alertas	189
Figura 119. Paso 3, para crear histograma de alertas.....	190
Figura 120. Histograma de alertas de un host	190
Figura 121. Historial de alertas	191
Figura 122. Pantalla principal para el reporte del sumario de alertas.....	192
Figura 123. Reporte estándar del sumario de alertas.....	193
Figura 124. Reporte personalizado del sumario de alertas	194
Figura 125. Listado de Notificaciones	194
Figura 126. Listado de log de eventos.....	195
Figura 127.Selección del objeto para verificar su configuración	196
Figura 128.Pantalla de ingreso a OCS Inventory NG	201
Figura 129. Consola Central de OCS.....	202

Figura 130. Menú de usuario	203
Figura 131. Ventana de distribución de PCs según Etiqueta.....	205
Figura 132. Ventana de distribución por Grupos.....	206
Figura 133. Ventana de descripción de Grupos	206
Figura 134. Ventana de descripción Todos los Programas	207
Figura 135. Búsqueda por varios criterios.....	207
Figura 136. Menú de administrador	209
Figura 137. Creación de un paquete	209
Figura 138. Categorías del Diccionario.....	211
Figura 139. Adicionar un nuevo agente manualmente.....	212
Figura 140. Menú de configuración	212
Figura 141. Solicitudes de registro	213
Figura 142. Solicitudes de Registro	214
Figura 143. Datos administrativos.....	214
Figura 144. Redundancia.....	215
Figura 145. Configuración de la etiqueta	216
Figura 146. Solicitud de Etiqueta al agente.....	216
Figura 147 Gestión de usuarios.....	217
Figura 148. Importación local.....	217
Figura 149. Interfaz web de Agente	218
Figura 150. Ventana de ingreso a la aplicación.....	219
Figura 151. Interfaz web pública	220
Figura 152. Ventana principal de la aplicación	220
Figura 153. Vista panel principal	222
Figura 154. Vista detalle de un ticket.....	223
Figura 155. Vista ventana de servicios	227
Figura 156. Vista de la ventana de FAQ	229
Figura 157. Vista de la ventana de estadísticas	230
Figura 158. Vista de la ventana de preferencias.....	231
Figura 159. Vista del Administrador de cambios	237
Figura 160. Vista de la ventana de mis cambios	238
Figura 161. Vista de la ventana mis órdenes de trabajo.....	239
Figura 162. Vista de la ventana del menú nuevo mensaje	239
Figura 163. Vista de la ventana del menú Tickets bloqueados	240
Figura 164. Crear tarea de respaldo.....	241
Figura 165. Opción Nueva Tarea	241
Figura 166. Selección de archivos a respaldar	243
Figura 167. Selección del horario del respaldo.....	243
Figura 168. Selección de la prioridad del respaldo	244
Figura 169. Opciones de compresión, clave de seguridad y encriptación.	245
Figura 170. Detalles de la nueva tarea creada.....	245
Figura 171. Ejecutar la tarea de respaldo.....	246
Figura 172. Respaldo exitoso de los archivos.....	246
Figura 173. Pantalla de Truecrypt	247

Figura 174. Selección del idioma de la aplicación	248
Figura 175. Ventana de creación de volúmenes	248
Figura 176. Pantalla del Asistente para la creación de Volumen TrueCrypt.....	248
Figura 177. Selección del tipo de volumen	249
Figura 178. Ventana de ubicación del volumen	250
Figura 179. Ventana de opciones de encriptación	250
Figura 180. Selección del tamaño del volumen	251
Figura 181. Ingreso de contraseña	251
Figura 182. Creación exitosa del volumen	252
Figura 183. Salir de la pantalla	252
Figura 184. Ventana de Truecrypt.....	253
Figura 185. Ingreso de contraseña	253
Figura 186. Montaje de unidad de disco duro	254
Figura 187. Volumen montado.....	254
Figura 188. Ventana para salir del sistema	255
Figura 189. Configuración de Webmin.....	256
Figura 190. Configuración del control de acceso IP	256
Figura 191. Vista del panel principal de Shorewall	257
Figura 192. Interfaz de Zonas.....	257
Figura 193. Creación de Zona de Red.....	257
Figura 194. Edición de Zona de Red	258
Figura 195. Vista del panel de Interfaces	258
Figura 196. Creación de Interfaz de Red	259
Figura 197. Vista del panel de Políticas.....	259
Figura 198. Creación de una política	260
Figura 199. Vista del panel de Reglas.....	261
Figura 200. Vista del panel de Hosts de Zona	261
Figura 201. Vista del panel principal de SquidGuard	262
Figura 202. Vista del panel de Source Groups	262
Figura 203. Vista de ventana de edición de los SourceGroup.....	263
Figura 204. Adición de un nuevo host.....	263
Figura 205. Eliminación de un host	264
Figura 206. Vista de las Listas de Control de Acceso.....	265
Figura 207. Edición de las ACL de un SourceGroup.....	265
Figura 208. Vista del panel del Servidor Proxy Squid	266
Figura 209. Vista del generador de informes de análisis de Squid	267
Figura 210. Interfaz de Ntop	268
Figura 211. Distribución de Tráfico	268
Figura 212. Troughput de la red.....	269
Figura 213. Página de inicio de la aplicación.....	269
Figura 214. Análisis de tráfico de las interfaces	270
Figura 215. Análisis de tráfico de la interfaz	270
Figura 216. Pantalla principal de SNORTTREPORT	271
Figura 217. Estadísticas de alertas por tipo de tráfico	272

Figura 218. Tabla de alertas detectadas	272
Figura 219. Listado de alertas	273
Figura 220. Detalle de eventos producidos desde IP origen.....	273
Figura 221. Paquete de herramientas de administración para Windows XP	304
Figura 222. Ejecución del paquete de herramientas	304
Figura 223. Proceso de instalación del paquete	305
Figura 224. Inicio de instalación del paquete	305
Figura 225. Progreso de la instalación	305
Figura 226. Finalización de la instalación	306
Figura 227. Paquete de herramientas de administración para Windows 7.....	306
Figura 228. Asistente para la instalación de herramientas de administración.....	307
Figura 229. Términos de licencia del software de Microsoft.....	307
Figura 230. Inicio de la instalación del paquete.....	307
Figura 231. Instalación terminada.....	308
Figura 232. Herramientas administrativas	308
Figura 233. Componentes necesarios para la instalación de iTALC.....	310
Figura 234. Ventana de error debido a que no se han agregado clases.....	311
Figura 235. Ventana de error debido a la no generación de claves.....	311
Figura 236. Ventana de error debido a la no configuración de claves.....	312
Figura 237. Ventana principal de iTALC master	315
Figura 238. Clave pública del maestro de Linux.....	316
Figura 239. Cambio de nombre y extensión a la clave pública del maestro.....	316
Figura 240. Clave pública con extensión .pub.....	316
Figura 241. Pantalla de inicio de instalación de Italc	317
Figura 242. Términos de la licencia de Italc	317
Figura 243. Ubicación de la instalación.....	318
Figura 244. Creación del directorio de instalación.....	318
Figura 245. Selección del cliente iTALC	318
Figura 246. Opciones de importación de clave pública	319
Figura 247. Ubicación de la clave pública	319
Figura 248. Servicio ITALC registrado.....	320
Figura 249. Instalación Finalizada	320
Figura 250. Contraseña del administrador de Nagios.....	321
Figura 251. Instalación de NCONF vía web	322
Figura 252. Ingreso de información de la base de datos	323
Figura 253. Ingreso de directorios	323
Figura 254. Instalación completa de Nconf.....	324
Figura 255. Verificación del estado de los servicios: OK.....	326
Figura 256. Verificación del estado de los servicios: Critical	326
Figura 257. Proceso de instalación de OCS Inventory.....	327
Figura 258. Verificación de la base de datos.....	328
Figura 259. Instalación de OCS Inventory completada	328
Figura 260. Ingreso a la aplicación con el usuario y clave por defecto	328
Figura 261. Ejecución del cliente OCS	329

Figura 262. Selección de la ubicación del cliente OCS	329
Figura 263. Proceso de instalación del cliente OCS	330
Figura 264. Proceso previo a la instalación de OCS Inventory	330
Figura 265. Inicio de la instalación del agente OCS.....	331
Figura 266. Licencia General Pública de OCS Inventory.....	331
Figura 267. Ingreso de IP del servidor OCS Inventory	332
Figura 268. Ubicación del agente OCS	332
Figura 269. Proceso de instalación de los archivos del agente OCS	333
Figura 270. Instalación completa del agente OCS.....	333
Figura 271. Instalación de OTRS vía web	336
Figura 272. Primer paso de la instalación de OTRS.....	336
Figura 273. Creación de la base de datos para OTRS.....	336
Figura 274. Configuración de la base de datos de OTRS.....	337
Figura 275. Creación satisfactoria de la base de datos	337
Figura 276. Configuración del sistema de OTRS.....	338
Figura 277. Datos informativos para el ingreso a OTRS.....	338
Figura 278. Error de ingreso a OTRS.....	339
Figura 279. Selección del idioma en la instalación de Cobian Backup.....	341
Figura 280. Licencia de Cobian Backup	341
Figura 281. Tipo de instalación Cobian Backup.....	342
Figura 282. Instalación Cobian Back completa.....	342
Figura 283. Archivo descargado con formato .exe	343
Figura 284. Inicio de la instalación	343
Figura 285. Selección del modo de instalación	344
Figura 286. Ubicación de los archivos de TrueCrypt.....	344
Figura 287. Progreso de la instalación de TrueCrypt	345
Figura 288. Instalación de la aplicación finalizada	345
Figura 289. Fin de la instalación	345
Figura 290. Reglas aplicadas en el firewall.....	350
Figura 291. Mensaje de error al ingresar a NTOP	366

ÍNDICE DE TABLAS

Tabla 1. Objetivos de control del anexo A de la norma ISO/IEC 27001	17
Tabla 2. Cláusulas del estándar ISO/IEC 27002:2005	19
Tabla 3. Direccionamiento IP de la red del Comando Provincial	27
Tabla 4. Equipos de red	27
Tabla 5. Estaciones de trabajo de la Comandancia	34
Tabla 6. Estación de trabajo de la Prevención	34
Tabla 7. Estaciones de trabajo de la Jefatura Financiera	35
Tabla 8. Estación de trabajo de Compras Públicas.....	36
Tabla 9. Estaciones de trabajo del departamento de Operaciones.....	37
Tabla 10. Estaciones de trabajo de Asuntos Internos	38
Tabla 11. Estaciones de trabajo de Relaciones Públicas	38
Tabla 12. Estaciones de trabajo de Policía Comunitaria	39
Tabla 13. Estaciones de trabajo de la Región Norte	40
Tabla 14. Estaciones de trabajo de recursos humanos.....	41
Tabla 15. Estaciones de trabajo de Recursos Logísticos	41
Tabla 16. Estaciones de trabajo de Asesoría Jurídica.....	42
Tabla 17. Estaciones de trabajo de Rastrillo	43
Tabla 18. Estaciones de trabajo de Inteligencia.....	43
Tabla 19. Estaciones de trabajo del departamento de Sistemas	44
Tabla 20. Resultados del indicador Confidencialidad de la Información	47
Tabla 21. Resultados del indicador Integridad de la Información	48
Tabla 22. Resultados del indicador Políticas de seguridad	50
Tabla 23. Resultados del indicador Clasificación y Control de Valores.....	51
Tabla 24. Resultados del indicador Aspectos organizativos para la seguridad.....	52
Tabla 25. Resultados del indicador Seguridad Física.....	54
Tabla 26. Valoración de activos.....	60
Tabla 27. Datos usados dentro de la institución.....	61
Tabla 28. Aplicaciones usadas en los diferentes departamentos	62
Tabla 29. Equipos informáticos pertenecientes al CP-12.....	63
Tabla 30. Equipamiento auxiliar del CP-12.....	63
Tabla 31. Redes de comunicaciones del CP-12	64
Tabla 32. Ubicación de las instalaciones del CP-12.....	64
Tabla 33. Personal del Departamento de Sistemas del CP-12	64
Tabla 34. Valoración de activos del CP-12	65
Tabla 35. Valores de degradación de un activo	67
Tabla 36. Valores representativos de frecuencia de amenazas en activos.....	68
Tabla 37. Niveles de valoración del riesgo	68
Tabla 38. Cuadro indicativo del nivel de madurez de una institución	71
Tabla 39. Valoración de impactos	72
Tabla 40. Valores del impacto acumulado en los activos dependientes	74
Tabla 41. Valores del impacto repercutido en los activos independientes	75
Tabla 42. Determinación del riesgo dentro del CP-12	76

Tabla 43. Objetivo, alcance y controles de la política de seguridad	83
Tabla 44. Objetivo, alcance y controles de la política de organización	85
Tabla 45. Objetivo, alcance y controles de la política de gestión de activos	87
Tabla 46. Objetivo, alcance y controles de la política de seguridad de Recursos Humanos	88
Tabla 47. Objetivo, alcance y controles de la política de seguridad física y ambiental	90
Tabla 48. Objetivo, alcance y controles de la política comunicaciones y operaciones.....	92
Tabla 49. Objetivo, alcance y controles de la política de control de acceso.....	94
Tabla 50. Objetivo, alcance y controles de la política de los sistemas de información	96
Tabla 51. Objetivo, alcance y controles de la política de gestión de incidentes.....	98
Tabla 52. Objetivo, alcance y controles de la política de gestión de continuidad	99
Tabla 53. Objetivo, alcance y controles de la política de cumplimiento.....	101
Tabla 54. Redistribución del direccionamiento IP.....	105
Tabla 55. Herramientas implementadas dentro del SGSI	106
Tabla 56. Información actualizada de la aplicación iTALC.....	111
Tabla 57. Información actual del software.....	114
Tabla 58. Información actual de Cobian Backup.....	118
Tabla 59. Información actual de TrueCrypt.....	119
Tabla 60. Puertos utilizados por las herramientas implementadas.....	125
Tabla 61. Direccionamiento IP utilizado con fines demostrativos	125
Tabla 62. Opciones del menú superior	148
Tabla 63. Descripción de las opciones del menú superior	159
Tabla 64. Opciones de menú lateral.....	160
Tabla 65. Comandos aplicados a los host.....	199
Tabla 66. Comandos aplicados a los servicios.....	200
Tabla 67. Comandos aplicados a los procesos	200
Tabla 68. Revisión de parámetros sobre los Equipos.....	204
Tabla 69. Grupos predeterminados de administración de OTRS	232
Tabla 70. Permisos disponibles para usuarios de OTRS.....	233

ÍNDICE DE ECUACIONES

Ecuación 1. Fórmula de muestreo.....	45
Ecuación 2. Ecuación de cálculo de riesgo	69
Ecuación 3. Ecuación general de cálculo del riesgo inicial.....	70
Ecuación 4. Cálculo total del riesgo inicial	70
Ecuación 5. Ecuación de cálculo del impacto acumulado.....	73
Ecuación 6. Ecuación de cálculo del riesgo acumulado	77
Ecuación 7. Cálculo del riesgo acumulado debido a incidentes en los activos el CP-12.....	78
Ecuación 8. Cálculo del riesgo acumulado debido a accesos no autorizados en los activos del CP-12.....	78
Ecuación 9. Ecuación de cálculo del riesgo repercutido	79
Ecuación 10. Cálculo del riesgo repercutido debido a incidentes en los activos el CP-12.....	79
Ecuación 11. Cálculo del riesgo repercutido debido a accesos no autorizados en los activos el CP-12.....	79
Ecuación 12. Cálculo de riesgo del Convertidor TP-LINK	296
Ecuación 13. Cálculo de riesgo del Router ADSL.....	296
Ecuación 14. Cálculo de riesgo del Servidor Proxy.....	296
Ecuación 15. Cálculo de riesgo del router Mikrotik.....	296
Ecuación 16. Cálculo de riesgo del Switch D-Link	296
Ecuación 17. Cálculo de riesgo de la antena.....	297
Ecuación 18. Cálculo de riesgo del Nano Station.....	297
Ecuación 19. Cálculo de riesgo de PC's de escritorio	297
Ecuación 20. Cálculo de riesgo del UPS Central.....	297
Ecuación 21. Cálculo de riesgo del generador eléctrico	297
Ecuación 22. Cálculo de riesgo de Impresoras multifunción	297
Ecuación 23. Cálculo de riesgo de Impresoras láser	298
Ecuación 24. Cálculo de riesgo de las copadoras.....	298

RESUMEN

Un Sistema de Gestión de la Seguridad de la Información (SGSI), es un sistema dinámico en constante evolución que debe ser evaluado y monitoreado, con métricas establecidas que permitan comparar de manera consciente y objetiva escenarios diferentes y tomar decisiones con respecto a los riesgos que se afrontan y los recursos que se invierten dentro de una organización.

Es necesario entonces lograr una metodología que conduzca a una solución eficaz y eficiente, desde el punto de vista técnico y económico, que provea los niveles de seguridad requeridos y brinde la confianza necesaria a una organización. Esta metodología deberá considerar aspectos como aplicaciones y servicios, así como el uso eficiente de los recursos tecnológicos como soporte de estos procesos. El presente proyecto aborda la problemática que se plantea al momento de implantar y gestionar un SGSI, tal como se define en la norma ISO/IEC 27000, para una Organización. Además, contempla los controles que deben ser implantados y las herramientas de gestión desarrolladas sobre software libre.

ABSTRACT

A Management System of Information Security (ISMS), is an evolving dynamic system that must be evaluated and monitored, with established metric for comparing consciously and objectively different scenarios and make decisions regarding the risks being faced and the resources invested in an organization.

It is therefore necessary to achieve a methodology that leads to an effective and efficient solution, since technically and economically, to provide the required security levels and provide the necessary confidence to an organization. This methodology should consider issues such as applications and services, and the efficient use of technology resources to support these processes. This project tackles the problem that arises when implementing and managing an ISMS as defined in ISO / IEC 27001, for an organization. Also provides controls to be implemented and the management tools built on free software.

PRESENTACIÓN

El Comando Provincial de Policía “Imbabura No 12” es una institución de carácter público que maneja información confidencial y de vital importancia por lo cual es fundamental que los recursos de red sean gestionados de manera eficaz.

La implementación del SGSI surge ante la necesidad de contar con un proceso sistemático, que sea conocido por toda la institución y que contenga tanto la documentación de políticas para el manejo de la información así como la utilización de herramientas que permitan dar soporte a usuarios.

El Sistema de Gestión de Seguridad de la Información es un conjunto de procesos orientado a establecer, implementar, operar, controlar, revisar, mantener y mejorar la seguridad de la información para garantizar su confidencialidad, integridad y disponibilidad. Este sistema establece un enfoque controlado para manejar la información sensible de la institución de forma que se mantenga segura cumpliendo con los requisitos de la norma ISO/IEC 27001:2005.

Además, con la implementación del SGSI se contribuye a mejorar la imagen de la institución al mostrar que se toman medidas para garantizar la seguridad de la información.

Una adecuada gestión de la seguridad de la información ayuda a disminuir los riesgos que la institución soporta y minimiza los daños en los activos de información, si alguno de los riesgos llega a materializarse.

CAPÍTULO I

FUNDAMENTO TEÓRICO

Dentro del presente capítulo se estudia la fundamentación teórica de la norma ISO¹/IEC² 27000 y los estándares derivados de ésta, que tienen como principio el desarrollo e implementación de un SGSI³, estos estándares son: 27001 y 27002. Además se explica el modelo PDCA⁴ en el cual está basada la norma ISO 27001, así como también los controles aplicables y requerimientos necesarios para el establecimiento e implementación del SGSI.

1.1 NORMA ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO e IEC, que proporcionan un marco de gestión de seguridad de la información, utilizable por cualquier tipo de organización pública o privada, grande o pequeña.

La norma ISO 27000 comprende un amplio rango de numeración para los estándares, que va desde 27000 a 27019 y de 27030 a 27044.

Para el caso de desarrollo del proyecto propuesto se toma en consideración el estudio de los estándares 27001 y 27002 que están directamente relacionados

¹ISO (International Standard Organization): Organización Internacional de Estandarización. Organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

²IEC (International Electrotechnical Commission): Comisión Electrotécnica Internacional. Organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas.

³SGSI: Sistema de Gestión de Seguridad de la Información. Proceso sistemático, documentado y conocido por toda la organización que se encarga de gestionar y mejorar la seguridad de la información.

⁴ PDCA: Plan, Do, Check, Act. Modelo de desarrollo del SGSI.

con la implementación y controles del Sistema de Gestión de Seguridad de la Información.

El estándar ISO 27002 es un conjunto de buenas prácticas en seguridad de la información. Contiene controles aplicables en relación a la gestión de la continuidad de actividades, la gestión de incidentes de seguridad, control de accesos o regulación de las actividades del personal interno o externo, que ayudan a la organización a implantar medidas que reduzcan sus riesgos en cuanto a seguridad de la información, mientras que el estándar ISO 27001 contiene un anexo A, que considera los controles del estándar ISO 27002 para su posible aplicación en el SGSI que implante cada organización; de esta manera existe una relación de controles necesarios para garantizar la seguridad de la información.

En el caso del estándar ISO 27005 que se refiere a Gestión de Riesgos, no es aplicable en este proyecto debido a que únicamente proporciona directrices y se apoya en los conceptos generales publicados en el estándar 27001 para asegurar el buen desempeño de los controles implantados dentro de una organización.

Sin embargo el análisis de riesgos necesario para conocer el grado de madurez de la institución se lo realiza haciendo uso de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) que proporciona una ayuda para detectar y planificar las medidas oportunas para mantener los riesgos bajo control.

1.1.1 TÉRMINOS Y DEFINICIONES

La norma ISO 27000 contiene términos y definiciones relacionados con la gestión y seguridad de la información que se emplean en toda la serie. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

Los términos más utilizados dentro de la norma ISO 27000 y que se mencionan en los estándares posteriormente descritos, están definidos a continuación con la finalidad de no obtener varios conceptos para un mismo término:

- **Activo:** Cualquier cosa que tenga valor para la organización.
- **Amenaza.-** Evento que puede provocar un incidente en la organización produciendo daños o pérdidas materiales y/o inmateriales.
- **Disponibilidad:** La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
- **Confidencialidad:** La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.
- **Integridad:** La propiedad de salvaguardar la exactitud e integridad de los activos.
- **Seguridad de información:** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

- **Evento de seguridad de la información:** Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.
- **Incidente de seguridad de la información:** Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.
- **SGSI:** La parte del sistema gerencial general, basado en un enfoque de riesgo institucional; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Análisis de riesgo:** Uso sistemático de la información para identificar fuentes y para estimar el riesgo.
- **Evaluación del riesgo:** Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
- **Tratamiento del riesgo:** Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.
- **Vulnerabilidad:** Susceptibilidad de algo para absorber negativamente incidencias externas.
- **Propietario:** Identifica a la persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento,

uso y seguridad de los activos. El término propietario no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

- **Enunciado de aplicabilidad:** Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.
- **Control:** Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.
- **Lineamiento:** Una descripción que aclara qué se debe hacer y cómo, para lograr los objetivos establecidos en las políticas.
- **Medios de procesamiento de la información:** Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.
- **Política:** Intención y dirección general expresada formalmente por la gerencia.
- **Riesgo:** Combinación de la probabilidad de un evento y su ocurrencia.

1.2 ESTÁNDAR INTERNACIONAL ISO/IEC 27001

Este estándar fue publicado el 15 de Octubre de 2005 por la ISO e IEC que conforman un sistema especializado para la estandarización universal. Es la norma principal de la serie ISO 27000 y contiene los requisitos de implementación del sistema de gestión de seguridad de la información.

El estándar ha sido preparado para proporcionar un modelo que permite establecer, implementar, monitorear, revisar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización.

1.2.1 ENFOQUE DEL PROCESO

El enfoque del proceso para la gestión de la seguridad de la información de este estándar fomenta que los usuarios enfatizen la importancia de:

- a) Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la misma;
- b) Implementar y operar controles para manejar los riesgos de la seguridad de la información;
- c) Monitorear y revisar el desempeño y la efectividad del SGSI; y
- d) Mejoramiento continuo en base a la medición del objetivo.

Este estándar internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI. PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase Actuar lleva de nuevo a la fase de Planificar para iniciar un nuevo ciclo de las cuatro fases.

La *Figura 1* muestra cómo se desarrolla el proceso de implantación de un SGSI:



Figura 1. Modelo de desarrollo PDCA

Fuente: <http://www.gestion-calidad.com/implantacion-iso-27001.html>

A continuación se detalla cada una de las fases del modelo PDCA:

- **Planificar (Plan)**

Dentro de esta fase se establecen políticas, objetivos, procesos y procedimientos relevantes para manejar el riesgo y mejorar la seguridad de la información. Se debe definir una política de seguridad que considere los requerimientos legales relativos a la seguridad de la información; además debe establecerse los criterios con los que se va a evaluar el riesgo y finalmente debe ser aprobada por la dirección o gerencia.

Aquí se define una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos de la institución, además de establecer los

criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable.

- **Hacer (Do)**

En esta fase se seleccionan e implementan los controles que reduzcan el riesgo a los niveles considerados como aceptables.

Se debe efectuar el cambio y/o las pruebas proyectadas según la decisión que se haya tomado y la planificación que se ha realizado.

- **Verificar (Check)**

Una vez realizada la acción e implantado el control, se debe verificar, evaluar y medir el desempeño del proceso en comparación con la política, objetivos, experiencias prácticas y reportar los resultados a la gerencia para su revisión.

- **Actuar (Act)**

Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar la forma de proceder, además es importante tener la seguridad de que las mejoras introducidas alcanzan los objetivos previstos.

1.2.2 ALCANCE DEL ESTÁNDAR

Este estándar internacional abarca todos los tipos de organizaciones, por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro.

Especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos generales de la organización.

El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

1.2.3 REFERENCIAS NORMATIVAS

El estándar internacional ISO/IEC 27001:2005 está basado en la norma ISO/IEC 17799:2005, cuyo contenido trata sobre: Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información.

1.2.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Definición de SGSI

Según la norma ISO 27000, en su página web define que:

Un SGSI es un Sistema de Gestión de la Seguridad de la Información, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita, de su origen o de la fecha de elaboración. Esta gestión debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Un SGSI es el modo más eficaz de conseguir que los riesgos se minimicen, asegurar la continuidad adecuada de las actividades de la institución hasta en los casos más extremos y de adaptar la seguridad a los cambios continuos que se producen en la organización y en su entorno. Aunque nunca se logre la seguridad total, es posible acercarse a ella mediante una mejora continua.

1.2.4.1. Requerimientos generales

La institución debe establecer, implementar, operar, monitorear, mantener y mejorar continuamente un SGSI documentado, es decir que todas las políticas establecidas, procedimientos de administración y el uso de las herramientas de gestión deben estar reflejadas de manera escrita, dentro del contexto de las actividades generales de la organización. Para propósitos de este estándar, los procesos utilizados se basan en el modelo PDCA.

1.2.4.2. Establecer y manejar el SGSI

- **Establecer el SGSI**

La *Figura 2* muestra los pasos a seguir para establecer el SGSI:

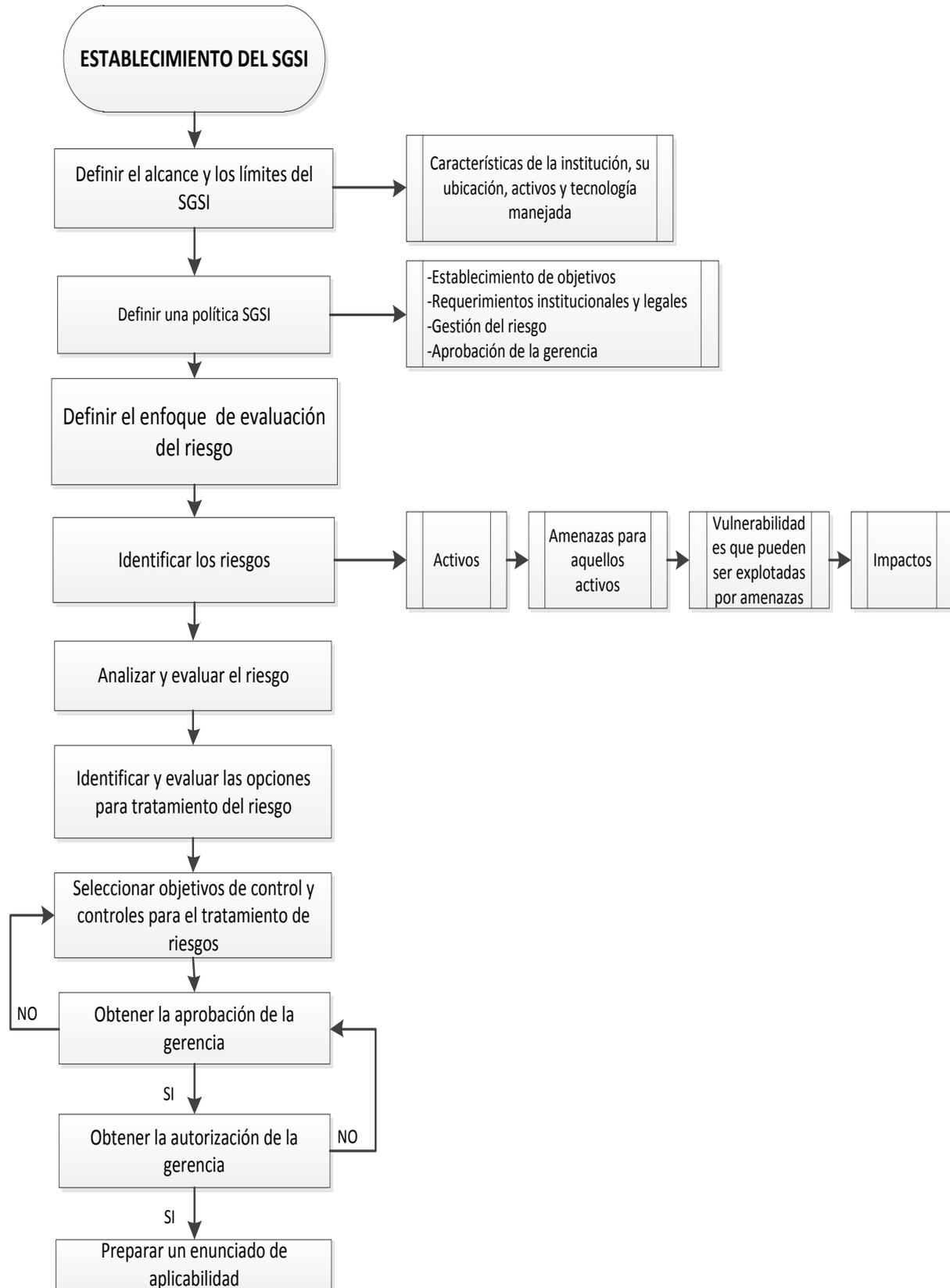


Figura 2. Procedimiento del establecimiento del SGSI
Fuente: <http://www.iso27000.es/>

- **Implementar y operar el SGSI**

En la *Figura 3* se muestra la manera en la que se debe implementar y operar el SGSI:

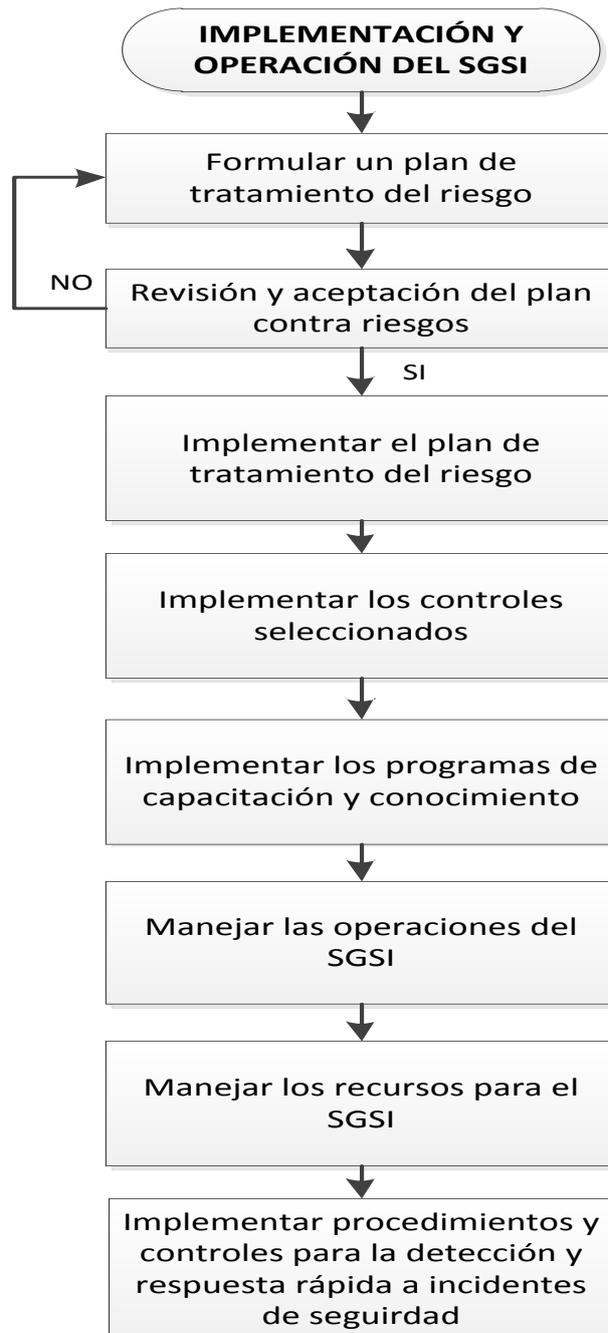


Figura 3. Procedimiento de implementación y operación del SGSI

Fuente: <http://www.iso27000.es/>

- **Monitorear y revisar el SGSI**

La *Figura 4* indica el procedimiento para monitorear y revisar el SGSI:

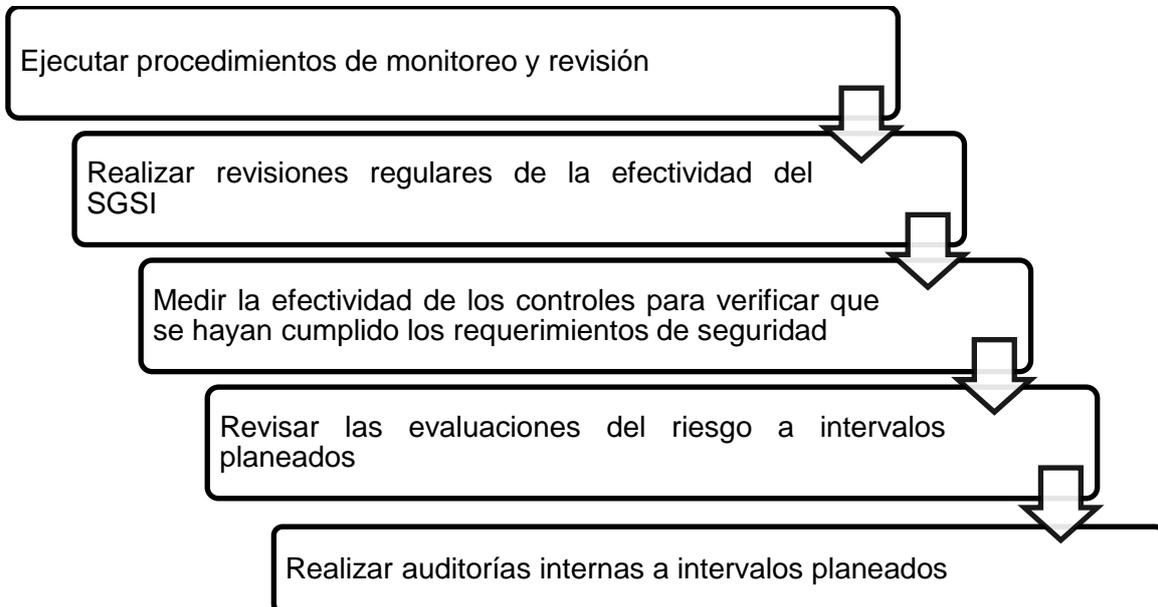


Figura 4. Procedimiento de monitoreo y revisión del SGSI

Fuente: <http://www.iso27000.es>

- **Mantener y mejorar el SGSI**

En la *Figura 5* se muestran las acciones que se deben tomar semestralmente para mantener y mejorar el SGSI:

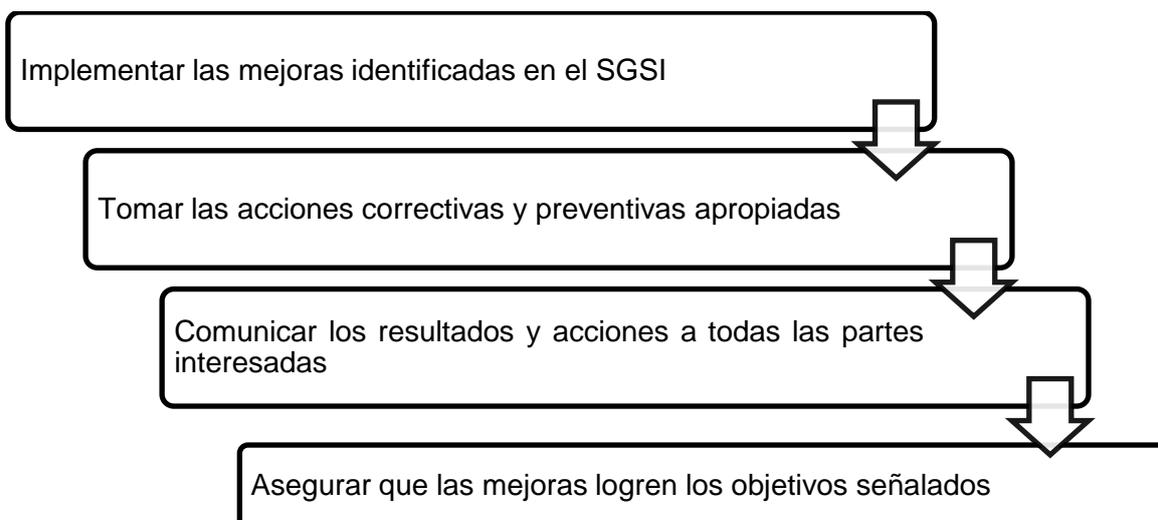


Figura 5. Procedimiento para mantener y mejorar el SGSI

Fuente: <http://www.iso27000.es/>

1.2.4.3. Requerimientos de documentación

- **General**

La documentación SGSI debe incluir lo siguiente:

- a) Enunciados documentados de la política SGSI y los objetivos;
- b) Alcance del SGSI;
- c) Procedimientos y controles de soporte del SGSI;
- d) Descripción de la metodología de evaluación del riesgo;
- e) Reporte de evaluación del riesgo;
- f) Plan de tratamiento del riesgo;
- g) Los procedimientos documentados necesarios por la organización
- h) Registros requeridos por este Estándar Internacional

La *Figura 6* muestra los documentos requeridos por este estándar:

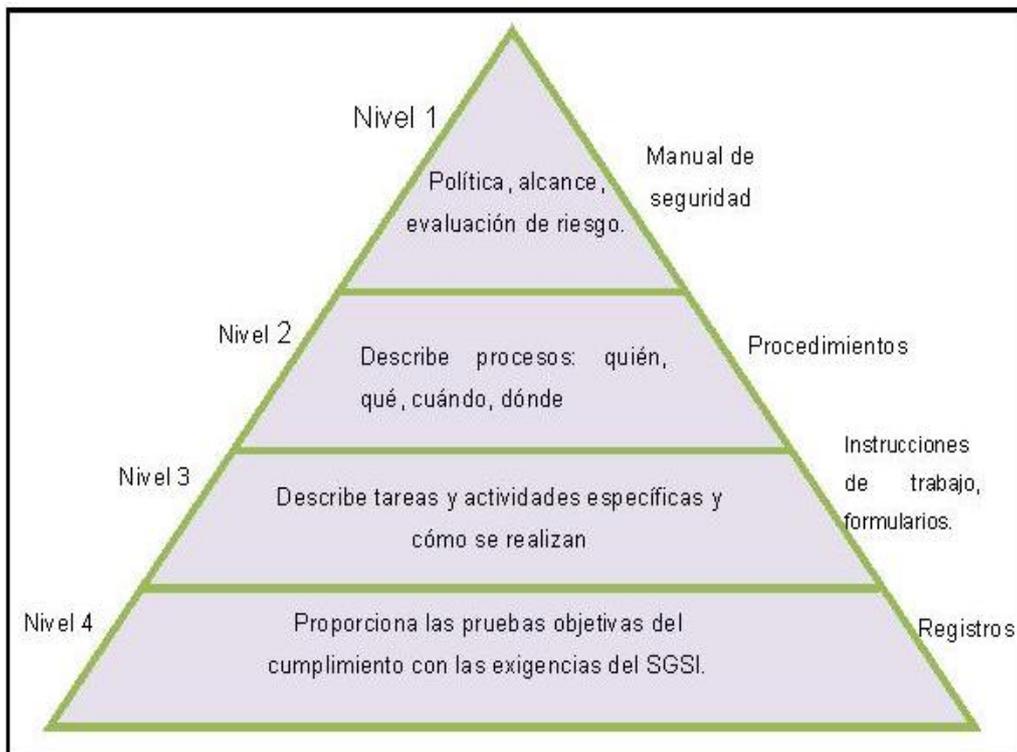


Figura 6. Documentos requeridos por el estándar ISO/IEC 27001

Fuente: http://1236_Carlos_Manuel_Aenor.pdf

1.2.5 RESPONSABILIDAD DE LA GERENCIA

- **Compromiso de la gerencia**

La gerencia debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al establecer una política SGSI, asegurar que se establezcan objetivos y planes SGSI.

- **Gestión de recursos**

- a) Provisión de recursos**

La organización debe determinar y proporcionar los recursos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI y brindar una seguridad adecuada mediante la correcta aplicación de todos los controles implementados llevando a cabo revisiones cuando sean necesarias.

- b) Capacitación, conocimiento y capacidad**

La organización debe asegurar que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas.

1.2.6 AUDITORÍAS INTERNAS SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar si los objetivos de control y procedimientos del SGSI cumplen con

los requerimientos de este estándar internacional, la legislación y regulaciones a las que está sometida la norma ISO 27000.

1.2.7 MEJORAMIENTO DEL SGSI

- **Mejoramiento continuo**

La organización debe mejorar continuamente la efectividad del SGSI a través del uso de políticas de seguridad de la información, objetivos de seguridad de la información, resultados de auditoría, análisis de los eventos monitoreados, acciones correctivas y preventivas, y la revisión gerencial.

- **Acción correctiva**

La organización debe realizar las acciones para eliminar la causa de las no-conformidades con los requerimientos del SGSI para poder evitar la recurrencia.

- **Acción preventiva**

La organización debe determinar la acción para eliminar la causa de las no-conformidades potenciales de los requerimientos SGSI para evitar su ocurrencia.

1.2.8 OBJETIVOS DE CONTROL Y CONTROLES

- **Anexo A (Normativo)**

Los objetivos de control y los controles de este anexo deben seleccionarse como parte del proceso SGSI.

Las cláusulas enumeradas desde A5 a A15 proporcionan lineamientos para la implementación de las mejores prácticas en soporte de los controles.

La *Tabla 1* muestra los principales objetivos de control aplicables al desarrollo e implementación del SGSI:

Tabla 1. Objetivos de control del anexo A de la norma ISO/IEC 27001

Fuente: <http://www.iso27000.es>

ANEXO	OBJETIVO DE CONTROL
A.5.	Política de seguridad
A.6.	Organización de la seguridad de la información
A.7.	Gestión de activos
A.8.	Seguridad de los recursos humanos
A.9.	Seguridad física y ambiental
A.10.	Gestión de las comunicaciones y operaciones
A.11.	Control de acceso
A.12.	Adquisición, desarrollo y mantenimiento de los sistemas de información
A.13.	Gestión de incidentes en la seguridad de la información
A.14.	Gestión de la continuidad comercial
A.15.	Cumplimiento

1.3 ESTÁNDAR INTERNACIONAL ISO/IEC 27002

Es una guía de buenas prácticas que fue publicada el 1 de Julio de 2007 basándose en la norma ISO 17799:2005 por lo que mantiene a 2005 como año de edición y describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es una norma certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

El objetivo del estándar ISO/IEC 27002:2005 es servir de guía a los responsables de la implementación de seguridad de la información de una organización. En este estándar se describe cada uno de los 11 dominios referentes a la seguridad de la información.

Los objetivos de control y los controles, deben ser implementados para satisfacer los requisitos identificados por la evaluación de riesgos, de esta manera se logra una práctica eficaz de gestión de la seguridad.

1.3.1 ALCANCE DEL ESTÁNDAR

Este estándar internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Sirve como un lineamiento práctico para desarrollar estándares de seguridad organizacional, prácticas de gestión de seguridad efectivas y para ayudar a crear confianza en las actividades inter-organizacionales.

1.3.2 CLÁUSULAS

Cada cláusula contiene un número de categorías de seguridad principales.

La *Tabla 2*, muestra las once cláusulas cada una acompañada por el número de objetivos de control principales:

Tabla 2. Cláusulas del estándar ISO/IEC 27002:2005

Fuente: <http://www.iso27000.es>

CLÁUSULA o DOMINIOS	# OBJETIVOS DE CONTROL
Política de Seguridad	1
Organización de la Seguridad de la Información	2
Gestión de Activos	2
Seguridad de Recursos Humanos	3
Seguridad Física y Ambiental (Entorno físico)	2
Gestión de Comunicaciones y Operaciones	10
Control de Acceso	7
Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	6
Gestión de Incidentes de Seguridad de la Información	2
Gestión de la Continuidad Comercial	1
Cumplimiento	3

1.3.2.1. Política de seguridad

Esta cláusula se enfoca en brindar apoyo y orientación a la gerencia o dirección, con respecto a la seguridad de la información, de acuerdo con los requisitos de la institución y los reglamentos y leyes pertinentes.

1.3.2.2. Organización de la Seguridad de la Información

Está orientada a gestionar y mantener la seguridad de la información y de los servicios de procesamiento de información a los cuales tienen acceso.

1.3.2.3. Gestión de Activos

El objetivo de la cláusula es mantener la protección adecuada de los activos de la institución y asegurar que la información reciba el nivel de protección adecuado.

1.3.2.4. Seguridad de Recursos Humanos

Este punto trata de asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones para las cuales están considerados.

1.3.2.5. Seguridad Física y Ambiental (Entorno físico)

Esta cláusula hace referencia a evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la institución.

1.3.2.6. Gestión de Comunicaciones y Operaciones

Se refiere a asegurar la operación correcta de los servicios de procesamiento de información para minimizar el riesgo de fallas en los sistemas manteniendo la integridad y disponibilidad de la información.

1.3.2.7. Control de Acceso

Esta cláusula permite controlar el acceso a la información con base en los requisitos de seguridad y de la institución evitando el acceso no autorizado a los servicios de red.

1.3.2.8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

Este punto hace referencia a que se debe garantizar que la seguridad es parte integral de los sistemas de información.

1.3.2.9. Gestión de Incidentes de Seguridad de la Información

Esta cláusula asegura que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

1.3.2.10. Gestión de la Continuidad Comercial

Este punto considera la disminución de interrupciones en las actividades de la institución para proteger los procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

1.3.2.11. Cumplimiento

Se refiere a evitar el incumplimiento de normativas legales, estatutos y requisitos de seguridad que se encuentre en vigencia dentro de la institución.

CAPÍTULO II

SITUACIÓN ACTUAL DE LA RED DE DATOS

En el capítulo 2 se realiza un análisis de la situación actual de la red de datos del Comando Provincial de Policía “Imbabura” No. 12, aquí se incluye la topología física de la red interna además de una descripción de los departamentos que se encuentran dentro del CP-12⁵ y de los equipos que conforman la infraestructura tecnológica. Se muestra también en detalle la encuesta aplicada al personal para evidenciar las falencias presentes en la institución.

2.1 ANÁLISIS DEL ESTADO ACTUAL DE LA ENTIDAD

El Departamento de Sistemas es el encargado de la administración y gestión de la red de datos del Comando Provincial de Policía “Imbabura No. 12”. El personal encargado de la administración de la red pertenece a la institución.

El Comando cuenta con una LAN⁶ inalámbrica que tiene poco tiempo de implementación y en la actualidad no posee mecanismos que garanticen la seguridad tanto a nivel de red como de información. Esta institución maneja información relevante en cada uno de sus diferentes departamentos, pero no existe ningún reglamento o documento que contenga la manera en la que se deben operar los diferentes recursos de la infraestructura tecnológica.

⁵ CP-12: Comando Provincial de Policía “Imbabura No. 12. Institución estatal de carácter civil y altamente especializada, cuya misión es atender la seguridad ciudadana, el orden público y proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional.

⁶ LAN (Local Area Network): Red de área Local. Es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros.

El personal que labora en los diferentes departamentos es rotativo, razón por la cual nadie toma precauciones al momento de manejar documentos o la información misma, además un gran porcentaje de las personas que se encuentran en oficinas desconoce cómo debe utilizar los equipos informáticos y recursos físicos de red.

Por ser una red nueva, no cuenta con la infraestructura tecnológica apropiada en lo referente a equipamiento, para la implementación del proyecto propuesto, sin embargo la implementación de las distintas herramientas se dimensiona en base a la disponibilidad de equipos dentro del CP-12.

La adquisición de nuevos equipos para la red se ve limitado por el aspecto económico, razón por la cual no se ha considerado esta inversión.

Sin embargo, después de implantado el proyecto y de los resultados que se obtengan se pondrá a consideración de las principales autoridades del CP-12, la adquisición de equipos que cumplan con los requerimientos necesarios para la implementación de nuevos proyectos haciendo énfasis en la importancia de estos equipos a futuro.

2.2 TOPOLOGÍA FÍSICA DE LA RED INTERNA

El Comando Provincial de Policía “Imbabura No 12” cuenta con una red inalámbrica interna para proporcionar el servicio de acceso a la Internet a sus 15 departamentos principales, tiene un enlace de 2 Mbps, que es distribuido

mediante la asignación de subredes, las mismas que están divididas de acuerdo a la disposición física de los departamentos dentro del Comando Provincial.

La *Figura 7* muestra la distribución de las subredes dentro de la institución:

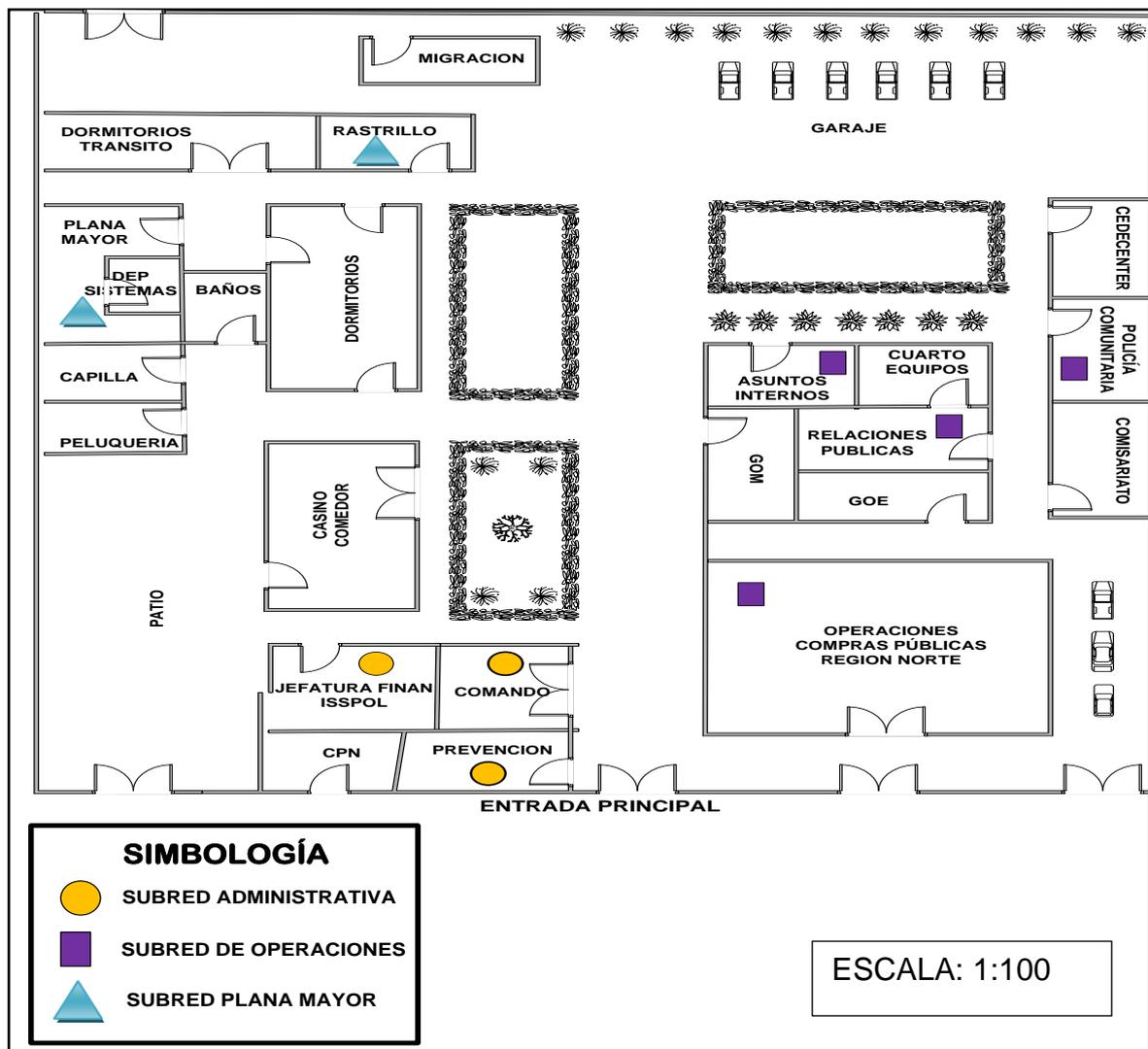


Figura 7. Esquema de distribución de subredes por disposición física
Fuente: Microsoft Visio2010

El Proveedor de Servicio de Internet es CNT EP⁷ que suministra el servicio mediante un cable de fibra óptica monomodo de 6 hilos. La red existente es clase C.

⁷ CNT EP.: Corporación Nacional de Telecomunicaciones, Empresa Pública proveedora de soluciones de telecomunicaciones.

Cada subred contiene un número de departamentos asignados, dependiendo de la función que desempeñe, de esta manera existen tres subredes que son:

- Subred Administrativa: Se encuentran todos los departamentos que están encargados de la administración financiera del Comando.
- Subred de Operaciones: Aquí se encuentran todos los departamentos relacionados a la parte operativa de la institución,
- Subred Plana Mayor: Se encuentran los departamentos que manejan recursos humanos, logísticos, jurídicos y de inteligencia de la institución, además se encuentra el departamento de sistemas que es el encargado de administrar la red del Comando Provincial.

La *Figura 8* muestra la topología física de la red del CP-12.

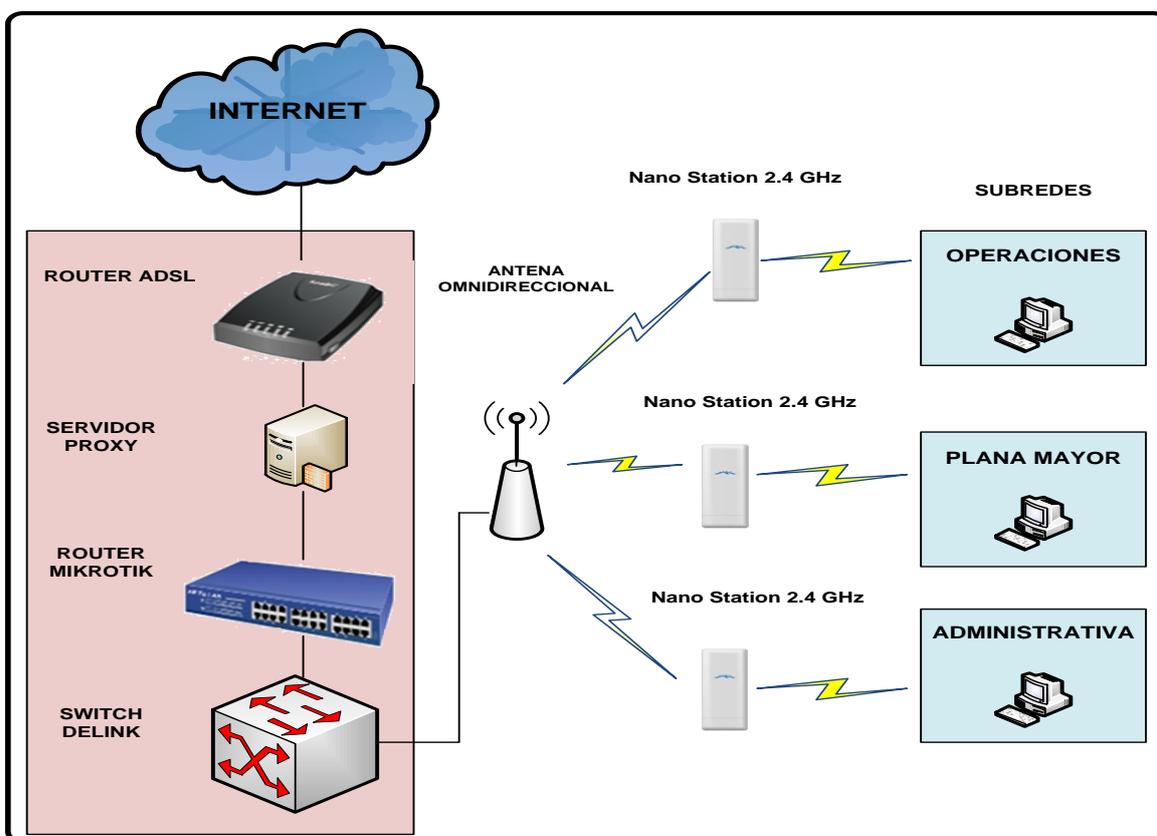


Figura 8. Topología física de la red del Comando Provincial
Fuente: Microsoft Visio 2010

El mapa distributivo que se muestra en la *Figura 9*, indica las diferentes dependencias que pertenecen a cada una de las subredes denotadas en la *Figura 7*.



Figura 9. Mapa distributivo departamental por subredes
Fuente: Información recopilada del CP-12

2.2.1 DIRECCIONAMIENTO IP⁸

Por motivos de seguridad y tomando en cuenta que el CP-12 es una institución pública que maneja datos sensibles, no se detalla el direccionamiento IP manejado para la asignación de subredes dentro del Comando, razón por la cual se toma como referencia un rango de direcciones IP para fines demostrativos.

La *Tabla 3* sirve como ejemplo para describir el direccionamiento IP del CP-12.

⁸ IP (Internet Protocol): Protocolo de Internet no orientado a conexión, usado tanto por el origen como por el destino para la comunicación de datos.

Tabla 3. Direccionamiento IP de la red del Comando Provincial
Fuente: Información recopilada del CP-12

DIRECCIONAMIENTO IP	
DESCRIPCIÓN	SUBRED
Red local	10.10.1.0/24
Red Wireless	10.10.2.0/24
Red de Internet	190.36.191.136/29

2.3 DESCRIPCIÓN DE LOS EQUIPOS DE RED

Los equipos de conectividad permiten la transferencia de información a nivel de capa 2 y 3 del modelo OSI. El CP-12 cuenta con un firewall configurado en un PC que desempeña la función de un servidor, trabaja con el sistema operativo Ubuntu 10.10 server.

Los equipos que conforman la parte activa de la red del Comando Provincial se muestran en la *Tabla 4*.

Tabla 4. Equipos de red
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	ESTADO
1	ConvertidorT P-LINK WDM Fast Ethernet	Operativo
1	Radio RouterOS 680 MHz, 2.4 GHz	Operativo
1	Router ADSL 877 Vo4.	Operativo
1	Router board Mikrotik RB 4500, 5 puertos	Operativo
1	Switch D-Link 10-100 Fast Ethernet DES-1008D 8 puertos.	Operativo
1	Antena Omnidireccional 12 dBi, 2.4 GHz	Operativa
3	Nano Station 14 dBi, 2.4 GHz.	Operativos
1	PC Pentium 4; CPU 2.80 GHz; 256 MB RAM.	Operativo

- **Convertidor TP-LINK WDM⁹ Fast Ethernet media Converter.**
 - Compatible con los estándares 802.3u 10/100 Base-TX, 100Base-FX.
 - El paso de enlace de fallas y errores minimizan oportunamente la pérdida causada por la falla en el enlace
 - Adopta la tecnología WDM, transmite y recibe datos en una sola fibra.
 - Half/Full-Dúplex.
 - Puerto RJ45 10/100Mbps.
 - Fibra Mono-Modo.
 - Hasta 20Km.
 - TX:1550 nm y RX: 1310nm.

- **Radio RouterOS 680 MHz, 2.4 GHz**
 - CPU¹⁰Atheros AR7241 de 400MHz embebido
 - Chip de memoria DDR¹¹ SDRAM¹² en placa
 - Puerto Fast Ethernet 10/100 Mbit/s con Auto-MDI/X¹³, L2MTU¹⁴ 2030
 - Radio integrado en 2GHz 802.11b/g/n con 2 conectores MMCX¹⁵

⁹WDM (WavelengthDivisionMultiplexing): La multiplexación por división de longitud de onda es una tecnología que multiplexa varias señales sobre una sola fibra óptica mediante portadoras ópticas de diferente longitud de onda.

¹⁰CPU: (Central ProcessingUnit): La Unidad Central de Procesamiento es el componente del computador y otros dispositivos programables, que interpreta las instrucciones contenidas en los programas y procesa los datos.

¹¹DDR:(Double Data Rate): En español significa Doble Tasa de Transferencia de Datos. Son módulos de memoria RAM que permite la transferencia de datos por dos canales distintos simultáneamente en un mismo ciclo de reloj.

¹²SDRAM (SynchronousDynamicRandom Access Memory): Es una memoria dinámica de acceso aleatorio que tiene una interfaz síncrona.

¹³MDI (Medium Dependent Interface): Interfaz Dependiente del Medio es un puerto o interfaz Ethernet cuyas conexiones eléctricas o pines normalmente corresponden a la distribución T568A de la norma TIA/EIA-568-B.

¹⁴MTU(Maximum Transfer Unit): La unidad máxima de transferencia es un término de redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones.

¹⁵MMCX(micro-miniatura coaxial): Conectores coaxiales RF. Cumplen con las especificaciones de la Unión Europea CECC 22 000.

- PoE¹⁶: 8-30V.
 - Dimensiones: 10.5 cm x 10.5 cm (4.13 in x 4.13 in)
 - Consumo: Hasta 4.5W, 18V a plena carga (0.245A)
 - Sistema Operativo: MikroTik RouterOS, licencia Level4
- **Router ADSL 877 Vo4.**
 - RAM¹⁷ 128 MB (instalados) / 256 MB (máx.)
 - Memoria Flash de 24 MB (instalados) / 52 MB (máx.)
 - Protocolo de direccionamiento RIP¹⁸-1, RIP-2
 - Protocolo de enlace de datos Ethernet, Fast Ethernet
 - Red / Protocolo de transporte PPTP¹⁹, L2TP²⁰, IPSec²¹, PPPoE²², PPPoA²³
 - Protocolo de señalización digital ADSL²⁴
 - Protocolo de gestión remota SNMP²⁵, Telnet, HTTP²⁶

¹⁶PoE (Powerover Ethernet): La alimentación a través de Ethernet es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar.

¹⁷RAM (Random Access Memory): La memoria de acceso aleatorio es donde el procesador recibe las instrucciones y guarda los resultados.

¹⁸RIP (RoutingInformationProtocol): Protocolo de Información de Enrutamiento utilizado por los routers para intercambiar información acerca de redes IP.

¹⁹PPTP (Point to Point TunnelingProtocol): Es un protocolo de comunicaciones desarrollado para implementar redes privadas virtuales.

²⁰L2TP (Layer 2 TunnelingProtocol): L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado.

²¹IPSec (Internet Protocol Security): Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

²²PPPoE (Point-to-Point Protocolover Ethernet): Protocolo Punto a Punto sobre Ethernet es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayoritariamente para proveer conexión de banda ancha mediante servicios de cable módem y xDSL.

²³PPPoA: Protocolo de Punto a Punto (PPP) sobre ATM (PPP over ATM), es un protocolo de red para la encapsulación PPP en capas ATM.El protocolo PPPoA se utiliza principalmente en conexiones de banda ancha, como cable y DSL.

²⁴ADSL: (Asymmetric Digital Subscriber Line): Línea de abonado digital asimétrica, es una tecnología de acceso a Internet de banda ancha.

²⁵SNMP (Simple Network Management Protocol): Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

- Protección firewall, soporte de DHCP²⁷, VPN²⁸, soporte VLAN²⁹, señal ascendente automática, soporte IPv6³⁰, Sistema de prevención de intrusiones (IPS³¹)
- Cumplimiento de normas IEEE³² 802.1x
- **Routerboard Mikrotik RB 4500, 5 puertos**
 - CPU Atheros AR7161 680 MHz
 - Chip de memoria 256 MB DDR
 - Almacenamiento: Chip de memoria 512MB
 - Cinco puertos Fast Ethernet 10/100/1000 Mbit/s
 - Sistema Operativo incluido RouterOS versión 3.0.- licencia nivel 5
 - Ofrece dos modalidades de funcionamiento: Infraestructura y Ad-Hoc
 - Compatible con 11g y equipos 11b.
 - Con tecnología CCA³³ que evita automáticamente los conflictos de canal con la función de selección de canal.

²⁶ HTTP (Hypertext Transfer Protocol): Protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la World Wide Web.

²⁷ DHCP (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.

²⁸ VPN (Virtual Private Network): Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.

²⁹ VLAN (Red de área local virtual) es un método de crear redes lógicamente independientes dentro de una misma red física.

³⁰ IPv6 (Protocolo de Internet versión 6) es una versión del protocolo Internet Protocol (IP), diseñada para reemplazar a IPv4, que actualmente está implementado en la gran mayoría de dispositivos que acceden a Internet.

³¹ IPS (Sistema de Prevención de Intrusos) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

³² IEEE: (Institute of Electrical and Electronics Engineers): Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización.

³³ CCA (Clear Channel Assessment): Evaluación de canal claro, evita automáticamente los conflictos de canal con la función de selección de canal.

- TL-WN910N Wireless N Cardbus Adapter cumple con los estándares IEEE 802.11n (Draft 2.0), IEEE 802.11g IEEE 802.11b. las tasas de transmisión inalámbrica puede alcanzar hasta 300Mbps.
 - El adaptador CardBus adopta tecnologías MIMO³⁴ que proporcionan mejor rendimiento inalámbrico, para tasas de hasta 300Mbps mejorando sustancialmente las tasas de transmisión, estabilidad y cobertura.
 - Puede operar de forma simultánea aplicaciones intensivas de ancho de banda, tales como voz y vídeo.
- **Switch D-Link 10-100 Fast Ethernet DES-1008D 8 puertos.**
 - Conmutador Nivel 2
 - 8 puertos 10/100Mbps
 - Soporte full-dúplex y half-dúplex para cada puerto
 - Puerto de interconexión MDI para expansiones sencillas
 - Autocorrección de la inversión de polaridad rx
 - Método de conmutación: Store and Forward
 - RAM buffer asignado dinámicamente para cada puerto
 - Auto aprendizaje de la configuración de red
 - Control de flujo IEEE 802.3x
 - Tabla de filtro para direcciones: 1K por dispositivo
 - RAM buffer: 1MB por dispositivo
 - Clase: 10/100 Mbps Fast Ethernet
 - Dimensiones: 196 x 115 x 28 mm

³⁴MIMO (Multiple-input Multiple-output): Múltiple entrada múltiple salida, se refiere a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos.

- Número de puertos: 8
- Tipo Conector: RJ45
- Disponibilidad Up-Link
- Soporta SNMP

- **Antena Omnidireccional 12 dBi, 2.4 GHz**
 - Antena profesional de 12 dBi
 - Soporte de montaje de acero pesado
 - Conector N Hembra integrado en cable de 12"
 - Compatible con dispositivos 802.11b/g
 - Retransmite internet sin línea telefónica
 - Omnidireccional de alta performance para estaciones base WiFi diseñado y optimizado para la frecuencia 2.4 GHz.
 - Esta antena liviana está especialmente diseñada para los sistemas IEEE 802.11b y 802.11g wireless LANs

- **Nano Station 14 dBi, 2.4 GHz.**
 - Frecuencia 2.4 GHz
 - Potencia 400mw
 - Estándar 802.11 b/g
 - Antena panel 14 dBi

- **Servidor Proxy**
 - El servidor proxy está montado sobre una plataforma Linux, utilizando el sistema Operativo Debian 6.

- El equipo cuenta con un procesador Pentium 4 con 80GB de disco duro y 2GB de memoria RAM.

2.4 DESCRIPCIÓN DE LOS DEPARTAMENTOS DEL CP-12

Dentro del Comando Provincial de Policía “Imbabura No. 12” existen 15 departamentos principales encargados de desempeñar funciones dentro de los ámbitos financiero, operativo y logístico. Estos departamentos manejan información de carácter confidencial por lo que están sometidos a la implementación del SGSI. Es importante mencionar que en toda la institución se trabaja sobre la plataforma Windows sin licenciamiento.

2.4.1 COMANDANCIA

La Comandancia es el departamento central dentro de la institución. Entre las principales funciones que realiza este departamento se encuentran:

- Receptar la información de todos los comandos a nivel provincial y nacional.
- Envío de oficios, memorandos, telegramas, correos al personal de la institución.

• ESTACIONES DE TRABAJO

Dentro de la Comandancia existen 3 estaciones de trabajo, a continuación en la *Tabla 5* se describen las características de los equipos de cómputo, así como el Sistema Operativo utilizado.

Tabla 5. Estaciones de trabajo de la Comandancia
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
1	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows Vista Service Pack 2
1	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows XP Service Pack 2
1	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows 7

- **TRATAMIENTO DE LA INFORMACIÓN**

Toda la información manejada en este departamento es de carácter público para el personal que labora dentro de la institución.

La información se respalda mediante el almacenamiento de documentos en el archivo y por medios digitales.

2.4.2 PREVENCIÓN

Este departamento tiene como función principal la elaboración de partes e informes concernientes a denuncias, accidentes de tránsito, contravenciones y quebrantamiento de la ley por parte de la ciudadanía.

- **ESTACIONES DE TRABAJO**

Dentro de la Prevención existe 1 sola estación de trabajo, con las características indicadas en la *Tabla 6*:

Tabla 6. Estación de trabajo de la Prevención
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
1	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows 7

- **TRATAMIENTO DE LA INFORMACIÓN**

La información que se maneja en este departamento es de carácter confidencial, únicamente lo que corresponde a denuncias puede ser dado a conocer. Toda esta información es archivada, pero no existe el respaldo de la misma en formato digital.

2.4.3 JEFATURA FINANCIERA

Se encarga del control de todos los bienes e inmuebles pertenecientes a la institución y de las respectivas actas de entrega y recepción de los mismos. Maneja toda la información correspondiente a préstamos tanto de policías en servicio activo como en servicio pasivo, supervivencia, montepíos. Además se encarga de la declaración de impuestos y del pago de facturas de bienes o servicios tales como adquisición de bienes muebles, mantenimiento de carros, mantenimiento de computadores, obras de remodelación.

- **ESTACIONES DE TRABAJO**

Existen 5 estaciones de trabajo que tienen las siguientes características, detalladas en la *Tabla 7*:

*Tabla 7. Estaciones de trabajo de la Jefatura Financiera
Fuente: Información recopilada del CP-12*

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows Vista Service Pack 2
1	Computador Pentium 4; CPU 3,00 GHz; 496 MB RAM	Windows XP Service Pack 3
2	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows 7

- **TRATAMIENTO DE LA INFORMACIÓN**

La información recopilada es archivada y se realiza un respaldo mensual de los archivos más importantes en formato digital.

2.4.4 COMPRAS PÚBLICAS

Aquí se realiza la adquisición de bienes muebles, artículos o servicios indispensable para la institución.

- **ESTACIONES DE TRABAJO**

Existe 1 sola estación de trabajo destinada para el departamento de Compras Públicas, con las siguientes características indicadas en la *Tabla 8*:

Tabla 8. Estación de trabajo de Compras Públicas
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
1	Computador Pentium 4; CPU 2,80 GHz; 512 MB RAM	Windows XP SP3

- **TRATAMIENTO DE LA INFORMACIÓN**

La información que maneja este departamento es considerada de carácter público para todos los miembros policiales. Esta información es únicamente archivada.

2.4.5 OPERACIONES

Es el departamento encargado de realizar evaluaciones y presentar informes sobre órdenes de servicio para obtener estadísticas que permitan determinar el desempeño del personal designado en eventos culturales, sociales o deportivos,

permitiendo planificar de mejor manera los operativos y la designación de personal.

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo dentro del departamento de Operaciones, detalladas en la *Tabla 9*:

Tabla 9. Estaciones de trabajo del departamento de Operaciones

Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows Vista Service Pack 1

- **TRATAMIENTO DE LA INFORMACIÓN**

Todos los informes sobre operativos planificados y designación de personal en algún orden de servicio son almacenados en el archivo y existe un respaldo semanal de la información en formato digital.

2.4.6 ASUNTOS INTERNOS

Se encarga de realizar investigaciones del personal de policía cuando se suscitan acontecimientos conflictivos que los involucren, presentación de partes informativos o denuncias tanto internas como externas.

Además se encarga de la realización de informes en base a la información procedente de las investigaciones para posteriormente emitirlos al señor Comandante de Policía quien en coordinación con la asesoría legal analizan si tal acontecimiento consta en el reglamento disciplinario y así determinar la sanción correspondiente.

- **ESTACIONES DE TRABAJO**

Para este departamento están designadas 4 estaciones de trabajo, indicadas en la *Tabla 10*:

Tabla 10. Estaciones de trabajo de Asuntos Internos
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
1	Computador Intel Core 2 Duo; CPU 2,66 GHz; 1,00 GB RAM	Windows 7
3	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows 7

- **TRATAMIENTO DE LA INFORMACIÓN**

Todas las denuncias receptadas, partes informativos y demás documentos son archivados y la información se respalda digitalmente cada mes.

2.4.7 RELACIONES PÚBLICAS

Procesa información sobre eventos institucionales, trabajo policial desempeñado por cada uno de los servicios y define estrategias de comunicación que sirvan para mejorar o mantener una buena imagen de la institución. Se relaciona con los medios de comunicación seleccionando el tipo de información que se puede y debe difundir.

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo, detalladas en la *Tabla 11*:

Tabla 11. Estaciones de trabajo de Relaciones Públicas
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows 7

- **TRATAMIENTO DE LA INFORMACIÓN**

Manejan información de carácter pública y privada. No realizan respaldos de la información de forma digital, únicamente la documentación es archivada.

2.4.8 POLICÍA COMUNITARIA

Este departamento es responsable del funcionamiento de las diferentes instalaciones de policías comunitarias en la ciudad. Se encargan de designar el personal para las diferentes zonas y elaborar informes de actividades de cada zona.

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo, detalladas en la *Tabla 12*:

Tabla 12. Estaciones de trabajo de Policía Comunitaria
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
1	Computador Intel Pentium 4; CPU 2,80 GHz; 512 MB RAM;	Windows XP Service Pack 3
1	Computador Intel Pentium 4; CPU 3,20 GHz; 448 MB RAM;	Windows XP Service Pack 3

- **TRATAMIENTO DE LA INFORMACIÓN**

Todos los informes de actividades de las diferentes zonas de la ciudad son almacenados en el archivo y existe un respaldo digital de la información cada trimestre.

2.4.9 REGIÓN NORTE

Este departamento está encargado de verificar el cumplimiento de todas las disposiciones dadas a los Comandos Provinciales de la Región Norte. Realizan todos los trámites relacionados con la Comandancia del Primer Distrito de la ciudad de Quito.

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo en este departamento, indicadas en la *Tabla 13*:

Tabla 13. Estaciones de trabajo de la Región Norte
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows 7

- **TRATAMIENTO DE LA INFORMACIÓN**

La información manejada dentro de este departamento es almacenada en el archivo y existe un respaldo mensual de la información en forma digital.

2.4.10 RECURSOS HUMANOS

En este departamento se realizan principalmente entrega de comparencias, cambio de personal, orden del cuerpo (listado de personal en servicio). Además realizan memorandos, comunicados al personal, actualización de datos. Manejan datos privados del personal de la institución.

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo, indicadas en la *Tabla 14*:

Tabla 14. Estaciones de trabajo de recursos humanos
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computador Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows 7

- **TRATAMIENTO DE LA INFORMACIÓN**

La información tanto privada como pública es almacenada en el archivo y se realiza un respaldo semestral de la información privada.

2.4.11 RECURSOS LOGÍSTICOS

Entre las principales funciones que realiza este departamento están:

- Mantenimiento del patio automotor.
- Matriculación de vehículos de servicio urbano y rural.
- Informes de accidentes de tránsito de vehículos.
- Abastecimiento de combustibles

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo en este departamento, indicadas en la *Tabla 15:*

Tabla 15. Estaciones de trabajo de Recursos Logísticos
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computadores Intel Core 2 Duo; CPU 2,66 GHz; 2,00 GB RAM	Windows XP Service Pack 2

- **TRATAMIENTO DE LA INFORMACIÓN**

La información que maneja este departamento es de carácter privado y no existe respaldo digital de la información.

2.4.12 ASESORÍA JURÍDICA

Este departamento se encarga de emitir criterios jurídicos solicitados por el Comandante Judicial. Además se encargan del manejo de estadísticas referentes a faltas disciplinarias del personal.

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo, indicadas en la *Tabla 16*:

Tabla 16. Estaciones de trabajo de Asesoría Jurídica
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computadores Intel Core 2Duo; CPU 2,67 GHz; 1,96 GB RAM	Windows XP Service Pack 2

- **TRATAMIENTO DE LA INFORMACIÓN**

No existe respaldo digital de la información, tampoco se almacena la información en el archivo.

2.4.13 RASTRILLO

Este departamento es el encargado del manejo del armamento, aquí se lleva un registro de todo el personal de policía que tiene autorizado su uso y se realiza un control de entrega y recepción del mismo. Además se lleva un inventario de todos los bienes con que cuenta este departamento tales como armamento, material símil, municiones, esposas, chalecos antibalas, escudos, cascos anti motín, entre otros. Adicionalmente para brindar seguridad a este departamento se cuenta con una alarma, detector de humo y cámaras de vigilancias las mismas que son monitoreadas desde la central de radio patrulla.

- **ESTACIONES DE TRABAJO**

Existe 1 estación de trabajo en este departamento, indicada en la *Tabla 17*:

Tabla 17. Estaciones de trabajo de Rastrillo

Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
1	Computador Intel Core 2Duo; CPU 2,66 GHz; 2.00 GB RAM	Windows 7

- **TRATAMIENTO DE LA INFORMACIÓN**

La información correspondiente tanto al inventario como al registro de entrega y recepción de armamento y otros recursos se encuentra almacenada digitalmente y en un libro de registros. Únicamente el personal de policía encargado accede a esta información evitando así que se pueda llevar a cabo alteraciones en la misma.

2.4.14 INTELIGENCIA

Se encarga de toda la función operativa de la institución, además de realizar operaciones de inteligencia, es decir de formular un plan estratégico antes de que se produzca cualquier altercado.

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo, indicadas en la *Tabla 18*:

Tabla 18. Estaciones de trabajo de Inteligencia

Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computadores Intel Core 2Duo; CPU 2,67 GHz; 1,96 GB RAM	Windows XP Service Pack 2

- **TRATAMIENTO DE LA INFORMACIÓN**

La información que maneja este departamento es de carácter privado.

Se hace un respaldo anual de la información utilizando CD's.

2.4.15 SISTEMAS

El departamento de Sistemas es el encargado de administrar la red del Comando Provincial de Policía "Imbabura No. 12", entre sus funciones está reparar y dar mantenimiento a equipos de cómputo e impresoras.

- **ESTACIONES DE TRABAJO**

Existen 2 estaciones de trabajo indicadas en la *Tabla 19*:

Tabla 19. Estaciones de trabajo del departamento de Sistemas

Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	SISTEMA OPERATIVO
2	Computadores Intel Core 2Duo; CPU 1,80 GHz; 0,98 GB RAM	Windows XP Service Pack 3

- **TRATAMIENTO DE LA INFORMACIÓN**

Dentro de este departamento se realiza un respaldo mensual de toda la información manejada, además se la almacena en el archivo.

2.5 SITUACIÓN ACTUAL

Con la finalidad de obtener datos acerca de temas específicos que permitan tener una visión respecto a la seguridad tanto en redes como de la información, se aplicó una encuesta en el CP-12 al personal encargado de los 15 departamentos de la institución, para posteriormente analizarlas y emitir un criterio acerca del tema tratado.

Debido a la limitación de tiempo que tiene el personal del CP-12 se eligió aplicar la encuesta utilizando preguntas cerradas para obtener información específica de una muestra de la población mediante el uso de cuestionarios estructurados para obtener datos precisos de las personas encuestadas.

En este paso se determina el número de encuestas a realizarse. Para conocer el número exacto de la muestra a la que se debe aplicar la encuesta, se debe hacer uso de la fórmula de muestreo, la cual nos permite obtener un número representativo del grupo de personas que se va a estudiar.

La fórmula de la muestra es la siguiente:

$$n = (Z^2 pqN) / (Ne^2 + Z^2 pq) \quad (1)$$

Ecuación 1. Fórmula de muestreo

Fuente: http://catarina.udlap.mx/u_dl_a/tales/documentos/lhr/nieto_s_p/capitulo3.pdf

Donde:

n: muestra: Es el número representativo del grupo de personas que se quiere estudiar (población) y, por tanto, el número de encuestas que se debe realizar.

N: población: es el grupo de personas que se va a estudiar.

z: nivel de confianza: mide la confiabilidad de los resultados. Lo usual es utilizar un nivel de confianza de 95% (1.96) o de 90% (1.65). Mientras mayor sea el nivel de confianza, mayor confiabilidad tendrán los resultados.

e: grado de error: mide el porcentaje de error que puede haber en los resultados. Lo usual es utilizar un grado de error de 15% o de 20%. Mientras menor margen de error, mayor validez tendrán los resultados.

p : probabilidad de ocurrencia: probabilidad de que ocurra el evento. Lo usual es utilizar una probabilidad de ocurrencia del 50%.

q : probabilidad de no ocurrencia: probabilidad de que no ocurra el evento. Lo usual es utilizar una probabilidad de no ocurrencia del 50%.

Para el caso del CP-12, se toma en consideración una población aproximada de 100 personas, un nivel de confianza de 95%, entonces:

$$\begin{aligned} Z &= 1.96 \\ p &= 0.5 \\ q &= 0.5 \\ N &= 100 \\ e &= 0.2 \end{aligned}$$

$$n = \frac{((1.96)^2 * 0.5 * 0.5 * 100)}{(100 * (0.2)^2 + (1.96)^2 * 0.5 * 0.5)}$$

$$n = 19.36$$

El resultado del muestreo da como referencia aproximadamente 20 personas para la aplicación de la encuesta. La encuesta realizada se encuentra en el ANEXO 1.

Las encuestas realizadas brindan un estimado de la situación actual en base a 6 indicadores de acción con un total de 53 preguntas cerradas que proporcionan información necesaria con respecto a la seguridad y manejo de la información dentro del CP-12, las preguntas del cuestionario están enfocadas a poner en conocimiento el nivel de seguridad en la red y en las medidas de salvaguarda con las que cuenta la institución para mitigar riesgos e incidentes.

A continuación se muestran los resultados numéricos de la encuesta aplicada en base a cada uno de los indicadores. Es importante mencionar que el valor total

obtenido se calcula también en porcentaje ya que este valor posteriormente influye en el análisis de riesgos que dará a conocer el nivel de madurez de la institución. Los gráficos estadísticos que indican los valores numéricos obtenidos en la encuesta para cada una de las preguntas de los 6 indicadores, se muestran en el ANEXO 2.

- **Indicador: *Confidencialidad de la Información***

Dentro de este indicador se trata de conocer si existen controles para salvaguardar la confidencialidad de la información y las medidas que se toman para proteger este aspecto. La *Tabla 20* muestra el resultado.

*Tabla 20. Resultados del indicador Confidencialidad de la Información
Fuente: Información recopilada en la aplicación de encuestas*

PREGUNTAS SI /NO	Si	No	Total
¿En la Institución hay una cultura de apoyo a la seguridad informática	10	10	20
¿Hay planes y medidas para mitigar o administrar una brecha de confidencialidad?	9	11	20
¿Se ha implementado seguridades para que personas no autorizadas no puedan observar información sensible y confidencial?	12	8	20
¿Hay controles físicos en las áreas donde se encuentran Sistemas de Computación y Sistemas de Información considerados críticos?	5	15	20
¿Hay controles de ingreso lógico para proteger la información y datos sensitivos de accesos externos?	5	15	20
¿Hay controles de ingreso lógico para proteger la información y datos sensitivos de accesos internos no autorizados?	7	13	20
Valor promedio del indicador	8	12	20
Porcentaje del indicador (%)	40	60	100

La *Figura 10* muestra la estadística correspondiente a este indicador.



Figura 10. Gráfico estadístico del indicador Confidencialidad de la Información
Fuente: Graficación en Microsoft Excel

En base a los resultados obtenidos, se puede evidenciar que la Confidencialidad de la Información es un punto al que se le debe dar mayor prioridad debido a que no se toman las medidas necesarias para prevenir la divulgación de información a personas o sistemas no autorizados.

- **Indicador: Integridad de la Información**

Dentro de este indicador se busca conocer el nivel de integridad que mantiene la información, así como los controles aplicables que se aplican.

La *Tabla 21* muestra los resultados de este indicador.

Tabla 21. Resultados del indicador Integridad de la Información
Fuente: Información recopilada en la aplicación de encuestas

PREGUNTAS SI/NO	Si	No	Total
¿Hay riesgos significativos de que haya errores durante el ingreso de información?	8	12	20
¿Hay riesgos significativos de que haya errores introducidos por programas, fallas de diseño, o mal funcionamiento en los sistemas y aplicaciones que se utilizan en su oficina?	14	6	20
¿Hay controles de ingreso lógico para proteger datos e información sensible de accesos externos no autorizados?	9	11	20
¿La Institución promueve una cultura de seguridad?	9	11	20
¿Hay controles de ingreso lógico para proteger datos e información sensible de accesos internos no autorizados?	7	13	20
Valor promedio del indicador	9,4	10,6	20
Porcentaje del indicador (%)	47	53	100

La *Figura 11* muestra el gráfico estadístico de este indicador.

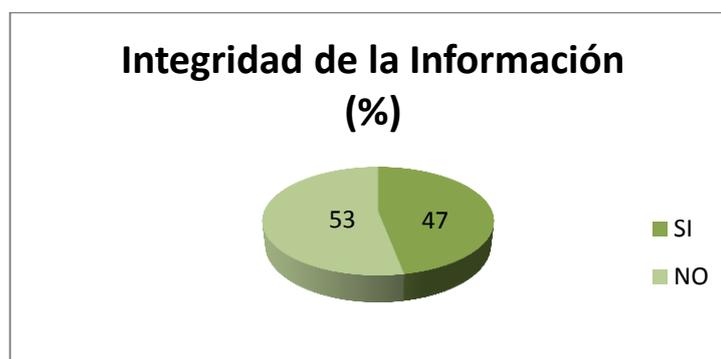


Figura 11. Gráfico estadístico del indicador Integridad de la Información
Fuente: Graficación en Microsoft Excel

Los resultados obtenidos muestran que aún no se puede garantizar totalmente la Integridad de la Información, debido a que no se toma las debidas precauciones que permitan mantener los datos libres de modificaciones no autorizadas. La violación de integridad está presente en un alto porcentaje dentro de la Institución y la mayoría del personal desconoce cómo actuar ante esta situación.

- **Indicador: Políticas de Seguridad**

Este indicador constituye la parte principal de la encuesta ya que dependiendo de los resultados se puede conocer si existe un documento que muestre por escrito todas las políticas concernientes a la seguridad de la información.

La *Tabla 22* muestra el resultado de este indicador.

Tabla 22. Resultados del indicador Políticas de seguridad
Fuente: Información recopilada en la aplicación de encuestas

PREGUNTAS SI /NO	Si	No	Total
¿Se dispone de un documento escrito de las políticas de seguridad que sea de conocimiento de todo el personal y responsables de la seguridad de la información?	5	15	20
¿De existir estas políticas se da cumplimiento a las mismas?	13	7	20
¿Las políticas tienen una definición de seguridad de la información, objetivos y alcances?	3	17	20
¿Las políticas tienen una explicación del proceso para reportar incidentes de seguridad?	0	20	20
¿Existe un período máximo de vida de las contraseñas?	0	20	20
¿En su dirección está definido el personal autorizado a acceder a los sistemas?	14	7	20
En caso de existir dicho listado de personal autorizado, ¿se incluye el tipo de acceso permitido?	8	12	20
¿Existen procedimientos de asignación y distribución de contraseñas?	6	14	20
¿Se dispone de un documento escrito de las políticas de seguridad que sea de conocimiento de todo el personal y responsables de la seguridad de la información?	4	16	20
¿Los enunciados de las políticas son revisados periódicamente, incluyendo cambios en los niveles de responsabilidad?	7	13	20
¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas?	11	9	20
¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?	11	9	20
Valor promedio del indicador	6,83	13,25	20
Porcentaje del indicador (%)	34	66	100

La *Figura 12* muestra el gráfico correspondiente a este indicador.

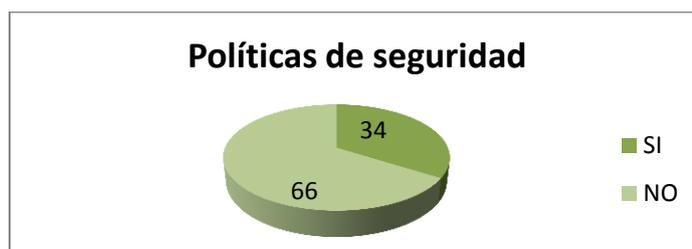


Figura 12. Gráfico estadístico del indicador Políticas de Seguridad
Fuente: Graficación en Microsoft Excel

Dentro del CP-12 no existe un plan de acción para afrontar riesgos de seguridad o un conjunto de reglas para el mantenimiento de cierto nivel de seguridad ya que no se han definido políticas de seguridad de la información.

- **Indicador: Clasificación y Control de Valores**

Este indicador permite conocer si existe un inventario de activos y su correcta clasificación. La *Tabla 23* muestra el resultado del indicador.

Tabla 23. Resultados del indicador Clasificación y Control de Valores
Fuente: Información recopilada en la aplicación de encuestas

PREGUNTAS SI /NO	Si	No	Total
¿Hay control de los inventarios del hardware, software y medios de almacenamiento de datos?	9	11	20
¿Tienen los bienes informáticos alguna forma de clasificación relativa a niveles de seguridad?	11	9	20
¿La información clasificada se etiqueta adecuadamente?	14	6	20
Valor promedio del indicador	11,33	8,67	20
Porcentaje del indicador (%)	56,65	43,35	100

La *Figura 13* muestra el gráfico estadístico del indicador.



Figura 13. Gráfico estadístico del indicador Clasificación y Control de Valores
Fuente: Graficación en Microsoft Excel

La clasificación y control de valores está en desarrollo dentro del CP-12, sin embargo aún se debe mantener un adecuado control en este indicador e implementar políticas que permitan elevar el nivel de seguridad tanto de la información así como también de los activos.

- **Indicador: Aspectos organizativos para la seguridad**

Este indicador da a conocer si existe una persona responsable de administrar y gestionar temas relacionados con la seguridad de la red y de la información. La *Tabla 24* muestra el resultado de este indicador.

Tabla 24. Resultados del indicador Aspectos organizativos para la seguridad
Fuente: Información recopilada en la aplicación de encuestas

PREGUNTAS SI /NO	Si	No	Total
¿Existe una persona responsable de administrar los asuntos relacionados con la seguridad informática?	20	0	20
¿Esta explícitamente definido la responsabilidad individual o compartida de seguridad sobre los procesos?	15	5	20
¿Los procesos de aprobación, adquisición e instalación de servicios para Tecnologías de Información en relación a seguridad son claros?	13	7	20
Valor promedio del indicador	16	4	20
Porcentaje del indicador (%)	80	20	100

La *Figura 14* muestra el gráfico correspondiente para el indicador.



Figura 14. Gráfico estadístico del indicador Aspectos organizativos para la seguridad
Fuente: Graficación en Microsoft Excel

Los aspectos organizativos dentro del CP-12 tienen un alto nivel de rendimiento, debido a que cada persona tiene asignada una función específica y existe un Departamento de Sistemas que se encarga de administrar los recursos tecnológicos.

Sin embargo, es importante que la institución cuente con un documento en el que se detallen políticas y acciones a ser cumplidas y que sirvan de apoyo para elevar el desarrollo de este indicador.

- **Indicador: Seguridad Física**

Este indicador da a conocer aspectos relacionados con la seguridad física del personal así como de los activos dentro de la institución.

La *Tabla 25* muestra el resultado de este indicador.

Tabla 25. Resultados del indicador Seguridad Física
Fuente: Información recopilada en la aplicación de encuestas

PREGUNTAS SI /NO	Si	No	Total
¿Está protegida la información que se transmite por cables de telecomunicaciones de forma que no es susceptible de interceptación?	7	13	20
¿Los Sistemas de Cómputo y Sistemas de Información críticos están protegidos de acceso no autorizado y están ubicados en áreas seguras?	15	5	20
¿Los Sistemas Computacionales y Sistemas de Información están protegidos contra las fallas eléctricas?	9	11	20
¿Los Sistemas de Computo son ubicados pensando en su protección ante posibles amenazas ambientales (incendio, inundación, terremoto)?	13	7	20
¿Está definido el personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que procesan información?	12	8	20
¿Existe una persona responsable de la seguridad física a nivel del departamento/unidad?	11	9	20
¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad física?	7	13	20
¿Existe personal de vigilancia en la institución?	15	5	20
¿Existe vigilancia en el departamento de cómputo las 24 horas?	20	0	20
¿El personal ajeno a operaciones sabe qué hacer en el caso de una emergencia?	15	5	20
¿Existe salida de emergencia?	14	6	20
¿Está definido el personal autorizado a acceder a los dispositivos y medios de almacenamiento de datos?	7	13	20
¿Existe una clara definición de funciones entre los mandos de la institución respecto a la seguridad física?	16	4	20
¿Se lleva una bitácora de las acciones de los operadores para evitar que realicen pruebas que puedan dañar los sistemas?	8	12	20
¿Se controla el acceso a los archivos y programas en producción a los programadores, analistas y operadores?	4	16	20
¿Se ha instruido al personal sobre qué medidas tomar en caso de que alguien pretenda entrar a las oficinas sin autorización?	12	8	20
¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?	13	7	20
¿Se hacen copias de seguridad de la información considerada importante en su departamento?	11	9	20
¿Se cuenta con copias de los archivos en lugar distinto al de la computadora/servidores?	9	11	20
¿Se tienen establecidos procedimientos de actualización a estas copias?	7	13	20
¿Se tienen establecidos procedimientos de verificación de estas copias?	8	12	20
¿Existe un sistema de video-vigilancia en su departamento/unidad?	20	0	20
¿Se controla el acceso de equipos electrónicos a los ambientes de trabajo?	15	5	20
¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento en especial cerca a los equipos de cómputo?	15	5	20
Valor promedio del indicador	11,8	8,20	20
Porcentaje del indicador (%)	59	41	100

La *Figura 15* muestra el gráfico correspondiente a este indicador.



Figura 15. Gráfico estadístico del indicador Seguridad Física
Fuente: Graficación en Microsoft Excel

La Seguridad Física dentro del CP-12 si constituye un factor fundamental pero no totalmente ya que aún no se cuenta con la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

- **ANÁLISIS DE RESULTADOS OBTENIDOS**

Una vez que se obtuvieron los resultados y las debidas apreciaciones de las encuestas aplicadas, el siguiente paso es la verificación de los resultados para dar una estimación que se acerque más a la realidad.

Se realizó la verificación en el sitio para emitir una conclusión definitiva y realizar un correcto análisis del riesgo el mismo que permite aplicar los controles adecuados y las políticas necesarias para la correcta implantación del SGSI.

En conclusión, el CP-12 es una institución que cuenta únicamente con los controles y seguridades básicas, constituyendo así un elemento fácil de vulnerar ya sea interna o externamente. Se debe implementar políticas que ayuden a proteger los activos que son considerados como primordiales,

entre ellos la información que es transmitida dentro de la institución. Además se debe designar los responsables de las dependencias asegurándose que conozcan la función que van a desempeñar.

Al no contar con salvaguardas frente a amenazas materializadas, el CP-12 está expuesto a un nivel alto de riesgo provocado ya sea por error humano o por falla en los activos, servicios o aplicaciones manejadas dentro de la institución.

La iniciativa para implementar un SGSI debe basarse en los objetivos planteados dentro del CP-12 relacionados con la seguridad de la información y darse a conocer a todo el personal con la finalidad de obtener la colaboración total tanto de autoridades como del resto de personas.

CAPÍTULO III

ANÁLISIS Y EVALUACIÓN DE RIESGOS

En este capítulo se desarrolló el análisis de riesgos utilizando la metodología MAGERIT, además del control de activos, análisis de amenazas, nivel de madurez de la institución y salvaguardas.

3.1 METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT, cumple con el objetivo primordial de garantizar la seguridad los sistemas de información, identificando problemas y definiendo políticas que los eviten.

MAGERIT define los procedimientos que sirven de guía para el establecimiento de la protección necesaria de los sistemas de información de una institución de carácter público. Además, cumple con objetivos adicionales que están enfocados a la realización de un análisis de riesgos dentro de la institución.

Estos objetivos son:

- Analizar los riesgos que soporta un determinado sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.
- Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados, mediante la gestión de riesgos. Basado en los resultados del análisis de

riesgos, se seleccionan e implantan las medidas o salvaguardas de seguridad adecuadas para reducir al mínimo aceptable los posibles perjuicios.

3.2 ADMINISTRACIÓN DE RIESGOS

Es importante asegurar que la institución alcance los objetivos relacionados con la seguridad de la información, para lo cual ésta debe dirigir y administrar las actividades de TI³⁵ con el fin de lograr un balance efectivo entre el manejo de riesgos y los beneficios encontrados. Para cumplir esto, los Directivos necesitan identificar las actividades más importantes que deben ser desarrolladas, midiendo el progreso hacia el cumplimiento de las metas y determinando la manera en la que se desarrollan los procesos de TI.

La *Figura 16* muestra un esquema de administración de riesgos que sirve como base para analizar y gestionar los riesgos de TI.

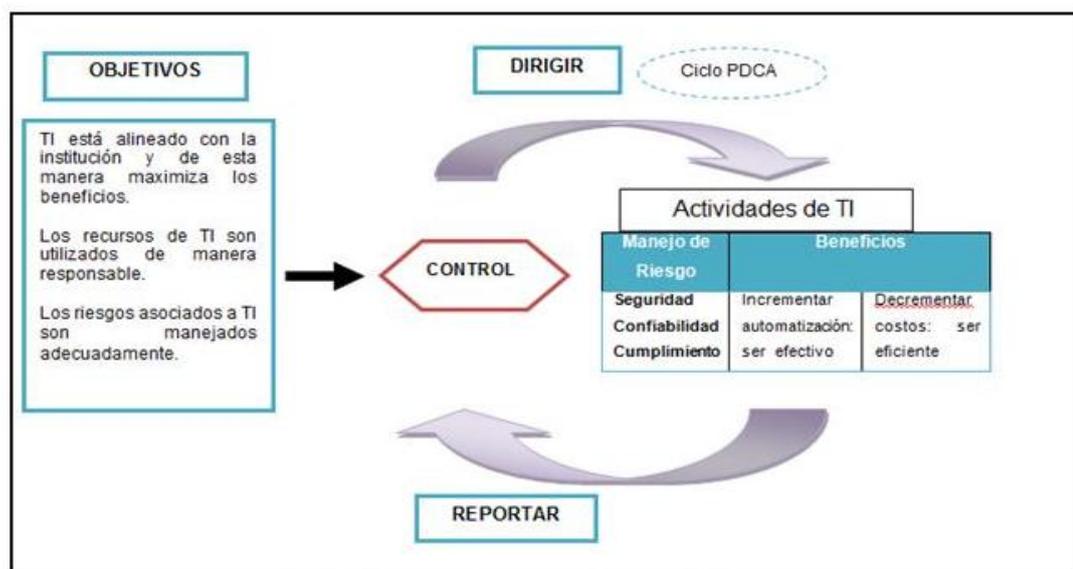


Figura 16. Esquema base para administración de riesgos
Fuente: http://www.iso27000.es/download/doc_iso27000_all.pdf

³⁵ TI: Tecnologías de Información: Tecnologías de Información: Se entiende como aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información.

3.3ANÁLISIS DE RIESGOS

El análisis de riesgos permite determinar qué tiene la institución y estimar el nivel de exposición a los riesgos presentes.

Este análisis se compone de tres elementos fundamentales:

- Activos
- Amenazas
- Salvaguardas

El primer paso consiste en la valoración de los activos, que son los elementos del sistema de información que aportan valor a la Institución.

En el siguiente paso se tratan las amenazas, esto implica todo aquello que puede provocar una vulnerabilidad. La probabilidad de la amenaza, el grado de vulnerabilidad y la severidad del impacto se relacionan entre sí para emitir un criterio acerca de la evaluación del riesgo.

Finalmente se debe realizar la selección de contramedidas o salvaguardas y una evaluación de su eficacia, que también identifica el riesgo residual. El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones basadas en un fundamento.

3.3.1 CONTROL DE ACTIVOS

Son considerados como activos los recursos del sistema de información o que tengan una relación con éste, y son necesarios para que la Institución funcione correctamente y alcance los objetivos propuestos por su gerencia.

La *Tabla 26* muestra el valor que se debe asignar a cada uno de los activos, clasificados según el daño que puedan ocasionar a la Institución en caso de que exista algún daño.

Tabla 26. Valoración de activos

Fuente: <http://www.slideshare.net/mmujiica/mi-defensa>

Valoración de activos			
Valor	Disponibilidad	Integridad	Confidencialidad
5	Este nivel abarca toda información, instalación o recurso cuya disponibilidad siempre debe garantizarse. Su pérdida es considerada como catastrófica para la Institución.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es en extremo importante y debe garantizarse bajo cualquier circunstancia. Su pérdida es considerada como catastrófica.	Este nivel abarca toda información, instalación o recurso calificado como de uso confidencial. Solo puede ser utilizado con autorización explícita
4	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por algunas horas.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es muy importante y debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso restringido. Solo puede ser utilizado por personal autorizado.
3	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 24 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad es de importancia media y debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso semi-restringido. Solo puede ser utilizado por personal interno.
2	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por 48 horas máximo.	Este nivel abarca toda información, instalación o recurso en el cual la integridad no es muy importante pero debe garantizarse.	Este nivel abarca toda información, instalación o recurso calificado como de uso interno. Solo puede ser utilizado por personal interno o usuarios/clientes.
1	Este nivel abarca toda información, instalación o recurso cuya disponibilidad puede estar detenida por varios días sin causar consecuencias.	Este nivel abarca toda información, instalación o recurso en el cual la pérdida de integridad es insignificante.	Este nivel abarca toda información, instalación o recurso calificado como de uso público.

El activo primordial es la información que maneja el sistema, es decir los datos, y alrededor de estos datos se identifican otros activos fundamentales:

- *Servicios*: que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- *Aplicaciones informáticas (software)*: que permiten manejar los datos.
- *Equipos informáticos (hardware)*: que permiten alojar datos, aplicaciones y servicios.
- *Soportes de información*: que son dispositivos de almacenamiento de datos.
- *Equipamiento auxiliar*: que complementa el material informático.
- *Redes de comunicaciones*: que permiten el envío y recepción de datos.
- *Instalaciones*: que acogen equipos informáticos y de comunicaciones.
- *Personal*: que explotan u operan todos los elementos anteriormente citados.

3.3.1.1 Identificación de activos del CP-12

A. Datos usados por los sistemas de información

La *Tabla 27* muestra la identificación de activos dentro del CP-12

*Tabla 27. Datos usados dentro de la institución
Fuente: Información recopilada del CP-12*

Datos		Descripción
BD	Sistema Integrado	Aplicaciones Personal, Nómina
	Postgres	
BD	Sistema Integrado	Aplicaciones Personal, Nómina,
	ORACLE	Inventarios, Sistema de documentación, Sanidad, Presupuesto en ORACLE
	Sistema Integrado SIIPNE	Sistema Integrado de Información de delitos de la Policía Nacional del Ecuador

B. Servicios

Internamente el Departamento de Sistemas brinda los siguientes servicios:

- Soporte en Redes
- Servicios de soporte
 - Internet
 - Red Local
 - Red Inalámbrica
 - Antivirus
- Mantenimiento de Hardware
- Soporte de Aplicaciones de Software.

C. Aplicaciones Informáticas

La *Tabla 28* muestra las aplicaciones usadas en el CP-12

*Tabla 28. Aplicaciones usadas en los diferentes departamentos
Fuente: Información recopilada del CP-12*

Aplicación	Descripción
Antivirus	NOD 32 con licencia para 60 máquinas
Microsoft Windows Professional	Sin licencia
Postgres	Versión Limitada (Gratis)
ORACLE	En Proceso De Descontinuación*
Firefox	
WinZip	
WinRar	
SistemaTiny	

*La Base de datos ORACLE está en proceso de descontinuación debido a que cuenta con soporte y actualizaciones únicamente hasta el año 2014.

D. Equipos Informáticos

La *Tabla 29* muestra equipos pertenecientes al CP-12

Tabla 29. Equipos informáticos pertenecientes al CP-12
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN
1	Convertidor TP-LINK WDM Fast Ethernet media Converter
1	Router ADSL 877 Vo4
1	Servidor Proxy
1	Router board Mikrotik RG-ENT
1	Switch D-Link 10-100 Fast Ethernet DES-1008D 8 puertos
1	Antena Omnidireccional
3	Nano Station 2.4 GHz
32	Computadores de escritorio completos*

*Todos los computadores de escritorio están equipados con su respectivo mouse, teclado, monitor y regulador.

E. Soportes de información

Dentro del Comando Provincial no existe un equipo para realizar el respaldo de la información. Toda la información de carácter privado y público se almacena en el archivo y en CD's.

F. Equipamiento auxiliar

La *Tabla 30* muestra el equipamiento auxiliar del CP-12

Tabla 30. Equipamiento auxiliar del CP-12
Fuente: Información recopilada del CP-12

Equipos	Descripción
UPS Central	UPS Central (6 KVA). Ubicada en el cuarto de equipos
Generador eléctrico	Generador eléctrico para toda la institución
Impresoras multifunción	10 en total (4 CANON , 6 HP)
Impresoras laser	4 en total (SAMSUNG)
Copiadoras	2 en total (LENOVO)

G. Redes de comunicaciones

La *Tabla 31* muestra las redes pertenecientes al CP-12

Tabla 31. Redes de comunicaciones del CP-12
Fuente: Información recopilada del CP-12

Red	Descripción
Red Local	Red local del CP-12. Compuesta por las subredes de cada uno de los departamentos
Red Wireless	Red inalámbrica corporativa Enlace de 2Mbps. FO monomodo de 6 hilos

H. Instalaciones

La *Tabla 32* muestra ubicación de las instalaciones dentro del CP-12

Tabla 32. Ubicación de las instalaciones del CP-12
Fuente: Información recopilada del CP-12

Instalaciones	Ubicación
Sector Operativo	Zona Nor-Oeste del CP-12
Sector Administrativo	Zona Nor-Este del CP-12
Asuntos Internos	Zona Centro
Plana Mayor	Zona Sur-Este del CP-12
Central Integrada de Atención Ciudadana (CIAC-I)	Zona Sur-Oeste del CP-12
Migración	Zona Sur

I. Personal

La *Tabla 33* muestra el personal encargado del área de sistemas del CP-12

Tabla 33. Personal del Departamento de Sistemas del CP-12
Fuente: Información recopilada del CP-12

Personal	Descripción
Jefe de Departamento	Jefe del Departamento de Sistemas del CP-12. Persona encargada de los sistemas de bases de datos
Encargado de Redes y Mantenimiento	Personal encargado de redes y mantenimiento de las computadoras
Usuarios del CP-12	Usuarios que utilizan los servicios prestados por el Departamento de Sistemas

3.3.1.2 Valoración de activos del CP-12

Los activos deben analizarse en tres aspectos fundamentales para la Institución como son: Disponibilidad (D), Integridad (I), Confidencialidad (C).

La *Tabla 34* muestra el listado de activos y su valoración.

Tabla 34. Valoración de activos del CP-12
Fuente: Información recopilada del CP-12

CANTIDAD	DESCRIPCIÓN	VALOR			V.
		PROPIO			ACUMULA
		D	I	C	DO
1	BD Sistema Integrado Postgres	5	-	5	5
1	BD Sistema Integrado ORACLE	5	-	-	5
1	Sistema Integrado SIIPNE	5	-	-	5
1	Convertidor TP-LINK WDM Fast Ethernet	5	-	-	5
1	Router ADSL 877 Vo4	5	-	-	5
1	Servidor Proxy	5	-	-	5
1	Router board Mikrotik RG-ENT	5	-	-	5
1	Switch D-Link 10-100	5	-	-	5
1	Antena Omnidireccional	5	-	-	5
3	Nano Station 2.4 GHz	5	-	-	5
32	Computadores de escritorio completos	4	-	5	4.5
1	UPS Central	5	-	-	5
1	Generador eléctrico	5	-	-	5
10	Impresoras multifunción	2	-	-	2
4	Impresoras laser	2	-	-	2
2	Copiadoras	2	-	-	2
1	Sector Operativo	5	-	-	5
1	Sector Administrativo	4	-	-	4
1	Asuntos Internos	4	-	-	4
1	Plana Mayor	5	-	-	5
1	Central Integrada de Atención Ciudadana	4	-	-	4
1	Migración	3	-	-	3
1	Jefe de Departamento	5	-	-	5
1	Encargado de Mantenimiento y Redes	5	-	-	5
Varios	Usuarios del CP-12	3	-	-	3
	Información de carácter privado	5	5	5	5
	Información de carácter público	5	5	1	3.67

De donde:

- Según la metodología MAGERIT, el máximo valor para calificar un activo considerado como primordial es 5 y la mínima valoración es 1 para aquellos activos que no provocan daños considerables en el caso de producirse una falla.
- El valor propio de un activo se debe establecer para cada uno de los tres aspectos indicados.
- El valor acumulado relaciona los valores propios de Disponibilidad, Integridad y Confidencialidad de cada activo.
- No todos los activos pueden valorarse en los tres aspectos definidos, en este caso si no cumple con algún aspecto tiene valor nulo y se representa mediante un guion medio (-) o las iniciales NA (No Aplica).

3.3.2 CONTROL DE AMENAZAS

Este proceso consiste en determinar las amenazas que pueden afectar a cada activo perteneciente a la institución. Las amenazas son sucesos que pueden ocurrir causando daños a los activos. Hay accidentes naturales como inundaciones, terremotos, etc., y desastres industriales en los que se encuentran la contaminación, fallos eléctricos, entre otros, ante los cuales el sistema de información es víctima pasiva.

De la misma manera existen amenazas que pueden ser causadas por las personas, que pueden ser desde un error de usuario hasta un ataque mal intencionado.

- **Valoración de las amenazas**

Para determinar si una amenaza puede ocasionar daños o no a un activo, se debe estimar cuán vulnerable es el activo, para esto es necesario realizar un análisis tomando en cuenta dos criterios:

- 1) Degradación: cuán perjudicado resulta el activo
- 2) Frecuencia: cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. Se suele caracterizar como una fracción del valor del activo.

La *Tabla 35* muestra los valores en porcentaje (%) de degradación de un activo en el caso de que la falla se materialice.

Tabla 35. Valores de degradación de un activo
Fuente: <http://www.slideshare.net/mmujica/mi-defensa>

DEGRADACIÓN DEL ACTIVO (Si la falla ocurre)		
DESCRIPCIÓN	DEGRADACIÓN %	VALOR
Baja	25	1
Media	50	2
Alta	75	3
Total	100	4

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de consecuencias fatales pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acumular un daño considerable. La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos.

La *Tabla 36*, muestra los valores representativos de frecuencia de ocurrencia de amenazas basados en una tasa anual, según indica la metodología MAGERIT. La frecuencia está expresada en tiempo (t).

Tabla 36. Valores representativos de frecuencia de amenazas en activos
Fuente: <http://www.slideshare.net/mmujiica/mi-defensa>

VALOR	TASA	OCURRENCIA	TIEMPO
4	100	muy frecuente	a diario
3	10	Frecuente	mensualmente
2	1	Normal	una vez al año
1	1/10	poco frecuente	cada varios años

- **Valoración del riesgo**

La *Tabla 37* muestra el nivel del riesgo con su respectivo valor numérico, entendiéndose al valor más alto como el más expuesto a amenazas dentro de la institución. La valoración del riesgo se expresa en porcentaje.

Tabla 37. Niveles de valoración del riesgo
Fuente: <http://www.slideshare.net/mmujiica/mi-defensa>

Nivel de factor de riesgo	Valor	Porcentaje %
Bajo	1 a 32	1-25
Medio	33 a 63	26-50
Alto	64 a 94	51-75
Extremadamente alto	95 a 125	76-100

- **Ecuación de cálculo del riesgo**

Para estimar el nivel de riesgo al que está expuesto un activo se debe aplicar la *Ecuación 2*:

$$\text{Riesgo} = \text{Valor_Activo} * \text{Degradación} * \text{Frecuencia} \quad (2)$$

Ecuación 2. Ecuación de cálculo de riesgo

Fuente: <http://www.slideshare.net/mmujuica/mi-defensa>

Donde:

- Valor_Activo (%): Es el valor que indica la importancia del activo para el desarrollo de las actividades del personal dentro de la institución.
- Degradación (%): Indica el valor de perjuicio que sufre un activo, si una amenaza llega a materializarse.
- Frecuencia (t): Indica el valor de frecuencia con la que un activo se ve amenazado.

El resultado obtenido al aplicar la *Ecuación 2* para cada uno de los activos del CP-12, debe ser interpretado en la *Tabla 37* para determinar el nivel de factor del riesgo.

El cálculo de riesgo para cada uno de los activos materiales se encuentra en el ANEXO 3.

3.3.2.1 Cálculo del riesgo inicial del CP-12

Para determinar el nivel de riesgo inicial dentro de la institución es necesario calcular el valor de riesgo de cada uno de los activos considerados como primordiales y que se muestran en la *Tabla 34*, para lo cual se debe aplicar la ecuación correspondiente al cálculo de riesgo.

En la realización del cálculo de riesgo inicial se toma en cuenta solo los activos materiales de la institución, ya que presentan un valor de degradación en un determinado tiempo. Se considera el valor de degradación igual a 2 según la

Tabla 35, debido a que los activos mencionados posteriormente se encuentran fuera del alcance de personal externo a la institución, además de que se encuentran protegidos de amenazas naturales pero pueden existir amenazas internas por parte de personas que laboran en el CP-12. En el caso de la frecuencia de ocurrencia de amenazas, se toma como referencia el valor 3 de acuerdo a la *Tabla 36*, ya que se toma en consideración que puede existir por lo menos una acción mal intencionada en el plazo de un mes dentro de la institución.

El cálculo de riesgo de cada uno de los activos materiales del CP-12 se encuentra en el ANEXO 3

Una vez obtenido el valor de riesgo de cada uno de los activos materiales, se establece el valor promedio del riesgo, aplicando la *Ecuación 3*:

$$\text{Riesgo inicial} = \frac{R_1 + R_2 + \dots + R_n}{\text{Total de activos materiales}} \quad (3)$$

Ecuación 3. Ecuación general de cálculo del riesgo inicial

Fuente: <http://www.slideshare.net/mmujuica/mi-defensa>

Donde:

- R1, R2,.. R_n: Valor de riesgo de cada uno de los activos materiales.
- Total de activos materiales: es el número de activos analizados.

Entonces:

$$\begin{aligned} \text{Riesgo inicial} &= \frac{30 + 30 + 30 + 30 + 30 + 30 + 30 + 27 + 30 + 30 + 12 + 12 + 12}{13} (\%) \\ \text{Riesgo inicial} &= \frac{333}{13} (\%) \\ \text{Riesgo inicial} &= 25.61 (\%) \\ \text{Riesgo inicial} &= \text{Medio} \end{aligned} \quad (4)$$

Ecuación 4. Cálculo total del riesgo inicial

Fuente: <http://www.slideshare.net/mmujuica/mi-defensa>

El valor del riesgo inicial de la institución es de 25.61%, según la *Tabla 37* este número se encuentra entre los valores aceptables de 33 a 63 correspondientes a un nivel medio de factor de riesgo, lo que permite establecer el nivel de madurez de la institución de acuerdo a la *Tabla 38*.

Tabla 38. Cuadro indicativo del nivel de madurez de una institución

Fuente: <http://www.slideshare.net/embed-services/152987>

EFICACIA (%)	NIVEL DE MADUREZ	DESCRIPCIÓN
0 - 9	0	Inexistente
10 - 49	1	Inicial
50 - 89	2	Intuitivo
90 - 94	3	Definido
95 - 99	4	Gestionado
100	5	Optimizado

De acuerdo a la Tabla anterior y con el valor de riesgo inicial calculado igual a 25.61, se deduce que el nivel de madurez del Comando Provincial de Policía “Imbabura No 12” es igual a 1 lo que representa un nivel Inicial y se caracteriza por procesos manuales, políticas y estándares de seguridad inexistentes, la seguridad global de la organización no está bien definida ya que no se tienen procedimientos ni herramientas para administrarla. En algunos casos la seguridad de los sistemas ni siquiera es centralizada y los usuarios de TI poseen todos los permisos y privilegios sobre la información.

La organización debe definir sus políticas de seguridad y con base a ellas, crear los procedimientos asociados.

3.3.3 DETERMINACIÓN DEL IMPACTO

El impacto es considerado como la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos y la degradación que causan las amenazas, se determina el impacto que estas tienen sobre el sistema.

La *Tabla 39* muestra el valor del impacto de una amenaza materializada tomando en cuenta los valores de degradación tanto para Disponibilidad e Integridad de los activos. Este valor está expresado en porcentaje (%).

Tabla 39. Valoración de impactos
Fuente: <http://www.slideshare.net/embed-services/152987>

AMENAZA	DEGRADACIÓN (%)			
	APLICACIONES		SERVIDORES/EQUIPOS	
	Confidencialidad	Disponibilidad	Confidencialidad	Disponibilidad
Incidentes	0	0	5	10
Acceso no autorizado	5	0	5	5

Dentro del campo de incidentes se considera toda amenaza que puede producirse accidentalmente como por ejemplo los incendios, fugas de agua, fallos con la energía eléctrica, cortocircuitos, etc.

3.3.3.1 Impacto acumulado

Se calcula sobre un activo teniendo en cuenta:

- Su valor acumulado
- Las amenazas a las que está expuesto

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, es decir tomando en cuenta los parámetros de Disponibilidad y Confidencialidad.

El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas que deberían existir para proteger los activos.

La fórmula específica para calcular el impacto acumulado se muestra a continuación en la *Ecuación 5*:

$$\text{Impacto}_{acum} \% = \text{Valor}_{acum} * \text{Degradación} \quad (5)$$

Ecuación 5. Ecuación de cálculo del impacto acumulado
Fuente: <http://www.slideshare.net/embed-services/152987>

- **Cálculo del impacto acumulado en los activos del CP-12**

Para realizar el cálculo del impacto es necesario separar los elementos dependientes, posteriormente se aplica la *Ecuación 5*, en cada uno de estos activos y luego se promedia los valores para obtener la cifra final correspondiente al impacto acumulado. La *Tabla 40* muestra estos valores.

Tabla 40. Valores del impacto acumulado en los activos dependientes
Fuente: Información recopilada del CP-12

ACTIVOS DEPENDIENTES	INCIDENTES			ACCESOS NO AUT.		
	D	C	T	D	C	T
Convertidor TP-LINK	$5 \times 0.05 = 0.25$	$5 \times 0.1 = 0.5$	0.75	$5 \times 0.05 = 0.25$	$5 \times 0.05 = 0.25$	0.5
Servidor Proxy	$5 \times 0.05 = 0.25$	$5 \times 0.1 = 0.5$	0.75	$5 \times 0.05 = 0.25$	$5 \times 0.05 = 0.25$	0.5
Router Mikrotik	$5 \times 0.05 = 0.25$	$5 \times 0.1 = 0.5$	0.75	$5 \times 0.05 = 0.25$	$5 \times 0.05 = 0.25$	0.5
Switch D-Link	$5 \times 0.05 = 0.25$	$5 \times 0.1 = 0.5$	0.75	$5 \times 0.05 = 0.25$	$5 \times 0.05 = 0.25$	0.5
Antena Omnidireccional	$5 \times 0.05 = 0.25$	$5 \times 0.1 = 0.5$	0.75	$5 \times 0.05 = 0.25$	$5 \times 0.05 = 0.25$	0.5
Nano Station	$5 \times 0.05 = 0.25$	$5 \times 0.1 = 0.5$	0.75	$5 \times 0.05 = 0.25$	$5 \times 0.05 = 0.25$	0.5
PC's de escritorio	$4 \times 0.05 = 0.20$	$5 \times 0.1 = 0.5$	0.70	$4 \times 0.05 = 0.20$	$5 \times 0.05 = 0.25$	0.45
UPS Central	$5 \times 0.05 = 0.25$	$5 \times 0.1 = 0.5$	0.75	$5 \times 0.05 = 0.25$	$5 \times 0.05 = 0.25$	0.5
Generador eléctrico	$5 \times 0.05 = 0.25$	$5 \times 0.1 = 0.5$	0.75	$5 \times 0.05 = 0.25$	$5 \times 0.05 = 0.25$	0.5
PROMEDIO TOTAL			0.74	TOTAL		0.49

De donde:

- Los incidentes no provocados causan un impacto del 74 % en activos.
- Los accesos no autorizados provocan un impacto del 49 % a los activos.

3.3.3.2 Impacto repercutido

Se calcula sobre un activo teniendo en cuenta:

- Su valor propio
- Las amenazas a que están expuestos los activos de los que depende.

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada. El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre los sistemas de información.

- **Cálculo del impacto repercutido en los activos del CP-12**

La *Tabla 41*, muestra el cálculo del impacto repercutido sobre los activos del CP-12 que son independientes y se utiliza su valor propio.

Tabla 41. Valores del impacto repercutido en los activos independientes

Fuente: Información recopilada del CP-12

ACTIVOS	INCIDENTES			ACCESOS NO AUT.		
	D	C	T	D	C	T
INDEPENDIENTES						
BD Postgres	$5*0=0$	$5*0=0$	0	$5*0=0$	$5*0.05=0.25$	0.25
BD ORACLE	$5*0=0$	$5*0=0$	0	$5*0=0$	$5*0.05=0.25$	0.25
Sistema Integrado	$5*0=0$	$5*0=0$	0	$5*0=0$	$5*0.05=0.25$	0.25
SIIPNE						
Impresora multifunción	$2*0.05=0.1$	$0*0.1=0$	0.1	$2*0.05=0.1$	$0*0.05=0$	0.1
Impresoras laser	$2*0.05=0.1$	$0*0.1=0$	0.1	$2*0.05=0.1$	$0*0.05=0$	0.1
Copiadoras	$2*0.05=0.1$	$0*0.1=0$	0.1	$2*0.05=0.1$	$0*0.05=0$	0.1
Información de carácter privado	$4*0=0$	$5*0=0$	0	$4*0=0$	$5*0.05=0.25$	0.25
Información de carácter público	$5*0=0$	$1*0=0$	0	$5*0=0$	$1*0.05=0.05$	0.05
	TOTAL		0.038	TOTAL		0.17

De donde:

- Los incidentes no provocados causan un impacto del 3.8 % en activos.
- Los accesos no autorizados provocan un impacto del 17 % a los activos.

3.3.4 DETERMINACIÓN DEL RIESGO

El riesgo es la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, se puede determinar el riesgo tomando en cuenta la frecuencia de ocurrencia. La *Tabla 42* muestra los riesgos más comunes a los que están expuestos los activos dentro del Comando Provincial de Policía.

3.3.4.1 Riesgo acumulado

Se calcula sobre un activo teniendo en cuenta:

- El impacto acumulado sobre un activo debido a una amenaza
- La frecuencia de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración.

La fórmula que permite calcular el riesgo acumulado es la que se muestra a continuación en la *Ecuación 7*, el riesgo acumulado está expresado en porcentaje (%).

$$\text{Riesgo}_{acum} = \text{Impacto}_{acum} * \text{Frecuencia} \quad (6)$$

Ecuación 6. Ecuación de cálculo del riesgo acumulado
Fuete: <http://www.slideshare.net/embed-services/152987>

Los valores de frecuencia de ocurrencia de una amenaza se muestran en la *Tabla 36*.

- **Cálculo del riesgo acumulado en los activos del CP-12**

Para el caso de ocurrencia de incidentes se toma como referencia un valor de frecuencia igual a 2 según la *Tabla 36*, debido a que no son comunes este tipo de sucesos.

En base a esto se puede determinar el riesgo acumulado provocado por incidentes en los activos del CP-12, aplicando la *Ecuación 6*.

El cálculo del riesgo acumulado debido a incidentes y a accesos no autorizados en los activos del CP-12 se muestra en la *Ecuación 7* y *Ecuación 8*, respectivamente.

$$\boxed{Riesgo_{acum} = 7.4 * 2 = 14.8 (\%)} \quad (7)$$

Ecuación 7. Cálculo del riesgo acumulado debido a incidentes en los activos el CP-12
Fuente: <http://www.slideshare.net/embed-services/152987>

Para el caso de accesos no autorizados se toma como referencia un valor igual a 3 según la *Tabla 36*, ya que suceden con mayor frecuencia.

Entonces, es posible determinar el riesgo acumulado debido a accesos no autorizados en los activos del CP-12.

$$\boxed{Riesgo_{acum} = 4.9 * 3 = 14.7 (\%)} \quad (8)$$

Ecuación 8. Cálculo del riesgo acumulado debido a accesos no autorizados en los activos del CP-12
Fuente: <http://www.slideshare.net/embed-services/152987>

Estos valores determinan que el riesgo acumulado dentro del CP-12 es bajo pero no insignificante, pero se debe tomar en cuenta la inexistencia de medidas que permitan contrarrestar a este tipo de riesgos.

3.3.4.2 Riesgo repercutido

Se calcula sobre un activo teniendo en cuenta:

- El impacto repercutido sobre un activo debido a una amenaza y
- La frecuencia de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración.

La fórmula que permite calcular el riesgo repercutido es la que se muestra a continuación en la *Ecuación 9*, el riesgo repercutido está expresado en porcentaje (%).

$$\boxed{Riesgo_{rep} = Impacto_{rep} * Frecuencia (\%)} \quad (9)$$

Ecuación 9. Ecuación de cálculo del riesgo repercutido
Fuente: <http://www.slideshare.net/embed-services/152987>

- **Cálculo del riesgo repercutido en los activos del CP-12**

Para poder realizar el cálculo del riesgo repercutido debido a incidentes, se toma como referencia el mismo valor de frecuencia utilizado para calcular el riesgo acumulado, es decir un valor igual a 2. El cálculo para este caso se muestra en la *Ecuación 10*.

$$\boxed{Riesgo_{rep} = 0.4 * 2 = 0.8 (\%)} \quad (10)$$

Ecuación 10. Cálculo del riesgo repercutido debido a incidentes en los activos el CP-12
Fuente: <http://www.slideshare.net/embed-services/152987>

Para el caso de accesos no autorizados se utiliza un valor de frecuencia igual a 3. El cálculo para este caso se muestra en la *Ecuación 11*.

$$\boxed{Riesgo_{rep} = 1.7 * 3 = 5.1(\%)} \quad (11)$$

Ecuación 11. Cálculo del riesgo repercutido debido a accesos no autorizados en los activos el CP-12
Fuente: <http://www.slideshare.net/embed-services/152987>

Estos valores determinan que el riesgo repercutido debido a accesos no autorizados dentro del CP-12 es mal alto que el producido por incidentes, pero se debe tomar en cuenta la inexistencia de medidas que permitan contrarrestar a este tipo de riesgos.

3.3.5 SALVAGUARDAS

Es importante mencionar que al momento el CP-12 no cuenta con medidas básicas de protección de la información, así como tampoco de sus activos más importantes.

Es necesario planificar el conjunto de salvaguardas pertinentes para disminuir tanto el impacto como el riesgo, reduciendo la degradación del activo (minimizando el daño), o reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

Para esto es necesario:

1. Establecer una política de la Organización al respecto, es decir directrices generales de quién es responsable de cada actividad.
2. Establecer objetivos a satisfacer para poder decir que la amenaza ha sido minimizada.
3. Establecer procedimientos de lo que se debe hacer.
4. Definir salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para minimizarlas.
5. Definir controles que permitan saber que todo lo anterior está funcionando según lo previsto

CAPÍTULO IV

DISEÑO E IMPLEMENTACIÓN DEL SGSI

Este capítulo abarca el diseño del SGSI, el desarrollo de políticas de seguridad y la implementación de herramientas de gestión para el CP-12. Se describe el funcionamiento y características de cada herramienta utilizada.

4.1 DISEÑO DEL SGSI

El diseño del SGSI está basado en 11 objetivos de control, cada uno de ellos debe cumplir con los requisitos que se muestran en la *Figura 17*.

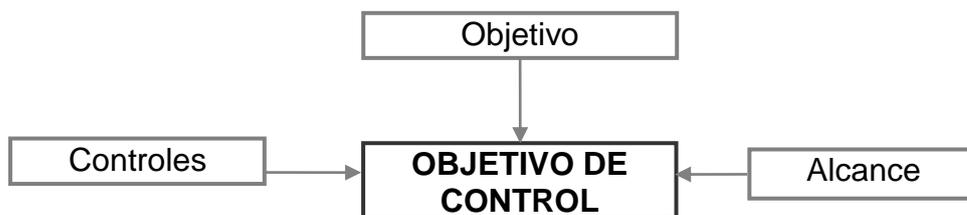


Figura 17. Requisitos de desarrollo para objetivos de control
Fuente: Norma ISO 27002

4.1.1. POLÍTICAS DE SEGURIDAD BASADAS EN OBJETIVOS DE CONTROL

Las políticas de seguridad basadas en objetivos de control tienen como finalidad brindar una guía de procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

Los beneficios de un sistema de seguridad con políticas claramente concebidas y bien elaboradas son inmediatos, ya que el CP-12 trabajará sobre una plataforma confiable. Con la implementación de las políticas se logran los objetivos de control indicados en el diseño del SGSI.

Las políticas descritas en este documento están enfocadas en dar cumplimiento a los objetivos de control implementados y fueron elaboradas en conjunto con el Jefe del departamento de Sistemas, Ing. Ángel Núñez y puestas a consideración del Comandante General del CP-12 para la respectiva aprobación, de igual manera la selección de las herramientas se basa en la funcionalidad que presta cada una de ellas y el soporte que brinda a los controles mencionados en la norma ISO 27002.

A continuación se listan los objetivos de control:

1. Política de Seguridad
2. Organización de la seguridad de la información
3. Gestión de activos
4. Seguridad de los recursos humanos
5. Seguridad física y ambiental (Entorno físico de los activos)
6. Gestión de las comunicaciones y operaciones
7. Control de acceso
8. Adquisición, desarrollo y mantenimiento de los sistemas de información
9. Gestión de incidentes en la seguridad de la información
10. Gestión de la continuidad comercial
11. Cumplimiento

4.1.1.1. Política de Seguridad

La *Tabla 43*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 43. Objetivo, alcance y controles de la política de seguridad

Fuente: <http://www.iso27000.es>

<p>Proporcionar la guía y apoyo de la Dirección para la seguridad de la información en relación a los requerimientos</p>	
<p>OBJETIVO: de la institución y a las leyes y regulaciones vigentes dentro del CP-12.</p>	
ALCANCE	CONTROLES
<p>a) Proteger los recursos de información del Comando Provincial de Policía “Imbabura” No. 12, y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.</p>	<p>El Comando General debe establecer una política clara y que estén acorde a los objetivos de la institución y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la organización.</p>
<p>b) Asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.</p>	
<p>c) Mantener la Política de Seguridad del CP-12 actualizada, a efectos de asegurar su vigencia y nivel de eficacia.</p>	

- POLÍTICAS DISEÑADAS

ACCESO A LA INFORMACIÓN

- El personal que labora para el CP-12 debe tener acceso sólo a la información necesaria para el desarrollo de sus actividades.
- En el caso de personas ajenas al CP-12, la persona responsable de generar la información debe autorizar sólo el acceso indispensable de

acuerdo con el trabajo realizado por estas personas, previa justificación.

Este proceso debe ser documentado.

- El otorgamiento de acceso a la información debe regularse mediante las normas y procedimientos definidos para tal fin.
- Todos los privilegios para el uso de los sistemas de información de la Institución deben terminar inmediatamente después de que el trabajador deje de prestar sus servicios a la Institución. El proceso de eliminación de privilegios debe estar regulado por una norma y procedimiento apropiado.
- Los proveedores o terceras personas solamente deben tener privilegios durante el período del tiempo requerido para llevar a cabo las funciones aprobadas.
- Para dar acceso a la información se tendrá en cuenta la clasificación asignada por la Institución.
- Se debe efectuar un registro de los eventos acontecidos a los diversos recursos informáticos de la plataforma tecnológica
- Basándose en el registro anterior, se debe hacer un seguimiento a los accesos realizados por los usuarios tanto a los sistemas, como a los datos.

- **HERRAMIENTA IMPLEMENTADA**

Para dar cumplimiento a este objetivo se utilizó la herramienta Controlador de Dominio. La descripción de dicha herramienta se encuentra en el Capítulo IV.

4.1.1.2. Organización de la seguridad de la información

La *Tabla 44*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 44. Objetivo, alcance y controles de la política de organización

Fuente: <http://www.iso27000.es>

OBJETIVO: Gestionar la seguridad de la información dentro del CP-12	
ALCANCE	CONTROLES
a) Se debe establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro del CP-12.	Los miembros de la Dirección deben respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización.
b) La Comandancia General debe aprobar la política de seguridad de la información, asignar los roles de seguridad, coordinar y revisar la implantación de la seguridad en toda la organización.	
c) Si fuera necesario, se debe establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información.	Se debe definir claramente todas las responsabilidades para la seguridad de la información.
d) Debe fomentarse un enfoque multidisciplinario de la seguridad de la información que implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros y la gestión de riesgos.	Se debe identificar y revisar regularmente en los acuerdos aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la institución.

- POLÍTICAS DISEÑADAS

ADMINISTRACIÓN DE CAMBIOS

Esta política es referente al desarrollo de aplicaciones y a los cambios en configuraciones de los servidores.

- Todo cambio (creación y modificación de programas, módulos, reportes, etc.) que afecte los recursos informáticos, debe ser solicitado por los usuarios y aprobado formalmente por el responsable de la administración del mismo.
- Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.
- Cualquier cambio debe quedar formalmente documentado desde su solicitud hasta su implantación.
- La documentación servirá de herramienta para efectuar el seguimiento y garantizar el cumplimiento de los procedimientos definidos.
- Todo cambio relacionado con modificación de accesos, mantenimiento de software o modificación de configuraciones debe realizarse de forma tal que no disminuya la seguridad existente.

- **HERRAMIENTA IMPLEMENTADA**

Para dar cumplimiento a este objetivo se utilizó la herramienta OTRS. La descripción de dicha herramienta se encuentra en el Capítulo IV.

4.1.1.3. Gestión de activos

La *Tabla 45*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 45. Objetivo, alcance y controles de la política de gestión de activos

Fuente: <http://www.iso27000.es>

Alcanzar y mantener una protección adecuada de los activos	
OBJETIVO:	de la institución asegurando que se aplica un nivel de protección adecuado a la información.
ALCANCE	CONTROLES
a) Todos los activos deben ser justificados y tener asignado un usuario responsable.	Todos los activos deben estar claramente identificados manteniendo un inventario con los
b) Se debe identificar a los usuarios responsables para todos los activos y asignarles la responsabilidad del mantenimiento y controles adecuados.	más importantes. La información debe clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la institución.

- POLÍTICAS DISEÑADAS

ADMINISTRACIÓN DE LA SEGURIDAD

- El análisis de riesgos para los Recursos Informáticos se debe ejecutar al menos una vez al año.
- Cualquier mejora, actualización o cambios asociados a los recursos tomados en cuenta en el análisis de riesgos, deben ser precedidos por una nueva evaluación del riesgo.
- Cualquier brecha de seguridad o sospecha de mala utilización en el Internet o la Intranet, de los recursos informáticos a cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial al personal de Seguridad Informática.
- El personal que realiza labores de administración es responsable de los controles sobre los activos.

- El personal encargado de la Seguridad de Información es el encargado de divulgar los estándares, políticas y procedimientos en dicha materia.
- El personal encargado de la Seguridad de Información es responsable de darle seguimiento a las políticas de relacionadas con dicha materia y reportar al Jefe del Departamento. En caso de detectarse un incumplimiento, el personal encargado de la Seguridad Informática reportará al Jefe del Departamento y a las oficinas de control interno.

- HERRAMIENTA IMPLEMENTADA

Para dar cumplimiento a este objetivo se utilizó la herramienta OCS Inventory. La descripción de dicha herramienta se encuentra en el Capítulo IV.

4.1.1.4. Seguridad de los recursos humanos

La *Tabla 46*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 46. Objetivo, alcance y controles de la política de seguridad de Recursos Humanos

Fuente: <http://www.iso27000.es>

OBJETIVO:	ALCANCE	CONTROLES
<p>Asegurar que el personal, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen.</p> <p>a) Las responsabilidades de la seguridad se deben definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del mismo.</p>		<p>Como parte de su obligación contractual, personal, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la institución para la seguridad de información.</p>

- POLÍTICAS DISEÑADAS

SEGURIDAD PARA TERCEROS USUARIOS

- Los propietarios de recursos informáticos que no sean propiedad de la Institución deben garantizar la legalidad del uso de dicho recurso. Se debe establecer un documento de acuerdo oficial entre las partes.
- Si se requiere utilizar recursos informáticos de la Institución para el funcionamiento de servicios u otras actividades que no sean propios de la Institución, dichos recursos serán administrados por el CP-12.
- Si es necesario que un usuario ajeno a la Institución acceda a algún recurso informático, se debe firmar un acuerdo de confidencialidad con dicho usuario.
- La conexión entre sistemas de la Institución y sistemas externos debe ser aprobada y certificada por el personal de Seguridad Informática para no afectar la seguridad de la información interna.
- Los equipos de terceros que se conecten a la red, deben cumplir con todas las normas internas de la Institución.
- La Institución se reserva el derecho de aprobar y/o cancelar la conexión con terceros.

- HERRAMIENTA IMPLEMENTADA

Para dar cumplimiento a este objetivo se utilizó la herramienta UTM. La descripción de dicha herramienta se encuentra en el Capítulo IV.

4.1.1.5. Seguridad física y ambiental (Entorno físico de los activos)

Esta política hace referencia al espacio físico y a las condiciones ambientales dentro de las instalaciones en donde están ubicados los activos del CP-12. La *Tabla 47*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 47. Objetivo, alcance y controles de la política de seguridad física y ambiental
Fuente: <http://www.iso27000.es>

OBJETIVO:	Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización. Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.	
	ALCANCE	CONTROLES
	a) Los servicios de procesamiento de información sensible deben ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deben estar protegidas físicamente contra accesos no autorizados, daños e interferencias.	Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.
	b) Debe protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.	Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. Se debe proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños.
	c) Así mismo, se debe considerar la ubicación y la baja de los equipos.	

- POLÍTICAS DISEÑADAS

SEGURIDAD FÍSICA

- Se deben implementar mecanismos de control de acceso tales como puertas de seguridad, RFID, sistema de alarma y circuitos cerrados de

televisión inteligentes en las dependencias críticas (por ejemplo, local de los servidores y puertas de entrada principales).

- Si un trabajador se encuentra a un visitante en un área restringida, el visitante debe ser cuestionado acerca de su propósito en el área y se debe informar a los responsables de la seguridad del edificio.
- En el local de los servidores se debe implementar un sistema automatizado para eliminar los incendios.
- Los locales desde donde se tiene acceso al cableado deben ser catalogados como zonas de alto riesgo, limitando el acceso a los mismos.
- Se debe registrar el ingreso y salida de todas las computadoras, módems y otros equipos de comunicaciones ajenos a la Institución.
- Los equipos no deben moverse o reubicarse sin la aprobación previa.
- Los empleados de la Institución se comprometen a NO utilizar la red regulada de energía para conectar otros equipos que no sean su estación de trabajo y/o la impresora que se le haya asignado.
- El personal ajeno a la Institución no está autorizado a utilizar los recursos informáticos de la Institución.

- **HERRAMIENTA IMPLEMENTADA**

Para dar cumplimiento a este objetivo se utilizó la herramienta OCS Inventory.

La descripción de dicha herramienta se encuentra en el Capítulo IV.

4.1.1.6. Gestión de las comunicaciones y operaciones

La *Tabla 48*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 48. Objetivo, alcance y controles de la política comunicaciones y operaciones

Fuente: <http://www.iso27000.es>

Asegurar la operación correcta y segura de los recursos de	
OBJETIVO:	tratamiento de información. Proteger la integridad del software y de la información.
ALCANCE	CONTROLES
a) Se deben establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información.	Se debe documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten.
b) Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.	Se debe controlar los cambios en los sistemas y en los recursos de tratamiento de la información.
c) Se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso.	La separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.

- POLÍTICAS DISEÑADAS

SEGURIDAD EN COMUNICACIONES

- La topología de red (direccionamiento IP, configuraciones, información relacionada con las medidas de seguridad, etc.) debe considerarse como información RESERVADA.
- Todas las conexiones a otras redes de datos deben protegerse mediante cifrado, detección de intrusos, autenticación y control de acceso.
- La salida de información hacia otras Instituciones o Empresas debe estar amparada por un acuerdo de confidencialidad.
- Las comunicaciones con equipos externos se realizarán utilizando conexiones seguras.

- Toda la información con un nivel de sensibilidad igual o superior a CONFIDENCIAL que se transmita por las redes de la Institución e Internet debe ser cifrada.

ALMACENAMIENTO Y RESPALDO

- La información que genera y soporta la infraestructura de tecnología informática del CP-12 deberá ser almacenada y respaldada, garantizando su disponibilidad.
- Se debe definir el procedimiento de crear las copias de respaldo, así como los tiempos de retención y rotación de dichas copias.
- El personal es responsable de la información generada y almacenada en sus estaciones de trabajo, así como el respaldo de la misma.
- El Departamento de Sistemas es el ente autorizado a realizar el seguimiento y control del cumplimiento de las políticas relacionadas con los respaldos.

- HERRAMIENTA IMPLEMENTADA

Para dar cumplimiento a este objetivo se utilizó las herramientas UTM y servidor de archivos conjuntamente con Cobian Backup y Truecrypt. La descripción de dicha herramienta se encuentra en el Capítulo IV.

4.1.1.7. Control de acceso

La *Tabla 49*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 49. Objetivo, alcance y controles de la política de control de acceso
Fuente: <http://www.iso27000.es>

OBJETIVO: Controlar los accesos a la información.	
ALCANCE	CONTROLES
a) Se debe controlar los accesos a la información, los recursos de tratamiento de la información y los procesos importantes en base a las necesidades de seguridad del CP-12	Se debe establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad de la institución. Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.

- POLÍTICAS DISEÑADAS

CONTRASEÑAS

- Capacitar a los usuarios en la creación de contraseñas.
- Garantizar que las contraseñas cumplan con las características siguientes:
 - ~ Utilizar al menos 8 caracteres.
 - ~ Utilizar letras mayúsculas, minúsculas, símbolos y números.
 - ~ Los usuarios deben cambiar las contraseñas cada 120 días.
 - ~ Los administradores deben cambiar las contraseñas cada 90 días.
 - ~ No deben reutilizarse contraseñas.
- Aplicar cada 60 días revisiones de la calidad de las contraseñas

CONTROL DE ACCESO

- Cada usuario debe disponer de un nombre de usuario y contraseña única.

- Las contraseñas son responsabilidad de sus propietarios. Dichas contraseñas serán generadas por el administrador y entregadas al usuario.
- Las contraseñas solo deben ser conocidas por su propietario.
- Los usuarios son responsables de las actividades llevadas a cabo con su nombre de usuario y/o contraseña.
- Las contraseñas deben tener una fecha de caducidad definida en base a la sensibilidad de la información a proteger. Para los sistemas de acceso a las estaciones de trabajo, se recomienda cambiarlas cada 90 días. Las claves de administración deben cambiarse cada 60 días.
- Los nombres de usuario no deben estar basados en las funciones de trabajo. Los nombres de usuario identifican a personas específicas. Para la asignación de nombres de usuario se toma en cuenta la primera letra del nombre y el apellido completo del usuario, por ejemplo:

Sergio Ramos: sramos

Norman Páez: npaez
- Se deben tener definidos los perfiles de usuario de acuerdo a la función y cargo de los usuarios.
- El nivel de administrador de los sistemas críticos debe estar controlado. Es decir, las actividades realizadas por alguien con nivel/privilegio de administrador, deben ser supervisadas.
- Antes de diseñar o adquirir un sistema, se deben especificar los requerimientos de seguridad necesarios.
- Los ambientes de desarrollo, pruebas y producción deben ser independientes.

- HERRAMIENTA IMPLEMENTADA

Para dar cumplimiento a este objetivo se utilizó las herramientas RPG y Controlador de Dominio. La descripción de dichas herramientas se encuentra en el Capítulo IV.

4.1.1.8. Adquisición, desarrollo y mantenimiento de los sistemas de información

La *Tabla 50*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 50. Objetivo, alcance y controles de la política de los sistemas de información
Fuente: <http://www.iso27000.es>

OBJETIVO:	Garantizar que la seguridad es parte integral de los sistemas de información.	
	ALCANCE	CONTROLES
	b) Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones propias de la institución, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios. Los requisitos de seguridad deben ser identificados y acordados previamente al desarrollo y/o implantación de los sistemas de información.	Evitar errores humanos, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

- POLÍTICAS DISEÑADAS

SEGURIDAD DE LA INFORMACIÓN

- Los usuarios son responsables de la información que manejan.
- Ningún personal del CP-12 debe suministrar cualquier información de la Institución a ningún ente externo sin las autorizaciones respectivas.
- Todos los usuarios tienen la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información que maneje,

especialmente si dicha información ha sido clasificada con algún nivel distinto al normal.

- Todo el personal debe firmar y renovar cada año, un acuerdo de confidencialidad y buen manejo de la información.
- Después de que el trabajador deje de prestar sus servicios, se compromete a entregar toda la información relacionada al trabajo realizado por él.
- Después de que el trabajador deje de prestar sus servicios, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante su trabajo en la Institución, directamente o través de terceros.
- La persona que detecte el mal uso de la información está en la obligación de reportar el hecho.
- Las políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar.

- **HERRAMIENTA IMPLEMENTADA**

Para dar cumplimiento a este objetivo se utilizó las herramientas Controlador de Dominio, Nagios y MRTG. La descripción de dichas herramientas se encuentra en el Capítulo IV.

4.1.1.9. Gestión de incidentes en la seguridad de la información

La *Tabla 51*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 51. Objetivo, alcance y controles de la política de gestión de incidentes
 Fuente: <http://www.iso27000.es>

<p>OBJETIVO: Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.</p>	
ALCANCE	CONTROLES
<p>a) Se deben establecer las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.</p> <p>b) Se debe aplicar un proceso de mejora continua en respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de información.</p>	<p>Se debe comunicar los eventos en la seguridad de información lo más rápido posible.</p> <p>Todo el personal, contratistas y terceros que son usuarios de los sistemas y servicios de información deben anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.</p>

- POLÍTICAS DISEÑADAS

CONTINGENCIA

- Se debe preparar, actualizar y validar periódicamente el plan de contingencias. Dicho plan debe garantizar la continuidad de operaciones en caso de desastres como terremotos, explosiones, actos terroristas, inundaciones etc.
- En dicho plan se describirán los procedimientos de neutralización y recuperación ante cualquier evento que afecte la confidencialidad, integridad y disponibilidad de la información.
- Partiendo de los resultados obtenidos en el análisis de riesgos, se determinarán las acciones a realizar para minimizar el riesgo.

- HERRAMIENTA IMPLEMENTADA

Para dar cumplimiento a este objetivo se utilizó la herramienta OTRS. La descripción de dichas herramientas se encuentra en el Capítulo IV.

4.1.1.10. Gestión de la continuidad comercial

La *Tabla 52*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 52. Objetivo, alcance y controles de la política de gestión de continuidad

Fuente: <http://www.iso27000.es>

Reaccionar a la interrupción de actividades y proteger sus	
OBJETIVO:	procesos críticos frente a desastres o grandes fallos de los sistemas de información.
ALCANCE	CONTROLES
a) Se debe implantar un proceso de gestión para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad mediante una combinación de controles preventivos y de recuperación.	Se debe identificar los eventos que puedan causar interrupciones a los procesos junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.
b) Se deben analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio, disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos.	Se debe desarrollar e implantar planes de mantenimiento o recuperación de las operaciones para asegurar la disponibilidad de la información, tras la interrupción o fallo de los procesos críticos de negocio.

- POLÍTICAS DISEÑADAS

SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS

- No se utilizarán servicios externos de correo electrónico.

- La Institución se reserva el derecho de acceder a todos los mensajes enviados por medio del correo electrónico. Para este efecto, cada usuario autorizará por escrito a la Institución a que realice las revisiones y/o auditorías respectivas directamente o a través de terceros.
- El personal no debe utilizar versiones escaneadas de firmas hechas a mano para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmada por la persona que la envía.
- La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la Institución. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.
- El personal que haya recibido aprobación para tener acceso a Internet, deberá aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.
- Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la oficina de informática, no utilizar el computador y desconectarlo de la red.

- **HERRAMIENTA IMPLEMENTADA**

Para dar cumplimiento a este objetivo se utilizó la herramienta iTALC. La descripción de dichas herramientas se encuentra en el Capítulo IV.

4.1.1.11. Cumplimiento

La *Tabla 53*, muestra el objetivo, alcance y controles relacionados con esta política.

Tabla 53. Objetivo, alcance y controles de la política de cumplimiento

Fuente: <http://www.iso27000.es>

OBJETIVO:	Evitar incumplimientos de ley, estatuto, regulación u obligación establecida dentro de la institución.	
	ALCANCE	CONTROLES
	a) El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad vigentes. Los requisitos legales específicos deben ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados.	Los registros importantes se deben proteger de la pérdida, destrucción y falsificación, de acuerdo al reglamento establecido y que esté en vigencia dentro de la institución.

- POLÍTICAS DISEÑADAS

REGISTROS

Se definen los documentos de registro que se requieran para el control de la actividad, de acuerdo a los lineamientos del sistema de seguridad diseñado, pudiéndose considerarse entre otros los siguientes:

- Registro de inspecciones.
- Registro y control de los soportes.
- Registro de software de nueva adquisición.
- Registro de entrada, salida y movimiento de tecnologías de información.
- Registro de incidencias de la Seguridad Informática.

SOFTWARE UTILIZADO

- El software utilizado debe garantizar la integridad de los datos.
- Se debe crear una cultura en los usuarios de la Institución sobre las implicaciones del uso de software ilegal. Dicha cultura se fomentará mediante la publicación de boletines y/o charlas al respecto.
- Se mantendrá un inventario de las licencias de software del CP-12 que permita su administración y control. El uso de este inventario permitirá detectar el uso de software no licenciado.
- Se establecerá un reglamento que limite el uso de software de demostración en las estaciones de la Institución.

ACTUALIZACIÓN DE HARDWARE

- Cualquier alteración en la configuración del hardware (procesador, memoria, tarjetas adicionales, etc.) debe ser autorizado por el personal responsable de los recursos.
- La reparación de los equipos que implique la apertura de los mismos será realizada solo por personal autorizado.
- El movimiento y/o re-ubicación de equipos (PC, servidores, equipamiento activo) debe documentarse y estar debidamente autorizado.

LISTADO DE USUARIOS CON ACCESO A REDES DE ALCANCE GLOBAL

- Se dispondrá de un Listado de Usuarios autorizados, especificando Nombre, Apellidos y Cargo que ocupa en la Institución, así como los Servicios para los que está autorizado.

- HERRAMIENTA IMPLEMENTADA

Para dar cumplimiento a este objetivo se utilizó la herramienta UTM. La descripción de dichas herramientas se encuentra en el Capítulo IV.

4.2. ARQUITECTURA DE RED IMPLEMENTADA

Previo a la implementación de herramientas se estructuró la red del CP-12 como se muestra en la *Figura 18*.

De acuerdo a las necesidades de la institución y sus debilidades, la solución planteada pretende mejorar los niveles de seguridad reduciendo al máximo las vulnerabilidades.

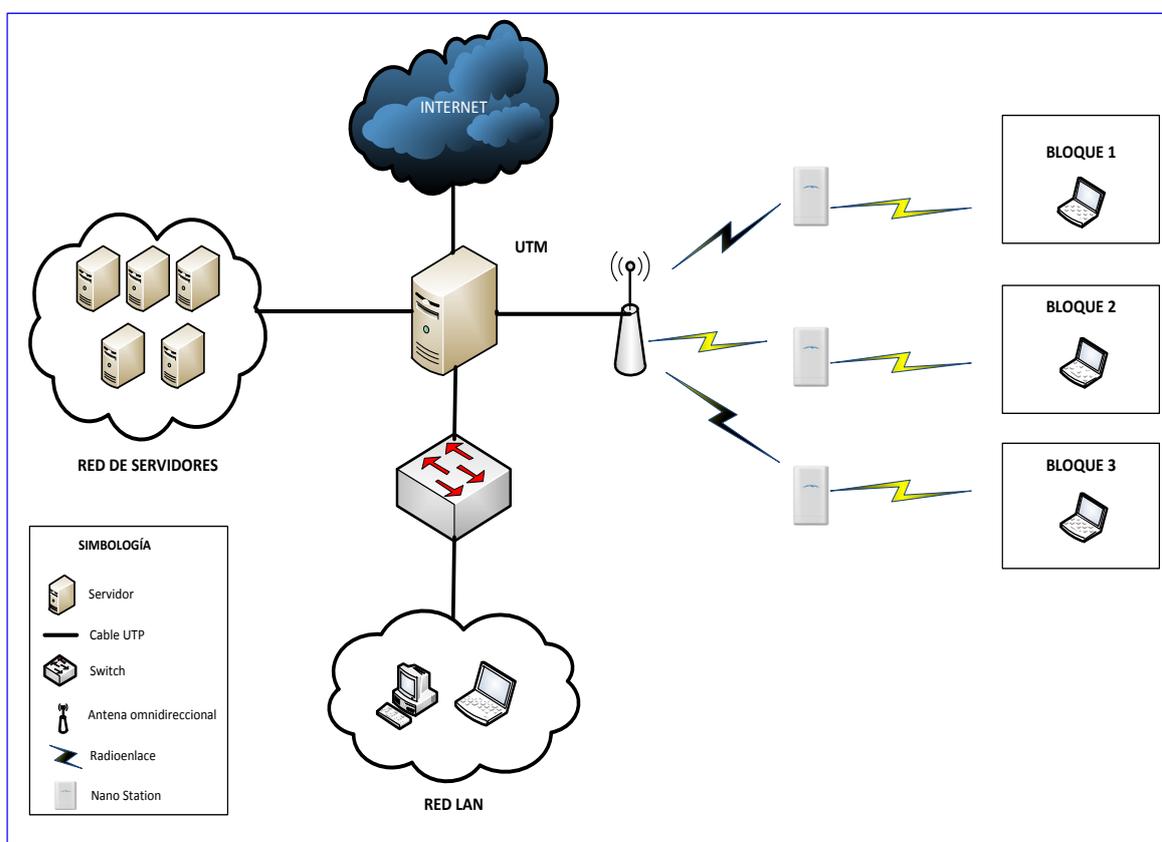


Figura 18. Arquitectura de red implementada en el CP-12
Fuente: Microsoft Visio 2010

La arquitectura de red implementada utiliza un servidor UTM desarrollado sobre software libre que controla el acceso de usuarios a los recursos de red del CP-12. Con la implementación de este servidor se reduce la posibilidad de obtención de información de manera no autorizada, además se controla el acceso de los usuarios hacia las aplicaciones necesarias para el desarrollo de sus actividades, de igual manera a los usuarios de la red LAN hacia servicios públicos. Sobre el servidor se encuentran funcionando los servicios firewall, proxy, IDS/IPS y NTOP. Además, la red está dividida en 3 zonas que limitan con el UTM implementado:

- *Zona LAN.*- Es la red interna LAN del CP-12 en donde se encuentran todos los usuarios. Esta zona es usada para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.
- *Zona de Servidores.*- Esta zona debe ser independiente del resto para poder controlar el acceso tanto de usuarios internos como de usuarios externos a la institución.
- *Zona Wireless.*- Esta zona al ser independiente permite controlar todo el tráfico desde y hacia la subred inalámbrica ya que no se tiene control de los usuarios que intentan acceder de esta manera.

4.2.1. REDISTRIBUCIÓN DE DIRECCIONAMIENTO IP

Para optimizar la distribución de direcciones IP se aplica máscaras de subred de tamaño variable VLSM (Variable Length Subnet Mask), reflejándose en la *Tabla 54*.

*Tabla 54. Redistribución del direccionamiento IP
Fuente: Microsoft Excel 2010*

DIRECCIONAMIENTO IP			
DESCRIPCIÓN	NOMBRE DE LA RED	MÁSCARA	GATEWAY
Red local	10.10.1.0	255.255.255.128	10.10.1.1
Red Wireless	10.10.1.128	255.255.255.192	10.10.1.129
Red de servidores	10.10.1.192	255.255.255.240	10.10.1.193
Red de Internet	190.36.191.136	255.255.255.248	190.36.191.137

4.3. IMPLEMENTACIÓN DE HERRAMIENTAS

Para el presente proyecto se ha optado por utilizar el sistema operativo GNU/LINUX UBUNTU server 10.04 LTS³⁶, para la implementación de herramientas debido a las siguientes características:

- Instalación sencilla.
- Posee una gran cantidad de elementos de software diferentes (paquetes).
- Es una distribución totalmente gratuita.
- Código fuente abierto.
- Fácil de actualizar.
- Seguimiento de actualizaciones.
- El soporte es apoyado por la comunidad a nivel mundial.
- No se necesita de entorno gráfico para los servicios a instalarse.

~ **UBUNTU SERVER 10.04 LTS**

Ubuntu es un sistema operativo que utiliza un núcleo Linux, y su origen está basado en Debian. Ubuntu está orientado al usuario novel y promedio,

³⁶LTS: Long Term Support (Soporte técnico extendido). - Los lanzamientos LTS contarán con actualizaciones de seguridad de paquetes de software por un periodo de tiempo extendido.

con un fuerte enfoque en la facilidad de uso y mejorar la experiencia de usuario. Está compuesto de múltiple software normalmente distribuido bajo una licencia libre o de código abierto.

4.3.1. HERRAMIENTAS USADAS EN EL SGSI

La *Tabla55* resume el control aplicado y la herramienta implementada dentro del proceso de diseño y ejecución del SGSI.

Tabla 55. Herramientas implementadas dentro del SGSI

Fuente: Información recopilada de ISO 27000

CONTROL	HERRAMIENTA	REQUERIMIENTO DE HARDWARE
Control de sesiones de usuario	- Controlador de dominio con Samba 4	- Disco Duro: 60 GB - Memoria RAM: 1.5 GB
Soporte remoto	- iTALC	- Disco Duro: 30 GB - Memoria RAM: 1.5GB
Monitoreo, Inventario IP y Helpdesk	- Nagios3-NCONF - OCS Inventory - OTRS - MRTG	- Disco Duro: 20 GB - Memoria RAM: 1.5 GB
Backup de usuario	- Servidor de archivos con samba 3 - Cobian	- Disco Duro: 5GB - Memoria RAM: 512MB
Cifrado	- True Crypt	- Disco Duro: 20 GB - Memoria RAM: 512MB
Seguridad	- UTM ○ IDS/IPS ○ Firewall ○ Proxy ○ NTOP	- Disco Duro: 30 GB - Memoria RAM: 2GB

4.3.2. DESCRIPCIÓN DE HERRAMIENTAS

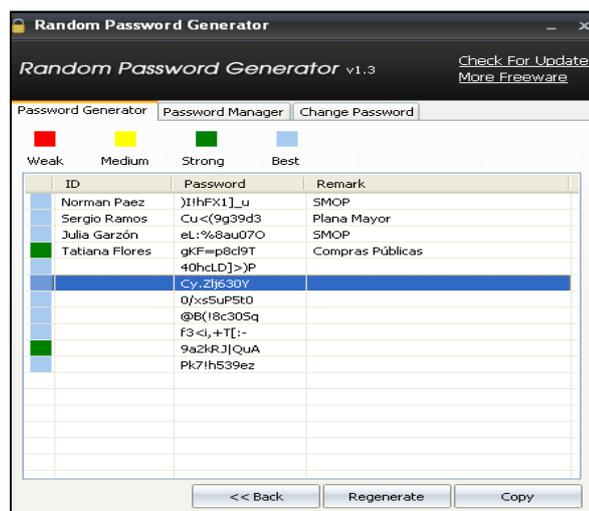
Las herramientas y aplicaciones utilizadas en el desarrollo del SGSI están descritas haciendo énfasis en su funcionalidad y características principales.

4.3.2.1. Generador de contraseñas RPG

IObit Random Password Generator es una herramienta que permite generar hasta cien contraseñas aleatorias. Únicamente es necesario escoger la longitud (desde seis hasta 64 caracteres), el tipo de caracteres y la cantidad de claves a crear.

Dependiendo del tipo y cantidad de caracteres, una contraseña será más o menos fuerte. IObit Random Password Generator indicará en la tabla de claves mediante una leyenda de cuatro colores. Evitar las contraseñas rojas ya que son débiles y fáciles de romper. Las azules, en cambio son inquebrantables.

En la *Figura 19*, se muestra la tabla de claves generadas por esta herramienta.



ID	Password	Remark
Norman Paez]1hFX1]_u	SMOP
Sergio Ramos	Cu<(9g39d3	Plana Mayor
Julia Garzón	eL:%8au07O	SMOP
Tatiana Flores	gKF=p8cl9T	Compras Públicas
	40hclD]>]P	
	Cy.Zlj630Y	
	0/xs5uP5t0	
	@B(18c305q	
	f3<!,+T[:-	
	9a2lR.]QuA	
	pk7lh539ez	

Figura 19. Generador de claves RPG
Fuente: Captura de pantalla

Características

- Cinco parámetros de generación
- Base de datos de contraseñas creadas
- Medidor de fuerza de las contraseñas

4.3.2.2. Controlador de dominio con Samba 4

La implementación del Controlador de dominio se realiza sobre Samba 4 que es un proyecto de código abierto y además es una opción alternativa a Microsoft AD³⁷.

Uno de los objetivos de Samba4 es implementar un controlador de dominio compatible con varios sistemas operativos.

Las principales características de Samba4 ya incluyen:

- Soporte para inicio de sesión del Controlador de dominio y protocolos de administración compatibles con clientes Windows XP³⁸, Windows 7 y Mac OS X³⁹.
- Un servidor interno LDAP⁴⁰, con la semántica de AD
- Un servidor DNS⁴¹ interno con soporte para la actualización dinámica
- Modelos flexibles de proceso.

³⁷ AD (Active Directory): Directorio Activo es un sistema que sirve para compartir recursos en un conjunto de dominios.

³⁸XP (eXPerience): Las letras "XP" provienen de la palabra eXPeriencia.

³⁹ Mac OS X: sistema operativo desarrollado y comercializado por Apple.

⁴⁰ LDAP (LightweightDirectory Access Protocol): Protocolo Ligero de Acceso a Directorios que permite el acceso a un servicio de directorio ordenado y distribuido.

⁴¹DNS (DomainNameSystem): Sistema de nombres de dominio es una base de datos distribuida, con información que se usa para traducir los nombres de dominio en números de protocolo de Internet.

- Arquitectura de base de datos flexible
- Soporte para Python - utilizado ampliamente como herramienta para gestión de cliente
- Subsistema genérico de seguridad
- Más del 50% del código se genera automáticamente

El controlador de Dominio es un servicio de directorio que almacena información acerca de los objetos de una red que en forma muy ordenada las pone a disposición de todos los usuarios y administradores que pertenecen a esa red. Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera.

- **Características del Controlador de dominio:**
 - ~ **Integración DNS:** Todos los servicios utilizan DNS para localizar y conectarse a todos los servicios de red. Como resultado, el DNS es un servicio requerido por el DC⁴².
 - ~ **Políticas basadas en objetos:** También conocido como políticas de grupo, estas opciones determinan el acceso del usuario a los recursos y cómo estos recursos pueden ser utilizados.

⁴²DC (Domain Controller): Controlador de dominio

- ~ **Seguridad centralizada:** DC autoriza el acceso de cada usuario a la red. Además, puede definir el control de acceso no sólo de cada objeto en el directorio, sino también en cada propiedad de cada objeto.
- ~ **Funcionalidad de escritorio:** los administradores pueden bloquear las configuraciones de escritorio en la red y evitar el acceso a las cosas que potencialmente podrían poner en peligro al sistema, tal como instalaciones de software y edición del Registro.

- **Requisitos de instalación**

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

- ~ Protocolo TCP/IP⁴³ instalado y configurado manualmente, es decir, sin contar con una dirección asignada por DHCP.
- ~ Tener un servidor de nombre DNS, para resolver la dirección de los distintos recursos físicos presentes en la red.
- ~ Poseer más de 250 MB en una unidad de disco.

L a instalación de Samba 4 se encuentra en el ANEXO 4.

4.3.2.3. iTALC

iTALC es una aplicación didáctica de monitorización, que ofrece la oportunidad de supervisar e influir en las actividades de los usuarios. Se trata de un software de uso libre y de muy sencilla instalación que permite controlar los

⁴³TCP/IP Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP): conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras.

equipos de usuarios a distancia. Permite ver el contenido de las pantallas de los usuarios en la propia pantalla del administrador, entre otras funciones como son:

- Realizar demostraciones desde su equipo.
- Bloquear los equipos.
- Control remoto de equipos.
- Envío de mensajes.
- Inicio de sesión remoto
- Apagar equipos.
- Obtener capturas de pantallas.

Gracias a esta aplicación se puede hacer un seguimiento de la actividad de cada usuario en su ordenador, generar presentaciones o guiar a un usuario con dificultades sin necesidad de abandonar el sitio de trabajo.

La instalación de Italc se encuentra en el ANEXO 5

- **Estado actual de iTALC**

La *Tabla 56* muestra información actual de la aplicación:

Tabla 56. Información actualizada de la aplicación iTALC
Fuente: <http://italc.sourceforge.net/>

iTALC	
	
Última versión estable	2.0.0 / 3 de agosto de 2011
Lenguaje de programación	C + +
Sistema operativo	<u>Linux</u> , <u>Microsoft Windows</u>
Tamaño	6,0 MB
Tipo	<u>Software</u>
Licencia	<u>GPL</u>

4.3.2.4. Nagios3-NCONF

Nagios es una aplicación de código abierto para monitoreo de sistemas y redes. Revisa equipos y servicios que se le especifica, alertando cuando el comportamiento de los mismos no sea el deseado.

Para poder añadir de una forma sencilla los sistemas que se desea, se utiliza NCONF como herramienta gráfica de configuración para Nagios.

NConf es una herramienta de código abierto que permite administrar los archivos de configuración de Nagios a través del uso de una interfaz gráfica de usuario, en lugar de mantener los archivos de configuración con un editor de texto.

Algunas de las características de NAGIOS son:

- Monitorear servicios de red (SMTP⁴⁴, POP3⁴⁵, HTTP, PING⁴⁶, etc.)
- Monitorear recursos de los hosts (carga de procesador, uso de disco, etc.)
- Notificaciones a contactos cuando un servicio o host tenga problemas y puedan resolverlo (definido por el usuario).
- Rotación de log automática.
- Chequeo de servicios paralizados.

⁴⁴SMTP (Simple Mail Transfer Protocol): Protocolo para la transferencia simple de correo electrónico es utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

⁴⁵POP3 (Post Office Protocol): Protocolo de Oficina Postal se utiliza para obtener los mensajes de correo electrónico almacenados en un servidor remoto.

⁴⁶PING (Packet Internet Groper): Rastreador de paquetes en redes que comprueba el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes ICMP de solicitud y de respuesta.

- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros.

La instalación de estas herramientas se encuentra en el ANEXO 6.

4.3.2.5. OCS Inventory

Open Computer and Software Inventory Next Generation (OCS-NG) es un software libre que permite a los usuarios administrar el inventario de sus activos de TI.

OCS-NG recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS ("agente OCS de inventario").

OCS puede utilizarse para visualizar el inventario a través de una interfaz web. Además, OCS comprende la posibilidad de implementación de aplicaciones en los equipos de acuerdo a criterios de búsqueda. OCS se basa en los estándares vigentes. El diálogo entre los equipos clientes y el servidor se basan

en HTTP (Hypertext Transfer Protocol) y el formato de los datos se realiza en XML⁴⁷.

El servidor de administración utiliza Apache, MySQL y Perl. OCS es multiplataforma.

- **Estado actual de OCS INVENTORY**

La *Tabla57* muestra información actual del software:

Tabla 57. Información actual del software
Fuente: <http://www.ocsinventory-ng.org/en/>

OCS (Inventario)	
	
Última versión estable	2.0 12 de Mayo de 2011
Sistema operativo	Multiplataforma (GNU/Linux, Unices, Windows, otros)
Licencia	GNU General Public License

La instalación de OCS inventory se encuentra en el ANEXO 7.

4.3.2.6. OTRS

OTRS (Open-source Ticket Request System), es una aplicación web Open Source que permite ofrecer servicio on-line con la utilización de tickets soportando multi-usuarios.

⁴⁷XML (eXtensibleMarkupLanguage): Lenguaje de marcas extensible es un lenguaje de marcas que permite definir la gramática de lenguajes específicos

El OTRS permite realizar una gestión integrada de las solicitudes de servicio, información o cualquier requerimiento que realice un usuario a un área, dirección o cualquier entidad o agente que le solicite asistencia. El Sistema de Tickets hace posible interactuar con los usuarios de las dependencias de una institución.

Características principales:

- *Interfaz Web:*
 - Fácil manejo y ejecución desde un navegador web
 - Se puede utilizar en la mayoría de los navegadores
 - Cuenta con un administrador del sistema desde la web
 - Cuenta con una interfaz gráfica web para manejar las solicitudes de los clientes.
 - Cuenta con una interfaz gráfica para que los usuarios puedan escribir nuevos correos, verificar el estado y respuesta de los tickets generados.
 - Soporta varios idiomas
 - Se puede personalizar la interfaz con diferentes temas incorporados.

- *Mail de la interfaz:*
 - Soporte para archivos adjuntos de correo
 - Los correos se pueden filtrar utilizando direcciones de correo
 - Auto respuesta para los clientes
 - Notificación por correo electrónico a los agentes sobre nuevos tickets

- *Sistema:*

- OTRS se ejecuta en varios sistemas operativos (LINUX, MICROSOFT WINDOWS, SOLARIS).
- Crea un identificador único por cada ticket generado
- OTRS soporta bases como MYSQL
- Apoyo a las cuentas de usuario, grupos de usuario y roles
- Apoyo a las diferentes zonas horarias

La instalación de OTRS se encuentra en el ANEXO 8.

4.3.2.7. Servidor de archivos con samba 3

Un servidor de archivos proporciona una ubicación central en la red, en la que puede almacenar y compartir los archivos con usuarios de la red. Cuando los usuarios necesiten un archivo importante, podrán tener acceso al archivo del servidor en lugar de tener que pasarlo entre distintos equipos.

Samba es un software que implementa de forma libre el protocolo de Servidor de Archivos SMB (Server Message Block) para los sistemas Unix.

El servidor Samba ofrece los siguientes servicios:

- Compartir uno o varios árboles de directorios.
- Compartir uno o más archivos distribuidos.
- Compartir la impresora instalada tanto en servidores como en clientes.
- Ayudar a los clientes a navegar por la red.
- Autenticación de clientes al conectarse a un dominio de Windows.

Samba 3 es mucho más rápido como servidor de archivos ya que al ser software libre otros lo pueden ver, variar, opinar, criticar y aportar cosas al código fuente y el resultado mejora ampliamente.

La instalación del servidor de archivos se encuentra en el ANEXO 9.

4.3.2.8. Cobian Backup

Es un programa multitarea capaz de crear copias de seguridad en un equipo, en una red local o incluso en/desde un servidor FTP⁴⁸. También soporta SSL⁴⁹. Se ejecuta sobre Windows y una de sus grandes ventajas es que consume muy pocos recursos.

Cada tarea de respaldo que se le asigne puede ejecutarse en el mismo instante, a diario, semanal, mensual o anualmente, o en un tiempo especificado. Además ofrece la opción de proteger todas las funciones del programa por contraseña. Existe la opción de cifrar sus ficheros usando 4 métodos diferentes de cifrado fuerte: RSA⁵⁰-Rijndael (1024-256-bits), Blowfish (128-bits), Rijndael (128-bits) o DES⁵¹ (64-bits).

La instalación de Cobian se encuentra en el ANEXO 10.

- **Estado actual de Cobian Backup**

La *Tabla 58* muestra la información actual de la aplicación:

⁴⁸FTP (File Transfer Protocol): Protocolo de transferencia de archivos. Permite transferir archivos locales hacia un servidor web

⁴⁹SSL (Secure Sockets Layer): Capa de conexión segura es un protocolo criptográfico que proporciona comunicaciones seguras por una red

⁵⁰RSA(Rivest, Shamir y Adleman):Es un sistema criptográfico de clave pública y es válido tanto para cifrar como para firmar digitalmente.

⁵¹DES (Data Encryption Standard) es un algoritmo de cifrado, es decir, un método para cifrar información.

Tabla 58. Información actual de Cobian Backup

Fuente: <http://www.cobian.se/>

CobianBackup	
	
Página web	http://www.cobian.se
Apertura de código	Febrero de 2007
Licencia	Mozilla Public License 1.1 (MPL 1.1)
Versión actual	10.1.1.816
Lenguaje de programación	Pascal
Líneas de código fuente	40.501

4.3.2.9. Truecrypt

Es una aplicación gratuita que permite crear volúmenes cifrados, de manera que todo lo que contengan estos volúmenes pueda ser accedido únicamente si se conoce la contraseña y el fichero clave que se utiliza en su creación.

Esta aplicación codifica y decodifica automáticamente los datos que se extraiga o grabe en una determinada unidad de volumen. Los datos que hayan sido guardados en una unidad cifrada no se pueden leer sin la contraseña o clave de cifrado correspondiente; además, permite crear un volumen oculto para brindar mayor seguridad.

Para cifrar los datos hace uso de algoritmos como son: AES⁵², Serpent⁵³ y Twofish⁵⁴ o una combinación de los mismos. La instalación de Truecrypt se encuentra en el ANEXO 11.

⁵² AES: Advanced Encryption Standard (Estándar de cifrado avanzado).- es un esquema de cifrado por bloques, esta técnica permite cifrar haciendo uso de una clave simétrica.

⁵³ Serpent: Es un algoritmo de cifrado simétrico de bloques, usa un tamaño de bloque de 128 bits y soporta tamaños de clave de 128, 192 y 256 bits de longitud.

- **Estado actual de TrueCrypt**

La *Tabla 59* muestra la información actual de la aplicación:

Tabla 59. Información actual de TrueCrypt

Fuente: <http://www.truecrypt.org/>

TrueCrypt	
	
Última versión estable	7.1a 7 de febrero de 2012; hace 7 meses
Género	Criptografía
Programado en	C, C++, Assembly
Sistema operativo	Multiplataforma
Licencia	TrueCrypt Collective License Version 1.4

4.3.2.10. UTM⁵⁵

Los sistemas de Gestión Unificada de Amenazas constituyen una solución de seguridad mejorada ya que integran múltiples tecnologías integradas cubriendo las exigencias básicas de protección integral.

El UTM combina un firewall, un proxy, IDS/IPS y herramientas de monitoreo, todo en un único equipo y a tiempo real.

Las funciones básicas de seguridad de un sistema UTM son:

- IDS/IPS para prevención y detección de intrusiones en la red centrada en el bloqueo de ataques contra PC y servidores.
- Funciones habituales de firewall(cortafuegos)

⁵⁴Twofish: Es un método de criptografía simétrica con cifrado por bloques. El tamaño de bloque en Twofish es de 128 bits y el tamaño de clave puede llegar hasta 256 bits.

⁵⁵(UnifiedThreat Management): Gestión Unificada de Amenazasse refiere a un firewall de red con múltiples funciones añadidas, trabajando a nivel de aplicación.

- Adicionalmente puede poseer acceso remoto y de sitio a sitio con soporte en VPN y SSL (basado en navegador).

- **Proxy**

Un servidor proxy es un equipo que actúa de intermediario entre un explorador web en Internet. Los servidores proxy ayudan a mejorar el rendimiento en Internet ya que almacenan una copia de las páginas web más utilizadas. Cuando un explorador solicita una página web almacenada en la colección (su caché) del servidor proxy, el servidor proxy la proporciona, lo que resulta más rápido que consultar la Web. Los servidores proxy también ayudan a mejorar la seguridad, ya que filtran algunos contenidos web y software malintencionado.

- **Ventajas:**

- **Control:** sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- **Velocidad:** Si varios clientes van a pedir el mismo recurso, el proxy guarda la respuesta de una petición para darla directamente cuando otro usuario la pida..
- **Filtrado:** El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- **Modificación:** Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.

- **Firewall**

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cuál de los servicios de red pueden ser accedidos dentro de esta por los que están fuera, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

- **Políticas del cortafuegos**

Hay dos políticas básicas en la configuración de un cortafuegos:

Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos 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.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso.

- **Ntop**

Ntop (Network Top) es una herramienta de monitorización de red en tiempo real. Es útil para controlar los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto y ayuda a detectar malas configuraciones de algún equipo o a nivel de servicio.

Posee un microservidor web desde el que cualquier usuario con acceso puede ver las estadísticas del monitorizaje. El software está desarrollado para plataformas Unix y Windows.

Características de Ntop:

- Es un proyecto de software libre ya consolidado
- Tiene interfaz web
- Dispone de gran variedad de informes
- Es capaz de analizar datos proporcionados por dispositivos de red
- Es un software multiplataforma (Windows, Linux, Solaris y MacOSX)

- **MRTG**

MRTG (Multi Router Traffic Grapher), es una herramienta que permite monitorizar varias características de los servidores reportando la información en gráfica visible por medio de un html.

MRTG es capaz de monitorizar:

- Carga del sistema.
- Capacidades Disco duros.
- Tráfico en interfaces de red.

Mediante MRTG es posible monitorizar cualquier variable SNMP que se quiera, de manera que se puede configurar para monitorizar la carga de un sistema, las sesiones abiertas por los usuarios de un determinado equipo, disponibilidad de módems. MRTG permite generar gráficas con cuatro niveles de detalle por cada interfaz: tráfico registrado en las últimas 24 horas, la última semana, el último mes y gráfica anual.

- **IPS/IDS**

IDS

Un sistema de detección de intrusos es aquel que determina cada vez que se está intentando realizar una actividad ilegal contra el sistema y guarda la evidencia de esta actividad para que el administrador pueda verificar y tomar medidas posteriores al intento de ataque.

IPS

Un sistema de prevención de intrusos (IPS) va más allá de la determinación de una actividad o posible actividad ilegal. El IPS además bloquea el host que está intentando realizar esta actividad determinada como ilegal de forma tal que aún en caso de que la actividad pueda ser potencialmente peligrosa, el atacante se quedará impedido de entrar al servicio que ofrecemos puesto que el IPS le bloquea a nivel de red.

El servicio de administración de IDS/IPS, está orientado a la detección y prevención de ataques efectuados desde Internet hacia la red interna de una organización, permitiendo tomar diferentes acciones de acuerdo a las políticas de seguridad establecidas por la organización.

Los IDS/IPS son un complemento ideal para los firewall, en la protección del tráfico malicioso que penetra exitosamente por el firewall para luego ingresar en la red corporativa. Los IDS/IPS pueden ser encontrados frecuentemente monitoreando diferentes segmentos de la red interna como zonas DMZ, LAN, etc. o monitorizando fuera de la red interna como el enlace a Internet. Una buena gestión y administración de IDS/IPS permite establecer acciones frente a los sucesos registrados, permitiendo realizar funciones preventivas, ayuda en el mantenimiento de políticas de seguridad frente a ataques y reduce la exposición de riesgo maximizando la protección de una organización.

La instalación de las herramientas que componen el UTM se encuentran en los ANEXOS 12, 13, 14, 15, 16.

4.3.2.11. Puertos utilizados por los servicios implementados

La *Tabla 60* muestra las herramientas implementadas y los puertos que utilizan cada uno de los servicios.

Tabla 60. Puertos utilizados por las herramientas implementadas
Fuente: Información obtenida mediante putty

HERRAMIENTA	PUERTO
Samba 4 DC	137, 138, 139, 445
iTALC	5800, 5900
Nagios3-NCONF	80
OTRS	80
OCS Inventory	80
Servidor de archivos con samba 3	137, 138, 139, 445
Proxy	3128
NTOP	3000
MRTG	80

4.3.2.12. Direccionamiento IP utilizado

El direccionamiento IP utilizado en los servidores implementados se detalla en la *Tabla 61*.

Tabla 61. Direccionamiento IP utilizado con fines demostrativos
Fuente: Microsoft Excel 2010

SERVIDOR	IP ASIGNADA
	10.10.1.1 (Red Local)
	10.10.1.129 (Red Wireless)
UTM	10.10.1.193 (Red de servidores)
	190.36.191.137 (Red de Internet)
Controlador de dominio	10.10.1.194
ITALC	10.10.1.195
Monitoreo	10.10.1.196
Servidor de Archivos	10.10.1.197

CAPÍTULO V

REVISIÓN DEL SGSI

Este capítulo hace referencia a las pruebas realizadas con el fin de comprobar el correcto funcionamiento de las herramientas implementadas y el cumplimiento de la funcionalidad de cada una de ellas.

5.1 POLÍTICAS DE SEGURIDAD IMPLEMENTADAS

Dentro del CP-12 se ha dispuesto la difusión de las nuevas políticas y herramientas que conforman el SGSI, con la finalidad de que todos los usuarios tengan una visión clara de los objetivos que se ha fijado la institución con respecto a la seguridad de la información.

Este proceso se llevará a cabo a través de una capacitación brindada por el Jefe del departamento de Sistemas, en donde se explicará detalladamente cada una de las políticas adoptadas.

Como prueba de que se está organizando todo lo necesario para que se realice la capacitación, se muestra la *Figura 20*, correspondiente a la Circular enviada por el departamento de Sistemas a todas las dependencias del CP-12.

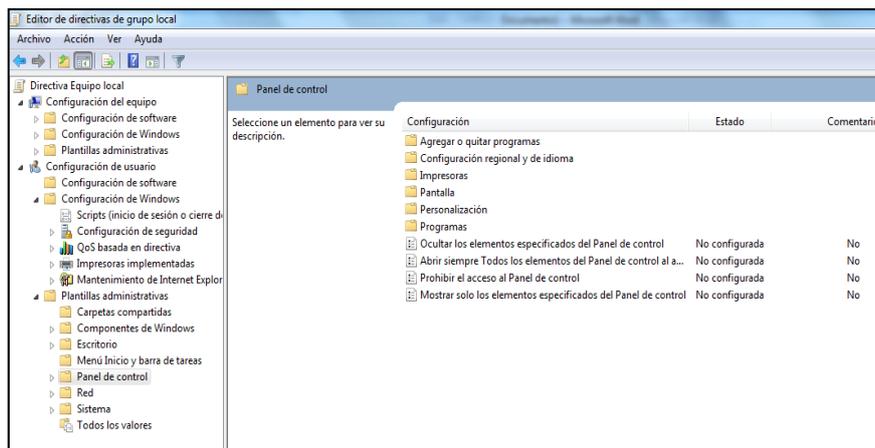


Figura 20. Circular informativa
Fuente: Archivo del CP-12

5.2 VERIFICACIÓN DEL FUNCIONAMIENTO DEL CONTROLADOR DE DOMINIO

El Controlador de Dominio restringe características de sistemas operativos Windows. En el siguiente ejemplo se bloqueará el acceso al panel de control. Para verificar el bloqueo se intentará acceder a las opciones del panel de control.

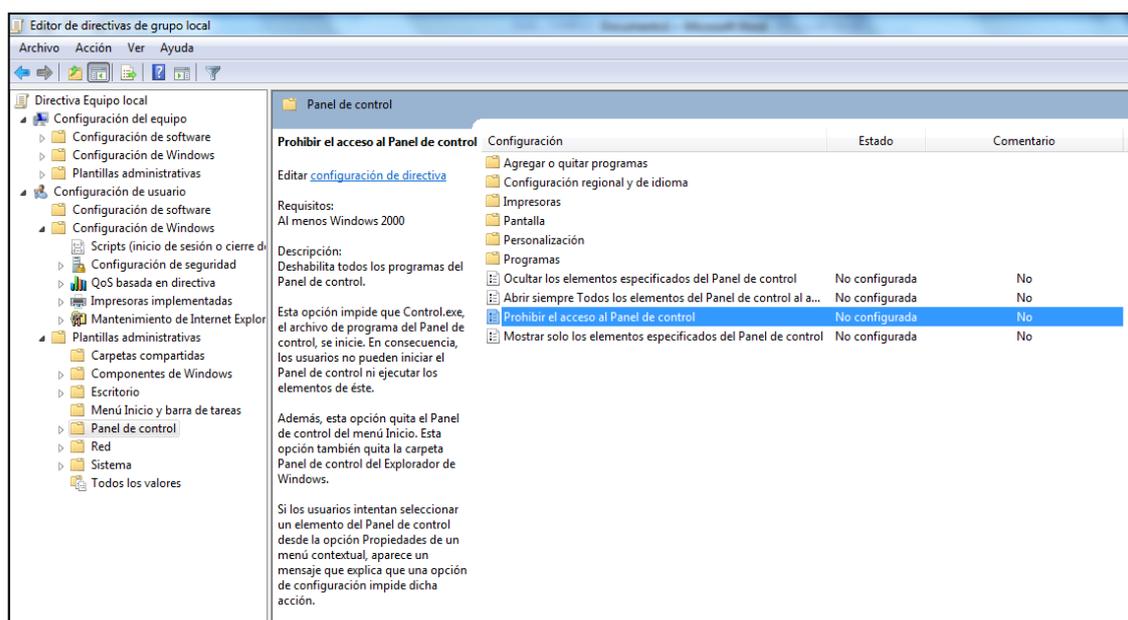
El primer paso es aplicar en las políticas del controlador de dominio la restricción del acceso al panel de control. Esta ventana se muestra en la *Figura 21*.



*Figura 21. Políticas del controlador de dominio
Fuente: Captura de pantalla*

El segundo paso es editar la política para lo cual se debe seleccionar las restricciones de acceso del panel de control. Estas opciones se muestran en la *Figura 22*.

Para el caso de este ejemplo se selecciona la política *Prohibir el acceso al Panel de control*.



*Figura 22. Selección de política de restricción del panel de control
Fuente: Captura de pantalla*

Finalmente se debe habilitar la restricción de acceso al panel de control, como se muestra en la *Figura 23*.

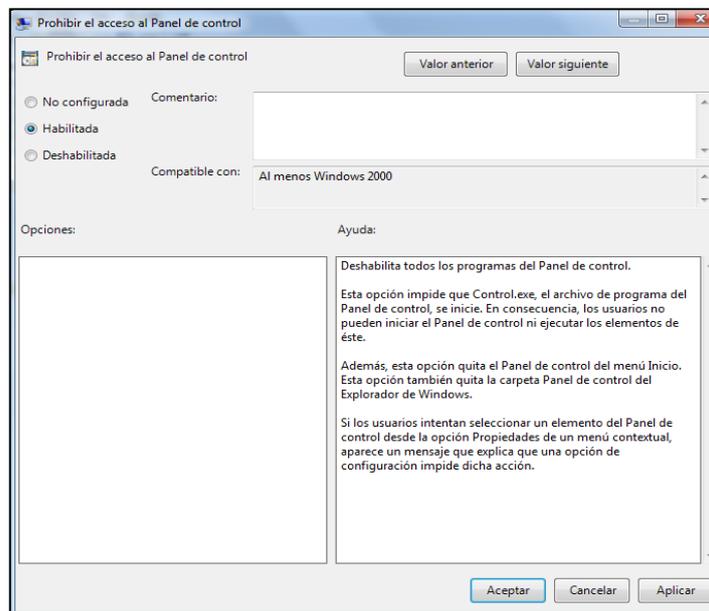


Figura 23. Habilitación de la política de restricción
Fuente: Captura de pantalla

Para verificar el funcionamiento de la política aplicada, se intentará acceder al panel de control.

Al intentar abrir el panel de control aparece el mensaje que se muestra en la *Figura 24*, en el que se indica que esta operación fue cancelada debido a las restricciones especificadas para este equipo.

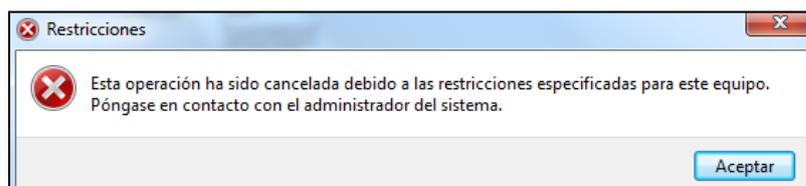


Figura 24. Mensaje de restricción de acceso al panel de control
Fuente: Captura de pantalla

Para volver a acceder al panel de control, únicamente se debe Deshabilitar la política de restricción.

5.3 VERIFICACIÓN DEL FUNCIONAMIENTO DE iTALC

La herramienta iTALC permite tomar control de manera remota de los equipos clientes que se encuentren dentro de la red.

En las *Figura 25*, mostrada a continuación se puede apreciar el panel del administrador y en el área de trabajo se muestran los equipos de los usuarios a los cuales se les puede controlar remotamente.

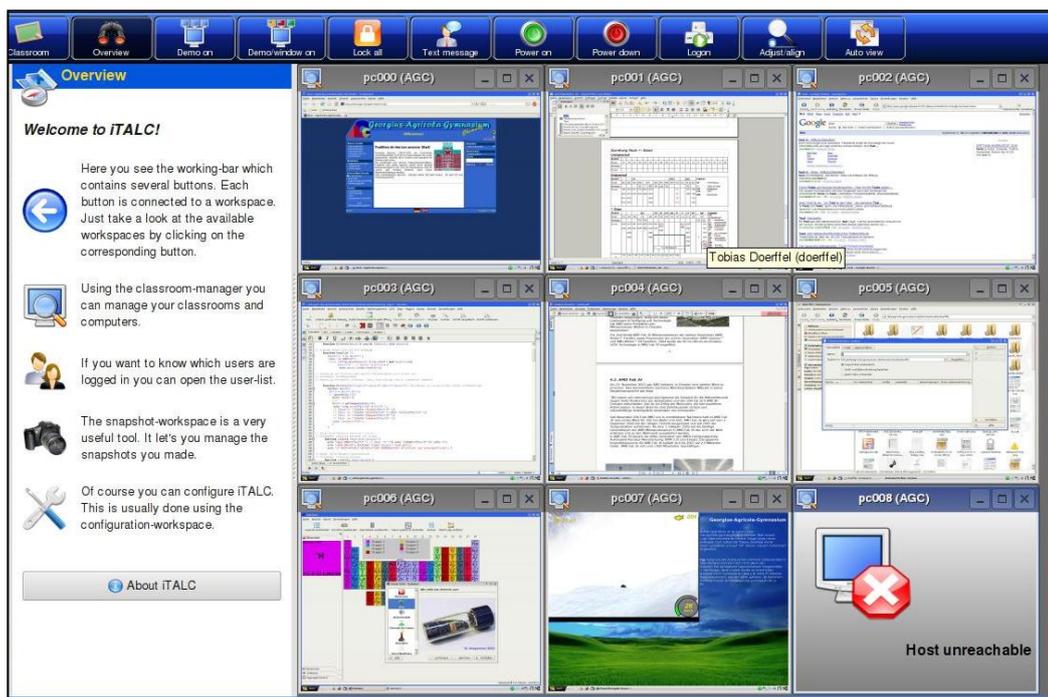
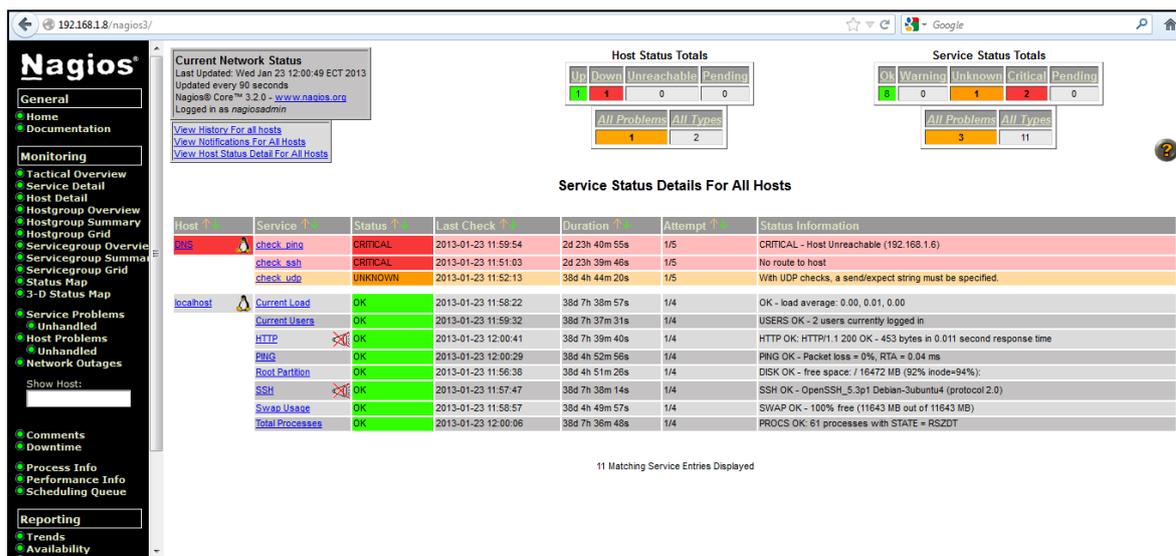


Figura 25. Panel principal del administrador de iTALC
Fuente: Captura de pantalla

5.4 VERIFICACIÓN DEL FUNCIONAMIENTO DE NAGIOS

Nagios es una herramienta que permite monitorear el estado de hosts, equipos, servicios y aplicaciones. En la *Figura 26*, se muestra de manera general el estado de los servicios de los hosts que se encuentran dentro de la red.



*Figura 26. Monitoreo de servicios mediante Nagios
Fuente: Captura de pantalla*

5.5 VERIFICACIÓN DEL FUNCIONAMIENTO DE OCS INVENTORY

Para verificar que la herramienta funciona correctamente se tomó como muestra a la oficina de Relaciones Públicas. El objetivo de esta prueba es comprobar el funcionamiento de dicha aplicación y emitir los reportes de las máquinas de los usuarios conectados a la LAN.

En la *Figura 27*, se puede apreciar los datos de manera general de los equipos que pertenecen a la oficina de Relaciones Públicas y que se están generando en el servidor. Esta es la pantalla principal que se muestra en el panel de administración.

Tag	Último inventario	Computador	Nombre usuario	Sistema Operativo	RAM(MB)	CPU(MHz)
NA	23/01/2013 11:36:51	WINDOWS7-PC	Windows 7	Microsoft Windows 7 Ultimate	4005	3100
NA	20/01/2013 19:44:51	UPCFERROCARRIL	UPC FERROCARRIL	Microsoft Windows 7 Ultimate	2048	2667

Figura 27. Recopilación de datos de equipos mediante OCS Inventory
Fuente: Captura de pantalla

Para ver en detalle toda la información de un equipo en particular, se seleccionó al equipo UPCFERROCARRIL. A continuación en la Figuras 28, 29 y 30, se muestra la información de hardware y software proporcionada por la herramienta.

Nombre:	UPCFERROCARRIL	Nombre del SO:	Microsoft Windows 7 Ultimate
Dominio:	WORKGROUP	Versión del SO:	6.1.7601
Dominio usuario:	N/A	Service pack:	Service Pack 1
Último inventario:	20/01/2013 19:44:51	Comentarios:	
Dirección IP:	192.168.0.64	Usuario Windows:	UPC FERROCARRIL
Nombre usuario:	UPC FERROCARRIL	Licencia Windows:	00426-OEM-8992662-00006
Memoria:	2048	Clave Windows:	FJGCP-4DFJD-GJY49-VJBQ7-HYRR2
Memoria virtual:	4095	Agente de usuario:	OCS-NG_windows_client_v4054
Nombre de red 1:	192.168.0.0		

Figura 28. Información del equipo UPCFERROCARRIL
Fuente: Captura de pantalla

Descripción	Tipo	Velocidad	Dirección MAC	Estado	Dirección IP	máscara	Punto de salida	Número de red	IP DHCP
NIC de Gigabit de Ethernet PCI-E de la familia Realtek RTL8168C(P)/8111C(P) (NDIS 6.20)	Ethernet	1 Gb/s	00:23:7D:2A:8C:8D	Up	192.168.0.64	255.255.255.0	192.168.0.1	192.168.0.0	

Figura 29. Información de la red a la que pertenece el equipo
Fuente: Captura de pantalla

SOFTWARE			
Editor	Nombre	Versión	Comentarios
Adobe Systems Inc.	Adobe AIR	1.0.4990	N/A
Adobe Systems Incorporated	Adobe Flash Player 10 ActiveX	10.0.32.18	N/A
Adobe Systems Incorporated	Adobe Flash Player 10 Plugin	10.0.32.18	N/A
AVAST Software	avast! Free Antivirus	7.0.1466.0	N/A
Adobe Systems Incorporated	Acrobat.com	1.1.377	N/A
Google Inc.	Google Chrome	24.0.1312.52	N/A
	Ituam 1.0		N/A
	K-Lite Codec Pack 5.4.4 (Full)	5.4.4	N/A
Microsoft Corporation	Microsoft .NET Framework 4 Client Profile	4.0.30319	N/A
Microsoft Corporation	Paquete de idioma de Microsoft .NET Framework 4 Client Profile ESN	4.0.30319	N/A
Mozilla	Mozilla Firefox 15.0.1 (x86 es-ES)	15.0.1	Mozilla Firefox 15.0.1 (x86 es-ES)
Mozilla	Mozilla Maintenance Service	15.0.1	Mozilla Maintenance Service 15.0.1 (x86 en-US)
Huawei Technologies Co.,Ltd	NIU Banda Ancha	21.003.25.01.484	N/A
NVIDIA Corporation	NVIDIA Drivers	1.4	N/A

*Figura 30. Información de Software del equipo
Fuente: Captura de pantalla*

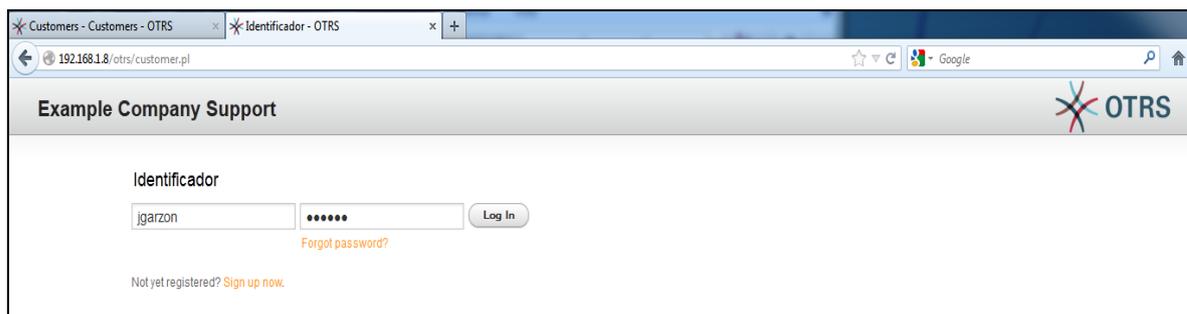
Con la información obtenida en los reportes, se lleva a cabo un inventario IP que facilita la administración de la LAN dentro del CP-12 además de mantener un control sobre los equipos que son utilizados por el personal que desempeña sus funciones dentro de la institución.

5.6 VERIFICACIÓN DEL FUNCIONAMIENTO DE OTRS

Para verificar la funcionalidad de la herramienta OTRS se realizó la generación de tickets desde una cuenta cliente que fue creada en el servidor para que pueda tener acceso como usuario del CP-12.

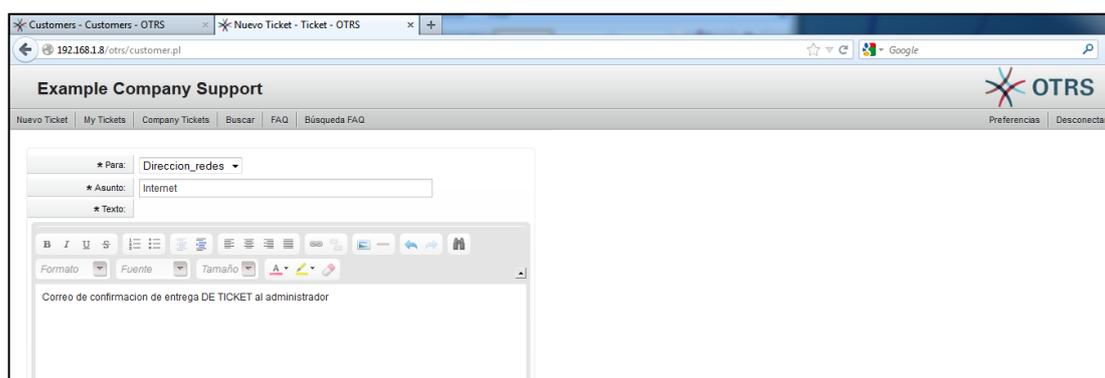
La cuenta creada pertenece a Julia Garzón, funcionaria del departamento de Relaciones Públicas del CP-12, cuyo nombre de usuario es jgarzon y la clave asignada para la realización de esta prueba es 201301.

Para poder generar un ticket el usuario ingresa mediante la dirección: http://ip_servidor/otrs/customer.pl, se abre una ventana como la que se muestra en la *Figura31*, en donde se ingresa los datos del usuario.



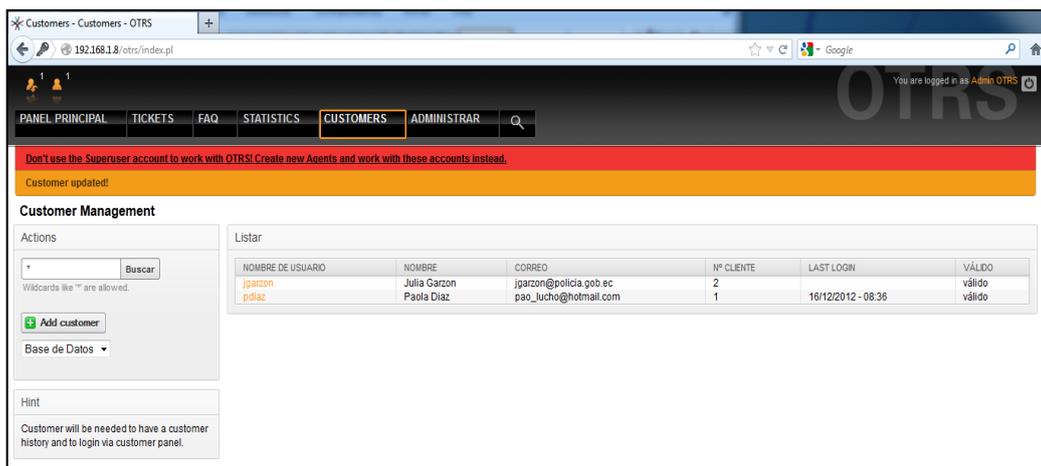
*Figura 31. Ingreso de datos del usuario de prueba
Fuente: Captura de pantalla*

Una vez que se validó el usuario, se va a escribir el correo indicando el problema presente y se va a enviar al administrador de la red. En la *Figura32*, se muestra este paso.



*Figura 32. Apertura de ticket de usuario
Fuente: Captura de pantalla*

Cuando se genera un ticket, este se pone en cola según el nivel de prioridad que fue dado por el usuario. En la *Figura33*, se muestra el ticket generado por el usuario jgarzon, dentro del panel del administrador.



*Figura 33. Ticket generado por el usuario
Fuente: Captura de pantalla*

De esta manera el administrador, puede gestionar los incidentes ocurridos y dar solución de una manera más rápida.

5.7 VERIFICACIÓN DEL FUNCIONAMIENTO DE MRTG

La herramienta MRTG permite monitorear la cantidad de tráfico de entrada y de salida por cada interfaz. Para el caso de pruebas se muestra el tráfico entrante y saliente por la interfaz eth0. En la *Figura 34*, se muestra la pantalla principal de monitoreo de MRTG.



*Figura 34. Pantalla principal de monitoreo de MRTG
Fuente: Captura de pantalla*

El monitoreo del tráfico se realizó en un día laborable en el que todos los equipos están en funcionamiento. En la *Figura 35*, se muestra el tráfico de entrada marcado en color verde y el tráfico de salida marcado en color azul.

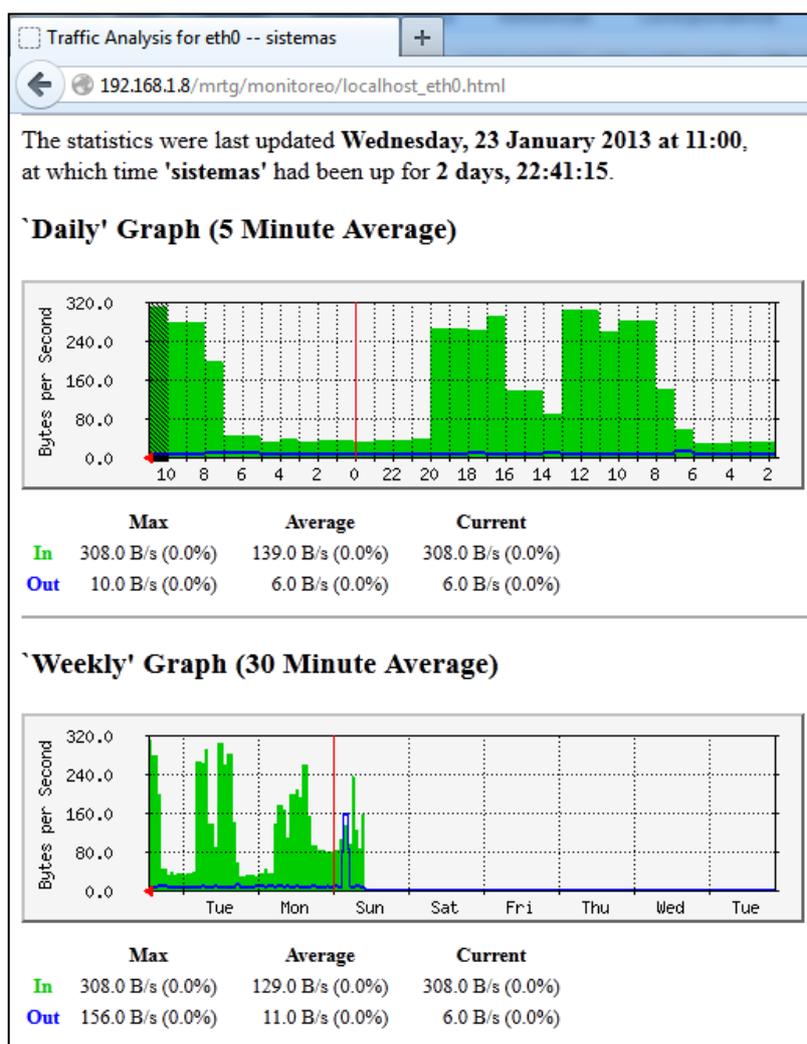


Figura 35. Tráfico de entrada y salida de la eth0
Fuente: Captura de pantalla

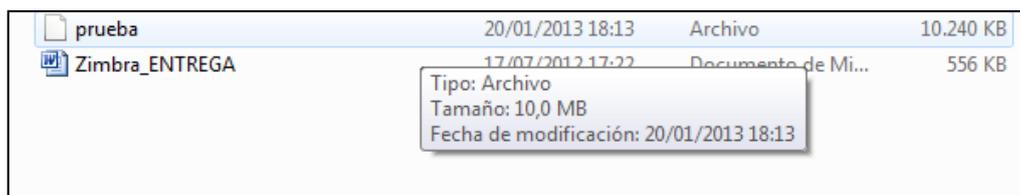
En el caso de que se sature una interfaz los datos se deben mostrar todo en color verde y al máximo nivel con eso se detecta que la conexión por dicha interfaz está saturada.

5.8 VERIFICACIÓN DEL FUNCIONAMIENTO DE COBIAN BACKUP Y TRUECRYPT

El funcionamiento de manera conjunta de Cobian Backup y Truecrypt para el respaldo y cifrado de datos permiten dar mayor seguridad a la información almacenada en el servidor de archivos.

Para el caso de ejemplo se va a respaldar la carpeta llamada *Prueba*, el tipo de respaldo realizado es completo y se efectúa cada día.

En la Figuras 36 y 37, se muestra el respaldo realizado y el reporte de Cobian sobre este respaldo.



*Figura 36. Respaldo realizado de la carpeta Prueba
Fuente: Captura de pantalla*

```

2013-01-26 17:37 The log tab has been cleared. The log file with its full content is still available from the
2013-01-26 17:37 *** A new backup has started. Number of tasks in queue: 1 ***
2013-01-26 17:37 Preventing the system from entering sleep mode...
2013-01-26 17:37 ** Backing up the task "Prueba" **
2013-01-26 17:37 Counting the files for the task "Prueba"...
2013-01-26 17:37 Creating the destination directory "D:\Prueba"

```

```

2013-01-26 17:37 Total backup time for "Prueba": 0 hours, 0 minutes, 0 seconds
2013-01-26 17:37 ** Backup done for the task "Prueba". Errors: 1. Processed files: 0. Backed up files: 0. Total size: 0 bytes
2013-01-26 17:37 --
2013-01-26 17:37 The system can now enter sleep mode
2013-01-26 17:37 Total backup time: 0 hours, 0 minutes, 3 seconds
2013-01-26 17:37 *** Backup done. Errors: 1. Processed files: 0. Backed up files: 0. Total size: 0 bytes
2013-01-26 17:37 --

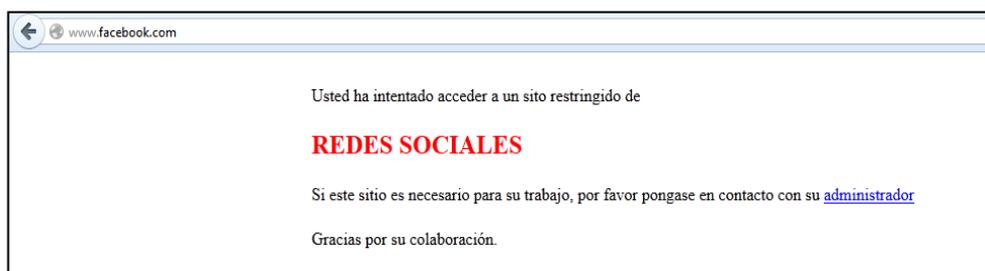
```

*Figura 37. Reporte de respaldo de Cobian
Fuente: Captura de pantalla*

5.9 VERIFICACIÓN DEL FUNCIONAMIENTO DEL UTM

Para comprobar las funcionalidades implementadas en el desarrollo del UTM se realizan las siguientes pruebas:

- Proxy: Para comprobar el funcionamiento del proxy a un usuario se le da acceso libre a internet, posteriormente se bloquea el acceso a ciertas páginas y se revisa el reporte de la navegación. En la *Figura 38* se muestra el mensaje que visualiza el usuario al intentar acceder a una página bloqueada.



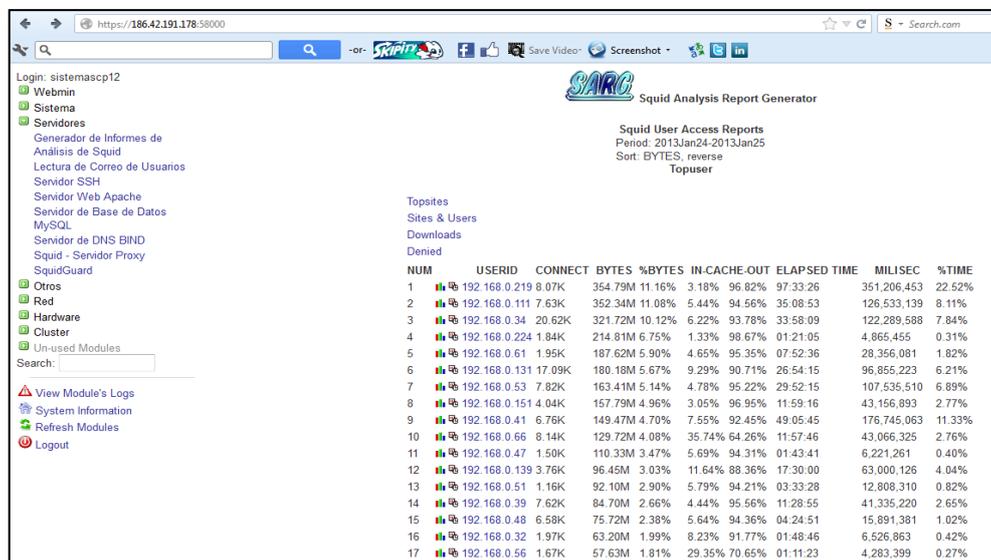
*Figura 38. Acceso denegado a páginas restringidas
Fuente: Captura de pantalla*

En la *Figura 39*, se muestra el reporte de navegación después de varios intentos por ingresar a páginas restringidas.



*Figura 39. Reporte de navegación del proxy
Fuente: Captura de pantalla*

Mediante la herramienta Sarg se puede obtener el reporte de navegación de los usuarios. La *Figura 40*, muestra el reporte generado.

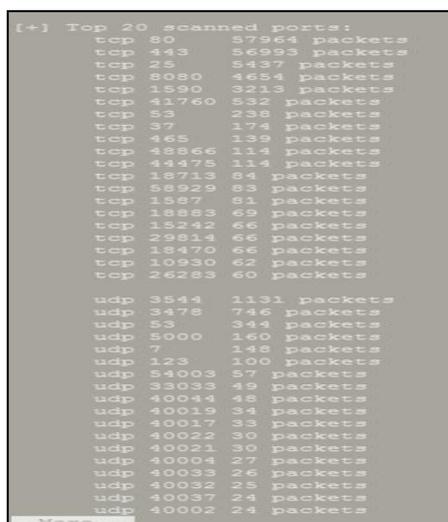


The screenshot shows the Sarg Squid Analysis Report Generator interface. The main content is a table titled 'Squid User Access Reports' for the period '2013Jan24-2013Jan25', sorted by 'BYTES, reverse'. The table has columns: NUM, USERID, CONNECT, BYTES, %BYTES, IN-CACHE-OUT, ELAPSED TIME, MILISEC, and %TIME. The data is as follows:

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILISEC	%TIME	
1	192.168.0.219	8.07K	354.79M	11.16%	3.18%	96.82%	97:33:26	351,206,453	22.52%
2	192.168.0.111	7.63K	352.34M	11.08%	5.44%	94.56%	35:08:53	126,533,139	8.11%
3	192.168.0.34	20.62K	321.72M	10.12%	6.22%	93.78%	33:58:09	122,289,588	7.84%
4	192.168.0.224	1.84K	214.81M	6.75%	1.33%	98.67%	01:21:05	4,865,455	0.31%
5	192.168.0.61	1.95K	187.62M	5.90%	4.65%	95.35%	07:52:36	28,356,081	1.82%
6	192.168.0.131	17.09K	180.18M	5.67%	9.29%	90.71%	26:54:15	96,855,223	6.21%
7	192.168.0.53	7.82K	163.41M	5.14%	4.78%	95.22%	29:52:15	107,535,510	6.89%
8	192.168.0.151	4.04K	157.79M	4.96%	3.05%	96.95%	11:59:16	43,156,893	2.77%
9	192.168.0.41	6.76K	149.47M	4.70%	7.55%	92.45%	49:05:45	176,745,063	11.33%
10	192.168.0.66	8.14K	129.72M	4.08%	35.74%	64.26%	11:57:46	43,066,325	2.76%
11	192.168.0.47	1.50K	110.33M	3.47%	5.69%	94.31%	01:43:41	6,221,261	0.40%
12	192.168.0.139	3.76K	96.45M	3.03%	11.64%	88.36%	17:30:00	63,000,126	4.04%
13	192.168.0.51	1.16K	92.10M	2.90%	5.79%	94.21%	03:33:28	12,808,310	0.82%
14	192.168.0.39	7.62K	84.70M	2.66%	4.44%	95.56%	11:28:55	41,336,220	2.65%
15	192.168.0.48	6.58K	75.72M	2.38%	5.64%	94.36%	04:24:51	15,891,381	1.02%
16	192.168.0.32	1.97K	63.20M	1.99%	8.23%	91.77%	01:48:46	6,526,863	0.42%
17	192.168.0.56	1.67K	57.63M	1.81%	29.35%	70.65%	01:11:23	4,283,399	0.27%

Figura 40. Reporte de navegación generado por Sarg
Fuente: Captura de pantalla

- IDS/IPS: desde la PC del usuario se realiza un escaneo de puertos al equipo. El IDS genera la alerta y el IPS luego de varios intentos lo bloquea. En la *Figura 41*, se muestra el escaneo de puertos realizado.



The screenshot shows a terminal window displaying the results of a port scan. The output is as follows:

```
[+] Top 20 scanned ports:
tcp 80      57954 packets
tcp 443     56993 packets
tcp 25      5437 packets
tcp 8080    4654 packets
tcp 15990   3213 packets
tcp 13760   532 packets
tcp 53      238 packets
tcp 37      174 packets
tcp 465     139 packets
tcp 48866   114 packets
tcp 44475   114 packets
tcp 18713   84 packets
tcp 58929   83 packets
tcp 15987   81 packets
tcp 18883   69 packets
tcp 15242   66 packets
tcp 29814   66 packets
tcp 18470   66 packets
tcp 10930   62 packets
tcp 26283   60 packets

udp 3544    1131 packets
udp 3478   746 packets
udp 53     344 packets
udp 5000   160 packets
udp 7      148 packets
udp 123    100 packets
udp 54003   57 packets
udp 33033   49 packets
udp 40044   48 packets
udp 40019   34 packets
udp 40017   33 packets
udp 40022   30 packets
udp 40021   30 packets
udp 40004   27 packets
udp 40033   26 packets
udp 40032   26 packets
udp 40037   24 packets
udp 40002   24 packets
```

Figura 41. Escaneo de puertos
Fuente: Captura de pantalla

En la *Figura 4 2*, se muestra la alerta generada por el IDS. En este reporte se indica el número total de ataques y la IP desde donde se produjo el mismo.

```

root@utms:~# psad -S | more
[+] psadwatchd (pid: 28700) %CPU: 0.0 %MEM: 0.0
Running since: Wed Jan 23 12:38:58 2013

[+] psad (pid: 28698) %CPU: 0.6 %MEM: 0.9
Running since: Wed Jan 23 12:38:58 2013
Command line arguments: [none specified]
Alert email address(es): root@localhost

[+] Version: psad v2.1.5

[+] Top 50 signature matches:
"ICMP PING" (icmp), Count: 2695, Unique sources: 370, Sid: 384
"ICMP traceroute" (icmp), Count: 522, Unique sources: 332, Sid: 385
"MSC Microsoft SQL Server communication attempt" (tcp), Count: 14, Unique sources: 8, Sid: 100205
"MSC MS Terminal Server communication attempt" (tcp), Count: 13, Unique sources: 7, Sid: 100077
"SCAN SYN FIN" (tcp), Count: 8, Unique sources: 1, Sid: 624
"MSC Radman Default install options attempt" (tcp), Count: 6, Unique sources: 3, Sid: 100204
"BACKDOOR Doomsday file upload attempt" (tcp), Count: 5, Unique sources: 3, Sid: 2375
"MSC VNC communication attempt" (tcp), Count: 1, Unique sources: 1, Sid: 100202

[+] Top 25 attackers:
192.168.0.151 DL: 3, Packets: 1763, Sig count: 0, (local IP)
210.4.18.81 DL: 3, Packets: 265, Sig count: 0
210.4.18.82 DL: 3, Packets: 266, Sig count: 0
210.4.18.83 DL: 3, Packets: 205, Sig count: 0
210.4.18.84 DL: 3, Packets: 249, Sig count: 0
210.4.18.85 DL: 3, Packets: 229, Sig count: 0
210.4.18.86 DL: 3, Packets: 251, Sig count: 0
31.222.74.4 DL: 3, Packets: 191, Sig count: 43
31.222.74.4 DL: 3, Packets: 168, Sig count: 36
111.177.111.133 DL: 2, Packets: 6, Sig count: 7
111.177.111.142 DL: 2, Packets: 6, Sig count: 7
111.177.111.143 DL: 2, Packets: 16, Sig count: 19
111.177.111.146 DL: 2, Packets: 19, Sig count: 14
112.123.174.26 DL: 2, Packets: 1, Sig count: 1
113.11.194.210 DL: 2, Packets: 2, Sig count: 2
113.204.249.6 DL: 2, Packets: 19, Sig count: 12
113.204.249.8 DL: 2, Packets: 16, Sig count: 19
115.238.244.12 DL: 2, Packets: 6, Sig count: 7
115.238.244.14 DL: 2, Packets: 12, Sig count: 14
115.238.244.22 DL: 2, Packets: 12, Sig count: 14
115.238.244.6 DL: 2, Packets: 6, Sig count: 7
115.238.244.8 DL: 2, Packets: 2, Sig count: 3

```

Figura 42. Alerta generada por el IDS
Fuente: Captura de pantalla

Luego de que se generó la alerta y después de varios intentos por obtener acceso el IPS se encarga de bloquear a la IP desde donde se intentó acceder erróneamente. En la *Figura43*, se muestra el bloqueo realizado por el IPS.

```

root@utms:~#
DST: 31.222.74.24 Scanned ports: TCP 80-443, Pkts: 21, Chain: FORWARD, Intf: eth1
DST: 143.166.11.222 Scanned ports: TCP 443, Pkts: 15, Chain: FORWARD, Intf: eth1
DST: 31.222.74.24 Scanned ports: TCP 80-443, Pkts: 141, Chain: FORWARD, Intf: eth1
DST: 212.73.202.119 Scanned ports: TCP 80, Pkts: 87, Chain: FORWARD, Intf: eth1
DST: 31.222.74.24 Scanned ports: TCP 80-443, Pkts: 154, Chain: FORWARD, Intf: eth1
DST: 93.184.71.15 Scanned ports: TCP 80, Pkts: 87, Chain: FORWARD, Intf: eth1
DST: 93.184.71.16 Scanned ports: TCP 80, Pkts: 84, Chain: FORWARD, Intf: eth1
DST: 69.25.21.23 Scanned ports: UDP 123, Pkts: 2, Chain: FORWARD, Intf: eth1
DST: 89.202.157.197 Scanned ports: TCP 80, Pkts: 87, Chain: FORWARD, Intf: eth1
DST: 93.184.71.21 Scanned ports: TCP 80, Pkts: 54, Chain: FORWARD, Intf: eth1
DST: 93.184.71.17 Scanned ports: TCP 80, Pkts: 84, Chain: FORWARD, Intf: eth1
DST: 143.166.11.223 Scanned ports: TCP 443, Pkts: 12, Chain: FORWARD, Intf: eth1
DST: 143.166.156.124 Scanned ports: TCP 443, Pkts: 21, Chain: FORWARD, Intf: eth1
DST: 84.233.195.62 Scanned ports: TCP 80, Pkts: 54, Chain: FORWARD, Intf: eth1
DST: 89.202.157.196 Scanned ports: TCP 80, Pkts: 87, Chain: FORWARD, Intf: eth1
DST: 69.25.21.21 Scanned ports: UDP 123, Pkts: 4, Chain: FORWARD, Intf: eth1
DST: 62.67.184.83 Scanned ports: TCP 80, Pkts: 72, Chain: FORWARD, Intf: eth1
DST: 89.202.149.49 Scanned ports: TCP 80, Pkts: 54, Chain: FORWARD, Intf: eth1
DST: 69.25.21.14 Scanned ports: UDP 123, Pkts: 1, Chain: FORWARD, Intf: eth1
DST: 72.247.130.70 Scanned ports: TCP 443, Pkts: 18, Chain: FORWARD, Intf: eth1
DST: 23.5.146.70 Scanned ports: TCP 443, Pkts: 3, Chain: FORWARD, Intf: eth1
DST: 62.67.184.78

```

Figura 43. Bloqueo realizado por el IPS
Fuente: Captura de pantalla

- NTOP: Esta herramienta de permite generar reportes de la red como se muestra en la *Figura 44*,

ntop (C) 1998-2007 - Luca Deri

About Summary All Protocols IP Utils Plugins Admin

Search ntop...

Network Traffic [TCP/IP]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only] Data: [All] [Sent Only] [Received Only]

Host	Domain	Data	FTP	PROXY	HTTP	DNS	Telnet	NBios-IP	Mail	SNMP	NEWS	DHCP-BOOTP	NFS	X11	SSH	Gnutella	Kaz
utn		210.0 MBytes 38.5 %	0	10.5 KBytes	204.5 MBytes	477.1 KBytes	0	0	0	0	0	0	0	0	60	62	0
192.168.0.1		100.4 MBytes 18.4 %	0	100.3 MBytes		0	76.9 KBytes	0	0	0	0	0	0	0	0	0	0
186.46.140.80		68.8 MBytes 12.6 %	0		68.8 MBytes	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.66		31.3 MBytes 5.7 %	0	31.2 MBytes	4.5 KBytes	521	0	18.3 KBytes	0	0	0	0	0	0	0	0	0
38.96.148.216		24.4 MBytes 4.5 %	0		24.4 MBytes	0	0	0	0	0	0	0	0	0	0	0	0
r7--sn-jou-0pvl.c.youtube.com		20.8 MBytes 3.8 %	0		20.8 MBytes	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.131		15.0 MBytes 2.8 %	0	15.0 MBytes	12.2 KBytes	4.2 KBytes	0	1.3 KBytes	0	0	0	0	0	0	0	0	0
192.168.0.139		10.4 MBytes 1.9 %	0	10.4 MBytes	13.6 KBytes	3.9 KBytes	0	0	0	0	0	0	0	0	0	0	0
192.168.0.35		10.0 MBytes 1.8 %	0	9.9 MBytes	35.7 KBytes	13.0 KBytes	0	7.5 KBytes	0	0	0	0	0	0	0	0	0
192.168.0.37		9.0 MBytes 1.7 %	0	9.0 MBytes		0	0	7.8 KBytes	0	0	0	0	0	0	0	0	0
190.152.185.244		4.6 MBytes 0.8 %	0	1.2 KBytes	7.9 KBytes	0	0	0	0	0	0	0	0	0	0	0	0
192.168.0.53		4.2 MBytes 0.8 %	0	4.2 MBytes	7.3 KBytes	0	0	3.9 KBytes	0	0	0	0	0	0	0	0	0
www.facebook.com		2.9 MBytes 0.5 %	0		2.9 MBytes	0	0	0	0	0	0	0	0	0	0	0	0
host156.hostmonster.com		2.8 MBytes 0.5 %	0		2.8 MBytes	0	0	0	0	0	0	0	0	0	0	0	0

Figura 44. Monitoreo de la red mediante NTOP
Fuente: Captura de pantalla

CAPÍTULO VI

MANUALES DE OPERACIÓN

El presente capítulo describe los manuales de administración y gestión de cada una de las herramientas implementadas.

6.1. CONTROLADOR DE DOMINIO

El presente manual describe en detalle la administración del controlador de dominio primario instalado sobre Samba 4 desde una PC con el sistema operativo Windows XP y otra con Windows 7.

- **ADMINISTRACIÓN DEL PDC DESDE WINDOWS 7**

Para poder administrar el PDC desde una PC con Windows 7 se debe incluir el equipo al dominio policia.gob.ec, para esto hacer clic en *Inicio*, clic derecho en *Equipo*, *Propiedades*, *Cambiar configuración*, *Nombre del equipo*, *Cambiar*. La *Figura45* muestra la ventana de cambios en donde se debe añadir el nombre del equipo y el dominio al que se va a asociar la PC.

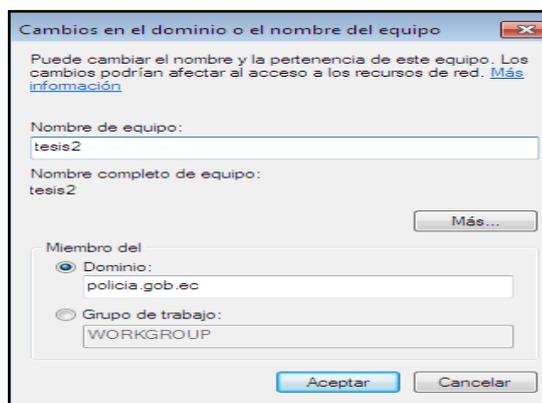


Figura 45. Ventana de configuración de equipo con Windows 7
Fuente: Captura de la configuración en Windows 7

Una vez ingresados los datos, clic en *Aceptar* y aparece la ventana que se muestra en la *Figura46*, aquí se debe ingresar el nombre del usuario administrador del dominio y la clave definida en la instalación de Samba 4, clic en *Aceptar*.

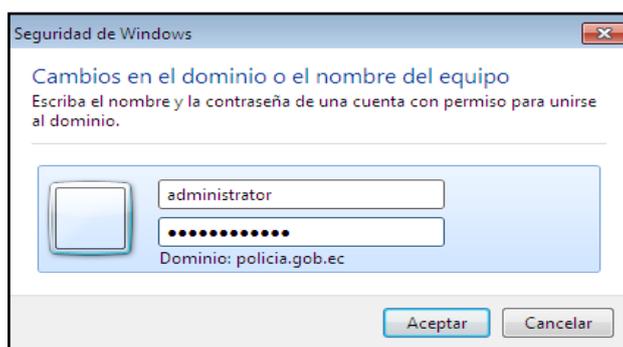


Figura 46. Ingreso de nombre de usuario y clave para administración.

Fuente: Captura de la configuración en Windows 7

Cuando el equipo se ha unido correctamente al dominio, aparece un cuadro de diálogo como se muestra en la *Figura47*.

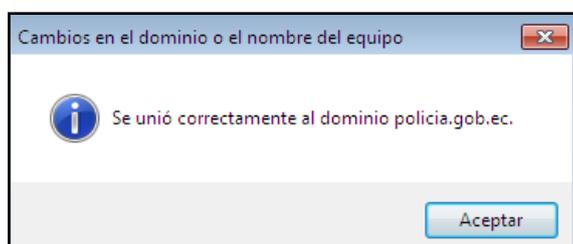


Figura 47. Asociación del equipo al dominio

Fuente: Captura de la configuración en Windows 7

Para empezar a administrar el PDC desde Windows 7 se debe iniciar sesión como administrador del dominio e introducir la clave anteriormente definida. Como se muestra en la *Figura48*, el usuario va a iniciar sesión en el dominio POLICIA.



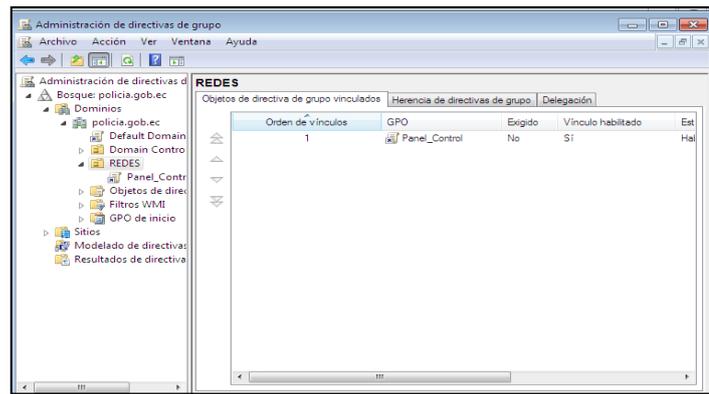
*Figura 48. Inicio de sesión del usuario administrador
Fuente: Captura de la configuración en Windows 7*

Una vez iniciada la sesión como administrador de dominio, hacer clic en *Inicio* y buscar la opción *Administración de directiva de grupo* como se muestra en la *Figura 49*.



*Figura 49. Opción: Administración de directivas de grupo
Fuente: Captura de la configuración en Windows 7*

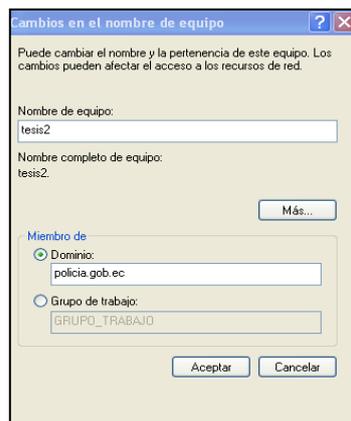
Dentro de la Opción *Administración de directivas de grupo* se encuentran las directivas que permiten la administración de equipos y de usuario. La *Figura 50* muestra la ventana de administración.



*Figura 50. Ventana de administración de directivas
Fuente: Captura de la configuración en Windows 7*

- **ADMINISTRACIÓN DEL PDC DESDE WINDOWS XP**

Para poder administrar el directorio activo desde una PC con Windows XP se debe incluir el equipo al dominio policia.gob.ec, para esto hacer clic en *Inicio*, clic derecho en *Mi PC*, *Propiedades*, *Nombre del equipo*, *Cambiar*. La *Figura51* muestra la ventana de cambios en donde se debe añadir el nombre del equipo y el dominio al que se va a asociar la PC.



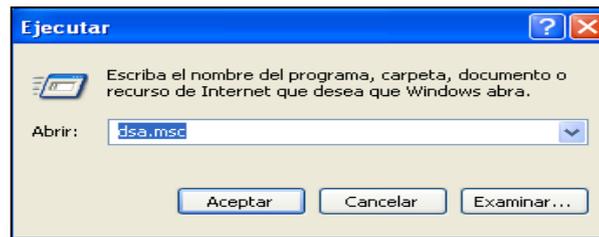
*Figura 51. Ventana de ingreso de nombre de equipo y dominio en Windows XP
Fuente: Captura de la configuración en Windows XP*

Una vez que se ha asociado el equipo al dominio, se debe iniciar sesión como administrador de dominio, como se muestra en la *Figura52*,



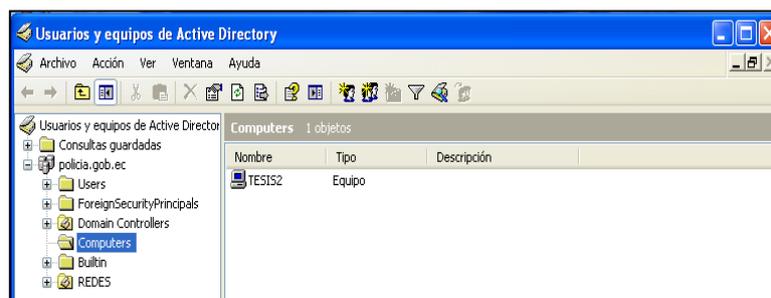
*Figura 52. Inicio de sesión de administrador desde Windows XP
Fuente: Captura de la configuración en Windows XP*

Dentro de la sesión de administrador del dominio ir a *Inicio, Ejecutar* e ingresar el comando `dsa.msc` que permite ejecutar la herramienta de administración remota del servidor de dominio, como se muestra en la *Figura53*.



*Figura 53. Ejecución del comando dsa.msc
Fuente: Captura de la configuración en Windows XP*

Cuando se ha ejecutado el comando, se abre la ventana de *Usuarios y equipos de Active Directory* en donde se puede ya configurar las herramientas de administración del PDC, como se muestra en la *Figura54*.



*Figura 54. Ventana de administración de herramientas de AD en Windows XP
Fuente: Captura de la configuración en Windows XP*

- **ADMINISTRACIÓN DE USUARIOS Y EQUIPOS DEL DC**

La ventana principal de Active Directory es como se muestra en la *Figura55*, cuenta con menús en la barra superior y en la barra lateral izquierda que facilitan su administración.

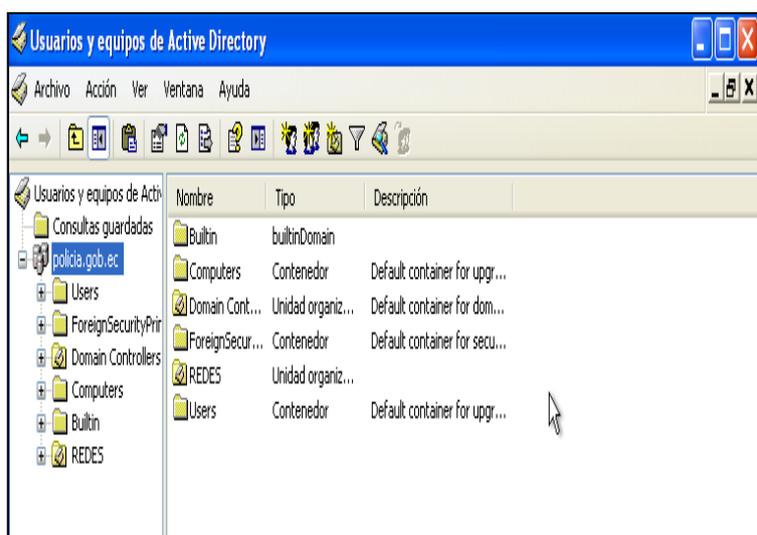


Figura 55. Ventana principal de Active Directory
Fuente: Captura de Active Directory

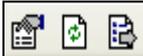
La *Figura56* muestra el menú de la barra superior del AD.



Figura 56. Menú superior
Fuente: Captura de Active Directory

La *Tabla 62* lista las opciones del menú de la barra superior.

Tabla 62. Opciones del menú superior
Fuente: Ventana de administración de Active Directory

	Atrás–Adelante: Permite avanzar o retroceder hacia el nivel anterior o el próximo nivel
	Permite subir a un nivel anterior
	Permite mostrar u ocultar el menú lateral y el panel de acciones
	Muestra las propiedades del dominio Actualiza la ventana de administración de AD Permite exportar listas.
	Proporciona ayuda sobre temas relacionados con el AD.
	Permite crear un nuevo usuario en el contenedor actual
	Permite crear un nuevo grupo en el contenedor actual
	Permite crear un nuevo departamento en el contenedor actual
	Permite establecer opciones de filtrado
	Permite encontrar objetos en AD
	Permite agregar objetos seleccionados en un grupo específico.

La *Figura 57* muestra el menú de la barra lateral izquierda del AD.

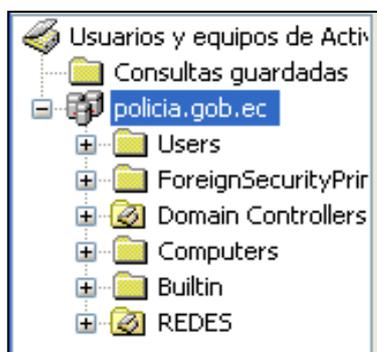


Figura 57. Menú lateral izquierdo
Fuente: Captura de Active Directory

Las opciones del menú lateral son las siguientes:

- Users: Muestra los usuarios de administración que tiene Active Directory por defecto
- Foreign Security Principals: Contenedor predeterminado para los identificadores de seguridad asociado con objetos de dominios externos de confianza.
- Domain Controllers: Muestra el nombre del servidor y el dominio al que pertenece.
- Computers: Muestra el equipo perteneciente al dominio.
- Builtin: Muestra un listado de usuarios administradores propios de AD, cada uno con su funcionalidad.

En este menú se muestran las unidades organizativas creadas en AD.

- **Creación de Unidades Organizativas (UO)**

Para crear una Unidad Organizativa dentro del dominio policía.gob.ec, clic derecho en el dominio, seleccionar la opción *Nuevo* y escoger *Unidad Organizativa*, como se muestra en la *Figura 58*.

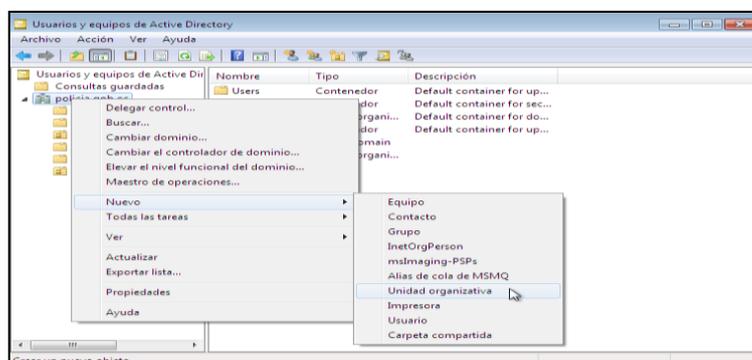


Figura 58. Creación de una Unidad Organizativa
Fuente: Captura de Active Directory

Aparece la ventana que se muestra en la *Figura 59*, aquí se debe ingresar el nombre de la UO, en este caso se crea la unidad TESIS. Clic en *Aceptar*.

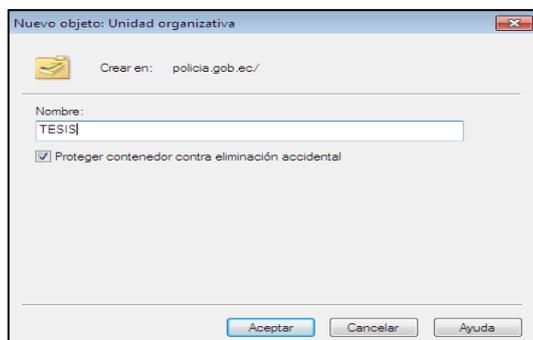


Figura 59. Ingreso de nombre de la Unidad Organizativa
Fuente: *Captura de Active Directory*

Una vez que se ha creado la UO, aparece en el panel lateral como se muestra en la *Figura 60*.

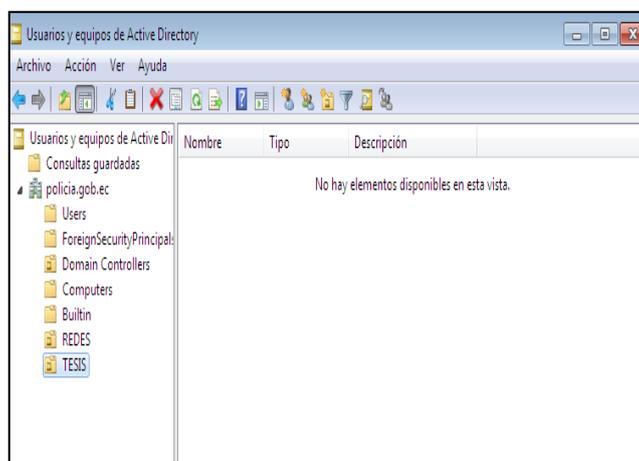
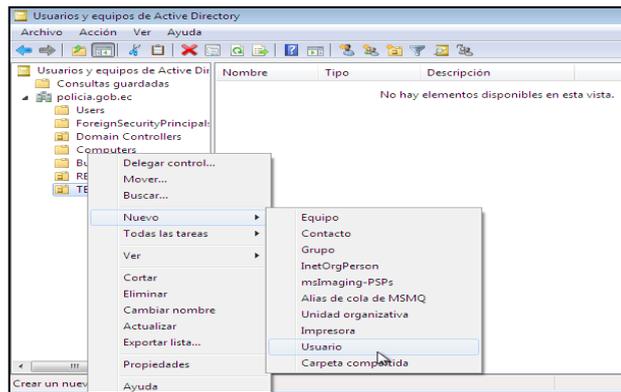


Figura 60. Unidad Organizativa creada
Fuente: *Captura de Active Directory*

- **Creación de usuarios**

Para crear un usuario dentro de una UO, seleccionar la Unidad Organizativa que en este caso es *TESIS*, *clic derecho*, seleccionar *Nuevo* y escoger la opción *Usuario*, como se muestra en la *Figura 61*.



*Figura 61. Creación de un usuario
Fuente: Captura de Active Directory*

Aparece la ventana que se muestra en la *Figura 62*, en donde se deben ingresar los datos del nuevo usuario. Clic en el botón *Siguiente*.

 A screenshot of the 'Nuevo objeto: Usuario' (New Object: User) dialog box. The title bar reads 'Nuevo objeto: Usuario'. Below the title bar, there is a user icon and the text 'Crear en: policia.gob.ec/TESIS'. The main area contains several input fields: 'Nombre de pila:' with 'María' entered; 'Iniciales:' with an empty field; 'Apellidos:' with 'Padilla' entered; 'Nombre completo:' with 'María Padilla' entered; 'Nombre de inicio de sesión de usuario:' with 'mpadilla' entered and '@policia.gob.ec' selected in the dropdown; and 'Nombre de inicio de sesión de usuario (anterior a Windows 2000):' with 'POLICIA\' and 'mpadilla' entered. At the bottom, there are three buttons: '< Atrás', 'Siguiente >', and 'Cancelar'.

*Figura 62. Ingreso de datos para el nuevo usuario
Fuente: Captura de Active Directory*

Antes de terminar con la creación del nuevo usuario es necesario que se le asigne una contraseña, como se muestra en la *Figura 63*.

*Figura 63. Asignación de contraseña para el nuevo usuario
Fuente: Captura de Active Directory*

Una vez que se ha creado el usuario, aparece una ventana con la información del mismo como se muestra en la *Figura 64*, para terminar clic en el botón *Finalizar*.

*Figura 64. Información de usuario creado
Fuente: Captura de Active Directory*

- **Creación de grupos**

Para crear un grupo dentro de una UO, seleccionar la Unidad Organizativa que en este caso es *TESIS*, *clic derecho*, seleccionar *Nuevo* y escoger la opción *Grupo*.

Aparece la ventana que se muestra en la *Figura 65*, aquí se debe ingresar el nombre del grupo, para este caso el grupo a ser creado es *Sistemas*. Clic en el botón *Aceptar*.

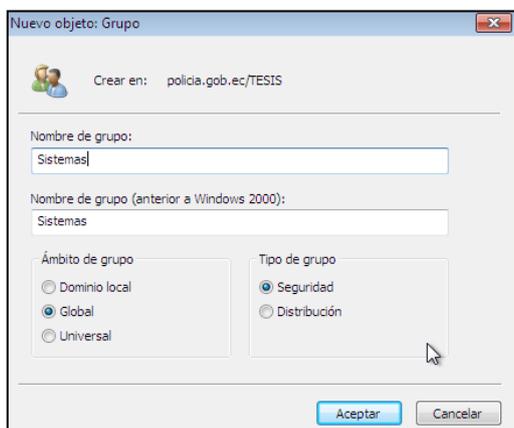


Figura 65. Ingreso del nombre del nuevo grupo
Fuente: Captura de Active Directory

Una vez que se ha creado el grupo aparece dentro de la UO TESIS como se muestra en la *Figura 66*.

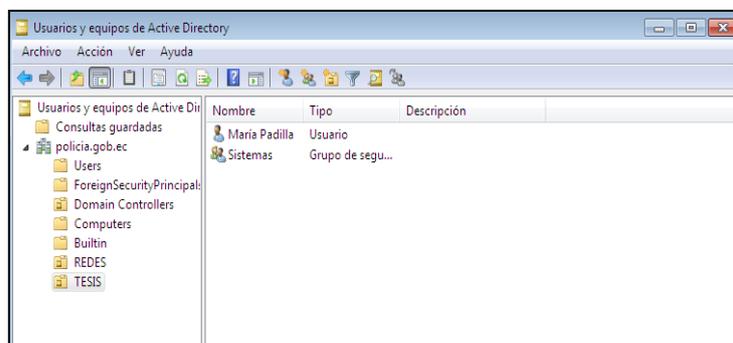


Figura 66. Grupo creado dentro de una unidad organizativa
Fuente: Captura de Active Directory

- **Administración de directivas de grupo**

Para administrar las directivas de las unidades organizativas creadas, hacer clic en *Inicio* y buscar la herramienta *Administración de directivas de grupo* como se muestra en la *Figura 67*.

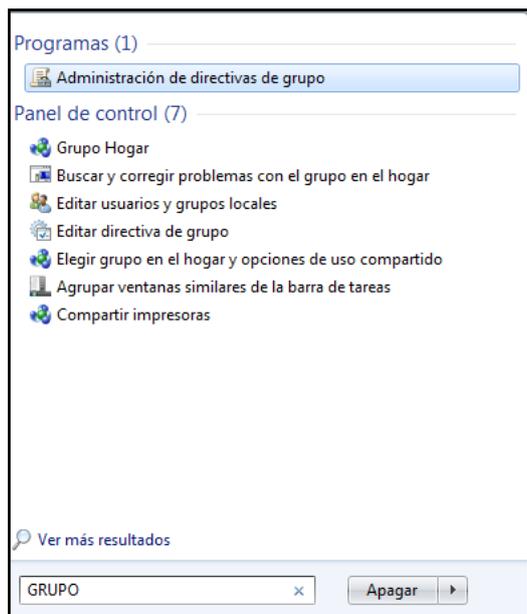


Figura 67. Administración de directivas de grupo
 Fuente: Captura de Administración de directivas de grupo

Dentro de esta herramienta, seleccionar la Unidad Organizativa a la que se le va a aplicar las directivas, para este caso de ejemplo seleccionar *TESIS*, clic derecho y seleccionar la opción *Crear un GPO en este dominio y vincularlo aquí*, como se muestra en la *Figura 68*.

GPO son las siglas en inglés de Objeto de directiva de grupo.

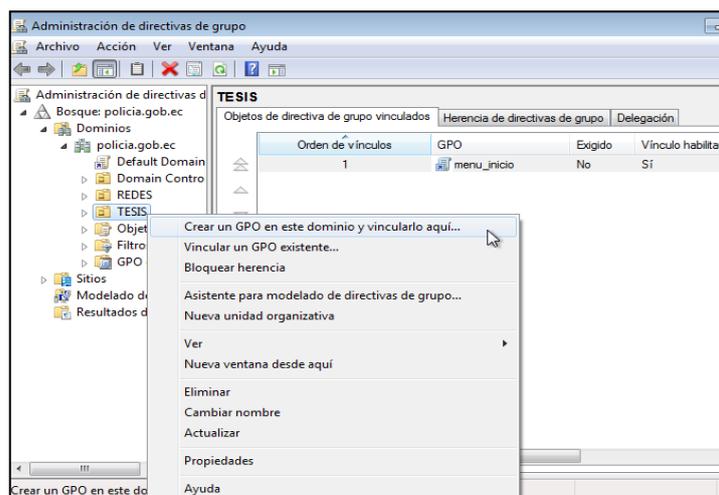


Figura 68. Creación de GPO para la Unidad organizativa
 Fuente: Captura de Administración de directivas de grupo

Aparece una ventana como la que se muestra en la *Figura 69*, en donde se debe ingresar el nombre de la directiva. Clic en *Aceptar*.

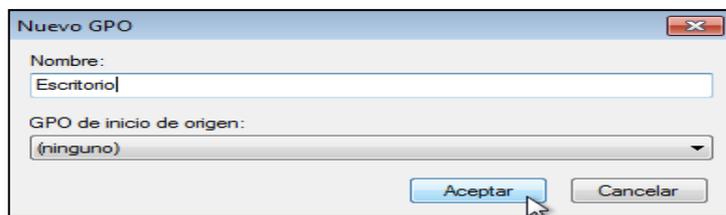


Figura 69. Ingreso de nombre de la directiva
Fuente: Captura de Administración de directivas de grupo

Cuando se ha creado la directiva, ésta se vincula a la unidad organizativa y está lista para editarse, para lo cual hacer clic derecho en la directiva creada y seleccionar la opción *Editar*, como muestra la *Figura 70*.

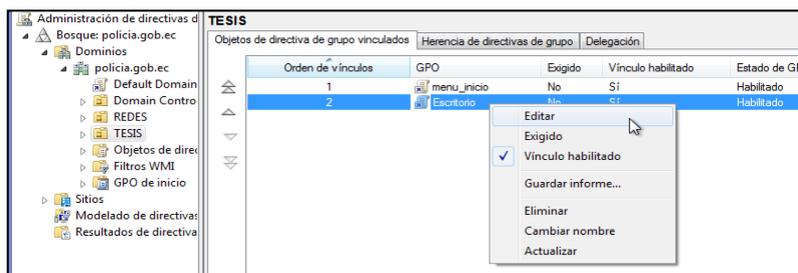


Figura 70. Edición de la directiva creada
Fuente: Captura de Administración de directivas de grupo

Aparece la ventana que se muestra en la *Figura 71*, seleccionar la carpeta *Directivas*, ya que es aquí en donde se encuentran todas las directivas aplicables.

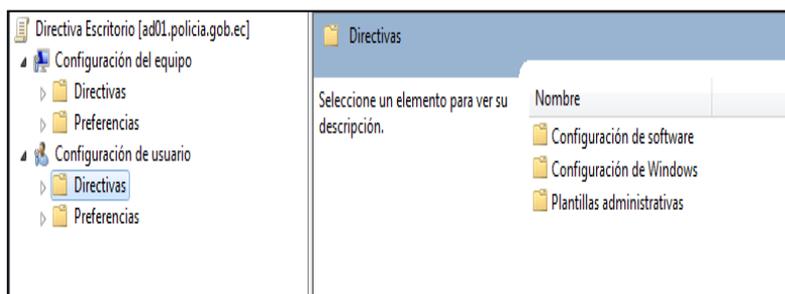


Figura 71. Directivas de grupos
Fuente: Captura de Administración de directivas de grupo

Desplegar la pestaña de la carpeta *Directivas* y seleccionar la directiva que se desea aplicar. En el panel derecho se visualizan las directivas. Hacer clic en la directiva, como se muestra en la *Figura 72*.

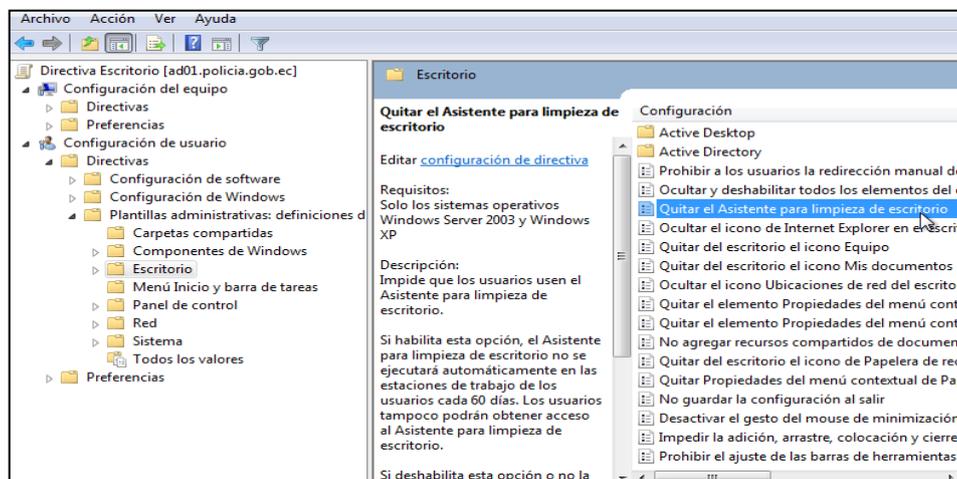


Figura 72. Selección de directivas

Fuente: Captura de Administración de directivas de grupo

Una vez que se ha seleccionado la directiva se debe habilitarla seleccionando la opción *Habilitada* y hacer clic en *Aceptar*, como se muestra en la *Figura 73*.

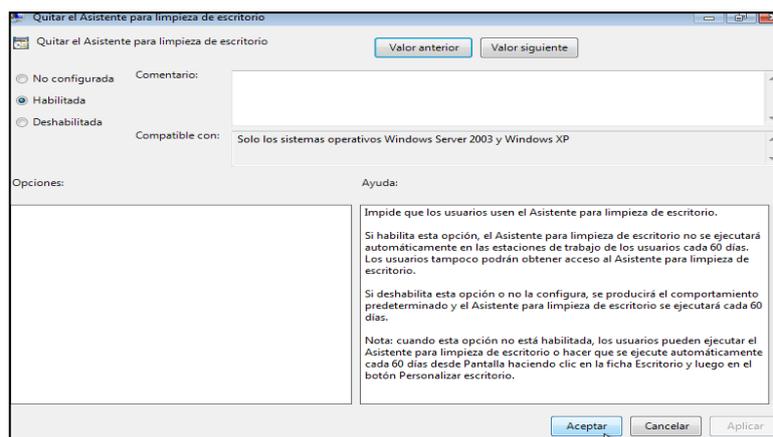


Figura 73. Habilitación de directiva

Fuente: Captura de Administración de directivas de grupo

De esta manera se establece un control sobre las acciones que realizan los usuarios que pertenecen al dominio policía.gob.ec.

6.2. iTALC

EJECUCIÓN DEL PROGRAMA

Una vez que iTALC se está ejecutando en la máquina cliente, va a aparecer el logo en la parte derecha de la barra de tareas, como se muestra en la *Figura 74*.



Figura 74. Logo de la aplicación
Fuente: Captura de Windows XP

Este servicio se ejecuta de manera oculta en la PC del usuario.

INTERFAZ DE USUARIO

La pantalla principal de la aplicación iTALC se muestra en la *Figura 75*:

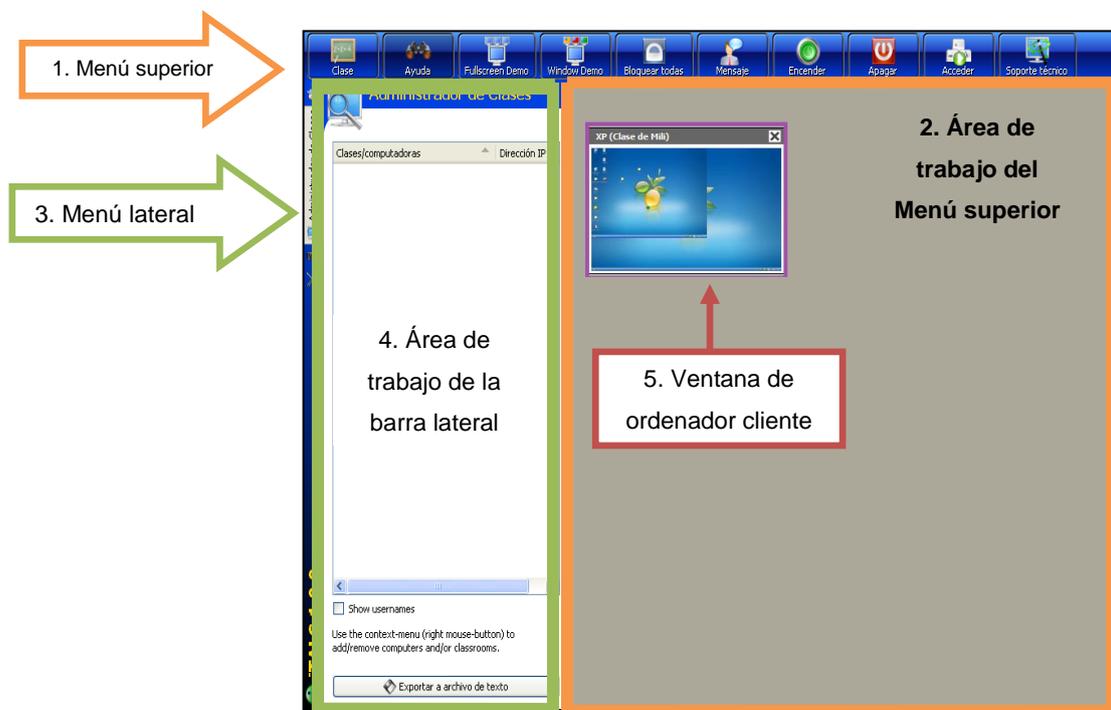


Figura 75. Pantalla principal de iTALC
Fuente: Captura de aplicación iTALC

La aplicación cuenta con las siguientes barras y áreas de trabajo:

- 1) Barra de Menú superior (herramientas y comandos relacionados con las máquinas clientes de los alumnos).
- 2) Área de trabajo del Menú superior.
- 3) Barra de Menú lateral (herramientas de configuración y ayuda).
- 4) Área de trabajo de la barra lateral.
- 5) Ventana de ordenador cliente.

- **Barra de Menú superior**

Esta barra está localizada en el extremo superior de la pantalla y cuenta con las opciones que se muestran en la *Figura 76*:



Figura 76. Barra de menú superior
Fuente: Captura de aplicación iTALC

La *Tabla 63* describe la funcionalidad de las opciones del menú superior

Tabla 63. Descripción de las opciones del menú superior

Fuente: http://www.crie.es/documentos/tic/jornadas/08_09/ITALC.pdf

	Clase: Permite elegir un grupo de usuarios y ocultar la máquina del administrador.
	Ayuda: Permite obtener una visión general de todos los ordenadores conectados, además todos los equipos bloqueados se desbloquean o se abandona el modo demostración al presionar este botón.
	Demo en pantalla completa: Al hacer clic en este botón, la pantalla del administrador se transfiere a todos los equipos. Los usuarios no pueden operar las computadoras, debido a que sus dispositivos de entrada se bloquean.
	Demo en ventana: En este modo la pantalla del administrador se transfiere a la pantalla de los usuarios en una ventana. Los usuarios pueden cambiar a otras ventanas para continuar su trabajo.
	Bloquear todos: Se bloquean los equipos de los usuarios, impidiendo cualquier ejecución.
	Mensajes de texto: Este botón permite enviar un mensaje de texto a todos los usuarios activos.
	Encender: Permite encender las máquinas de los usuarios.
	Apagar: Permite apagar las máquinas de los usuarios.
	Iniciar sesión: Esta opción permite iniciar sesión en todas las computadoras de los usuarios escribiendo el nombre de usuario y contraseña.
	Soporte técnico: Esta función da la oportunidad de controlar cualquier PC-cliente, que no pertenece a un grupo de usuarios.
	Ajustar/Alinear: Permite que las ventanas sean alineadas y a su vez que se ajusten al mayor tamaño posible.
	Autoajuste: Sirve para alinear todas las ventanas activas en orden.

- **Área de trabajo del menú superior**

Dentro de esta área se encuentran todas las ventanas de los ordenadores de los usuarios conectados, aquí se puede visualizar a cada uno de ellos.

- **Barra de Menú lateral**

Se encuentra ubicada en la parte lateral izquierda del programa y contiene las opciones que se describen en la *Tabla 64*:

Tabla 64. Opciones de menú lateral

Fuente: http://www.crie.es/documentos/tic/jornadas/08_09/ITALC.pdf

	Ayuda: Ofrece información sobre la utilización de la aplicación.
	Administrador de Clases: Configuración de los equipos que conforman el aula, cada uno con su nombre y su dirección IP.
	Capturas: Permite capturar pantallas de los equipos de usuarios. Cada captura es un fichero PNG del escritorio del equipo, con el usuario, fecha y hora. Se pueden visualizar o borrar las capturas.
	Configuración: Parámetros de configuración general como los intervalos de actualizaciones, la calidad de los gráficos en las demostraciones, o si por defecto el control remoto permite operar en el equipo remoto o sólo visualizar.

- **Área de trabajo de la barra lateral**

En esta área se despliegan todas las opciones del menú lateral con sus respectivas ventanas para su posterior configuración.

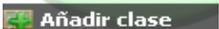
- **Ventana de ordenador cliente**

La ventana del ordenador cliente se muestra en el área de trabajo del menú superior siempre y cuando se encuentre conectada.

ACCIONES SOBRE LOS USUARIOS

- **Agregar clase**

Para agregar una clase o grupo se debe seleccionar la opción *Administrador de clase*  en el menú de la barra lateral. Dentro de este menú hacer clic derecho y seleccionar la opción *Añadir clase*



Aparece una nueva ventana como la que se muestra en la *Figura 77*, en la que se ingresa el nombre del nuevo grupo o clase y se confirma con *Aceptar*. El nuevo grupo aparece en el Administrador de clases.

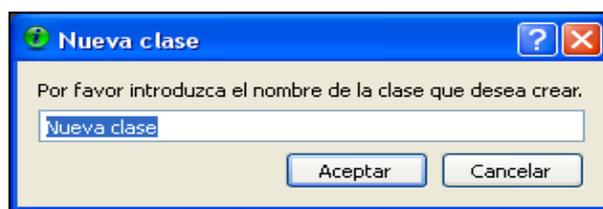


Figura 77. Ventana de ingreso de nombre de grupos
Fuente: Captura de aplicación iTALC

- **Agregar computadora**

Para agregar una computadora a un grupo, seleccionar dentro del menú *Administrador de clase*  la opción *Añadir ordenador*



Aparece la ventana que se muestra en la *Figura 78*, en la que se debe escribir el nombre de la computadora y la dirección IP del equipo. No es obligatorio escribir la dirección MAC ya que este campo es opcional. Además permite elegir a qué grupo o clase el equipo debe ser asignado. Confirmar con *OK*.



Figura 78. Ingreso de datos del nuevo ordenador
Fuente: Captura de aplicación iTALC

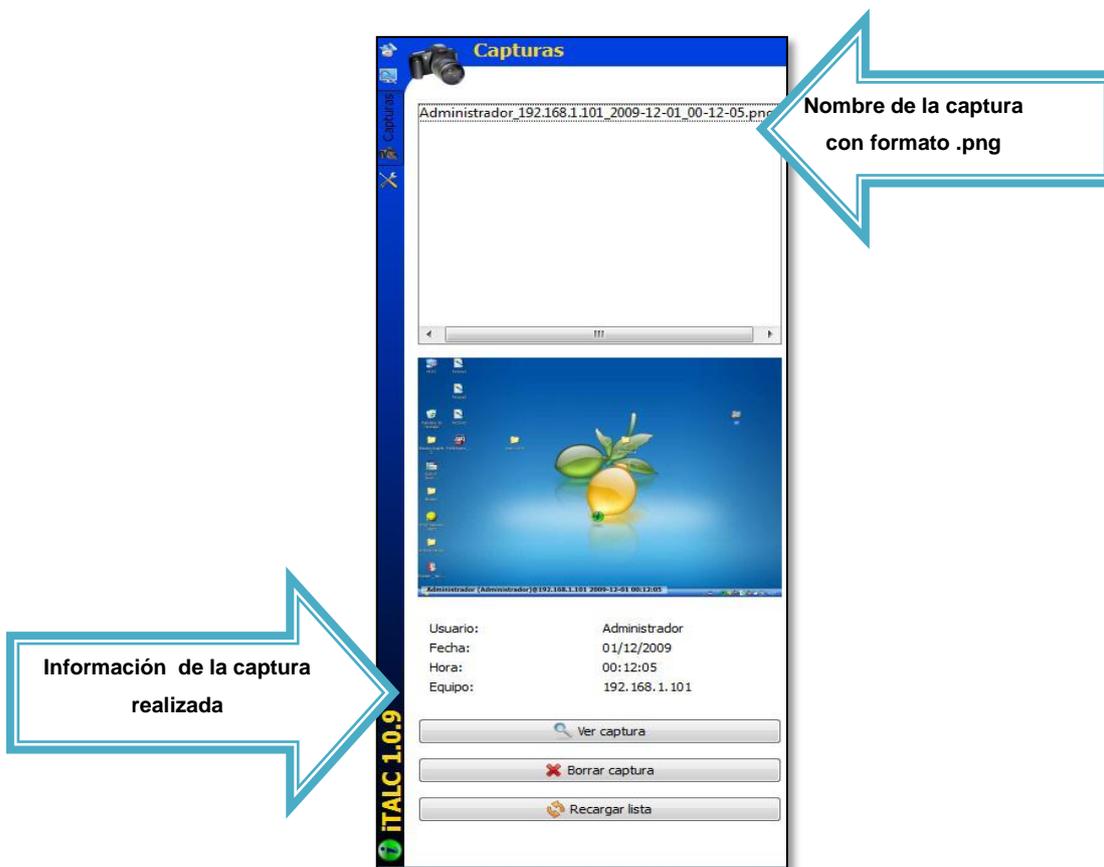
- **Realizar capturas**

Para realizar capturas del escritorio de la pantalla de un PC conectado se selecciona la opción *Capturas*  del menú lateral.

Este botón permite tres opciones:

- Ver captura: para ver la captura que se ha seleccionado
- Borrar captura: para eliminar la captura seleccionada.
- Recargar lista: para actualizar la lista de capturas.

Cada captura realizada se guarda con extensión png, incluyendo el usuario, la fecha, la hora y el equipo, como se muestra en la *Figura 79*.



*Figura 79. Ventana de capturas de pantalla
Fuente: Captura de aplicación iTALC*

- **Configuración de Italc**

Este menú permite realizar ajustes a la configuración por defecto de la aplicación. La *Figura80*, muestra la ventana de configuración de la aplicación.

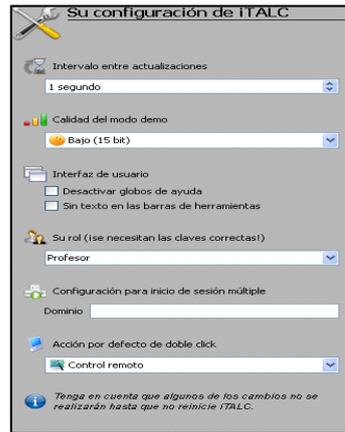


Figura 80. Ventana de configuración de Italc
Fuente: Captura de aplicación iTALC

- **Intervalo entre las actualizaciones:** Aquí se establece el intervalo hasta la próxima actualización de los ordenadores conectados a la computadora de administración.
- **Calidad del modo demo:** Permite elegir la profundidad de color que se desee utilizar en el modo de demostración.
- **Interfaz de usuario:** Aquí se puede activar o desactivar opciones en las barras de menú.
- **Su rol:** Permite escoger la función del usuario de la máquina.
- **Configuración para multi-sesión:** Ingresar el dominio para iniciar una sesión múltiple.
- **Acción por defecto de doble clic:** Puede elegir qué caso debe ser ejecutado en un doble clic.

- **Enviar mensajes de texto**

Para acceder a esta opción se selecciona el botón *Mensaje de texto* aparece la ventana en la que se escribe el mensaje de texto. Al hacer clic en *OK*, el mensaje se envía a todos los equipos activos. La *Figura 81*, muestra la ventana que permite enviar los mensajes de texto.

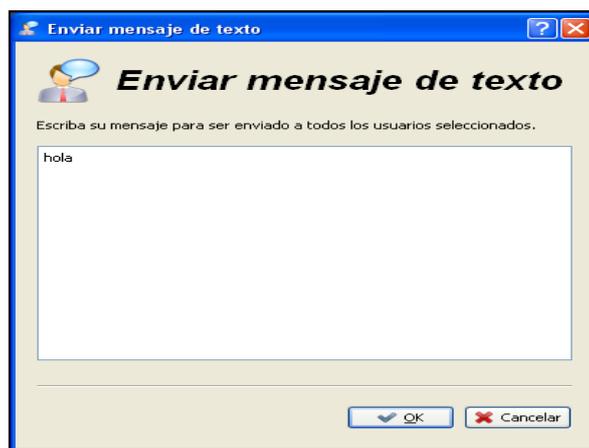


Figura 81. Ventana para ingresar mensajes de texto
Fuente: Captura de aplicación iTALC

- **Apagar equipos**

Para apagar todos los equipos de los usuarios se presiona el botón *Apagar*  ubicado en el menú superior y aparece la ventana que se muestra en la *Figura 82* en la que se debe confirmar la acción a realizar.

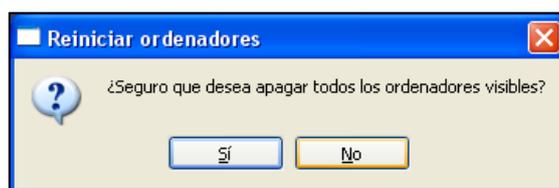


Figura 82. Ventana para confirmación de acción
Fuente: Captura de aplicación iTALC

- **Iniciar sesión en PC de usuarios**

Para iniciar sesión en la máquina de un usuario se selecciona la opción *Iniciar sesión* y aparece la ventana que se muestra en la *Figura 83*, en la que se debe ingresar el nombre del usuario, la contraseña y el dominio al que pertenece.



Figura 83. Ventana de acceso remoto
Fuente: Captura de aplicación iTALC

- **Soporte técnico**

Seleccionar la opción *Soporte técnico* y aparece un cuadro de diálogo como el de la *Figura 84*, en el que se debe ingresar la dirección IP de la PC que se desea controlar y para confirmar se da clic en *OK*. Un vez que se accede a la PC cliente aparece un cuadro de diálogo en la pantalla del usuario. Este cuadro de diálogo informa al usuario que alguien externo desea tener acceso a este equipo. Deberá confirmar este cuadro de diálogo haciendo clic en *Sí* o haciendo clic en *Siempre para esta sesión* para permitir el acceso externo.



*Figura 84. Ventana de soporte técnico
Fuente: Captura de aplicación iTALC*

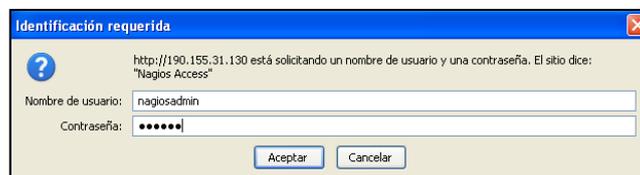
6.3. NAGIOS3-NCONF

NConf es la herramienta web que facilita la configuración del software de supervisión Nagios3.

NAGIOS 3

Mediante la interfaz Web, Nagios permite monitorear el entorno de la red. Para ingresar a la aplicación se debe realizar los siguientes pasos:

- 1.- Abrir una ventana en cualquier explorador WEB
- 2.- En el campo de Dirección ingresar la dirección: `http://IP_servidor/nagios3`
- 3.- Presionar *Enter* y aparece la ventana que se muestra en la *Figura 85*:



*Figura 85. Ventana de Autenticación
Fuente: Captura de la interfaz web de nagios3*

En esta ventana el administrador de red debe registrarse ingresando Usuario y Contraseña. Hacer clic en *Aceptar*.

Al ingresar a la aplicación se muestra la pantalla principal de Nagios. En el lado izquierdo de la página principal se muestra el menú de opciones de Monitoreo y en el lado derecho se muestra el contenido de cada opción. El menú de opciones consta de 4 partes Principales, como se muestra en la *Figura 86*:

- General,
- Monitoring
- Reporting (Informes)
- System (Sistema)



Figura 86. Pantalla principal de nagios3
 Fuente: Captura de la interfaz web de nagios3

- **GENERAL**

La información que ofrece este menú es acerca de Nagios 3. Muestra las herramientas que incluye con relación a versiones anteriores y documentación que puede ayudar al usuario en caso de dudas sobre la aplicación.

- **HOME**

Al hacer clic sobre el menú *Home* se muestra la página principal de Nagios 3, en la misma que se puede acceder a los enlaces: *Read what's new in Nagios 3* para revisar los cambios nuevos que posee en relación

a versiones anteriores y www.nagios.org/ para acceder a la página oficial de Nagios.

– DOCUMENTATION

Al hacer clic sobre este menú se ingresa se muestra dos enlaces: <http://www.nagios.org> para consultar información en la página oficial de Nagios y *Table of Contents* para consultar documentación respecto a la aplicación (instalación, configuración, funcionamiento, etc.).

• MONITORING

La información que se muestra en esta sección es sobre eventos y sucesos que ocurren en la red detectados por Nagios.

– TACTICAL OVERVIEW

Al hacer clic sobre este menú se muestra la ventana de la *Figura 87*:



Figura 87. Información del estado actual de la red
Fuente: Captura de la interfaz web de nagios3

Esta ventana muestra la información general del monitoreo de la red.

Desde esta ventana se puede revisar la información sobre:

- ~ *Network Outages (Caídas de servicio de la red).*- Aquí se muestra la información de los hosts con caída de servicio, estado, servicios afectados, y acciones tomadas.
- ~ *Host Detail (Detalles de host).*-Permite ver los detalles de los host que están en estado Down, Unreachable, Up y Pending (Abajo, Inalcanzable, Arriba y Pendiente).
- ~ *Service detail (Detalles de servicios).*-En este menú se puede revisar el estado de los servicios Critical, Warning, Unknown, Ok, Pending (Crítico, Alerta, Desconocido, Bien, Pendiente).
- ~ *Monitoring Features (Monitoreo de Funciones).*- Esta sección permite habilitar y deshabilitar las funciones de Flap detection, Notifications, Event handlers, Active Checks y Passive Checks (Detecciones de Flap, Notificaciones, Controladores de eventos, Controles Activos y Controles Pasivos). El monitoreo de funciones se muestra en la *Figura 88*,

Monitoring Features				
Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled	Enabled	Enabled	Enabled	Enabled
All Services Enabled				
No Services Flapping	All Hosts Enabled	All Hosts Enabled	All Hosts Enabled	All Hosts Enabled
All Hosts Enabled				
No Hosts Flapping				

Figura 88. Funciones de Monitoreo
Fuente: Captura de la interfaz web de nagios3

Flap Detection: Nagios admite opciones de detección de host y servicios que están en estado *flapping*. Este estado se produce cuando un host o servicio cambia con demasiada frecuencia (se cae y se levanta enseguida en un periodo de tiempo corto) provocando una tormenta de notificaciones de problemas y de recuperaciones.

Notificaciones: La razón de enviar notificaciones es realizar la verificación del servicio y la verificación lógica de host.

Event Handlers: Los controladores de eventos son comandos que se ejecutan cada vez que se produce un cambio de estado de un host o servicio. Un uso obvio para los controladores de eventos (especialmente con los servicios) es la capacidad que posee Nagios para solucionar los problemas de manera preactiva antes de realizar una notificación. Otro uso potencial de los controladores de eventos es el registro de eventos de hosts y servicios a una base de datos externa.

Active Checks: Los controladores activos son usados para monitorear los hosts y servicios que se encuentran dentro del mismo segmento en el que se encuentra el host de Nagios.

Verificaciones Pasivas: Las verificaciones de host y servicio que se llevan a cabo se presentan a Nagios por aplicaciones externas llamadas controles pasivos. Los controles pasivos pueden ser

contrastados con controles activos, los cuales son controles de hosts o servicios que han sido iniciados por Nagios.

– SERVICE DETAIL

Esta ventana muestra el detalle del estado de todos los servicios de los diferentes host, como indica la *Figura 89*.

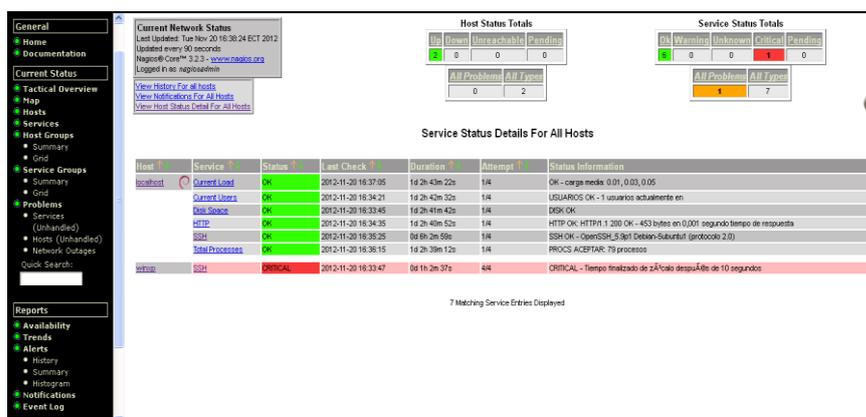


Figura 89. Detalle de Servicios
Fuente: Captura de la interfaz web de nagios3

Dentro de esta ventana se puede conocer de forma rápida el estado de los host. Así también en la parte superior izquierda del contenido permite ver de forma directa el historial de todos los host, notificaciones de los host y el detalle del estado de los host.

– HOST DETAIL

Esta ventana muestra el detalle del estado de todos los host. Al hacer clic sobre esta opción del menú principal aparece la ventana que se muestra en la *Figura 90*:

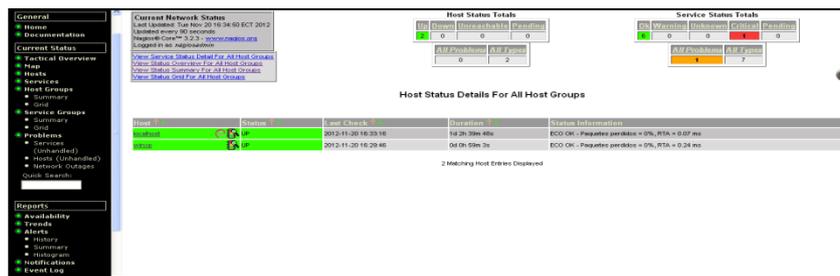


Figura 90. Detalle del estado de host
Fuente: Captura de la interfaz web de nagios3

Dentro de esta ventana se puede conocer de forma rápida el estado de los servicios. Así también en la parte superior izquierda del contenido permite ver de forma directa el detalle del estado de los servicios, una descripción general del estado, un resumen de estado y una tabla de estado por grupos de host.

– HOSTGROUP OVERVIEW

Esta ventana muestra un resumen general de los servicios agrupados por grupos de host. Para acceder a esta opción del menú principal, hacer clic sobre *Hostgroup Overview*, aparece la ventana que se muestra en la *Figura 91*:

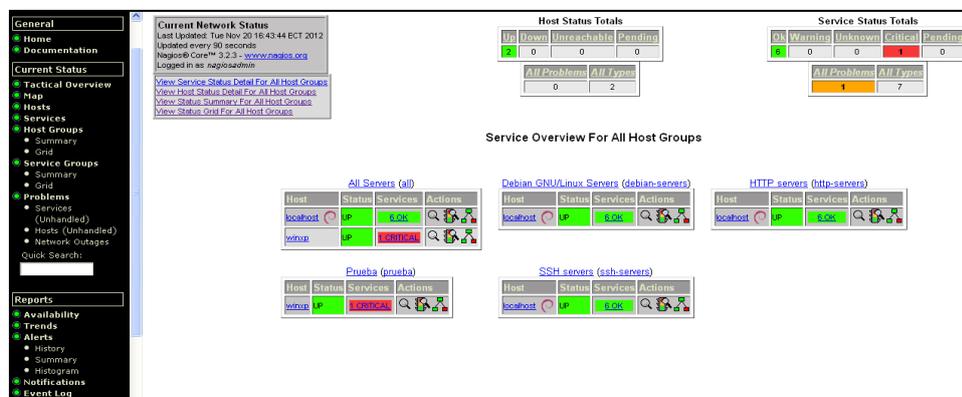


Figura 91. Resumen general de grupos de host.
Fuente: Captura de la interfaz web de nagios3

Para ver la información correspondiente a los host o servicios dar clic sobre su nombre o estado.

○ HOSTGROUP SUMMARY

Para acceder a esta opción hacer clic sobre *Hostgroup Summary* del menú principal. En esta ventana se muestra un resumen del estado de los host y los servicios por grupos de host, como indica la *Figura 92*.

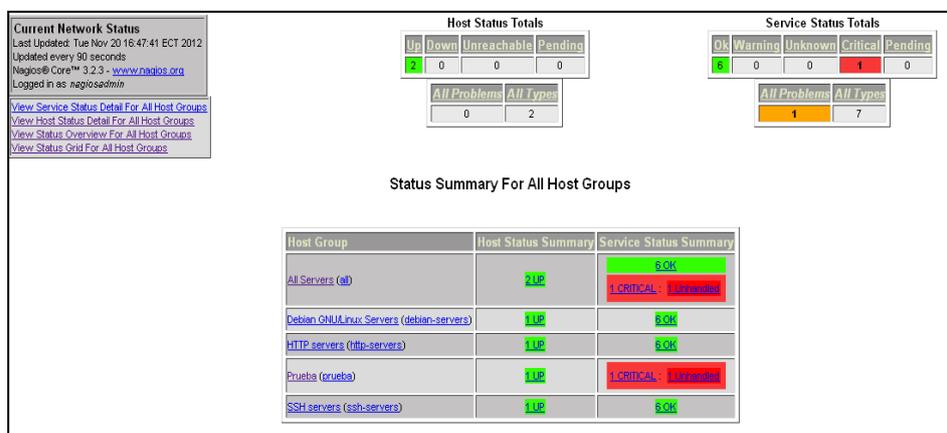


Figura 92. Resumen de estado de grupos de host

Fuente: Captura de la interfaz web de nagios3

Para ver todos los host que pertenecen a un determinado grupo dar clic sobre el nombre del grupo. Para ver la lista de los host o servicios en determinado estado dar clic sobre el estado respectivo.

○ HOSTGROUP GRID

Para acceder a esta opción hacer clic sobre *Hostgroup Grid* del menú principal. Esta ventana muestra el estado de la red agrupándolos por grupos de host. La *Figura 93* muestra esta ventana.

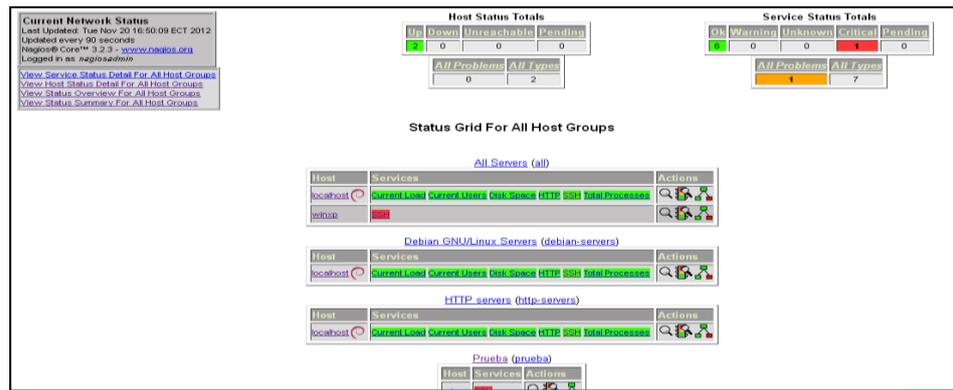


Figura 93. Estado de la red por grupos de host
Fuente: Captura de la interfaz web de nagios3

– SERVICEGROUP OVERVIEW

Para acceder a esta opción hacer clic sobre *Servicegroup* del menú principal. En esta ventana se muestra información general de los servicios, agrupados por grupos de servicios, como indica la *Figura 94*.

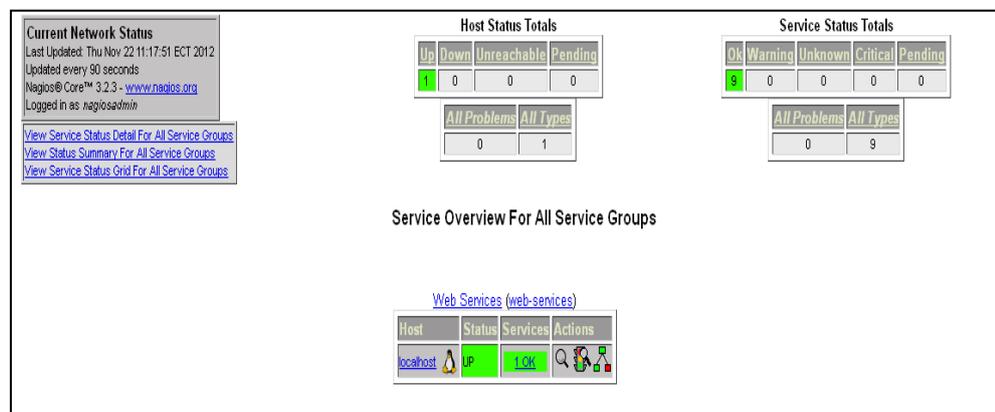


Figura 94. Información general por grupos de servicios
Fuente: Captura de la interfaz web de nagios3

○ SERVICEGROUP SUMMARY

Para acceder a esta opción hacer clic sobre *Servicegroup Summary* del menú principal. En esta ventana se muestra un resumen de estado en base a los grupos de servicio, como indica la *Figura 95*.

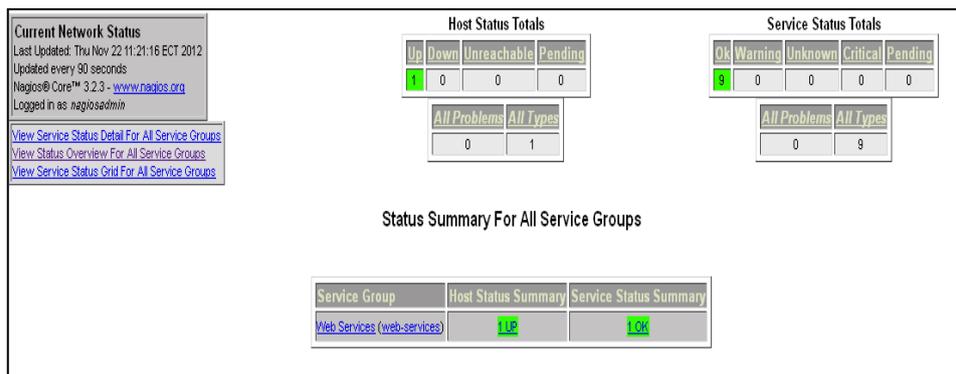


Figura 95. Resumen general por grupos de servicios
 Fuente: Captura de la interfaz web de nagios3

○ SERVICEGROUP GRID

Para acceder a esta opción hacer clic sobre *Servicegroup Grid* del menú principal. En esta ventana se muestra una tabla de estado en base a los grupos de servicio, como indica la *Figura 96*.

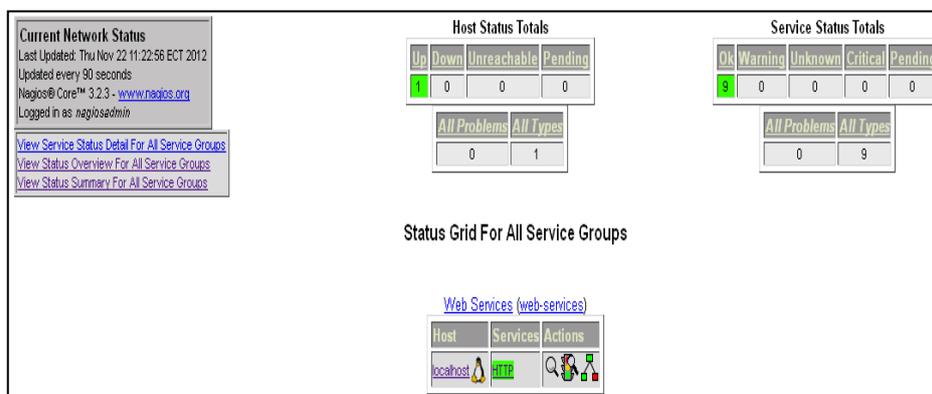


Figura 96. Estado de la red por grupos de servicios
 Fuente: Captura de la interfaz web de nagios3

– STATUS MAP

Para acceder a esta opción hacer clic sobre *Map* del menú principal. Aparece la ventana que se muestra en la *Figura 97*:

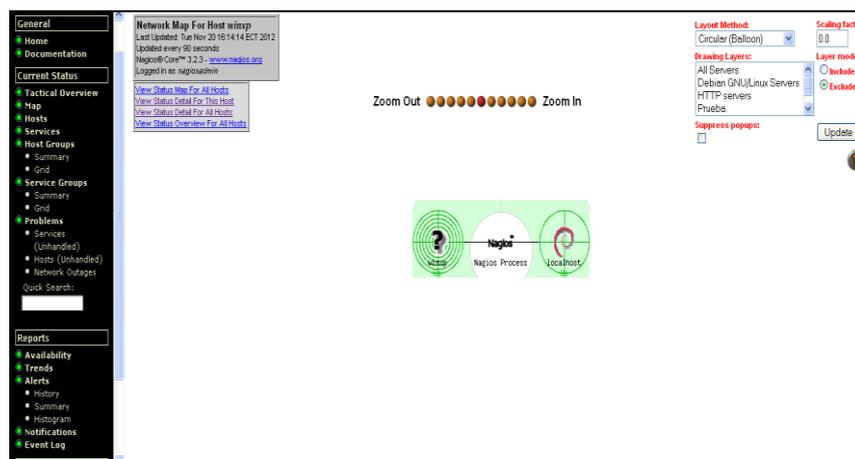


Figura 97. Mapa de estado
Fuente: Captura de la interfaz web de nagios3

La opción *Map*(Mapa) muestra una ventana con todos los hosts de la red en forma gráfica en 2-D, indicando el estado de cada host con su respectivo nombre.

Al colocar el puntero sobre cualquier host aparece una pequeña nota descriptiva acerca de dicho host, como se muestra en la *Figura 98*.

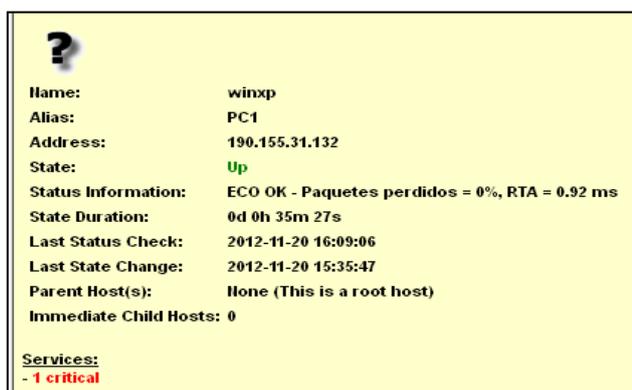


Figura 98. Nota descriptiva del host
Fuente: Captura de la interfaz web de nagios3

Al hacer doble clic sobre el host aparece una ventana con todos los servicios que tiene activado dicho host, como se muestra en la *Figura 99*.

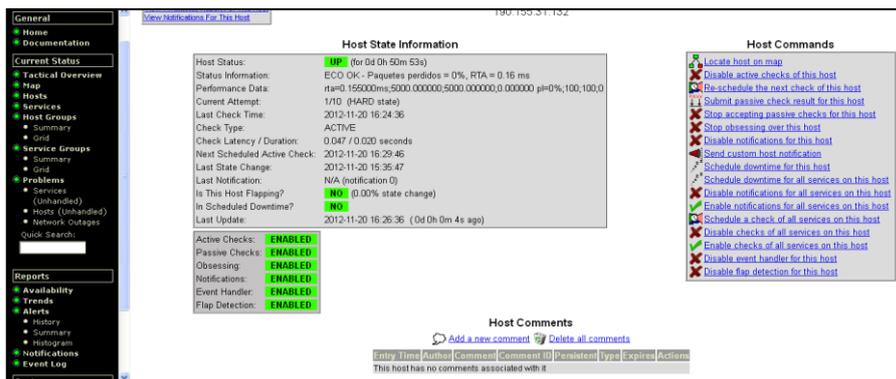


Figura 99. Detalle de servicios activos en un host
Fuente: Captura de la interfaz web de nagios3

Para revisar la información sobre algún servicio de este host hacer clic sobre el nombre del servicio.

– 3-D STATUS MAP

Esta opción permite visualizar el mapa de estado de los hosts de la red en 3-D. Al hacer clic sobre esta opción, va a querer grabar el archivo en la PC y no lo va abrir. La ventana que aparece es como la de la Figura 100:



Figura 100. Descarga de archivo para mapa 3D
Fuente: Captura de la interfaz web de nagios3

Para que funcione adecuadamente esta opción se debe instalar un cliente VRML (Virtual Reality Modeling Language), el cual es un plugin para el navegador, para esto se puede utilizar muchas opciones, por ejemplo:

- FreeWRL
- OpenVRML
- Cortona VRML Client

– SERVICE PROBLEMS

En esta ventana se muestra el nombre del host, el estado, la fecha y hora de la última verificación, el número de intentos y la información del estado.

Para verificar en detalle el servicio con problema hacer clic sobre el nombre del servicio, como se muestra en la *Figura 101*.

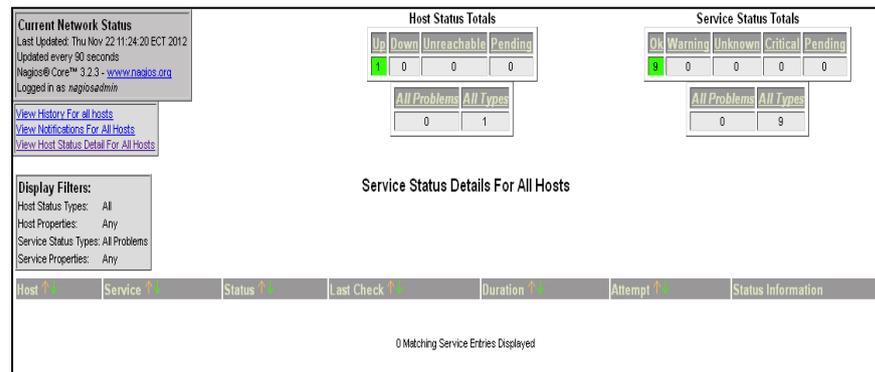


Figura 101. Detalle de servicios con problemas
 Fuente: Captura de la interfaz web de nagios3

– HOST PROBLEMS

Para acceder a esta opción hacer clic sobre *Host Problems* del menú principal. En esta ventana se muestran todos los host con problemas (en caso de que lo haya), el estado, la última verificación, la duración y la información del estado. Para verificar el detalle del host con problema dar clic sobre el nombre del host, como se muestra en la *Figura 102*.

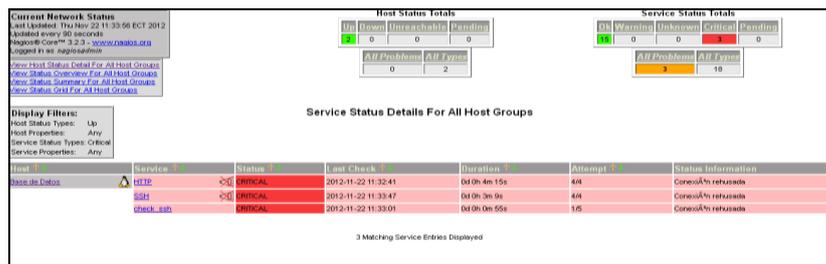


Figura 102. Detalle de host con problemas
 Fuente: Captura de la interfaz web de nagios3

– NETWORK OUTAGES

Para acceder a esta opción hacer clic sobre *Network Outages* del menú principal. En esta ventana se muestran las redes con caídas de servicio (en caso de que las haya), indicando la severidad, el host, el estado, la duración del estado, el número de host afectados, el número de servicios afectados y las acciones, como se muestra en la *Figura 103*.

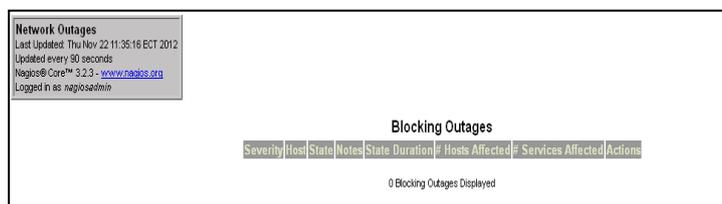


Figura 103. Caídas de servicio en la red
 Fuente: Captura de la interfaz web de nagios3

– SHOW HOST

En la parte izquierda de la pantalla en el menú principal, se muestra un cuadro de texto en el cual se puede ingresar el host o grupo de host que se desee mostrar, como indica la *Figura 104*,



Figura 104. Búsqueda rápida de host o grupo de host
 Fuente: Captura de la interfaz web de nagios3

– COMMENTS

Para acceder a esta opción hacer clic sobre *Comments* del menú principal. Esta opción permite ingresar comentarios a los host o/y servicios. Para añadir un nuevo comentario dar clic sobre el enlace *Add a new host comment* o *Add a new service comment* según sea el caso. La *Figura 105*, muestra esta ventana.

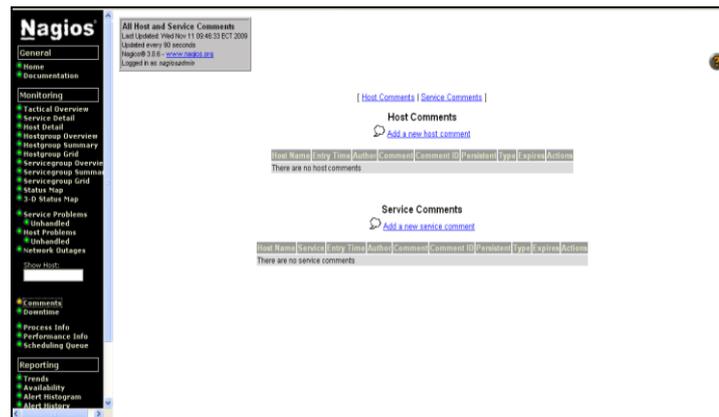


Figura 105. Ingreso de comentarios
Fuente: Captura de la interfaz web de nagios3

Los comentarios pueden ser útiles cuando existen varios administradores para compartir información relacionada con algún problema de cierto equipo. Si no se activa la opción *Persistnet*, el comentario será automáticamente borrado la próxima vez que Nagios sea reiniciado.

– DOWNTIME

Para acceder a esta opción hacer clic sobre *Downtime* del menú principal. Esta opción permite programar el tiempo de inactividad de un host o servicio según sea el caso. Para esto hacer clic sobre el enlace deseado.

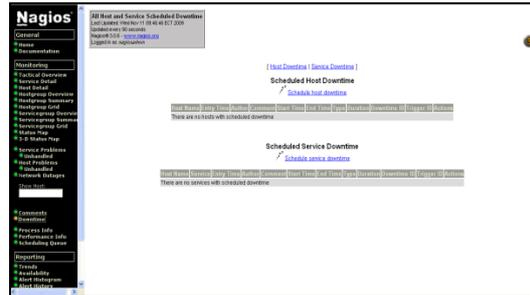


Figura 106. Programación de tiempos de inactividad
Fuente: Captura de la interfaz web de nagios3

Por ejemplo para programar el tiempo de inactividad de un host en particular dar clic en *Schedule host downtime*. Aparece la siguiente ventana en la cual es necesario llenar la información correspondiente.

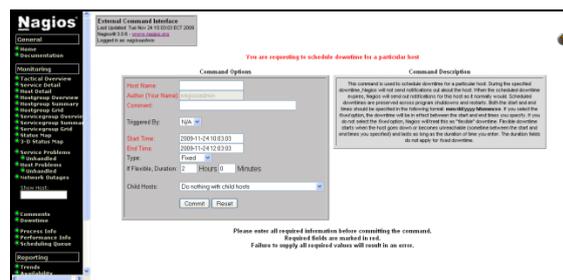


Figura 107. Programación de tiempos de inactividad en un host
Fuente: Captura de la interfaz web de nagios3

Durante el tiempo de inactividad especificado, Nagios no enviará notificaciones acerca del host o servicio.

Cuando expire el tiempo de inactividad programado, Nagios enviará notificaciones de este host o servicio como lo haría normalmente. Los tiempos de parada programada se conservan a través de cierres de programa y reinicio. Tanto los tiempos de inicio y fin deben ser especificados en el siguiente formato: dd / mm / aaaa hh: mm: ss. Si selecciona la opción *fixed*, el tiempo de inactividad estará entre el inicio y finalización que se especifique. Si no se selecciona la opción *fixed*,

Nagios entenderá como tiempo de inactividad "flexible", en el que, el tiempo de inactividad se inicia cuando el host se cae o se vuelve inalcanzable (en algún momento entre el inicio y de finalización que se ha especificado) y dura el tiempo en que se tarde en volver a entrar.

– PROCESS INFO

Para acceder a esta opción hacer clic sobre *Process Info* del menú principal. En esta ventana se muestra la información de procesos de Nagios, como la versión del programa, hora de inicio del programa, tiempo de ejecución, entre otros, como se indica a continuación:

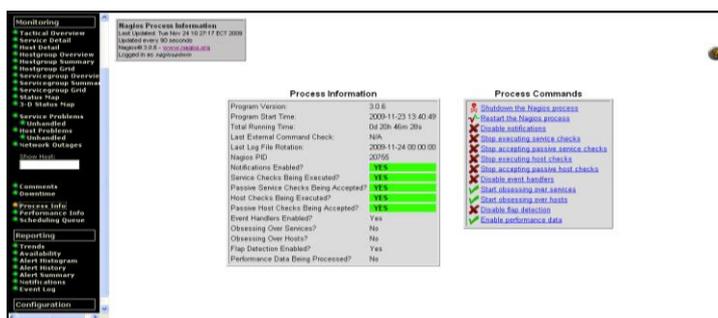


Figura 108. Información de procesos de Nagios

Fuente: Captura de la interfaz web de nagios3

– PERFORMANCE INFO

Para acceder a esta opción hacer clic sobre *Performance Info* del menú principal. En esta ventana se muestra la información relativa al rendimiento de los servicios y host. La verificación de los servicios y host tanto activos como pasivos, se muestra durante escalas de tiempo transcurridos de 1 minuto, 5 minutos, 15 minutos y 1 hora. Además del número de host y servicios verificados desde que inició el programa.

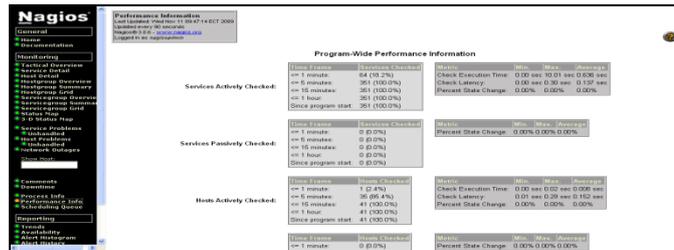


Figura 109. Información del rendimiento de host y servicios
Fuente: Captura de la interfaz web de nagios3

En esta ventana también se muestra un resumen de la verificación de los host y servicios.

– SCHEDULING QUEUE

Para acceder a esta opción hacer clic sobre *Scheduling Queue* del menú principal. Esta ventana muestra la cola de verificación de host y servicios. Por medio de esta verificación constante se puede determinar el estado de los mismos.

• REPORTING

En esta sección se encuentra el menú de opciones que se utilizan para revisar reportes de disponibilidad, notificaciones y alarmas de los hosts y servicios de los dispositivos de la red.

– TRENDS

Esta opción es usada para crear un gráfico de los estados de host o servicio durante un período de tiempo arbitrario. Se pueden revisar los estados ocurridos desde el día actual, hasta el año pasado dependiendo de la necesidad del administrador.

Para revisar esta información se debe realizar lo siguiente, clic sobre *Trends* del menú principal, aparece la ventana que se muestra en la *Figura 110*:



Figura 110. Paso 1, para crear reportes de estado
Fuente: Captura de la interfaz web de nagios3

Esta pestaña permite seleccionar dos tipos de reporte: reporte de host y reporte de servicio. Seleccionar el tipo de reporte que se desea crear en Una vez seleccionado el tipo de reporte hacer clic en el botón `[Continue to Step 2]`, aparece la ventana que se muestra en la *Figura 111*:

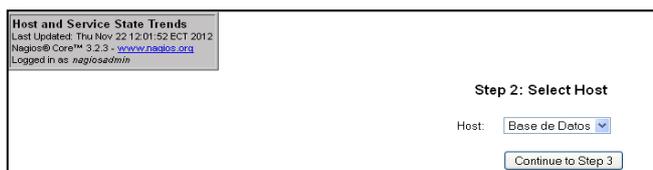


Figura 111. Paso 2, para crear reportes de estado
Fuente: Captura de la interfaz web de nagios3

Desplegar la pestaña para seleccionar el host del que se desea realizar el reporte, a continuación hacer clic sobre `[Continue to Step 3]`. Aparece la ventana que se muestra en la *Figura 112*:

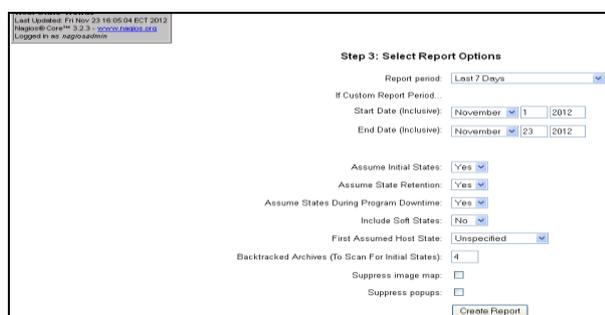


Figura 112. Paso 3, para crear reportes de estado
Fuente: Captura de la interfaz web de nagios3

En esta ventana se seleccionan los parámetros que se desea para crear el reporte. Una vez establecidas las opciones se crea el reporte haciendo clic sobre .

– AVAILABILITY

Estos reportes indican los porcentajes de disponibilidad de un host, grupo de host, servicio o grupos de servicios. Indicando la disponibilidad de cada estado.

Para crear este tipo de reportes se hace clic sobre el menú principal *Availability*, aparece la ventana que se muestra en la *Figura 113*, en la que se debe seleccionar el tipo de reporte que se desea crear.



Figura 113. Paso 1, para crear reportes de disponibilidad
Fuente: Captura de la interfaz web de nagios3

Los tipos de reportes que son posibles de realizar pueden ser de un host, grupo de host, un servicio o grupo de servicios

Luego hacer clic sobre .

Aparece la ventana que se muestra en la *Figura 114*:

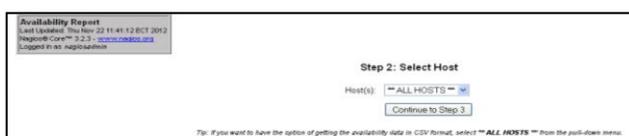


Figura 114. Paso 2, para crear reportes de disponibilidad
Fuente: Captura de la interfaz web de nagios3

En esta ventana se debe especificar o determinar el host, grupo de hosts, servicio o grupo de servicios del cual se desea crear el reporte, luego hacer clic sobre .

Aparece la siguiente ventana, que se muestra en la *Figura 115*:

The screenshot shows a web form titled "Step 3: Select Report Options". The form includes the following fields and options:

- Report Period:** A dropdown menu set to "Last 7 Days".
- If Custom Report Period...:** A section for custom date ranges.
 - Start Date (Inclusive):** A date selector showing "November 1 2012".
 - End Date (Inclusive):** A date selector showing "November 22 2012".
- Report time Period:** A dropdown menu set to "None".
- Assume Initial States:** A dropdown menu set to "Yes".
- Assume State Retention:** A dropdown menu set to "Yes".
- Assume States During Program Downtime:** A dropdown menu set to "Yes".
- Include Soft States:** A dropdown menu set to "No".
- First Assumed Host State:** A dropdown menu set to "Unspecified".
- First Assumed Service State:** A dropdown menu set to "Unspecified".
- Backtracked Archives (To Scan For Initial States):** A text input field containing the number "4".
- Output in CSV Format:** An unchecked checkbox.
- Create Availability Report!** A button at the bottom right of the form.

Figura 115. Paso 3, para crear reportes de disponibilidad
Fuente: Captura de la interfaz web de nagios3

Esta ventana permite especificar las opciones que se desea incluir en el reporte. Las opciones son las siguientes:

ReportPeriod: Establece el periodo que se desee para crear el reporte, al desplegar el campo se pueden seleccionar la opción más adecuada.

Start Date (Inclusive): Establece la fecha desde la que se desee iniciar el reporte.

End Date (Inclusive): Establece la fecha hasta la que se desea realizar el reporte.

Report time period: Establece el periodo de tiempo trabajado, sin trabajar, las 24 horas durante 7 días, o ningún caso.

Assume Initial States: Se puede seleccionar Yes o No de acuerdo al criterio del administrador. Esta opción permite asumir o no estados iniciales.

Assume State Retention: En esta opción se puede o no asumir estados retenidos.

Assume States During Program Downtime: Esta opción permite asumir o no los estados durante el tiempo de inactividad del software.

Include Soft States: Se puede incluir o no estados Soft. Este estado ocurre cuando un host o servicio se recupera de un error de software.

First Assumed Host State: Se puede asumir primero el estado de host. Esta opción crea reportes de acuerdo a la opción seleccionada: Unspecified, Current State, Host Up, Host Down y Host Unreachable la opción seleccionada aparece de distinto color en el reporte.

First Assumed Service State: Se puede asumir primero el estado de servicio. Esta opción crea reportes de acuerdo a la opción seleccionada: Unspecified, Current State, Service Ok, Service Warning, Service Unknown y Service Critical, la opción seleccionada aparece de distinto color en el reporte.

Backtracked Archives (To Scan For Initial States): Permite seleccionar el número de archivos anteriores para buscar estados iniciales. Estos archivos se pueden seleccionar desde 0 hasta 60.

Una vez definidas todas las opciones se hace clic sobre

para crear el reporte de disponibilidad.

La ventana que se abre es similar a la que se muestra en la *Figura 116*:

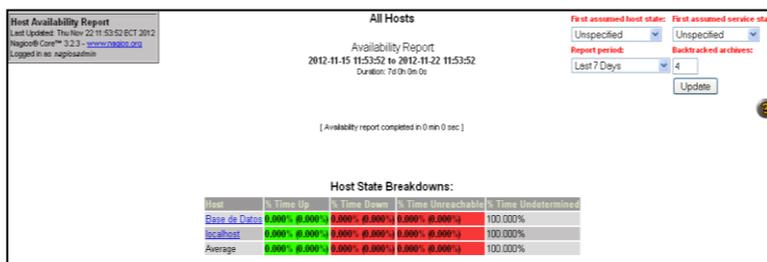


Figura 116. Reporte de disponibilidad del grupo de host

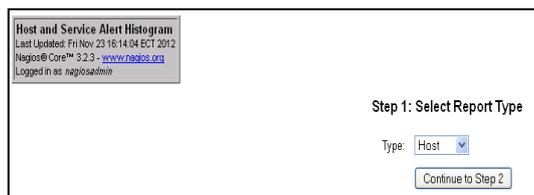
Fuente: Captura de la interfaz web de nagios3

Esta ventana contiene todos los hosts que pertenecen al grupo linux con averías en el estado de host. Para revisar el reporte de un host en particular hacer clic sobre el nombre del host del que se desea revisar la información.

– ALERT HISTOGRAM

Esta opción del menú principal permite crear un registro que muestra la información de las alertas producidas en el transcurso del tiempo tanto en los Host como en los servicios.

Para crear un reporte de este tipo se realizan los siguientes pasos, hacer clic sobre el menú *Alert Histogram*, se abre la ventana que se muestra en la *Figura 117*:



*Figura 117. Paso 1, para crear histogramas de alertas
Fuente: Captura de la interfaz web de nagios3*

En esta ventana se selecciona el tipo de reporte que se desea crear, sea este de un Host o un Servicio, luego se hace clic sobre

Continue to Step 2

En este caso se seleccionará el tipo de reporte *Service*, aparece la ventana que se muestra en la *Figura 118*:



*Figura 118. Paso 2, para crear histogramas de alertas
Fuente: Captura de la interfaz web de nagios3*

En esta ventana se determina el servicio del que se desea crear el reporte. En el campo desplegable se busca el servicio, se hace clic sobre él y se a continuación se presiona en

Continue to Step 3

Se abre la ventana de opciones que se muestra en la *Figura 119* en la que el administrador definirá las opciones con las que desea crear el registro.

Host Alert Histogram
 Last Updated: Fri Nov 23 16:15:20 ECT 2012
 Nagios® Core™ 3.2.3 - www.nagios.org
 Logged in as nagiosadmin

Step 3: Select Report Options

Report Period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Statistics Breakdown:

Events To Graph:

State Types To Graph:

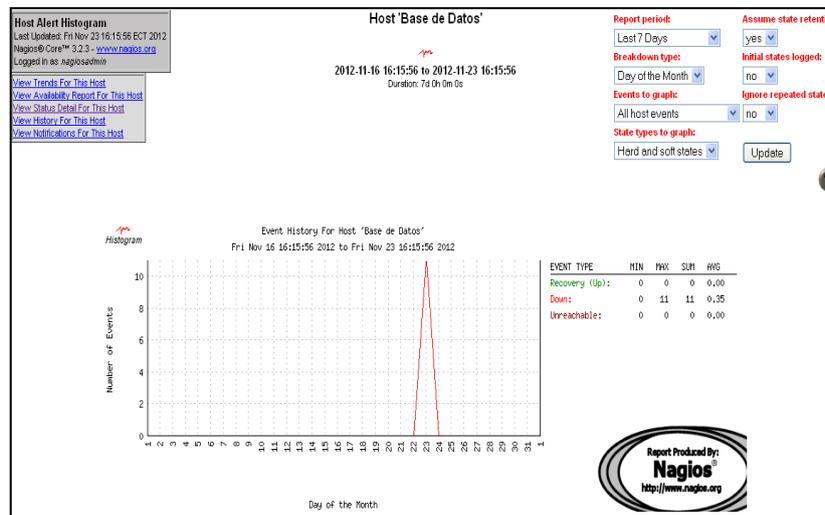
Assume State Retention:

Initial States Logged:

Ignore Repeated States:

*Figura 119. Paso 3, para crear histograma de alertas
 Fuente: Captura de la interfaz web de nagios3*

Una vez establecidas todas las opciones se hace clic sobre , aparece la ventana que se muestra en la *Figura 120*, con un diagrama del número de eventos producidos en función del tiempo seleccionado en las opciones anteriores.



*Figura 120. Histograma de alertas de un host
 Fuente: Captura de la interfaz web de nagios3*

Si se desea crear un reporte del mismo servicio o host con otros parámetros, se modifica las opciones que se encuentran en la parte superior derecha de la ventana y se presiona sobre el botón Update.

– ALERT HISTORY

Esta opción permite revisar todas las alertas tanto de software como de hardware producidas con su respectiva hora y fecha, además indica el nombre del host y servicio en el que sucedió con su respectivo estado (Ok, Critical, Warning, etc.). La ventana se muestra en la *Figura 121*.

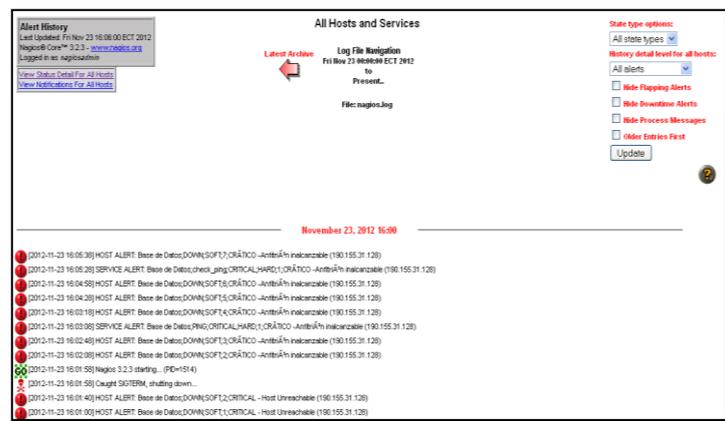


Figura 121. Historial de alertas
Fuente: Captura de la interfaz web de nagios3

Si se desea revisar las alertas especificando el tipo de alerta o el tipo de estado se modifica las opciones que se encuentra en la parte superior derecha de la ventana y se presiona *Update*.

- ~ Las alertas de color verde indican que el host o servicio ya está bien.
- ~ Las alertas de color rojo indican que el host o servicio está en estado crítico.
- ~ Las alertas de color amarillo indican que existe un peligro con el host o servicio.

– ALERT SUMMARY

Esta opción permite crear un reporte con el sumario de alertas producidas de acuerdo al criterio del administrador.

Los reportes pueden ser del tipo estándar o personalizado. Para crear estos tipos de reportes se debe realizar lo siguiente, hacer clic sobre la opción *Alert Summary* que se encuentra en el menú principal, aparece la ventana que se muestra en la *Figura 122*:

*Figura 122. Pantalla principal para el reporte del sumario de alertas
Fuente: Captura de la interfaz web de nagios3*

Esta ventana posee dos secciones:

1. *Standard Reports*:

Esta opción permite crear reportes estándar seleccionando en la pestaña desplegable el tipo de reporte que se desea crear.

En esta opción *Type Report* se puede seleccionar: *25 Most Recent Hard Alerts*, *25 Most Recent Hard Host Alerts*, *25 Most Recent Hard*

Service Alerts, Top 25 Hard Host Alert Producers y Top 25 Hard Service Alert Producers. Hacer clic sobre

Aparece la ventana que se muestra en la *Figura 123*:

Alert Summary Report
Last Updated: Fri Nov 23 16:12:39 ECT 2012
Nagios@Core™ 3.2.3 - www.nagios.org
Logged in as nagiosadmin

Most Recent Alerts
2012-11-16 16:12:39 to 2012-11-23 16:12:39
Duration: 7d 0h 0m 0s

Report Options Summary:
Alert Types: Host & Service Alerts
State Types: Hard States
Host States: Up, Down, Unreachable
Service States: Ok, Warning, Unknown, Critical

Displaying all 10 matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
2012-11-23 16:10:28	Service Alert	Base de Datos	check_ping	CRITICAL	HARD	CRÁTICO - Anfitrión inalcanzable (190.155.31.128)
2012-11-23 16:08:08	Service Alert	Base de Datos	PING	CRITICAL	HARD	CRÁTICO - Anfitrión inalcanzable (190.155.31.128)
2012-11-23 16:07:48	Host Alert	Base de Datos	N/A	DOWN	HARD	CRÁTICO - Anfitrión inalcanzable (190.155.31.128)
2012-11-23 16:05:28	Service Alert	Base de Datos	check_ping	CRITICAL	HARD	CRÁTICO - Anfitrión inalcanzable (190.155.31.128)
2012-11-23 16:03:08	Service Alert	Base de Datos	PING	CRITICAL	HARD	CRÁTICO - Anfitrión inalcanzable (190.155.31.128)
2012-11-22 11:53:11	Service Alert	Base de Datos	check_ssh	CRITICAL	HARD	Conexión rehusada
2012-11-22 11:33:51	Service Alert	Base de Datos	SSH	CRITICAL	HARD	Conexión rehusada
2012-11-22 11:32:51	Service Alert	Base de Datos	HTTP	CRITICAL	HARD	Conexión rehusada
2012-11-20 10:35:27	Service Alert	localhost	SSH	OK	HARD	SSH OK - OpenSSH_5.9p1 Debian-Subuntu1 (protocolo 2.0)
2012-11-19 14:01:31	Service Alert	localhost	SSH	CRITICAL	HARD	Conexión rehusada

Figura 123. Reporte estándar del resumen de alertas
Fuente: Captura de la interfaz web de nagios3

En esta ventana se muestra un listado de host y servicios con las alertas producidas, estado del servicio, hora y fecha. Si se desea revisar los detalles de un host o servicio, hacer clic sobre el enlace con el nombre del host o servicio. Para crear un nuevo reporte se hace clic sobre el botón .

2. Custom Report Options

Esta sección permite personalizar las opciones antes de crear un reporte resumido de alertas.

Una vez establecidas las opciones que se desea incluir en el reporte se hace clic sobre y aparece la ventana que se muestra en la *Figura 124*:

Alert Summary Report
 Last Updated: Fri Nov 23 16:18:00 ECT 2012
 Nagios® Core™ 3.2.3 - www.nagios.org
 Logged in as: nagiosadmin

Most Recent Alerts
 2012-11-16 16:10:00 to 2012-11-23 16:10:00
 Duration: 7d 0h 0m 0s

Report Options Summary:
 Alert Types: Host & Service Alerts
 State Types: Soft & Hard States
 Host States: Up, Down, Unreachable
 Service States: OK, Warning, Unknown, Critical
[Generate New Report](#)

Displaying most recent 25 of 32 total matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
2012-11-23 16:00:08	Service Alert	Base de Datos	CRAC	CRITICAL	HARD	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:07:48	Host Alert	Base de Datos	N/A	DOWN	HARD	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:06:48	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:06:38	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:05:38	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:05:28	Service Alert	Base de Datos	check_nms	CRITICAL	HARD	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:04:58	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:04:28	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:03:18	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:03:08	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:02:48	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:02:08	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
2012-11-23 16:01:48	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÍTICO - Host Unreachable (190.155.31.128)
2012-11-23 16:01:00	Host Alert	Base de Datos	N/A	DOWN	SOFT	CRÍTICO - Host Unreachable (190.155.31.128)
2012-11-22 11:53:11	Service Alert	Base de Datos	check_sst	CRITICAL	HARD	ConexiA'n rechazada
2012-11-22 11:48:11	Service Alert	Base de Datos	check_sst	CRITICAL	SOFT	ConexiA'n rechazada
2012-11-22 11:43:11	Service Alert	Base de Datos	check_sst	CRITICAL	SOFT	ConexiA'n rechazada
2012-11-22 11:38:11	Service Alert	Base de Datos	check_sst	CRITICAL	SOFT	ConexiA'n rechazada

Figura 124. Reporte personalizado del sumario de alertas
 Fuente: Captura de la interfaz web de nagios3

Esta ventana muestra un listado de las alertas producidas de acuerdo a las opciones seleccionadas en las opciones antes detalladas.

Para revisar detalladamente la información de un host o servicio en particular, hacer clic sobre el nombre.

Si se desea crear un nuevo reporte hacer clic sobre [Generate New Report](#)

– NOTIFICATIONS

Esta opción muestra la lista de las más recientes notificaciones producidas. La Figura 125 muestra esta opción.

Contact Notifications
 Last Updated: Fri Nov 23 16:16:44 ECT 2012
 Nagios® Core™ 3.2.3 - www.nagios.org
 Logged in as: nagiosadmin

All Contacts
 Log File Navigation
 Fri Nov 23 16:16:44 ECT 2012
 to Present...
 File: nagios.log

[Latest Archive](#)

Notification detail level for all contacts:
 Order Entries First: [Update](#)

Host	Service	Type	Time	Contact	Notification Command	Information
Base de Datos	N/A	HOST DOWN	2012-11-23 16:07:48	nagiosadmin	notify-host-by-email	CRÁTICO - AntirfA'n inalcanzable (190.155.31.128)
Base de Datos	check_sst	CRITICAL	2012-11-22 11:53:11	nagiosadmin	notify-service-by-email	ConexiA'n rechazada
localhost	SSH	OK	2012-11-20 10:38:27	root	notify-service-by-email	SSH OK - OpenSSH_5.9p1 Debian-Subuntri (protocolo 2.0)
localhost	SSH	CRITICAL	2012-11-19 14:01:31	root	notify-service-by-email	ConexiA'n rechazada

Figura 125. Listado de Notificaciones
 Fuente: Captura de la interfaz web de nagios3

Si se desea revisar notificaciones anteriores hacer clic sobre



Para mostrar notificaciones de acuerdo al nivel de detalle, seleccionar la

Notification detail level for all contacts:

opción en la pestaña desplegable

All notifications

Si se desea revisar los detalles de un host, servicio o contacto, hacer clic sobre el nombre.

– EVENT LOG

Esta opción muestra una lista de todos los logs de eventos producidos, y se encuentran ordenados primero los más recientes y si se desea revisar logs anteriores se navega usando las flechas.

Al hacer clic sobre la opción Alert Logs del menú principal se muestra la ventana:

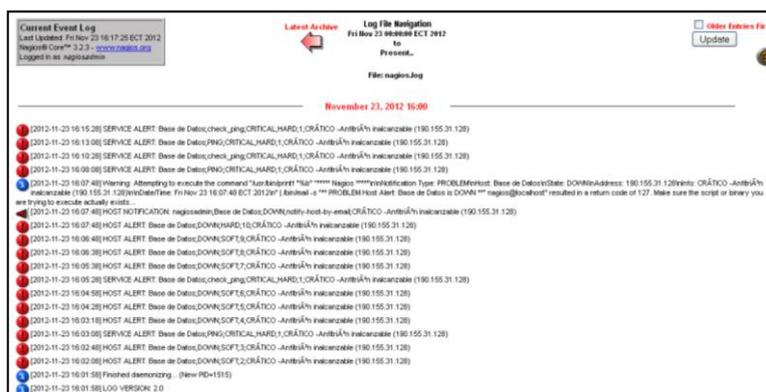


Figura 126. Listado de log de eventos
Fuente: Captura de la interfaz web de nagios3

• CONFIGURATION

Esta sección sólo permite revisar más no modificar o cambiar las configuraciones que se encuentran aplicadas sobre los objetos que se muestran en la pestaña desplegable



Los objetos que se pueden revisar son: *Hosts*, *Host Dependencies*, *Host Escalations*, *Host Groups*, *Services*, *Service Groups*, *Service Dependencies*, *Service Escalations*, *Contacts*, *Contact Groups* y *Timeperiods Commands*.

Las configuraciones que se deseen realizar en Nagios se las debe aplicar por consola en el server.

Para revisar las configuraciones aplicadas se realiza lo siguiente:

Se hace clic sobre la opción *View Config* del menú principal, aparece la ventana de la *Figura 127*:



Figura 127. Selección del objeto para verificar su configuración

En la pestaña desplegable se selecciona el objeto del que se desea revisar la configuración y a continuación hacer clic sobre

Las configuraciones que permite revisar son:

Hosts esta opción se utiliza para definir un servidor físico, estación de trabajo, dispositivo, etc. que pertenece a la red.

Host dependencies son una característica avanzada de Nagios que permiten eliminar las notificaciones de hosts basados en el estado de uno o más hosts. *Los host dependencies* son opcionales y se dirige principalmente a usuarios avanzados que realizan el seguimiento de configuraciones complicadas.

Host Escalations son opcionales y se utilizan para escalar las notificaciones para un host en particular.

Host Groups se utiliza para agrupar a uno o más hosts para simplificar la configuración.

Services se utiliza para identificar un "servicio" que se ejecuta en un host. El término "servicio" se utiliza de manera muy informal. Puede significar un servicio real que se ejecuta en el host (POP, SMTP, HTTP, etc.) o algún otro tipo de métricas asociadas con el host (respuesta a un ping, el número de usuarios registrados, el espacio libre en disco, etc.).

Service Groups se utiliza para agrupar uno o varios servicios, para simplificar la configuración con trucos sobre algún objeto.

Service Dependencies son una característica avanzada de Nagios que permiten eliminar las notificaciones y activar controles de los servicios

basados en el estado de uno o más servicios. *Service Dependencies* son opcionales y se dirige principalmente a usuarios avanzados que realizan el seguimiento de configuraciones complicadas.

Service Escalations son completamente opcionales y se utilizan para escalar las notificaciones para un servicio particular.

Contacts se utiliza para identificar a alguien, quien debe ser contactado en caso de un problema en la red.

Contact Group se utiliza para agrupar a uno o más contactos, con el fin de enviar notificaciones de alerta o recuperación.

Timeperiods Commands es una lista de veces durante varios días que se consideran "válidos" para las notificaciones y controles de servicio. Se trata de rangos de tiempo para cada día de la semana que "rotan" una vez que la semana ha llegado a su fin.

– **COMANDOS EXTERNOS**

○ **HOST COMMANDS**

Los comandos que se pueden aplicar a los host se describen a continuación en la *Tabla 65*:

Tabla 65. Comandos aplicados a los host
Fuente: Ayuda de Nagios

 Locate host on map	Muestra localización del host en el mapa.
 Disable active checks of this host	Desactiva el control activo de un host. Es utilizado para evitar temporalmente que Nagios tenga el control activo de un host en particular.
 Re-schedule the next check of this host	Programa la próxima verificación del host. Nagios volverá a verificar el host en un momento específico.
 Submit passive check result for this host	Presenta el resultado de verificación pasiva para el host.
 Stop accepting passive checks for this host	Deja de aceptar la verificación pasiva del host. Todos los resultados de verificación pasiva que se encuentran para el host serán ignorados.
 Disable notifications for this host	Deshabilita las notificaciones del host. Se deberá volver a habilitar las notificaciones para este host antes de que las alertas puedan enviarse en el futuro. El deshabilitar las notificaciones de este comando no deshabilita los servicios asociados con este host.
 Send custom host notification	Envía notificaciones personalizadas para el host. Útil en situaciones de emergencia cuando es necesario notificar a los administradores de una cuestión relativa a un sistema de control o de servicio.
 Schedule downtime for this host	Programa de inactividad para el host. Durante el tiempo de inactividad especificado, Nagios no enviará notificaciones acerca de este.
 Disable notifications for all services on this host	Desactiva las notificaciones para todos los servicios del host. Esto no impide que las notificaciones sean enviadas a menos que también se deshabilite esta opción.
 Enable notifications for all services on this host	Habilita las notificaciones para todos los servicios del host.
 Schedule a check of all services on this host	Programa la verificación para todos los servicios del host.
 Disable checks of all services on this host	Programa la comprobación de todos los servicios del host. Si selecciona la opción <i>forcé</i> Nagios obligará a verificar el estado de todos los servicios de los host.
 Enable checks of all services on this host	Habilita la verificación de todos los servicios para el host.
 Disable event handler for this host	Deshabilita el control de eventos para el host.
 Disable flap detection for this host	Deshabilita la detección flap para el host.

○ SERVICE COMMANDS

Los comandos que se pueden aplicar a los servicios se describen a continuación en la *Tabla 66*:

Tabla 66. Comandos aplicados a los servicios
Fuente: Ayuda de Nagios

 Disable active checks of this service	Deshabilita la verificación activa de un servicio.
 Re-schedule the next check of this service	Re-programa la próxima verificación de un servicio.
 Start accepting passive checks for this service	Acepta el inicio de la verificación pasiva de un servicio.
 Acknowledge this service problem	Reconocer el problema de este servicio.
 Disable notifications for this service	Deshabilita las notificaciones de este servicio.
 Delay next service notification	Retarda la próxima notificación de servicio.
 Send custom service notification	Envía notificaciones personalizadas del servicio.
 Schedule downtime for this service	Programa de inactividad para este servicio.
 Disable event handler for this service	Deshabilita el control de eventos para el servicio.
 Disable flap detection for this service	Deshabilita la detección flap para el servicio.

○ PROCESS COMMANDS

Los comandos que se pueden aplicar a los procesos se describen a continuación en la *Tabla 67*:

Tabla 67. Comandos aplicados a los procesos
Fuente: Ayuda de Nagios

 Shutdown the Nagios process	Cerrar el proceso de Nagios.
 Restart the Nagios process	Reiniciar el proceso de Nagios.
 Disable notifications	Deshabilitar notificaciones.
 Stop executing service checks	Detener la ejecución de verificación de los servicios.
 Stop accepting passive service checks	Dejar de aceptar la verificación pasiva de servicios.
 Stop executing host checks	Detener la ejecución de verificación de host.
 Stop accepting passive host checks	Dejar de aceptar la verificación pasiva de host.
 Disable event handlers	Deshabilitar el control de eventos.
 Start obsessing over services	Permite el procesamiento de verificación vía comandos OCHP para el servicio especificado.
 Start obsessing over hosts	Permite el procesamiento de verificación vía comandos OCHP para el host especificado.
 Disable flap detection	Deshabilitar la detección flap.
 Enable performance data	Habilitar los datos de rendimiento.

6.4. OCS INVENTORY

La administración y monitoreo de OCS permite realizarla vía Web. Para ingresar a la consola de OCS con el privilegio de Administrador debe realizar lo siguiente:

1. Ingrese a cualquier explorador Web (Internet Explorer, Mozilla Firefox, etc.)
2. En el campo de Dirección ingrese la dirección IP del servidor de monitoreo.
`http://ip-servidor/ocsreports` según sea el caso.
3. Presione Enter

En la *Figura 128* se puede observar la pantalla de autenticación de usuarios que permite ingresar a la consola de OCS Inventory NG. En la parte superior derecha puede seleccionar el idioma, en este caso se seleccionará la bandera que representa el idioma español: . En la pantalla ingresar el nombre de administrador, contraseña y presione *Aceptar*.



Figura 128. Pantalla de ingreso a OCS Inventory NG
Fuente: Captura de la aplicación OCS Inventory

CONSOLA DE ADMINISTRACIÓN DE OCS Inventory NG

Al ingresar a la consola de administración de OCS se muestra la pantalla de la *Figura 129*:



Figura 129. Consola Central de OCS
Fuente: Captura de la aplicación OCS Inventory

La consola de OCS se encuentra estructurada en cuatro partes:

- Los íconos que se encuentran en la parte superior izquierda muestran el menú de usuario, que permiten examinar la información de los equipos inventariados.
- Los íconos de la parte superior derecha muestran el menú de administración que permiten la configuración y administración de las opciones del sistema.
- Bajo los íconos de administración se encuentran las opciones para examinar los equipos inventariados.
- En la parte central de la pantalla de administración se muestra el inventario generado por los agentes.

MENÚ DE USUARIO

Este menú se encuentra en la parte superior izquierda de la pantalla principal de la aplicación y permite: mirar todos los computadores, la distribución de Pc's por etiqueta, ver los grupos creados en la red, todos los programas del equipo y búsquedas por varios criterios, respectivamente. El menú se muestra en la *Figura 130*.

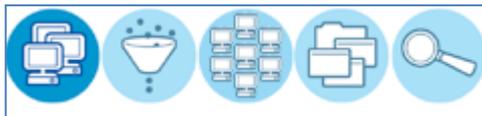


Figura 130. Menú de usuario

Fuente: Captura de la aplicación OCS Inventory

TODOS LOS COMPUTADORES

Al hacer clic sobre el ícono  se presenta al administrador un listado de todos los equipos inventariados con la información de cada uno.

El administrador puede generar un reporte de los equipos inventariados haciendo clic sobre la opción: **241 Resultado** [\(Descargar\)](#)

El archivo que se descarga tiene la extensión .csv y puede visualizarse en cualquier aplicación de hoja de cálculo, base de datos o editores de texto.

El listado de los equipos se lo puede presentar en grupos de 5, 10, 15, 20, 50 y 100 equipos de acuerdo a la necesidad del usuario. Esta opción se selecciona desplegando la pestaña **Mostrar:** .

Esta ventana también permite revisar más información agregando las columnas disponibles en la pestaña: .

Al hacer clic sobre la pantalla principal mostrará la información de los equipos configurada por defecto.

Los parámetros que permite revisar mediante la opción *Adicionar columna* son:

Tabla 68. Revisión de parámetros sobre los Equipos

Fuente: Ayuda de OCS Inventory

Parámetro	Descripción
Agente	Versión del agente OCS instalado
Bdate	Fecha de fabricación del BIOS
CPU (MHz)	Velocidad del Procesador en MHz
Calidad	Valor representativo del tiempo en que un equipo permanece Activo. (Útil para la función IPDiscover)
Computador	Nombre del equipo
Descripción	Descripción definida en el equipo
Dirección IP	Dirección IP de la tarjeta de red
Dominio	Dominio al que pertenece el equipo
Entidad	Organización a la que pertenece el equipo
Fabricante	Nombre del fabricante del equipo
Fabricante del BIOS	Nombre del fabricante del BIOS
Fidelidad	Número total de conexiones al servidor del computador. (Útil para la función IPDiscover)
Lastcome	Fecha y hora del último inventario
Modelo	Modelo de la Mainboard
Nombre usuario	Nombre del usuario que ha iniciado una sesión
Número de CPU	Número de procesadores
Número serial	Número serial
Propietario	Propietario
RAM (MB)	Capacidad de la memoria RAM en MB
Service Pack	Versión del Service Pack instalado
Sistema Operativo	Sistema Operativo del equipo
Swap	Espacio de intercambio del disco duro
Tag	Etiqueta asignada al equipo
Tipo de CPU	Tipo de procesador
User domain	Dominio al que pertenece el usuario
Versión BIOS	Versión del BIOS
Winprodid	Número licencia Windows
Winprodkey	Clave del Sistema Operativo
Último inventario	Fecha y hora del inventario más reciente

ETIQUETA/DISTRIBUCIÓN DE PCs

Al hacer clic sobre el segundo ícono , se muestra la agrupación de PC's según la etiqueta, enlistando las etiquetas existentes como se puede observar en la *Figura 131*:



Figura 131. Ventana de distribución de PCs según Etiqueta
Fuente: Captura de la aplicación OCS Inventory

El administrador puede generar un reporte de los equipos inventariados según el Tag, haciendo clic sobre la opción: **2 Resultado (Descargar)**.

El archivo que se descarga tiene la extensión .csv y puede visualizarse en cualquier aplicación de hoja de cálculo, base de datos o editores de texto.

Si se desea revisar los equipos que pertenecen a una etiqueta en particular, hacer clic sobre el número en la columna.

GRUPOS

Al hacer clic sobre el ícono , se muestra las opciones de los grupos que ha creado, haga clic en los iconos de los grupos. Se puede ver tres pestañas que se muestran en la *Figura 132*:

- Grupos dinámicos: para ver la lista de grupos dinámicos.
- Grupos estáticos: para ver la lista de grupos estáticos.

- Grupos de servidores: para ver la lista de grupos de servidores de la redistribución.

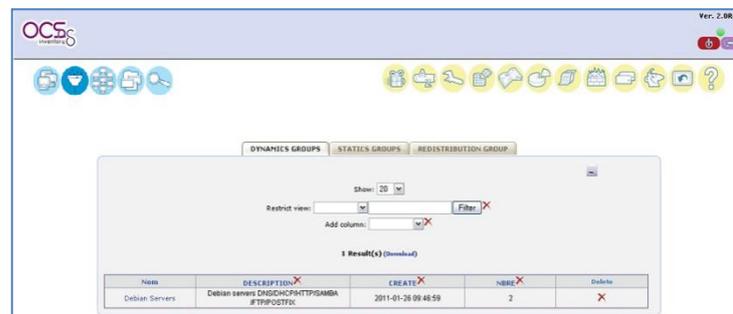


Figura 132. Ventana de distribución por Grupos
Fuente: Captura de la aplicación OCS Inventory

Al hacer clic en un nombre del grupo, se puede ver informaciones diversas sobre el grupo:

- Nombre del grupo
- Fecha
- Consulta (la consulta SQL que corresponde a los parámetros de varios criterios de búsqueda dinámica para grupos)
- Descripción

Puede editar la descripción y el nombre del grupo, haciendo clic en el lápiz como se muestra en la *Figura 133*.



Figura 133. Ventana de descripción de Grupos
Fuente: Captura de la aplicación OCS Inventory

TODOS LOS PROGRAMAS

Al hacer clic sobre el ícono , se muestra datos de todos los programas instalados en la máquina en orden alfabético como muestra la *Figura 134* a continuación:

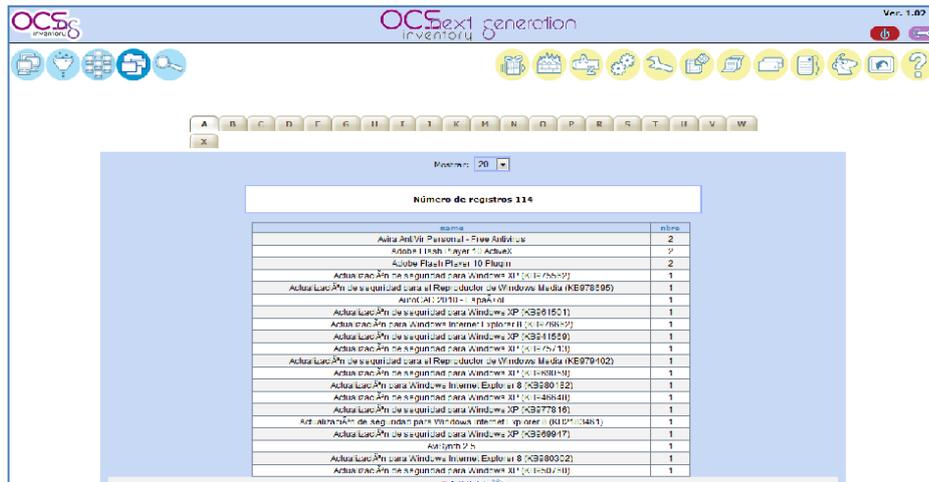


Figura 134. Ventana de descripción Todos los Programas
Fuente: Captura de la aplicación OCS Inventory

BÚSQUEDA POR VARIOS CRITERIOS

Al hacer clic sobre el ícono , se realizan búsquedas específicas según el parámetro deseado. La ventana que se muestra es como la de la *Figura 135*:



Figura 135. Búsqueda por varios criterios
Fuente: Captura de la aplicación OCS Inventory

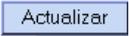
En la pestaña desplegable se selecciona el parámetro de búsqueda, se llena la información correspondiente y se presiona *Buscar*.

Al presionar el botón  se recupera la pantalla inicial.

INFORMACIÓN DE UN AGENTE

Para acceder a la información de un agente, se hace clic en el nombre del computador, el cual se encuentra en letras azules, este vínculo lleva al usuario a una pantalla en la que se presenta la información del agente de manera más detallada.

Esta pantalla presenta la información en cuatro partes:

- La primera permite ver los datos de forma general como: nombre del equipo, dominio al cual pertenece el equipo, fecha y hora del último sondeo de inventario, RAM, memoria virtual, IP de red para cada conexión que tiene creada dicho equipo, que sistema operativo y versión tiene, usuario por el cual inicio el equipo, número y clave de licencia de Windows, etc.
- La segunda parte ofrece una cantidad de íconos que permiten examinar determinado dato del equipo.
- La tercera parte permite editar los datos de etiquetas o de alguna columna adicionada por el administrador. Para editar esta opción hacer clic sobre .
- En la cuarta parte existen dos íconos:
 1.  Imprime los datos de toda la página.

2.  Muestra la información completa del equipo en forma de tablas.

MENÚ DE ADMINISTRADOR

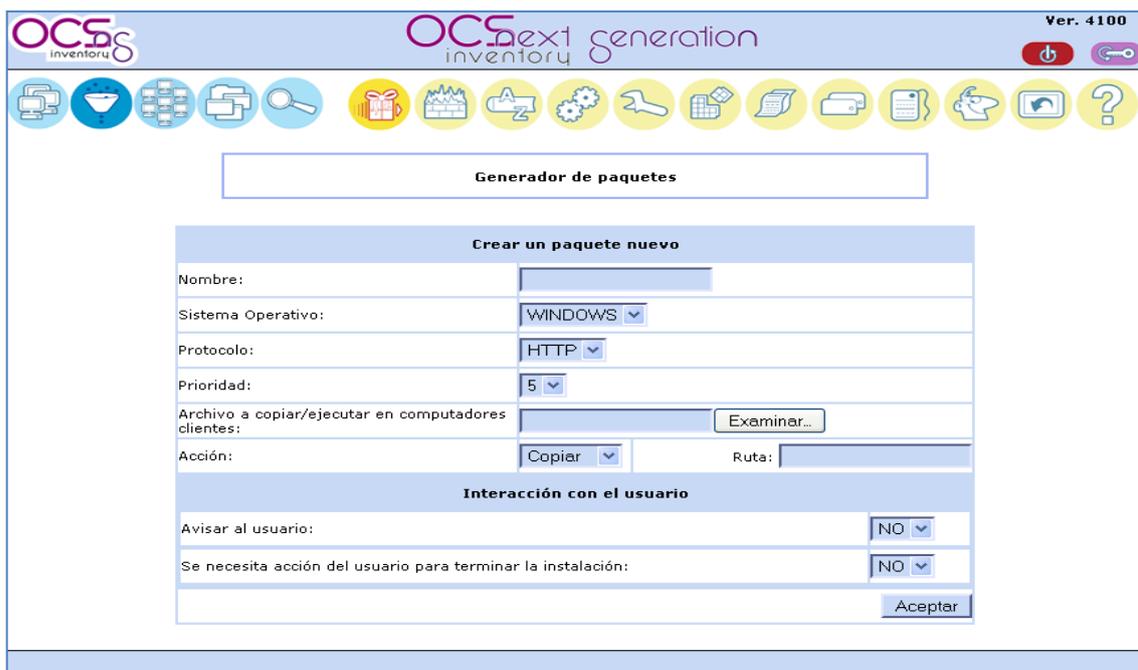
Éste menú brinda todas las opciones de configuración de OCSNG, así como también permite la gestión de usuarios, entre otras opciones que se verán a continuación. La *Figura 136*, muestra las opciones de este menú.



Figura 136. Menú de administrador
Fuente: Captura de la aplicación OCS Inventory

PAQUETES

Esta sección permite crear paquetes, verificar los paquetes por activar y los activados. La ventana se muestra en la *Figura 137*.



Crear un paquete nuevo	
Nombre:	<input type="text"/>
Sistema Operativo:	WINDOWS ▾
Protocolo:	HTTP ▾
Prioridad:	5 ▾
Archivo a copiar/ejecutar en computadores clientes:	<input type="text"/> <input type="button" value="Examinar..."/>
Acción:	Copiar ▾ Ruta: <input type="text"/>
Interacción con el usuario	
Avisar al usuario:	NO ▾
Se necesita acción del usuario para terminar la instalación:	NO ▾
<input type="button" value="Aceptar"/>	

Figura 137. Creación de un paquete
Fuente: Captura de la aplicación OCS Inventory

DESCUBRIR IPs



La característica de descubrimiento de direcciones IP permite a OCS Inventory NG identificar los dispositivos conectados a la red.

Esta opción permite:

- **Ver información de la red:** Se puede mirar la lista de subredes configuradas en su red.
- **Consultas por IP:** Puede escanear consultas de direcciones IP específicas para obtener información sobre un computador. Ingrese la dirección IP y la Máscara y haga clic en “Aceptar” para ejecutar la búsqueda.

- **Configurar:** Esta opción le permitirá configurar:  [Tipo de dispositivos de red](#)  [Nombres de subredes](#)

La opción  [Tipo de dispositivos de red](#) es útil cuando existen elementos de red a los cuales no es posible instalar el agente de OCS, por ejemplo impresoras, escáner, switches, routers, etc. Se crea el tipo de dispositivos de red para inventariar estos equipos y a su vez pertenezcan a un tipo.

La opción  [Nombres de subredes](#) sirve para agregar una subred con los parámetros:

DICCIONARIO



El diccionario de software se utiliza para clasificar el software detectado.

Existen 3 categorías por defecto, como se muestra en la *Figura 138*:

- **NEW:** incluye todo el software nuevo o aún no clasificados.

- IGNORED: Se puede poner en esta categoría todo el software que no desea importar en GLPI.
- UNCHANGED: Se presenta todo el software que este sin cambios.

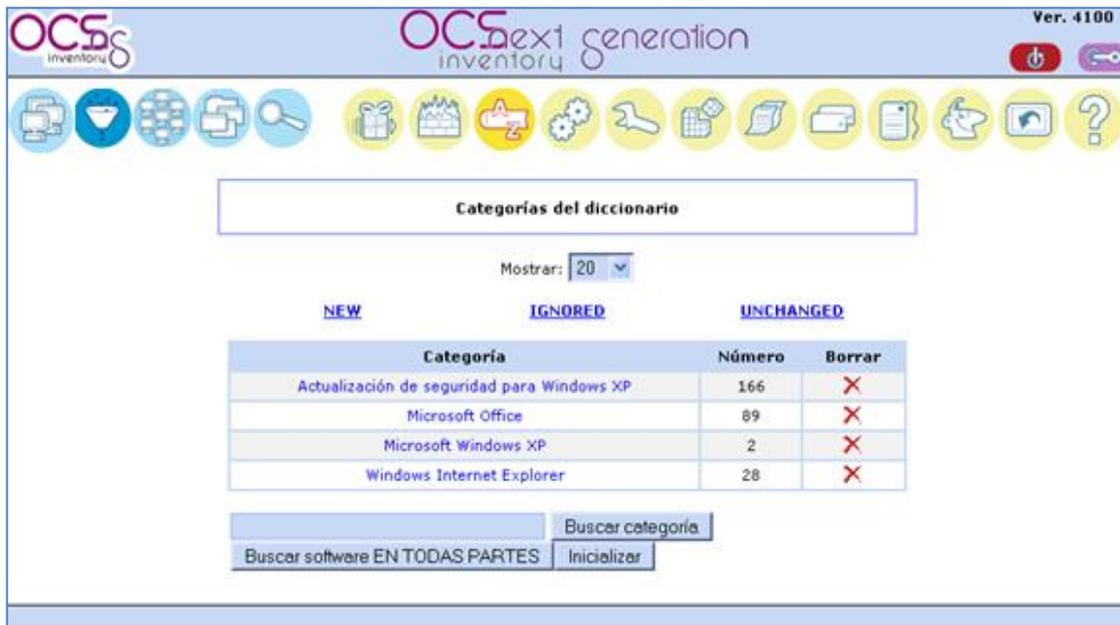


Figura 138. Categorías del Diccionario
Fuente: Captura de la aplicación OCS Inventory

En la parte inferior de la pantalla existe la opción para realizar búsquedas sobre un software en particular o de alguna categoría de software existente.

AGENTE

Permite agregar manualmente un agente a la base de datos del inventario de OCS inventory NG, como se muestra en la *Figura 139*.



*Figura 139. Adicionar un nuevo agente manualmente
Fuente: Captura de la aplicación OCS Inventory*

Para agregar el Agente se debe realizar:

1. Descargar el agente en un directorio
2. Hacer clic en
3. Buscar el archivo en el directorio descargado
4. Hacer clic en

Una vez añadido el agente, aparecerá los detalles en la parte inferior de la pantalla. Si se desea borrar el agente de la base de datos, hacer clic en .

CONFIGURAR

Permite configurar las opciones generales de OCS, como se muestra en la *Figura 140*,



*Figura 140. Menú de configuración
Fuente: Captura de la aplicación OCS Inventory*

REGISTRO

El agente OCS Inventory NG para Windows es capaz de consultar en el registro para los computadores inventariados, un valor de clave o todos los valores de una clave bajo las ramas del registro HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG (y HKEY_DYN_DATA para computadores basados en Windows 9X).



Figura 141. Solicitudes de registro
Fuente: Captura de la aplicación OCS Inventory

Hacer clic en el botón “Adicionar” para agregar una nueva consulta como se muestra en la *Figura 142*. Introducir un nombre para esta consulta, seleccionar la rama del registro (HKEY_LOCAL_MACHINE en este ejemplo), introducir la clave del registro (SOFTWARE\Microsoft\Office\10.0\Registration\{9011040C-6000-11D3-8CFE-0050048383C9}) y el nombre del valor a consultar (Product ID) y confirmar. Colocar una estrella (*) en el campo “Nombre de la clave que se va a leer” para obtener todos los valores de la clave (Esto es útil para obtener todos los

valores de la clave “HKLM\Software\Microsoft\Windows\CurrentVersion\Run” para conocer por ejemplo, que procesos se inician automáticamente).



Figura 142. Solicitudes de Registro
Fuente: Captura de la aplicación OCS Inventory

DATOS ADMINISTRATIVOS

OCS Inventario GN le permite almacenar información personalizada para cada uno de los equipos inventariados.

Esta información administrativa se almacena tanto en el servidor como en el cliente para evitar cualquier pérdida de datos.

Esta ventana se muestra en la *Figura 143*,



Figura 143. Datos administrativos
Fuente: Captura de la aplicación OCS Inventory

REDUNDANCIA



A veces, es imposible para el servidor saber si dos equipos son los mismos o no, esta opción permite elegir el tipo de comparación que se desee en el menú desplegado de la parte superior derecha, como se muestra en la *Figura 144*.

- *Resumen redundancia*: Muestra el número de equipos redundantes detectado con la comparación de cada método.
- *Nombre del computador + Número serial, Nombre del computador + Dirección MAC, Dirección MAC + Números Serial*: Estos son los criterios de los métodos de comparación, la más fiable ya que devuelve todos los equipos que tienen dos criterios en común.
- *Sólo nombre del computador, Sólo serial, Sólo dirección MAC*: Se trata de un criterio de los métodos de comparación, sólo muestra a todos los equipos que comparten un parámetro.

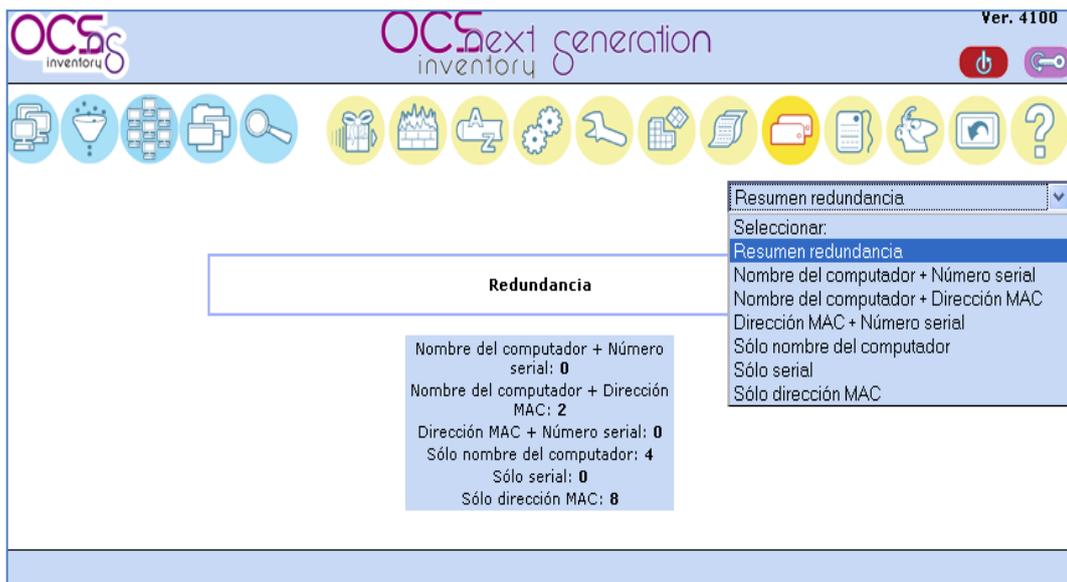


Figura 144. Redundancia

Fuente: Captura de la aplicación OCS Inventory

ARCHIVOS DE CONFIGURACIÓN DE LA ETIQUETA

Esta ventana emergente solicita la "TAG" valor que se utiliza para los equipos de clase. Ésta etiqueta de archivo se genera durante la instalación del servidor, y aquí puede ser editado. La ventana se muestra en la *Figura 145*.



Figura 145. Configuración de la etiqueta
 Fuente: Captura de la aplicación OCS Inventory

El servidor solicita el TAG a los agentes cuando se esté haciendo un inventario de equipos. La ventana que aparece es como la de la *Figura 146*:

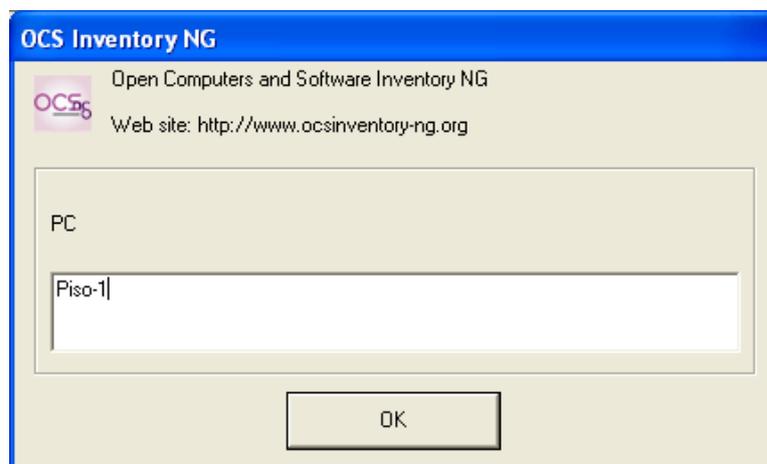


Figura 146. Solicitud de Etiqueta al agente
 Fuente: Captura de la aplicación OCS Inventory

GESTIÓN DE USUARIOS

Muestra todos los usuarios configurados en el servidor de Administración OCS Inventory NG. La *Figura 147*, muestra esta ventana.



Figura 147 Gestión de usuarios
Fuente: Captura de la aplicación OCS Inventory

Puede adicionar nuevos usuarios se introduce el nombre, contraseña (el usuario podrá cambiarla cuando ingrese a la consola), y se selecciona el tipo.

IMPORTAR LOCALMENTE

OCS también permite inventariar equipos que no se encuentren en red. Los inventarios pueden importarse desde un archivo con la extensión **.ocs** a través de cualquier medio de almacenamiento (CD, flash memory, etc.). La *Figura 148*, muestra esta opción.



Figura 148. Importación local
Fuente: Captura de la aplicación OCS Inventory

Para importar el archivo se debe realizar lo siguiente:

1. Hacer clic en .
2. Buscar y seleccionar el archivo con extensión .csv en el medio de almacenamiento.
3. Hacer clic en .

6.5. OTRS

Todos los agentes o administradores deben usar la interfaz web para trabajar con OTRS, ya que estos son los encargados de responder a las solicitudes de los clientes, pueden crear nuevas entradas para los clientes u otros agentes, escribir entradas sobre las llamadas telefónicas con los clientes, escribir entradas de preguntas frecuentes o editar los datos del cliente, etc.

INTERFAZ WEB DE ADMINISTRACIÓN

Los agentes pueden ingresar a la pantalla de acceso mediante la dirección <http://ip-servidor/otrs/index.pl> en un navegador web, como se muestra en la *Figura 149*.

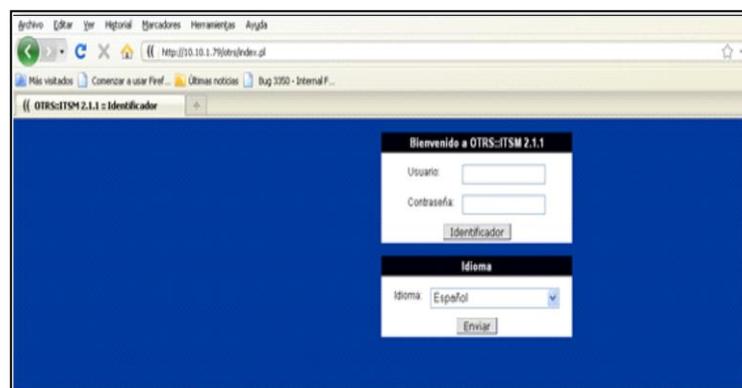


Figura 149. Interfaz web de Agente
Fuente: Captura de la herramienta OTRS

En la ventana que se muestra en la *Figura 150*, ingresar el nombre de usuario y contraseña y presionar el botón *Identificador*.



Bienvenido a OTRS

Nombre de Usuario:

Contraseña:

[Perdió su contraseña](#)

Figura 150. Ventana de ingreso a la aplicación
Fuente: Captura de la herramienta OTRS

INTERFAZ WEB DE CLIENTE

Los clientes disponen de una interfaz web especial en OTRS. A través de esta interfaz web los clientes pueden acceder al Sistema, obtener una visión general sobre los tickets propios, crear y editar entradas, cambiar la configuración de la cuenta, etc.

Los clientes pueden acceder a la pantalla de ingreso mediante la dirección URL <http://ip-servidor/otrs/customer.pl> en un navegador web.

INTERFAZ WEB PÚBLICA

Además de las interfaces web para agentes y clientes el sistema OTRS tiene una interfaz web pública que está disponible a través del módulo FAQ. Esta proporciona un acceso público al sistema de preguntas frecuentes, y le permite al visitante buscar a través de las FAQ sin necesidad de ninguna autorización. La *Figura 151*, muestra el acceso a la interfaz web pública.



Figura 151. Interfaz web pública
Fuente: Captura de la herramienta OTRS

Para acceder a la interfaz web pública en un navegador web escribir la siguiente dirección <http://ipservidor/otrs/faq.pl> o también la dirección <http://ipservidor/otrs/public.pl>.

INGRESO A LA INTERFAZ DE ADMINISTRACIÓN

Como se mencionó anteriormente los agentes pueden ingresar a la pantalla de acceso mediante la dirección <http://ip-servidor/otrs/index.pl> en un navegador web. La ventana principal de la aplicación se muestra en la *Figura 152*.

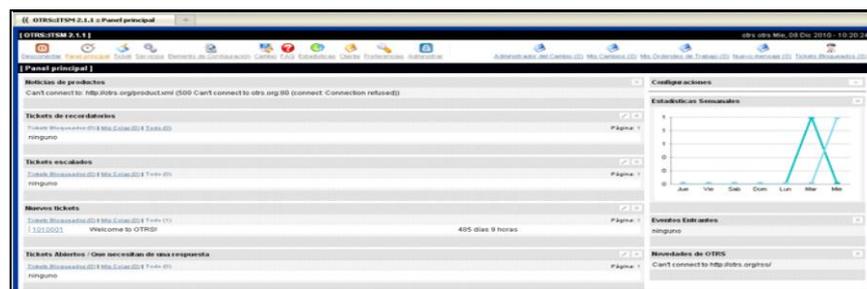


Figura 152. Ventana principal de la aplicación
Fuente: Captura de la herramienta OTRS

Después de que un agente ha ingresado correctamente al sistema OTRS, la interfaz web se carga. Por defecto se visualizará el panel principal después de la entrada, el cual muestra una visión general y rápida sobre los tickets en las

diferentes colas, tickets de recordatorios, nuevos tickets, estadísticas semanales, etc.

Para una mejor comprensión a la interfaz web se la puede dividir en diferentes áreas. En la barra de la parte superior de la ventana se muestra información de carácter general como la hora, fecha, nombre del usuario y la dirección de correo electrónico. También en el lado izquierdo se tiene un enlace que se puede utilizar para recargar la página.

La barra inferior es la barra de navegación. Esta muestra los botones que permiten navegar en las diferentes áreas o módulos del sistema, permitiendo ejecutar algunas acciones globales. La barra de navegación se divide en dos partes. En la zona izquierda se encuentra el botón de cierre de sesión, el botón para activar el Panel Principal, un botón para ver los Tickets, Servicios, Elementos de Configuración, Cambios, el Área de FAQ, Estadísticas, Gestión de Clientes, Preferencias y el Botón de Administración.



En el lugar derecho de la barra de navegación se puede obtener una visión general de cuántas entradas se han bloqueado y los mensajes nuevos que han llegado, el número de órdenes de trabajo, el número de cambio a realizarse, así como también el número de cambios en los cuales el agente es el Administrador.



PANEL PRINCIPAL

El panel principal muestra una vista en general de los tickets del sistema en cada una de sus colas, como tickets escalados, tickets nuevos, tickets abiertos.

Así también en el lado derecho se muestra un cuadro con las estadísticas semanales de los tickets creados. La *Figura 153* muestra el panel principal.

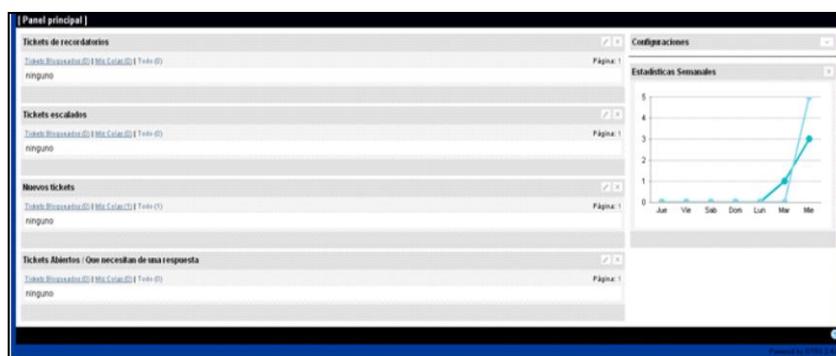


Figura 153. Vista panel principal
Fuente: Captura de la herramienta OTRS

TICKET

En esta ventana se muestran todas las colas definidas en las preferencias del agente, indicando el número de tickets nuevos y abiertos para las respectivas colas, desde esta ventana se tiene acceso a cada una de las colas creadas. Para acceder a un determinado tickets se debe hacer clic sobre el ticket deseado y se mostrará un detalle del mismo.

La barra en negro indica el número del ticket creado junto con su título, además en la parte derecha se muestra la antigüedad que tiene el mismo.

La barra de color gris de abajo en la parte derecha indica la fecha y hora de creación y en la parte izquierda muestra las acciones que se pueden realizar con el ticket seleccionado antes de que este haya sido bloqueado por alguno de los agentes.

[Bloquear](#) - [Detalle](#) - [Historia](#) - [Prioridad](#) - [Nota](#) - [Cerrar](#)

Bloquear

Se debe bloquear un ticket cuando se va a trabajar en él, de esta manera este ticket ya no estará disponible para los demás agentes.

Detalle

Dentro de este link se muestra el detalle de ticket creado, así como el historial del mismo. Además en la parte derecha se muestra la información del ticket y su respectivo estado.

La *Figura 154*, muestra el detalle de un ticket.

Inicio - Bloquear - Historia - Prioridad - Nota - Cerrar		2009/2009 - 02/02 2009/2009 - 02/02	Ticket: incidente Estado: nuevo Códic: Mantenimiento Bloqueado: desbloquear Prioridad: root@localhost (Admin OTRB)	Creado: 2009/2009 - 02/02 20:00:00
1 - 2 - Inicio - Bloquear - Historia - Prioridad - Nota - Cerrar		2009/2009 - 02/02 2009/2009 - 02/02	Tiempo para a Primera Respuesta: 5 horas 37 minutos Tiempo para a Actualización: 2009/2009 - 08:18 5 horas 47 minutos Tiempo para a Solución: 2009/2009 - 08:20 40 horas 27 minutos 21/08/2009 - 19:00	Urgencia: - Impacto: - Prioridad: 3 - normal
De: nancy nancy-nramon@redsoluciones.net Para: Mantenimiento Asunto: nuevo ticket Creado: 2009/2009 - 02/02 20:00:00 nuevo ticket				
		Resultado de Destacar: Fecha de Destacar: Fecha local de reparación: Fecha local de recuperación: Fecha de Verificación: Tiempo contabilizado: 0 IF cBote: nramon@redsoluciones.net		

Figura 154. Vista detalle de un ticket
 Fuente: Captura de la herramienta OTRS

Las opciones que se permiten realizar sobre el ticket son:

Atrás: vuelva a la página anterior

Bloquear: bloquea un tickets para un agente, una vez que un ticket ha sido bloqueado ya no estará disponible para los demás agentes.

Historia: muestra un historial de todo lo realizado con el ticket en cuestión.

Imprimir: imprime el ticket seleccionado en formato pdf.

Prioridad: permite cambiar la prioridad del ticket.

Campos ITSM adicionales: permite incluir campos relacionados a las fechas de reparación, recuperación y el vencimiento de un ticket.

Vincular: permite enlazar un ticket con:

- FAQ
- Cambio
- Ítem de Configuración
- Computador
- Hardware
- Localización
- Redes
- Software
- Orden de Trabajo
- Ticket

Propietario: indica el propietario del ticket, el mismo que puede ser cambiado para otro agente mediante este enlace, con una nota interna.

Cliente: indica los datos del cliente generador del ticket especificado, además de los tickets abiertos por el cliente.

Decisión: permite agregar una nota de decisión la misma que puede tener los siguientes resultados:

- Aprobado
- Pendiente
- Pospuesto
- Pre-aprobado
- Rechazado

Nota: permite agregar una nota al respecto del ticket creada. La misma que puede ser una nota interna o externa.

Mezclar: permite fusionar un ticket con otro.

Pendiente: Permite cambiar el ticket al estado:

- Recordatorio Pendiente
- Pendiente por auto cerrado+
- Pendiente por auto cerrado-

La nota creada puede ser de tipo interno o externo.

Cerrar: Cierra un ticket.

Historia

Muestra un historial de todo lo realizado con el ticket en cuestión.

Prioridad

Permite cambiar la prioridad del ticket, la misma que puede ser:

- 1 muy bajo
- 2 bajo
- 3 normal

- 4 alto
- 5 muy alto

Nota

Permite agregar una nota al respecto del ticket creada. La misma que puede ser una nota interna o externa.

Cerrar

Cierra un ticket con cualquiera de los siguientes estados:

- Cerrado exitosamente
- Cerrado sin éxito
- Cerrado con solución provisional

La nota creada puede ser de tipo interno o externo.

Menús adicionales

Al ingresar al menú ticket se muestran además los siguientes submenús.

Ver cola: muestra los tickets contenidos en la cola

Ticket Telefónico: Permite crear un ticket de las solicitudes telefónicas requeridas por los usuarios.

Ticket de Email: Permite crear un ticket de las solicitudes hechas vía email por los usuarios.

Buscar: Permite buscar los tickets del sistema por diferentes parámetros #Ticket, título, N° cliente, identificador, tipos, Campos de email (de, para, copia, asunto, texto), resultado de decisión, servicios, SLA, prioridad, estados, etc.

SERVICIOS

Lista los servicios creados en el sistema, como se muestra en la *Figura 155*:



Figura 155. Vista ventana de servicios
Fuente: Captura de la herramienta OTRS

Estos servicios se los crea mediante el botón Administración- Servicios.

Submenús

Servicios: Lista los servicios creados en el sistema.

SLA: Lista los acuerdos de nivel de servicio definidos por el área de TI.

ELEMENTO DE CONFIGURACIÓN

Brinda la posibilidad de introducir las características de cada uno de los elementos de configuración por clases.

Clases

- Computer
- Hardware
- Location
- Network
- Software

Submenús

Resumen: Muestra la cantidad de elementos configurados por cada clase.

Nuevo: Brinda la posibilidad de llenar los campos del nuevo elemento a insertar.

Buscar: Permite realizar la búsqueda de un elemento de configuración perteneciente a cualquiera de esas clases descritas.

CAMBIO

Muestra un listado de los cambios que se tienen previstos realizar en el sistema o que se hayan realizado previamente. Contando con la posibilidad de tener un históricos de los cambios realizados

Submenús

Al hacer clic sobre el icono “Cambio” se muestran los siguientes iconos.



Resumen: Muestra un resumen de todos los cambios realizados.

Agenda: Muestra los cambios previos a realizar.

PIR: Revisión post implementación. Una vez que se haya realizado el cambio planificado de ser necesario se realiza una revisión de su implementación, y este cambio se adiciona en este ticket.

Plantilla: Brinda la posibilidad de predeterminedar un cambio mediante una plantilla, para ser usado en posteriores cambios programados.

Buscar: Brinda la posibilidad de buscar algún cambio específico.

Nuevo: Permite crear un nuevo cambio a realizar.

FAQ

Este icono brinda la posibilidad de reflejar y publicar a usuarios y clientes las preguntas que con más frecuencia se realizan, aportando a la base de datos de conocimientos básicos. La *Figura 156*, muestra esta ventana

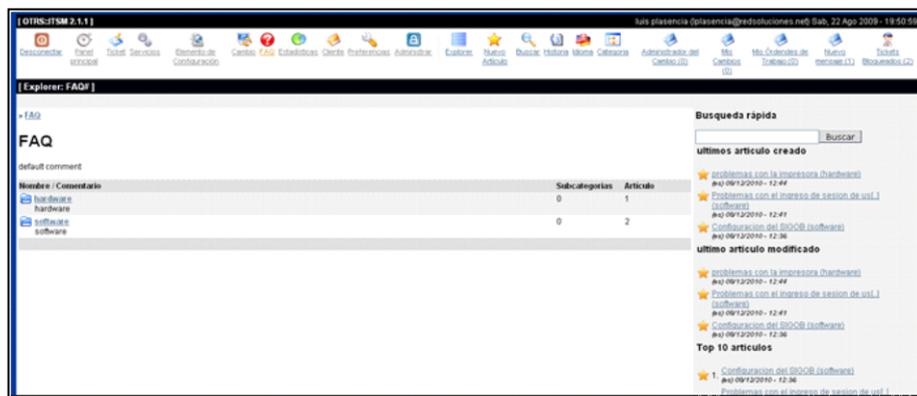


Figura 156. Vista de la ventana de FAQ
Fuente: Captura de la herramienta OTRS

Esta base de conocimientos se aporta con los nuevos artículos que los administradores vayan añadiendo.

Submenús

Explorer: muestra un listado de todos los FAQ creados en el sistema. Los FAQ creados pueden ser de diferentes tipos dependiendo de su uso.

- **Internos:** pueden ser vistos solo por los agentes del sistema.
- **Externos:** pueden ser vistos para todos los usuarios registrados en el sistema

- **Públicos:** para ver estos FAQ no es necesario que se acceda con un determinado usuario, ya que se ingresa por medio de la interfaz web pública.

Nuevo artículo: permite crear un nuevo FAQ en el sistema, dentro de la categoría seleccionada.

Buscar: permite buscar algún artículo en especial.

Historia: muestra un historial de los FAQ creados.

Idioma: permite crear nuevos idiomas para la creación de los FAQ.

Categoría: permite crear nuevas categorías, mediante las cuales se puede tener una mejora administración de los FAQ.

ESTADISTICAS

Mediante este enlace se tienen diferentes tipos de estadísticas predefinidas por el sistema en base a diferentes parámetros, las mismas que pueden ser editadas en base a los requerimientos del administrador.

La *Figura 157*, muestra la ventana de estadísticas.

State	Título	Objeto	Descripción
10001	List of the most time-consuming tickets	Lista de tickets	List of tickets closed last month which required E[]
10002	List of open tickets, sorted by time left until escalation deadline expires	Lista de tickets	List of open tickets, sorted by time left until esc[]
10003	List of tickets closed, sorted by solution time	Lista de tickets	List of tickets closed last month, sorted by solut[]
10004	New Tickets	AcumulacionDeTickets	Total number of new tickets per day and queue whic[]
10005	List of open tickets, sorted by time left until solution deadline expires	Lista de tickets	List of open tickets, sorted by time left until sol[]
10006	List of tickets closed last month	Lista de tickets	List of all tickets closed last month. Order by ag[]
10007	Changes of status in a monthly overview		Monthly overview, which reports status changes per[]
10008	List of tickets closed, sorted by response time.	Lista de tickets	List of tickets closed last month, sorted by respo[]
10009	List of open tickets, sorted by time left until response deadline expires	Lista de tickets	List of open tickets, sorted by time left until re[]
10010	List of tickets created last month	Lista de tickets	List of all tickets created last month. Order by a[]
10011	Overview about all tickets in the system	AcumulacionDeTickets	Current state of all tickets in the system withou[]
10012	Total number of all tickets ever created per Ticket-Type and Priority.	AcumulacionDeTickets	Total number of all tickets ever created per Ticke[]
10013	Total number of all tickets ever created per Ticket-Type and State.	AcumulacionDeTickets	Total number of all tickets ever created per Ticke[]
10014	Total number of all tickets ever created per Ticket-Type and Queue.	AcumulacionDeTickets	Total number of all tickets ever created per Ticke[]
10015	Total number of all tickets ever created per Ticket-Type and Service.	AcumulacionDeTickets	Total number of all tickets ever created per Ticke[]
10016	Monthly overview of all tickets created in the last month per Ticket-Type.	AcumulacionDeTickets	Monthly overview of all tickets created in the las[]
10017	Monthly overview of all tickets created in the last month per Priority.	AcumulacionDeTickets	Monthly overview of all tickets created in the las[]
10018	Monthly overview of all tickets created in the last month per State.	AcumulacionDeTickets	Monthly overview of all tickets created in the las[]
10019	Monthly overview of all tickets created in the last month per Queue.	AcumulacionDeTickets	Monthly overview of all tickets created in the las[]

Figura 157. Vista de la ventana de estadísticas
Fuente: Captura de la herramienta OTRS

Submenús

Resumen: muestra un listado de las estadísticas predefinidas por el sistema.

Nuevo: permite crear nuevas estadísticas en función de las necesidades de los administradores.

Importar: permite importar estadísticas para ser cargados en el sistema.

PREFERENCIAS

Permite definir las preferencias de la interfaz del administrador en el mismo en que se pueden definir diferentes parámetros en base a la interfaz de usuario, gestión de correo y otras opciones como la vista de colas, el horario fuera de oficina, entre otras.

Estas preferencias deben ser definidas por cada Agente.

La *Figura 158*, muestra la ventana de preferencias.

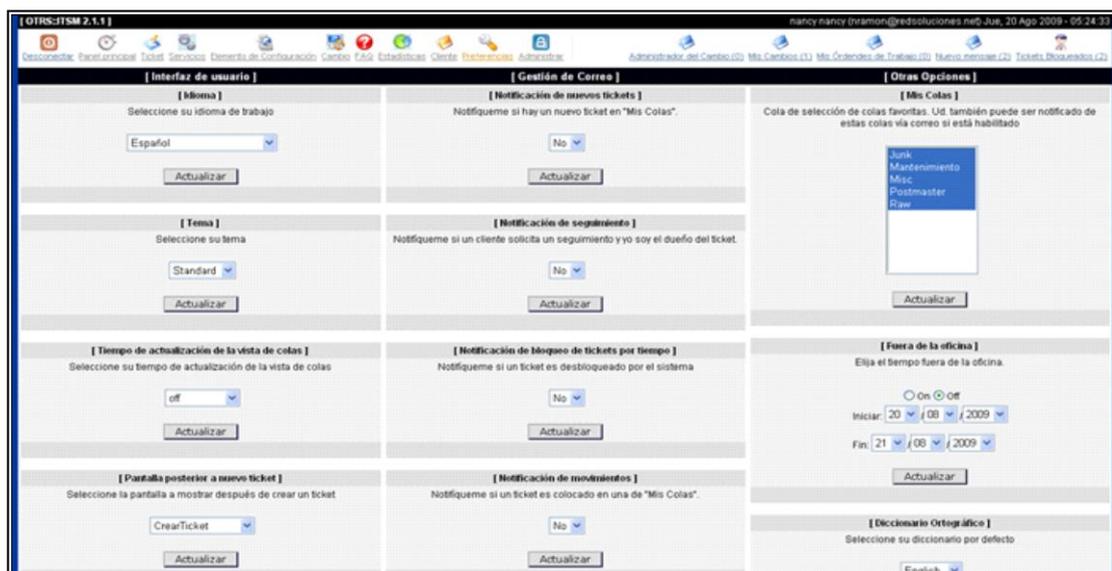


Figura 158. Vista de la ventana de preferencias
Fuente: Captura de la herramienta OTRS

ADMINISTRAR

Mediante este botón se administra toda la herramienta dentro de las cuales se tiene.

Usuarios

Por defecto los usuarios miembros de este grupo tienen todos los privilegios de Administración.

Grupos

Cada cuenta de usuario creada pertenece a un grupo o rol.

Después de la instalación del OTRS tres grupos predefinidos están disponibles.

Los grupos determinados para la administración se muestran en la *Tabla 69*:

Tabla 69. Grupos predeterminados de administración de OTRS

Fuente: Ayuda de OTRS

Grupos	Descripción
admin .	Grupo al que pertenecen los usuarios que deben realizar tareas administrativas en el sistema.
stats .	Los usuarios de este grupo pueden acceder a las estadísticas del módulo de OTRS y generarlas.
Users.	Este es el grupo donde los agentes deben pertenecer, los cuales deben tener permiso de lectura y escritura. Los usuarios que están en este grupo y posean permiso de escritura podrán además utilizar todas las funciones del sistema de tickets.

Una visión general de todos los grupos y usuarios en el sistema se muestra en la parte inferior de la pantalla.

Los usuarios pueden tener diferentes derechos en un grupo. A continuación, la *Tabla 70* muestra una lista de los permisos disponibles:

Tabla 70. Permisos disponibles para usuarios de OTRS
Fuente: Ayuda de OTRS

Permisos	Descripción
ro	Acceso de solo lectura a los Tickets y mensajes que entre a las colas de este grupo
move into	Derecho de mover los tickets o mensajes que entren a las colas que pertenecen a este grupo.
create	Derecho de crear los tickets o mensajes en las colas que pertenecen a este grupo.
owner	Derecho de actualización del propietario del ticket o mensaje en las colas que pertenecen a este grupo.
priority	Derecho de cambiar la prioridad del ticket o mensaje en las colas que pertenecen a este grupo.
rw	Derecho de lectura y escritura de los tickets o mensajes en las colas que pertenecen a este grupo.

Su administración se la realiza en el archivo de configuración de la herramienta, `/opt/otrs/Kernel/Config.pm`

Roles

Los roles son una característica muy eficaz y útil para gestionar y modificar los derechos de acceso de usuarios de una manera muy simple y rápida, sin embargo no es aconsejable utilizar los roles una vez que se utilicen grupos de usuario ya que su administración se dificulta y pueden darse varios errores en su utilización.

Clientes

Los clientes son todos aquellos que acceden a la interfaz web de clientes

por medio de <http://ip-servidor/otrs/customer.pl>. Esta interfaz de usuario cliente le permite acceder a sus propios tickets.

Para crear un nueva cuenta de usuario cliente se debe crearlo en el controlador de dominio institucional y agregar el atributo mail, como se indicó anteriormente.

Grupos de Clientes

Los clientes también se pueden añadir a un grupo. Esta característica puede ser útil, si desea agregar algunos clientes de la misma empresa que sólo tendrán acceso a una o a varias colas.

Las Colas

Una cola en OTRS es de alguna manera comparable a un archivo de bandeja de entrada del correo, pero con algunas características más, estos pueden almacenar una serie de mensajes pero con la diferencia que los del correo se guardaran de otra manera.

Saludos, firmas, anexos y respuestas.

Para acelerar la respuesta a los tickets y normalizar el aspecto de las mismas es posible definir respuestas en OTRS. Una respuesta puede ser vinculada a una o más colas y una cola se puede vincular a una o varias respuestas. Las diferentes respuestas se muestran debajo de cada ticket en el Queue View o en "Mi colas".

Saludos

El saludo es un módulo de texto en la respuesta. El saludo puede ser

vinculado a una o más colas como se describe en la sección acerca de las colas. Sólo si un saludo está vinculado a una cola este es usado si el ticket que pertenece a esa cola es respondido. Con el vínculo "Saludos" se permite gestionar los diferentes saludos del sistema.

Firmas

Otro módulo de texto de una respuesta es la firma. Sólo si una firma está vinculada a una cola esta se incluirá en el texto de respuesta. A través del vínculo "firmas" se puede administrar las firmas en el sistema.

Adjuntos

Otro elemento opcional en una respuesta puede ser incluir uno o más archivos adjuntos. El archivo adjunto se enviará si es utilizado en la respuesta, pero a través de las casillas de verificación es posible desactivar el archivo adjunto en la pantalla de respuesta de los tickets.

Respuestas Automáticas

OTRS está diseñado para poder enviar respuestas a los usuarios clientes. Las respuestas automáticas se envían si ocurren eventos importantes tales como por ejemplo, si un ticket es creado en una cola, si se recibe un seguimiento para un ticket, si un ticket es cerrado o rechazado por el sistema, etc. A través del enlace "Auto respuestas" las auto respuestas del sistema pueden ser administradas. Cuando se crea una respuesta automática se puede seleccionar posteriormente el evento que debe conllevar dicha respuesta.

Direcciones de Correos

Para habilitar OTRS para enviar mensajes necesita al menos una dirección válida de correo electrónico para ser utilizada por el sistema. Debido a que muchas configuraciones necesitan más de una dirección de correo OTRS es capaz de trabajar con muchas direcciones de correo electrónico al mismo tiempo.

Notificaciones

A través del link preferencias los agentes y clientes pueden seleccionar los eventos del sistema para los cuales desean ser notificados.

A través del vínculo "notificación" en el área del administrador se podrá gestionar las notificaciones del sistema.

SMIME

OTRS puede procesar mensajes de entrada codificados con SMIME como también brinda la posibilidad de firmar los correos salientes. Antes de que esta característica se pueda utilizar, se necesita activar y cambiar algunos parámetros de configuración en el sysconfig.

El vínculo SMIME en el área de administración de OTRS le permite gestionar los certificados SMIME.

PGP

Usted puede utilizar OTRS para descifrar y cifrar mensajes con PGP. Además, puede firmar los mensajes salientes. Antes de utilizar esta

característica necesita activar la y cambiar algunos parámetros de configuración en el SysConfig.

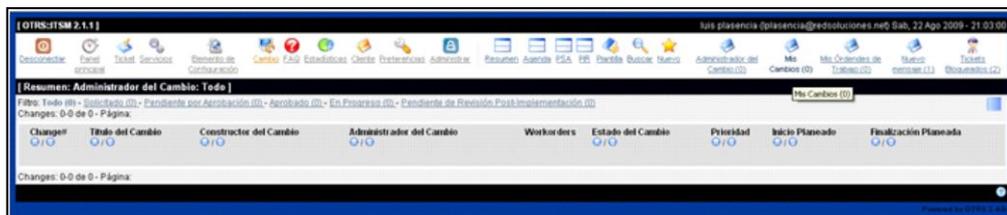
ADMINISTRADOR DE CAMBIOS

Por medio de este enlace se pueden verificar los cambios en los cuales se tiene a cargo la administración de un cambio y verificar el estado en que este se encuentra.

Los estados pueden ser:

- Solicitado
- Pendiente por aprobación
- Aprobado
- En progreso
- Pendiente de Revisión Post-Implementación.

La *Figura 159*, muestra la ventana de Administrador de cambios.



*Figura 159. Vista del Administrador de cambios
Fuente: Captura de la herramienta OTRS*

Submenús

Al hacer clic sobre el icono “Administrador de Cambios” se muestran los

siguientes iconos.

Resumen: Muestra un resumen de todos los cambios realizados.

Agenda: Muestra los cambios previos a realizar.

PIR: Revisión post implementación. Una vez que se haya realizado el cambio planificado de ser necesario se realiza una revisión de su implementación, y este cambio se adiciona en este ticket.

Plantilla: Brinda la posibilidad de predeterminar un cambio mediante una plantilla, para ser usado en posteriores cambios programados.

Buscar: Brinda la posibilidad de buscar algún cambio específico.

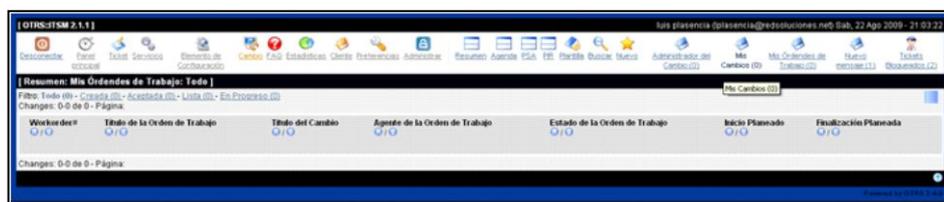
Nuevo: Permite crear un nuevo cambio a realizar.

MIS CAMBIOS

En esta ventana se muestran los cambios planificados por los agentes, estos cambios pueden estar en base a los siguientes estados:

- Creada
- Aceptada
- Lista
- En progreso

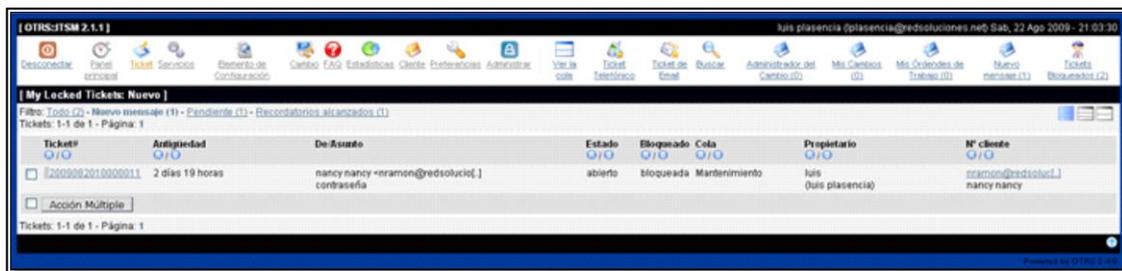
La *Figura 160*, muestra la ventana de la opción mis cambios.



*Figura 160. Vista de la ventana de mis cambios
Fuente: Captura de la herramienta OTRS*

MIS ÓRDENES DE TRABAJO

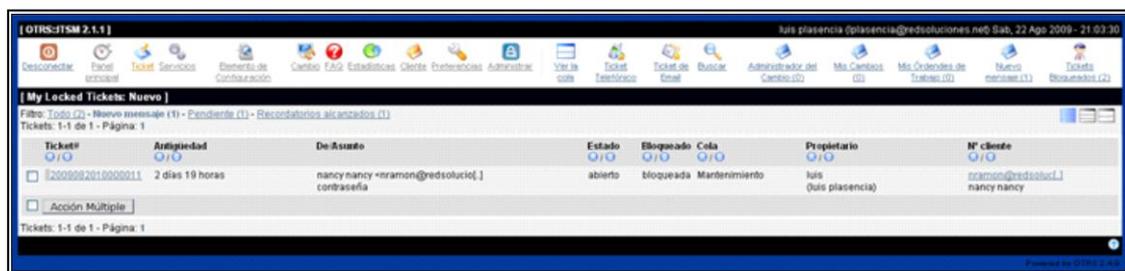
Dentro de un cambio se puede crear varias órdenes de trabajo, las mismas que deben ser realizadas para dar por terminada una tarea, cada una de las cuales tiene una persona ejecutora del cambio. Dentro de este vínculo se pueden verificar las ordenes de trabajo que el agente tiene a su cargo. La *Figura 161*, muestra la ventana de la opción Mis órdenes de trabajo.



*Figura 161. Vista de la ventana mis órdenes de trabajo
Fuente: Captura de la herramienta OTRS*

NUEVO MENSAJE

En este enlace se pueden verificar los nuevos mensajes que han llegado al sistema. La *Figura 162*, muestra la ventana de esta opción.



*Figura 162. Vista de la ventana del menú nuevo mensaje
Fuente: Captura de la herramienta OTRS*

TICKETS BLOQUEADOS

En este enlace se muestran los tickets que se encuentran bloqueados por el agente, y que aún no han sido cerrados. La *Figura 163*, muestra la ventana de este menú.

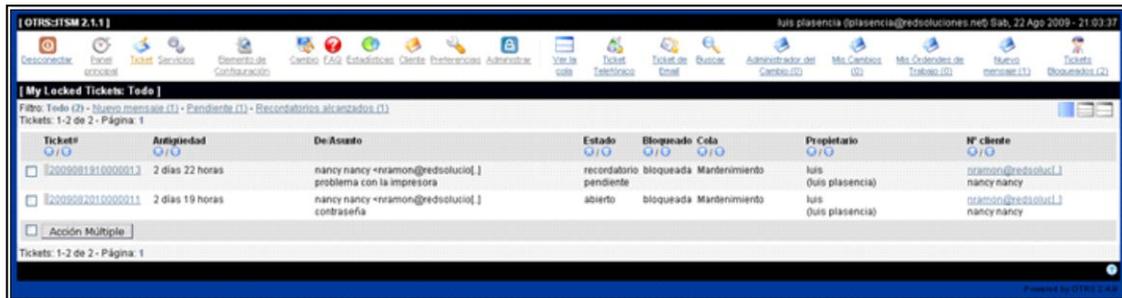


Figura 163. Vista de la ventana del menú Tickets bloqueados
Fuente: Captura de la herramienta OTRS

6.6. SERVIDOR DE ARCHIVOS CON SAMBA 3

Para que un usuario pueda autenticarse en samba, lo primero es crear al usuario ingresando en la consola la siguiente línea de código:

```
adduser -a pdiaz
```

El siguiente paso es asignarle la contraseña al usuario nuevo de la siguiente manera:

```
smbpasswd -a pdiaz
```

De esta manera el nuevo usuario ya puede autenticarse con su clave en el servidor.

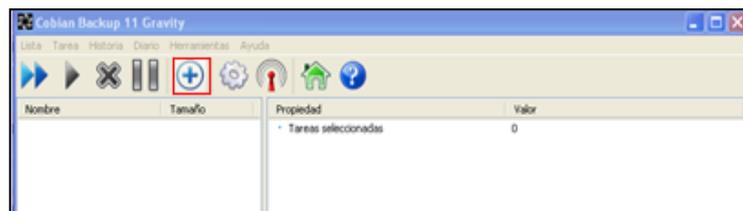
6.7. COBIAN

Para empezar a utilizar la aplicación, hacer doble clic en el icono de Cobian .

Creación de copias de seguridad

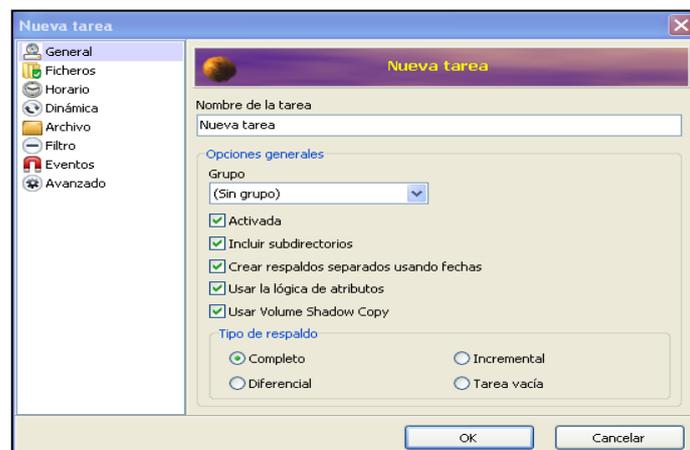
En esta sección se indica la forma de usar el programa para crear una tarea de respaldo.

Lo primero que se debe hacer es crear una copia de seguridad. Para ello, en la ventana que se muestra en la *Figura 164*, presionar el botón *Crear una tarea nueva*.



*Figura 164. Crear tarea de respaldo.
Fuente: Captura de ventana*

Aparece la ventana que se muestra en la *Figura 165*.



*Figura 165. Opción Nueva Tarea
Fuente: Captura de ventana*

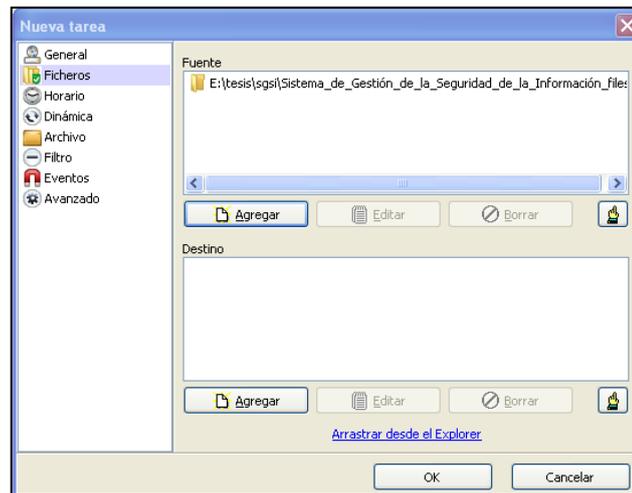
Escribir el nombre de la tarea y seleccionar el tipo de copia de seguridad (completa, incremental o diferencial). Cuando se haya seleccionado una opción hacer clic en *OK*.

Es importante conocer que existen distintos métodos para realizar copias de seguridad: completa, diferencial e incremental.

- **Copia de seguridad completa:** Como su nombre indica, se copiarán todos los ficheros y carpetas que se indique. El tamaño que ocupará la copia de seguridad será el mismo que el que ocupen los datos a respaldar. La primera copia de seguridad a realizar deberá ser siempre de este tipo.
- **Copia de seguridad diferencial:** Se copiarán los ficheros que hayan cambiado desde la última copia de seguridad completa que se realizó. Si un fichero cambia después de una copia de seguridad completa, éste se copiará de nuevo en todas las copias de seguridad diferenciales que se realicen.
- **Copia de seguridad incremental:** Solamente se copiarán los ficheros que hayan cambiado entre el momento en el que se realizó la última copia de seguridad (ya sea ésta completa o incremental) y el momento en el que se realice la copia incremental.

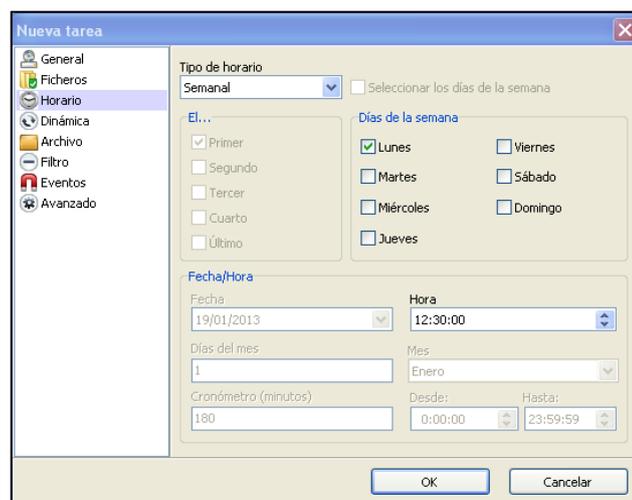
El siguiente paso es seleccionar los ficheros y/o carpetas de los que se va a realizar la copia de seguridad, hacer clic en el botón *Agregar*. La *Figura 166*, muestra esta ventana.

En la parte inferior de la ventana denominada Destino el usuario puede escoger la ubicación donde se guardarán los archivos, ya sea en el mismo disco duro, una dirección de red o ambas, hacer clic en el botón *Agregar*.



*Figura 166. Selección de archivos a respaldar.
Fuente: Captura de ventana*

La opción *Horario* determina cuando se realizará el respaldo. Se puede establecer la periodicidad (diaria, semanal, etc.), los días de la semana, la fecha y la hora de la copia de seguridad. Esta ventana se muestra en la *Figura 167*.



*Figura 167. Selección del horario del respaldo.
Fuente: Captura de ventana*

La opción *Dinámica*, permite seleccionar el nivel de prioridad y el número de copias que se desea realizar. La *Figura 168*, muestra esta ventana.

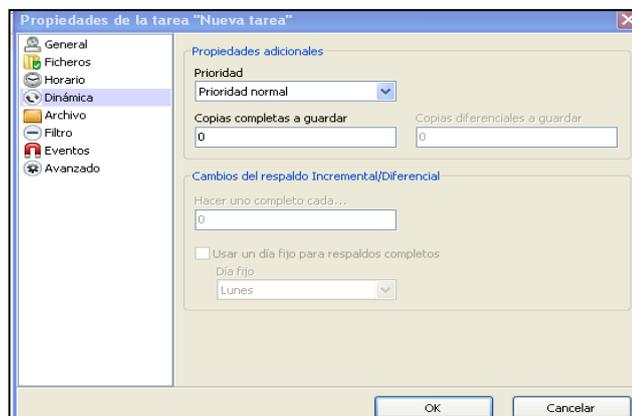


Figura 168. Selección de la prioridad del respaldo
Fuente: Captura de ventana

La opción *Archivo* está destinada para establecer las acciones que se van a realizar sobre los archivos de respaldo es decir cómo serán afectados al momento de almacenarse. En la *Figura 169*, se muestra esta ventana.

En la sección *Compression* se puede seleccionar la opción para comprimir la copia de seguridad en un archivo zip (opción recomendable), así como dividir el fichero comprimido en otros de menor tamaño, protegerlo con contraseña, e incluir un pequeño comentario de referencia.

En la sección *Cifrado fuerte* se puede escoger si se desea cifrar la copia de seguridad (comprimido o no) con algoritmos de cifrado avanzados como son:

- AES (256-bits)
- AES (192-bits)
- AES (128-bits)

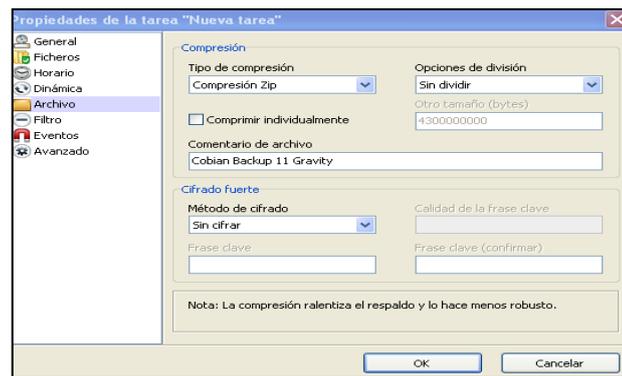


Figura 169. Opciones de compresión, clave de seguridad y encriptación.
Fuente: Captura de ventana

En la opción *Filtro* si se puede excluir ciertos archivos que no necesitan ser respaldados.

Las opciones *Eventos* y *Avanzado* incluyen la posibilidad de ejecutar programas antes y después de la copia de seguridad, por ejemplo, si antes del respaldo el usuario desea que se cierre una aplicación y después del respaldo abrir otra.

Finalmente pulsar el botón OK y se tendrá creada la tarea de copia de seguridad con Cobian Backup 11. Aparecerá una ventana indicando los detalles de la nueva tarea.

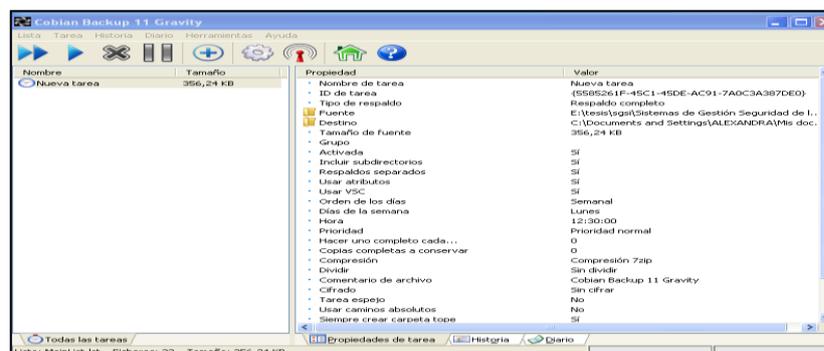
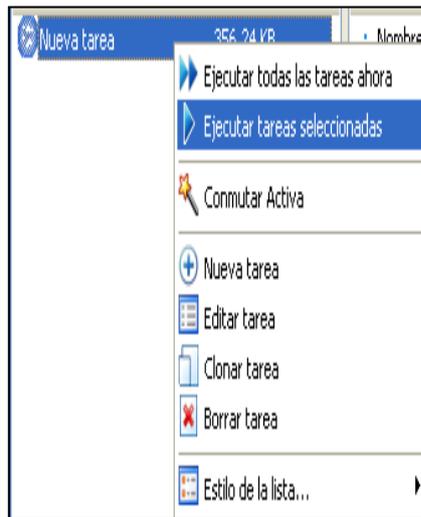


Figura 170. Detalles de la nueva tarea creada.
Fuente: Captura de ventana

Una vez creada la tarea de copia de seguridad se la debe poner en funcionamiento y para ello, pulsar sobre el ícono de la tarea con el botón derecho y seleccionar la opción *Ejecutar tareas seleccionadas*:



*Figura 171. Ejecutar la tareas de respaldo.
Fuente: Captura de ventana*

Inmediatamente se inicia la copia de los archivos y para cerciorarse que el respaldo se ha realizado correctamente, se debe ubicar la siguiente línea *Respaldo terminado para la tarea*.

```

2013-01-19 20:50 Comprimiendo al archivo "C:\Documents and Settings\Al
2013-01-19 20:50 Cambiando el objeto de historia a Aparcado. Causa: p
2013-01-19 20:50 Tiempo total de respaldo para "Nueva tarea": 0 horas,
2013-01-19 20:50 ** Respaldo terminado para la tarea "Nueva tarea". En
2013-01-19 20:50 --
2013-01-19 20:50 El sistema puede ahora entrar en modo de suspensión
2013-01-19 20:50 Tiempo total de backup: 0 horas, 0 minutos, 18 segund
2013-01-19 20:50 *** Respaldo terminado. Errores: 1. Ficheros procesa
2013-01-19 20:50 --

```

*Figura 172. Respaldo exitoso de los archivos.
Fuente: Captura de ventana*

6.8. TRUE CRYPT

Para empezar a utilizar esta herramienta, abrir la aplicación y la pantalla principal que se muestra es como la de la *Figura 173*:

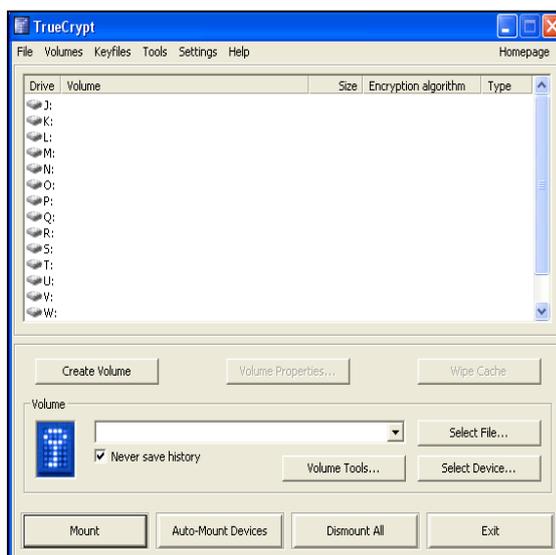


Figura 173. Pantalla de Truecrypt
Fuente: Captura de pantalla de la aplicación Truecrypt

TRADUCCIÓN DEL IDIOMA

Para traducir TrueCrypt al español escoger las siguientes opciones:

- Settings
- Language
- Download Language Pack

Aquí se debe descargar el fichero zip de idioma español y descomprimirlo en la misma carpeta donde se instaló TrueCrypt. Posteriormente reiniciar TrueCrypt y volver a: Settings, Language y escoger Español como se muestra en la *Figura 174*:

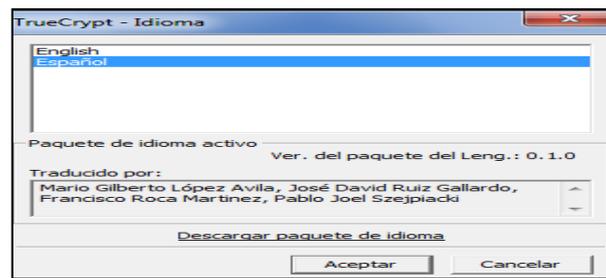


Figura 174. Selección del idioma de la aplicación
Fuente: Captura de pantalla de la aplicación Truecrypt

CREACIÓN DE UN NUEVO VOLUMEN

Para crear un nuevo volumen hacer clic sobre la opción Crear Volumen, como se muestra en la Figura 175:

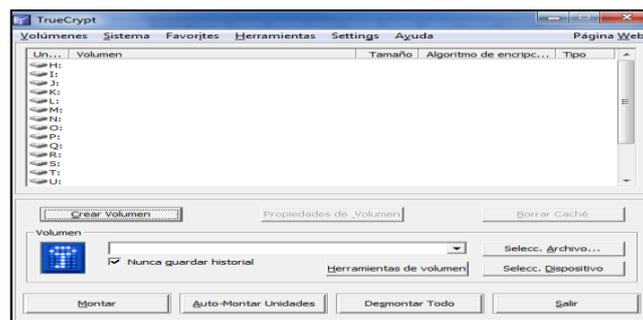


Figura 175. Ventana de creación de volúmenes
Fuente: Captura de pantalla de la aplicación Truecrypt

Aparece el Asistente para la Creación de Volumen como se muestra en la ventana de la Figura 176:



Figura 176. Pantalla del Asistente para la creación de Volumen TrueCrypt
Fuente: Captura de pantalla de la aplicación Truecrypt

Aquí aparecen tres opciones:

1. *Create and Encrypted file container*: Permite crear un contenedor dentro del cual se almacenan los archivos y cuando se monte dicho baúl es decir se quiera mirar lo que hay dentro se montará como disco duro virtual.
2. *Encrypt a non-system partition/Drive*: Esta opción encripta una partición o un disco duro externo.
3. *Encriptar la partición del sistema o la unidad system*: Esto cifra la partición del sistema actual, normalmente el disco C

Seleccionar una de las opciones anteriores y pulsar *Siguiente*.

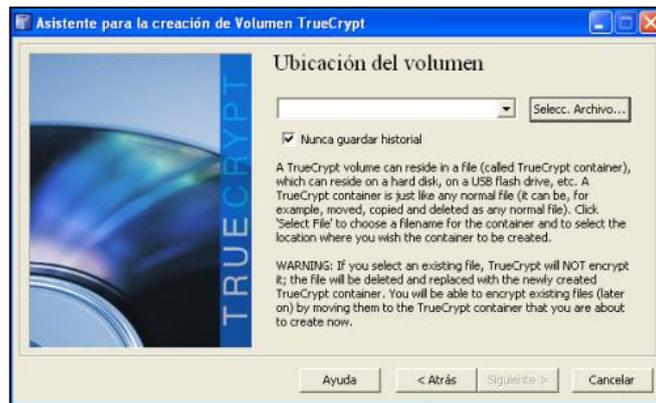
TrueCrypt permite crear dos tipos de volúmenes: *Oculto y Común*, que se muestran en la Figura. Seleccionar una opción y pulsar *Siguiente 177*.



*Figura 177. Selección del tipo de volumen
Fuente: Captura de pantalla de la aplicación Truecrypt*

A continuación aparece la ventana que se muestra en la *Figura 178*, en donde se debe elegir en qué lugar se va a crear el volumen TrueCrypt, puede ser

en una partición del disco duro, un dispositivo USB o cualquier medio de almacenamiento. Pulsar *Seleccionar Archivo* para elegir la ubicación donde se va a guardar y asignar el nombre para el volumen, luego presionar *Siguiente*.



*Figura 178. Ventana de ubicación del volumen
Fuente: Captura de pantalla de la aplicación Truecrypt*

En la siguiente ventana mostrada en la *Figura 179*, se debe escoger un método específico de cifrado para el Volumen Común. Este será utilizado para cifrar los datos que serán almacenados en dicho Volumen.



*Figura 179. Ventana de opciones de encriptación
Fuente: Captura de pantalla de la aplicación Truecrypt*

Una vez que se seleccione los algoritmos de cifrado, pulsar *Siguiente* y aparece la siguiente ventana que se muestra en la *Figura 180*:



Figura 180. Selección del tamaño del volumen
Fuente: Captura de pantalla de la aplicación Truecrypt

En ésta ventana se debe asignar el *Tamaño del volumen* sea en KB MB o GB, luego presionar *Siguiente*, aparece la ventana mostrada en la *Figura 181*:

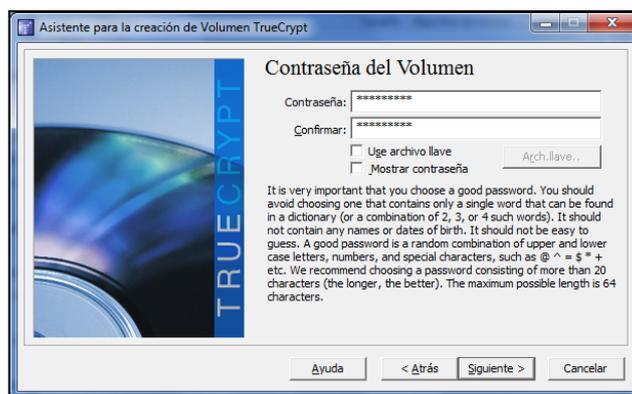


Figura 181. Ingreso de contraseña
Fuente: Captura de pantalla de la aplicación Truecrypt

En esta pantalla se ingresa la contraseña, la misma que debe tener por lo menos 8 caracteres incluyendo letras y números para mayor seguridad. Además si se desea tener un nivel superior de seguridad se puede elegir un archivo de cualquier extensión para el cifrado del volumen, pero es importante tener en

cuenta que si el archivo con el que se cifró se pierde, la información no puede ser recuperada.

Una vez ingresada la contraseña, confirmarla y luego pulsar *Siguiente*. En la siguiente pantalla se debe seleccionar el sistema de ficheros de preferencia y se debe mover el ratón durante al menos 30 segundos, para aumentar la aleatoriedad de la clave, luego presionar *Format* para dar formato al volumen. Al finalizar el formateo aparece el mensaje que se muestra en la *Figura 182*:



Figura 182. Creación exitosa del volumen
 Fuente: Captura de pantalla de la aplicación Truecrypt

Esto significa que el volumen está bien creado. Presionar sobre *Aceptar* y aparece la siguiente ventana:



Figura 183. Salir de la pantalla
 Fuente: Captura de pantalla de la aplicación Truecrypt

Si se desea crear otro volumen se hace clic en *Siguiente*, caso contrario se hace clic en *Salir*.

UTILIZACIÓN

Para empezar a utilizar el nuevo volumen cifrado es necesario montar las unidades, para esto, se debe abrir la ventana de TrueCrypt y elegir una letra de unidad y luego pulsar *Seleccionar archivo*, como se muestra en la *Figura 184*:

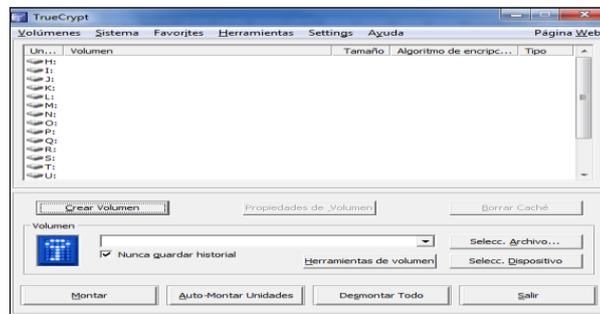


Figura 184. Ventana de Truecrypt
Fuente: Captura de pantalla de la aplicación Truecrypt

Ubicar el directorio en el que se creó el fichero anteriormente y seleccionarlo. Al pulsar *Montar* se pedirá la contraseña y si es necesario el archivo de cifrado. La *Figura 185* muestra esta ventana.

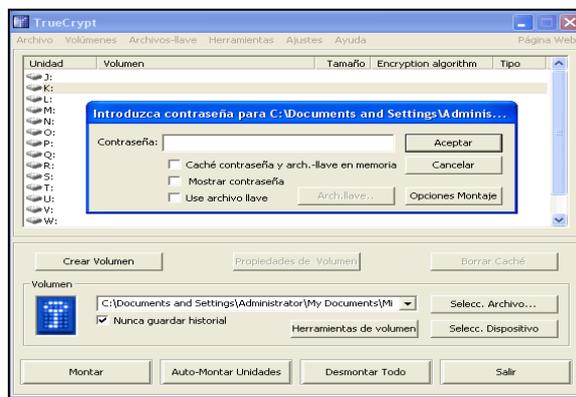


Figura 185. Ingreso de contraseña
Fuente: Captura de pantalla de la aplicación Truecrypt

Si la contraseña es correcta se montará una unidad de disco duro que es donde se guardará los archivos que se desea mantener cifrados. En la *Figura 186*, se puede apreciar esta ventana.

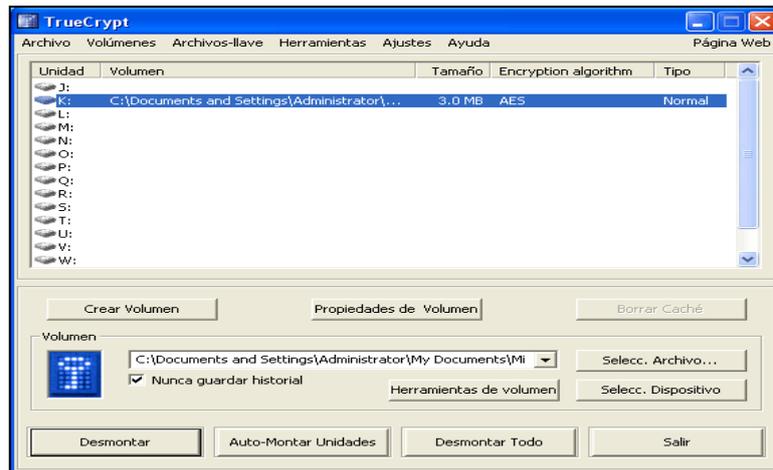


Figura 186. Montaje de unidad de disco duro
Fuente: Captura de pantalla de la aplicación Truecrypt

Para verificar que el volumen está creado, ir a Mi PC. En la siguiente ventana que se muestra en la *Figura 187* se puede ver que se encuentra como otra unidad de disco.

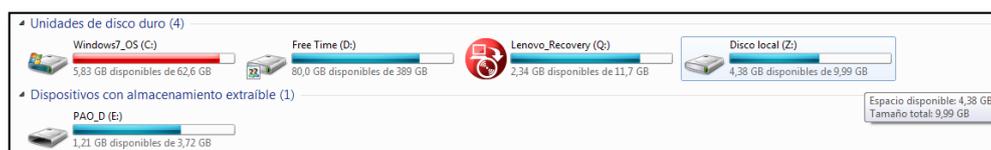
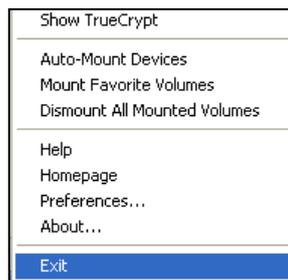


Figura 187. Volumen montado
Fuente: Captura de pantalla de la aplicación Truecrypt

SALIR DE LA APLICACIÓN

Para salir de la aplicación dar un clic derecho en el botón  ubicado en la parte inferior derecha de la pantalla y escoger la opción *Salir*.



*Figura 188. Ventana para salir del sistema
Fuente: Captura de pantalla de la aplicación Truecrypt*

6.9. FIREWALL

ADMINISTRACIÓN DEL FIREWALL CON WEBMIN

Webmin es una herramienta de configuración de sistemas accesible vía web para Open Solaris, GNU/Linux y otros sistemas Unix. Con él se pueden configurar aspectos internos de muchos sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, así como modificar y controlar muchas aplicaciones libres.

CONTROL DE ACCESO IP

Para la administración de este servidor se encuentra abierto el acceso sólo a las direcciones IP correspondientes a los encargados de su Administración, lo cual permite tener control ante accesos no autorizados.

Para agregar, modificar o eliminar direcciones IP con acceso al servidor, ingresar a éste con el usuario *designado*. Posteriormente se mostrará la página principal, en el panel izquierdo desplegar la pestaña *Webmin*, hacer clic sobre

Configuración de Webmin y en el panel Central hacer clic sobre *Control de Acceso a IP*. La *Figura 189*, muestra la ventana principal de Webmin.



Figura 189. Configuración de Webmin
Fuente: Captura de pantalla

Dentro de esta opción se indica el listado de las direcciones IP que tienen acceso a la administración del servidor. Esta ventana se muestra en la *Figura 190*.

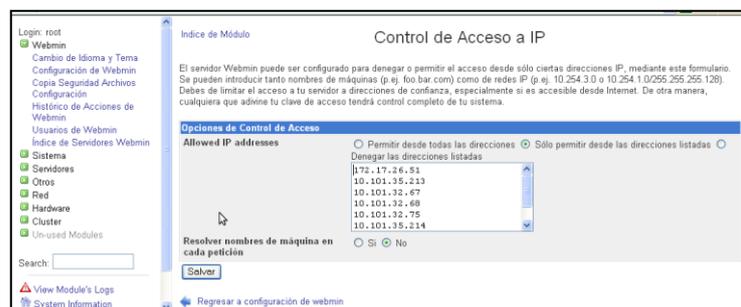


Figura 190. Configuración del control de acceso IP
Fuente: Captura de pantalla

Luego de realizar algún cambio presionar el Botón *Salvar*. Este archivo de configuración se encuentra en el fichero `/etc/webmin/miniserv.conf`

SHOREWALL

Para ingresar a Shorewall en el menú lateral izquierdo desplegar la opción *Red* y escoger la opción *Cortafuegos Shorewall* y se mostrará la ventana de la *Figura 191*:



Figura 191. Vista del panel principal de Shorewall
Fuente: Captura de pantalla

Aquí se encuentran las diferentes opciones para configurar Shorewall.

Zonas

Para crear una nueva zona o modificar una ya existente seleccionar la opción *Zonas de Red* y se mostrará la interfaz de la *Figura 192*:

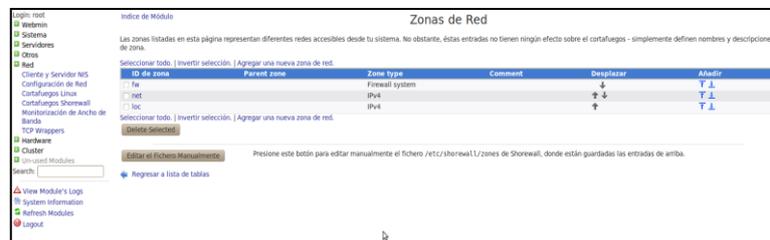


Figura 192. Interfaz de Zonas
Fuente: Captura de pantalla

Para crear una nueva zona seleccionar la opción *Agregar una nueva zona de red* mostrándose la siguiente interfaz de la *Figura 193*:

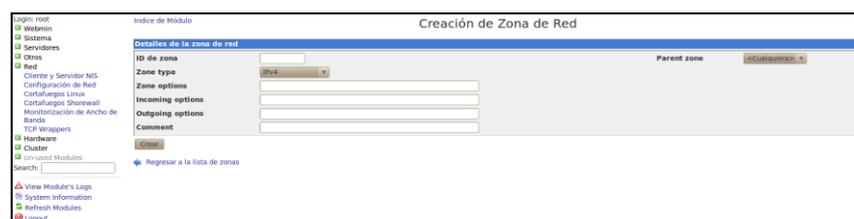


Figura 193. Creación de Zona de Red
Fuente: Captura de pantalla

En la ventana que se muestra en la opción *ID de zona* especificar el nombre de la zona que se va a crear y en la opción *Zone Type* seleccionar IPV4 y finalmente presionar el botón *Crear*.

Para editar una zona ya existente seleccionar la zona a modificar, en la cual se debe editar las opciones *ID de zona* y *Zone Type* y finalmente presionar el botón *Salvar* para guardar los cambios realizados.

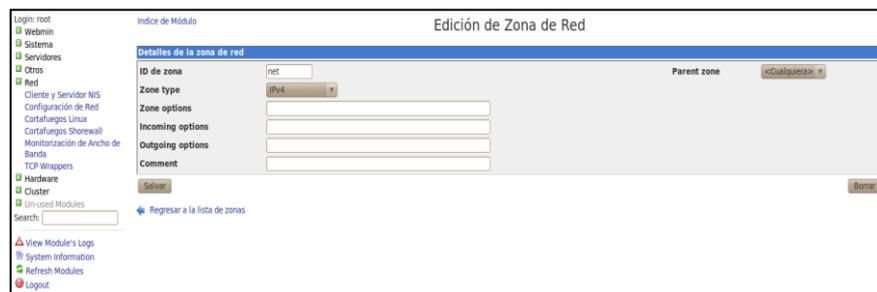


Figura 194. Edición de Zona de Red
Fuente: Captura de pantalla

Para eliminar una zona se debe seleccionarla y presionar el botón *Borrar* eliminándose la zona especificada.

Interfaces

Para definir una nueva interfaz o modificar una ya existente seleccionar la opción *Interfaces de Red* y se mostrará la pantalla de la *Figura 195*:



Figura 195. Vista del panel de Interfaces
Fuente: Captura de pantalla

Para agregar una interfaz de red seleccionar la opción *Agregar una nueva interfaz de red* mostrándose la pantalla de la *Figura 196*:



Figura 196. Creación de Interfaz de Red
Fuente: Captura de pantalla

En la ventana que se muestra en la opción *Interfaz* especificar la interfaz de red física y en la opción *Nombre de Zona* seleccionar la zona que va a asociarse a dicha interfaz. Finalmente presionar el botón *Crear*.

Políticas

Para definir una nueva política o modificar una ya existente seleccionar la opción *Políticas por Defecto* mostrándose la siguiente pantalla:



Figura 197. Vista del panel de Políticas
Fuente: Captura de pantalla

Para agregar una nueva política seleccionar la opción *Agregar una nueva política por defecto* mostrándose la interfaz de la *Figura 198*:



Figura 198. Creación de una política
Fuente: Captura de pantalla

En la interfaz seleccionar la opción *Zona Origen* especificando la zona desde la cual se va permitir o denegar el acceso. A continuación seleccionar la opción *Zona Destino* especificando la zona a la cual se denegará o permitirá el acceso. Luego definir la política que se va aplicar entre las zonas seleccionadas anteriormente entre las que se tiene:

- ACCEPT: Permitir el tráfico entre las zonas seleccionadas.
- DROP: Denegar el tráfico entre las zonas seleccionadas.
- REJECT: Rechazar el tráfico entre las zonas seleccionadas.

Finalmente seleccionar la opción *Nivel de Syslog* en la cual se puede especificar el tipo de información que se registrará en los logs y presionar el botón *Crear* con lo cual la nueva política quedará establecida.

Reglas

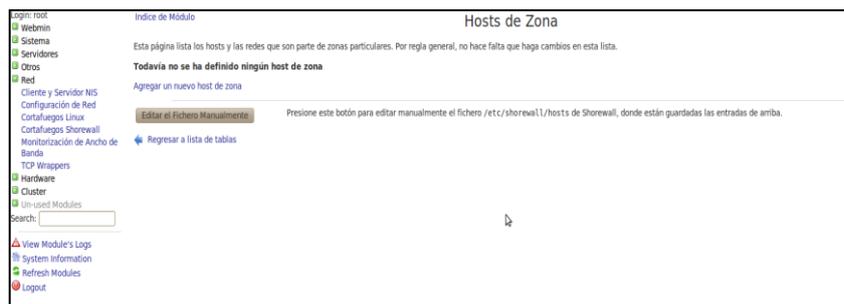
Para crear una nueva regla o modificar una ya existente seleccionar la opción *Reglas del Firewall* mostrándose la interfaz de la *Figura 199*:

Acción	Origen	Destino	Protocolo	Puertos de origen	Puertos destino	Desplazar	Añadir
<input type="checkbox"/> DNAT	Zona net	Host 18.18.1.68-88 de la zona Loc	TCP	Cualquiera	80	↓	T ↓
<input type="checkbox"/> PingDROP	Zona net	Cortafuegos		Cualquiera		↑ ↓	T ↓
<input type="checkbox"/> DNSACCEPT	Cortafuegos	Zona net		Cualquiera		↑ ↓	T ↓
<input type="checkbox"/> ACCEPT	Cortafuegos	Zona Loc	ICMP	Cualquiera		↑ ↓	T ↓
<input type="checkbox"/> ACCEPT	Cortafuegos	Zona net	ICMP	Cualquiera		↑ ↓	T ↓
<input type="checkbox"/> ACCEPT	Zona Loc	Cortafuegos	ICMP	Cualquiera		↑ ↓	T ↓
<input type="checkbox"/> ACCEPT	Cortafuegos	Zona net	TCP	Cualquiera	25,80,8080,443,81,82,10000,2082,2095,53,110,21,143,22022	↑ ↓	T ↓
<input type="checkbox"/> ACCEPT	Zona Loc	Cortafuegos	TCP	Cualquiera	3128,22,22022,58000,10000,21,25,110,443,2082,2095,143,53	↑ ↓	T ↓
<input type="checkbox"/> ACCEPT	Zona Loc	Zona net	TCP	Cualquiera	465,995,25,110,143,22,22022,75,1723	↑ ↓	T ↓
<input type="checkbox"/> ACCEPT	Zona Loc	Cortafuegos	UDP	Cualquiera	53	↑ ↓	T ↓

*Figura 199. Vista del panel de Reglas
Fuente: Captura de pantalla*

Hosts

Para crear un nuevo hosts o modificar uno ya existente en función de una determinada zona seleccionar la opción *Hosts de Zona* mostrándose la interfaz de la *Figura 200*:



*Figura 200. Vista del panel de Hosts de Zona
Fuente: Captura de pantalla*

6.10.PROXY

ADMINISTRACIÓN DEL PROXY CON SQUIDGUARD

SquidGuard es un sistema de filtrado web por listas negras, es decir que guarda una lista de las URLs o dominios a las que se puede denegar o permitir el acceso al usuario.

Para ingresar a SquidGuard en el menú lateral izquierdo desplegar la opción Servidores Proxy y escoger la opción SquidGuard y se mostrará la ventana de la *Figura 201*:



Figura 201. Vista del panel principal de SquidGuard
Fuente: Captura de pantalla

Dentro del menú de SquidGuard se distinguen los diferentes grupos de acceso como se muestra a continuación:

Source Groups

Para permitir o denegar el acceso de navegación de ciertas URLs o dominios a los usuarios se los debe dividir por grupos. Para crear un grupo se lo realiza de la siguiente manera:



Figura 202. Vista del panel de Source Groups
Fuente: Captura de pantalla

En el cuadro de texto ubicado en la parte inferior escribir el nombre del grupo y presionar el botón *Add Source Group*.

Cada grupo abarca un conjunto de ACLs de acceso con los cuales se dan los respectivos permisos de navegación.

Los Sourcegroup contienen las direcciones IP del grupo de usuarios al que pertenece, para agregar usuarios al grupo creado anteriormente en la pantalla de SquidGuard escoger la opción *Sourcegroups* y se mostrará la pantalla de la *Figura 203*.

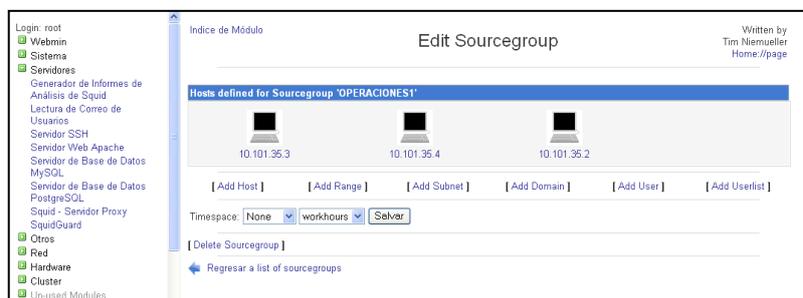


Figura 203. Vista de ventana de edición de los SourceGroup
Fuente: Captura de pantalla

En la ventana que se muestra se puede editar los usuarios del grupo especificado, dentro de la cual se tienen varias opciones como añadir host, añadir un rango de direcciones, añadir subredes, entre otras.

Para añadir un nuevo host seleccionar la opción *Add Host* y escribir la dirección IP del usuario que se desea añadir y luego presionar el botón *Salvar*, como se muestra en la *Figura 204*.

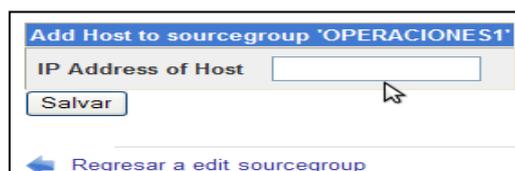


Figura 204. Adición de un nuevo host
Fuente: Captura de pantalla

Para borrar una dirección IP hacer doble clic sobre el host y en la ventana que se muestra en la *Figura 205*, presionar el botón *Borrar*.



Figura 205. Eliminación de un host
Fuente: Captura de pantalla

Si se desea borrar un grupo presionar el botón *Delete Sourcegroup* ubicado en la parte inferior de la ventana. Se debe tener en cuenta que al presionar este botón se borrarán todos los usuarios que contenga el grupo.

La configuración de los Sourcegroups se localiza en el fichero */etc/squid/squidGuard.conf*; luego de realizar algún cambio es necesario aplicar un reload al squid para que se apliquen los cambios, con el siguiente comando:
/etc/init.d/squid reload

Access Control Lists

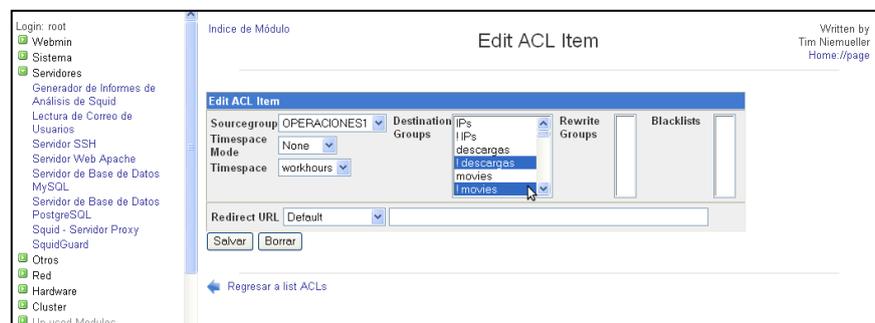
Las listas de control de acceso indican las URL o dominios a los cuales los usuarios tendrán acceso o no, cada uno de los grupos Source Groups tiene sus propias listas de acceso.

Para editar las listas de control de acceso en la pantalla de SquidGuard escoger la opción Access Control Lists y se mostrará una pantalla similar a la de la *Figura 206*:



*Figura 206. Vista de las Listas de Control de Acceso
Fuente: Captura de pantalla*

Dentro de esta ventana se muestra un listado de los grupos creados cada uno con sus respectivas reglas. Para editar las ACL escoger el grupo y hacer doble clic sobre él, dentro de la pantalla que se muestra en la *Figura 207*, se distinguen las categorías de los dominios o URL que se pueden aplicar a los grupos.



*Figura 207. Edición de las ACL de un SourceGroup
Fuente: Captura de pantalla*

Así también se tienen las opciones *Any* para permitir un acceso total o *None* para restringir todo.

Es importante tener en cuenta que luego de restringir el acceso a ciertos dominios o URL se debe además escoger además la opción *Any*, para indicar que

hay excepción de los dominios restringidos pueda navegar en todos los sitios web.

Cabe notar que para indicar que se niegue el acceso a ciertos sitios web se debe seleccionar la opción que se encuentra precedida del signo de admiración (!)

Servidor Proxy Squid

Para desplegar la opción de Proxy-Squid seleccionar la opción *Squid Proxy Server* del menú lateral izquierdo con lo cual se mostrará la ventana de la *Figura 208*:



Figura 208. Vista del panel del Servidor Proxy Squid
Fuente: Captura de pantalla

Generador de informes de análisis de Squid (Sarg)

SARG es una herramienta que lee los archivos generados por proxy squid y emite reportes detallados del acceso de los usuarios a través del proxy; por defecto los reportes son mostrados de manera descendiente, mostrándose primero las direcciones IP que más accedieron a la web y dentro de la dirección IP se desglosan los sitios accedidos de manera detallada.

Estos reportes se obtienen de manera automática, o también se pueden obtener los reportes al momento de ser necesario.

Para abrir el generador de informes de Squid en el menú lateral izquierdo dentro del menú *Servidores* seleccionar *Generador de Informes de Análisis de Squid*, y se mostrará la ventana de la *Figura 209*:



Figura 209. Vista del generador de informes de análisis de Squid
Fuente: Captura de pantalla

En la ventana que se muestra se pueden realizar dos acciones:

- *Generar informe ahora*: con esta opción se genera de forma inmediata un informe.
- *Ver informe Generado*: para ver el informe más recientemente generado.

6.11.NTOP

Para ingresar a la aplicación abrir el navegador de internet y digitamos la siguiente dirección: `http://ip_servidor:3000` con lo cual aparecerá la interfaz de la *Figura 210*:

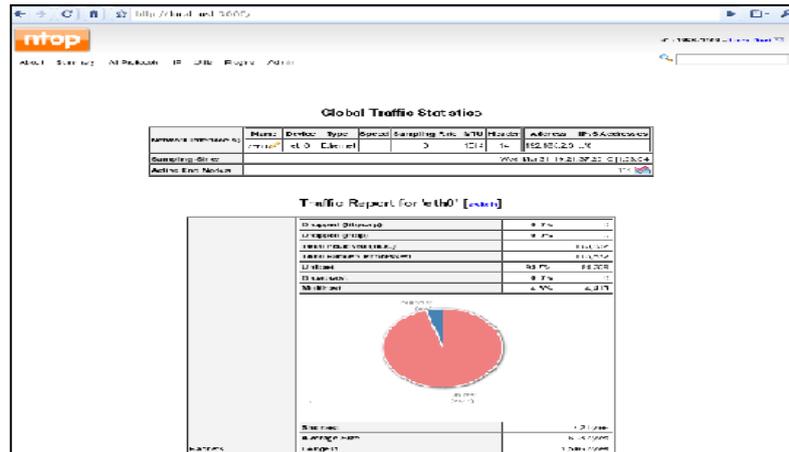


Figura 210. Interfaz de Ntop
Fuente: Captura de pantalla

La información más importante proporcionada por Ntop es la que se muestra en las Figuras 211 y 212:

Distribución De Tráfico

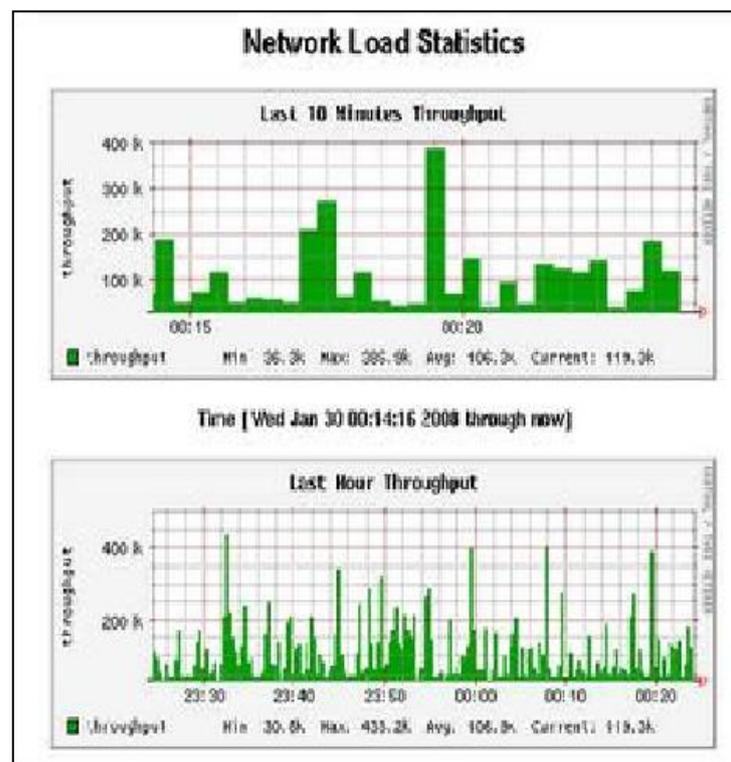


Figura 211. Distribución de Tráfico
Fuente: Captura de pantalla

Troughput De La Red

The screenshot shows the ntop interface with the 'Network Throughput: Remote Hosts - Data Sent+Received' view. The table below represents the data shown in the screenshot.

Host	Domain	Data			Packets		
		Current	Avg	Peak	Current	Avg	Peak
195.114.402.455.deploy.akamaitechnologies.com	deploy.akamaitechnologies.com	0.0 sec	0.0 sec	3.4 bytes	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
195.114.402.457.deploy.akamaitechnologies.com	deploy.akamaitechnologies.com	0.0 sec	0.0 sec	25.6 bytes	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
195.114.402.461.deploy.akamaitechnologies.com	deploy.akamaitechnologies.com	0.0 sec	0.0 sec	3.0 bytes	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec
data.cerent.com	cerent.com	0.1 sec	0.1 sec	6.3 bytes	0.1 Pkts/sec	0.1 Pkts/sec	0.1 Pkts/sec
dns.cachefl.com	cachefl.com	0.2 sec	0.2 sec	155.6 bytes	0.2 Pkts/sec	0.2 Pkts/sec	0.2 Pkts/sec
qumax.com	qumax.com	0.2 sec	0.2 sec	23.4 bytes	0.2 Pkts/sec	0.2 Pkts/sec	0.2 Pkts/sec
newsroom.cisco.com	cisco.com	0.2 sec	0.2 sec	102.7 bytes	0.2 Pkts/sec	0.2 Pkts/sec	0.2 Pkts/sec
stats.www.ibm.com	ibm.com	0.2 sec	0.2 sec	207.0 bytes	0.2 Pkts/sec	0.2 Pkts/sec	0.2 Pkts/sec
www.304.com	304.com	0.3 sec	0.3 sec	267.4 bytes	0.3 Pkts/sec	0.3 Pkts/sec	0.3 Pkts/sec
www.suomi.com	suomi.com	0.3 sec	0.3 sec	73.0 bytes	0.3 Pkts/sec	0.3 Pkts/sec	0.3 Pkts/sec
www.163.com	163.com	0.5 sec	0.5 sec	47.3 bytes	0.5 Pkts/sec	0.5 Pkts/sec	0.5 Pkts/sec

Figura 212. Troughput de la red
Fuente: Captura de pantalla

Es recomendable utilizar esta herramienta solo cuando sea necesario, pues al almacenar datos de todo el tráfico de red, puede ser un consumidor de recursos extraordinario, dejando sin espacio en el sistema a otras aplicaciones.

6.12.MRTG

INGRESO A LA APLICACIÓN

Para ingresar a la aplicación abrir el navegador de internet y digitar la siguiente dirección: http://ip_servidor/mrtg con lo cual aparecerá la interfaz de la

Figura 213:

The screenshot shows the 'Index of /mrtg' page. The table below represents the content of the index page.

Name	Last modified	Size	Description
Parent Directory		-	
core775/	02-Mar-2010 15:20	-	
piso_2_1/	02-Mar-2010 13:02	-	
piso_2_2/	02-Mar-2010 13:26	-	
piso_3/	02-Mar-2010 14:38	-	
piso_4/	02-Mar-2010 14:46	-	
piso_5/	02-Mar-2010 15:01	-	
planta_b_1/	02-Mar-2010 13:07	-	
planta_b_2/	02-Mar-2010 13:03	-	
subsuelo_1/	02-Mar-2010 12:27	-	

Apache/2.2.9 (Debian) PHP/5.2.6-1+etonyG with Suhosin-Patch Server at 172.17.26.51 Port 80

Figura 213. Página de inicio de la aplicación
Fuente: Captura de pantalla

En la ventana se muestra un listado de interfaces de red activas. Para acceder a uno de ellos dar clic sobre el nombre y se mostrará un resumen del análisis de tráfico por interfaz como se indica en la *Figura 214*.

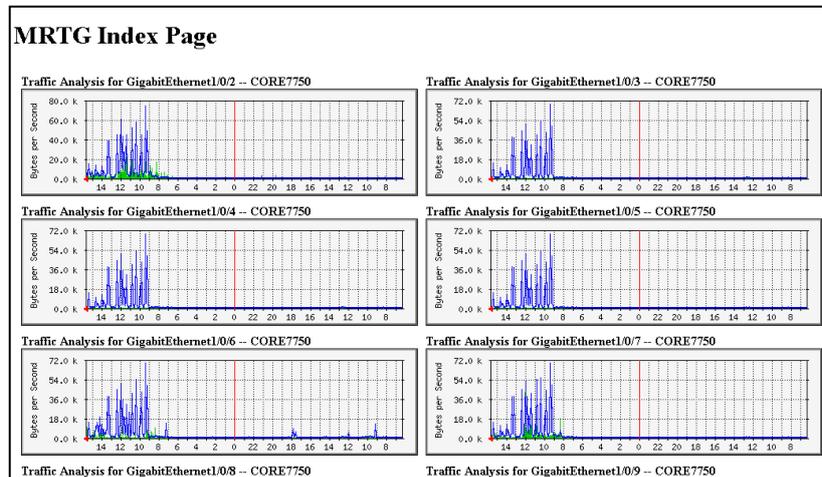


Figura 214. Análisis de tráfico de las interfaces
Fuente: Captura de pantalla

En la ventana que se despliega se mostrará el análisis de tráfico de cada una de las interfaces. Para ver en detalle el análisis de tráfico de una interfaz, hacer clic sobre la imagen correspondiente.

Se mostrará una ventana como la de la *Figura 215* indicando el análisis de tráfico por interfaz diaria, semanal, mensual y anual.

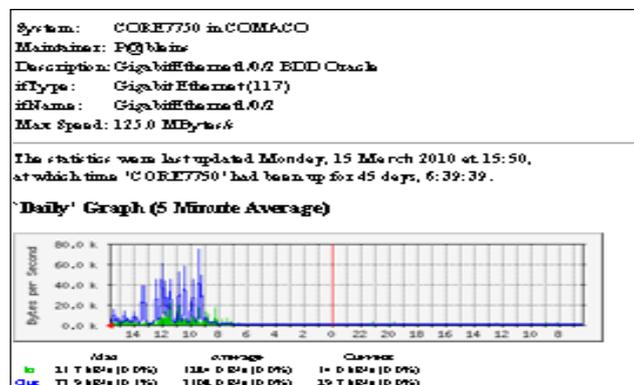


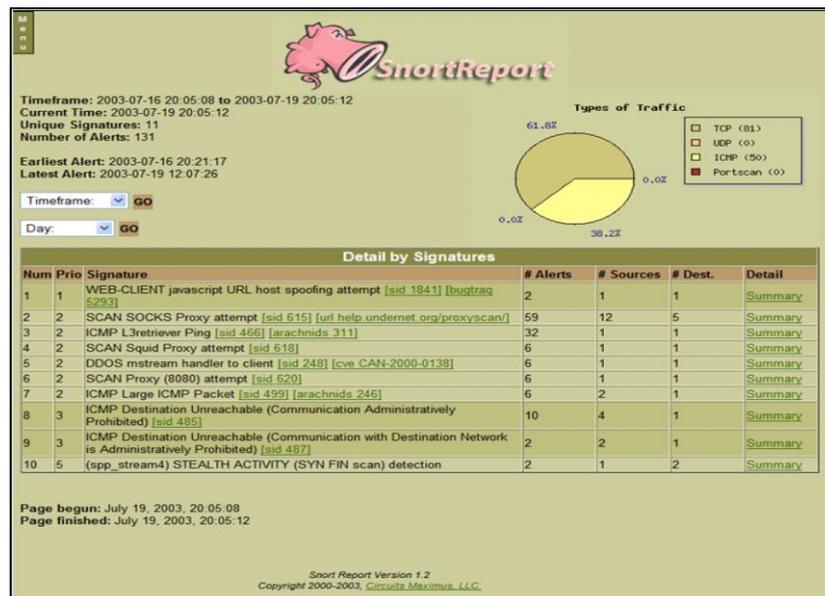
Figura 215. Análisis de tráfico de la interfaz
Fuente: Captura de pantalla

Por defecto, MRTG cada cinco minutos recolecta la información de los dispositivos y ejecuta los scripts que se le indican en la configuración.

MRTG supervisa tanto el tráfico entrante como saliente de cada una de las interfaces de los switch monitoreados.

6.13.IDS/IPS

Para ingresar a la aplicación de Snortreport, en un navegador web ejecutar la IP seguido por el nombre snortreport y se muestra la página de inicio de la *Figura 216*:



*Figura 216. Pantalla principal de SNORTREPORT
Fuente: Captura de pantalla*

En el lado superior derecho de la pantalla se muestra un gráfico como el de la *Figura 217*, con las estadísticas de las alertas ocurridas por cada tipo de tráfico.

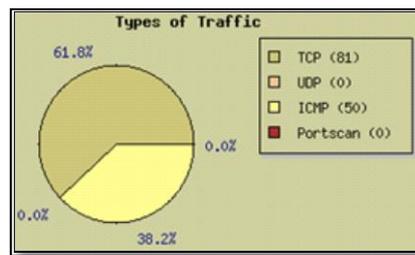


Figura 217. Estadísticas de alertas por tipo de tráfico
Fuente: Captura de pantalla

En la parte inferior de la página principal se muestra un resumen de las alertas detectadas, mostrados en una tabla como la de la Figura 218:

Detail by Signatures						
Num	Prio	Signature	# Alerts	# Sources	# Dest.	Detail
1	1	WEB-CLIENT javascript URL host spoofing attempt [sid 1841] [bugtraq 5293]	2	1	1	Summary
2	2	SCAN SOCKS Proxy attempt [sid 615] [url help.undernet.org/proxyscan/]	59	12	5	Summary
3	2	ICMP L3retriever Ping [sid 466] [arachnids 311]	32	1	1	Summary
4	2	SCAN Squid Proxy attempt [sid 618]	6	1	1	Summary
5	2	DDOS mstream handler to client [sid 248] [cve CAN-2000-0138]	6	1	1	Summary
6	2	SCAN Proxy (8080) attempt [sid 620]	6	1	1	Summary
7	2	ICMP Large ICMP Packet [sid 499] [arachnids 246]	6	2	1	Summary
8	3	ICMP Destination Unreachable (Communication Administratively Prohibited) [sid 485]	10	4	1	Summary
9	3	ICMP Destination Unreachable (Communication with Destination Network is Administratively Prohibited) [sid 487]	2	2	1	Summary
10	5	(spp_stream4) STEALTH ACTIVITY (SYN FIN scan) detection	2	1	2	Summary

Figura 218. Tabla de alertas detectadas
Fuente: Captura de pantalla

Esta tabla muestra 7 columnas, en las mismas que se detalla:

- Num: Número de alerta.
- Prio: Prioridad de la alerta
- Signature: Descripción de la alerta
- # Alerts: Cantidad de alertas
- # Sources: Número de IP origen. (De donde se está produciendo una actividad sospechosa).
- # Dest. Número de IP de destino. (Hacia donde se está dirigiendo una actividad sospechosa).

- Detail: Para revisar con detalle las alertas generadas.

Para revisar con detalle cada alerta hacer clic sobre la palabra *Summary*, aparece la ventana que se muestra en la *Figura 219*:

Sources Triggering This Attack Signature					
Source IP	FQDN	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
		2	2	1	1

Destinations Receiving This Attack Signature					
Dest IP	FQDN	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
		29	29	1	16

*Figura 219. Listado de alertas
Fuente: Captura de pantalla*

En esta página se muestra un listado de las IP origen que están provocando tráfico sospechoso y la cantidad de alertas por cada una.

Si se desea verificar con más detalle las alertas de una IP origen en particular, hacer clic sobre la IP y se muestra una ventana como la de la *Figura 220*, con la información de las alertas:

```

Signatures with 10.101.35.219 as a Source (24 events)
CID:318469 [**] COMMUNITY_SIP TCP/IP message flooding directed to SIP proxy [**]
2011-01-07 19:00:21 10.101.35.219:4689 -> 172.17.26.245:3000
TCP TTL:63 TOS:0x0 ID:47374 IFLen:52 HLen:5 CSumIP:0x8D6F
***A*** Seq:0x6943B88C Ack:0x38F780F7 Win:0x5C CSumTCP:0x11C
TCP Options (3) => NO-OP NO-OP Timestamp:1B3C0186
CID:318473 [**] COMMUNITY_SIP TCP/IP message flooding directed to SIP proxy [**]
2011-01-07 19:01:21 10.101.35.219:4689 -> 172.17.26.245:3000
TCP TTL:63 TOS:0x0 ID:37541 IFLen:60 HLen:5 CSumIP:0x3D0
***** Seq:0xA136A18 Ack:0x0 Win:0x1400 CSumTCP:0x019F
TCP Options (5) => MSS:05B4 SACKOK Timestamp:1B3C3CBE NO-OP WS:06
CID:318477 [**] COMMUNITY_SIP TCP/IP message flooding directed to SIP proxy [**]
2011-01-07 19:02:22 10.101.35.219:47201 -> 172.17.26.245:3000
TCP TTL:63 TOS:0x0 ID:53025 IFLen:52 HLen:5 CSumIP:0x775C
***A*** Seq:0xD995BA61 Ack:0xAAA75600 Win:0x81 CSumTCP:0xA08F
TCP Options (3) => NO-OP NO-OP Timestamp:1B3C77C1
CID:318481 [**] COMMUNITY_SIP TCP/IP message flooding directed to SIP proxy [**]
2011-01-07 19:03:23 10.101.35.219:47418 -> 172.17.26.245:3000
TCP TTL:63 TOS:0x0 ID:7552 IFLen:52 HLen:5 CSumIP:0x28FE
***A*** Seq:0x1306B028 Ack:0xE369D510 Win:0x5C CSumTCP:0x6572
TCP Options (3) => NO-OP NO-OP Timestamp:1B3CB340
CID:318485 [**] COMMUNITY_SIP TCP/IP message flooding directed to SIP proxy [**]
2011-01-07 19:04:23 10.101.35.219:50587 -> 172.17.26.245:3000
TCP TTL:63 TOS:0x0 ID:62391 IFLen:52 HLen:5 CSumIP:0x52C6
***A*** Seq:0x4BFE1FB4 Ack:0x1B9CCB7C Win:0x82 CSumTCP:0x2F3B
TCP Options (3) => NO-OP NO-OP Timestamp:1B3CE47

```

*Figura 220. Detalle de eventos producidos desde IP origen
Fuente: Captura de pantalla*

En esta ventana se muestra el sentido del envío del tráfico, el tipo de tráfico que se envió, y cuantos eventos se produjeron.

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

- El Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma ISO/IEC 27001, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua, que consiste en Planificar- Hacer-Verificar-Actuar, de igual manera tiene también su fundamento en la norma ISO/IEC 27002:2005, que recoge una lista de objetivos de control y controles necesarios para lograr los objetivos de seguridad de la información.
- Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información.
- Una política de seguridad es una forma de comunicarse con los usuarios, ya que las mismas establecen un instructivo de comportamiento del personal, en relación con los recursos y servicios tecnológicos de la organización.
- La información, como uno de los principales activos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para lograrlos objetivos de la institución.

- Llegar a tener seguridad total en una red es inalcanzable pero con la mejora continua y la adopción de métodos y estándares de seguridad de la información se mantiene un nivel de seguridad aceptable que reduce los riesgos de la red.
- El uso de software libre en instituciones públicas se ha convertido en un factor fundamental en la gestión, administración y seguridad de las tecnologías de la información.
- La implementación de herramienta de monitoreo de redes es fundamental para asegurar el funcionamiento de los sistemas informáticos y para evitar fallos en la red.
- La asignación de responsables de activos y de la implantación de contramedidas permite que las probabilidades de éxito de la implantación del SGSI aumenten.

7.2. RECOMENDACIONES

- La política de seguridad de la institución debe partir de una visión estratégica y gestionarse bajo un enfoque de protección integral e integrada a los objetivos del CP-12.
- Se debe informar de manera detallada a los usuarios, personal y demás autoridades del CP-12, todas las normas y mecanismos que deben cumplir y utilizar para proteger los activos de la institución.

- Se debe realizar evaluaciones periódicas del funcionamiento tanto de la infraestructura tecnológica como las normas y políticas que se están aplicando en la institución con el fin de verificar si se están mitigando los riesgos de seguridad de la información, y en el caso de que no se estén cumpliendo les permita tomar medidas.
- Generar planes de concientización de los usuarios con la finalidad de mejorar el uso de las tecnologías de la información y evitar que por razones de desconocimiento no se aproveche al máximo los recursos disponibles en la institución.
- Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y limitar el impacto de los mismos.
- Es importante resaltar que cada vez que se incorpora una nueva herramienta de TI a la institución se debe actualizar el análisis de riesgos para poder mitigar de forma responsable los riesgos.
- Se debe buscar el compromiso y soporte gerencial, de manera que el proyecto sea asistido desde la dirección, y sea esta la primera en dar ejemplo a la hora de utilizar las medidas necesarias para definir, aplicar y mantener la seguridad en la institución.

REFERENCIAS BIBLIOGRÁFICAS

RECURSOS BIBLIOGRÁFICOS EN LÍNEA

Bitberry Software ApS. (Octubre 2012). Seguridad de la información. Disponible en: <http://www.bitzipper.com/es/aes-encryption.html>

Consejo Superior de Informática. (Enero 2012) MAGERIT. Versión 1.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas.

ISO/IEC, ISO 27000.(Noviembre 2011). Normativa ISO y estándares referentes. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf

Gestión de calidad, Implantación ISO 27001:2005. (Diciembre 2011). Disponible en: <http://www.gestion-calidad.com/implantacion-iso-27001.html>

Martínez Esparza, Miguel. (Junio 2012). Implementación iTALC. Disponible en: <http://recursostic.educacion.es/observatorio/web/es/software/software-educativo/1001-italc>

Mendoza Rosendo A., SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN.CASO: CENTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN. Venezuela. 2008. Disponible en <http://www.slideshare.net/mmujica/mi-defensa>

TEXTOS

ANDRÉS, Ana; GÓMEZ, Luis Antonio, Guía de aplicación de la norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para Pymes. 1ª edición. Editorial AENOR. España. 2009.

BURCH, John G, Diseño de sistemas de información. 1ª edición. Editorial Noriega. 2007.

HUMPHREYS, Ted; PLACA, Angélica, Directrices sobre los requisitos y preparación para la certificación de SGSI según ISO/IEC 27001. Editorial Instituto de normalización Británico. Gran Bretaña. 2007.

ICONTEC; Sistema de Gestión de la Seguridad de la Información (SGSI). Compendio. 2da edición. Editorial Instituto colombiano de Normas Técnicas y Certificación. Colombia. 2009.

MARCOMBO, Alexander, Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:2005. 1ª edición. Editorial Alfaomega Grupo Editor. México. 2007.

PAGE, Kogan, Gobierno de TI: Una guía para la gerencia de seguridad de datos e ISO27001/ISO27002. Cuarta edición. 2008.

NORMAS ISO

ISO/IEC 27001, Estándar Internacional: Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Establecimiento del SGSI. Primera Edición 2005 - 10 – 15.

ISO/IEC 27002, Estándar Internacional: Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. Primera Edición 2005 - 06- 15.

ISO/IEC, ISO 27000. Normativa ISO y estándares referentes. Disponible en: http://www.iso27000.es/download/doc_iso27000_all.pdf[Consulta: 21 de Diciembre de 2011].

GLOSARIO DE TÉRMINOS

ACTIVO: Cualquier cosa que tenga valor para la organización.

AMENAZA: Evento que puede provocar un incidente en la organización produciendo daños o pérdidas materiales y/o inmateriales.

DISPONIBILIDAD: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

CONFIDENCIALIDAD: La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

INTEGRIDAD: La propiedad de salvaguardar la exactitud e integridad de los activos.

SEGURIDAD DE INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

SGSI: La parte del sistema gerencial general, basado en un enfoque de riesgo institucional; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

ANÁLISIS DE RIESGO: Uso sistemático de la información para identificar fuentes y para estimar el riesgo.

EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

GESTIÓN DEL RIESGO: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

TRATAMIENTO DEL RIESGO: Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.

VULNERABILIDAD: Susceptibilidad de algo para absorber negativamente incidencias externas.

PROPIETARIO: Identifica a la persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos.

ENUNCIADO DE APLICABILIDAD: Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.

CONTROL: Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales.

LINEAMIENTO: Una descripción que aclara qué se debe hacer y cómo, para lograr los objetivos establecidos en las políticas.

MEDIOS DE PROCESAMIENTO DE LA INFORMACIÓN: Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

POLÍTICA: Intención y dirección general expresada formalmente por la gerencia.

RIESGO: Combinación de la probabilidad de un evento y su ocurrencia.

ANEXOS

ANEXO 1
ENCUESTA APLICADA EN EL CP-12

La presente encuesta tiene la finalidad de conocer la situación actual de la institución con respecto a seguridad de la información.

Marque con una X la opción que considere conveniente.

Indicador: *Confidencialidad de la Información*

PREGUNTAS SI /NO

Si No

¿En la Institución hay una cultura de apoyo a la seguridad informática?

¿Hay planes y medidas para mitigar o administrar una brecha de confidencialidad?

¿Se ha implementado seguridades para que personas no autorizadas no puedan observar información sensitiva y confidencial?

¿Hay controles físicos en las áreas donde se encuentran Sistemas de Computación y Sistemas de Información considerados críticos?

¿Hay controles de ingreso lógico para proteger la información y datos sensitivos de accesos externos?

¿Hay controles de ingreso lógico para proteger la información y datos sensitivos de accesos internos no autorizados?

Indicador: *Integridad de la Información*

PREGUNTAS SI /NO

Si No

¿Hay riesgos significativos de que haya errores durante el ingreso de información?

¿Hay riesgos significativos de que haya errores introducidos por programas, fallas de diseño, o mal funcionamiento en los sistemas y aplicaciones que se utilizan en su oficina?

¿Hay controles de ingreso lógico para proteger datos e información sensitiva de accesos externos no autorizados?

¿La Institución promueve una cultura de seguridad?

¿Hay controles de ingreso lógico para proteger datos e información sensitiva de accesos internos no autorizados?

Indicador: *Políticas de Seguridad*

PREGUNTAS SI /NO

Si No

¿Se dispone de un documento escrito de las políticas de seguridad que sea de conocimiento de todo el personal y responsables de la seguridad de la información?

¿De existir estas políticas se da cumplimiento a las mismas?

¿Las políticas tienen una definición de seguridad de la información, objetivos y alcances?

¿Las políticas tienen una explicación del proceso para reportar incidentes de seguridad?

¿Existe un período máximo de vida de las contraseñas?

¿En su dirección está definido el personal autorizado a acceder a los sistemas?

En caso de existir dicho listado de personal autorizado, ¿se incluye el tipo de acceso permitido?

¿Existen procedimientos de asignación y distribución de contraseñas?

¿Se dispone de un documento escrito de las políticas de seguridad que sea de conocimiento de todo el personal y responsables de la seguridad de la información?

¿Los enunciados de las políticas son revisados periódicamente, incluyendo cambios en los niveles de responsabilidad?

¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas?

¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?

Indicador: *Clasificación y Control de Valores*

PREGUNTAS SI /NO

Si No

¿Hay control de los inventarios del hardware, software y medios de

almacenamiento de datos?

¿Tienen los bienes informáticos alguna forma de clasificación relativa a niveles de seguridad?

¿La información clasificada se etiqueta adecuadamente?

Indicador: Aspectos organizativos para la seguridad

PREGUNTAS SI /NO

Si No

¿Existe una persona responsable de administrar los asuntos relacionados con la seguridad informática?

¿Esta explícitamente definido la responsabilidad individual o compartida de seguridad sobre los procesos?

¿Los procesos de aprobación, adquisición e instalación de servicios para Tecnologías de Información en relación a seguridad son claros?

Indicador: Seguridad Física

PREGUNTAS SI /NO

Si No

¿Está protegida la información que se transmite por cables de telecomunicaciones de forma que no es susceptible de interceptación?

¿Los Sistemas de Cómputo y Sistemas de Información críticos están protegidos de acceso no autorizado y están ubicados en áreas seguras?

¿Los Sistemas Computacionales y Sistemas de Información están protegidos contra las fallas eléctricas?

¿Los Sistemas de Computo son ubicados pensando en su protección ante posibles amenazas ambientales (incendio, inundación, terremoto)?

¿Está definido el personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que procesan información?

¿Existe una persona responsable de la seguridad física a nivel del departamento/unidad?

¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad física?

¿Existe personal de vigilancia en la institución?

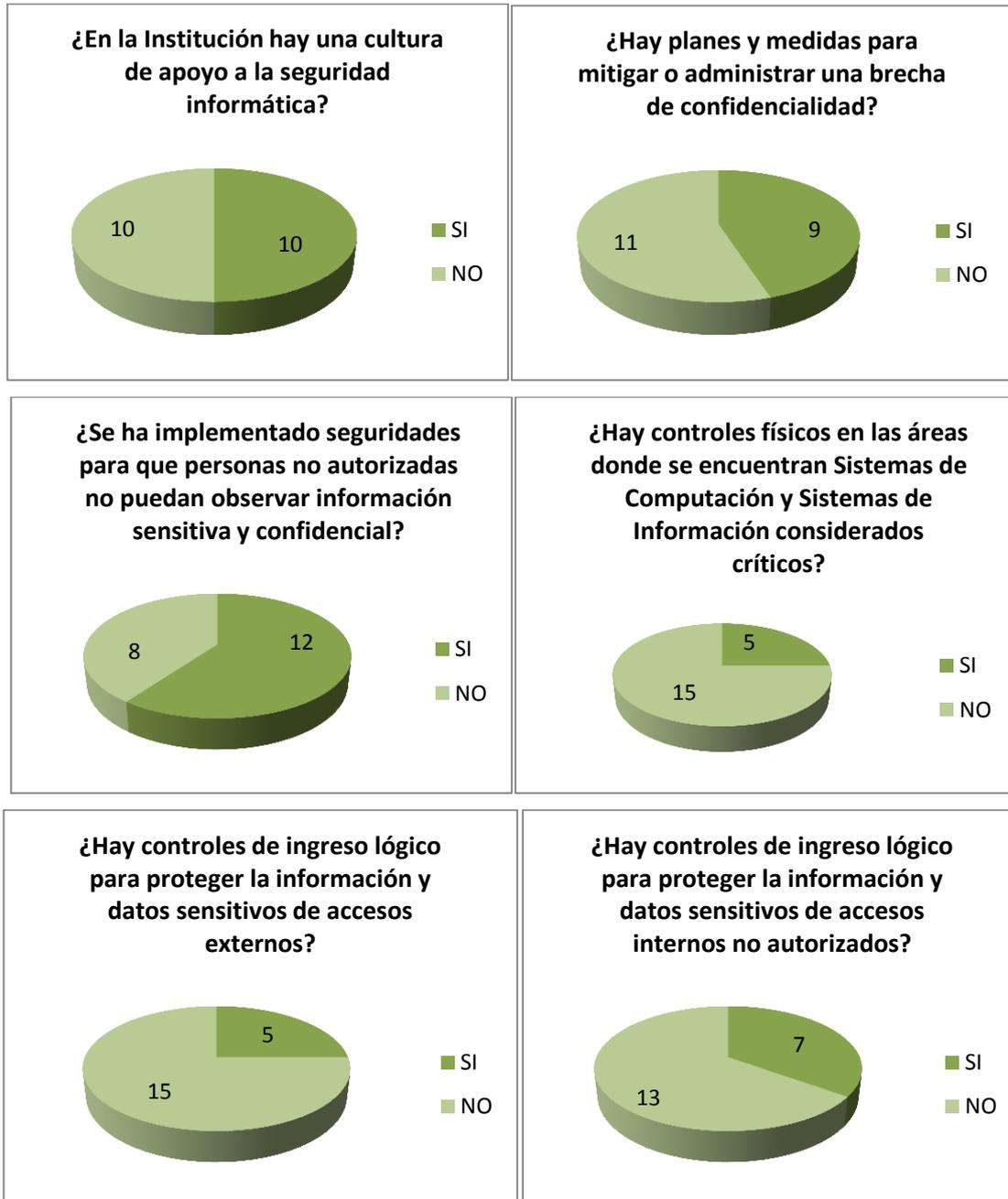
¿Existe vigilancia en el departamento de cómputo las 24 horas?

-
- ¿El personal ajeno a operaciones sabe qué hacer en el caso de una emergencia (incendio)?
 - ¿Existe salida de emergencia?
 - ¿Está definido el personal autorizado a acceder a los dispositivos y medios de almacenamiento de datos?
 - ¿Existe una clara definición de funciones entre los mandos de la institución respecto a la seguridad física?
 - ¿Se lleva una bitácora de las acciones de los operadores para evitar que realicen pruebas que puedan dañar los sistemas?
 - ¿Se controla el acceso a los archivos y programas en producción a los programadores, analistas y operadores?
 - ¿Se ha instruido al personal sobre qué medidas tomar en caso de que alguien pretenda entrar a las oficinas sin autorización?
 - ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?
 - ¿Se hacen copias de seguridad de la información considerada importante en su departamento?
 - ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora/servidores?
 - ¿Se tienen establecidos procedimientos de actualización a estas copias?
 - ¿Se tienen establecidos procedimientos de verificación de estas copias?
 - ¿Existe un sistema de video-vigilancia en su departamento/unidad?
 - ¿Se controla el acceso de equipos electrónicos a los ambientes de trabajo?
 - ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento en especial cerca a los equipos de cómputo?
-

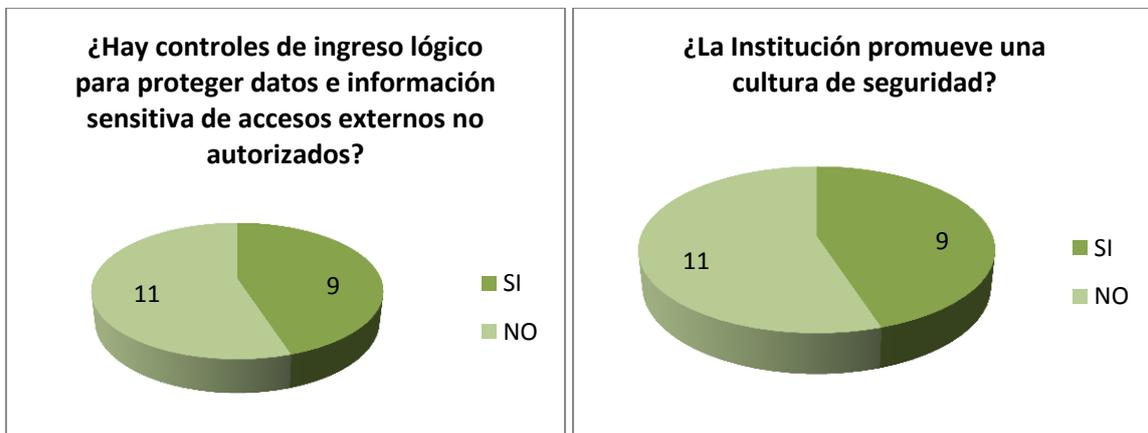
ANEXO 2

RESULTADOS DE LA ENCUESTA APLICADA

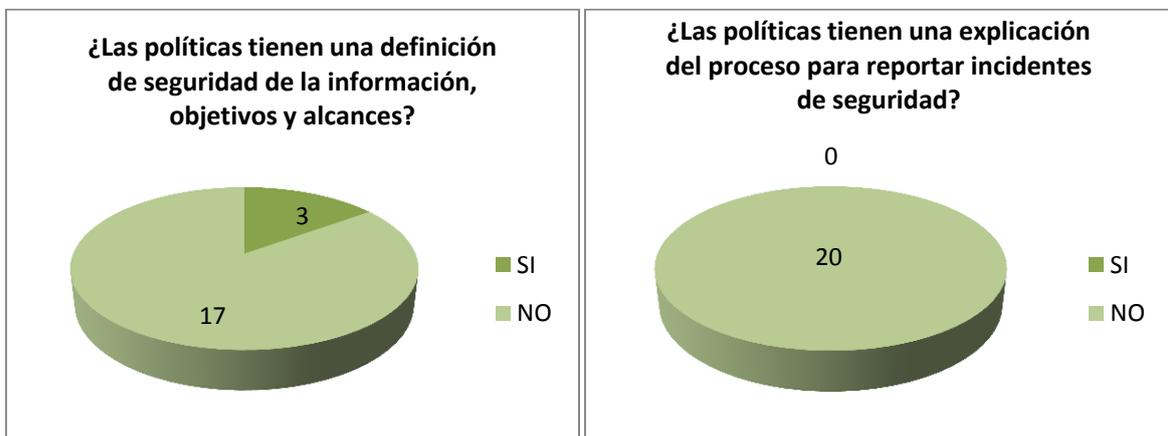
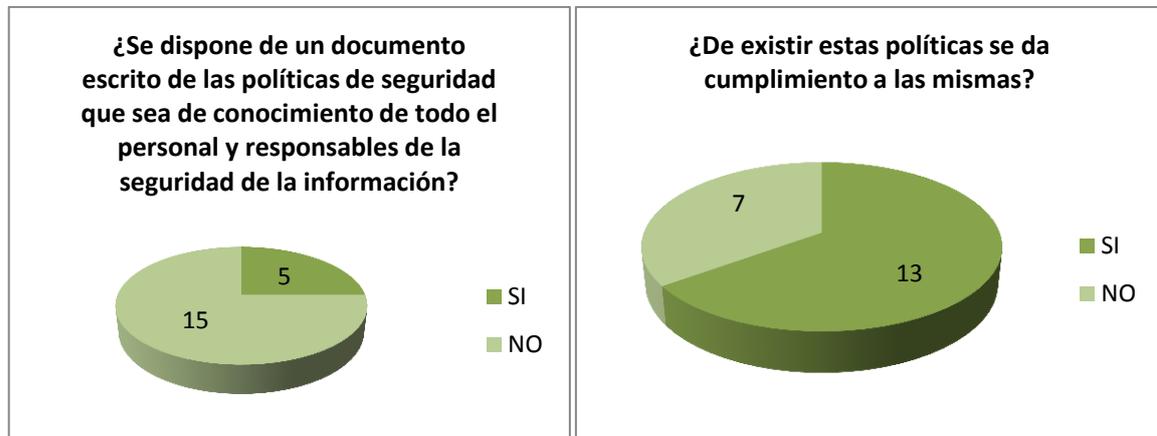
- **Indicador: *Confidencialidad de la Información***



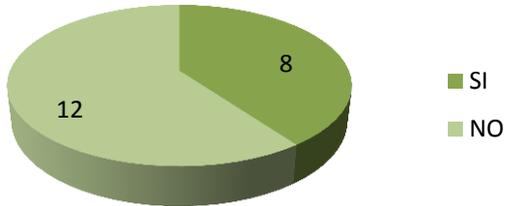
- **Indicador: *Integridad de la Información***



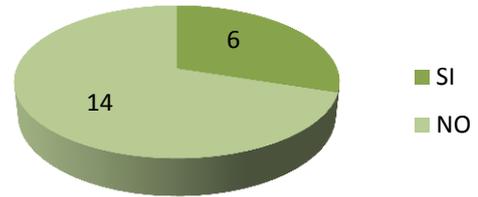
- **Indicador: Políticas de Seguridad**



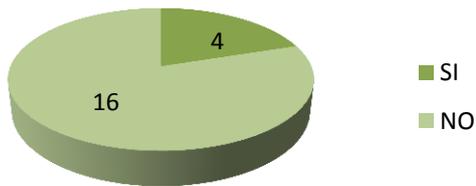
En caso de existir dicho listado de personal autorizado, ¿se incluye el tipo de acceso permitido?



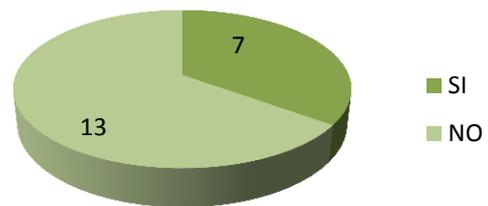
¿Existen procedimientos de asignación y distribución de contraseñas?



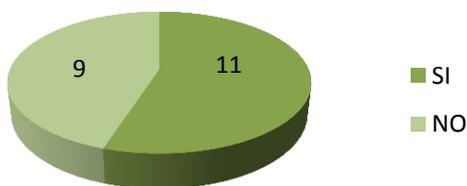
¿Se dispone de un documento escrito de las políticas de seguridad que sea de conocimiento de todo el personal y responsables de la seguridad de la información?



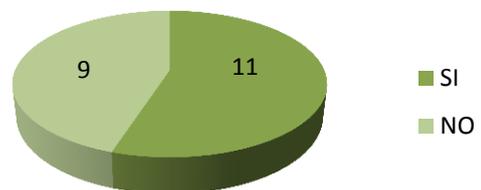
¿Los enunciados de las políticas son revisados periódicamente, incluyendo cambios en los niveles de responsabilidad?



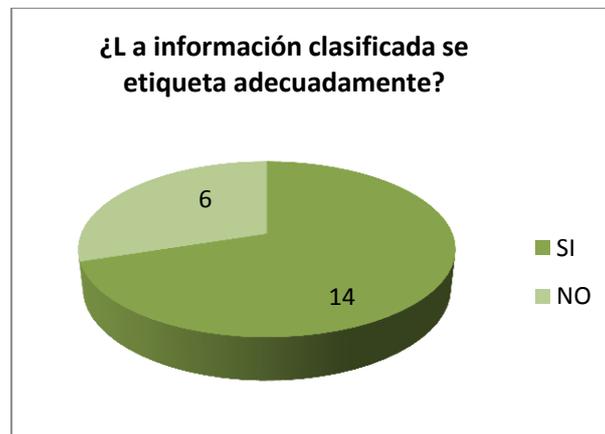
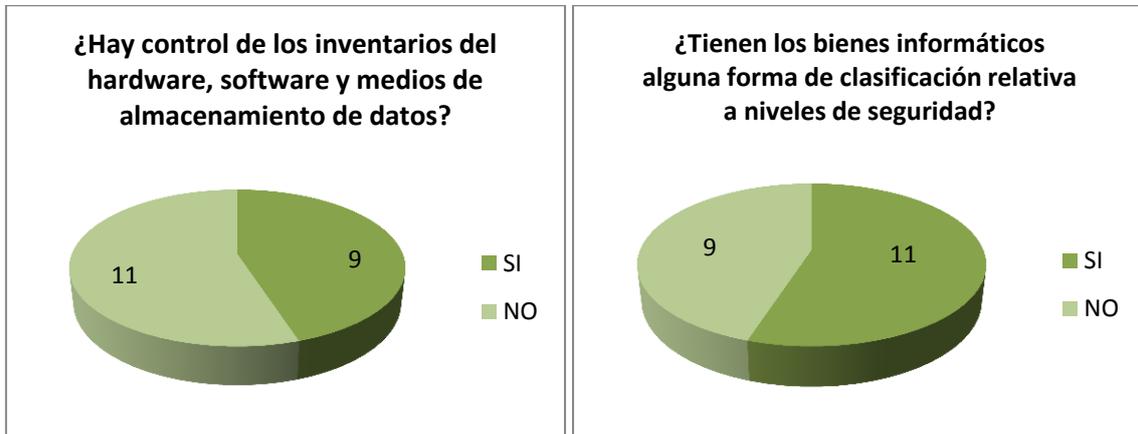
¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas?



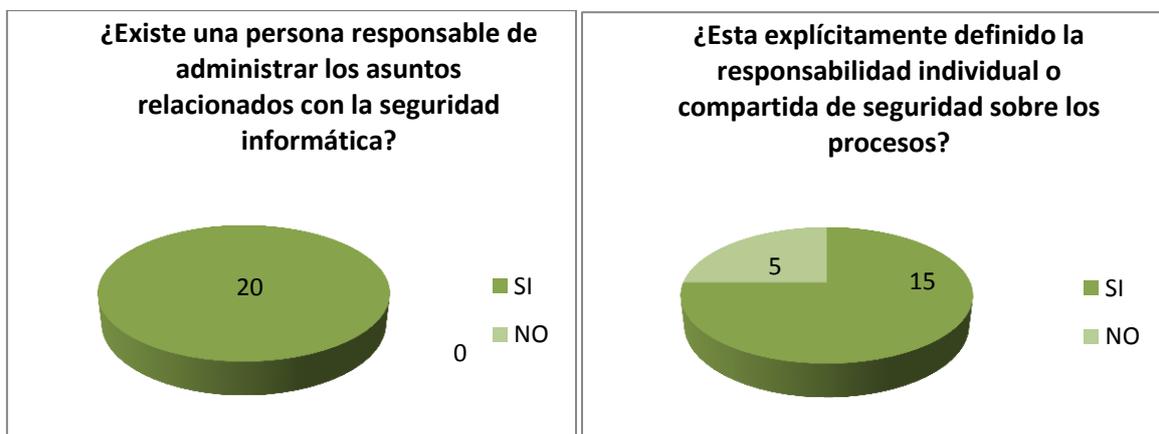
¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?



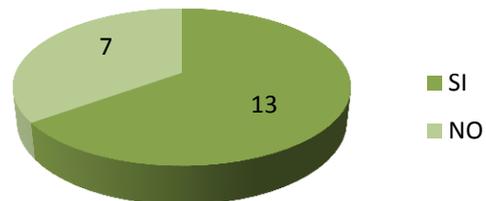
- **Indicador: Clasificación y Control de Valores**



- **Indicador: Aspectos organizativos para la seguridad**

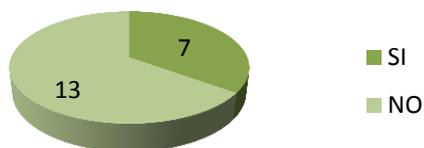


¿Los procesos de aprobación, adquisición e instalación de servicios para Tecnologías de Información en relación a seguridad son claros?

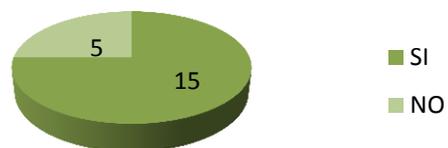


• **Indicador: Seguridad Física**

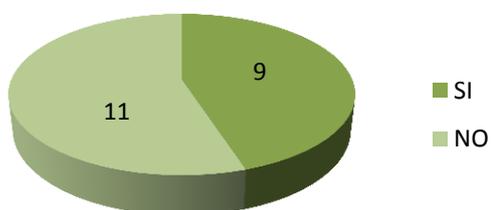
¿Está protegida la información que se transmite por cables de telecomunicaciones de forma que no es susceptible de interceptación?



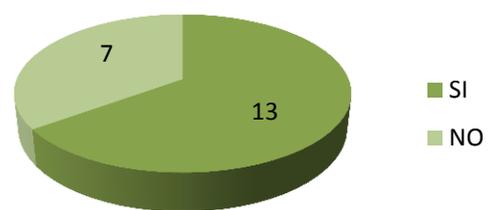
¿Los Sistemas de Cómputo y Sistemas de Información críticos están protegidos de acceso no autorizado y están ubicados en áreas seguras?



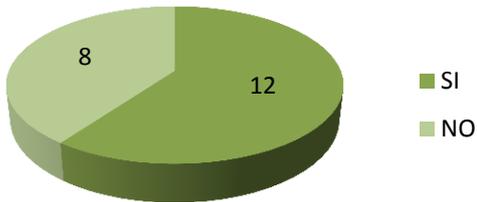
¿Los Sistemas Computacionales y Sistemas de Información están protegidos contra las fallas eléctricas?



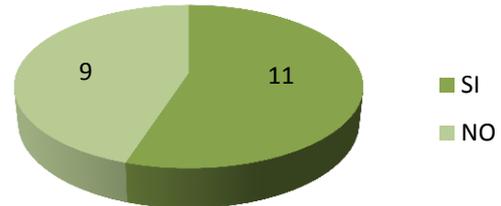
¿Los Sistemas de Computo son ubicados pensando en su protección ante posibles amenazas ambientales (incendio, inundación, terremoto)?



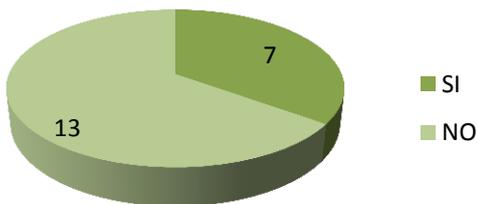
¿Está definido el personal autorizado a acceder a los locales donde se encuentran ubicados los sistemas que procesan información?



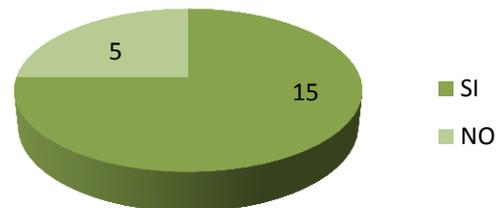
¿Existe una persona responsable de la seguridad física a nivel del departamento/unidad?



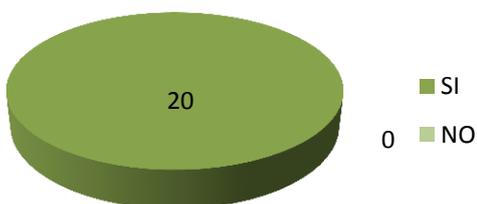
¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad física?



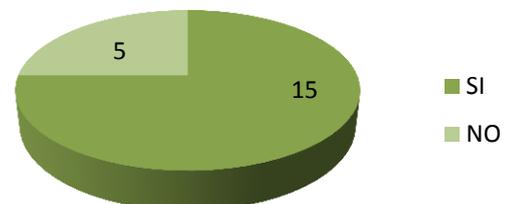
¿Existe personal de vigilancia en la institución?



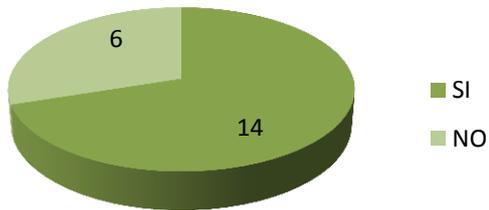
¿Existe vigilancia en el departamento de cómputo las 24 horas?



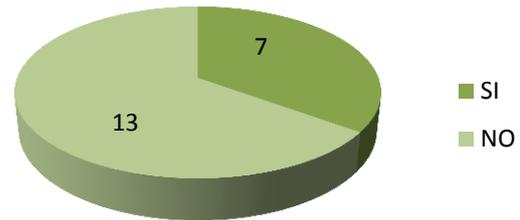
¿El personal ajeno a operaciones sabe qué hacer en el caso de una emergencia (incendio)?



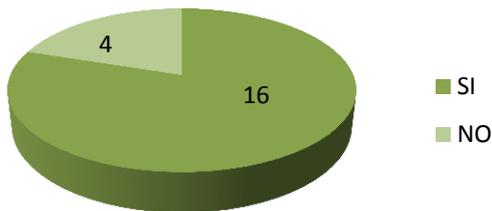
¿Existe salida de emergencia?



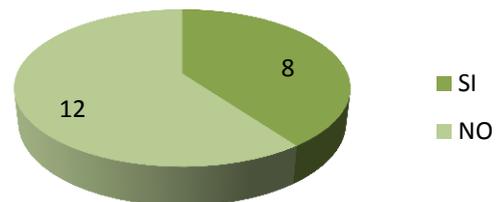
¿Está definido el personal autorizado a acceder a los dispositivos y medios de almacenamiento de datos?



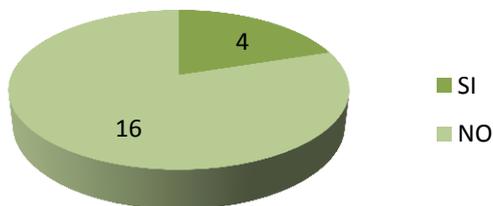
¿Existe una clara definición de funciones entre los mandos de la institución respecto a la seguridad física?



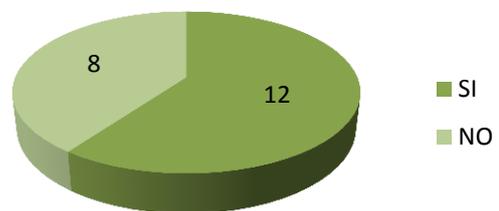
¿Se lleva una bitácora de las acciones de los operadores para evitar que realicen pruebas que puedan dañar los sistemas?



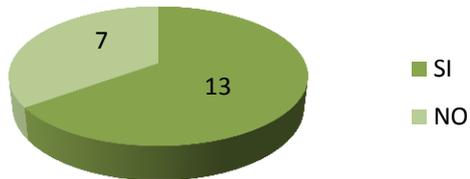
¿Se controla el acceso a los archivos y programas en producción a los programadores, analistas y operadores?



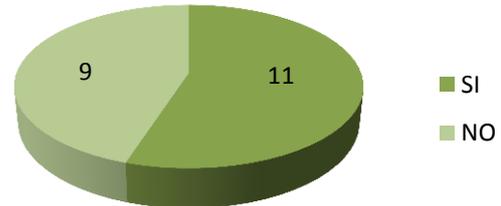
¿Se ha instruido al personal sobre qué medidas tomar en caso de que alguien pretenda entrar a las oficinas sin autorización?



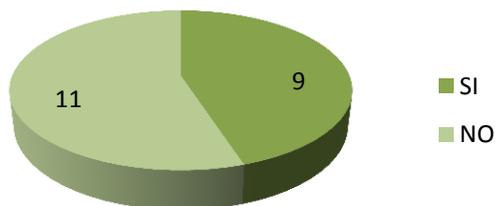
¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?



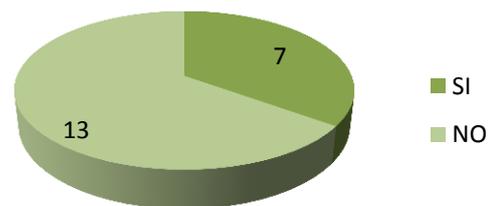
¿Se hacen copias de seguridad de la información considerada importante en su departamento?



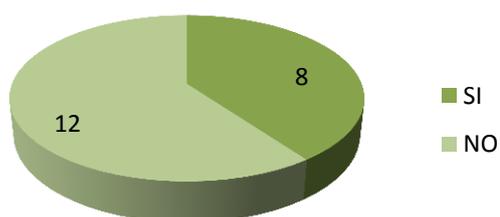
¿Se cuenta con copias de los archivos en lugar distinto al de la computadora/servidores?



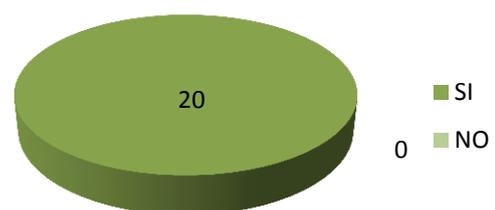
¿Se tienen establecidos procedimientos de actualización a estas copias?

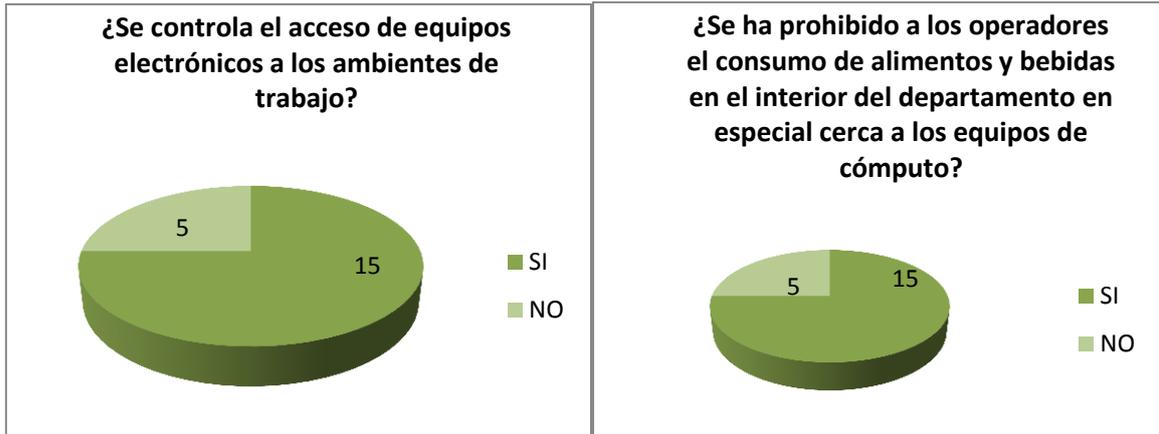


¿Se tienen establecidos procedimientos de verificación de estas copias?



¿Existe un sistema de video-vigilancia en su departamento/unidad?





ANEXO 3

CÁLCULO DE RIESGO DE ACTIVOS MATERIALES

A continuación se citan los activos materiales del CP-12:

- **Convertidor TP-LINK WDM Fast Ethernet**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 12. Cálculo de riesgo del Convertidor TP-LINK

- **Router ADSL 877 Vo4**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 13. Cálculo de riesgo del Router ADSL

- **Servidor Proxy**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 14. Cálculo de riesgo del Servidor Proxy

- **Routerboard Mikrotik RG-ENT**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 15. Cálculo de riesgo del router Mikrotik

- **Switch D-Link 10-100**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 16. Cálculo de riesgo del Switch D-Link

- **Antena Omnidireccional**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 17. Cálculo de riesgo de la antena

- **Nano Station 2.4 GHz**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 18. Cálculo de riesgo del Nano Station

- **Computadores de escritorio completos**

$$\begin{aligned} \text{Riesgo} &= 4.5 * 2 * 3 \\ \text{Riesgo} &= 27 \end{aligned}$$

Ecuación 19. Cálculo de riesgo de PC's de escritorio

- **UPS Central**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 20. Cálculo de riesgo del UPS Central

- **Generador eléctrico**

$$\begin{aligned} \text{Riesgo} &= 5 * 2 * 3 \\ \text{Riesgo} &= 30 \end{aligned}$$

Ecuación 21. Cálculo de riesgo del generador eléctrico

- **Impresoras multifunción**

$$\begin{aligned} \text{Riesgo} &= 2 * 2 * 3 \\ \text{Riesgo} &= 12 \end{aligned}$$

Ecuación 22. Cálculo de riesgo de Impresoras multifunción

- **Impresoras láser**

$$\text{Riesgo} = 2 * 2 * 3$$

$$\text{Riesgo} = 12$$

Ecuación 23. Cálculo de riesgo de Impresoras láser

- **Copiadoras**

$$\text{Riesgo} = 2 * 2 * 3$$

$$\text{Riesgo} = 12$$

Ecuación 24. Cálculo de riesgo de las copiadoras

ANEXO 4

INSTALACIÓN DE SAMBA 4

Previo a la instalación se debe asignar la dirección IP del servidor (10.10.1.194), para esto se debe escribir la siguiente línea de código en la consola de configuración.

```
nano /etc/hosts
```

Se abre una ventana con la siguiente información:

```
127.0.0.1 localhost
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
```

En esta ventana se debe ingresar la dirección IP del servidor y el dominio al que pertenece, el script editado queda de la siguiente manera:

```
127.0.0.1 localhost
10.10.1.194 ad01.policia.gob.ec ad01
# The following lines are desirable for IPv6 capable hosts
#::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
```

Una vez editado el script, Guardar (Ctrl + O) y Salir (Ctrl + X).

Para iniciar la instalación, escribir la siguiente línea de código:

```
apt-get install samba4
```

Esta instrucción descarga todos los paquetes necesarios para la instalación de Samba 4.

Se debe abrir el fichero que se indica a continuación, para editarlo:

```
nano /var/lib/dpkg/status
```

Dentro del fichero se debe cambiar:

```
"half-configured" con "installed"
```

Una vez editado el script, Guardar (Ctrl + O) y Salir (Ctrl + X).

Para continuar con la configuración se debe remover el archivo smb.conf, para lo cual se debe ingresar la siguiente línea de código:

```
rm /etc/samba/smb.conf
```

La siguiente línea permite definir el dominio y la clave de administrador para el Controlador de Dominio:

```
/usr/share/samba/setup/provision --realm=policia.gob.ec --domain=POLICIA --adminpass='miclave' --  
server-role=dc
```

Donde 'realm' es el dominio real, 'domain' es el identificador del dominio y adminpass es la clave de administrador.

Para iniciar Samba4, escribir las siguientes líneas de código:

```
samba -iM single -d 4  
initctl start samba4
```

Ahora es necesario instalar los clientes de Samba4, para lo cual escribir:

```
apt-get install samba4-clients
smbclient -L localhost -U%
```

DC necesita de un servidor de nombre de dominios (DNS), para esto se debe instalar bind9, como se muestra a continuación:

```
apt-get install bind9
```

Para editar el archivo named.conf, se debe escribir lo siguiente:

```
nano /etc/bind/named.conf
```

Incluir la siguiente línea dentro del archivo named.conf:

```
include "/var/lib/samba/private/named.conf";
```

Una vez editado el script, Guardar (Ctrl + O) y Salir (Ctrl + X).

En el archivo named.conf.options, se debe incluir las siguientes líneas:

```
nano /etc/bind/named.conf.options

dnssec-validation no;
auth-nxdomain no; # conform to RFC1035
listen-on-v6 { any; };
allow-query { any; };
allow-recursion { any; };
tkey-gssapi-keytab "/var/lib/samba/private/dns.keytab";
```

Una vez editado el fichero, Guardar (Ctrl + O) y Salir (Ctrl + X).

Para editar el siguiente archivo, ingresar la línea a continuación:

```
nano /etc/apparmor.d/usr.sbin.named
```

Agregar

```
/var/lib/samba/private/** rwk,
/var/lib/samba/private/dns/** rwk,
/usr/lib/i386-linux-gnu/samba/bind9/** rwm,
/usr/lib/i386-linux-gnu/samba/gensec/** rwm,
/usr/lib/i386-linux-gnu/ldb/modules/ldb/** rwm,
/usr/lib/i386-linux-gnu/samba/ldb/** rwm,
/var/tmp/** rw,
```

Una vez editado el script, Guardar (Ctrl + O) y Salir (Ctrl + X).

Ahora se debe reiniciar los servicios, para esto escribir las siguientes líneas

```
/etc/init.d/apparmor restart
/etc/init.d/bind9 restart
```

Si todo está funcionando correctamente, se muestra OK al reiniciar los servicios.

Instalar el mecanismo de autenticación de kerberos el cual permite autenticar sistemas Windows en sistemas Linux.

```
apt-get install krb5-user

cp /var/lib/samba/private/krb5.conf /etc
ln -s /var/lib/samba/private/dns.keytab /etc/krb5.keytab
kinitadministrator@POLICIA.GOB.EC

klist -e
```

Instalar un servidor de tiempo el cual sincroniza la hora del servidor con la de los clientes.

```
apt-get install ntp
nano /etc/ntp.conf
server pdc.policia.gob.ec

ntpdate -B pdc.policia.gob.ec
/etc/init.d/ntprestart
ntpq -p
```

Los usuarios con acceso de búsqueda en un archivo o directorio pueden recuperar una lista de nombres de atributos definidos para ese archivo o directorio, por lo que es necesario asociar un fichero o directorio a un usuario definidos en los nodos a nivel de filesystem.

```
apt-get install attr
touch test.txt
setfattr -n user.test -v test test.txt
setfattr -n security.test -v test2 test.txt
getfattr -d test.txt
getfattr -n security.test -d test.txt
/etc/init.d/samba4 restart
```

Para finalizar se establece como propietario a bind de los ficheros de autenticación del DNS.

```
chownbind:bind /var/lib/samba/private/dns.keytab
chownbind:bind /var/lib/samba/private/dns
```

ADMINISTRACIÓN DEL CONTROLADOR DE DOMINIO DESDE WINDOWS XP

Para poder administrar el servidor con DC desde una máquina con Windows XP se debe instalar un paquete de herramientas de administración de Windows Server 2003 Service Pack 2 para las ediciones x86.

El paquete de herramientas de administración permite a los administradores instalar las herramientas de administración de Windows Server 2003 SP2 en un equipo en el que se esté utilizando un sistema operativo de la familia de Windows Server 2003 o bien Windows XP Professional, con el fin de realizar funciones de administración de un servidor remoto.

El paquete que se debe descargar es:

WindowsServer2003-KB340178-SP2-x86-ESN.msi

Como se muestra en la *Figura 221*:



Figura 221. Paquete de herramientas de administración para Windows XP
 Fuente: <http://www.microsoft.com/en-us/download/details.aspx?id=6315>

Una vez que se haya descargado el paquete, hacer doble clic en él para que se ejecute, como se muestra en la *Figura 222*.



Figura 222. Ejecución del paquete de herramientas
 Fuente: Captura de la instalación

Clic en el botón Ejecutar para que empiece la instalación.
La *Figura 223* muestra el proceso de instalación:

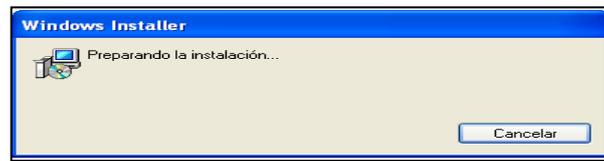


Figura 223. Proceso de instalación del paquete
Fuente: Captura de la instalación

Cuando se está iniciando la instalación aparece la ventana que se muestra en la *Figura 224*, dar clic en el botón Siguiente:



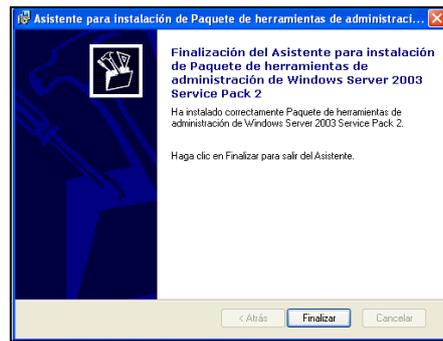
Figura 224. Inicio de instalación del paquete
Fuente: Captura de la instalación

Esperar mientras se instalan todos los componentes del paquete, la *Figura 225*, muestra el progreso de la instalación.



Figura 225. Progreso de la instalación
Fuente: Captura de la instalación

Cuando se haya terminado de instalar el paquete aparece una ventana como se muestra en la *Figura 226*, dar clic en Finalizar.



*Figura 226. Finalización de la instalación
Fuente: Captura de la instalación*

De esta manera ya es posible administrar el servidor desde una PC con Windows XP.

ADMINISTRACIÓN DEL DC DESDE WINDOWS 7

Las herramientas de administración remota del servidor para Windows 7 con SP1 permiten a los administradores de TI administrar funciones y características instaladas desde un equipo remoto que ejecuta Windows 7 o Windows 7 con SP1.

El paquete que se debe descargar es:

WindowsServer2003-KB340178-SP2-x86-ESN.msi

Como se muestra en la *Figura 227*:



*Figura 227. Paquete de herramientas de administración para Windows 7
Fuente. <http://www.microsoft.com/en-us/download/details.aspx?id=7887>*

Abrir la carpeta en la que se ha descargado el paquete, hacer doble clic en él para desempaquetarlo y a continuación se inicia el Asistente para la instalación de las

Herramientas de administración remota del servidor para Windows 7 con SP1, como se muestra en la *Figura 228*.

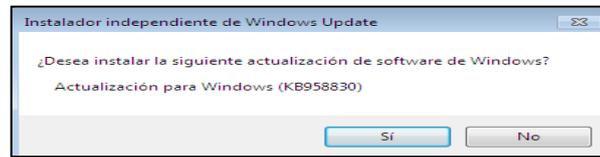


Figura 228. Asistente para la instalación de herramientas de administración
Fuente: Captura de la instalación

Aceptar las Condiciones de la licencia y la Garantía limitada para instalar el paquete de Herramientas de administración. La *Figura 229* muestra esta ventana.



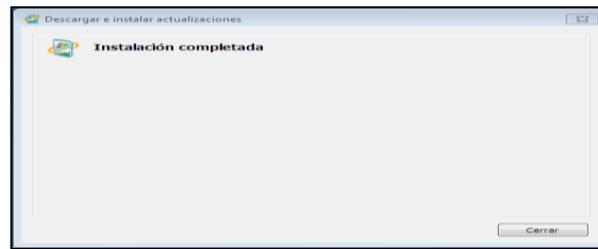
Figura 229. Términos de licencia del software de Microsoft
Fuente: Captura de la instalación

La *Figura 230* muestra el inicio de la instalación.



Figura 230. Inicio de la instalación del paquete
Fuente: Captura de la instalación

Completar todos los pasos necesarios del asistente y hacer clic en Finalizar para salir del asistente cuando la instalación haya finalizado, como se muestra en la *Figura 231*.



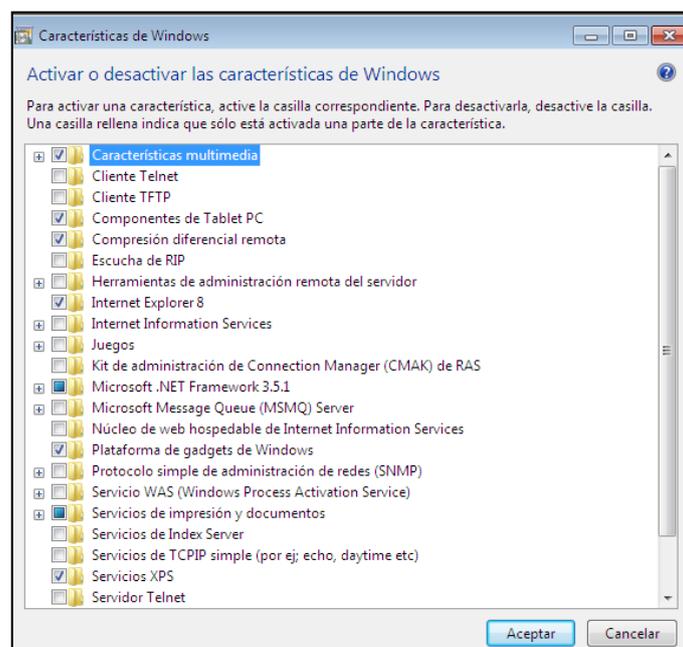
*Figura 231. Instalación terminada
Fuente: Captura de la instalación*

Hacer clic en Inicio, Panel de control y, a continuación, en Programas.

En la sección Programas y características, hacer clic en Activar o desactivar las características de Windows. Si el Control de cuentas de usuario pide que permita que se abra el cuadro de diálogo de las características de Windows, hacer clic en Continuar.

En el cuadro de diálogo Características de Windows, expandir las Herramientas de administración remota del servidor. Seleccionar las Herramientas de administración remota que desea instalar. Hacer clic en Aceptar.

La *Figura 232* muestra las herramientas de administración.



*Figura 232. Herramientas administrativas
Fuente: Captura de la instalación*

Los accesos directos para los complementos instalados por las Herramientas de administración remota del servidor para Windows 7 con SP1 se agregan a la lista de Herramientas administrativas del menú Inicio.

De esta manera ya es posible administrar el servidor desde una PC con Windows 7.

ANEXO 5 INSTALACIÓN DE ITALC

La instalación de la aplicación se la divide en dos partes, la del maestro y la de los clientes.

- **INSTALACIÓN DEL MAESTRO**

Es recomendable tener el sistema actualizado por lo que se debe realizar el siguiente procedimiento:

- ~ Abrir el Terminal de Ubuntu
- ~ Escribir la siguiente línea: *sudo apt-get update*.
- ~ Presionar la tecla Enter.
- ~ Escribir *sudo apt-get upgrade*.
- ~ Presionar Enter.

Antes de iniciar con la instalación se debe buscar en los repositorios los componentes necesarios para que iTALC funcione correctamente, para esto abrir un terminal y escribir la siguiente línea:

```
apt-cache search italc
```

La *Figura 233* muestra los componentes necesarios que iTALC necesita para su funcionamiento.

```
root@ubuntu:~# apt-cache search italc
italc-client - Enseñanza y aprendizaje inteligentes con computadores (parte cli
ente)
italc-master - Enseñanza y aprendizaje inteligente con computadoras (parte maes
tra)
libitalc - Intelligent Teaching and Learning with Computers (library)
```

Figura 233. Componentes necesarios para la instalación de iTALC
Fuente: Capturas mediante putty

Una vez hecho esto, se procede a la instalación de los paquetes ITALC-Master, ITALC-Client y libitalc, para ello escribir en el terminal la siguiente línea:

```
apt-get install italc-client italc-master libitalc
```

Con esto se instala el paquete completo con la última versión estable del maestro (ITALC Master Application) y la versión del cliente (ITALC Client Application).

Configuración del Maestro

Una vez instalada la aplicación proceder a ejecutarla desde el terminal escribiendo la palabra *italc*, presionar la tecla *Enter* y se visualizan las siguientes pantallas de error.

La *Figura 234*, muestra la primera pantalla de error que aparece porque aún no se ha creado ninguna clase dentro del programa, hacer clic en *Aceptar* para continuar con la configuración.

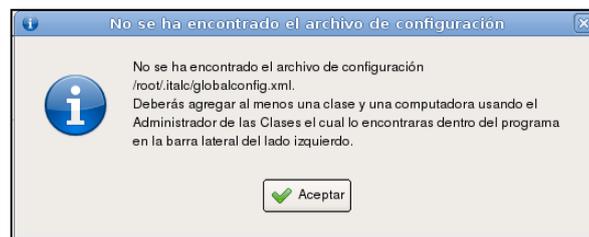


Figura 234. Ventana de error debido a que no se han agregado clases
Fuente: Captura de la configuración de iTALC

Aparece la segunda pantalla de error en la configuración, como se muestra en la *Figura 235*, esto se debe a que todavía no se han generado las claves de autenticación, hacer clic en *Aceptar* para continuar.



Figura 235. Ventana de error debido a la no generación de claves
Fuente: Captura de la configuración de iTALC

Finalmente, la última ventana de error indica que aún no se han configurado las claves pública y privada lo que impide que la aplicación se ejecute, como se muestra en la *Figura 236*.



Figura 236. Ventana de error debido a la no configuración de claves
Fuente: Captura de la configuración de iTALC

Para solucionar estos problemas se procede a generar las claves de autenticación (privada y pública) en el equipo maestro y copiar la clave pública desde este equipo a cada uno de las computadoras de los clientes.

Generación de claves

La siguiente instrucción crea dos archivos con el mismo nombre *key* pero en directorios diferentes */etc/italc/keys/public/teacher* y */etc/italc/keys/private/teacher* la primera es la clave pública y la segunda es la clave privada.

```
sudoica -role teacher -createkeypair
```

Si todo se ha hecho correctamente debe aparecer el siguiente mensaje:

```
creating new key-pair ... saved key-pair in
/etc/iTALC/keys/private/teacher/key
/etc/iTALC/keys/public/teacher/key

For now the file is only readable by root and members of group root
(if you didn't ran this command as non-root).

I suggest changing the ownership of the private key so that the file is
readable by all members of a special group to which all users belong
who are allowed to use ltaic
```

- Clave Privada

La llave privada ubicada en */etc/italc/keys/private/teacher/key* debe poseer únicamente permisos de lectura y ser accesible sólo por los usuarios que ejecutarán iTALC. Lo correcto es introducir todos los usuarios que van a ejecutar iTALC en un grupo por ejemplo llamado iTALC. Además se debe cambiar la propiedad del fichero (el grupo al que pertenece) que contiene esta clave y asignarle los permisos necesarios únicamente a este grupo.

Creación del grupo

```
# addgroupitalc
```

Creación de usuarios

```
# useradd -m nuevo_usuario
```

Ahora se debe incluir a él o los usuarios creados dentro del grupo italc:

```
#adduser nuevo_usuario italc
```

Finalmente se debe cambiar el grupo al que pertenece este fichero, y establecer los permisos necesarios para el grupo ejecutando para ello las siguientes instrucciones:

```
#chgrp -R iTALC /etc/italc/keys/private
#chmod -R o-rwx /etc/italc/keys/private/
```

- Clave Pública

La clave pública que se ha generado en el equipo maestro se encuentra ubicada en el directorio

`/etc/iTALC/keys/public/teacher/key` y es utilizada por el equipo maestro para autenticarse con los clientes por lo cual debe copiarse en todos los equipos clientes.

Inicio del Servicio

La aplicación de iTALC maestro está basado en un entorno gráfico, por lo que es necesario editar dos ficheros correspondientes a gdm que es el servicio que maneja el entorno gráfico. Los archivos a editar son los siguientes:

```
sudoedit /etc/gdm/Init/Default
sudoedit /etc/gdm/PreSession/Default
```

En todas las máquinas que van hacer la función de maestro, hay que incluir las órdenes siguientes en los 2 ficheros descritos anteriormente, al inicio justo por debajo de los comentarios:

```
killallica          # Mata cualquier sesión previa que esté ejecutándose
/usr/local/bin/ica6  # Inicia el servicio
```

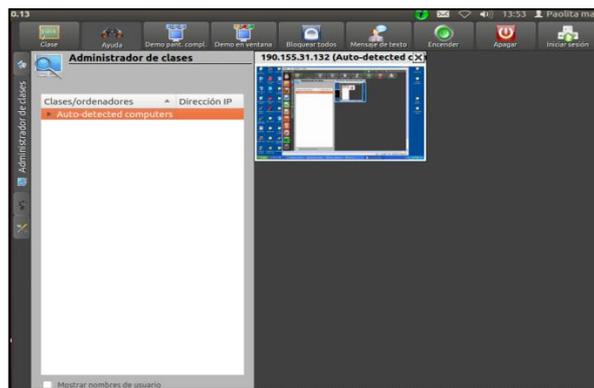
Realizados los cambios mencionados anteriormente se procede a reiniciar el servicio gdm para que los cambios tengan efecto.

```
# /etc/init.d/gdmrestart
```

Finalmente se procede a ejecutar la aplicación digitando para ello en un terminal de comandos la siguiente instrucción:

```
# italc
```

Con ello se abrirá la ventana correspondiente a iTALC maestro tal como se muestra en la *Figura 237*:



*Figura 237. Ventana principal de iTALC master
Fuente: Captura de la aplicación iTALC*

- **INSTALACIÓN DE LOS CLIENTES**

Italc master puede monitorear clientes Windows y Linux pero dentro del CP-12 todos los usuarios utilizan una plataforma Windows por lo que se describe la instalación de la aplicación iTALC únicamente para este sistema operativo.

- **Cliente Windows**

Se describe el proceso de instalación de la versión 1.0.8 de iTALC en Microsoft Windows XP.

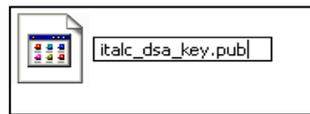
Primero se debe poseer la clave pública del maestro iTALC. El inconveniente que surge al usar la clave del maestro proveniente de una máquina Linux para la instalación del cliente en Windows XP, es que el archivo "key" (clave pública del maestro), no tiene extensión, por lo que no es detectada por el instalador iTALC en Windows como una clave de tipo pública.

En este caso la clave pública del maestro se ha copiado en una memoria flash en la carpeta `\iTALC final\publickey del maestro\` como se ve en la *Figura 238*.



*Figura 238. Clave pública del maestro de Linux
Fuente: Captura de pantalla en Windows XP*

Hacer clic derecho sobre el archivo y seleccionar *Cambiar nombre* y reemplazar “key” por “italc_dsa_key.pub” y presionar *Enter*, como se indica en la *Figura 239*.



*Figura 239. Cambio de nombre y extensión a la clave pública del maestro
Fuente: Captura de pantalla en Windows XP*

Como se puede observar en la *Figura 240*, Windows XP detecta el cambio de extensión en el archivo porque se ha añadido la extensión “.pub” equivalente a público, ya que en Windows existe la herramienta Microsoft Office Publisher que casualmente trabaja con archivos cuya extensión es “.pub”, sin embargo esto no afecta en nada la instalación del cliente.



*Figura 240. Clave pública con extensión .pub
Fuente: Captura de pantalla en Windows XP*

Para proseguir con la instalación, descargar la aplicación iTALC (<http://sourceforge.net/projects/iTALC/>), descomprimir el archivo

donde se desee y ejecutar el Setup.exe con un doble clic. Aparece una pantalla de Bienvenida como se indica en la *Figura 241*, hacer clic en *Next* para continuar.



Figura 241. Pantalla de inicio de instalación de Italc
Fuente: Captura de pantalla en Windows XP

En la ventana siguiente aceptar los términos de la licencia, para ello seleccionar *I agree* y hacer clic en *Next*, como se muestra en la *Figura 242*.

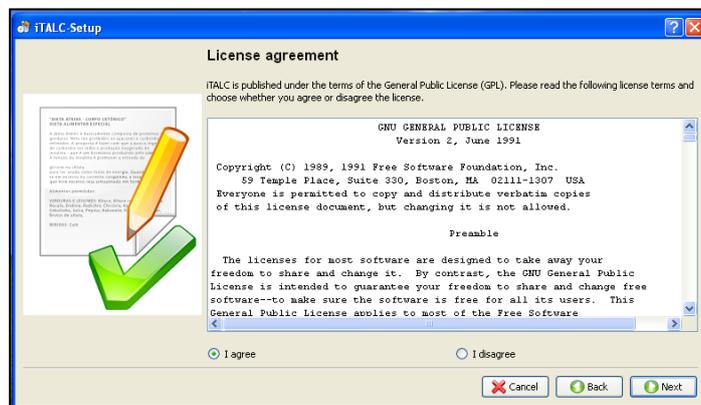


Figura 242. Términos de la licencia de Italc
Fuente: Captura de pantalla en Windows XP

Seleccionar la ubicación donde se va a instalar iTALC (es recomendable la ubicación por default) y hacer clic en *Next*, como muestra la *Figura 243*.



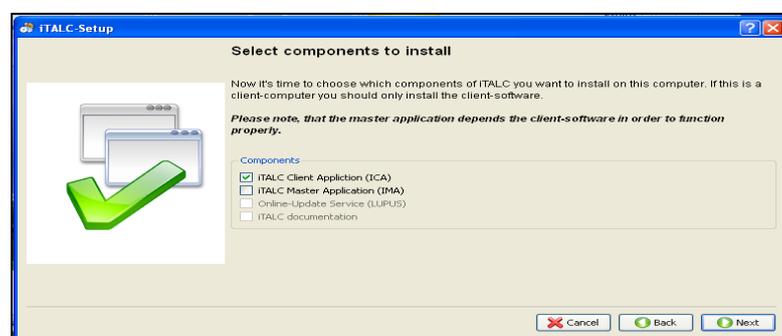
*Figura 243. Ubicación de la instalación
Fuente: Captura de pantalla en Windows XP*

En la ventana que se muestra en la *Figura 244*, hacer clic en **Sí**, para crear la carpeta o directorio de instalación.



*Figura 244. Creación del directorio de instalación
Fuente: Captura de pantalla en Windows XP*

En la pantalla que se muestra en la *Figura 245*, se puede escoger una instalación maestra o cliente, pero en este caso sólo se desea instalar un cliente por lo que se elige la opción del cliente (ICA) y presionar el botón *Next*.



*Figura 245. Selección del cliente iTALC
Fuente: Captura de pantalla en Windows XP*

La *Figura 246*, muestra la ventana de opciones de seguridad y por defecto está seleccionada la segunda opción, aquí se debe hacer clic en la imagen de la carpeta ubicada a la derecha.



Figura 246. Opciones de importación de clave pública
Fuente: Captura de pantalla en Windows XP

Una vez hecho esto se debe buscar la ubicación de la clave pública del maestro, en este caso en la unidad flash *E:\ITALC final\publickey del maestro* y presionar *Aceptar*, como se muestra en la *Figura 247*.



Figura 247. Ubicación de la clave pública
Fuente: Captura de pantalla en Windows XP

Si la clave pública ha sido aceptada se habilita el botón *Next*, lo que significa que se puede seguir con la instalación, ya que en paso anterior estaba bloqueada.

Por último presionar el botón *Finalizar*.

Aparece una pantalla de confirmación de que los servicios de iTALC cliente fueron registrados correctamente, como se indica en la *Figura 248*, clic en *OK*.

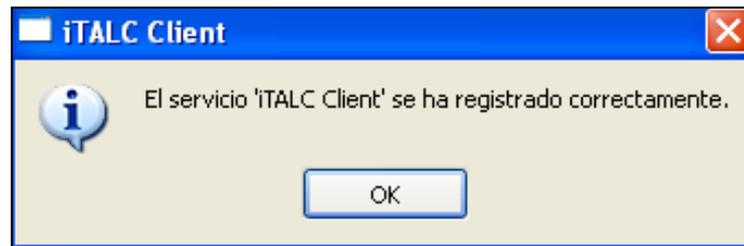


Figura 248. Servicio ITALC registrado
Fuente: Captura de pantalla en Windows XP

Finalmente se terminará con la instalación presionando el botón *Quit*, como se muestra en la *Figura 249*.



Figura 249. Instalación Finalizada
Fuente: Captura de pantalla en Windows XP

ANEXO 6

INSTALACIÓN DE NAGIOS 3 Y NCONF

La herramienta de monitoreo NAGIOS3 necesita de los siguientes paquetes para que funcione de manera adecuada, para esto el primer paso es instalarlos:

```
apt-get install build-essential libgd2-xpm-dev apache2 php-pearrrdtool librrds-perl php5-gd php5-common
php5 libapache2-mod-php5
```

Reiniciar el servicio apache2 con el siguiente comando:

```
/etc/init.d/apache2 restart
```

Para instalar esta herramienta de monitoreo se ejecuta el siguiente comando:

```
apt-get install nagios3 nagios-plugins
```

En el proceso de instalación aparecerá una ventana como la que se muestra en la *Figura 250*:

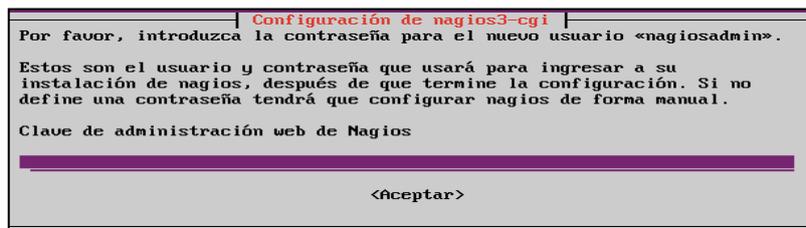


Figura 250. Contraseña del administrador de Nagios
Fuente: Captura de pantalla de instalación de Nagios3

En esta ventana se ingresa la contraseña para el usuario administrador de nagios (nagiosadmin) y luego aparecerá otra ventana similar para la validación de dicha contraseña.

Finalmente, reiniciar el servicio de nagios3 con el siguiente comando:

```
/etc/init.d/nagios3 restart
```

Para instalar la herramienta de administración NCONF, se debe descargar el paquete y extraer en el directorio que se desea guardar. Las siguientes líneas de código muestran el proceso a realizarse.

```
mkdir ~/downloads
cd ~/downloads
wget http://sourceforge.net/projects/nconf/files/nconf/1.3.0-0/nconf-1.3.0-0.tgz
cd /var/www
tar zxvf ~/downloads/nconf-1.2.6-0.tgz
cd /var/www/nconf
chown www-data config output static_cfg temp
chmod 777 /usr/local/nagios/bin/nagios
```

- **Instalación de NCONF**

Crear enlace simbólico:

```
ln -s /usr/sbin/nagios3 /var/www/nconf/bin/
```

Setear permisos de escritura en los directorios

```
chmod 777 -R /var/www/nconf/config
```

```
chmod 777 -R /var/www/nconf/output
```

```
chmod 777 -R /var/www/nconf/static_cfg
```

```
chmod 777 -R /var/www/nconf/temp
```

Ejecutar en el navegador: http://ip_servidor/nconf/INSTALL.php, como se muestra en la *Figura 251*.



Figura 251. Instalación de NCONF vía web
Fuente: Captura de instalación de Nconf

El siguiente paso de la instalación es asociar la base de datos con esta herramienta, se debe ingresar la ip del servidor de la base de datos, el nombre de la base de datos, el nombre de usuario de la base de datos y la contraseña utilizada por el usuario, como se muestra en la *Figura 252*. Si los datos son correctos, hacer clic en *Next*.

Figura 252. Ingreso de información de la base de datos
Fuente: Captura de instalación de Nconf

La siguiente pantalla que aparece es la de configuración general, aquí se debe ingresar los directorios en donde se encuentran instaladas las herramientas. La *Figura 253* muestra esta pantalla. Hacer clic en *Next*.

Figura 253. Ingreso de directorios
Fuente: Captura de instalación de Nconf

Finalmente, se crean las configuraciones básicas como se muestra en la *Figura 254*. Todo debe aparecer en estado OK y una vez que se ha terminado de instalar hacer clic en *Finish*.

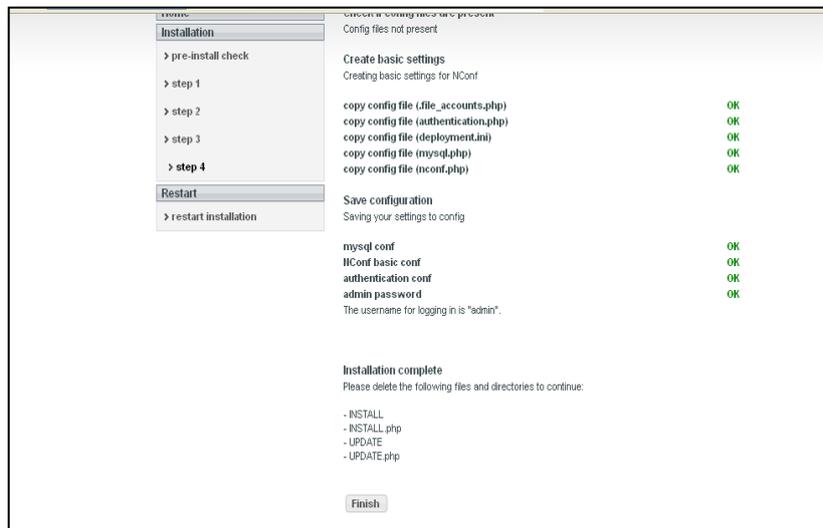


Figura 254. Instalación completa de Nconf
Fuente: Captura de instalación de Nconf

Una vez que se termina de instalar la herramienta se deben borrar los siguientes ficheros:

```
rm -rf /var/www/nconf/UPDATE*
rm -rf /var/www/nconf/INSTALL*
```

Para integrar la herramienta de administración NCONF con la herramienta de monitoreo NAGIOS3, borrar o comentar las líneas que inician con `cfg_file` del fichero:

```
nano /etc/nagios3/nagios.cfg
```

Agregar las líneas:

```
cfg_dir=/etc/nagios3/global
cfg_dir=/etc/nagios3/Default_collector
```

Crear el directorio:

```
mkdir /etc/nagios3/import
```

Modificar el fichero:

```
/var/www/nconf/ADD-DNS/deploy_local.sh
```

Cambiar las líneas:

```
OUTPUT_DIR="/var/www/nconf/output/"
```

```
NAGIOS_DIR="/etc/nagios3/"
```

```
/etc/init.d/nagios3 reload
```

Establecer permisos

```
chmod 755 /var/www/nconf/ADD-DNS/deploy_local.sh
```

Programar tarea

```
crontab -e
```

```
**** */var/www/nconf/ADD-DNS/deploy_local.sh
```

Generar configuración desde nconf

```
/var/www/nconf/ADD-DNS/deploy_local.sh
```

Reiniciar el servicio de nagios3

```
/etc/init.d/nagios3 restart
```

INDICADORES DE ESTADO

Cuando Nagios recopila la información de los servidores dentro de la red, muestra el estado de cada servicio monitoreado, si todos los servicios están arriba, estos se muestran en color verde como se indica en la *Figura 255*.

The screenshot shows the Nagios interface with a sidebar on the left containing navigation options like 'General', 'Monitoring', and 'Service Problems'. The main content area is titled 'Service Status Details For All Hosts' and displays a table with columns: Host, Service, Status, Last Check, Duration, Attempt, and Status Information. All services listed are in an 'OK' status.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Controlador de Dominio	check_ping	OK	2013-03-07 16:35:35	8d 8h 5m 43s	1/10	PING OK - Packet loss = 0%, RTA = 0.54 ms
	check_ssh	OK	2013-03-07 16:36:10	8d 8h 5m 8s	1/10	SSH OK - OpenSSH_5.9p1 Debian-SukuntuL1 (protocol 2.0)
	check_tcp	OK	2013-03-07 16:34:44	7d 21h 36m 34s	1/10	TCP OK - 0.001 second response time on port 135
	check_tcp_2	OK	2013-03-07 16:34:19	7d 21h 36m 59s	1/10	TCP OK - 0.001 second response time on port 389
TALC	check_ping	OK	2013-03-07 16:33:55	8d 3h 2m 23s	1/10	PING OK - Packet loss = 0%, RTA = 0.41 ms
	check_ssh	OK	2013-03-07 16:32:50	8d 3h 3m 28s	1/10	SSH OK - OpenSSH_5.9p1 Debian-SukuntuL1 (protocol 2.0)
	check_tcp	OK	2013-03-07 16:32:44	8d 2h 18m 34s	1/10	TCP OK - 0.001 second response time on port 5800
	check_tcp_2	OK	2013-03-07 16:31:39	8d 2h 19m 39s	1/10	TCP OK - 0.001 second response time on port 5900
Monitoreo	Current Load	OK	2013-03-07 16:33:51	8d 7h 52m 27s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	2013-03-07 16:34:41	8d 7h 51m 37s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	2013-03-07 16:35:31	8d 7h 50m 47s	1/4	HTTP OK: HTTP/1.1 200 OK - 453 bytes in 0.007 second response time
	PING	OK	2013-03-07 16:31:21	8d 7h 49m 57s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	Root Partition	OK	2013-03-07 16:32:11	8d 7h 49m 7s	1/4	DISK OK - free space: / 16462 MB (92% inode=94%)
	SSH	OK	2013-03-07 16:33:01	8d 7h 48m 17s	1/4	SSH OK - OpenSSH_5.3p1 Debian-SukuntuL4 (protocol 2.0)
	Swap Usage	OK	2013-03-07 16:34:16	8d 7h 52m 11s	1/4	SWAP OK - 100% free (11643 MB out of 11643 MB)
Servidor de Archivos	check_ping	OK	2013-03-07 16:32:53	8d 7h 53m 25s	1/10	PING OK - Packet loss = 0%, RTA = 0.45 ms
	check_ssh	OK	2013-03-07 16:33:45	8d 7h 52m 33s	1/10	SSH OK - OpenSSH_5.3p1 Debian-SukuntuL4 (protocol 2.0)
	check_tcp	OK	2013-03-07 16:34:37	8d 7h 51m 41s	1/10	TCP OK - 0.001 second response time on port 139
	check_tcp_2	OK	2013-03-07 16:35:29	8d 7h 50m 49s	1/10	TCP OK - 0.000 second response time on port 445
UTM	check_http	OK	2013-03-07 16:31:58	8d 7h 39m 20s	1/10	HTTP OK: HTTP/1.1 200 OK - 479 bytes in 0.002 second response time

Figura 255. Verificación del estado de los servicios: OK
Fuente: Captura de pantalla

Si existen problemas con los servicios monitoreados, Nagios mostrará el servidor en color rojo, como se indica en la Figura 256.

The screenshot shows the Nagios interface with a sidebar on the left. The main content area is titled 'Service Status Details For All Hosts' and displays a table with columns: Host, Service, Status, Last Check, Duration, Attempt, and Status Information. The 'SWP' host has a 'check_ping' service in a 'CRITICAL' status.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
SWP	check_ping	CRITICAL	2013-01-23 11:59:54	2d 23h 40m 55s	1/5	CRITICAL - Host Unreachable (192.168.1.6)
	check_ssh	CRITICAL	2013-01-23 11:51:03	2d 23h 39m 48s	1/5	No route to host
	check_udp	UNKNOWN	2013-01-23 11:52:13	38d 4h 44m 20s	1/5	With UDP checks, a send/expect string must be specified

Figura 256. Verificación del estado de los servicios: Critical
Fuente: Captura de pantalla

Para solucionar este problema, se debe reiniciar el servidor que se encuentre en estado crítico para que los servicios estén arriba.

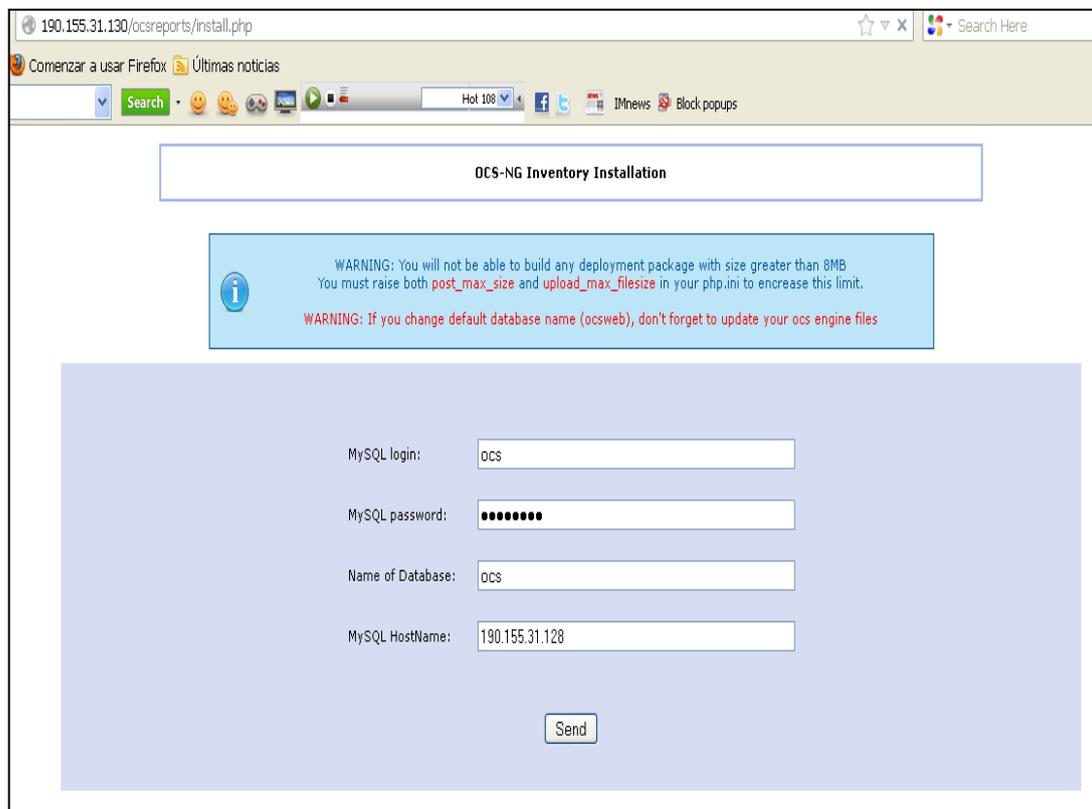
ANEXO 7

INSTALACIÓN DE OCS INVENTORY SERVER

Para instalar la herramienta OCS INVENTORY, escribir en la consola la siguiente línea de código:

```
apt-get install ocsinventory-server
```

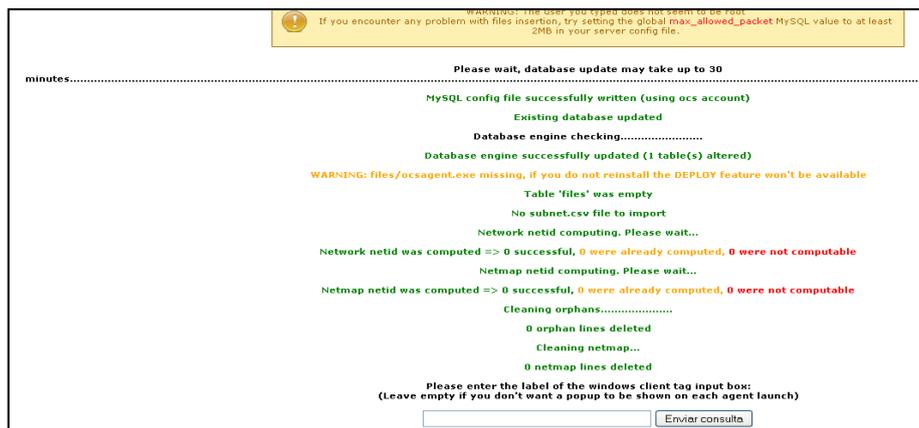
Ejecutar en el navegador: `http://ip_servidor/ocsreports/install.php`, como se muestra en la *Figura 257*.



The screenshot shows a web browser window with the address bar displaying `190.155.31.130/ocsreports/install.php`. The page title is "OCS-NG Inventory Installation". A warning message is displayed in a blue box: "WARNING: You will not be able to build any deployment package with size greater than 8MB. You must raise both `post_max_size` and `upload_max_filesize` in your `php.ini` to increase this limit. WARNING: If you change default database name (ocsweb), don't forget to update your ocs engine files". Below the warning, there is a form with four input fields: "MySQL login:" with the value "OCS", "MySQL password:" with masked characters "●●●●●●", "Name of Database:" with the value "OCS", and "MySQL HostName:" with the value "190.155.31.128". A "Send" button is located at the bottom of the form.

Figura 257. Proceso de instalación de OCS Inventory
Fuente: Captura de instalación de OCS Inventory

Se debe ingresar la información de la base de datos y hacer clic en el botón *Send*. Si los datos ingresados son correctos, va a mostrarse una ventana como la de la *Figura 258*. Hacer clic en *Enviar Consulta*.



*Figura 258. Verificación de la base de datos.
Fuente: Captura de instalación de OCS Inventory*

Finalmente, aparece la ventana que se muestra en la *Figura 259*, que indica que la instalación ha finalizado, además muestra el usuario login y la clave para ingresar a la aplicación.



*Figura 259. Instalación de OCS Inventory completada
Fuente: Captura de instalación de OCS Inventory*

Para ingresar al servidor OCS, abrir un navegador y ejecutar `http://ip_servidor/ocsreports/index.php`, como se muestra en la *Figura 260*, ingresar el usuario y la clave proporcionados en el proceso de instalación.



*Figura 260. Ingreso a la aplicación con el usuario y clave por defecto
Fuente: Captura de instalación de OCS Inventory*

INSTALACIÓN DE OCS INVENTORY CLIENTE

Para instalar el cliente OCS, ejecutar el paquete de instalación y aparece la ventana que se muestra en la *Figura 261*, hacer clic en *Next* para continuar con la instalación.

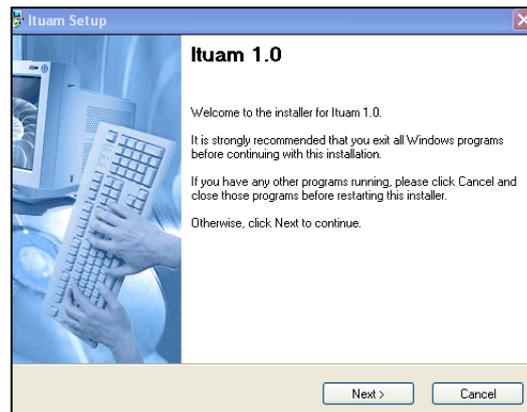


Figura 261. Ejecución del cliente OCS
Fuente: Captura de instalación del cliente OCS Inventory

Escoger la ubicación donde se va a instalar el cliente OCS y hacer clic en *Next*, como se muestra en la *Figura 262*.

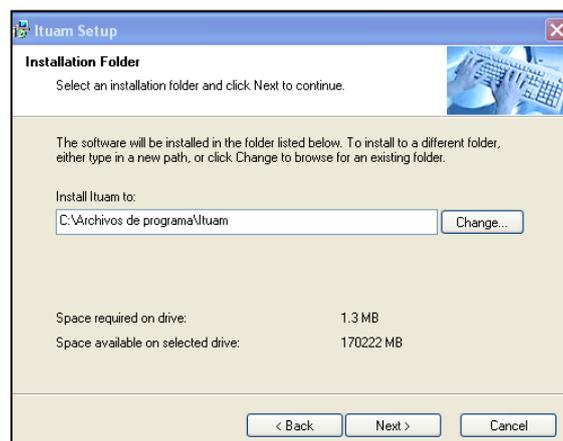


Figura 262. Selección de la ubicación del cliente OCS
Fuente: Captura de instalación del cliente OCS Inventory

Hacer clic en *Next* en la ventana que se muestra en la *Figura 263*, para continuar con la instalación.

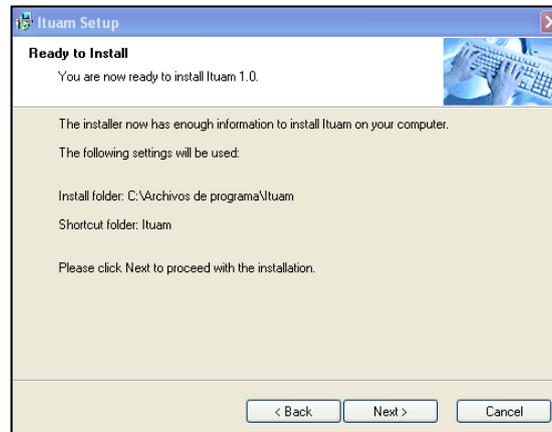


Figura 263. Proceso de instalación del cliente OCS
Fuente: Captura de instalación del cliente OCS Inventory

Para continuar con la instalación hacer clic en *Next* en la ventana que se muestra en la *Figura 264*.

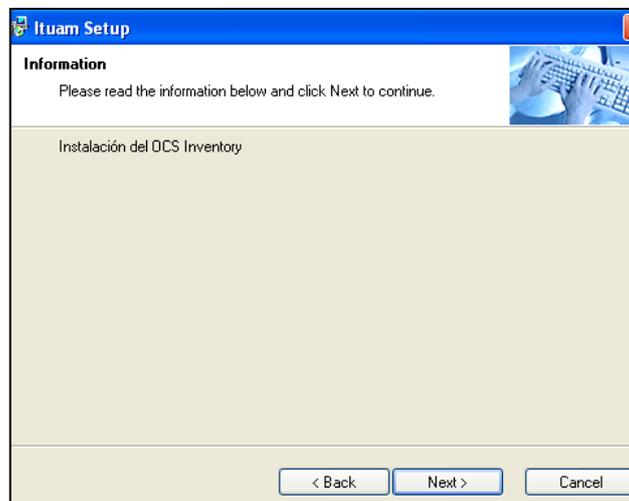
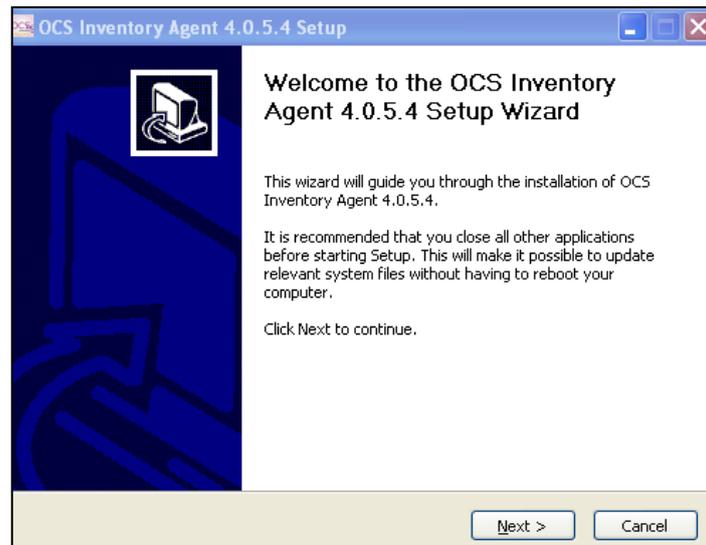


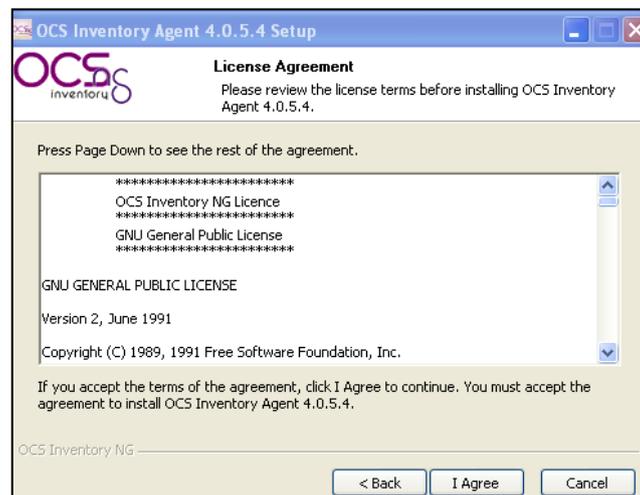
Figura 264. Proceso previo a la instalación de OCS Inventory
Fuente: Captura de instalación del cliente OCS Inventory

Para iniciar con la instalación del agente hacer clic en *Next* de la ventana mostrada en la *Figura 265*.



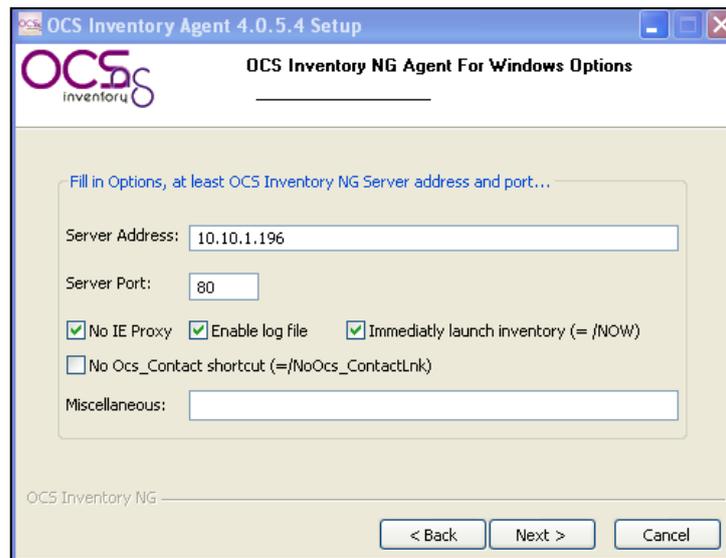
*Figura 265. Inicio de la instalación del agente OCS
Fuente: Captura de instalación del cliente OCS Inventory*

El siguiente paso es aceptar la licencia de la aplicación, para lo cual hacer clic en el botón *I Agree* de la ventana que se muestra en la *Figura 266*.



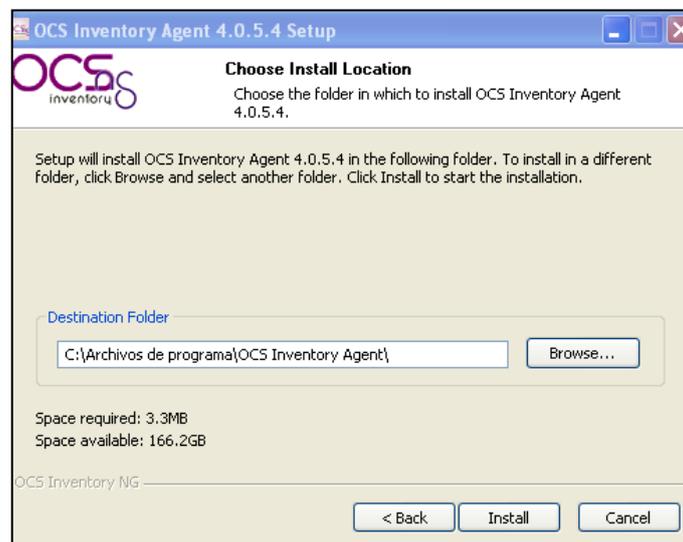
*Figura 266. Licencia General Pública de OCS Inventory
Fuente: Captura de instalación del cliente OCS Inventory*

A continuación aparece la ventana que se muestra en la *Figura 267*, se debe ingresar la dirección IP del servidor OCS Inventory (10.10.1.196) y hacer clic en *Next* para continuar.



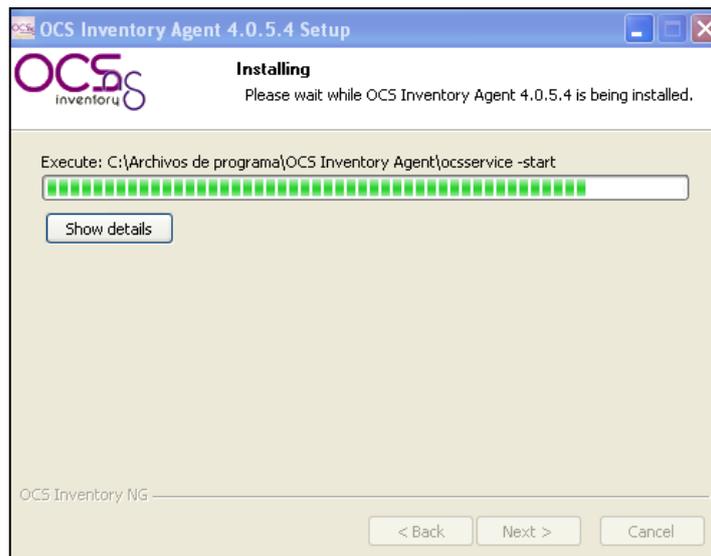
*Figura 267. Ingreso de IP del servidor OCS Inventory
Fuente: Captura de instalación del cliente OCS Inventory*

La ventana que se muestra en la *Figura 268*, permite escoger la ubicación del agente OCS, una vez que se haya elegido hacer clic en *Install* para continuar.



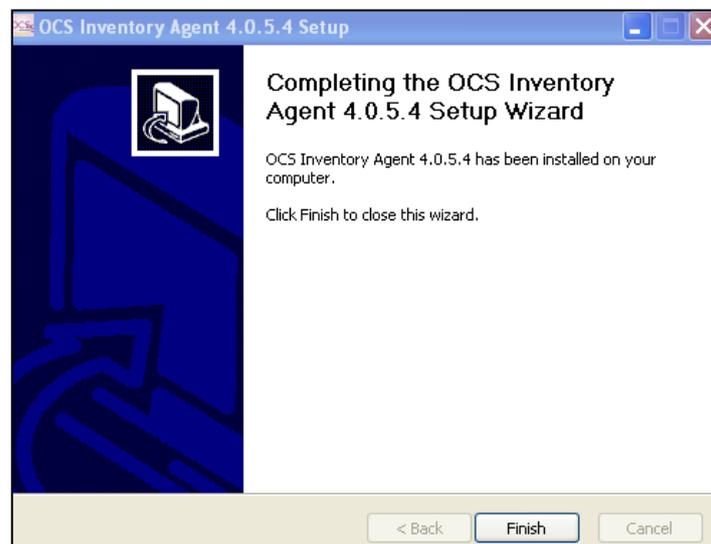
*Figura 268. Ubicación del agente OCS
Fuente: Captura de instalación del cliente OCS Inventory*

Mientras se instala el agente OCS aparece la ventana que se muestra en la *Figura 269*, en donde se indica el proceso de instalación de los archivos correspondientes.



*Figura 269. Proceso de instalación de los archivos del agente OCS
Fuente: Captura de instalación del cliente OCS Inventory*

Una vez que se termina la instalación aparece la ventana que se muestra en la *Figura 270*, hacer clic en *Finish* para cerrar la ventana.



*Figura 270. Instalación completa del agente OCS
Fuente: Captura de instalación del cliente OCS Inventory*

ANEXO 8 INSTALACIÓN DE OTRS

Instalar los paquetes esenciales:

```
apt-get install apache2 php5 php-pear php5-gd php5-cli php5-mysql mysql-server build-essential
```

Descargar los paquetes necesarios de las siguientes url's:

```
http://ftp.otrs.org/pub/otrs/packages/
```

```
http://ftp.otrs.org/pub/otrs/
```

```
wget http://ftp.otrs.org/pub/otrs/otrs-3.0.17.tar.gz
```

```
wget http://ftp.otrs.org/pub/otrs/packages/Calendar-1.9.5.opm
```

```
wget http://ftp.otrs.org/pub/otrs/packages/FAQ-2.0.7.opm
```

```
wget http://ftp.otrs.org/pub/otrs/packages/TimeAccounting-2.0.2.opm
```

```
wget http://ftp.otrs.org/pub/otrs/itsm/packages30/ITSMChangeManagement-3.0.6.opm
```

```
wget http://ftp.otrs.org/pub/otrs/itsm/packages30/ITSMConfigurationManagement-3.0.6.opm
```

```
wget http://ftp.otrs.org/pub/otrs/itsm/packages30/ITSMCore-3.0.6.opm
```

```
wget http://ftp.otrs.org/pub/otrs/itsm/packages30/ITSMIncidentProblemManagement-3.0.6.opm
```

```
wget http://ftp.otrs.org/pub/otrs/itsm/packages30/ITSMServiceLevelManagement-3.0.6.opm
```

```
wget http://ftp.otrs.org/pub/otrs/itsm/packages30/GeneralCatalog-3.0.6.opm
```

```
wget http://ftp.otrs.org/pub/otrs/itsm/packages30/ImportExport-3.0.6.opm
```

```
tar -xvzf otrs-3.0.17.tar.gz
```

```
mv otrs-3.0.17/ /opt/otrs
```

Instalar los módulos perl necesarios

```
aptitude install libapache2-mod-perl2 libdbd-mysql-perl libnet-dns-perl libnet-ldap-perl libio-socket-ssl-perl libpdf-
```

```
api2-perl libsoap-lite-perl libgd-text-perl libgd-graph-perl libapache-dbi-perl
```

Verificar que se encuentren instalados los módulos de perl que sean necesarios para cada funcionalidad.

```
perl /opt/otrs/bin/otrs.CheckModules.pl
```

Instalar los módulos faltantes usando cpan

```
cpan
```

```
install Encode::HanExtra
install JSON::XS
install Text::CSV_XS
```

Crear el usuario y grupo para otrs

```
useradd -r -d /opt/otrs/ -c 'OTRS user' otrs
usermod -g www-data otrs
```

Preparar los ficheros de configuración de otrs

```
cd /opt/otrs/Kernel
cp Config.pm.dist Config.pm
cp Config/GenericAgent.pm.dist Config/GenericAgent.pm
```

Copiar todos los ficheros descargados con la extensión .opm en el directorio /opt/otrs/var/packages/

```
cd
cp Calendar-1.9.5.opm FAQ-2.0.7.opm TimeAccounting-2.0.2.opm ITSMChangeManagement-3.0.5.opm
ITSMConfigurationManagement-3.0.5.opm ITSMCore-3.0.5.opm ITSMIncidentProblemManagement-3.0.5.opm
ITSMServiceLevelManagement-3.0.5.opm GeneralCatalog-3.0.5.opm ImportExport-3.0.5.opm
/opt/otrs/var/packages
```

Poner los permisos para el directorio de otrs

```
cd /opt/otrs
bin/otrs.SetPermissions.pl --otrs-user=otrs --otrs-group=otrs --web-user=www-data --web-group=www-data
/opt/otrs
```

Agregar la configuración hacia Apache

```
cp /opt/otrs/scripts/apache2-httpd.include.conf /etc/apache2/conf.d/otrs.conf
```

Reiniciar el servicio de apache

```
/etc/init.d/apache2 restart
```

Iniciar la instalación vía Web

```
http://127.0.0.1/otrs/installer.pl
```

La *Figura 271*, muestra el ingreso a la instalación de OTRS vía web. Hacer clic en *Siguiente*.



Figura 271. Instalación de OTRS vía web
Fuente: Captura de la instalación de OTRS

En el primer paso de la instalación se muestra la licencia de la herramienta OTRS. Hacer clic en *Aceptar licencia*. La *Figura 272* muestra esta ventana.



Figura 272. Primer paso de la instalación de OTRS
Fuente: Captura de la instalación de OTRS

El segundo paso de la instalación es crear la base de datos. La *Figura 273* muestra este paso. Se debe ingresar un usuario y la clave. Hacer clic en *Check database settings*.

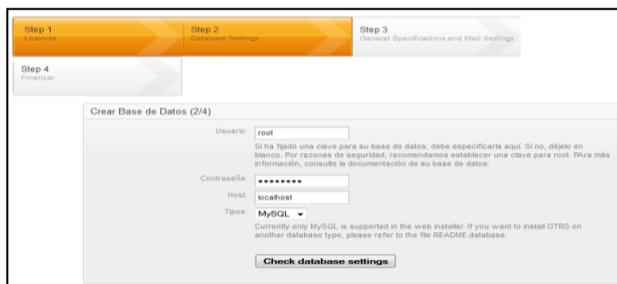


Figura 273. Creación de la base de datos para OTRS
Fuente: Captura de la instalación de OTRS

En la ventana que se muestra en la *Figura 274*, se debe crear un usuario nuevo para la base de datos e ingresar la clave para este usuario. Ingresar el nombre para la base de datos y pulsar en la opción *Crear*. Hacer clic en *Siguiente*.

The screenshot shows a window titled 'Step 4 Finalizar' with a sub-header 'Crear Base de Datos (2/4)'. It contains several input fields and a 'Crear' button. The fields are: 'Usuario' (root), 'Contraseña' (masked with asterisks), 'Host' (localhost), 'Tipo' (MySQL), 'Usuario-Base de datos (Nuevo)' (otrs), 'Contraseña' (masked with asterisks), 'DB... host' (localhost), and 'Base de Datos' (otrs). A 'Crear' button is located below the 'Base de Datos' field, and a 'Siguiente...' button is at the bottom right.

Figura 274. Configuración de la base de datos de OTRS
Fuente: Captura de la instalación de OTRS

Una vez que se ha creado la base de datos, aparece la ventana que se muestra a continuación en la *Figura 275*, hacer clic en *Siguiente*.

The screenshot shows a window titled 'Step 4 Finalizar' with a sub-header 'Crear Base de Datos (2/4)'. It displays a list of completed database operations, each followed by the word 'Hecho.' in green. The operations are: 'Creating database 'otrs': Hecho.', 'Creating tables 'otrs-schema.mysql.sql': Hecho.', 'Inserting initial inserts 'otrs-initial_insert.mysql.sql': Hecho.', 'Foreign Keys 'otrs-schema-post.mysql.sql': Hecho.', 'Creating database user 'otrs@localhost': Hecho.', and 'Reloading grant tables: Hecho.'. At the bottom, it says 'Database setup successful' and has a 'Siguiente...' button.

Figura 275. Creación satisfactoria de la base de datos
Fuente: Captura de la instalación de OTRS

El tercer paso es la configuración del sistema como se muestra en la *Figura 276*, en esta ventana se debe ingresar el dominio y el nombre de la organización y hacer clic en *Siguiente*.

Step 4
Finalizar

Configuración del sistema (3/4)

ID de sistema: 10
The identifier of the system. Each ticket number and each HTTP session ID contain this number.

FQDN del sistema: policia.gob.ec
Fully qualified domain name of your system.

Correo del Administrador: pao_lucho@hotmail.com
Email address of the system administrator.

Organización: POLICIA

Traza

Módulo de trazas: Syslog
Log backend to use.

LogFile: /var/log/otrs.log
Log file location is only needed for File-LogModule!

Interface Web

Default language: Español
Default language.

Revisar record MX: No
Email addresses that are manually entered are checked against the MX records found in DNS. Don't use this option if your DNS is slow or does not resolve public addresses.

Siguiete...

*Figura 276. Configuración del sistema de OTRS
Fuente: Captura de la instalación de OTRS*

El cuarto paso de la instalación se muestra en la *Figura 277*, en esta ventana aparece la información con la que se debe ingresar vía web a la aplicación OTRS.

Step 1
Licencia

Step 2
Database Settings

Step 3
General Specifications and Mail Settings

Step 4
Finalizar

Finalizado (4/4)

Página de inicio: <http://192.168.1.8/otrs/index.pl>

Usuario: root@localhost

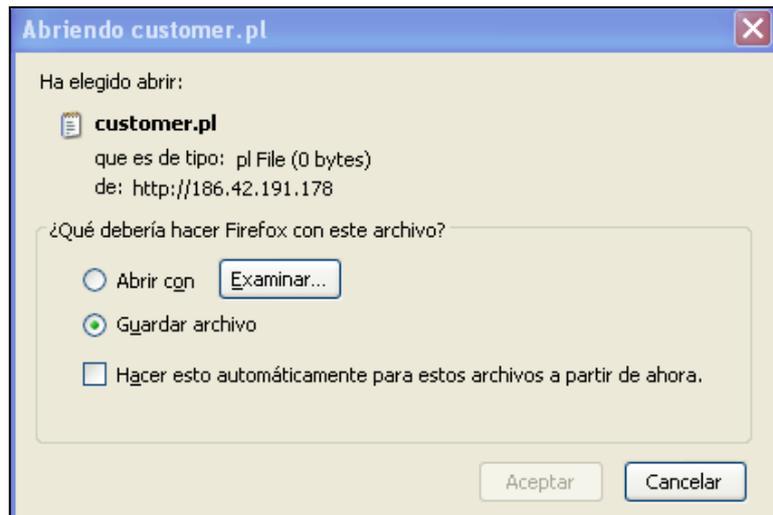
Contraseña: root

((enjoy))
Su equipo OTRS

*Figura 277. Datos informativos para el ingreso a OTRS
Fuente: Captura de la instalación de OTRS*

PROBLEMAS COMUNES

Si al ingresar a la administración, cuenta de usuario o FAQ de OTRS se muestra la ventana de la *Figura 278*.



*Figura 278. Error de ingreso a OTRS
Fuente: Captura de pantalla*

Se debe reiniciar el servicio de apache, utilizando la siguiente línea de código:

```
/etc/init.d/apache2 restart
```

ANEXO 9

INSTALACIÓN DEL SERVIDOR DE ARCHIVOS

Para instalar el servidor de archivos, se debe ejecutar las siguientes líneas de código.

```
apt-get install samba quota-tool
```

Una vez instalado se debe editar el fichero de configuración smb.conf, para esto se debe ingresar en la consola la siguiente línea:

```
nano /etc/samba/smb.conf
```

En este fichero se debe configurar el directorio en donde se van a almacenar las carpetas de los usuarios.

Finalmente reiniciar el servicio:

```
/etc/init.d/smbd restart
```

ANEXO 10

INSTALACIÓN DE COBIAN BACKUP

Se puede realizar la descarga del software desde siguiente página web:

<http://www.cobiansoft.com/index.htm>

Una vez descargado, hacer doble clic en el paquete cbSetup.exe y seleccionar el idioma, hacer clic en *Próximo* como se muestra en la *Figura 279*.



Figura 279. Selección del idioma en la instalación de Cobian Backup.

Aparece una nueva ventana en donde se acepta las condiciones de uso. La *Figura 280*, muestra esta ventana.



Figura 280. Licencia de Cobian Backup

En la pantalla que se muestra en la *Figura 281*, escoger el tipo de instalación a realizar.



Figura 281. Tipo de instalación Cobian Backup.

Al seleccionar la opción *Como un servicio*, el programa se ejecuta simplemente arrancando el ordenador, aunque ningún usuario inicie sesión en el equipo.

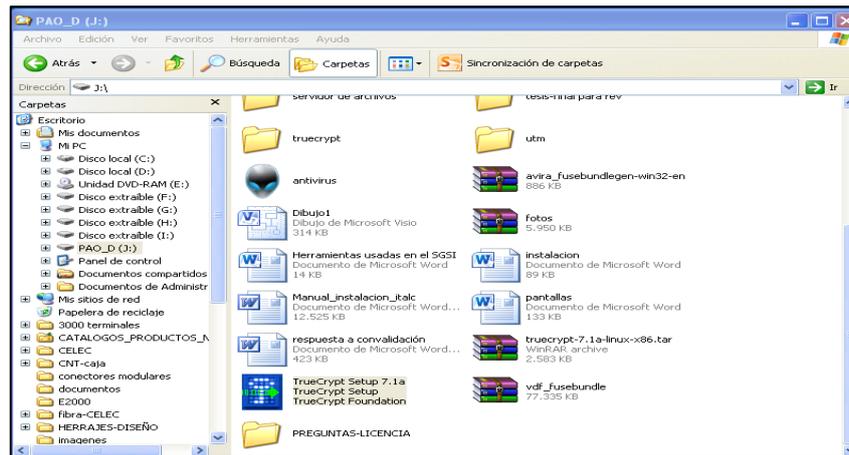
Si la instalación se realizó sin ningún problema, hacer clic en el botón *Terminar*, como se muestra en la *Figura 282*.



Figura 282. Instalación Cobian Back completa.

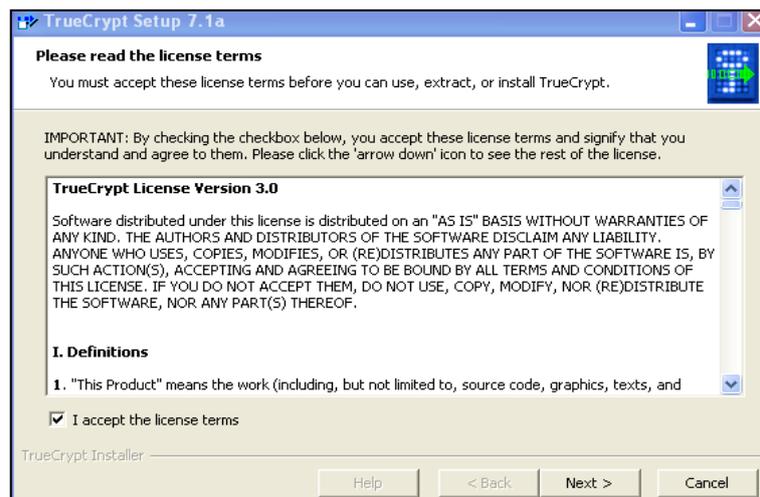
ANEXO 11 INSTALACIÓN DE TRUCCRYPT

Para la instalación de TrueCrypt se debe descargar el archivo .exe, como se muestra en la *Figura 283*.



*Figura 283. Archivo descargado con formato .exe
Fuente: Captura de la instalación*

Ejecutar el archivo haciendo doble clic, aparece la ventana que se muestra en la *Figura 284*, marcar la casilla y dar clic en el botón Next.



*Figura 284. Inicio de la instalación
Fuente: Captura de la instalación*

Escoger la opción Install y pulsar el botón Next para continuar con la instalación, como se muestra en la *Figura 285*.

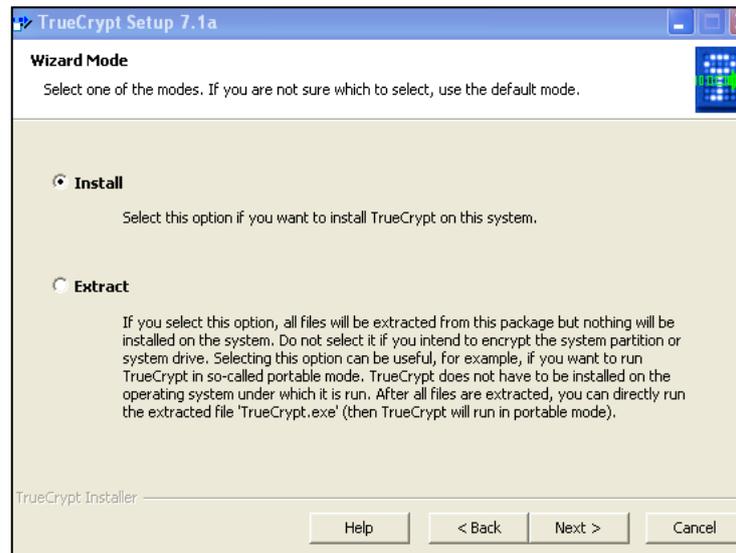


Figura 285. Selección del modo de instalación
Fuente: Captura de la instalación

La *Figura 286* muestra la ventana en donde se elige la ubicación de instalación de los archivos. Pulsar el botón Install para continuar.

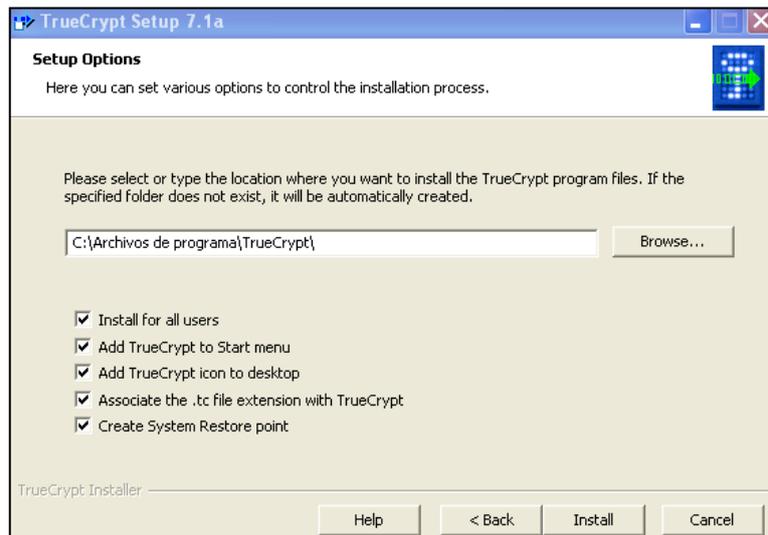
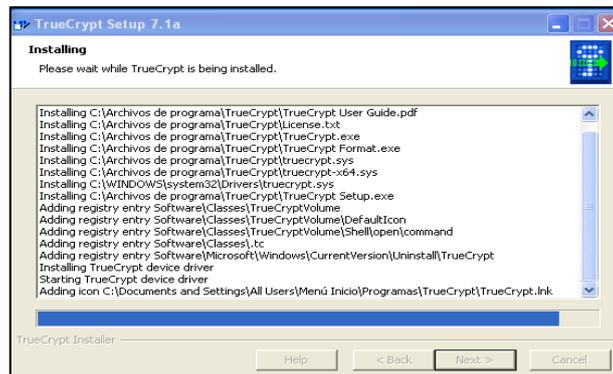


Figura 286. Ubicación de los archivos de TrueCrypt
Fuente: Captura de la instalación

El progreso de la instalación se muestra en la *Figura 287*.



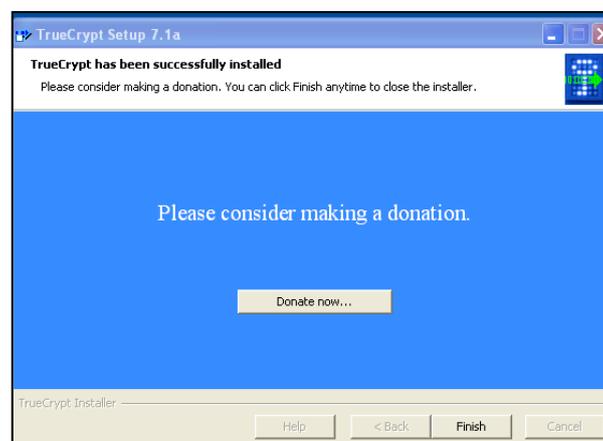
*Figura 287. Progreso de la instalación de TrueCrypt
Fuente: Captura de la instalación*

Una vez que la instalación haya terminado aparece una ventana como la que se muestra en la *Figura 288* que indica que la aplicación se instaló satisfactoriamente. Pulsar en el botón Aceptar.



*Figura 288. Instalación de la aplicación finalizada
Fuente: Captura de la instalación*

Para terminar con la instalación pulsar en el botón Finish como se muestra en la *Figura 289*.



*Figura 289. Fin de la instalación
Fuente: Captura de la instalación*

ANEXO 12

INSTALACIÓN DEL FIREWALL

Para la realización del firewall se utilizó el generador de iptables Shorewall, para instalarlo se ejecuta el comando:

```
apt-get install shorewall shorewall-doc
```

CONFIGURACIÓN BÁSICA DE SHOREWALL

La configuración básica de Shorewall se describe a continuación:

1. Habilitar la ejecución de shorewall modificando el fichero de la siguiente manera:

```
#nano /etc/default/shorewall
```

Cambiar el parámetro startup=0 a startup=1, guardar los cambios y salir.

2. Copiar los ficheros necesarios para la configuración del firewall, ejecutando:

```
#cd /usr/share/doc/shorewall-common/default-config/  
#cp zones interfaces policy rules masq hosts tunnels /etc/shorewall/
```

3. Modificar el archivo /etc/shorewall/shorewall.conf habilitando la opción de reenvío de paquetes

```
#nano /etc/shorewall/shorewall.conf
```

Cambiar `IP_FORWARDING=Keep` por `IP_FORWARDING=Yes`
guardar los cambios y salir.

Configuración del archivo de zonas

zones: En este fichero se establecen las zonas del cortafuegos.

Editar al archivo `/etc/shorewall/zones` especificando la siguiente información:

```
#nano /etc/shorewall/zones

#####
#####
#ZONE TYPE OPTIONS IN OUT
fw firewall           #Zona de defecto del firewall
net ipv4              #Zona de acceso a internet
loc ipv4              #Zona de la red LAN
srv ipv4              #Zona de servidores
wir ipv4              #Zona wireless
#LAST LINE — ADD YOUR ENTRIES BEFORE THIS ONE — DO NOT REMOVE
```

Configuración del fichero interfaces

interfaces: Permite establecer las interfaces de red físicas asociadas a cada zona.

Editar al archivo `/etc/shorewall/interfaces` especificando los siguientes datos:

```
#nano /etc/shorewall/interfaces

GNU nano 2.2.2 File: /etc/shorewall/interfaces
# Shorewall version 4 - Interfaces File
# For information about entries in this file, type "man shorewall-interfaces"
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-interfaces.html
#
```

```
#####
#####
#ZONE INTERFACE   BROADCAST   OPTIONS
net  eth0         detect  dhcp,tcpflags,routefilter,nosmurfs,logm$ #Interfaz de red asociada a la zona
loc  eth1         detect  tcpflags,routefilter,nosmurfs,logmarti$
srv  eth2         detect  tcpflags,routefilter,nosmurfs,logmarti$
wir  eth3         detect  tcpflags,routefilter,nosmurfs,logmarti$
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Configuración del fichero policy

policy: En éste fichero se definen las políticas para permitir o restringir el tráfico entre zonas.

Editar el archivo `/etc/shorewall/policy` especificando los siguientes datos:

```
#nano /etc/shorewall/policy

GNU nano 2.2.2   File: /etc/shorewall/policy   Modified
#
# Shorewall version 4 - Policy File
# For information about entries in this file, type "man shorewall-policy"
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-policy.html
#####
#####
#SOURCE   DEST     POLICY   LOG     LIMIT:BURST
#
#                               LEVEL
$FW  loc  ACCEPT                #Se acepta el tráfico desde el firewall hacia la red local
$FW  net  ACCEPT                #Se acepta el tráfico desde el firewall hacia la red internet
$FW  srv  ACCEPT                #Se acepta el tráfico desde el firewall hacia la red de servidores
```

```

$FW wir ACCEPT          #Se acepta el tráfico desde el firewall hacia la red wireless

loc $FW REJECT info    #Se restringe el tráfico desde la red local hacia el firewall
loc net REJECT info    #Se restringe el tráfico desde la red local hacia la red de internet
loc srv REJECT info    #Se restringe el tráfico desde la red local hacia la red de servidores
loc wir REJECT info    #Se restringe el tráfico desde la red local hacia la red wireless

```

Configuración del fichero rules

rules: En este fichero es donde realmente se definen las reglas del cortafuegos. Permite establecer excepciones a las políticas definidas en el archivo anterior.

Editar al archivo `/etc/shorewall/rules` y agregue las siguientes políticas:

```

#nano /etc/shorewall/rules

# Abrir el puerto 80 o servicio HTTP para un servidor web
HTTP/ACCEPT net fw

# Abrir el puerto 3452 para el protocolo TCP
ACCEPT net fw tcp 3452

#Abrir el puerto SSH únicamente a una IP permitida
SSH/ACCEPT net:ipl.ip2.ip3 fw

```

De esta manera se pueden ir estableciendo más reglas de acuerdo a las políticas de seguridad definidas.

Formato de una regla

Una regla básica tiene la siguiente estructura:

Acción	Fuente	Destino	Protocolo	Puerto
ACCEPT	loc	\$FW	tcp	22022

Si se desea aplicar una regla sobre un puerto y protocolo específico se debe declarar de la siguiente forma:

```
ACCEPT loc $FW tcp 22,80,22022,58000
```

En la *Figura 290*, se muestra las reglas aplicadas al firewall.

```
GNU nano 2.2.2 File: /etc/shorewall/rules
#
# Shorewall version 4 - Rules File
#
# For information on the settings in this file, type "man shorewall-rules"
#
# The manpage is also online at
# http://www.shorewall.net/manpages/shorewall-rules.html
#
#####
#ACTION SOURCE DEST PROTO DEST SOURCE ORIGINAL RATE USER/ MARK
### ACCESO Temporal
DNAT net srv:10.10.1.196 tcp 902,80,443
DNAT net:186.42.191.179 srv:10.10.1.194 tcp 22

### Acceso externo hacia el firewall
ACCEPT net $FW tcp 22022,80,3000,58000
#ACCEPT net:200.110.78.140 $FW tcp 80
ACCEPT net:186.42.191.179 $FW tcp 3128,58000,3000

### Acceso del firewall hacia internet
ACCEPT $FW net tcp
ACCEPT $FW net udp

### Acceso de la red local hacia los servicios del firewall
ACCEPT loc $FW tcp 3128,22022,58000,3000,80,53
ACCEPT loc $FW udp 53,67

### Acceso de los servidores hacia internet
ACCEPT srv net tcp
ACCEPT srv net udp
ACCEPT srv $FW udp 53

### Acceso de la red local hacia los servidores
ACCEPT loc srv tcp
ACCEPT loc srv udp

### Acceso desde los servidores hacia el firewall
ACCEPT srv $FW tcp 22022
ACCEPT srv:10.10.1.196 $FW tcp 22022,80,3128
```

Figura 290. Reglas aplicadas en el firewall
Fuente: Captura mediante putty

En los logs de este servidor se puede verificar las conexiones tanto aceptadas o rechazadas para ello digitar:

```
tail -f /var/log/messages
```

Luego de realizar cambios en el archivo de reglas es necesario reiniciar el servicio de shorewall para que se apliquen los cambios, para lo cual se debe digitar:

```
/etc/init.d/shorewall restart
```

INICIAR EL SERVICIO DE SHOREWALL

Verificar las configuraciones realizadas anteriormente digitando el siguiente comando:

```
#shorewall check
```

Este comando ejecuta el firewall en modo debug y va verificando línea a línea y si existen errores en alguna configuración, en cuyo caso muestra un mensaje de ERROR.

Reiniciar el servicio shorewall para que los cambios aplicados tengan efecto.

```
#!/etc/init.d/shorewall restart
```

```
#Instalar Webmin
```

```
aptitude install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions
```

```
cd /tmp
```

```
wget http://prdownloads.sourceforge.net/webadmin/webmin_1.570_all.deb
```

```
dpkg -i webmin_1.570_all.deb
```

```
rmwebmin_1.570_all.deb
```

```
cd /etc/squid/
```

```
#Descargar acls Squidguard
```

```
wget wget http://squidguard.shalla.de/Downloads/shallalist.tar.gz
```

```
tar -zxvf shallalist.tar.gz
```

```
mv BL/ acls
```

```
rm -rf shallalist.tar.gz
```

```
chown -R proxy.proxy /etc/squid/acls/
```

ANEXO 13 INSTALACIÓN DEL PROXY

Para instalar las herramientas utilizadas para el proxy se ejecuta el siguiente comando:

```
apt-get install squid squidguard sarg apache2
```

CONFIGURACIÓN DEL PROXY

A continuación se detalla el proceso de configuración del proxy y sus herramientas:

Configuración de squid

Editar el archivo `/etc/squid/squid.conf` especificando la siguiente información:

```
#Definir la red que estará autorizada a navegar por el proxy
acl localnet src 10.10.1.0/25          #Red Local
acl localnet src 10.10.1.128/26      #Red wireless

#Permitir la navegación libre sin restricciones
http_access allow localnet
http_access allow localhost

#Bloquear todo excepto lo anterior
http_access deny all

#Permitir comunicación ip a equipos de la localnet
icp_access allow localnet
icp_access deny all
```

```

#Definición del puerto en el que se levantará servicio de proxy
http_port 3128

#Definición del tamaño del cache del proxy, es recomendable hasta 30 Gb.
cache_dir ufs /var/spool/squid 20000 16 256

#Definición del tamaño máximo de los objetos que se almacenarán en la cache
maximum_object_size 20480 KB

#Cantidad de peticiones que serán redireccionadas para la verificación de filtros de urls
url_rewrite_children 10

#Redirección de solicitud de páginas web a squidguard
redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

```

Guardar los cambios realizados y salir.

Verificar la configuración realizada ejecutando el siguiente comando:

```
#squid -NCdl
```

Configuración de SquidGuard

Descargar las listas negras para SquidGuard.

```
#cd /tmp
#wget http://squidguard.shalla.de/Downloads/shallalist.tar.gz
```

Descomprimir el archivo descargado anteriormente.

```
#tar -xvzf shallalist.tar.gz
```

Mover el directorio BL hacia el directorio /etc/squid/renombrándolo como acls.

```
#mv BL /etc/squid/acls
```

Modificar el fichero `/etc/squid/squidGuard.conf` especificando la siguiente información:

```
#Directorio donde se encuentran las listas negras
dbhome /etc/squid/acls

#Directorio donde se almacenarán los archivos de log
logdir /var/log/squid

#Grupos de usuarios al cual se permitirá o negará la navegación a Internet.
source Super-Rest {
ip      10.10.1.133
}

#Definición de clases de listas negras.

destination movies {
domainlist    movies/domains
urllist    movies/urls
redirect http://10.10.1.1/error.html
}

destination adv {
domainlist    adv/domains
urllist    adv/urls
redirect http:// 10.10.1.1/error.html
}

destination aggressive {
domainlist    aggressive/domains
urllist    aggressive/urls
redirect http:// 10.10.1.1/error.html
```

```
}
```

```
destination alcohol {  
  domainlist    alcohol/domains  
  urllist    alcohol/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination automobile {  
  domainlist    automobile/bikes/domains  
  urllist    automobile/bikes/domains  
  domainlist    automobile/boats/domains  
  urllist    automobile/boats/domains  
  domainlist    automobile/cars/domains  
  urllist    automobile/cars/domains  
  domainlist    automobile/planes/domains  
  urllist    automobile/planes/domains  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination chat {  
  domainlist    chat/domains  
  urllist    chat/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination costtraps {  
  domainlist    costtraps/domains  
  urllist    costtraps/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination dating {  
  domainlist    dating/domains  
  urllist    dating/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination downloads {  
  domainlist    downloads/domains  
  urllist    downloads/urls  
  redirect http://10.10.1.1/error.html  
}
```

```
destination drugs {  
  domainlist    drugs/domains  
  urllist    drugs/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination dynamic {  
  domainlist    dynamic/domains  
  urllist    dynamic/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination finance {  
  domainlist    finance/banking/domains  
  urllist    finance/banking/urls  
  domainlist    finance/insurance/domains  
  urllist    finance/insurance/urls  
  domainlist    finance/moneylending/domains  
  urllist    finance/moneylending/urls  
  domainlist    finance/other/domains
```

```
urllist  finance/other/urls
domainlist  finance/realestate/domains
urllist  finance/realestate/urls
domainlist  finance/trading/domains
urllist  finance/trading/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination fortunetelling {
domainlist  fortunetelling/domains
urllist  fortunetelling/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination forum {
domainlist  forum/domains
urllist  forum/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination gamble {
domainlist  gamble/domains
urllist  gamble/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination government {
domainlist  government/domains
urllist  government/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination hacking {
domainlist  hacking/domains
urllist  hacking/urls
}
```

```
redirect http:// 10.10.1.1/error.html
}
destination hobby {
domainlist      hobby/cooking/domains
urllist  hobby/cooking/urls
domainlist      hobby/games-misc/domains
urllist  hobby/games-misc/urls
domainlist      hobby/games-online/domains
urllist  hobby/games-online/urls
domainlist      hobby/gardening/domains
urllist  hobby/gardening/urls
domainlist      hobby/pets/domains
urllist  hobby/pets/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination homestyle {
domainlist      homestyle/domains
urllist  homestyle/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination hospitals {
domainlist      hospitals/domains
urllist  hospitals/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination imagehosting {
domainlist      imagehosting/domains
urllist  imagehosting/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination isp {  
  domainlist      isp/domains  
  urlist    isp/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination jobsearch {  
  domainlist      jobsearch/domains  
  urlist    jobsearch/urls  
  redirect    http:// 10.10.1.1/error.html  
}
```

```
destination library {  
  domainlist      library/domains  
  urlist    library/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination military {  
  domainlist      military/domains  
  urlist    military/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination models {  
  domainlist      models/domains  
  urlist    models/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination music {  
  domainlist      music/domains  
  urlist    music/urls
```

```
redirect http:// 10.10.1.1/error.html  
}
```

```
destination news {  
domainlist    news/domains  
urllist  news/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination podcasts {  
domainlist    podcasts/domains  
urllist  podcasts/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination politics {  
domainlist    politics/domains  
urllist  politics/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination porn {  
domainlist    porn/domains  
urllist  porn/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination radiotv {  
domainlist    radiotv/domains  
urllist  radiotv/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination redirector {  
  domainlist    redirector/domains  
  urlist    redirector/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination religion {  
  domainlist    religion/domains  
  urlist    religion/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination remotecontrol {  
  domainlist    remotecontrol/domains  
  urlist    remotecontrol/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination ringtones {  
  domainlist    ringtones/domains  
  urlist    ringtones/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination science {  
  domainlist    science/astronomy/domains  
  urlist    science/astronomy/urls  
  domainlist    science/chemistry/domains  
  urlist    science/chemistry/urls  
  redirect http:// 10.10.1.1/error.html  
}
```

```
destination searchengines {
```

```
domainlist      searchengines/domains
urllist  searchengines/urls
redirect http:// 10.10.1.1/error.html
}

destination sex {
domainlist      sex/education/domains
urllist  sex/education/urls
domainlist      sex/lingerie/domains
urllist  sex/lingerie/urls
redirect http:// 10.10.1.1/error.html
}

destination shopping {
domainlist      shopping/domains
urllist  shopping/urls
redirect http:// 10.10.1.1/error.html
}

destination socialnet {
domainlist      socialnet/domains
urllist  socialnet/urls
redirect http:// 10.10.1.1/error.html
}

destination education {
domainlist      education/schools/domains
urllist  education/schools/urls
redirect http:// 10.10.1.1/error.html
}

destination spyware {
domainlist      spyware/domains
urllist  spyware/urls
```

```
redirect http:// 10.10.1.1/error.html  
}
```

```
destination tracker {  
domainlist tracker/domains  
urllist tracker/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination updatesites {  
domainlist updatesites/domains  
urllist updatesites/urls  
redirect http://10.10.1.1/error.html  
}
```

```
destination violence {  
domainlist violence/domains  
urllist violence/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination warez {  
domainlist warez/domains  
urllist warez/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination weapons {  
domainlist weapons/domains  
urllist weapons/urls  
redirect http:// 10.10.1.1/error.html  
}
```

```
destination webmail {
```

```
domainlist    webmail/domains
urllist    webmail/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination webphone {
domainlist    webphone/domains
urllist    webphone/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination webradio {
domainlist    webradio/domains
urllist    webradio/urls
redirect http:// 10.10.1.1/error.html
}
```

```
destination webtv {
domainlist    webtv/domains
urllist    webtv/urls
redirect http:// 10.10.1.1/error.html
}
```

Guardar los cambios realizados y salir.

Verificar si existen errores en la configuración realizada digitando el siguiente comando:

```
#squidGuard -d
```

Compilar y generar las bases de datos para todas las listas negras descargadas.

```
#squidGuard -C all
```

Cambiar el propietario y el grupo del directorio */etc/squid/acls*.

```
#chown -R proxy.proxy /etc/squid/acls
```

Reiniciar el servicio proxy para que los cambios realizados tengan efecto.

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

Configuración de Sarg

Crear el directorio /var/www/squid-reports

```
#mkdir /var/www/squid-reports
```

Modificar el archivo /etc/sarg/sarg.conf especificando la siguiente información:

```
#Especificar el archivo de log de squid
access_log /var/log/squid/access.log
```

```
#Editar el directorio de salida en donde se generarán los reportes
output_dir /var/www/squid-reports
```

Guardar los cambios realizados y salir.

Modificar el archivo /etc/sarg/sarg-reports.conf especificando la siguiente información:

```
HTMLDOUT=/var/www/squid-reports
```

Guardar los cambios realizados y salir.

Generar un reporte ejecutando el siguiente comando:

```
#sarg-reports today
```

Verificar que el reporte se ha generado listando el contenido del directorio/var/www/squid-reports

```
#ls -l /var/www/squid-reports/
```

Visualizar el reporte generado ingresando en un browser la siguiente dirección:

```
http://ip_servidor/squid-reports/
```

ANEXO 14

INSTALACIÓN DEL NTOP

Para instalar la herramienta se ejecuta el comando:

```
apt-get install ntop
```

CONFIGURACIÓN

Para cambiar la configuración se modifica el fichero `/var/lib/ntop/init.cfg`, en el cual se puede especificar las interfaces en las cuales ntop estará escuchando.

ERROR COMÚN

Si al ingresar a la herramienta NTOP, se muestra el mensaje de la *Figura 291*,



Figura 291. Mensaje de error al ingresar a NTOP
Fuente: Captura de pantalla

Se debe parar el servicio NTOP con la siguiente línea:

```
/etc/init.d/ntop stop
```

Y nuevamente iniciar el servicio:

```
/etc/init.d/ntop start
```

ANEXO 15

INSTALACIÓN DEL MRTG

Para instalar esta herramienta de monitoreo, ejecutar la siguiente línea de comando

```
apt-get install mrtg
```

CONFIGURACIÓN DE MRTG

Para supervisar la carga de tráfico es necesario ejecutar los siguientes comandos:

Paso 1.

Crear el archivo de configuración snmp, por ejemplo mon01.cfg, que contenga todas las interfaces detectadas al consultar el dispositivo que tiene dirección IP, por ejemplo 127.0.0.1.

```
cfgmaker --ifref=name jcanalu@127.0.0.1 > /etc/mrtg/mon01.cfg
```

Paso 2.

El siguiente comando permite visualizar el archivo de configuración creado, en este caso mon01.cfg y cambiar el WorkDir, al nombre que se le quiera dar para este dispositivo, por ejemplo en este caso /var/www/mrtg/mon01

```
vi /etc/mrtg/mon01.cfg
```

Paso 3.

Para crear el directorio especificado anteriormente, donde se guardarán los ficheros de las estadísticas de tráfico del dispositivo incorporado se debe escribir

el siguiente comando, nótese que debe coincidir con el nombre de la carpeta que se puso en el Workdir del paso anterior.

```
mkdir /var/www/mrtg/mon01
```

Paso 4.

El siguiente comando permite crear la página index.html, de acuerdo al fichero de configuración creada en el paso 1, dentro de la carpeta creada en el paso anterior. Nótese que el fichero se crea dentro de la carpeta creada en el paso anterior y que se especifica el nombre del fichero de configuración creado en el paso uno.

```
indexmaker /etc/mrtg/mon01.cfg > /var/www/mrtg/mon01/index.html
```

Paso 5

Finalmente entrar al cron del sistema y añadir una entrada para que se actualicen las estadísticas de tráfico para el dispositivo cada cinco minutos. Nótese que se especifica el nombre del fichero de configuración creado en el paso 1.

```
crontab -e  
0-55/5 * * * * env LANG=C /usr/bin/mrtg /etc/mrtg/mon01.cfg
```

ANEXO 16 INSTALACIÓN DEL IDS/IPS

INSTALACIÓN DEL IDS

Para instalar snort se debe realizar lo siguiente:

```
apt-get install mysql-server php5 php5-cli php5-gd php5-mysql libphp-  
jpgraph snort-mysql
```

CONFIGURACIÓN DEL IDS

Modificar el archivo `/etc/snort/snort.debian.conf` especificando los siguientes datos:

```
#nano /etc/snort/snort.debian.conf  
  
DEBIAN_SNORT_HOME_NET="red a proteger/máscara"  
DEBIAN_SNORT_INTERFACE="eth0"
```

Guardar los cambios realizados y salir.

Crear la base de datos para snort ejecutando los siguientes comandos:

```
#mysql -u root -p
```

Especificar la contraseña para el usuario root

```
mysql> create database snort;  
mysql> grant all privileges on snort.* to snort@127.0.0.1 identified by snort1102';  
mysql> flush privileges;  
mysql> exit
```

Crear las tablas dentro de la base de datos snort utilizando el script `create_mysql.gz` ubicado en el directorio `/usr/share/doc/snort-mysql/`

```
#cd /usr/share/doc/snort-mysql/  
#zcat create_mysql.gz | mysql -u root -h localhost -p snort
```

Especificar la contraseña para el usuario root

Modificar el archivo /etc/snort/snort.conf especificando los siguientes datos:

```
#nano /etc/snort/snort.conf
```

Buscar las palabras output database

```
output database: log, mysql, user=snort password=snort!102 dbname=snort  
host=127.0.0.1
```

Guardar los cambios realizados y salir.

Eliminar el archivo/etc/snort/db-pending-config

```
#rm /etc/snort/db-pending-config
```

Reiniciar el servicio de snort para que los cambios realizados tengan efecto.

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

Instalación Y Configuración De SNORTREPORT

Descargar el paquete SNORTREPORT con el siguiente comando:

```
#cd /tmp  
#wget http://hem.bredband.net/jpgraph/jpgraph-1.27.1.tar.gz
```

Descomprimir el paquete descargado anteriormente:

```
#tar -zxvf jpgraph1.27.1.tar.gz
```

Copiar el directorio src a /var/www y renombrarlo con jpgraph

```
#cp -r jpgraph1.27.1/src /var/www/jpgraph
```

Descargar el paquete snortreport ejecutando los siguientes comandos:

```
#cd /tmp
```

```
#wget http://www.symmetrixtech.com/ids/snortreport-1.3.1.tar.gz
```

Descomprimir el archivo descargado anteriormente en el directorio /var/www y renombrarlo a snortreport.

```
#tar -zxvf snortreport1.3.1.tar.gz -C /var/www/
```

```
#cd /var/www
```

```
#mv snortreport1.3.1 snortreport
```

Modificar el archivo /var/www/snortreport/srconf.php y especificar los siguientes datos:

```
# nano /var/www/snortreport/srconf.php
```

Llenar la información de la base de datos en los siguientes parámetros:

```
$server = "127.0.0.1";
```

```
$user = "snort";
```

```
$pass = "snort1102";
```

```
$dbname = "snort";
```

Especificar el Path de las librerías para generar los gráficos.

```
define("JPGRAPH_PATH", "/var/www/jpgraph/");
```

Reiniciar el servicio de apache2 y en un navegador web ejecutar la IP seguido por el nombre snortreport.

INSTALACIÓN DEL PSAD-IPS

El administrador recibirá mensajes de reportes.

La opción a configurar en /etc/psad/psad.conf es EMAIL_ADDRESSES.

EMAIL_ADDRESSES you@domain1.com, you@domain2.com;

El administrador recibirá un mensaje similar al siguiente:

```

===== Mon Dec 15 00:01:42 2010 =====
Danger level: [2] (out of 5)
Scanned UDP ports: [1027: 1 packets, Nmap: -sU]
iptables chain: INPUT, 1 packets
Source: 60.222.224.133
DNS: [No reverse dns info available]
Destination: 200.84.43.36
DNS: dc8542b24.dslam-172-17-16-241-0170-352.dsl.cantv.net
Overall scan start: Mon Dec 15 00:01:41 2010
Total email alerts: 1
Complete UDP range: [1027]
Syslog hostname: fricky
Global stats: chain: interface: TCP: UDP: ICMP:
INPUT eth1 0 1 0
[+] UDP scan signatures:
"MISC Windows popup spam attempt"
dst port: 1027 (no server bound to local port)
psad_id: 100196
chain: INPUT
packets: 1
classtype: misc-activity
reference: (url) http://www.linklogger.com/UDP1026.htm
[+] Whois Information:
% [whois.apnic.net node-2]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html
inetnum: 60.220.0.0 - 60.223.255.255
netname: CNCGROUP-SX

```



```
fax-no: +86-351-4088347
e-mail: hxx@public.ty.sx.cn
nic-hdl: XH63-AP
mnt-by: MAINT-CHINANET-SX
changed: hxx@public.ty.sx.cn 20010208
source: APNIC
===== Mon Dec 15 00:01:42 2010 =====
```

En este mensaje se tiene la información detallada de quién realizó el ataque. Cuando se tiene habilitada la opción de autobloqueo se recibe un mail con la información siguiente:

```
To: administrador-psad@gmail.com
Subject: [psad-status] added iptables auto-block against 60.15.177.166 for 3600 seconds
# o en caso reverso
To: administrador-psad@gmail.com
Subject: [psad-status] removed iptables block against 60.222.224.139
```

ACTUALIZACIÓN DE FIRMAS

La actualización de firmas se realiza ejecutando el comando siguiente:

```
#psad -sig-update
```

Este comando se encuentra programado para ser realizado periódicamente en el CRON.