

## **DECLARACIÓN**

Yo, Joel Ricardo Vasco Rodríguez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

---

**Joel Ricardo Vasco Rodríguez**

## **CERTIFICACIÓN**

Certifico que el presente trabajo fue desarrollado por Joel Ricardo Vasco Rodríguez, bajo mi supervisión.

---

**Ing. Juan Herrera**  
**DIRECTOR DE PROYECTO**

# INDICE GENERAL

DECLARACIÓN.....	I
CERTIFICACIÓN .....	II
INDICE GENERAL.....	III
INDICE DE FIGURAS .....	VIII
INDICE DE TABLAS.....	XI
RESUMEN.....	XII
PRESENTACION .....	XIII
<b>1 MARCO TEÓRICO .....</b>	<b>1</b>
1.1 INTRANETS E INTEREDES.....	1
1.1.1 DEFINICIÓN Y CARACTERÍSTICAS DE UNA INTRANET.....	1
1.1.2 TECNOLOGÍA USADA EN LAS INTRANETS.....	2
1.1.3 VENTAJAS DE UNA INTRANET.....	3
1.1.4 DESVENTAJAS DE UNA INTRANET.....	4
1.1.5 DEFINICIÓN Y CARACTERÍSTICAS DE UNA INTERRED.....	4
1.1.5.1 Protocolos.....	5
1.1.5.2 Arquitectura.....	6
1.2 E-BUSINESS .....	7
1.2.1 DEFINICIÓN .....	7
1.2.2 CLASIFICACIÓN.....	7
1.2.2.1 Hacia los Clientes.....	7
1.2.2.1.1 E-Commerce.....	7
1.2.2.1.2 CRM (Customer Relationship Management).....	7
1.2.2.2 Interno de la Organización.....	7
1.2.2.2.1 KM (Knowledge Management).....	7
1.2.2.2.2 BI (Business Intelligence).....	8
1.2.2.2.3 ERP (Enterprise Resource Planning).....	8
1.2.2.3 Hacia Proveedores.....	8
1.2.2.3.1 SCM (Supply Chain Management).....	8
1.2.3 MODELOS DE E-BUSINESS.....	8
1.2.3.1 Business to Business (B2B).....	8
1.2.3.2 Business to Customer (B2C).....	9
1.2.3.3 Customer to Business (C2B).....	9
1.2.3.4 Customer to Customer (C2C).....	9
1.2.4 BENEFICIOS DEL E-BUSINESS.....	9
1.3 VPN'S .....	9
1.3.1 ORIGEN.....	9
1.3.2 DEFINICIÓN.....	10
1.3.3 CARACTERÍSTICAS.....	11
1.3.4 FUNCIONAMIENTO BÁSICO.....	12
1.3.5 TECNOLOGÍA USADA.....	12
1.3.5.1 Tecnología de túnel.....	12
1.3.5.2 Tecnología de autenticación.....	13
1.3.5.3 Tecnología de encriptación.....	14
1.3.5.4 Tecnología de firewall.....	15
1.4 CONCEPTOS DE SEGURIDAD.....	15
1.4.1 INTRODUCCIÓN.....	15
1.4.2 ENFOQUE .....	16
1.4.3 DEFINICIÓN .....	17
1.4.4 ELEMENTOS A PROTEGER.....	18
1.4.4.1 Información.....	19
1.4.4.2 Equipos que la soportan.....	19
1.4.4.2.1 Software .....	19
1.4.4.2.2 Hardware.....	20
1.4.4.2.3 Organización.....	20

1.4.4.3	Personas que la utilizan.....	20
1.4.5	<b>AMENAZAS, VULNERABILIDADES Y RIESGOS.....</b>	<b>21</b>
1.4.5.1	Definiciones.....	21
1.4.5.2	Tipos de amenazas.....	22
1.4.5.3	Tipos de vulnerabilidades.....	22
1.4.5.4	Cómo Protegerse.....	25
<b>2</b>	<b>REDISEÑO DE LA INFRAESTRUCTURA INTERED.....</b>	<b>27</b>
2.1	<b>ESTADO ACTUAL.....</b>	<b>27</b>
2.1.1	<b>DESCRIPCIÓN DE LA EMPRESA.....</b>	<b>27</b>
2.1.1.1	Historia.....	27
2.1.1.2	Misión.....	27
2.1.1.3	Visión.....	28
2.1.1.4	Estrategia.....	28
2.1.1.5	Metas.....	28
2.1.1.6	Política de calidad de la organización.....	29
2.1.1.6.1	Valores Institucionales.....	29
2.1.1.6.2	Eficiencia y Eficacia.....	29
2.1.1.6.3	Trabajo en Equipo.....	30
2.1.2	<b>FLUJO DE PROCESOS.....</b>	<b>30</b>
2.1.3	<b>RED FÍSICA.....</b>	<b>34</b>
2.1.4	<b>SEGURIDADES.....</b>	<b>37</b>
2.1.4.1	Seguridades Físicas.....	37
2.1.4.2	Seguridades Lógicas.....	37
2.2	<b>ALCANCE.....</b>	<b>38</b>
2.3	<b>OBJETIVOS.....</b>	<b>39</b>
2.3.1	<b>OBJETIVO GENERAL.....</b>	<b>39</b>
2.3.2	<b>OBJETIVOS ESPECÍFICOS.....</b>	<b>39</b>
2.4	<b>ANÁLISIS DE REQUERIMIENTOS.....</b>	<b>39</b>
2.4.1	<b>TIPOS DE SERVICIOS REQUERIDOS.....</b>	<b>39</b>
2.4.2	<b>TIPO DE HARDWARE REQUERIDO.....</b>	<b>41</b>
2.4.3	<b>TIPO DE SOFTWARE REQUERIDO.....</b>	<b>42</b>
2.4.3.1	Software base.....	42
2.4.3.2	Software de productividad.....	42
2.4.3.3	Software de protección.....	43
2.4.4	<b>ANÁLISIS DE RIESGOS.....</b>	<b>43</b>
2.4.4.1	<b>ACTIVOS A PROTEGER.....</b>	<b>44</b>
2.4.4.1.1	PROCESOS.....	44
2.4.4.1.2	APLICACIONES.....	45
2.4.4.1.3	SERVICIOS.....	45
2.4.4.1.4	HARDWARE.....	46
2.4.4.1.5	EQUIPO DE COMUNICACIONES.....	47
2.4.4.1.6	Software.....	47
2.4.4.1.7	DATOS.....	48
2.4.4.1.8	PERSONAL.....	48
2.4.4.2	<b>VULNERABILIDADES.....</b>	<b>50</b>
2.4.4.2.1	De Hardware:.....	50
2.4.4.2.2	Naturales:.....	50
2.4.4.2.3	Físicas:.....	50
2.4.4.2.4	De Software:.....	51
2.4.4.2.5	De Comunicación:.....	51
2.4.4.2.6	Humanas:.....	51
2.4.4.3	<b>AMENAZAS.....</b>	<b>51</b>
2.4.4.3.1	Naturales.....	52
2.4.4.3.2	Intencionales.....	52
2.4.4.3.3	Involuntarias.....	53
2.4.4.4	<b>CLASIFICACIÓN DE ACTIVOS.....</b>	<b>53</b>
2.4.4.4.1	Aplicaciones y procesos.....	53
2.4.4.4.2	Servicios.....	54
2.4.4.4.3	Hardware.....	54

2.4.4.4.4	Equipo de comunicaciones .....	54
2.4.4.4.5	Software .....	54
2.4.4.4.6	Personal .....	55
2.4.4.5	Evaluación del impacto .....	55
2.4.4.6	PROBABILIDAD DE OCURRENCIA DE LA AMENAZA. ....	57
2.4.4.7	Evaluación del nivel de riesgo. ....	59
2.5	CONSIDERACIONES DE REDISEÑO LAN .....	61
2.5.1	ASPECTOS OPERATIVOS.....	61
2.5.1.1	ACCESO A INTERNET.....	61
2.5.1.2	USO DE APLICACIONES.....	62
2.5.2	INFRAESTRUCTURA REQUERIDA .....	63
2.6	CONSIDERACIONES DE REDISEÑO VPN .....	63
2.6.1	ASPECTOS OPERATIVOS.....	64
2.6.2	INFRAESTRUCTURA REQUERIDA. ....	65
2.7	CONSIDERACIONES ECONÓMICAS.....	65
2.7.1	COSTO DE EQUIPOS SERVIDORES. ....	65
2.7.2	COSTO DE LOS EQUIPOS ESTACIONES DE TRABAJO.....	66
2.7.3	COSTO DE SERVICIOS DE COMUNICACIÓN. ....	66
2.7.4	COSTO DE PROTECCIÓN FÍSICA DE EQUIPOS.....	67
2.7.5	COSTO DE PROTECCIÓN DE DATOS Y COMUNICACIONES. ....	67
<b>3</b>	<b>ANÁLISIS Y DISEÑO DE LA INTRANET SEGURA .....</b>	<b>69</b>
3.1	ANÁLISIS DE REQUERIMIENTOS PARA EL SERVICIO WEBMAIL .....	69
3.1.1	FUNCIONALIDAD REQUERIDA. ....	69
3.1.2	REQUERIMIENTOS DE HARDWARE .....	70
3.1.3	REQUERIMIENTOS DE SOFTWARE .....	70
3.1.4	REQUERIMIENTOS DE COMUNICACIONES.....	71
3.2	ANÁLISIS DE REQUERIMIENTOS PARA EL SERVICIO DE CALENDARIO ELECTRÓNICO. ....	71
3.2.1	FUNCIONALIDAD REQUERIDA. ....	71
3.2.2	REQUERIMIENTOS DE HARDWARE.....	72
3.2.3	REQUERIMIENTOS DE SOFTWARE .....	73
3.3	DEFINICIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INTRANET .....	73
3.3.1	POLÍTICAS DE SEGURIDAD EN SOFTWARE .....	73
3.3.1.1	De protección contra código malicioso. ....	73
3.3.1.2	De actualización de sistema operativo y aplicaciones.....	73
3.3.2	POLÍTICAS DE SEGURIDAD PARA CONTROL DE ACCESO Y UTILIZACIÓN DE SERVICIOS E INFORMACIÓN.....	73
3.3.2.1	De control de acceso y utilización del correo electrónico e Internet. ....	73
3.3.2.2	De utilización de cuentas de usuarios. ....	73
3.3.2.3	Del acceso a información electrónica disponible en la red. ....	74
3.3.2.4	Del control de acceso y utilización del servicio de VPN. ....	74
3.3.2.5	Del control de acceso y utilización del enlace punto a punto con las obras en construcción. ....	74
3.3.3	POLÍTICAS DE RESPALDOS Y RECUPERACIÓN DE ARCHIVOS.....	74
3.3.4	NORMAS. ....	74
3.3.4.1	Normas de seguridad en software .....	75
3.3.4.1.1	De protección contra código malicioso: .....	75
3.3.4.1.2	De actualización de sistema operativo y aplicaciones: .....	75
3.3.4.2	Normas de seguridad para control de acceso y utilización de servicios e información. 75	75
3.3.4.2.1	De control de acceso y utilización del correo electrónico e Internet. ....	75
3.3.4.2.2	De utilización de cuentas de usuarios.....	76
3.3.4.2.3	Del acceso a información electrónica disponible en la red.....	77
3.3.4.2.4	Del control de acceso y utilización del servicio de VPN.....	77
3.3.4.2.5	Del control de acceso y utilización del enlace punto a punto con las obras en construcción. ....	77
3.3.4.3	Normas de respaldos y recuperación de archivos.....	77
3.3.5	PROCEDIMIENTOS .....	78

3.3.5.1	Procedimientos de seguridad en software.....	78
3.3.5.1.1	Para protección contra código malicioso.....	78
3.3.5.1.2	Para actualización del sistema operativo y aplicaciones.....	79
3.3.5.2	Procedimientos de seguridad para control de acceso y utilización de servicios e información.....	80
3.3.5.2.1	De control de acceso y utilización del correo electrónico e Internet.....	80
3.3.5.2.2	De utilización de cuentas de usuarios.....	81
3.3.5.2.3	Del acceso a información electrónica disponible en la red:.....	82
3.3.5.2.4	Del control de acceso y utilización del servicio de VPN.....	82
3.3.5.2.5	Del control de acceso y utilización del enlace punto a punto con las obras en construcción.....	83
3.3.5.3	Procedimientos de respaldos y recuperación de archivos.....	83
3.3.5.3.1	Para la creación de respaldos en el servidor:.....	83
3.3.5.3.2	Para la recuperación de información.....	84
3.4	ANÁLISIS DE REQUERIMIENTOS DE LA VPN.....	85
3.4.1	NECESIDADES DE LA EMPRESA.....	85
3.4.2	CARACTERÍSTICAS DE LOS USUARIOS.....	86
3.4.3	RESTRICCIONES.....	86
3.4.4	REQUERIMIENTOS DE HARDWARE.....	86
3.4.4.1	Para la empresa constructora.....	86
3.4.4.2	Para la empresa de asistencia técnica.....	87
3.4.5	REQUERIMIENTOS DE SOFTWARE.....	87
3.4.5.1	Para los servidores.....	87
3.4.5.2	Para las estaciones de trabajo.....	87
3.4.6	REQUERIMIENTOS DE COMUNICACIONES.....	87
3.5	CARACTERIZACIÓN DE LA APLICACIÓN PARA CONTROL DE PRESUPUESTOS.....	88
3.5.1	ANTECEDENTES.....	88
3.5.2	FUNCIONALIDAD REQUERIDA PARA LA NUEVA APLICACIÓN.....	89
3.5.3	CARACTERÍSTICAS DE LA NUEVA APLICACIÓN.....	90
<b>4</b>	<b>DESARROLLO E IMPLANTACIÓN DE LA INTRANET SEGURA.....</b>	<b>91</b>
4.1	CONFIGURACIÓN Y PERSONALIZACIÓN DEL SERVICIO WEBMAIL.....	91
4.1.1	ACCESO AL SERVICIO.....	91
4.1.2	ENVIAR MENSAJES.....	92
4.1.3	PERSONALIZAR EL SERVICIO.....	93
4.2	CONFIGURACIÓN Y PERSONALIZACIÓN DEL SERVICIO DE CALENDARIO ELECTRÓNICO.....	95
4.2.1	INTRODUCCIÓN.....	95
4.2.2	LISTA DE CONTACTOS.....	96
4.2.2.1	Crear y organizar contactos.....	96
4.2.2.2	Modificar y eliminar contactos.....	97
4.2.3	CITAS.....	98
4.2.3.1	Configuración del horario laboral.....	98
4.2.3.2	Programar Citas.....	99
4.2.3.3	Modificar y eliminar una cita.....	101
4.2.4	TAREAS.....	101
4.2.4.1	Configuración.....	101
4.2.4.2	Creación y seguimiento de tareas.....	102
4.2.4.3	Modificación y Eliminación de Tareas.....	103
4.3	IMPLANTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INTRANET.....	103
4.3.1	IMPLANTACIÓN DE POLÍTICAS DE SEGURIDAD EN SOFTWARE.....	104
4.3.1.1	Protección contra código malicioso.....	104
4.3.1.1.1	Instalación de antivirus, antispyware y cortafuegos personal.....	104
4.3.1.1.2	Demostración de revisión total de una estación de trabajo en busca de código malicioso empleando el antivirus y antispyware instalados.....	105
4.3.1.1.3	Actualización de antivirus y antispyware.....	105
4.3.1.1.4	Revisión total de estaciones de trabajo en busca de código malicioso.....	106
4.3.1.2	Actualización de sistema operativo y aplicaciones.....	106
4.3.1.3	Instalación de un servidor cortafuegos corporativo.....	107

4.3.2	<i>IMPLANTACIÓN DE POLÍTICAS DE SEGURIDAD PARA CONTROL DE ACCESO Y UTILIZACIÓN DE SERVICIOS E INFORMACIÓN.</i>	107
4.3.2.1	Demostración de utilización de Internet y correo electrónico.	107
4.3.2.2	Políticas de cuentas de usuario.	108
4.3.2.2.1	Creación de cuentas de usuario	108
4.3.2.2.2	Soporte al usuario en el uso de su cuenta de dominio.	108
4.3.2.3	Acceso a información electrónica disponible en la red.	109
4.3.2.3.1	Demostración de acceso a información electrónica disponible en la red.	109
4.3.2.3.2	Configuración de carpetas compartidas en el servidor.	109
4.3.2.4	Implementación y uso de los enlaces VPN.	109
4.3.2.4.1	Implantación del enlace permanente entre Quito y Guayaquil.	109
4.3.2.4.2	Implantación de enlaces punto a punto entre obras en construcción y oficina central.	109
4.3.2.5	respaldos y recuperación de archivos.	109
4.3.2.5.1	Demostración de Respaldos y recuperación de archivos.	109
4.3.2.5.2	Configuración de carpetas compartidas en el servidor para respaldos.	110
4.4	<b>IMPLANTACIÓN DE LA VPN.</b>	110
4.5	<b>PRUEBAS DE FUNCIONAMIENTO DE LA APLICACIÓN PARA CONTROL DE PRESUPUESTOS EN AMBIENTE E-BUSINESS.</b>	112
4.5.1	<i>ACCESO A LOS SISTEMAS DE CONTABILIDAD Y PRESUPUESTOS.</i>	113
4.5.2	<i>CREACIÓN DE UNA OBRA.</i>	115
4.5.3	<i>CREACIÓN DEL PRESUPUESTO LICITATORIO.</i>	117
4.5.4	<i>CREACIÓN E IMPORTACIÓN DE RUBROS EN EL PRESUPUESTO.</i>	118
4.5.5	<i>CREACIÓN DEL PRESUPUESTO DETALLADO INICIAL.</i>	119
4.5.6	<i>OBTENCIÓN DE CRONOGRAMAS.</i>	120
4.5.7	<i>OBTENCIÓN DE REPORTE.</i>	122
4.5.8	<i>MANEJO DE MATERIALES, MANO DE OBRA Y EQUIPOS EN EL MÓDULO DE MANTENIMIENTO.</i>	124
4.5.8.1	Manejo de materiales.	124
4.5.8.2	Manejo de equipos	125
4.5.8.3	Manejo de Mano de Obra.	127
4.5.9	<i>INTEGRACIÓN CON EL SISTEMA CONTABLE: Y CREACIÓN AUTOMÁTICA DE CUENTAS CONTABLES AL LICITAR UNA OBRA.</i>	129
4.5.9.1	Creación de unidades de medida.	129
4.5.9.2	Creación automática de cuentas contables el licitar una obra.	130
<b>5</b>	<b>CONCLUSIONES Y RECOMENDACIONES.</b>	<b>133</b>
5.1	CONCLUSIONES.	133
5.2	RECOMENDACIONES	135
	<b>BIBLIOGRAFIA</b>	<b>137</b>
	<b>GLOSARIO</b>	<b>140</b>
	<b>ANEXO A - MATRIZ DE RIESGO</b>	<b>144</b>
	<b>ANEXO B - DIAGRAMA DE LA NUEVA RED</b>	<b>147</b>
	<b>ANEXO C - ARCHIVO DE CONFIGURACION DEL ENLACE VPN</b>	<b>149</b>
	<b>ANEXO D - CONFIGURACION DE POLITICAS DE CONTRASEÑAS Y BLOQUEO DE CUENTAS DE USUARIO</b>	<b>153</b>

## INDICE DE FIGURAS

<b>FIGURA</b>	<b>TITULO</b>	<b>PAGINA</b>
Figura 1.1	Dos redes físicas conectadas mediante un enrutador	5
Figura 1.2	(a) Ilusión de una sola red que ofrece TCP/IP a los usuarios y las aplicaciones. (b) Estructura física real	6
Figura 1.3	Esquema físico y equivalente lógico de una VPN	10
Figura 1.4	Cliente conectado a la red corporativa	12
Figura 2.1	Flujo de procesos empleados en las actividades de construcción	33
Figura 2.2	Red física correspondiente al segundo piso de la empresa	36
Figura 2.3	Red física correspondiente a la planta baja de la empresa constructora	37
Figura 4.1	Certificado digital del servicio WebMail	91
Figura 4.2	Comunicaciones seguras exitosamente establecidas	92
Figura 4.3	Buzón de mensajes entrantes	92
Figura 4.4	Opciones disponibles para componer mensajes	93
Figura 4.5	Opciones de configuración del servicio	94
Figura 4.6	Opciones para configuración de interfaz gráfica	94
Figura 4.7	Página principal de Microsoft Outlook	95
Figura 4.8	Accesos directos	96
Figura 4.9	Ingreso de datos de un nuevo contacto	96
Figura 4.10	Criterios de clasificación de contactos	97
Figura 4.11	Contactos clasificados según la organización a la que pertenecen	97
Figura 4.12	Modificación de un contacto	98
Figura 4.13	Eliminación de un contacto	98
Figura 4.14	Configuración de la semana laboral del usuario	99
Figura 4.15	Calendario	99
Figura 4.16	Creación de una cita	100
Figura 4.17	Periodicidad de una cita	101
Figura 4.18	Ventana de opciones de tareas	101
Figura 4.19	Creación de una nueva tarea	102
Figura 4.20	Diagrama de escala de tiempo de las tareas	103
Figura 4.21	Esquema del enlace VPN entre las dos empresas y enlaces con obras	112
Figura 4.22	Pantalla de acceso común	113
Figura 4.23	Accesos a los sistemas de contabilidad y control de presupuestos	114
Figura 4.24	Menú de la aplicación de control de presupuestos	114
Figura 4.25	Menú de la aplicación de contabilidad	115
Figura 4.26	Opción para creación de una obra	115
Figura 4.27	Datos generales de una nueva obra	116
Figura 4.28	Porcentajes de costos indirectos	116
Figura 4.29	Menú de creación del presupuesto licitatorio	117



Figura 4.30	Selección de obra a ser presupuestada	117
Figura 4.31	Datos generales de obra y opciones de importación de rubros	118
Figura 4.32	Obra sin rubros	118
Figura 4.33	Creación de un nodo contenedor de rubros	119
Figura 4.34	Nodos contenedores de rubros de la obra estándar	119
Figura 4.35	Conversión del presupuesto licitatorio al presupuesto detallado inicial	120
Figura 4.36	Opción para exportación del cronograma de equipo	120
Figura 4.37	Exportación del cronograma de equipo de una obra dada	121
Figura 4.38	Detalles del cronograma de equipo exportado a Microsoft Project	121
Figura 4.39	Selección de la ubicación del archivo	121
Figura 4.40	Menú de informes	122
Figura 4.41	Listado de obras de las cuales se pueden obtener reportes	122
Figura 4.42	Listado de costos por rubros y total	123
Figura 4.43	Valores generales de materiales, equipos, mano de obra y transporte	123
Figura 4.44	Reporte detallado de materiales	124
Figura 4.45	Módulo de mantenimiento	124
Figura 4.46	Listado de materiales empleados por la empresa constructora	125
Figura 4.47	Listado de equipos	126
Figura 4.48	Detalles de un equipo	126
Figura 4.49	Confirmación de creación de un nuevo equipo	127
Figura 4.50	Listado de mano de Obra	127
Figura 4.51	Ingreso de datos correspondientes a una nueva mano de obra	128
Figura 4.52	Confirmación de creación de una nueva mano de obra	128
Figura 4.53	Listado de unidades	129
Figura 4.54	Edición de una unidad de medida	129
Figura 4.55	Agregación de "Kilómetro" dentro de las unidades	130
Figura 4.56	Organización del plan de cuentas utilizado en el sistema contable	130
Figura 4.57	Creación de una nueva obra del tipo <i>Edificación</i>	131
Figura 4.58	Licitación de la obra	132
Figura 4.59	Creación automática de cuentas contables de una obra	132
Figura B1	Diagrama de la nueva red – segundo piso.	147
Figura B2	Diagrama de la nueva red – planta baja	148
Figura D1	Seleccionar <i>Active Directory Users and Computers</i>	153
Figura D2	Acceso a las propiedades del dominio	154
Figura D3	Edición de la política de dominio por defecto	154
Figura D4	Acceso a las políticas de cuentas de usuario	155

Figura D5	Valores por defecto para las políticas de contraseñas	156
Figura D6	Número de contraseñas recordadas	156
Figura D7	Período mínimo de validez	157
Figura D8	Configuración automática de la política <i>Maximum password age</i>	157
Figura D9	Longitud mínima de la contraseña	158
Figura D10	Obtener el contenido de los requerimientos de seguridad	158
Figura D11	Detalle de la especificación de requerimientos de complejidad	159
Figura D12	Políticas de bloqueo de cuentas	160
Figura D13	Número de intentos fallidos de acceso	160
Figura D14	Tiempo durante el cual la cuenta permanecerá bloqueada	161
Figura D15	La cuenta permanecerá bloqueada hasta que el Administrador la desbloquee	161

## INDICE DE TABLAS

<b>TABLA</b>	<b>TITULO</b>	<b>PAGINA</b>
Tabla 2.1	Características de computadores de la red actual	34
Tabla 2.2	Listado de impresoras de la red actual	35
Tabla 2.3	Características de hardware para las estaciones de trabajo de la oficina central	41
Tabla 2.4	Características de hardware para el servidor cortafuegos	41
Tabla 2.5	Características de hardware para el servidor controlador de dominio	41
Tabla 2.6	Software base a instalarse en el servidor controlador de dominio	42
Tabla 2.7	Evaluación del impacto	56
Tabla 2.8	(continuación) Evaluación del impacto	57
Tabla 2.9	Evaluación de la probabilidad de ocurrencia de amenazas	58
Tabla 2.10	(continuación) Evaluación de la probabilidad de ocurrencia de amenazas	59
Tabla 2.11	Evaluación del nivel de riesgo	60
Tabla 2.12	(continuación) Evaluación del nivel de riesgo	61
Tabla 2.13	Componentes del costo del servidor controlador de dominio	66
Tabla 2.14	Costo del servidor cortafuegos	66
Tabla 2.15	Costo de las estaciones de trabajo	66
Tabla 2.16	Costo de servicios de comunicación	67
Tabla 2.17	Costo de dispositivos de protección física	67
Tabla 2.18	Costo de software antivirus	67
Tabla 3.1	Comparación de requerimientos de hardware de Internet Explorer	70
Tabla 3.2	Comparación de requerimientos de hardware de Outlook 2003	72
Tabla A1	Definición de niveles de impacto	144
Tabla A2	Definición de probabilidad de ocurrencia de amenazas	145
Tabla A3	Matriz de nivel de riesgo	145
Tabla A4	Definición de nivel de riesgo	146

## RESUMEN

El presente proyecto aborda asuntos relacionados a la seguridad informática en infraestructura de interred cuyo enfoque principal se aplica en el ámbito de la seguridad lógica de la información a través de Intranets, E-Business y VPN's (Red Privada Virtual).

El primer capítulo presenta un resumen teórico referente a conceptos de intranets, interredes, VPN's, e-Business y seguridad informática, temas necesarios para el desarrollo de este proyecto.

En el segundo capítulo se realiza un análisis de la situación actual de los recursos informáticos en ámbitos físico y lógico, así como la descripción general de los procesos empresariales para contar con las bases suficientes para realizar un análisis de requerimientos de nuevos servicios y rediseño de la infraestructura en uso. También se toman en cuenta consideraciones de carácter económico necesarias para la implantación de los rediseños y nuevos servicios definidos.

En el capítulo tercero se realiza el análisis de requerimientos de los nuevos servicios establecidos como necesarios en el capítulo anterior. También se definen las políticas normas y procedimientos de seguridad a implantarse en la empresa y se efectúa una caracterización de la nueva aplicación que apoyará las actividades fundamentales de la compañía.

El capítulo cuarto considera todos los aspectos prácticos de la implantación de nuevos servicios, políticas, normas y procedimientos de seguridad, y rediseños de la infraestructura informática. También constan pruebas realizadas con la nueva aplicación la cual automatiza procesos de control de presupuestos y gestión contable en un ambiente Web seguro.

## **PRESENTACION**

La utilización de sistemas informáticos automatizados es de amplia adopción por parte de las organizaciones que pretendan sobrevivir en un ambiente cada vez más competitivo. Por esta razón existe la necesidad de contar con sistemas informáticos confiables.

No puede hablarse de sistemas informáticos seguros, sino confiables, ya que la seguridad informática total es inalcanzable. Además, la seguridad informática no es un fin o una meta, sino un medio para llegar a las metas propuestas.

Este proyecto constituye una primera aproximación en el campo de la seguridad informática que realiza una determinada empresa, considerando nuevos servicios y nueva infraestructura necesarios para mejorar la calidad de los servicios ofrecidos.

Este proyecto constituye también un marco de referencia para futuros trabajos que se realizarán en el campo de la seguridad informática, específicos para esta empresa.

# CAPITULO I

## 1 MARCO TEÓRICO

### 1.1 INTRANETS E INTEREDES.

#### 1.1.1 DEFINICIÓN Y CARACTERÍSTICAS DE UNA INTRANET.

“Intranet es la implantación o integración en una red local o corporativa de tecnologías avanzadas de publicación electrónica basadas en web en combinación con servicios de mensajería, compartición de recursos, acceso remoto y toda una serie de facilidades cliente/servidor proporcionadas por la pila de protocolos TCP/IP, diseñado inicialmente para la red global Internet.

Su propósito fundamental es optimizar el flujo de información con el objeto de lograr una importante reducción de costos en el manejo de documentos y comunicación interna. Es una herramienta de gestión que permite una potente difusión de información y mecanismos de colaboración entre el personal”<sup>1</sup>.

El hardware fundamental no es lo que construye una Intranet, lo que importa son los protocolos TCP/IP.

Un concepto importante dentro de la Intranet consiste en el uso del navegador como interfase única para todo usuario. De esta manera no importa la plataforma empleada, el usuario no requiere capacitación para una interfase diferente para cada servicio que ofrece la Intranet, reduciendo de esta manera tiempo y costo de capacitación así como la complejidad de administración<sup>2</sup>.

Una Intranet se diferencia de Internet en que esta última es de acceso público y global, abierta a cualquiera que tenga una conexión; en tanto que las Intranets están restringidas a aquellas personas que están conectadas a la red privada de la organización.

---

<sup>1</sup> HERRERA, Juan. Intranets – Extranets Presentaciones de guías pedagógicas de la materia.

<sup>2</sup> CARDENAS, Claudia. Indice de Seguridad en Tecnologías de Información.

### 1.1.2 TECNOLOGÍA USADA EN LAS INTRANETS.

La mayoría del software que se usa es estándar: navegadores como Navigator de Netscape e Internet Explorer de Microsoft, las aplicaciones personalizadas generalmente se construyen usando el lenguaje de programación Java y el de guión de CGI<sup>3</sup>.

Una Intranet se basa en el modelo cliente/servidor, según lo cual son necesarios ciertos componentes de hardware y de software.

En lo referente al hardware, se necesitará:

- Servidores.
- PC de los usuarios con sus respectivos periféricos. Son llamados “equipos cliente”
- Un sistema de conexión que puede ser vía cable o vía inalámbrica que conecte los servidores con los equipos cliente.
- Tarjetas de conexión a red, concentradores, repetidores, máquinas que actúan como firewalls (cortafuegos).

En lo referente al software, se necesitará:

- Sistema(s) operativo(s) de red, que reside en clientes como en servidores, tales como: Unix, Novell Netware, Windows2003Server, Windows XP, etc.
- Aplicaciones de red para cliente y servidor tales como: navegadores, servidor web, programas de correo electrónico, programas de transferencia de archivos, etc. No es necesario que los programas cliente y servidor se ejecuten en un mismo sistema operativo.
- Protocolos de comunicación web estándares. Los sistemas operativos de red actuales ya cuentan con compatibilidad para TCP/IP, que son los protocolos que se usan al interior de una Intranet.

---

<sup>3</sup> MARTINEZ, Matías. Intranet.

### **1.1.3 VENTAJAS DE UNA INTRANET.**

Las organizaciones empresariales o educativas han descubierto que los servicios que funcionan muy bien en Internet y de los cuales se benefician ampliamente serán del mismo modo valiosos al interior de su organización, razón por la cual las Intranets se han vuelto tan populares.

Entre las múltiples ventajas que ofrecen las intranets se tiene:

- Posibilidad de restringir el acceso que tienen los usuarios a la información publicada o servicios ofrecidos.
- Facilidad de acceso a la intranet remotamente. Con una conexión a Internet los usuarios pueden acceder a información o recursos desde sus casas o mientras viajan como si estuvieran conectados localmente.
- Mejoramiento en los procesos de las áreas empresariales de servicio al cliente, ventas y marketing, producción y operaciones, ingeniería, recursos humanos, administración, contabilidad y finanzas.
- Con la posibilidad de acceder a tiempo a información crítica, esta tecnología mejora el proceso de toma de decisiones. Es posible organizar y mantener información centralizada o distribuida según se requiera o se facilite para la obtención y actualización.
- Disminución en el costo de mantenimiento de la red interna.
- Implantación de servicios y aplicaciones tales como: correo electrónico, transferencia de archivos, servicio de directorio, trabajo en equipo, acceso a bases de datos.
- Facilidad de obtener información actualizada en tiempo real las 24 horas, los 365 días del año. Esta información, disponible para usuarios y clientes, puede incluir noticias, manuales, procedimientos, planes de acción, material de formación, folletos de marketing y productos, listas de precios, información comercial, etc.



#### **1.1.4 DESVENTAJAS DE UNA INTRANET.**

Entre las desventajas pueden citarse:

- Riesgos de seguridad ante el acceso no autorizado a información organizacional.
- Caos potencial debido al cambio de procesos y sistemas.
- Al implantar la intranet puede presentarse una resistencia por parte del personal o elementos directivos de la organización ante el cambio en su forma habitual de trabajar.

#### **1.1.5 DEFINICIÓN Y CARACTERÍSTICAS DE UNA INTERRED.**

La Intranet de una organización por lo general comienza siendo una red LAN y conforme se obtienen mayores beneficios y/o las necesidades de la organización aumenten, la Intranet puede llegar a convertirse en una red WAN, para lo cual es necesario interconectar las diferentes redes con las cuales cuenta la organización<sup>4</sup>.

Una Interred es un grupo de redes físicas conectadas mediante enrutadores que se configuran para pasar tráfico entre las computadoras conectadas a las redes del grupo. Como consecuencia se tiene que las Interredes hacen uso de los protocolos TCP/IP.

El componente de hardware básico para conectar redes heterogéneas es el enrutador. Un enrutador es una computadora de propósito especial dedicada a interconectar redes, por lo tanto poseen procesador, memoria convencional así como interfaces de E/S para todas las redes a las que se conectan.

---

<sup>4</sup> CORNER, Douglas. Redes de computadores, Internet e interredes.

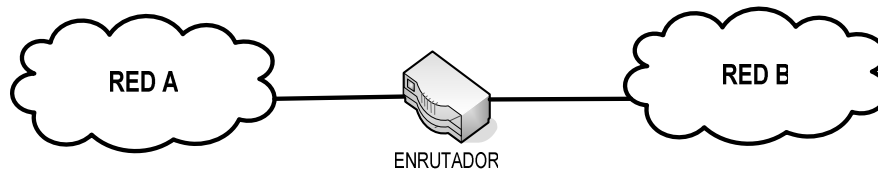


Figura 1.1. Dos redes físicas conectadas mediante un enrutador.

La red trata las conexiones al enrutador igual que las conexiones a las computadoras. El enrutador puede conectar redes de diferentes tecnologías lo que incluye diferentes medios, esquemas de direccionamiento físico y formatos de cuadro.

#### 1.1.5.1 Protocolos.

La capacidad para conectar redes de diferentes tecnologías se logra gracias al conjunto de protocolos de Interred llamados TCP/IP, la familia de protocolos que más destacó para el propósito de interconectividad. Los investigadores que desarrollaron la arquitectura de las Interredes también desarrollaron TCP/IP. Esto sucedía en los años setenta, casi al mismo tiempo que se desarrollaban las redes LAN<sup>5</sup>.

TCP/IP define el término *host* como cualquier sistema de cómputo que se conecte a una interred y ejecute una aplicación. El *host* puede ser una pequeña computadora personal o un *mainframe*. Los protocolos TCP/IP permiten que cualquier par de *host* se comuniquen a pesar de las diferencias de hardware.

Puede decirse que una interred es una red virtual porque el sistema de comunicación es una abstracción. Esto quiere decir que, aunque una combinación de hardware y software ofrece la ilusión de una red uniforme, no existe tal red.

La siguiente figura muestra el concepto de red virtual y su estructura física correspondiente.

---

<sup>5</sup> CORNER, Douglas. Redes de computadores, Internet e interredes.

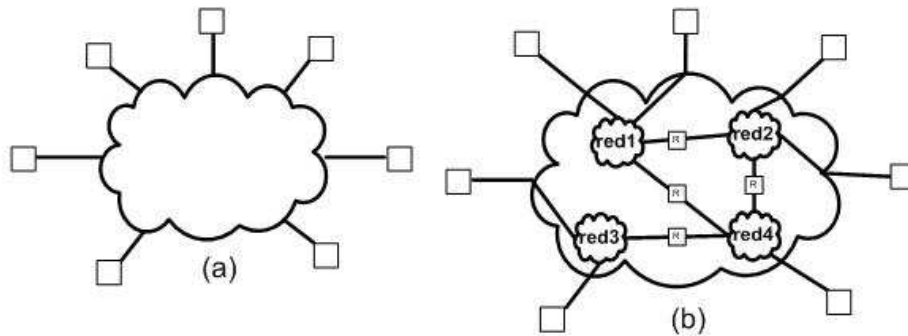


Figura 1.2. (a) Ilusión de una sola red que ofrece TCP/IP a los usuarios y las aplicaciones. (b) Estructura física real<sup>6</sup>.

### 1.1.5.2 Arquitectura.

Los enrutadores comerciales pueden conectar más de dos redes con lo cual se puede conseguir conectar a todas las redes con un solo enrutador. Sin embargo las organizaciones usan más de un enrutador para conectar todas sus redes por las siguientes razones:

Evitar sobrecargar el CPU y la memoria del enrutador con la tarea de procesar todos los paquetes de todas las redes.

Proveer de redundancia para aumentar la confiabilidad de la Interred. Los protocolos usados permiten a los enrutadores enviar el tráfico por trayectorias alternas si hay fallas en una red o enrutador.

Los detalles de la topología de la Interred dependen con frecuencia del ancho de banda de las redes físicas, el tráfico esperado, requisitos de confiabilidad y costo del hardware de enrutamiento.

<sup>6</sup> Fuente: CORNER, Douglas. Redes de computadores, Internet e interredes.

## **1.2 E-BUSINESS**

### **1.2.1 DEFINICIÓN**

“E-Business se define como cualquier actividad de negocio basada en Internet que transforma las relaciones internas y externas para crear valor y explotar oportunidades de mercado conducidas por las nuevas reglas de la economía digital”<sup>7</sup>.

En un sentido más complejo y dependiendo de la orientación del negocio, el E-Business puede ser clasificado.

### **1.2.2 CLASIFICACIÓN**

#### **1.2.2.1 Hacia los Clientes**

##### *1.2.2.1.1 E-Commerce*

Puede ser tan simple como una página de un catálogo con un número de teléfono, o puede extenderse de manera tal que procese tarjetas de crédito en tiempo real para que los clientes puedan comprar productos y recibirlos más tarde

##### *1.2.2.1.2 CRM (Customer Relationship Management)*

Dirigido a todos los aspectos relacionados con la atención y el servicio al cliente, coordina a todos los departamentos involucrados en esta atención: departamentos de ventas, marketing y relaciones con los clientes.

#### **1.2.2.2 Interno de la Organización**

##### *1.2.2.2.1 KM (Knowledge Management)*

Para la gestión del conocimiento y cuyo objetivo es lograr que la información dentro de una organización llegue a todo aquel que la necesite, procesada de forma tal que sea posible llevarla a la práctica.

---

<sup>7</sup> HERRERA, Juan.E-Business. Presentaciones de guías pedagógicas de la materia.

#### *1.2.2.2.2 BI (Business Intelligence)*

Centrado en el apoyo a la toma de decisiones y la evaluación de indicadores de negocio.

#### *1.2.2.2.3 ERP (Enterprise Resource Planning)*

Podemos considerar este software como la tecnología subyacente de gestión interna sobre la cual basar el resto de modelos del negocio de e-business. El término ERP deriva de MRP (Material Requirement planning) herramienta para el control de procesos productivos. Los sistemas ERP administran los procesos del negocio para la optimización de la cadena de valor que sirve a todos los departamentos dentro de la empresa. El software ERP incluye diversas funcionalidades: facturación, contabilidad, compras, producción, soporte, informes de gestión y recursos humanos, entre otras.

### **1.2.2.3 Hacia Proveedores**

#### *1.2.2.3.1 SCM (Supply Chain Management)*

Gestiona los procesos de negocio tanto internos como externos de la empresa implicando a todos los agentes que directa indirectamente están implicados, desde la producción a la distribución. El SCM incluye el aprovisionamiento de materias primas, proveedores, la atención al cliente, la logística y en general toda la cadena de valor de la empresa, optimizando los procesos más que automatizándolos, como es el caso del ERP.

### **1.2.3 MODELOS DE E-BUSINESS**

El e-business engloba a toda una serie de modelos de negocios basados en tecnología Internet, encaminados a mejorar las relaciones comerciales al interior de las empresas y sus relacionadas, entre estos modelos tenemos:

#### **1.2.3.1 Business to Business (B2B)**

El modelo más significativo y de mayor crecimiento, se establecen negocios entre las compañías que de acuerdo a las necesidades se definen los tipos de soluciones.

### **1.2.3.2 Business to Customer (B2C)**

Compañías intensivas en atención al cliente. Una empresa vende bienes y servicios al usuario o consumidor final, usualmente mediante catálogos o sistemas de subastas.

### **1.2.3.3 Customer to Business (C2B)**

Usualmente funciona como una subasta en reversa, donde el precio lo establece el consumidor ya sea solo o en grupo para lograr economías de escala y el negocio tiene la opción de aceptarlo o no.

### **1.2.3.4 Customer to Customer (C2C)**

Modelo de subastas en donde una persona puede comprar un bien o un servicio a otra persona, para esta transacción se necesita de un intermediario de confianza.

## **1.2.4 BENEFICIOS DEL E-BUSINESS**

El resultado de implementar E-business en las organizaciones es incrementar utilidades a través de:

- Reducción de costos. Eliminación de antigua infraestructura de ventas.
- Nuevos Canales de Venta. Por las nuevas alianzas con socios de negocios.
- Acceso a nuevos mercados. Debido al amplio alcance de Internet.
- Mejora de procesos de negocio. Obligatoriamente se debe mejorar la calidad de los procesos de negocio para competir globalmente.

## **1.3 VPN'S**

### **1.3.1 ORIGEN.**

Las VPN's nacen de la necesidad de interconectar las diferentes redes de una organización y de proveer acceso a los usuarios móviles, para lo cual se tienen tres alternativas:

- **Módem:** Las desventajas son el costo de las llamadas, el cual se incrementaría si las sucursales a conectar se encuentran en otras zonas del país o incluso en otro país; además la calidad y velocidad de la conexión no serían adecuadas.
- **Línea Privada:** La organización debe extender un cable de cobre o fibra, o utilizar medios inalámbricos que conecten un punto a otro. Esto resulta en un costo muy elevado.
- **VPN:** Los costos son bajos ya que se realizan llamadas locales y también existe la ventaja de que los datos viajen encriptados y seguros, con una buena calidad y velocidad.

### 1.3.2 DEFINICIÓN.

“Una VPN (Virtual Private Network por sus siglas en inglés) o Red Privada Virtual es una red privada que se extiende a distintos puntos remotos mediante el uso de una red pública de transporte (generalmente insegura), por ejemplo, Internet. Una VPN usa un proceso de encapsulamiento y encriptación de los paquetes de datos”<sup>8</sup>.

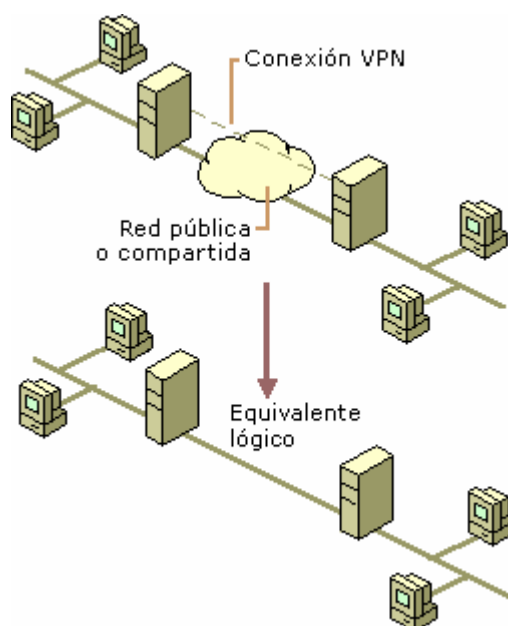


Figura 1.3. Esquema físico y equivalente lógico de una VPN<sup>9</sup>.

<sup>8</sup> Universidad de Valencia. Red Privada Virtual.

<sup>9</sup> Fuente: Microsoft TechNet. Noviembre 2004.

### 1.3.3 CARACTERÍSTICAS.

Una VPN ofrece:

- Confidencialidad. Se consigue a través de encriptación.
- Integridad. IPSec asegura que los datos no son modificados en el tránsito.
- Autenticación de usuarios. Por medio del uso de certificados digitales.
- Control de acceso a la red. Por medio de políticas de acceso configuradas en los servidores VPN de la red corporativa.
- No repudio. Por medio de certificados digitales.

Ventajas:

- Ahorro de costos directos.
- Reducción del tiempo de aprendizaje.
- Reducción de equipos.
- Reducción de soporte técnico necesario.
- Aumento de flexibilidad.
- Escalabilidad: extiende la red WAN a más usuarios remotos
- Soporta más conexiones y ancho de banda.
- Basadas en rendimiento, fiabilidad de conexión, cantidad de información y no en tiempo de conexión y en distancia.

Desventajas:

- No garantizan la disponibilidad. Si no se cuenta con una conexión a Internet entonces no puede crearse una conexión VPN a la red corporativa.
- No se garantiza el ancho de banda, ya que se usa una red pública.
- Gestión de claves de acceso y autenticación delicada y laboriosa.
- La fiabilidad es menor que en una línea dedicada.
- Mayor carga en el cliente VPN (encapsulación y cifrado).
- Mayor complejidad en la configuración del cliente (proxy, servidor de correo, etc ).



- Una VPN se considera segura, pero no hay que olvidar que la información sigue viajando por Internet (no seguro y expuesto a ataques).

### 1.3.4 FUNCIONAMIENTO BÁSICO.

- El usuario remoto establece una conexión con su ISP local, conectándose a la red de éste de una forma normal.
- Cuando desee conectarse a la red corporativa, el usuario inicia el túnel enviando una petición a un servidor VPN de la red corporativa.
- El servidor VPN autentifica al usuario y crea el otro extremo del túnel.
- El usuario comienza a enviar datos a través del túnel, los cuales son cifrados (encriptados) por el software VPN del cliente antes de ser enviados sobre la conexión del ISP.
- El servidor VPN recibe los datos y los descifra, propagando los datos hacia la red corporativa. Cualquier información devuelta al usuario remoto es cifrada antes de enviarse por Internet.



Figura 1.4 Cliente conectado a la red corporativa.<sup>10</sup>

### 1.3.5 TECNOLOGÍA USADA.

#### 1.3.5.1 Tecnología de túnel.

La tecnología de túneles ("Tunneling") es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de

<sup>10</sup> Fuente. Microsoft TechNet. Noviembre 2004

algún protocolo. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. Al establecer los túneles virtuales entre dos puntos se negocian esquemas de encriptación y autenticación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

Los dos protocolos de túnel más usados son PPTP y L2TP. La principal diferencia entre estos protocolos radica en que L2TP puede trabajar en un mayor rango de tipos de interredes, no solamente IP.

#### **1.3.5.2 Tecnología de autenticación.**

Las técnicas de autenticación son esenciales en las VPN's, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto.

Los protocolos de autenticación más comunes son<sup>11</sup>:

- PAP-Password Authentication Protocol: Usa passwords de texto claro para autenticar usuarios.
- SPAP-Shiva Password Authentication Protocol: Es un mecanismo de encriptación reversible de dos vías que es empleado por *Shiva*, un fabricante de hardware.
- CHAP-Challenge Handshake Authentication Protocol: También conocido como MD5-CHAP. Es un protocolo de autenticación basado en el método de desafío-respuesta. Usa la función de hashing MD5, la cual es un estándar de la industria.
- MS-CHAP-Microsoft Challenge Handshake Authentication Protocol: Es la extensión de CHAP hecha por Microsoft para autenticar estaciones remotas Windows. También existe de esta casa comercial el protocolo MS-CHAPv2, el cual ofrece autenticación mutua, claves de encriptación inicial más robustas y diferentes claves de encriptación para el envío y recepción de datos.

---

<sup>11</sup> MICROSOFT OFICIAL CURRICULUM. Managing a Microsoft Windows 2000 Network Environment.

### 1.3.5.3 Tecnología de encriptación.

Existen dos tipos de técnicas de encriptación que se usan en las VPN:

- encriptación de clave secreta o privada.
- encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. Lo que la una encripta la otra desencripta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente útiles para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPNs es IPSec, que consiste en un conjunto de propuestas del IETF que delinean un protocolo IP seguro para IPv4 e IPv6. IPSec provee encriptación a nivel de IP<sup>12</sup>.

IPSec provee: no repudio, confidencialidad, integridad, autenticidad y protección antirepetición mediante dos protocolos : Authentication Header (AH) y Encapsulated Security Payload (ESP).

---

<sup>12</sup> HEVIA, Mariano. Virtual Private Networks.

#### **1.3.5.4 Tecnología de firewall.**

Un firewall es un sistema o grupo de sistemas que impone una política de filtrado de flujo de red entre la red privada de una organización y las redes externas (incluye a Internet). El firewall determina cual de los servicios de red pueden ser accesados dentro de ésta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información de las redes externas deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico y el mismo podrá ser inmune a la penetración.

Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

## **1.4 CONCEPTOS DE SEGURIDAD**

### **1.4.1 INTRODUCCIÓN**

Desde el surgimiento de la raza humana en el planeta, la información estuvo presente bajo diversas formas y técnicas. El hombre buscaba representar sus hábitos, costumbres e intenciones en diversos medios que pudiesen ser utilizados por él y por otras personas, además de la posibilidad de ser llevados de un lugar a otro. La información valiosa era registrada en objetos preciosos y sofisticados, pinturas magníficas, entre otros, que se almacenaban con mucho cuidado en locales de difícil acceso, a cuya forma y contenido sólo tenían acceso quienes estuviesen autorizados o listos para interpretarla.

En la actualidad la información es el objeto de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación nos presenta un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales, y, en muchos casos, llegando a tener un valor superior. Por esto y otros motivos, la

seguridad de la información es un asunto tan importante para todos, pues afecta directamente a los negocios de una empresa o de un individuo.

#### **1.4.2 ENFOQUE**

Este trabajo no se pretende adentrarse en temas de seguridad que se podría considerar “de alto nivel”, como la necesaria en un entorno militar, de inteligencia, en una gran empresa que maneje datos muy útiles para sus competidores o en otro tipo de entornos que involucran gran peligro.

Un fallo en la seguridad de los sistemas informáticos de una central nuclear puede ser catastrófico. Un pequeño fallo en los sistemas encargados de lanzar un satélite costaría miles de millones de dólares, o si en lugar de ser un satélite es un misil, las consecuencias serían nefastas. Por fortuna para todos nosotros, esos sistemas son altamente seguros y por supuesto no son simples ordenadores conectados a Internet ni siquiera a redes de propósito general.

Lo más probable es que todas estas cosas queden demasiado lejos a la mayoría de los mortales. Los problemas de seguridad diarios son intrusiones, virus, negaciones de servicio contra un servidor dado, es decir, algo mucho más terrenal que todo lo anterior. Es en este tipo de entornos donde los mecanismos que se estudiarán se pueden aplicar mas fácilmente, tanto por las características de los sistemas utilizados como por el “relativamente” bajo peligro de los atacantes, los intrusos potencialmente interesados en nuestras máquinas serán individuos que sólo buscan un cierto status social en un grupo de aficionados a la piratería, o que vieron una película y tratan de emular a los actores. Gente que ante la más mínima dificultad para acceder a una red, la abandonará y se dedicará a objetivos más fáciles. Contra este tipo de personas es contra quien han de dedicarse mayores esfuerzos. Es inútil intentar parar a un atacante profesional, pagado, o muy interesado en nuestras máquinas o sistemas; el que su ataque tenga éxito es sólo cuestión de tiempo, y seguramente depende más de la suerte que tenga él frente a la que tengamos nosotros.

Pero estos atacantes son minoría, y lo que debemos buscar es defendernos contra la mayoría.

Los conceptos de seguridad aquí tratados se aplican a redes “normales”, las cuales se entienden como entornos con unos requerimientos de seguridad medios. Como ejemplos de estas redes tenemos: redes de investigación y desarrollo (universidades, centros de investigación, etc.), las de empresas medianas y las de proveedores de acceso a Internet.

### 1.4.3 DEFINICIÓN

Podemos entender a la seguridad como una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadores, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) mas que de seguridad; por tanto, se habla de sistemas fiables en lugar de sistemas seguros<sup>13</sup>.

De ahora en adelante se usará el concepto de *seguridad de la información* y no simplemente de *seguridad*, para poder dar enfoque a los sistemas informáticos.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos: integridad, confidencialidad y disponibilidad<sup>14</sup>.

**Integridad:** Significa que los objetos sólo pueden ser modificados por elementos autorizados, y de una manera controlada.

---

<sup>13</sup> VILLALON, Antonio. Seguridad en Unix y Redes v2.1

<sup>14</sup> ACADEMIA Latinoamericana de seguridad informática. Modulo 1

Este aspecto nos permite garantizar que la información no ha sido alterada en su forma y contenido, por tanto, es íntegra. Una información íntegra es una información que no ha sido alterada de forma indebida o no autorizada.

Por lo tanto, para garantizar la integridad, es necesario que todos los elementos que componen la base de gestión de la información se mantengan en sus condiciones originales definidas por sus responsables y propietarios.

La quiebra de integridad ocurre cuando la información se corrompe, falsifica o burla.

**Confidencialidad:** La confidencialidad nos dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.

Garantizar la confidencialidad es una de las tareas más difíciles de implementar, pues involucra a todos los elementos que forman parte de la comunicación de la información, desde su emisor, el camino que ella recorre, hasta su receptor. Y también, cuanto más valiosa es una información, mayor debe ser su grado de confidencialidad.

Pérdida de confidencialidad significa pérdida de secreto.

**Disponibilidad:** Indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados; es el contrario de la negación de servicio.

Una vez que nos aseguramos que la información correcta llegue a los destinatarios o usuarios correctos, ahora lo que debemos garantizar es que llegue en el momento oportuno. Se refiere a la disponibilidad de la información y de toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento.

#### **1.4.4 ELEMENTOS A PROTEGER.**

Lo que la seguridad de la información busca proteger son los elementos que forman parte de la comunicación<sup>15</sup>:

---

<sup>15</sup> ACADEMIA Latinoamericana de seguridad informática. Modulo 1

- Información.
- Equipos que la soportan.
- Personas que la utilizan

Estos tres elementos son conocidos con el nombre de *activos*. Un activo es todo aquel elemento que compone el proceso de la comunicación, partiendo desde la información, su emisor, el medio por el cual se transmite, hasta su receptor. Los activos son elementos que la seguridad de la información busca proteger. Los activos poseen valor para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados.

#### **1.4.4.1 Información.**

Información registrada en medio electrónico o físico, que sea de importancia para la empresa y sus negocios.

Algunos ejemplos son:

- Documentos
- Informes
- Manuales
- Patentes
- Información de mercado
- Código de programación
- Planillas de sueldos de empleados
- Plan de negocios de una empresa, etc.

Posibles vulnerabilidades: robo de documentos, pérdida de archivos de configuración, etc.

#### **1.4.4.2 Equipos que la soportan.**

Dentro de esta categoría se encuentran: software, hardware y organización.

##### *1.4.4.2.1 Software*

Todos los programas de computadora que se utilizan para la automatización de procesos, es decir, acceso, lectura, tránsito y almacenamiento de la información.



Posibles vulnerabilidades: fallas publicadas no reparadas que puedan representar accesos indebidos a los equipos, pérdida de los sistemas de respaldo, etc.

#### *1.4.4.2.2 Hardware.*

Representa toda la infraestructura tecnológica que brinda soporte a la información durante su uso, tránsito y almacenamiento. Es todo el conjunto formado por todos los elementos físicos de un sistema informático.

Posibles vulnerabilidades: Fallas eléctricas, inundaciones, robo de equipos portátiles, etc.

#### *1.4.4.2.3 Organización.*

Aspectos que componen la estructura física y organizativa de las empresas. Representa a la organización lógica y física que tiene el personal dentro de la empresa.

Posibles vulnerabilidades: Ubicación insegura de equipos, documentos o personas, estructura organizacional que no permita los cambios necesarios en materia de seguridad.

#### **1.4.4.3 Personas que la utilizan.**

Individuos que utilizan la estructura tecnológica y de comunicación de la empresa y que manejan la información.

El enfoque de la seguridad en los usuarios, está orientado hacia la toma de conciencia de formación del hábito de la seguridad para la toma de decisiones y acción por parte de todos los empleados de una empresa, desde su alta dirección hasta los usuarios finales de la información, incluyendo los grupos que mantienen en funcionamiento la estructura tecnológica, como los técnicos, operadores y administradores de ambientes tecnológicos.

Posibles vulnerabilidades: olvido de contraseñas, falta de cooperación por parte de los usuarios en materia de seguridad, descuido de parte de los usuarios en el manejo de la información, etc.

De los tres elementos vistos anteriormente, la información constituye el principal elemento a proteger, por ser el más amenazado y el más difícil de recuperar. Un sistema operativo puede ser reinstalado al igual que una aplicación, se pueden restaurar sin problemas desde su medio original, sin embargo en el caso de la información, no existe un medio original desde el cual restaurar.

#### **1.4.5 AMENAZAS, VULNERABILIDADES Y RIESGOS.**

##### **1.4.5.1 Definiciones**

**Amenazas:** Son agentes capaces de explotar los fallos de seguridad, que denominamos *puntos débiles* y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa o persona, afectando a sus negocios o actividades<sup>16</sup>.

Las amenazas son constantes y pueden ocurrir en cualquier momento.

**Puntos débiles o vulnerabilidades:** Son los elementos que, al ser explotados por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o empresa<sup>17</sup>.

**Riesgo:** Es la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando la confidencialidad, la integridad y la disponibilidad de la información<sup>18</sup>.

Uno de los objetivos de la seguridad de la información es impedir que las amenazas exploten puntos débiles y afecten alguno de los principios básicos de la seguridad de la información (integridad, disponibilidad, confidencialidad), causando daños al negocio de las empresas.

Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles de un ambiente de tecnología de la información. Al

---

<sup>16/17/18</sup> ACADEMIA Latinoamericana de seguridad informática. Modulo 1

ser identificados los puntos débiles, será posible dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección.

Otro objetivo de la seguridad de la información es la corrección de puntos débiles existentes en el ambiente en que se usa la información, con el objeto de reducir los riesgos a que está sometida, evitando así la concretización de una amenaza.

#### **1.4.5.2 Tipos de amenazas.**

**Amenazas Naturales:** Condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos.

**Intencionales:** Son amenazas deliberadas, fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.

**Involuntarias:** Son amenazas resultantes de acciones inconscientes de usuarios, por virus electrónicos (software malicioso en general), muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores y accidentes.

Entre las amenazas más frecuentes se encuentran: la ocurrencia de virus, la divulgación de contraseñas y la acción de hackers<sup>19</sup>.

#### **1.4.5.3 Tipos de vulnerabilidades.**

**Físicas:** Son aquellas presentes en los ambientes en los cuales la información se está almacenando o manejando.

Como ejemplos de este tipo de vulnerabilidad se distinguen: instalaciones inadecuadas del espacio de trabajo, ausencia de recursos para el combate a incendios; disposición desorganizada de cables de energía y de red, ausencia de identificación de personas y de locales, etc.

Estos puntos débiles, al ser explotados por amenazas, afectan principalmente la disponibilidad.

---

<sup>19</sup> ACADEMIA Latinoamericana de seguridad informática. Modulo 1

**Naturales:** Aquellas relacionados con las condiciones de la naturaleza que puedan colocar en riesgo la información.

La probabilidad de estar expuestos a las amenazas naturales es determinante en la elección y montaje de un ambiente. Se deberán tomar cuidados especiales con el local, de acuerdo con el tipo de amenaza natural que pueda ocurrir en una determinada región geográfica.

Entre los ejemplos de este tipo de vulnerabilidad se encuentran: ambientes sin protección contra incendios, locales próximos a ríos propensos a inundaciones, infraestructura incapaz de resistir a las manifestaciones de la naturaleza como terremotos, maremotos, huracanes etc.

**De Hardware:** Los posibles defectos en la fabricación o configuración de los equipos de la empresa que pudieran permitir el ataque o alteración de los mismos. Como ejemplos tenemos: la ausencia de actualizaciones conforme con las orientaciones de los fabricantes de los programas que se utilizan, conservación inadecuada de equipos, falta de configuración de respaldos o equipos de contingencia.

**De Software:** Los puntos débiles de aplicaciones permiten que ocurran accesos indebidos a sistemas informáticos incluso sin el conocimiento de un usuario o administrador de red.

Encontramos vulnerabilidades en las aplicaciones (en sus configuraciones o instalaciones indebidas de estos programas) y en los sistemas operativos.

Ejemplos de vulnerabilidades en las aplicaciones: clientes de e-mail que permiten la ejecución de códigos maliciosos, editores de texto que permiten la ejecución de virus de macro, etc.

Ejemplos de vulnerabilidades en los sistemas operativos: configuración e instalación inadecuada, ausencia de actualización, programación insegura etc.

**De Medios de Almacenamiento:** Son los soportes físicos o magnéticos que se utilizan para almacenar la información. Entre los tipos de soporte o medios de almacenamiento de la información que están expuestos podemos citar: disquetes, CD-ROMs, cintas magnéticas, discos duros, así como lo que está registrado en papel.

Si los soportes que almacenan información, no se utilizan de forma adecuada, el contenido en los mismos podrá estar vulnerable a una serie de factores que podrán afectar la integridad, disponibilidad y confidencialidad de la información. Los medios de almacenamiento podrán ser afectados por puntos débiles que podrán dañarlos e incluso dejarlos indisponibles.

Como ejemplos tenemos: plazo de validez y caducidad, defecto de fabricación uso incorrecto, lugar de almacenamiento en locales insalubres o con alto nivel de humedad, magnetismo o estática, moho, etc.

**De Comunicación:** Abarca todo el tránsito de la información. Donde sea que la información transite, ya sea vía cable, satélite, fibra óptica u ondas de radio, debe existir seguridad. El éxito en el tránsito de los datos es un aspecto crucial en la implementación de la seguridad de la información.

Hay un gran intercambio de datos a través de medios de comunicación que rompen barreras físicas tales como teléfono, Internet, WAP, fax, télex etc.

Siendo así, estos medios deberán recibir tratamiento de seguridad adecuado con el propósito de evitar que:

- Cualquier falla en la comunicación haga que una información quede no disponible para sus usuarios, o por el contrario, estar disponible para quien no posee derechos de acceso.
- La información sea alterada en su estado original, afectando su integridad.

Por lo tanto, la seguridad de la información también está asociada con el desempeño de los equipos involucrados en la comunicación, pues se preocupa por: la calidad del ambiente que fue preparado para el tránsito, tratamiento, almacenamiento y lectura de la información.

Ejemplos de este estilo pueden ser: ausencia de sistemas de encriptación en las comunicaciones que pudieran permitir que personas ajenas a la organización obtengan información privilegiada, mala elección de sistemas de comunicación para envío de mensajes de alta prioridad de la empresa pudiera provocar que no alcanzaran el destino esperado o bien se intercepte el mensaje en su tránsito.

**Humanas:** Esta categoría de vulnerabilidad está relacionada con los daños que las personas pueden causar a la información y al ambiente tecnológico que la soporta. Los puntos débiles humanos también pueden ser intencionales o no. Muchas veces, los errores y accidentes que amenazan a la seguridad de la información ocurren en ambientes institucionales. La mayor vulnerabilidad es el desconocimiento de las medidas de seguridad adecuadas para ser adoptadas por cada elemento constituyente, principalmente los miembros internos de la empresa.

Destacamos dos puntos débiles humanos por su grado de frecuencia:

- La falta de capacitación específica para la ejecución de las actividades inherentes a las funciones de cada uno.
- La falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, insatisfacciones etc.

En lo que se refiere a las vulnerabilidades humanas de origen externo, podemos considerar todas aquéllas que puedan ser exploradas por amenazas como: vandalismo, estafas, invasiones, etc.

Ejemplos de este tipo de vulnerabilidad: contraseñas débiles, falta de uso de criptografía en la comunicación, compartimiento de identificadores tales como nombre de usuario o credencial de acceso, etc.

#### **1.4.5.4 Cómo Protegerse.**

Para proteger un sistema se debe realizar un análisis de las amenazas potenciales que puede sufrir, las pérdidas que podrían generarse, y la probabilidad de su ocurrencia; a partir de este análisis se diseña una política de seguridad que defina responsabilidades y reglas a seguir para evitar tales amenazas o minimizar sus efectos en caso de que se produzcan. A los mecanismos utilizados para implementar esta política de seguridad se les denomina *mecanismos de seguridad*; constituyen la herramienta básica para garantizar la protección de los sistemas<sup>20</sup>.

---

<sup>20</sup> VILLALON, Antonio. Seguridad en Unix y Redes v2.1.

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación.

Los mecanismos de prevención son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad; por ejemplo, el uso de cifrado en la transmisión de datos se puede considerar un mecanismo de este tipo, ya que evita que un posible atacante escuche las conexiones hacia o desde un sistema en la red.

Por mecanismos de detección se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación; ejemplos de estos mecanismos son los programas de auditoria.

Finalmente, los mecanismos de recuperación son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste a su funcionamiento correcto; ejemplos de estos mecanismos son la utilización de copias de seguridad o el *hardware* adicional. Dentro de este último grupo de mecanismos de seguridad se encuentra un subgrupo denominado mecanismos de análisis forense, cuyo objetivo no es simplemente retornar al sistema a su modo de trabajo normal, sino averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de nuestra red.

## **CAPITULO II**

### **2 REDISEÑO DE LA INFRAESTRUCTURA INTERED**

#### **2.1 ESTADO ACTUAL**

##### **2.1.1 DESCRIPCIÓN DE LA EMPRESA.**

###### **2.1.1.1 Historia.**

El presente trabajo fue realizado para una empresa constructora ubicada en la ciudad de Guayaquil, la cual se encuentra entre las empresas líderes en su ramo debido al tipo y gran cantidad de obras que han sido construidas bajo su dirección.

Esta empresa fue fundada en 1982 y durante su existencia ha demostrado una constante actividad en el campo de la ingeniería y la construcción tanto en el sector público como en el privado.

Sus inicios fueron con proyectos de viviendas de interés social, para luego en su constante conquista del mercado asumir la responsabilidad de la planificación, construcción y comercialización de: edificios comerciales y residenciales, centros educativos, estaciones de servicios, mercados, presas de tierra, sistemas de alcantarillado pluvial, y de aguas servidas, plantas de tratamiento, lagunas de estabilización y sistemas de agua potable.

En el presente año incursionaron en el sistema de “Diseño, Construcción y Financiamiento” para el cuerpo de ingenieros del ejército de los Estados Unidos en la Base Aérea de Manta, calificándolos como contratistas en esta organización Global.

###### **2.1.1.2 Misión.**

Esta es una empresa en constante crecimiento, comprometida a producir bienes y servicios en el Ecuador y en los países donde se encuentre mediante



la Planificación, Producción y Comercialización de todo tipo de edificaciones, productos inmobiliarios, obras de saneamiento ambiental y de infraestructura general de excelente calidad, generando riquezas morales y materiales para el cliente, la empresa y la comunidad.

Cultura empresarial:

- Actitud positiva al cambio.
- Innovación constante.
- Trabajo en equipo.
- Vocación de servir.
- Autoresponsabilidad.
- Integración y compañerismo.
- Convivencia en armonía.

#### **2.1.1.3 Visión.**

La mencionada empresa, al año 2005, será líder en planificación y construcción de obras de saneamiento ambiental, estaciones de servicios, mercados, proyectos de regeneración urbana y edificaciones en general; gozará de la confianza de organismos internacionales en señal de alta valoración que merecerá su profesionalismo y calidad competitiva de sus obras, que le crearán ventajas significativas en los concursos existentes.

#### **2.1.1.4 Estrategia.**

Esta empresa direccionará sus gestiones propiciando el mejoramiento profesional de su personal frente a las nuevas tecnologías, educando y formando nuevos líderes empresariales; buscará optimizar las comunicaciones intra y extra institucional, impulsando la autogestión.

#### **2.1.1.5 Metas.**

Al 2005 esta empresa tiene como meta general dotarse de la infraestructura tecnológica a nivel de recursos humanos y materiales que le permitan la autogestión. También lograr la unificación de la comunicación interna y de la comunicación institucional, siempre para obtener que la sociedad tenga una visión unificada de la empresa.

### **2.1.1.6 Política de calidad de la organización**

Esta es una organización que determina la calidad como fundamento de su filosofía institucional: por consiguiente, utiliza la siguiente política como medio para hacer operativa su Misión y Visión. La política de calidad tiene como sigla **VET** que identifica los siguientes medios:

V: Valores institucionales.

E: Eficiencia y eficacia en el trabajo.

T: Trabajo en equipo.

#### *2.1.1.6.1 Valores Institucionales.*

Primordialmente respeto a las personas denominadas clientes internos y externos, así como a la comunidad en general.

Este respeto se manifiesta en los siguientes valores integrados:

- Amabilidad: calidez en el rostro y trato educado.
- Responsabilidad: cumplimiento de las funciones y procedimientos.
- Honestidad: manifestando siempre la verdad.
- Lealtad: actuando de manera consecuente con la empresa y sus integrantes.
- Compañerismo: brindando apoyo a todo el personal.
- Puntualidad: haciendo el mejor uso del tiempo.
- Seguridad: valorando la vida personal y la de los demás así como el cuidado del patrimonio de la institución.

#### *2.1.1.6.2 Eficiencia y Eficacia.*

La empresa trabaja por resultados obtenidos eficientemente. Se determinan los siguientes criterios como importantes para este fin:

- Utilización de la planificación estratégica y operativa identificando metas, objetivos y programas de trabajo.
- Optimización de la comunicación a través del desarrollo de competencias básicas: escucha activa, asertividad, negociación y solución de conflictos, y control emocional.
- Empleo adecuado de los avances tecnológicos desarrollando una cultura informática en beneficio del desarrollo personal e institucional.

- Desarrollo de actividad evaluadora para retroalimentar permanentemente el desarrollo del trabajo utilizando criterios e indicadores objetivos.

#### 2.1.1.6.3 *Trabajo en Equipo.*

El personal se organizará en equipos conducidos por líderes que ejercen el mando. Estos equipos se integran para el logro de metas, cumplimiento de funciones y aplicación de procedimientos establecidos.

El trabajo en equipo articula la dinámica de la eficiencia y la eficacia, teniendo como valor implícito el mejoramiento continuo del desarrollo personal y profesional.

### **2.1.2 FLUJO DE PROCESOS.**

El proceso general en la construcción de una obra consta de la siguiente serie de pasos:

1. La gerencia de acuerdo a sus contactos o conocimientos del negocio busca licitaciones, obteniendo de esta manera las bases para concursar.
2. El área de presupuestos genera un presupuesto preliminar llamado Presupuesto Licitatorio y prepara toda la documentación contractual.
3. La documentación preparada es enviada para concursar.
4. Si la obra no es adjudicada, toda la documentación preparada es archivada.
5. Si el concurso ha sido ganado, la Superintendencia General de la compañía desarrolla toda la planificación de la obra, lo que implica, entre otras cosas, afinar el Presupuesto Licitatorio (el precio unitario no podrá ser alterado), y preparar el resto de documentación contractual.

6. Gerencia y Presidencia estudian la documentación preparada hasta el momento para dar su aprobación. En caso de que la documentación no sea aprobada, Superintendencia General realiza las correcciones pertinentes.
7. Una vez que Gerencia y Presidencia dan su aprobación, de manera coordinada entre Superintendencia General y el área de Presupuestos, al presupuesto se le agregan los detalles necesarios para dar inicio a los trabajos de la obra obteniéndose el Presupuesto Detallado Inicial. Se genera también el Cronograma Inicial.
8. Cuando los trabajos de construcción de la obra se encuentran en marcha, el Superintendente de Obra solicita recursos (material, mano de obra, equipo) semanalmente a través de una Nota de Pedido.
9. En las oficinas centrales se verifican los requerimientos contra el presupuesto utilizando el sistema de presupuestos.
10. El área de compras se contacta con varios proveedores para solicitar mínimo tres cotizaciones.
11. El área de compras evalúa las cotizaciones y selecciona la más conveniente.
12. Gerencia y Presidencia se contactan con el proveedor para negociar valores, cantidades y plazos.
13. Desde las oficinas centrales se notifica a la obra de la entrega de materiales que realizará el proveedor. El proveedor entrega la mercadería en la obra con la guía de remisión.
14. En la obra, el Superintendente de Obra registra en el sistema de inventarios las cantidades de productos entregados asociados a un número de guía de remisión.

15. De manera cotidiana es necesario sacar materiales de la bodega de obra, para lo cual se realiza una validación contra stock. Si la validación arroja una respuesta negativa, el Superintendente de Obra generará una Nota de Pedido.
16. Si existe suficiente material en bodega, en el sistema de inventarios se realiza un egreso de mercadería. En el egreso constan solamente cantidades.
17. En las oficinas centrales el área de Presupuestos realiza una comparación mensual de los últimos valores presupuestados y gastados, generando de esta manera el Presupuesto Detallado Ajustable.
18. En las oficinas centrales el área de Contabilidad realiza los registros pertinentes en el sistema de contabilidad utilizando la factura entregada por el proveedor.
19. El área de contabilidad emite el cheque correspondiente para pagar al proveedor.
20. Si la construcción aún no llega a su fin, el Superintendente de Obra generará una nueva Nota de Pedido.
21. Si la construcción de la obra ha concluido se efectúa el cierre de obra.

Cabe anotar lo siguiente:

- Cuando la información necesita enviarse desde cualquier obra hasta la oficina central y viceversa, se la transporta en disquetes.
- Todos los sistemas mencionados están basados en plataforma D.O.S.
- No se usa un sistema de gestión de bases de datos.
- El único sistema que existe en cualquiera de las obras es el de inventarios.

Esta serie de pasos se muestran en la siguiente figura.

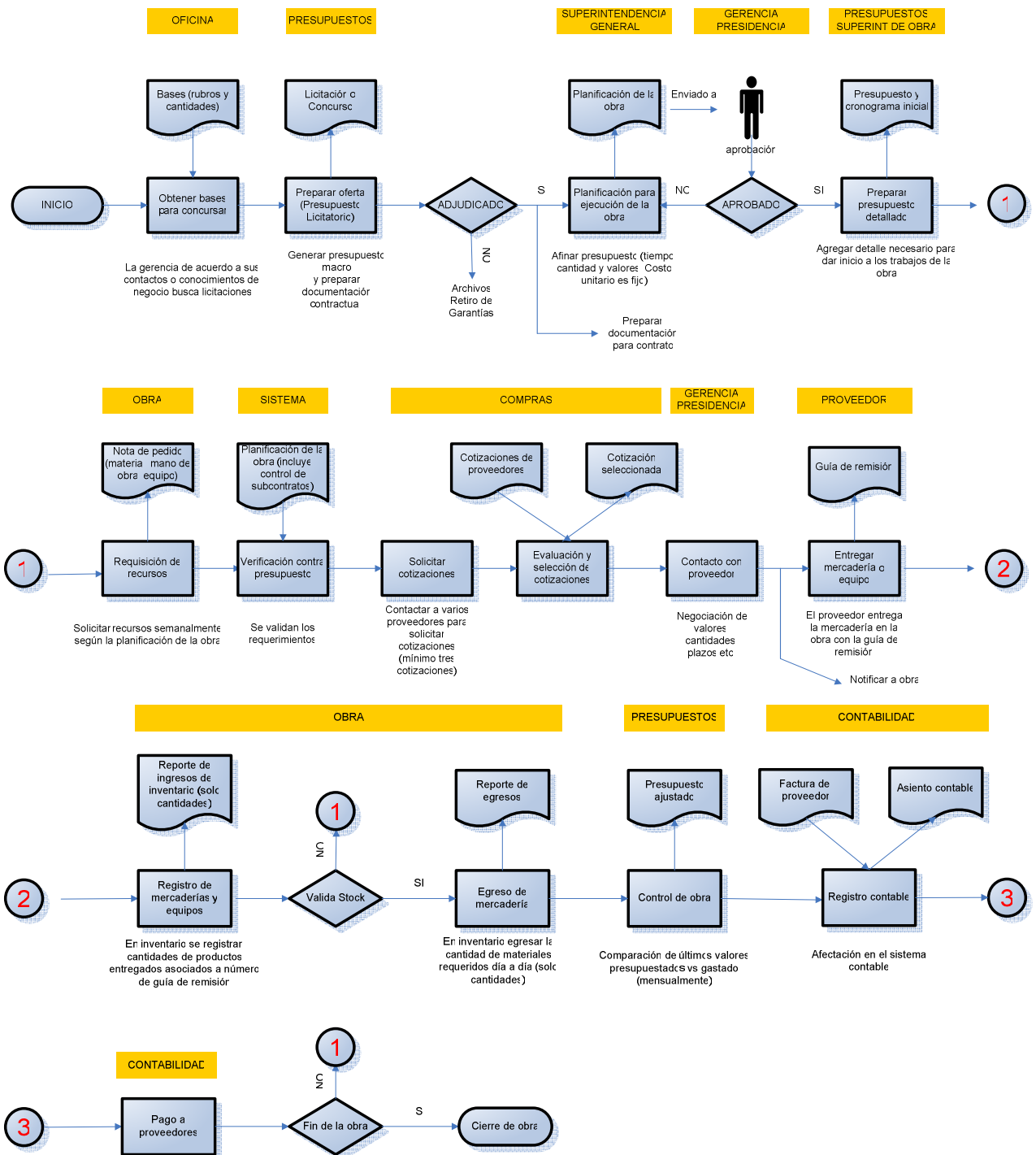


Figura 2.1 Flujo de procesos empleados en las actividades de construcción.

### 2.1.3 RED FÍSICA.

Actualmente la red física de la empresa consta de una red LAN en la oficina central y en cada obra, todas éstas independientes entre sí. Únicamente en la oficina central existe acceso a Internet. Todas las redes se encuentran en un ambiente de grupo de trabajo (workgroup).

Los computadores son equipos clones cuyas características son las siguientes:

Ubicación	Nombre de PC	Procesador	Memoria	Disco	Sistema Operativo
Oficina Central	contab1	Pentium II	128MB	20GB	Windows98
Oficina Central	contab2	Pentium II	64MB	20GB	Windows98
Oficina Central	contab3	Pentium II	64MB	20GB	Windows98
Oficina Central	contab4	Pentium I	32MB	10GB	Windows98
Oficina Central	presup1	Pentium II	64MB	20GB	Windows98
Oficina Central	presup2	Pentium II	64MB	20GB	Windows98
Oficina Central	presup3	Pentium I	64MB	20GB	Windows98
Oficina Central	presup4	Pentium I	64MB	20GB	Windows98
Oficina Central	presup5	Pentium I	64MB	20GB	Windows98
Oficina Central	presidencia	Pentium II	64MB	20GB	Windows98
Oficina Central	gerencia	Pentium II	64MB	20GB	Windows98
Oficina Central	recepcion	Pentium I	32MB	10GB	Windows98
Oficina Central	temp1	Pentium II	64MB	20GB	Windows98
Oficina Central	temp2	Pentium II	64MB	20GB	Windows98
Oficina Central	ecuaserver	Pentium II	256MB	40GB	Windows2000 Server
Obra-esmeraldas	esme1	Pentium II	64MB	20GB	Windows98
Obra-esmeraldas	esme2	Pentium II	64MB	20GB	Windows98
Obra-esmeraldas	esme3	Pentium II	64MB	20GB	Windows98
Obra-trinitaria	trinitaria1	Pentium II	64MB	20GB	Windows98
Obra-trinitaria	trinitaria2	Pentium II	64MB	20GB	Windows98
Obra-trinitaria	trinitaria3	Pentium II	64MB	20GB	Windows98

Tabla 2.1 Características de computadores de la red actual<sup>21</sup>.

El equipo denominado “ecuaserver” desempeña las funciones de servidor de archivos y punto de acceso a Internet.

<sup>21</sup> Las obras en construcción al inicio del presente trabajo son las mencionadas en la tabla 2.2

Las impresoras son las siguientes:

Marca	Modelo
EPSON	FX-980
EPSON	FX-890
EPSON	FX-2170
EPSON	STYLUS C83
EPSON	LX-300
HP	LASER JET 1200
HP	DESKJET 695C
HP	LASER JET 4100
HP	LASER JET 1200
LEXMARK	Z25

Tabla 2.2 Listado de impresoras de la red actual.

El equipo de comunicación es el siguiente:

- Switch 3Com de 20 puertos (oficina central).
- Patch Panel de 20 puertos (oficina central).
- Switch de 8 puertos (uno en cada obra, ver tabla 2.2)

La red de la oficina central consta de cableado estructurado y un enlace a Internet dial-up de 64Kbps. Todas las estaciones de trabajo de la oficina central poseen acceso a Internet. La siguiente figura muestra la configuración de la red física de la oficina central (ver siguiente página).





Figura 2.2. Red física correspondiente al segundo piso de la empresa constructora.

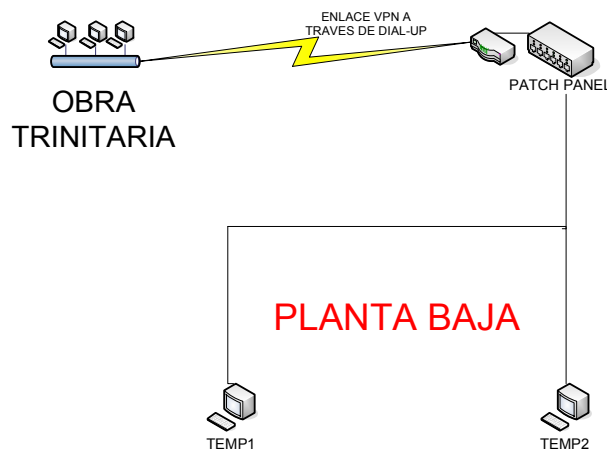


Figura 2.3. Red física correspondiente a la planta baja de la empresa constructora.

## 2.1.4 SEGURIDADES.

### 2.1.4.1 Seguridad Física.

En lo relacionado a la seguridad de las instalaciones físicas se tiene:

- Guardia de seguridad las 24 horas, los 7 días de la semana.
- Puerta metálica de acceso al edificio.
- Puerta de acceso a las dependencias de la planta baja.
- Puerta de acceso al segundo piso.
- En todo el edificio se cuenta con sistemas de aire acondicionado.
- Recepción cuenta con una cámara de vigilancia ubicada en la puerta de entrada al edificio.

En lo relacionado a la seguridad del equipo de cómputo:

- Únicamente 5 computadores poseen regulador de voltaje.
- El servidor no posee un dispositivo de provisión ininterrumpida de energía eléctrica (UPS).
- El área donde se encuentra el servidor es totalmente accesible.

### 2.1.4.2 Seguridad Lógicas.

- No existe configurado un ambiente de dominio, es decir, la red opera bajo un ambiente de grupo de trabajo.
- No existe un servidor cortafuegos.

- Todo computador posee acceso a Internet a pesar de que determinado personal no lo requiere.
- No existe política de actualización del sistema operativo. La aplicación antivirus no es actualizada de forma adecuada.
- Los jefes de las áreas de presupuestos y contabilidad realizan respaldos de sus respectivos sistemas en el servidor de archivos cada vez que lo crean necesario.
- No existe control sobre las impresiones. Todo el personal puede imprimir en cualquier impresora a la que tenga acceso.

## **2.2 ALCANCE**

El presente trabajo inicia con un análisis de la situación actual de la empresa en aspectos tales como seguridades físicas y lógicas, internas como externas, configuración de la red LAN y VPN, y servicios requeridos, para diseñar e implantar soluciones adecuadas a las necesidades presentes de la empresa.

Teniendo en mente el concepto de seguridad, se expedirán una serie de políticas que mejoren la estabilidad de la red sin afectar el trabajo cotidiano de todo el personal.

Las políticas de seguridad se enfocarán prioritariamente en la seguridad lógica de la oficina central, luego en las obras en construcción. No se realizará énfasis en la seguridad física, aunque sí será tomada en cuenta.

Se implantará una aplicación web de control de presupuestos de obras públicas la cual resultará de gran utilidad en el seguimiento cotidiano de las diferentes obras. Esta aplicación cuenta con la ventaja de proporcionar información en línea y en tiempo real a cualquier hora y desde cualquier lugar. Debido a la naturaleza de la información que maneja esta aplicación, se implantarán comunicaciones seguras mediante SSL entre el servidor web que hospeda la mencionada aplicación y cualquier terminal que haga uso de ella.

## **2.3 OBJETIVOS**

### **2.3.1 OBJETIVO GENERAL.**

Rediseñar la red LAN y VPN de la empresa tomando en cuenta aspectos de seguridad lógica y física así como nuevos servicios, acorde a las necesidades actuales de la empresa.

### **2.3.2 OBJETIVOS ESPECÍFICOS.**

Analizar las prácticas de seguridad lógica y física presentes, para implementar los cambios pertinentes según las necesidades actuales de la empresa.

Implantar nuevos servicios necesarios según requerimientos administrativos y operacionales de la empresa.

Analizar la configuración actual de la red LAN y VPN de la empresa, tomando en cuenta los objetivos anteriores, para aplicar un rediseño acorde a las necesidades actuales de la empresa.

## **2.4 ANÁLISIS DE REQUERIMIENTOS**

### **2.4.1 TIPOS DE SERVICIOS REQUERIDOS.**

Debido a la dinámica empresarial actual, las necesidades del personal son las siguientes:

#### **Necesidades de comunicación.**

- Dotar al personal de un servicio adecuado que responda a sus necesidades de comunicación internas (compañeros de trabajo, obras en construcción) como externas (socios de negocios, clientes, proveedores).
- Mejorar la coordinación en el trabajo compartido entre la oficina central y las obras en construcción.
- Evitar el uso excesivo de papel.

El servicio adecuado para satisfacer estas necesidades es el de Correo Electrónico.

**Necesidades de conectividad.**

- Conectividad entre la oficina central y las obras en construcción con la finalidad de extender la utilización de la aplicación de control de presupuestos a las obras en construcción.
- Comunicaciones seguras entre la oficina central y las obras en construcción debido a que el sistema de control de presupuestos maneja información crítica, la cual tiene el carácter de confidencial.
- Debido a la cantidad y naturaleza de trabajo realizado por todo el personal, se han contratado los servicios profesionales de asistencia técnica y de mantenimiento de la red informática a una empresa ubicada en la ciudad de Quito. Para mejorar estos servicios es necesario contar con un enlace permanente entre estas dos empresas.

El servicio de conectividad será implantado en dos fases:

Como se estableció en el numeral 2.2, la nueva aplicación será una aplicación Web que ofrece comunicaciones seguras, para lo cual se implantarán enlaces punto a punto entre la oficina central y las obras en construcción. La justificación de la implantación de estos enlaces en lugar de enlaces VPN se encuentra en el numeral 2.6

La empresa constructora y la empresa que brinda los servicios de asistencia técnica se mantendrán enlazadas por medio de un enlace permanente de Red Privada Virtual con la finalidad de conseguir confidencialidad en las comunicaciones.

**Necesidades de planificación de tareas.**

Según el nivel de responsabilidad que el personal posea, el número de actividades a realizar se incrementa notoriamente, de manera que se requiere llevar un registro de las actividades realizadas y planificar otras.

El tercer servicio a implantar es el de Calendario Electrónico.

## 2.4.2 TIPO DE HARDWARE REQUERIDO

En actividad coordinada conjuntamente con los niveles directivos de la empresa se decidió que los computadores para las estaciones de trabajo y servidores sean de una marca reconocida en el mercado.

Tomando en cuenta las expectativas de crecimiento empresarial, se estableció que para las estaciones de trabajo el hardware sea el siguiente:

Componente	Valor	Cantidad
Disco duro	80GB	1 disco
Procesador	Pentium IV	1 procesador
Memoria	512MB	1 banco
Tarjeta de red	Fast Ethernet 10/100	1 tarjeta

Tabla 2.3 Características de hardware para las estaciones de trabajo de la oficina central.

Para los equipos servidores se tiene:

- Servidor cortafuegos y de acceso a Internet:

Componente	Valor	Cantidad
Disco duro	80GB	1 disco
Procesador	Pentium IV	1 procesador
Memoria	512MB	1 banco
Tarjeta de red	Fast Ethernet 10/100	2 tarjetas

Tabla 2.4 Características de hardware para el servidor cortafuegos.

- Servidor controlador de dominio:

Componente	Valor	Cantidad
Disco duro	160GB	2 discos/80GB
Procesador	Intel Xeon	1 procesador
Memoria	1GB	2 bancos/512MB
Tarjeta de red	Fast Ethernet 10/100	1 tarjeta

Tabla 2.5 Características de hardware para el servidor controlador de dominio.

### 2.4.3 TIPO DE SOFTWARE REQUERIDO.

En reuniones conjuntas con cada una de las áreas de la empresa (directiva, administrativa y operativa) se acordó continuar utilizando sistemas operativos y paquetes ofimáticos de Microsoft.

Esta decisión se basó en el hecho de que anteriormente en la red se encontraban instalados este tipo de productos de la marca mencionada, y por lo tanto el personal desarrolló destrezas de manejo en productos Microsoft.

#### 2.4.3.1 Software base.

Cantidad	Descripción	Utilización
1	Windows 2003 Server Enterprise Edition	Servidor controlador de dominio
1	SQL Server 2000 Standard Edition	Servidor controlador de dominio

Tabla 2.6 Software base a instalarse en el servidor controlador de dominio.

Debe aclararse que las licencias del sistema operativo de las estaciones de trabajo son de tipo OEM.

Se decidió instalar un sistema operativo Linux para el servidor cortafuegos debido a que la empresa que brinda el servicio de asistencia técnica posee mayor experiencia trabajando en la mencionada plataforma al configurar servidores destinados a este tipo de actividades y debido a temas de licenciamiento por reducción de costos.

#### 2.4.3.2 Software de productividad.

Recabando las necesidades de las diferentes áreas de la empresa, el software de productividad incluye:

- Paquetes ofimáticos:

Microsoft Word: Debido a que todo el personal necesita un procesador de palabras sea cual fuere su actividad dentro de la empresa.

Microsoft Excel: Todo el personal requiere realizar listados o cálculos matemáticos.

Microsoft Power Point: El área directiva necesita presentar las fortalezas de la empresa y trabajos realizados a quienes requieran contratar sus servicios.

Microsoft Outlook: Todo personal requerirá contar con una herramienta que le permita planificar actividades, llevar un registro histórico de las mismas y armar un listado de contactos.

Microsoft Project: Determinados ingenieros civiles realizan las tareas de planificación y concatenación de fases necesarias para llevar a cabo una obra de construcción.

- Paquetes de diagramación:

AutoCad: Muy útil herramienta de diagramación para el equipo de ingenieros civiles.

#### **2.4.3.3 Software de protección.**

- Software Antivirus:

McAfee VirusScan: Todo equipo que lleve instalado sistema operativo Microsoft deberá contar con este paquete antivirus. Se decidió emplear este producto debido a sus fortalezas como detector antivirus y porque actualmente se encuentra en uso en la red de la oficina central y los computadores de las obras.

- Software Antispyware:

Lavasoft AdAware: Gratuita herramienta antispyware.

#### **2.4.4 ANÁLISIS DE RIESGOS.**

Existen multitud de propuestas para realizar análisis de riesgos, pero todo método posee los siguientes puntos principales, los cuales se emplearán en el presente trabajo:<sup>22</sup>

---

<sup>22</sup> PELTIER, Thomas. Effective Risk Analysis.



- Identificación de activos a ser protegidos.
- Identificación las vulnerabilidades.
- Identificación de amenazas.
- Agrupación de activos en entidades.
- Evaluación del riesgo.
- Recomendación de controles.

De las dos técnicas de evaluación existentes, cualitativa y cuantitativa, se empleará la evaluación cualitativa por tratarse de una técnica sencilla, intuitiva y porque toma en cuenta una estimación de pérdidas potenciales; por el contrario, la evaluación cuantitativa involucra cálculos complejos y datos difíciles de estimar<sup>23</sup>.

En la evaluación cualitativa se emplearán los siguientes tres niveles:

- ALTO cuya abreviatura es A
- MEDIO cuya abreviatura es M
- BAJO cuya abreviatura es B

La evaluación del riesgo se lo consigue a través de tres pasos: evaluación de impacto, evaluación de probabilidad de ocurrencia y determinación de nivel de riesgo. Para este propósito se empleará la Matriz de Riesgo establecida por el Instituto Nacional de Estándares y Tecnología – NIST de los Estados Unidos (Ver Anexo A).

El detalle de la evaluación realizada en el presente proyecto consta a partir del numeral 2.4.4.5 “Evaluación del impacto” página 65.

#### **2.4.4.1 ACTIVOS A PROTEGER**

##### *2.4.4.1.1 PROCESOS*

Los procesos a ser tomados en cuenta dentro del presente análisis de riesgos son los involucrados en la construcción de una obra (ver figura 2.1) los cuales se encuentran detallados en el numeral 2.1.2 pero que se los realiza por medio

---

<sup>23</sup> VILLALON, Antonio. Seguridad en Unix y Redes v2.1

de las aplicaciones de control presupuestario o de contabilidad. Estos procesos se indican a continuación:

Procesos realizados por el sistema de presupuestos:

- Preparar la oferta, es decir, preparar el presupuesto licitatorio.
- Afinar el presupuesto licitatorio, lo que incluye el ingreso de información de la planificación de la obra.
- Preparar presupuesto detallado.
- Verificación contra presupuesto cuando se solicitan recursos por parte de la obra.
- Registro de ingreso mercaderías y equipos de bodega de obra tras realizar una compra a un proveedor.
- Registro de egreso de mercaderías y equipos de bodega de obra previa validación contra stock.
- Control de avance de obra el cual consiste en comparar los valores y cantidades gastadas versus los valores y cantidades del presupuesto detallado inicial.

Procesos realizados por el sistema de contabilidad:

- Registro contable de la factura del proveedor por concepto de bienes o servicios entregados en una determinada obra.
- Pago a proveedores.

#### *2.4.4.1.2 APLICACIONES*

- Sistema de presupuestos
- Sistema contable

Estas dos aplicaciones son sobre las cuales se apoya toda actividad de construcción de una obra, por lo tanto, son de índole crítica.

Cualquier tipo de falla sobre cualquiera de estas dos aplicaciones supondría una paralización de toda actividad de razón de ser de la empresa por el tiempo que tome llevar estas aplicaciones a su funcionamiento normal.

#### *2.4.4.1.3 SERVICIOS.*

- Enlace dial-up a Internet.

La empresa tiene contratado el servicio de acceso a Internet por medio de línea telefónica.

Cabe mencionar que existe queja por parte del personal que labora en la oficina central acerca de la frecuencia con la que cae este servicio.

Este servicio día a día se va tornando más necesario para cumplir con las necesidades de comunicación que la empresa ha adquirido con proveedores, clientes, socios de negocios y resto de personal.

#### *2.4.4.1.4 HARDWARE*

La empresa, en su oficina central, cuenta con un servidor y catorce estaciones de trabajo. El servidor permanece en funcionamiento las veinticuatro horas del día, los siete días de la semana, los trescientos sesenta y cinco días del año. Todas las estaciones de trabajo permanecen en funcionamiento entre ocho y diez horas al día los días laborables, y unas cuantas se encuentran en funcionamiento ciertos días feriados y fines de semana cuando el trabajo de la empresa así lo requiera.

Cada obra en proceso de construcción cuenta con una o dos estaciones de trabajo, las cuales son utilizadas entre ocho y diez horas en los días laborables.

Los computadores de la empresa son:

- Computador de gerencia.
- Computador de presidencia.
- Computador del jefe de presupuestos.
- Computador del jefe de contabilidad.
- Computadores del resto personal presupuestos.
- Computadores del resto personal de contabilidad.
- Computador de recepción.
- Computadores del área de equipos<sup>24</sup>.
- Computadores de obras.
- Servidor Compaq Proliant ML370.

Las características de cada uno de los nuevos computadores de la oficina central y de las obras en construcción se encuentran en el numeral 2.1.3.

---

<sup>24</sup> Equipos de construcción.

#### 2.4.4.1.5 *Equipo de comunicaciones.*

El siguiente es el equipo empleado para las comunicaciones internas (LAN de la oficina central) y externas (acceso a internet)

- Patch Panel
- Switch
- Modem del servidor

#### 2.4.4.1.6 *Software.*

El software ha sido categorizado de la siguiente manera:

- Sistema operativo.
- Software antivirus.
- Software de productividad

Los sistemas operativos de los computadores mencionados en la sección de hardware son Microsoft Windows 98 para las estaciones de trabajo de la oficina central y de las obras en construcción, y Microsoft Windows 2000 Server para el servidor.

El software antivirus instalado en todo computador sin excepción alguna es McAfee Antivirus v 4.1.

El software de productividad encontrado en las estaciones de trabajo es:

Paquetes ofimáticos: Microsoft Word 2000, Microsoft Excel 2000, Microsoft Power Point 2000, Microsoft Project 2000. Instalados según las necesidades de cada usuario.

Paquete de diagramación: AutoCad v 14. Instalado en todas las estaciones de trabajo de las obras en construcción y en dos estaciones de trabajo de la oficina central (*presup2* y *presup3*)

Paquete de gestión de archivos (necesario para los sistemas de presupuestos y contable): Microsoft Fox Pro v 2.6. Este paquete se encuentra instalado en toda estación de trabajo que requiera utilizar cualquiera de los dos sistemas mencionados.

#### 2.4.4.1.7 *DATOS*

Los datos almacenados en los computadores considerados en el presente trabajo incluyen aquellos generados por cualquier proceso involucrado en la construcción de una obra.

De esta manera, los datos almacenados en cada estación de trabajo incluyen:

- Bases de una licitación por la cual se desea concursar.
- Documentación preparada para concursar en la licitación de una obra determinada.
- Presupuestos generados por el sistema de presupuestos: licitatorio, licitatorio afinado, detallado inicial, ajustado.
- Cronogramas generados por el sistema de presupuestos.
- Listas de precios de materiales.
- Listas de costo por hora de maquinaria.
- Listas de categorías de profesionales de la construcción con sus respectivos sueldos.
- Planificación de todas las fases de la construcción de una obra.
- Reportes de ingreso de mercadería en bodega de obra.
- Reportes de egreso de mercadería en bodega de obra.
- Todo asiento contable generado por el sistema contable.

La anterior lista contempla toda documentación o información en formato digital que se genera a lo largo de todo el proceso de construcción de una obra y que es almacenada en las estaciones de trabajo o en el servidor; es necesario indicar que existe información adicional que se genera y permanece en papel.

La información más importante de la empresa es la que se encuentra en la oficina central.

#### 2.4.4.1.8 *PERSONAL*

El personal que forma parte de la empresa es:

- Personal que labora en la oficina central:
  - Presidencia.
  - Gerencia.

- Jefe del área de presupuestos.
- Jefe del área de contabilidad.
- Resto de personal del área de presupuestos
- Resto de personal del área de contabilidad.
- Personal del área de equipos.
- Recepcionista.
- Guardia.
- Conserje.
- Mensajero.

Es necesario recalcar que la empresa cuenta con dos ingenieros civiles de planta, a los cuales se los ha incorporado en el área de presupuestos.

Pueden considerarse cargos críticos por el nivel de responsabilidad manejado y por el impacto que causaría la ausencia de uno de ellos, los siguientes cargos:

- Presidencia.
- Gerencia.
- Jefe del área de presupuestos.
- Jefe del área de contabilidad.

Las anteriores cuatro personas poseen en sus manos las tareas de toma de decisiones en la empresa.

Personal que labora en las obras en construcción:

- Superintendente de obra.
- Resto personal de obra.
- Guardia.

El primero de esta lista es el cargo considerado crítico, ya que en sus manos se encuentra la responsabilidad de llevar adelante las tareas de construcción de la obra, lo que incluye tareas de administración, supervisión y control.

#### **2.4.4.2 VULNERABILIDADES**

El presente trabajo se enfoca en realizar un análisis de riesgos primordialmente en las instalaciones de la oficina central. Las instalaciones utilizadas en las obras para alojar al equipo informático y al personal que lo emplea varían de una obra a otra, manteniendo únicamente en común el estar dotadas de sistemas de aire acondicionado y reguladores de voltaje en cada estación de trabajo.

Conforme a la clasificación de vulnerabilidades presentadas en el numeral 1.4.5.3 se han encontrado las siguientes vulnerabilidades:

##### *2.4.4.2.1 De Hardware:*

- La mayoría de equipos no cuentan con reguladores de voltaje.
- El servidor no cuenta con UPS.
- No existe una política de mantenimiento de los equipos informáticos.

##### *2.4.4.2.2 Naturales:*

- La empresa se ubica en la ciudad de Guayaquil, por lo tanto existe propensión a padecer problemas de inundaciones o altos niveles de humedad.

##### *2.4.4.2.3 Físicas:*

- El área del servidor es totalmente accesible, lo cual abre las posibilidades de causar daño al servidor de manera intencional o accidental.
- Posible falla de los sistemas de aire acondicionado.
- El único acceso en el que se cuenta con vigilancia es la puerta principal de entrada al edificio.
- Las oficinas de gerencia y presidencia permanecen abiertas todo el tiempo en el cual no son utilizadas.
- No existe restricción alguna que impida el uso del resto de puertas del edificio de la oficina central.
- Existe un solo extintor de incendios, el cual se ubica en la planta baja.

#### 2.4.4.2.4 *De Software:*

- La red opera bajo un ambiente de grupo de trabajo, por lo tanto, la seguridad lógica de cada computador queda a criterio de su respectivo usuario.
- El antivirus es actualizado a criterio de cada usuario.
- No existe política de actualización del sistema operativo.
- No existe política de respaldos.
- No existe política de impresiones.
- Los sistemas de presupuestos y contabilidad no tienen definidos perfiles de usuarios.
- Las aplicaciones de presupuestos y contabilidad han sido modificadas en el transcurso del tiempo conforme a las necesidades de la empresa, lo cual las ha desorganizado.
- No existe restricción de acceso a las carpetas compartidas del servidor.

#### 2.4.4.2.5 *De Comunicación:*

- No existe un servidor cortafuegos.
- No existe un regulador de voltaje para la línea telefónica empleada por el modem del servidor.

En lo concerniente al uso de Internet se encontró lo siguiente:

- Todo el personal posee acceso a Internet sin restricción de horarios.
- No existe restricción en cuanto al tipo de información que pueden descargar los usuarios desde Internet.
- No existe restricción en cuanto al tipo de información a la que pueden acceder los usuarios desde Internet.

#### 2.4.4.2.6 *Humanas:*

- Todo el personal cuenta con conocimientos informáticos muy básicos.
- Se emplean contraseñas débiles.
- No existe gran conciencia acerca de seguridad informática.

### **2.4.4.3 AMENAZAS**

Conforme a la clasificación de amenazas presentadas en 1.4.5.2 se han encontrado las siguientes:



#### 2.4.4.3.1 *Naturales*

- Inundaciones.

En la oficina central no existe gran riesgo debido a que la gran mayoría de equipo informático se encuentra en el segundo piso; únicamente dos estaciones de trabajo se encuentran en la planta baja. Esta amenaza representa mayor riesgo en las obras en construcción debido a que las instalaciones donde se aloja al personal y equipo informático se ubican apenas a un metro sobre el suelo.

- Fuego.

En la oficina central se cuenta con un extintor de incendios. No existe un sistema automático de combate al fuego.

- Terremotos.
- Erupción volcánica.
- Humedad.

Se cuenta con sistemas de aire acondicionado en todo ambiente de la oficina central e instalaciones de obras, lo cual permite mantener la humedad en niveles aceptables.

- Calor.

Los sistemas de aire acondicionado proveen de temperaturas adecuadas para el personal y equipo informático.

- Polvo.

Los sistemas de aire acondicionado también cuentan con el servicio de filtrado de partículas presentes en el aire.

#### 2.4.4.3.2 *Intencionales*

- Robo.

El hecho de contar con un guardia de seguridad en las oficinas centrales ayuda a disminuir la probabilidad de que esta amenaza se concrete. En las obras en construcción el robo es más probable debido a que se encuentra protegido únicamente por un cerramiento y además se almacenan materiales y maquinaria.

- Sabotaje
- Vandalismo
- Entrada a zonas restringidas.

#### 2.4.4.3.3 *Involuntarias*

- Código Malicioso.

Debido a que todo el personal no es lo suficientemente consciente acerca de la seguridad informática, pueden emplear información proveniente de fuentes no confiables, lo cual podría desatar una infección en la red.

- Ataques de hackers.
- Cortes de energía eléctrica.

La probabilidad de que esta amenaza se concrete es alta debido a que nuestro país cuenta con un historial importante de temporadas de racionamiento del fluido eléctrico.

- Variaciones de energía eléctrica.

Existe alta probabilidad de que se presente esta amenaza debido a que la calidad del sistema eléctrico en todo el país no reúne las condiciones adecuadas para evitar este tipo de problema.

- Mala utilización del equipo informático.
- Mal funcionamiento del equipo informático.

Las dos amenazas previas pueden presentarse debido a que el personal no cuenta con una instrucción informática adecuada. Si el equipo es utilizado de una manera inapropiada, entonces el equipo puede llegar a funcionar incorrectamente.

- Interrupción de comunicaciones.

Existe alta probabilidad de que esta amenaza se concrete debido al servicio deficiente ofrecido por el ISP y por el tipo de enlace contratado.

#### 2.4.4.4 CLASIFICACIÓN DE ACTIVOS

Se agruparon los activos identificados en grupos denominados entidades empleando criterios de dependencia o similitud de importancia<sup>25</sup>.

##### 2.4.4.4.1 *Aplicaciones y procesos.*

La aplicación de presupuestos resulta de gran utilidad en los siguientes procesos de la construcción de una obra:

- Preparación de presupuestos
- Planificación de las fases de la construcción

---

<sup>25</sup> TOIGO, John. Disaster Recovery Planning Preparing for the Unthinkable

- Control de inventarios (ingreso y egreso de materiales de bodega de obra)
- Control presupuestario de avance de obra

La aplicación de presupuestos se encuentra instalada en toda estación de trabajo del área de presupuestos.

La aplicación de contabilidad resulta de gran utilidad en los siguientes procesos de la construcción de una obra:

- Registro contable de las facturas entregadas por parte de los proveedores
- Pago a proveedores

La aplicación de contabilidad se encuentra instalada en toda estación de trabajo del área de contabilidad.

Debido a su similar nivel de importancia, estas dos aplicaciones serán agrupadas en una sola entidad.

#### 2.4.4.4.2 *Servicios*

- Enlace a Internet.

#### 2.4.4.4.3 *Hardware*

- Servidor.

Según lo indicado en la sección *personal* dentro de la sección de activos, se han clasificado las estaciones de trabajo de la siguiente manera:

- Pcs de directivos: estaciones de trabajo de Gerencia, Presidencia, Jefe de presupuestos, Jefe de contabilidad.
- Pcs de obras: estaciones de trabajo de las obras en construcción.
- Resto de Pcs.

#### 2.4.4.4.4 *Equipo de comunicaciones*

- Equipo de comunicación interna: patch panel, switch.
- Equipo de comunicación externa: modem del servidor.

#### 2.4.4.4.5 *Software*

A excepción de las aplicaciones, se ha decidido incluir todo elemento de software en el computador en el cual se encuentre instalado o almacenado.

Con fines descriptivos únicamente, el software se lo ha clasificado de la siguiente manera:

- Sistemas operativos: estaciones de trabajo y servidor.
- Software antivirus: todo computador lo tiene instalado.
- Software de productividad: instalado en todo computador. En el servidor se tiene instalado Microsoft Word 2000 ya que ocasionalmente es necesario revisar un documento.
- Datos almacenados en el servidor.
- Datos almacenados en estaciones de trabajo.

#### *2.4.4.4.6 Personal*

El personal ha sido clasificado en primer lugar por el lugar en el que trabaja, y en caso de ser necesario, por el nivel de responsabilidad.

Oficina central:

- Personal directivo: Gerencia, Presidencia, Jefe del área de presupuestos, Jefe del área de contabilidad.
- Personal de apoyo: resto de personal del área de presupuestos, resto de personal del área de contabilidad, personal del área de equipos, recepcionista.
- Personal de servicio: guardia, mensajero y conserje.

Obras en construcción:

- Personal de obras: todo personal que labore en las instalaciones de cualquier obra en construcción.

#### **2.4.4.5 Evaluación del impacto**

A continuación se muestra la evaluación del impacto de las amenazas sobre cada una de las entidades de activos.

ENTIDADES DE ACTIVOS						
AMENAZAS	Aplicaciones	Enlace a internet	Servidor	Pcs directivos	Pcs de obras	Resto de pcs
Inundaciones.	A	M	A	A	A	M
Fuego	A	M	A	A	A	M
Terremotos.	A	M	A	A	A	M
Erupción volcánica	M	B	M	M	M	B
Humedad	A	M	A	A	A	M
Calor	A	M	A	A	A	M
Polvo	A	M	A	A	A	M
Robo	A	M	A	A	A	M
Sabotaje	A	B	A	A	A	M
Vandalismo	A	A	A	A	A	A
Entrada a zonas restringidas	B	B	M	M	A	M
Malware	A	M	A	A	A	A
Ataques de hackers	A	M	A	A	A	M
Cortes/Variaciones de energía eléctrica	A	A	A	A	A	M
Mala utilización del equipo informático	A	M	M	M	M	B
Mal funcionamiento del equipo informático	A	M	A	A	A	M
Interrupción de comunicaciones	A	M	B	B	B	B

Tabla 2.7 Evaluación del impacto.

ENTIDADES DE ACTIVOS						
AMENAZAS	Eq. Comunic interna	Eq. Comunic externa	Personal directivo	Personal de apoyo	Personal de obras	Personal de servicio
Inundaciones.	B	M	B	B	B	B
Fuego	A	A	A	A	A	A
Terremotos.	A	A	A	A	A	A
Erupción volcánica	B	B	M	M	M	M
Humedad	A	A	M	M	M	M
Calor	A	A	M	M	M	M
Polvo	M	M	M	M	M	M
Robo	A	M	A	A	A	A
Sabotaje	A	B	A	A	A	A
Vandalismo	A	A	A	A	A	A
Entrada a zonas restringidas	B	B	M	M	M	A
Malware	B	M	B	B	B	B
Ataques de hackers	B	B	B	B	B	B
Cortes/Variaciones de energía eléctrica	M	B	B	B	B	B
Mala utilización del equipo informático	M	M	B	B	B	B
Mal funcionamiento del equipo informático	M	M	B	B	B	B
Interrupción de comunicaciones	A	A	B	B	B	B

Tabla 2.8 (continuación) Evaluación del impacto.

#### 2.4.4.6 PROBABILIDAD DE OCURRENCIA DE LA AMENAZA.

En las siguientes tablas se encuentra la evaluación de la probabilidad de ocurrencia de las amenazas(ver siguiente página).

ENTIDADES DE ACTIVOS						
AMENAZAS	Aplicaciones	Enlace a Internet	Servidor	Pcs directivos	Pcs de obras	Resto de pcs
Inundaciones.	M	M	M	M	A	M
Fuego	B	M	B	B	A	B
Terremotos.	M	M	M	M	M	M
Erupción volcánica	M	M	M	M	M	M
Humedad	M	M	M	M	M	M
Calor	B	B	B	B	B	B
Polvo	M	M	M	M	M	M
Robo	M	B	M	M	M	M
Sabotaje	B	B	B	B	A	B
Vandalismo	M	B	M	M	A	M
Entrada a zonas restringidas	M	M	M	M	A	M
Malware	A	A	A	A	A	A
Ataques de hackers	M	M	A	A	A	M
Cortes/Variaciones de energía eléctrica	M	B	M	M	M	M
Mala utilización del equipo informático	M	M	M	M	M	M
Mal funcionamiento del equipo informático	A	A	M	A	A	A
Interrupción de comunicaciones	M	M	M	M	A	M

Tabla 2.9 Evaluación de la probabilidad de ocurrencia de amenazas.

ENTIDADES DE ACTIVOS						
AMENAZAS	Eq. Comunic interna	Eq. Comunic externa	Personal directivo	Personal de apoyo	Personal de obras	Personal de servicio
Inundaciones.	B	M	M	M	M	M
Fuego	B	B	B	B	B	B
Terremotos.	M	M	M	M	M	M
Erupción volcánica	M	M	M	M	M	M
Humedad	M	M	M	M	M	M
Calor	B	B	B	B	B	B
Polvo	M	M	M	M	M	M
Robo	B	M	M	M	A	M
Sabotaje	B	B	B	B	A	B
Vandalismo	M	M	M	M	A	A
Entrada a zonas restringidas	M	M	M	M	A	M
Malware	A	A	A	A	A	B
Ataques de hackers	A	A	A	M	A	B
Cortes/Variaciones de energía eléctrica	M	M	M	M	M	M
Mala utilización del equipo informático	M	M	M	M	M	B
Mal funcionamiento del equipo informático	M	A	A	A	A	B
Interrupción de comunicaciones	M	A	M	M	A	B

Tabla 2.10 (continuación) Evaluación de la probabilidad de ocurrencia de amenazas.

#### 2.4.4.7 Evaluación del nivel de riesgo.

El nivel de riesgo se obtiene multiplicando el impacto por la probabilidad de ocurrencia. Ver Anexo A.



ENTIDADES DE ACTIVOS						
AMENAZAS	Aplicaciones	Enlace a Internet	Servidor	Pcs directivos	Pcs de obras	Resto de pcs
Inundaciones.	M	M	M	M	A	M
Fuego	B	M	B	B	A	B
Terremotos.	M	M	M	M	M	M
Erupción volcánica	M	B	M	M	M	B
Humedad	M	M	M	M	M	M
Calor	B	B	B	B	B	B
Polvo	M	M	M	M	M	M
Robo	M	B	M	M	M	M
Sabotaje	B	B	B	B	A	B
Vandalismo	M	B	M	M	A	M
Entrada a zonas restringidas	B	B	M	M	A	M
Malware	A	M	A	A	A	A
Ataques de hackers	M	M	A	A	A	M
Cortes/Variaciones de energía eléctrica	M	B	M	M	M	M
Mala utilización del equipo informático	M	M	M	M	M	B
Mal funcionamiento del equipo informático	A	M	M	A	A	M
Interrupción de comunicaciones	M	M	B	B	B	B

Tabla 2.11 Evaluación del nivel de riesgo.

AMENAZAS	ENTIDADES DE ACTIVOS					
	Eq. Comunic interna	Eq. Comunic externa	Personal directivo	Personal de apoyo	Personal de obras	Personal de servicio
Inundaciones.	B	M	B	B	B	B
Fuego	B	B	B	B	B	B
Terremotos.	M	M	M	M	M	M
Erupción volcánica	B	B	M	M	M	M
Humedad	M	M	M	M	M	M
Calor	B	B	B	B	B	B
Polvo	M	M	M	M	M	M
Robo	B	M	M	M	A	M
Sabotaje	B	B	B	B	A	B
Vandalismo	M	M	M	M	A	A
Entrada a zonas restringidas	B	B	M	M	M	M
Malware	B	M	B	B	B	B
Ataques de hackers	B	B	B	B	B	B
Cortes/Variaciones de energía eléctrica	M	B	B	B	B	B
Mala utilización del equipo informático	M	M	B	B	B	B
Mal funcionamiento del equipo informático	M	M	B	B	B	B
Interrupción de comunicaciones	M	A	B	B	B	B

Tabla 2.12 (continuación) Evaluación del nivel de riesgo.

## 2.5 CONSIDERACIONES DE REDISEÑO LAN

### 2.5.1 ASPECTOS OPERATIVOS

El trabajo a ser desempeñado por todo el personal, principalmente de la oficina central, involucrará lo siguiente:

#### 2.5.1.1 ACCESO A INTERNET.

El área directiva y los jefes de cada departamento requieren hoy en día gran versatilidad en las comunicaciones para poder realizar sus tareas cotidianas sin abandonar sus puestos de trabajo.

Las tareas que requieren de comunicación a Internet son:

- Manejo de cuentas bancarias empresariales en el Banco Bolivariano.
- Consultas de información del estado de la empresa ante el SRI.
- Consulta de información legal, costos, sueldos de trabajadores, nuevos materiales, etc. en la página Web de la Cámara de Comercio de Guayaquil.
- Comunicación vía correo electrónico con proveedores, socios de negocios, clientes y resto del personal de la empresa, especialmente con el personal que labora en las obras en construcción.
- Últimamente la demanda de un servicio de correo electrónico más confiable se ha hecho necesaria, ya que con frecuencia cada vez mayor se envían archivos anexos a los mensajes electrónicos, lo cual requiere un enlace de mayor ancho de banda al ofrecido por un enlace dial-up y se requiere también que el enlace permanezca sin cortes la mayor parte del tiempo.

#### **2.5.1.2 USO DE APLICACIONES**

Debido a las necesidades actuales de la empresa de contar con información actualizada y en línea, la empresa ha decidido construir una nueva versión de sus aplicaciones de control de presupuestos y de contabilidad.

Se requiere que a esta aplicación tengan acceso las siguientes áreas de la empresa: directiva, administrativa y operativa.

Esta nueva aplicación juntará en una sola las dos aplicaciones anteriores, permitiendo interacción entre sí para evitar trabajo redundante innecesario a las áreas de presupuestos y contabilidad, permitiéndoles enfocar sus esfuerzos en mejorar la calidad y cantidad de sus actividades diarias.

De esta manera, en conjunto con el área directiva de la empresa se decidió implantar lo siguiente:

- Configurar la red LAN de la oficina central bajo un ambiente de dominio.
- Contratar los servicios de acceso a Internet por medio de una conexión IP Connect (Clear Channel) de 128Kbps.
- Restringir el acceso a Internet al personal que no lo requiera.

- Establecer políticas y las restricciones necesarias en el servidor de archivos para que las tareas de respaldo puedan realizarse de manera adecuada.
- Se establecerán permisos de impresión sobre aquellas impresoras que soporten impresión en red.
- El servidor controlador de dominio desempeñará adicionalmente los papeles de servidor de archivos y de base de datos (necesario para la aplicación de control de presupuestos).
- Se seguirán usando las mismas impresoras manteniendo el esquema indicado en la figura 2.2
- La configuración de la red mantendrá el mismo esquema que el indicado en la figura 2.2

### **2.5.2 INFRAESTRUCTURA REQUERIDA**

Ya se cuenta con la infraestructura requerida para poder implantar un ambiente de dominio para la red LAN de la oficina central, es decir, puede aprovecharse el cableado estructurado que anteriormente ya estaba implantado.

Puede, de igual manera, aprovecharse el patch panel y switch existentes, sin ningún tipo de problemas sobre el desempeño en el tráfico de la red.

No son necesarias nuevas tomas de energía eléctrica, ya que el número de computadores sigue siendo el mismo, al igual que las impresoras.

## **2.6 CONSIDERACIONES DE REDISEÑO VPN**

Las consideraciones del presente numeral enfatizan la necesidad de contar con comunicaciones permanentes y confiables entre la oficina central y las obras en construcción.

Aspectos relacionados del enlace VPN con la empresa de asistencia técnica serán tratados en el numeral 3.4.

### **2.6.1 ASPECTOS OPERATIVOS.**

Desde hace un tiempo atrás, la compañía necesita mejorar las comunicaciones con sus obras en construcción sin importar el lugar en el que se encuentren. Hasta el momento la única conexión VPN utilizada por la empresa consistía en la que enlazaba la obra en construcción en el sector “Trinitaria” con la oficina central.

Esta conexión padecía de los siguientes problemas:

- El ancho de banda era insuficiente para realizar las tareas necesarias.
- El enlace con el ISP caía con demasiada frecuencia.

Debido a la importancia y magnitud de la obra del sector “Trinitaria” fue la única a la que se le proveyó de este servicio. El resto de obras debían permanecer aisladas por falta de una infraestructura adecuada.

La necesidad de comunicación con las distintas obras requiere ser atendida a la brevedad posible para mejorar los niveles de competitividad y mantenerse como una empresa constructora de renombre.

Resulta imperativo, en el trabajo diario, el poder mantener enlaces de comunicación informática, entre la oficina central y las obras en construcción, para poder establecer mejores niveles de supervisión del avance de una obra y solucionar cualquier tipo de inconveniente. Para esto se requiere contar con información actualizada y en línea de todo cuanto acontece al interior de una obra en construcción.

Los enlaces desde obras con la oficina central serán el fundamento sobre la cual se apoyen dos servicios que permitirán contar con información actualizada:

- Correo electrónico. (Más detalles en el numeral 3.2.)
- Nueva aplicación de contabilidad y control de presupuestos. (Más detalles en el numeral 3.5)

### **2.6.2 INFRAESTRUCTURA REQUERIDA.**

Para poder atender a todas las obras en construcción de mejor manera, se decidió conjuntamente con el área directiva lo siguiente:

- Por motivos de ahorro en costos de servicios de comunicación, se contratarán enlaces de datos IP Connect (Clear Channel) de 64Kbps para cada obra actualmente en construcción. Ver anexo B.
- Ya que el área operativa requiere acceso a la nueva aplicación mencionada en el numeral 2.5.1.3, ésta será una aplicación Web que implemente comunicaciones seguras, conforme a lo establecido en el numeral 2.2.

Debido a que estos enlaces no hacen uso de infraestructura pública alguna, no se los utilizarán para implementar enlaces VPN. La encriptación en las comunicaciones las implementarán las aplicaciones de correo electrónico y, de control de presupuestos y contabilidad mediante SSL.

## **2.7 CONSIDERACIONES ECONÓMICAS**

El análisis de costos a realizar se enfocará en los siguientes aspectos:

- Costo de los equipos servidores y las respectivas licencias necesarias.
- Costo de las estaciones de trabajo y las respectivas licencias necesarias.
- Costo de los servicios de comunicación: acceso a Internet y enlaces dedicados con las obras.
- Costo de protección física de equipos.
- Costo de protección de datos y comunicaciones.

### **2.7.1 COSTO DE EQUIPOS SERVIDORES.**

Como ya se estableció anteriormente en el numeral 2.4.2, los dos servidores necesarios desempeñarán las funciones siguientes:

Controlador de dominio, servidor de archivos, servidor de bases de datos.  
Servidor cortafuegos y punto de acceso a Internet.

- Servidor controlador de dominio:

Cantidad	Descripción	Costo - USD
1	HP Proliant ML 350	3000
1	Licencia Win2003 Advanced Sever	700
1	Licencia SQL Server 2000 Standard Edition con 20 licencias CAL	2000
TOTAL:		5700

Tabla 2.13 Componentes del costo del servidor controlador de dominio.

- Servidor cortafuegos:

Cantidad	Descripción	Costo - USD
1	HP Evo D220	1100

Tabla 2.14 Costo del servidor cortafuegos.

## 2.7.2 COSTO DE LOS EQUIPOS ESTACIONES DE TRABAJO.

Las características de los equipos que desempeñarán las funciones de estaciones de trabajo son las mismas para la oficina central.

Cantidad	Descripción	Costo unitario - USD	Costo total - USD
14	HP Evo D220	900	12600
14	Licencia Microsoft Office 2003 Professional	450	6300
TOTAL:			18900

Tabla 2.15 Costo de las estaciones de trabajo.

Cabe recalcar que el tipo de licencia de las estaciones de trabajo es OEM, por lo tanto el precio de la licencia está incluido en el precio de la estación de trabajo.

En las obras se emplearán los equipos de la oficina central los cuales fueron reemplazados.

## 2.7.3 COSTO DE SERVICIOS DE COMUNICACIÓN.

Al ISP contratado se le solicitaron los siguientes servicios:

- Servicio de acceso ilimitado. Este enlace será empleado para implementar una conexión VPN permanente con la empresa de asistencia técnica ubicada en la ciudad de Quito, con el propósito de obtener asistencia técnica.

- Servicio de enlaces de datos IP Connect (Clear Channel) de 64Kbps

Cantidad	Descripción	Costo unitario mensual - USD	Costo total mensual - USD
1	Acceso ilimitado a internet IP Connect (Clear Channel)-128Kbps	450	450
3	Enlace dedicado de datos IP Connect (Clear Channel)-64Kbps	280	840
TOTAL:			1290

Tabla 2.16 Costo de servicios de comunicación.

#### 2.7.4 COSTO DE PROTECCIÓN FÍSICA DE EQUIPOS.

En base a lo detallado en el numeral 2.1.4, el costo de la protección física de equipos es el siguiente.

Cantidad	Descripción	Costo unitario - USD	Costo total - USD
14	Estabilizador de voltaje	150	2100
1	dispositivo de provisión ininterrumpida de energía eléctrica (UPS)	500	500
1	División modular para separación del área de servidores	350	350
TOTAL:			2950

Tabla 2.17 Costo de dispositivos de protección física.

Los estabilizadores de voltaje antiguos se los destinará a las obras en construcción.

#### 2.7.5 COSTO DE PROTECCIÓN DE DATOS Y COMUNICACIONES.

Cantidad	Descripción	Costo unitario - USD	Costo total - USD
15	Licencia antivirus McAfee	80	1200

Tabla 2.18 Costo de software antivirus.



Cabe mencionar que no es necesario pagar licencia alguna del software usado en el equipo cortafuegos y de acceso a Internet ya que se instalará Red Hat v9.0 como sistema operativo.

## **CAPITULO III**

### **3 ANALISIS Y DISEÑO DE LA INTRANET SEGURA**

#### **3.1 ANÁLISIS DE REQUERIMIENTOS PARA EL SERVICIO WEBMAIL**

##### **3.1.1 FUNCIONALIDAD REQUERIDA.**

Las actividades diarias de todo el personal, especialmente de la oficina central, incluye, entre otras, el mantener contacto fluido con clientes, proveedores, socios de negocios y compañeros de trabajo. Han de acordarse fechas de entrega de materiales, entrega de documentación contractual, emisión de notas de pedido, creación y ajuste de cronogramas de trabajo, emisión de órdenes de pago, ingreso de facturas, ingreso/egreso de materiales de bodega, pago a los trabajadores, etc.

El servicio de correo electrónico junto con el servicio telefónico constituyen el pilar fundamental de las comunicaciones de esta empresa constructora.

El servicio de correo electrónico requiere disponibilidad no solamente durante el período laboral, sino durante todo el día, todos los días del año, sin importar si se trata de fines de semana o días feriados.

Se recomienda que este servicio sea accesible desde Internet debido a las siguientes razones:

- Existe personal que labora gran parte del tiempo en las obras en construcción.
- En casos extremos existe la necesidad de acceso a este servicio desde el hogar.
- Debido a los pocos o nulos conocimientos de informática de los usuarios, es necesario que el usuario cuente siempre con una misma interfaz, y que sus mensajes y lista de contactos sean siempre los mismos.

Debido a que el servicio será accesible desde Internet, es necesario que cuente con comunicaciones seguras las cuales se implementarán mediante SSL.

### 3.1.2 REQUERIMIENTOS DE HARDWARE

Este servicio puede ser empleado sin ningún tipo de problema mediante cualquier estación de trabajo de la oficina central, incluso desde las estaciones de trabajo de las obras en construcción las cuales poseen características inferiores en este aspecto.

En la siguiente tabla se hace una comparación de los requerimientos de hardware de Internet Explorer v6 con las características de las nuevas estaciones de trabajo.

Componente del sistema	Requerimientos de Internet Explorer	Características de las nuevas estaciones de trabajo (oficina central)	Características de las anteriores estaciones de trabajo (obras en construcción)
Procesador	486 a 66MHz. Se recomienda un procesador Pentium	Intel Pentium IV de 2.0GHz	Pentium II
Espacio en disco	12MB para Windows XP. 12,4MB para Windows 98	Disco de 80GB	Disco de 20GB
Memoria RAM	32MB para Windows XP. 16MB para Windows 98	512MB	64MB

Tabla 3.1 Comparación de requerimientos de hardware de Internet Explorer<sup>26</sup>.

### 3.1.3 REQUERIMIENTOS DE SOFTWARE

Debido a que este servicio será accesado desde el Web, el único requerimiento a cumplir es el de contar con un navegador Web compatible con los sistemas operativos disponibles.

Internet Explorer v6 puede ser instalado en los siguientes sistemas operativos<sup>27</sup>: Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP.

<sup>26/27</sup> Fuente: Sitio de descarga de Internet Explorer v6 Service Pack 1.

### **3.1.4 REQUERIMIENTOS DE COMUNICACIONES.**

Si el servicio es accesado desde la oficina central, no existe requerimiento adicional de comunicaciones, se lo podrá utilizar mediante la red LAN.

Si el servicio es accesado desde cualquier obra en construcción, la misma deberá tener instalado el enlace dedicado de datos la oficina central.

Si el servicio es accesado desde cualquier otra ubicación fuera de las instalaciones de la empresa, se deberá contar con una conexión a Internet, sin importar el tipo (dial-up, xDSL, cablemodem, etc).

## **3.2 ANÁLISIS DE REQUERIMIENTOS PARA EL SERVICIO DE CALENDARIO ELECTRÓNICO.**

### **3.2.1 FUNCIONALIDAD REQUERIDA.**

Conforme la empresa se ha ido expandiendo y adquiriendo mayor renombre en su ámbito, la cantidad de trabajo a realizar por el personal va en aumento, a pesar de que en determinados casos se ha contratado más personal.

El objetivo del servicio de calendario electrónico es el de ayudar a organizar las tareas que debe realizar e información que debe manejar todo el personal como parte de sus actividades cotidianas al interior de esta empresa constructora.

Todo empleado, especialmente aquel que labora en la oficina central, en términos generales, maneja el siguiente tipo de información:

- Listados de clientes, proveedores, socios de negocios y la información correspondiente de estas personas.
  - Conjunto de tareas a realizar planificadamente: preparar presupuestos, ingresar datos contables, planificar la construcción de una obra, preparar el rol de pagos, etc
-

- Conjunto de tareas a realizar de manera emergente o espontánea: ajustar presupuestos, preparar información contractual, ajustar cronogramas, crear notas de pedido, etc.

Debido a estas razones, se hace pertinente la implantación de una aplicación de calendario electrónico que brinde las siguientes facilidades:

- Manejo de un listado de contactos de clientes, proveedores, socios de negocios y compañeros de trabajo.
- Creación y seguimiento de tareas previamente planificadas.
- Creación de actividades con sus respectivos recordatorios.
- Capacidad de hacer cambios a la lista de actividades cuando otras de mayor prioridad se presenten.
- Como se mencionó en el capítulo 2, la aplicación a utilizar es Microsoft Outlook 2003, la cual ofrece toda la funcionalidad requerida en forma satisfactoria. Esta aplicación también ofrece los servicios de un cliente de correo electrónico, pero se empleará únicamente el componente de calendario electrónico.

### 3.2.2 REQUERIMIENTOS DE HARDWARE

La aplicación antes referida puede ser instalada sin problema en las estaciones de trabajo actuales de la oficina central, ya que sus características se ajustan perfectamente a los requerimientos especificados por el fabricante.

En la siguiente tabla se hace una comparación de los requerimientos de hardware de la aplicación con las características de las nuevas estaciones de trabajo.

Elemento	Requerimientos de la aplicación	Características de las nuevas estaciones de trabajo
Procesador	Intel Pentium III de 233MHz o superior	Intel Pentium IV de 2.0GHz
Memoria RAM	128MB como mínimo	512MB
Pantalla	Super VGA 800x600 o superior	Super VGA configurada en 1024x768

Tabla 3.2 Comparación de requerimientos de hardware de Outlook 2003<sup>28</sup>.

<sup>28</sup> Fuente: Página de requisitos del sistema de Outlook 2003.

### **3.2.3 REQUERIMIENTOS DE SOFTWARE**

El único requerimiento al respecto es el del sistema operativo, ya que esta aplicación puede instalarse en las siguientes versiones de Microsoft Windows<sup>29</sup>: Windows 2000 con SP3 o posterior, Windows XP o posterior.

Las nuevas estaciones de trabajo cuentan Windows XP Professional SP2.

## **3.3 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INTRANET**

### **3.3.1 POLÍTICAS DE SEGURIDAD EN SOFTWARE**

#### **3.3.1.1 De protección contra código malicioso.**

- Todo computador de la oficina central o cualquier obra en construcción debe contar con software antivirus, antispyware y cortafuegos personal
- La empresa deberá contar con un servidor cortafuegos corporativo.

#### **3.3.1.2 De actualización de sistema operativo y aplicaciones.**

- Todo software base y aplicaciones instalados en todo computador deberán ser actualizados periódicamente, si son susceptibles de ello.

### **3.3.2 POLÍTICAS DE SEGURIDAD PARA CONTROL DE ACCESO Y UTILIZACIÓN DE SERVICIOS E INFORMACIÓN**

#### **3.3.2.1 De control de acceso y utilización del correo electrónico e Internet.**

- Se emplearán estos servicios únicamente para tareas laborales.
- Estos servicios permanecerán disponibles todo el tiempo, sin restricción de horario

#### **3.3.2.2 De utilización de cuentas de usuarios.**

- Todo usuario de la red deberá contar con una cuenta de usuario.
- Todo usuario accederá a los servicios e información ofrecidos en la red por medio de una cuenta de usuario.

---

<sup>29</sup> Fuente: Página de requisitos del sistema de Outlook 2003.

**3.3.2.3 Del acceso a información electrónica disponible en la red.**

- A toda información que deba compartirse se le aplicarán restricciones de acceso adecuadas para garantizar la confidencialidad necesaria conforme a las actividades del personal

**3.3.2.4 Del control de acceso y utilización del servicio de VPN.**

- Se implantará un enlace VPN permanente con la empresa de asistencia técnica.

**3.3.2.5 Del control de acceso y utilización del enlace punto a punto con las obras en construcción.**

- Por motivos económicos, toda obra contará con un enlace punto a punto permanente con la oficina central (ver numeral 2.5.1.3).

**3.3.3 POLÍTICAS DE RESPALDOS Y RECUPERACIÓN DE ARCHIVOS**

- Toda información importante para la realización de las actividades laborales de todo el personal será respaldada de manera periódica.
- En los casos únicamente necesarios, la empresa de asistencia técnica será la encargada de realizar los respaldos y recuperación de archivos.

**3.3.4 NORMAS.**

Nota: Para facilitar la comunicación entre la empresa constructora y la empresa de asistencia técnica, la primera cuenta ya con una persona de asistencia técnica interna que desempeñará el papel de intermediario en las comunicaciones entre las dos empresas, realizará también tareas de apoyo cuando la empresa de asistencia técnica así lo requiera.

Cuando las condiciones lo ameriten, el área directiva y la empresa de asistencia técnica mantendrán comunicación directa.

### **3.3.4.1 Normas de seguridad en software**

#### *3.3.4.1.1 De protección contra código malicioso:*

- La empresa de asistencia técnica será la encargada de instalar software antivirus, antispyware y cortafuegos personal en todo computador de la compañía.
- Cada usuario será responsable de revisar totalmente su estación de trabajo en busca de virus y spyware. El área directiva y la empresa de asistencia técnica acordarán la frecuencia de realización de esta actividad.
- La empresa de asistencia técnica será la encargada de instalar un servidor cortafuegos corporativo para minimizar los ataques externos y permitir únicamente el tráfico necesario para las actividades laborales del personal
- El área directiva y la empresa de asistencia técnica acordarán la frecuencia con la que ésta última actualizará el software antivirus, antispyware y reglas de filtrado del servidor cortafuegos corporativo. Se aplicará el siguiente esquema en las reglas de filtrado:  
“Está prohibido todo lo que no está expresamente permitido”.

#### *3.3.4.1.2 De actualización de sistema operativo y aplicaciones:*

- El área directiva y la empresa de asistencia técnica acordarán la frecuencia con la que ésta última actualizará el sistema operativo y aplicaciones de todo computador.

### **3.3.4.2 Normas de seguridad para control de acceso y utilización de servicios e información.**

#### *3.3.4.2.1 De control de acceso y utilización del correo electrónico e Internet.*

- El usuario no permitirá el uso de su cuenta de correo electrónico a otros usuarios.
- El usuario no podrá emplear su cuenta de correo electrónico para tareas ajenas a sus actividades laborales
- En caso de que el usuario reciba mensajes sospechosos o potencialmente dañinos en su buzón de correo electrónico, no los deberá abrir o leer y los eliminará de manera inmediata; además reportará el incidente al personal de soporte interno que a su vez



reportará el incidente a la empresa de asistencia técnica la cual tomará las medidas necesarias para evitar en lo posible la futura recepción de este tipo de mensajes.

- Todo mensaje que tenga más de 60 días deberá ser eliminado del servidor de correo electrónico.
- El tamaño máximo de archivos anexos a un mensaje es de 1MB.
- Toda cuenta de correo electrónico poseerá un límite de almacenamiento, el cual será establecido de manera coordinada entre el área directiva y la empresa de asistencia técnica.
- Cuando la cuenta alcance el 100% de su capacidad de almacenamiento, se rechazará todo mensaje entrante para esa cuenta.

#### 3.3.4.2.2 *De utilización de cuentas de usuarios.*

- La empresa de asistencia técnica será la responsable de crear, bloquear, desbloquear y eliminar las cuentas de usuario tras solicitud proveniente del personal de soporte interno.
- La cuenta de administrador será manejada por personas designadas de la empresa de asistencia técnica y por el personal de soporte interno.
- Los usuarios accederán a servicios e información disponibles en la intranet mediante el uso de su identificador de usuario y contraseña.
- La primera vez que el usuario emplee su cuenta para acceder a la red deberá cambiar su contraseña.
- El período de validez de una contraseña es de 90 días.
- Al ingresar una nueva contraseña, el sistema verificará que sea diferente a las tres últimas contraseñas utilizadas
- El tamaño mínimo de la contraseña será de 8 dígitos y deberá estar formada por caracteres alfanuméricos.
- El número de intentos fallidos por medio del uso de una cuenta de usuario será de tres, tras lo cual la cuenta permanecerá bloqueada; únicamente por medio de la cuenta de administrador podrá ser desbloqueada.

#### 3.3.4.2.3 *Del acceso a información electrónica disponible en la red.*

- El personal de soporte interno será el que proporcione la información necesaria para que la empresa de asistencia técnica implante los permisos de acceso adecuados a la información compartida en la red

#### 3.3.4.2.4 *Del control de acceso y utilización del servicio de VPN.*

- De preferencia, se contratará a un mismo ISP sus servicios para la empresa constructora en Guayaquil y para la empresa de asistencia técnica en Quito.
- El personal técnico de la oficina de asistencia técnica podrá emplear el enlace VPN a la oficina central de la empresa constructora, únicamente con fines de proporcionar asistencia técnica previamente solicitada por el personal de soporte interno.
- Desde la empresa constructora no se podrá acceder a ningún recurso de la empresa de asistencia técnica.

#### 3.3.4.2.5 *Del control de acceso y utilización del enlace punto a punto con las obras en construcción.*

- En cualquier obra en construcción, toda estación de trabajo hará uso del enlace dedicado por medio de una sola estación de trabajo, la cual será configurada para tal efecto. El mencionado enlace se empleará únicamente para la utilización del servicio de correo electrónico y la nueva aplicación de contabilidad y presupuestos, así como para recibir asistencia técnica remota por parte de la empresa de asistencia técnica.

#### **3.3.4.3 Normas de respaldos y recuperación de archivos.**

- Cada usuario será responsable de respaldar en el servidor los archivos que creyere pertinentes. Esta actividad se realizará mensualmente.
- Los jefes de las áreas de contabilidad y presupuestos serán los encargados de respaldar en el servidor la información generada por las aplicaciones de contabilidad y presupuestos correspondientemente. Esta actividad se realizará semanalmente.
- El usuario será el responsable de recuperar información de sus respaldos cuando así se lo requiera.

- Los jefes de las áreas de contabilidad y presupuestos serán los encargados de recuperar información de los respaldos de las aplicaciones de contabilidad y presupuestos correspondientemente cuando así se lo requiera.
- Cuando existan dificultades para respaldar o recuperar información, la empresa de asistencia técnica será contactada para solucionar tales situaciones.

### **3.3.5 PROCEDIMIENTOS**

#### **3.3.5.1 Procedimientos de seguridad en software.**

##### *3.3.5.1.1 Para protección contra código malicioso.*

##### Para revisión de virus y spyware en los computadores:

- Todo viernes, antes de finalizar su periodo laboral, cada usuario se encargará de revisar totalmente su estación de trabajo en busca de virus y spyware. El personal de soporte interno se encargará de realizar la revisión en el servidor.
- Al finalizar la tarea, en caso de haber código maligno que no pudo ser removido, lo reportará al personal de soporte interno, que solicitará ayuda a la empresa de asistencia técnica.
- Al siguiente día, aprovechando de que la red se encuentra casi inactiva, la empresa de asistencia técnica se encargará de encontrar y aplicar la solución adecuada para lograr remover todo código maligno de todo computador.

##### Para actualización de software antivirus y antispymware:

- Cada viernes por la mañana, el personal delegado por parte de la empresa de asistencia técnica, deberá obtener de Internet los archivos necesarios para actualizar antivirus y antispymware.
- Se copiarán los mencionados archivos (empleando el enlace VPN) en un computador destinado para la realización de pruebas, el cual será utilizado exclusivamente para este propósito.

- A continuación, se copiarán los archivos de actualización desde el computador de pruebas hacia las demás, y se procederá con la actualización.

Para actualización de reglas de filtrado del servidor cortafuegos corporativo:

- El área directiva en conjunto con la empresa de asistencia técnica establecerán el listado de personas que deben tener acceso a Internet y el tipo de servicios accesibles por éstos en Internet.
- En base al listado enviado, un delegado de la empresa de asistencia técnica será la encargada de crear las reglas pertinentes en el servidor cortafuegos corporativo.

*3.3.5.1.2 Para actualización del sistema operativo y aplicaciones.*

- Trimestralmente, en un fin de semana acordado entre el área directiva y la empresa de asistencia técnica, se instalarán las actualizaciones al sistema operativo y aplicaciones.
- El personal de soporte interno se encontrará en las instalaciones de la oficina central para colaborar en esta tarea.
- Se otorgará acceso a Internet a todo computador que no lo tiene, durante el fin de semana únicamente.
- La actualización primero se realizará en el computador de pruebas.
- Para el caso de archivos de actualización que sobrepasen los 5MB, se los descargará en el computador de pruebas, para copiarlos desde ahí hacia las demás estaciones de trabajo.
- Una vez hecha toda verificación en el computador de pruebas, la actualización se realizará computador por computador, descargando las actualizaciones directamente de Internet.
- Una vez completada esta tarea, se aplicarán en el servidor cortafuegos las mismas reglas de filtrado presentes antes del inicio de estas tareas.

### **3.3.5.2 Procedimientos de seguridad para control de acceso y utilización de servicios e información**

#### *3.3.5.2.1 De control de acceso y utilización del correo electrónico e Internet.*

##### Para crear una cuenta:

- Tras solicitud verbal o por medio telefónico por parte del personal de soporte interno, la empresa de asistencia técnica creará la cuenta de correo electrónico.
- El personal técnico realiza pruebas de funcionamiento desde la estación de trabajo del usuario, y dejará creado un acceso directo al servicio de correo electrónico en el escritorio de la estación de trabajo del usuario.

##### Para eliminación de mensajes antiguos:

- Cada semana, la empresa de asistencia técnica revisará el servidor de correo electrónico en busca de mensajes almacenados por más de 60 días para proceder a eliminarlos.
- La empresa de asistencia técnica envía al personal de soporte interno el listado de cuentas que posean mensajes almacenados por más de 60 días. El personal de soporte interno se encarga de notificar a los respectivos usuarios para que revisen sus cuentas de correo electrónico.
- Al siguiente día, la empresa de asistencia técnica eliminará los mensajes almacenados por más de 60 días en el servidor de correo electrónico.

##### Para eliminación de mensajes al sobrepasar la capacidad de la cuenta:

- En la revisión semanal antes mencionada, la empresa de asistencia técnica también revisará el servidor de correo electrónico para identificar cuentas que hayan alcanzado y superado el 95% de su capacidad de almacenamiento.
- La empresa de asistencia técnica envía al personal de soporte interno el listado de cuentas cuya capacidad de almacenamiento se haya alcanzado o sobrepasado. El personal de soporte interno se encarga de notificar a los respectivos usuarios para que revisen sus cuentas de correo electrónico.

- Al siguiente día, la empresa de asistencia técnica eliminará mensajes en orden cronológico de llegada, hasta que la cuenta alcance el 80% de su capacidad de almacenamiento.

#### 3.3.5.2.2 *De utilización de cuentas de usuarios.*

Nota. Deberá existir una solicitud previa por parte del personal de soporte interno a la empresa de asistencia técnica para que ésta realice tareas de creación, eliminación, bloqueo y desbloqueo de cuentas.

#### Para la creación de cuentas de usuario:

- Para usuarios de planta el identificador de la cuenta estará formado por el nombre y apellido del usuario con su respectiva letra inicial en mayúscula, separados por un espacio en blanco.
- Para usuarios temporales (practicantes, etc) el identificador de la cuenta se formará por el vocablo "Temporal" seguido de dos dígitos para llevar una numeración ascendente.
- La descripción incluirá el departamento al cual pertenece el usuario, su nombre y apellido, y si el usuario es de planta o temporal.

#### Para el desbloqueo de cuentas:

- Si tras superar el límite de intentos fallidos de acceso, la cuenta ha sido bloqueada, el personal de soporte interno solicitará a la empresa de asistencia técnica el desbloqueo de la cuenta de usuario.

#### Para creación de contraseñas de usuario:

- La longitud y composición de la contraseña se regirá a lo indicado en las normas establecidas para cuentas de usuario.

Los detalles de la composición de la contraseña son:

- La contraseña debe contener al menos un caracter de tres de los siguientes grupos de caracteres:
  - Letras minúsculas
  - Letras mayúsculas
  - Dígitos
  - Caracteres especiales, por ejemplo: @, ¡, %, \$, etc.

- No emplear el mismo identificador de la cuenta de usuario.
- No emplear fechas de nacimiento propia o de personas conocidas.
- No emplear palabras que se encuentren en el diccionario, ni siquiera escritas en sentido inverso<sup>30</sup>.

#### 3.3.5.2.3 *Del acceso a información electrónica disponible en la red:*

- El personal de soporte interno entrega a la empresa de asistencia técnica un listado de carpetas que deberán compartirse en el servidor y estaciones de trabajo, junto con los nombres de los usuarios que podrán accederlas y el respectivo nivel de acceso asociado (lectura, escritura, ejecución, etc.)
- El personal delegado de la empresa de asistencia técnica implementa lo solicitado.
- El personal técnico creará los accesos necesarios en la estación de trabajo de cada usuario a las carpetas compartidas a las cuales se les ha otorgado acceso.

#### 3.3.5.2.4 *Del control de acceso y utilización del servicio de VPN.*

##### Para la configuración del enlace:

- La empresa de asistencia técnica configurará los servidores propio y de la empresa constructora, necesarios para implementar el mencionado enlace.

##### Para la utilización del enlace:

- Cuando ocurra algún desperfecto, mal funcionamiento o se requiera asistencia técnica por cualquier motivo en algún equipo de cómputo, el personal de soporte interno solicitará ayuda a la empresa de asistencia técnica.
- La mencionada empresa designará al personal adecuado, y se empleará el enlace VPN permanente para atender la solicitud realizada.

---

<sup>30</sup> Ayuda de Windows Server 2003 y National Cyber Security Alliance

3.3.5.2.5 *Del control de acceso y utilización del enlace punto a punto con las obras en construcción.*

Para la configuración del enlace:

- La empresa de asistencia técnica enviará a un grupo de personal técnico a las dependencias de la obra en construcción para realizar la instalación del enlace punto a punto y configuración del resto de estaciones de trabajo (si las hay) para que se beneficien del mencionado enlace.
- El resto del grupo técnico, coordinadamente desde la oficina central, realizará las conexiones necesarias a los modem de datos y verificará la exitosa implantación del enlace.

Para la utilización del enlace:

- Cuando ocurra algún desperfecto, mal funcionamiento o se requiera asistencia técnica por cualquier motivo en algún equipo de cómputo de la obra, el superintendente informará al personal de soporte interno los problemas, que solicitará ayuda a la empresa de asistencia técnica.
- La mencionada empresa designará al personal adecuado, y se empleará el enlace VPN permanente para atender la solicitud realizada.

### **3.3.5.3 Procedimientos de respaldos y recuperación de archivos**

3.3.5.3.1 *Para la creación de respaldos en el servidor:*

Información de usuarios:

- La empresa de asistencia técnica creará en el servidor carpetas destinadas al almacenamiento de los respaldos de cada usuario; las compartirá aplicando las restricciones adecuadas para que su propietario sea el único usuario que pueda accederla.
- Cada usuario, a primera hora del primer día lunes del mes, revisará sus archivos respaldados en el servidor y procederá a eliminar aquellos que no los necesite más.
- A continuación, creará copias de respaldo de los archivos que creyere pertinentes en la carpeta que le ha sido asignada en el servidor.



- En caso de existir problemas para realizar estas tareas, los reportará al personal de soporte interno que solicitará ayuda a la empresa de asistencia técnica.

#### Información de las aplicaciones:

- La empresa de asistencia técnica creará en el servidor carpetas destinadas al almacenamiento de los respaldos de las aplicaciones de contabilidad y presupuestos; las compartirá aplicando las restricciones adecuadas para que el jefe del área de contabilidad y del área de presupuestos, correspondientemente, sea el único usuario que pueda accederla.
- Los mencionados jefes de área, a primera hora del día lunes, revisarán los respaldos de sus respectivas aplicaciones en el servidor y procederán a eliminar aquellos que no los necesiten más.
- A continuación, crearán copias de respaldo de los archivos que creyeren pertinentes en las carpetas que les han sido asignadas en el servidor.
- En caso de existir problemas para realizar estas tareas, los reportará al personal de soporte interno que solicitará ayuda a la empresa de asistencia técnica.

#### *3.3.5.3.2 Para la recuperación de información.*

##### Recuperación de información de usuarios.

- Cuando el usuario crea necesario obtener un archivo de los respaldados en el servidor, se conectará a este último por medio del acceso creado en su estación de trabajo.
- Una vez conectado a su carpeta ubicada en el servidor, procederá a buscar el archivo requerido.
- Abrirá el archivo para cerciorarse de que su contenido le resulta de utilidad.
- Podrá copiar fragmentos del contenido del mismo o reemplazar el archivo que reside en su estación de trabajo.
- En caso de existir problemas para realizar estas tareas, los reportará al personal de soporte interno que solicitará ayuda a la empresa de asistencia técnica.

### Recuperación de información de las aplicaciones:

- Cuando algún jefe de las áreas de contabilidad o presupuestos crea necesario obtener un archivo respaldado en el servidor de las aplicaciones de contabilidad o presupuestos, respectivamente, se conectará al servidor por medio del acceso directo creado en el escritorio de su estación de trabajo.
- Una vez conectado a la carpeta deseada, procederá a buscar el(los) archivo(s) requerido(s).
- Procederá a copiarlo(s) en una carpeta temporal en su estación de trabajo.
- Abrirá el(los) archivo(s) con la aplicación respectiva para cerciorarse de que su contenido le resulta de utilidad.
- Podrá copiar fragmentos del contenido del (los) mismo(s) o reemplazar el(los) archivo(s) que reside(n) en su estación de trabajo.
- En caso de existir problemas para realizar estas tareas, los reportará al personal de soporte interno que solicitará ayuda a la empresa de asistencia técnica.

## **3.4 ANÁLISIS DE REQUERIMIENTOS DE LA VPN.**

### **3.4.1 NECESIDADES DE LA EMPRESA.**

Es necesario contar con un servicio de mantenimiento informático. Por varias razones, este servicio será contratado a otra empresa, para de este modo poder enfocar todos sus esfuerzos y recursos en la actividad propia de la empresa: construcción de obras civiles.

La VPN se empleará para implementar un enlace permanente con la empresa de asistencia técnica antes mencionada, para facilitar las tareas de mantenimiento de los recursos informáticos de la compañía.

El servicio de asistencia técnica se requiere no solamente en oficina central, sino también en las distintas obras en construcción.

### **3.4.2 CARACTERÍSTICAS DE LOS USUARIOS.**

Quienes emplearán el enlace VPN será el personal de la empresa de asistencia técnica informática.

Este personal es el encargado de solucionar todo problema informático ocurrido en la empresa constructora (oficina central u obras en construcción) o atender cualquier tipo de requerimiento del tema.

Casi toda actividad de asistencia técnica será desarrollada remotamente desde las instalaciones de la empresa de asistencia técnica.

### **3.4.3 RESTRICCIONES.**

Las restricciones se derivan de lo indicado en el numeral 3.3.4.2.4 el cual establece las normas del control de acceso y utilización del servicio de VPN.

Aquí las restricciones que se aplican:

- Este enlace será empleado únicamente con el propósito de brindar servicios de asistencia técnica remota.
- Toda requisición de asistencia será previamente solicitada por la empresa constructora.
- Desde la empresa constructora no se podrá acceder a ningún recurso de la empresa de asistencia técnica.

Los servidores VPN de estas empresas requerirán ser configurados para cumplir con estas restricciones.

### **3.4.4 REQUERIMIENTOS DE HARDWARE.**

#### **3.4.4.1 Para la empresa constructora.**

El servidor VPN será implantado en un computador que posee las mismas características que las nuevas estaciones de trabajo.

Se instalará Red Hat v9.0 como sistema operativo. Esto debido a consideraciones económicas (ahorrar el precio de una licencia Microsoft) y razones técnicas (el personal de asistencia técnica posee más experiencia implementando VPNs en plataforma linux)

#### **3.4.4.2 Para la empresa de asistencia técnica.**

La empresa de asistencia técnica cuenta con un servidor en el cual se implementará el enlace VPN permanente con la oficina central de la empresa constructora.

Toda estación de trabajo de la empresa de asistencia técnica puede utilizar este enlace sin problema alguno.

### **3.4.5 REQUERIMIENTOS DE SOFTWARE.**

#### **3.4.5.1 Para los servidores.**

Red Hat v9.0 puede proveer este servicio sin problema alguno, se requiere solamente la instalación de determinados paquetes RPM y configuración de un archivo de texto.

#### **3.4.5.2 Para las estaciones de trabajo.**

Con la finalidad de facilitar las tareas de asistencia técnica y para evitar saturar el ancho de banda de este enlace, se deberá contar con una aplicación VNC.

El cliente de esta aplicación será instalada en todo computador de la empresa constructora tanto en la oficina central como en las obras en construcción, incluyendo el servidor cortafuegos.

El servidor de esta aplicación será instalada en toda estación de trabajo de la empresa de asistencia técnica.

### **3.4.6 REQUERIMIENTOS DE COMUNICACIONES.**

La empresa constructora requiere de un enlace dedicado a Internet. Las conexiones dial-up no ofrecen la estabilidad ni el ancho de banda requeridos.

Conforme a lo indicado en el numeral 2.6.2, se decidió la contratación de un enlace dedicado a Internet IP Connect (Clear Channel) de 128Kbps.

La empresa de asistencia técnica ya cuenta con un enlace dedicado a Internet con el suficiente ancho de banda para poder implementar el mencionado enlace.

### **3.5 CARACTERIZACIÓN DE LA APLICACIÓN PARA CONTROL DE PRESUPUESTOS.**

#### **3.5.1 ANTECEDENTES.**

Para poder comprender las características y ventajas que ofrecerá la nueva aplicación es necesario indicar las características de la anterior aplicación y la manera con la que se operaba usando ésta última.

Las actividades propias de esta empresa dan inicio cuando se obtienen las bases para concursar en la licitación de la construcción de una obra civil.

Tras preparar el presupuesto licitatorio y haber ganado el concurso, el área de presupuestos, entre otra documentación, prepara el presupuesto detallado inicial. Es entonces en este punto que éste presupuesto es enviado al área de contabilidad, impreso o en formato digital (documentos de Word y Excel).

El área de contabilidad de encarga de la creación de las cuentas contables, conforme al plan de cuentas utilizado en la empresa, necesarias para el presupuesto que les ha sido enviado.

Cuando los trabajos de construcción se encuentran en ejecución, se envía a oficina central una Nota de Pedido, la cual es un documento con el que se solicitan materiales y equipos. Empleando el sistema de presupuestos se compara esta solicitud contra lo presupuestado. Si recibe aprobación, se comprará lo solicitado y se entregará en obra.

Una vez entregados materiales y equipos, el área de contabilidad ingresa la información que consta en la factura entregada por el proveedor. En obra, el superintendente ingresa en el módulo de inventarios del sistema de presupuestos los materiales y equipos recibidos según lo especificado en la guía de remisión, la cual es un documento entregado por el proveedor. En este punto existe la necesidad de verificar que la factura y la guía de remisión contengan la misma información.

En obra, cuando se requiere egresar materiales y equipo de bodega, el superintendente registra este movimiento en el módulo de inventarios, además prepara documentación que contiene el mismo tipo de información para enviarla a oficina central al área de contabilidad, para que se realice la afectación contable pertinente.

Además, cuando el área directiva o socios de negocios desean conocer a la fecha el costo de la obra en comparación con los valores presupuestados, el personal de las áreas de contabilidad y presupuestos deben intercambiar información de sus sistemas para conseguir que los valores cuadren.

Como puede observarse, las aplicaciones de las áreas de contabilidad y presupuestos trabajan de manera aislada, y se hace muy necesario el hecho de que puedan trabajar coordinadamente. En base a esta necesidad se encargó el desarrollo de una nueva aplicación que integre en una sola a estas dos aplicaciones.

No era recomendable modificar las aplicaciones existentes para que pudieran trabajar juntas, ya que son aplicaciones antiguas basadas en plataforma D.O.S, no se ajustan a las nuevas necesidades de obtención de información actualizada, ni se benefician de las ventajas que ofrece un sistema de gestión de bases de datos.

### **3.5.2 FUNCIONALIDAD REQUERIDA PARA LA NUEVA APLICACIÓN.**

Conforme a lo indicado en el numeral anterior, las características fundamentales con las que debe contar la nueva aplicación son:

- Integrar en una sola aplicación las aplicaciones de contabilidad y presupuestos.
- Permitir que las áreas de presupuestos y contabilidad trabajen de manera coordinada y paralela. Esto se conseguirá cuando determinada información ingresada en un subsistema se vea reflejada en el otro.

- Proveer información actualizada y en línea de toda la información referente a la obra conforme al avance cotidiano de la misma.
- Proveer acceso centralizado a la aplicación, para evitar el instalar la aplicación en las estaciones de trabajo donde sea requerida.
- Utilizar un sistema de gestión de bases de datos.
- Aplicar restricciones de acceso a los diferentes módulos en base a perfiles de usuario.

### **3.5.3 CARACTERÍSTICAS DE LA NUEVA APLICACIÓN.**

Conforme a la funcionalidad indicada en el numeral anterior, las características de esta aplicación son:

- Agrupa las dos aplicaciones, contabilidad y control de presupuestos, cada una como un módulo componente de la nueva aplicación.
- El sistema de presupuestos realizará de manera automática afectación contable en las cuentas correspondientes para un determinado presupuesto.
- El sistema de contabilidad realizará añadidos en el área de gastos imprevistos al interior de un determinado presupuesto.
- Es una aplicación Web que permitirá el acceso desde las obras en construcción y brindar reportes actualizados con diferentes niveles de detalle del estado de obra.
- Ofrece funcionalidad restringida en base a perfiles de usuario.
- Adicionalmente se le agregó un módulo de administración.

Esta aplicación fue desarrollada con el lenguaje C# de Microsoft Visual Studio. Utiliza el sistema de gestión de bases de datos Microsoft SQL Server Standard Edition. Se la puede utilizar mediante cualquier navegador Web, especialmente Internet Explorer de Microsoft (por razones de compatibilidad).

Cabe destacar que para poder implementar la interdependencia de los módulos de contabilidad y presupuestos, fue necesario reestructurar el plan de cuentas empleado hasta el momento en la empresa constructora.

## CAPITULO IV

### 4 DESARROLLO E IMPLANTACIÓN DE LA INTRANET SEGURA

#### 4.1 CONFIGURACIÓN Y PERSONALIZACIÓN DEL SERVICIO WEBMAIL

Conforme a la funcionalidad deseada para este servicio la cual consta en el numeral 3.1.1, en esta sección se revisará la manera cotidiana de utilización del servicio WebMail por parte de los usuarios de la empresa constructora como apoyo en sus actividades laborales, lo que incluye las siguientes acciones:

- Enviar mensajes.
- Personalizar el servicio.

##### 4.1.1 ACCESO AL SERVICIO

La dirección a utilizarse es la siguiente: *https://200.105.238.163/webmail*.

Debido a que este servicio ofrece comunicaciones seguras mediante SSL, el usuario debe aceptar el certificado digital.

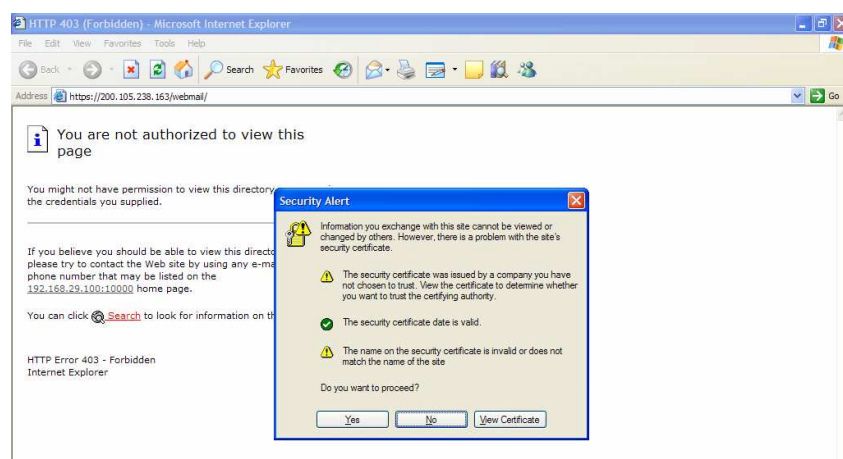


Figura 4.1. Certificado digital del servicio WebMail.



En la pantalla de autenticación el usuario ingresará su nombre de usuario y contraseña que le han sido asignados para la utilización de este servicio. En las zonas resaltadas de la siguiente figura puede constatarse el hecho de que las comunicaciones seguras se consiguieron establecer.

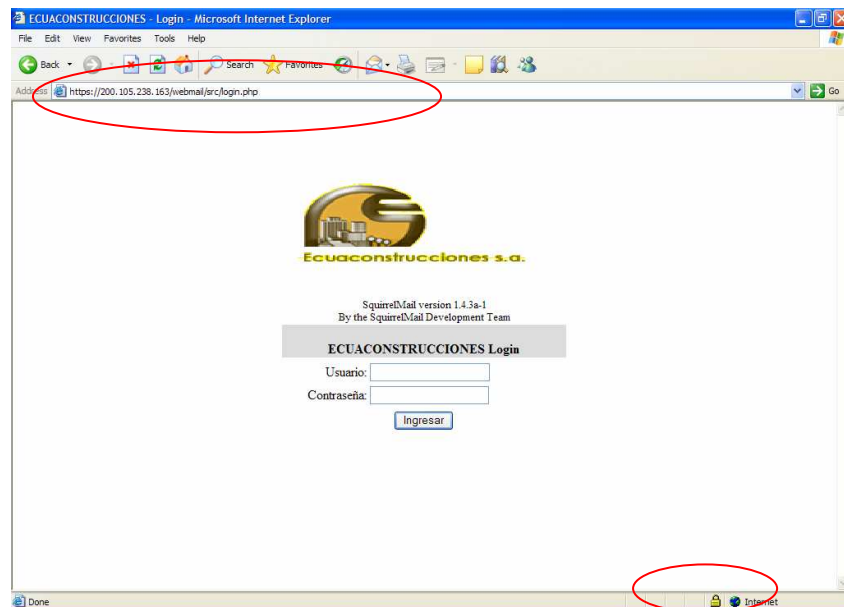


Figura 4.2. Comunicaciones seguras exitosamente establecidas.

#### 4.1.2 ENVIAR MENSAJES.

Al utilizar por primera vez este servicio, la pantalla principal tendrá el siguiente aspecto.

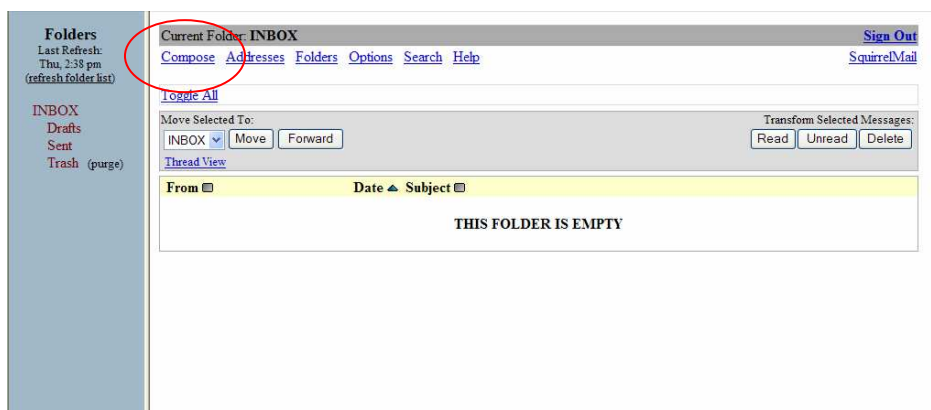


Figura 4.3. Buzón de mensajes entrantes.

Con la opción *Compose* del menú ubicado en la parte superior (resaltado en la figura anterior) el usuario puede enviar mensajes. Los típicos campos empleados en la composición de un mensaje de correo electrónico implementa este servicio, además ofrece opciones tales como fijación de prioridad, conformación de lectura o almacenar el mensaje como borrador y no ser enviado.

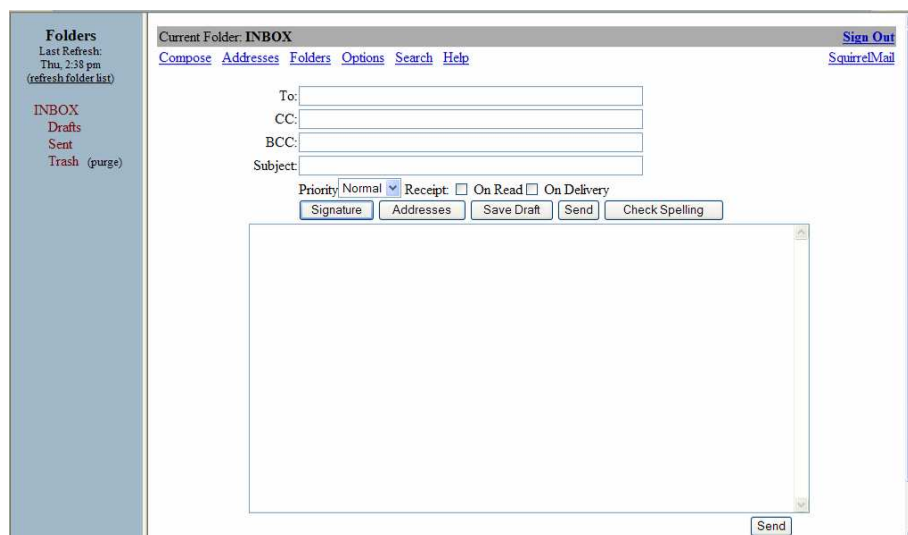


Figura 4.4. Opciones disponibles para componer mensajes.

Estas opciones le ofrecen al usuario la funcionalidad necesaria para su uso como parte de sus tareas laborales cotidianas.

#### 4.1.3 PERSONALIZAR EL SERVICIO

Este servicio permite que su interfaz gráfica, así como otros aspectos sean configurados por parte del usuario para ajustarse a sus necesidades o preferencias. Entre las opciones que el usuario puede configurar se encuentran:

- Información personal tal como el nombre o dirección.
- Resaltado de mensajes en base a la dirección del emisor.
- Ordenamiento de listados de mensajes en orden cronológico, alfabético, etc.
- Opciones de aviso cuando un mensaje nuevo ha llegado.

- Opciones de despliegue en pantalla tal como colores, idioma, etc.
- Opciones para manipulación de carpetas.
- Opciones de diccionario para revisión ortográfica de los mensajes a enviarse.

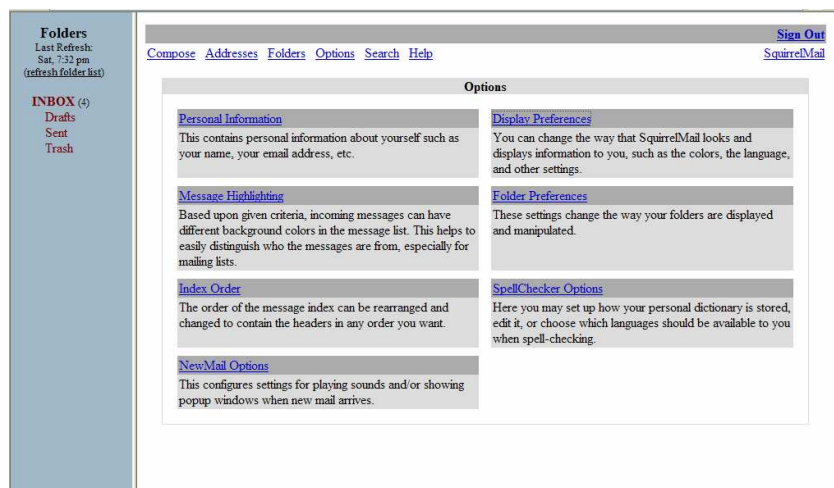


Figura 4.5. Opciones de configuración del servicio.

Mediante la opción *Display Preferences* (parte superior izquierda) el usuario tiene la posibilidad de configurar, entre otras, opciones de idioma y opciones avanzadas de despliegue de mensajes recibidos, como lo indica la siguiente pantalla.

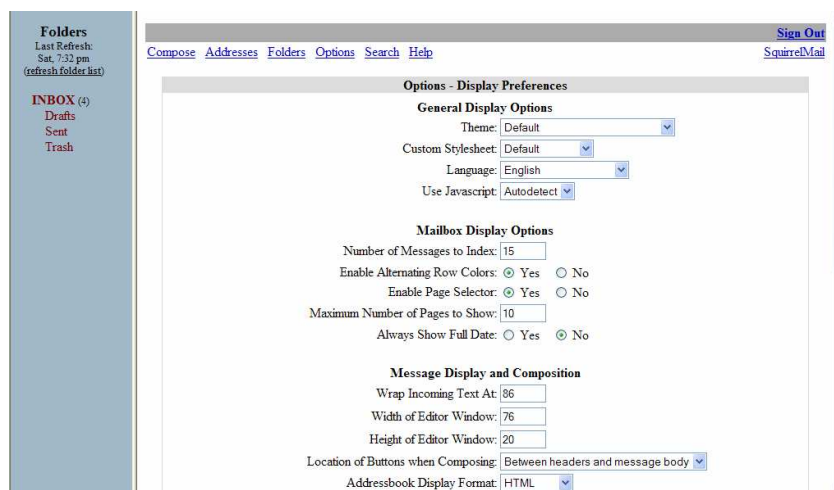


Figura 4.6. Opciones para configuración de interfaz gráfica.

## 4.2 CONFIGURACIÓN Y PERSONALIZACIÓN DEL SERVICIO DE CALENDARIO ELECTRÓNICO.

Conforme a lo especificado en el numeral 3.2.1, en esta sección se revisará la manera en la que el usuario empleará el calendario electrónico en sus actividades laborales cotidianas, las cuales son:

- Lista de contactos: crear, organizar, modificar y eliminar contactos.
- Citas: programar, modificar y eliminar citas.
- Tareas: crear, modificar, eliminar y dar seguimiento a tareas.

### 4.2.1 INTRODUCCIÓN.

La siguiente figura muestra la página principal de Microsoft Outlook 2003 cada vez que este programa es iniciado.

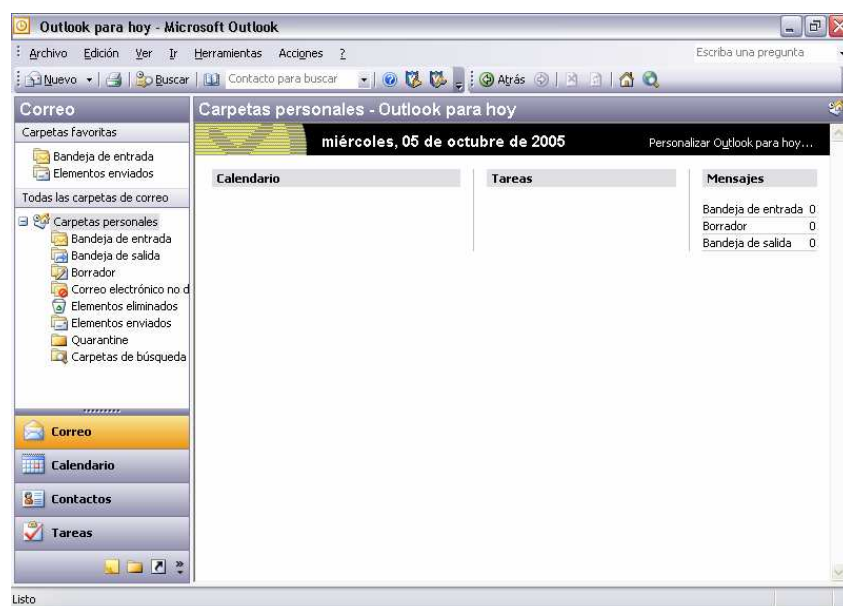


Figura 4.7 Página principal de Microsoft Outlook

En la parte inferior izquierda se encuentra la sección de accesos directos, de los cuales el usuario utilizará los tres últimos.



Figura 4.8 Accesos directos

## 4.2.2 LISTA DE CONTACTOS.

### 4.2.2.1 Crear y organizar contactos.

Al crear un contacto el usuario puede ingresar la siguiente información:

- Nombre, puesto y organización.
- Direcciones del trabajo, particular y otras.
- Números de teléfono de trabajo, fax, móvil y particular.
- Direcciones de correo electrónico, paginas web y mensajería instantánea.
- Información profesional como departamento, oficina, profesión, nombre de jefe, nombre de asistente, etc.

Figura 4.9 Ingreso de datos de un nuevo contacto.

Tras haber ingresado algunos contactos en el calendario electrónico, el usuario tiene a su disposición algunos criterios de clasificación de contactos; de esta

manera los podrá organizar conforme a sus necesidades. El usuario tiene a su disposición los siguientes criterios de clasificación.

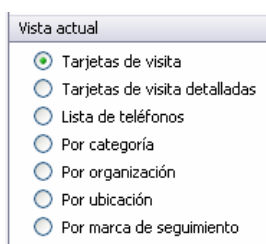


Figura 4.10 Criterios de clasificación de contactos.

Por ejemplo, en la siguiente figura se indica la lista de contactos según la organización a la que pertenecen.

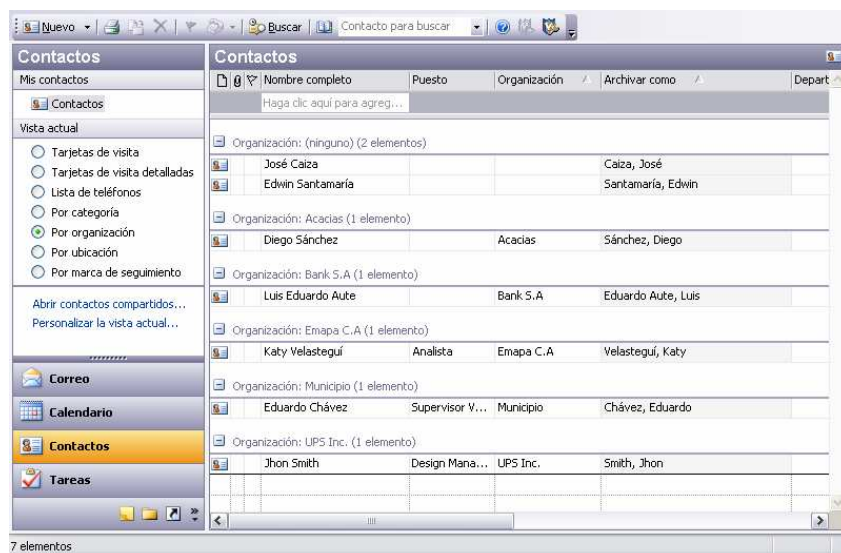


Figura 4.11 Contactos clasificados según la organización a la que pertenecen.

El usuario podrá emplear el criterio de clasificación que mejor se ajuste a sus necesidades.

#### 4.2.2.2 Modificar y eliminar contactos.

Con el paso del tiempo, los datos de un contacto podrán cambiar y para otros ya no habrá necesidad de mantenerlos almacenados. El usuario necesitará modificar y eliminar contactos también.

Este servicio le permite al usuario realizar estas acciones de manera sencilla.

Para modificar un contacto, el usuario podrá hacerlo tan sólo haciendo clic sobre el ítem que se desee modificar (dirección, números telefónicos, de fax, etc).

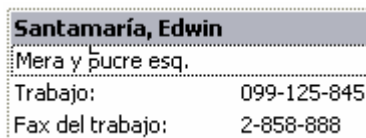


Figura 4.12 Modificación de un contacto.

La eliminación de un contacto el usuario lo podrá hacer marcando con el ratón el contacto y presionar la tecla SUPR o haciendo clic derecho sobre el contacto y seleccionar *Eliminar*.

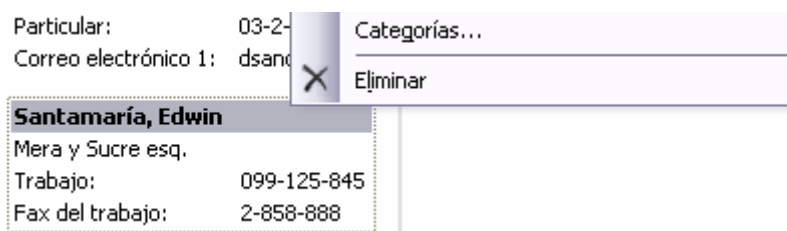


Figura 4.13 Eliminación de un contacto.

## 4.2.3 CITAS.

### 4.2.3.1 Configuración del horario laboral.

Considerando que las citas y eventos se realizan únicamente dentro del horario laboral, primeramente el usuario deberá configurar este horario, que Outlook lo denomina *semana laboral*.

Por defecto, la semana laboral está definida de lunes a viernes entre las 8 de la mañana y las 5 de la tarde. El usuario podrá configurar su semana laboral seleccionando los días laborables, y las horas de inicio y fin de su jornada diaria(ver siguiente página).

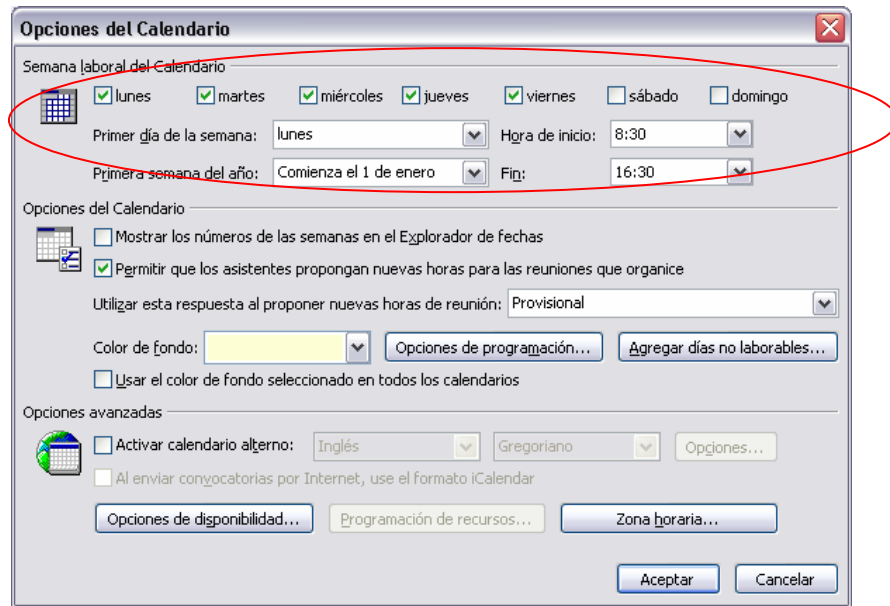


Figura 4.14 Configuración de la semana laboral del usuario.

#### 4.2.3.2 Programar Citas.

La programación de citas y eventos puede ayudar al usuario a gestionar su planificación diaria. La diferencia única entre cita y evento radica en que la cita ocupa parte del día y el evento suele durar todo el día; el mismo método para programar citas se emplea para programar eventos.

Al seleccionar el acceso directo *Calendario*, aparecerá en pantalla la fecha correspondiente al día actual. Si el usuario desea crear la cita para otra fecha, la debe seleccionar del calendario ubicado en la parte superior izquierda.



Figura 4.15 Calendario.

Para crear la cita se debe hacer doble clic en la hora en la cual se desea programarla. Puede el usuario ingresar datos tales como:



- Asunto.
- Ubicación
- Hora de inicio y de fin, o si la cita ocupará todo el día.
- Tiempo previo a la hora de inicio de la cita en el que ocurrirá un recordatorio, 15 minutos es el valor por defecto.
- Alguna nota, etc.

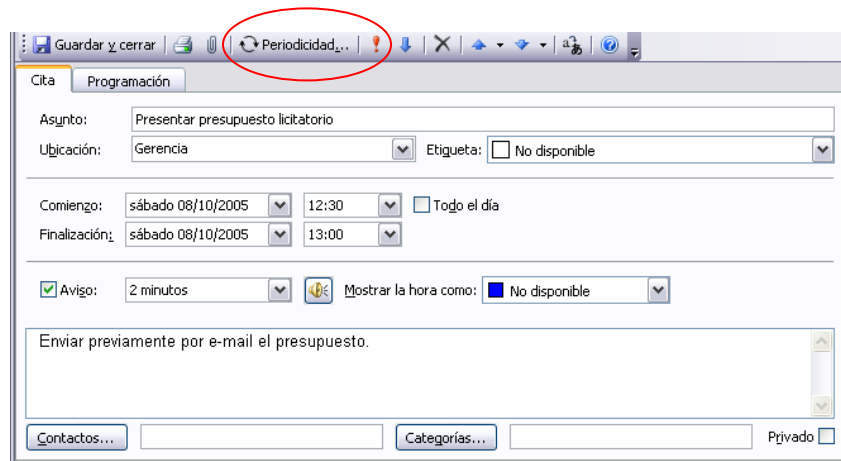


Figura 4.16 Creación de una cita.

Este servicio también ofrece la posibilidad de crear citas o eventos periódicos, lo cual resultará de gran utilidad a determinados usuarios, quienes deben realizar tareas repetitivas cotidianamente mientras una obra se encuentra en construcción. Si se desea que la cita sea periódica, se la configura mediante el botón *Periodicidad* (resaltado en la imagen anterior).

**Repetir cita**

**Hora de la cita**  
 Inicio: 12:30 Fin: 13:00 Duración: 30 minutos

**Frecuencia**  
 Diaria Repetir cada 1 semanas el:  
 Semanal  lunes  martes  miércoles  jueves  
 Mensual  viernes  sábado  domingo  
 Anual

**Intervalo de repetición**  
 Comienzo: sábado 08/10/2005  Sin fecha de finalización  
 Finalizar después de: 10 repeticiones  
 Finalizar el: sábado 10/12/2005

Aceptar Cancelar Quitar repetición

Figura 4.17 Periodicidad de una cita.

#### 4.2.3.3 Modificar y eliminar una cita.

El usuario podrá ver el contenido de una cita al hacer doble clic sobre la tarea o hacer clic derecho y seleccionar *Abrir*. Tras hacer los cambios necesarios, mediante el botón *Guardar y cerrar* se aplicarán los cambios.

Para eliminar una cita, se la debe marcar con el ratón y presionar la tecla SUPR, o hacer clic derecho sobre la cita y seleccionar *Eliminar*.

#### 4.2.4 TAREAS.

Las tareas permiten al usuario crear actividades a las que les debe dar seguimiento.

##### 4.2.4.1 Configuración.

Le resultará de utilidad al usuario asignar colores a las tareas atrasadas y a las tareas completadas.

**Opciones de Tareas**

Opciones de Tareas

Color de tareas atrasadas: [Red color selector]

Color de tareas completadas: [Grey color selector]

Guardar copias actualizadas de las tareas asignadas en mi lista de tareas

Enviar informes de estado cuando se hayan completado las tareas asignadas

Establecer avisos para las tareas con fecha de vencimiento

Aceptar Cancelar

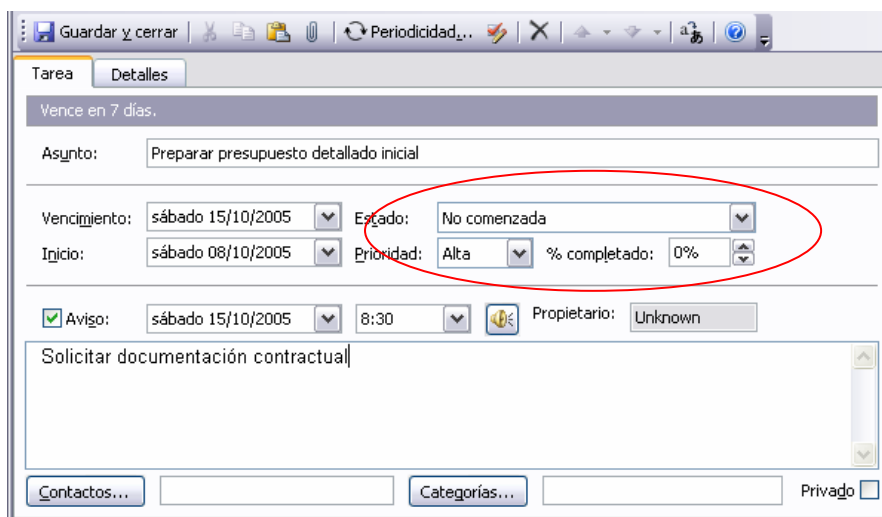
Figura 4.18 Ventana de opciones de tareas.

#### 4.2.4.2 Creación y seguimiento de tareas.

La creación de una tarea es similar a la creación de una cita. Pueden ingresarse datos tales como:

- Asunto.
- Fechas de vencimiento e inicio.
- Fecha y hora de recordatorio.
- Prioridad.
- Porcentaje de completitud.
- Alguna nota, etc.

Al usuario le resultarán de gran utilidad los campos *Estado*, *Prioridad* y *%completado* para darle seguimiento a una determinada tarea.



The screenshot shows a web-based task creation interface. At the top, there are navigation buttons: 'Guardar y cerrar', a clipboard icon, a folder icon, a printer icon, and a 'Periodicidad...' button. Below this is a tabbed interface with 'Tarea' and 'Detalles' tabs. A status bar indicates 'Vence en 7 días.'. The main form fields are: 'Asunto:' with the value 'Preparar presupuesto detallado inicial'; 'Vencimiento:' with a dropdown set to 'sábado 15/10/2005'; 'Inicio:' with a dropdown set to 'sábado 08/10/2005'; 'Estado:' with a dropdown set to 'No comenzada'; 'Prioridad:' with a dropdown set to 'Alta'; and '% completado:' with a spinner set to '0%'. A red oval highlights the 'Estado:', 'Prioridad:', and '% completado:' fields. Below these are fields for 'Aviso:' (checked), 'sábado 15/10/2005', '8:30', a reminder icon, and 'Propietario:' with the value 'Unknown'. A text area contains the note 'Solicitar documentación contractual'. At the bottom, there are buttons for 'Contactos...', 'Categorías...', and a 'Privado' checkbox.

Figura 4.19 Creación de una nueva tarea.

Mediante el botón *Periodicidad* se puede configurar la frecuencia con la que se repite una tarea. Se configura de manera idéntica a la periodicidad de las citas (ver Figura 4.15).

Puede el usuario configurar la visualización de sus tareas en una escala de tiempo.

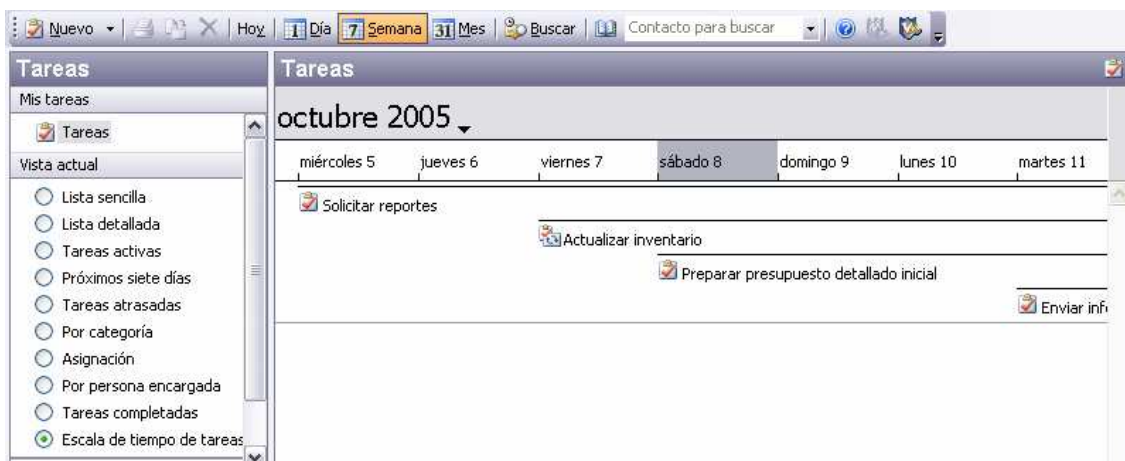


Figura 4.20 Diagrama de escala de tiempo de las tareas.

#### 4.2.4.3 Modificación y Eliminación de Tareas.

Se accesa al contenido de una tarea mediante un clic derecho sobre la misma y seleccionar *Abrir*, o simplemente con un doble clic. Tras haber hecho los cambios necesarios hacer clic en el botón *Guardar y cerrar*.

Cuando el usuario requiera eliminar una tarea lo puede hacer marcando con el ratón la tarea a eliminar y presionar la tecla SUPR o hacer clic derecho sobre la misma y seleccionar *Eliminar*.

### 4.3 IMPLANTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INTRANET.

El presente trabajo enfatiza su enfoque en la seguridad lógica de los recursos disponibles en la intranet de la empresa constructora.

Como ya se detalló en el capítulo anterior, toda política norma y procedimiento de seguridad tratan únicamente temas relacionados con la seguridad lógica de la intranet. Se prefirió dar prioridad a la seguridad lógica, ya que afecta de forma más cercana a las actividades cotidianas de todo el personal que labora en la mencionada empresa.

Ciertos aspectos relacionados con la seguridad física fueron considerados en el análisis de riesgos realizado en el capítulo 2.

Ya que la seguridad de un ambiente informático debe ser revisada y evaluada con determinada frecuencia, en un futuro trabajo al respecto podrá considerarse en mayor profundidad aspectos relacionados con la seguridad física.

Con la finalidad de proteger el ambiente de producción, se destinó una estación de trabajo para realizar todo tipo de pruebas antes de aplicar actualizaciones o nuevas medidas de seguridad en la intranet.

Este computador de pruebas antes fue utilizado en una de las obras y debido a que ésta concluyó y no se la requiere en ninguna obra en construcción por el momento, se decidió destinarla de manera permanente para la realización de pruebas. Si a futuro se requiere de este computador para alguna obra en construcción, se procederá a comprar otra.

El servidor cortafuegos corporativo también fue configurado como servidor VPN.

Con la finalidad de facilitar las tareas de asistencia técnica remota a través del enlace VPN, se instaló en todo computador de la empresa constructora el componente servidor de una aplicación VNC.

Al inicio de los trabajos de implantación de las políticas de seguridad, la empresa constructora tenía las siguientes obras en proceso de construcción:

- Guasmo Sur.
- Terminal Río Daule.
- Bastión Popular.

#### **4.3.1 IMPLANTACIÓN DE POLÍTICAS DE SEGURIDAD EN SOFTWARE.**

##### **4.3.1.1 Protección contra código malicioso**

###### *4.3.1.1.1 Instalación de antivirus, antispyware y cortafuegos personal.*

Siguiendo las políticas normas y procedimientos mencionados en el capítulo anterior, se procedió a instalar en todo computador software antivirus y

antispyware en todo computador de la oficina central y de las obras actualmente en construcción.

Las aplicaciones instaladas fueron:

- Virus Scan Enterprise v8.0i de McAfee
- Ad-Aware SE Personal v1.06 de Lavasoft

De manera inmediata se procedió a actualizar a la fecha a estas dos aplicaciones.

El cortafuegos personal a utilizar es aquel incluido por defecto en los sistemas operativos Microsoft empleados, es decir, Windows XP versión Profesional y Windows Server 2003 edición Enterprise.

#### *4.3.1.1.2 Demostración de revisión total de una estación de trabajo en busca de código malicioso empleando el antivirus y antispyware instalados.*

De manera coordinada entre el área directiva y la empresa de asistencia técnica, se convocó a una reunión a todo el personal de la empresa constructora en la cual se hicieron demostraciones de carácter técnico para que los empleados aprendan a utilizar los nuevos servicios, aplicaciones, políticas, normas y procedimientos.

Una de las charlas de esta reunión consistió en el modo en el cual los usuarios deben realizar una revisión periódica total de su respectiva estación de trabajo empleando las aplicaciones antivirus y antispyware. Además se les indicó cómo proceder en caso de que algún código malicioso no fuera removido.

Se les indicó que la frecuencia con la cual deben realizar esta tarea es semanal, conforme a lo especificado en los procedimientos de seguridad informática.

#### *4.3.1.1.3 Actualización de antivirus y antispyware.*

Durante el período de contacto mantenido con la empresa constructora desde el inicio de implantación de las políticas de seguridad, se llegó a realizar una sola actualización de antivirus y antispyware desde la ciudad de Quito, empleando la conexión VPN.

En esta ocasión se procedió conforme a lo especificado en las políticas de seguridad, es decir, primeramente se descargaron de Internet los archivos de actualización de las dos aplicaciones, y a continuación, mediante una conexión VNC a cada estación de trabajo, se copiaron los archivos del computador de pruebas y se actualizaron estas aplicaciones.

*4.3.1.1.4 Revisión total de estaciones de trabajo en busca de código malicioso.*

Esta tarea se la pudo realizar una sola vez, durante el período mencionado en el numeral anterior.

Como todo el personal ya conocía el procedimiento, todos ejecutaron la tarea de la manera establecida. Cabe señalar que en esta ocasión ningún código malicioso fue detectado en ningún computador de la oficina central u obras en construcción.

**4.3.1.2 Actualización de sistema operativo y aplicaciones.**

En el mencionado período no se realizaron actualizaciones desde Internet de ningún sistema operativo o aplicación.

El sistema operativo de las estaciones de trabajo, tras haber sido instalado, fue actualizado con el Paquete de Servicios 2 (Service Pack 2) para Microsoft Windows XP Profesional.

El sistema operativo del servidor controlador de dominio, tras haber sido instalado, fue actualizado con el Paquete de Servicios 1 (Service Pack 1) para Microsoft Windows Server 2003.

El sistema de gestión de bases de datos instalado en el servidor controlador de dominio es SQL Server 2000 Standard Edition, el cual fue actualizado con el correspondiente Paquete de Servicios 3 (Service Pack 3), tras haber sido instalado.

El paquete ofimático Microsoft Office 2003 Edición Profesional, tras haber sido instalado, fue actualizado con el correspondiente Paquete de Servicios 1 (Service Pack 1).

#### **4.3.1.3 Instalación de un servidor cortafuegos corporativo.**

Por política dictada en el numeral 3.3.1.1 se procedió a instalar un servidor cortafuegos corporativo en la empresa constructora.

Este servidor se instaló en un computador de idénticas características al de una estación de trabajo de la oficina central.

Este servidor cuenta con sistema operativo Red Hat versión 9.0, y la aplicación cortafuegos es *iptables*.

Tras acuerdo entre el área directiva y la empresa de asistencia técnica, el esquema de filtrado aplicado se basa en el número IP de la estación de trabajo que desea navegar en Internet.

No se aplicó restricción al tráfico correspondiente al correo electrónico.

Al servidor controlador de dominio le fue restringido totalmente su acceso a Internet.

Durante el período de contacto mantenido con la empresa constructora desde el inicio de implantación de las políticas de seguridad no se realizaron cambios a las reglas de filtrado del servidor cortafuegos.

### **4.3.2 IMPLANTACIÓN DE POLÍTICAS DE SEGURIDAD PARA CONTROL DE ACCESO Y UTILIZACIÓN DE SERVICIOS E INFORMACIÓN.**

#### **4.3.2.1 Demostración de utilización de Internet y correo electrónico.**

En la reunión mencionada en 4.3.1.1.2 se dieron a conocer también las reglas de utilización de los servicios de Internet y correo electrónico conforme se detalla en las políticas de seguridad del capítulo 3.

A continuación se hizo una demostración del uso de Internet y cómo guardar en disco duro información que se crea importante.

En la demostración referente al servicio de correo electrónico, se indicó además de su utilización, la forma de revisar la antigüedad de los mensajes recibidos, cómo eliminarlos o guardarlos, y qué hacer ante un mensaje electrónico no deseado.



Durante el período de contacto mantenido con la empresa constructora desde el inicio de implantación de las políticas de seguridad no fue necesaria la eliminación de mensajes por parte de ningún usuario. Deberá transcurrir un tiempo más para que esta acción sea realizada.

#### **4.3.2.2 Políticas de cuentas de usuario.**

##### *4.3.2.2.1 Creación de cuentas de usuario*

En base al listado de usuarios proveído por el personal de soporte interno, se crearon cuentas de usuario en el servidor controlador de dominio, siguiendo las políticas de seguridad detalladas en el capítulo 3.

Toda cuenta de usuario posee el perfil de usuario normal, existe una sola cuenta con privilegios administrativos, esta es la cuenta “Administrador”.

##### *4.3.2.2.2 Soporte al usuario en el uso de su cuenta de dominio.*

En la reunión de información técnica antes mencionada, se les mencionó que de ahora en adelante la red operará bajo un esquema de dominio. Se explicó en qué consiste este concepto y los beneficios de seguridad y administración centralizada.

Se mencionaron las políticas referentes a las cuentas de usuario.

Se les indicó que para poder utilizar su respectiva estación de trabajo deberán ingresar su nombre de usuario y contraseña, y cómo construirla, según lo especificado por las políticas de seguridad.

Cuando el usuario se disponía a usar por primera vez su nueva estación de trabajo, de manera individual se asistió al usuario en la creación de su nueva contraseña.

Se mencionó el procedimiento a seguir en caso de que superen el número de intentos de acceso fallidos al dominio.

#### **4.3.2.3 Acceso a información electrónica disponible en la red.**

##### *4.3.2.3.1 Demostración de acceso a información electrónica disponible en la red.*

En la charla correspondiente a este tema hubo una demostración de acceso a una carpeta compartida a todo usuario ubicada en el servidor, y lo que ocurre cuando se intenta acceder a una carpeta compartida para la cual el usuario no tiene permisos de acceso.

##### *4.3.2.3.2 Configuración de carpetas compartidas en el servidor.*

Al finalizar la reunión, se procedió a asignar permisos a las carpetas compartidas según los requerimientos laborales de los usuarios; esta acción se la realizó coordinadamente con el personal de soporte interno, que conocía de antemano estos requerimientos. A continuación se crearon accesos directos a las mencionadas carpetas en las estaciones de trabajo de los usuarios que lo requieren y se comprobó su funcionamiento.

#### **4.3.2.4 Implementación y uso de los enlaces VPN.**

##### *4.3.2.4.1 Implantación del enlace permanente entre Quito y Guayaquil.*

Para más detalles al respecto referirse al numeral 4.4

##### *4.3.2.4.2 Implantación de enlaces punto a punto entre obras en construcción y oficina central.*

En las obras en construcción se implementó el enlace dedicado punto a punto hacia la oficina central para lo cual se empleó un modem de datos en cada obra y otro de estos dispositivos en la oficina central. Los enlaces dedicados con las obras representan una extensión de la red LAN y no se requiere de implantación de routers.

Cabe recalcar que en las obras ya se contaba con el equipo de comunicaciones y cableado necesario para implantar una pequeña red LAN.

#### **4.3.2.5 respaldos y recuperación de archivos.**

##### *4.3.2.5.1 Demostración de Respaldos y recuperación de archivos.*

En la charla referente a este tema se mencionó la importancia y ventajas de realizar respaldos de archivos importantes.

Se indicó que cada persona poseerá una carpeta ubicada en el servidor, en la cual podrán realizar sus copias de respaldo, la cual es de responsabilidad de cada quien, ya que únicamente el usuario podrá tener acceso a su carpeta.

A continuación se realizó una demostración de cómo crear copias de respaldo en el servidor y también de la imposibilidad de obtener acceso a la carpeta empleando otra cuenta de usuario.

Se demostró también la manera de recuperar archivos respaldados.

La demostración también incluyó la forma en la cual los jefes de las áreas de contabilidad y presupuestos pueden realizar respaldos y recuperación de la información de las aplicaciones de contabilidad y respaldos.

#### *4.3.2.5.2 Configuración de carpetas compartidas en el servidor para respaldos.*

Al finalizar la reunión de información técnica, se procedió a crear una carpeta compartida en el servidor por cada usuario y se aplicaron los permisos de acceso adecuados de manera que sea el usuario el único con la capacidad de accederla.

## **4.4 IMPLANTACIÓN DE LA VPN.**

Este tipo de enlace tiene como propósito el facilitar las tareas de asistencia técnica remota que desde la ciudad de Quito la empresa de asistencia técnica brinda a la empresa constructora.

Debido a los problemas padecidos por el anterior enlace a Internet, se decidió contratar a otro ISP un enlace dedicado. Por motivos de facilidad en el manejo del enlace VPN se decidió contratar el enlace dedicado al mismo ISP de la empresa de asistencia técnica.

En el servidor de la empresa constructora en el que se va a configurar el mencionado enlace se decidió instalar Red Hat v9.0 por motivos de compatibilidad, ya que el mismo sistema operativo se encuentra instalado en el

servidor de la empresa de asistencia técnica en el cual se configurará también este enlace.

La aplicación utilizada para implementar este enlace es *VTUN*.

A continuación se procedió a instalar los siguientes paquetes proveídos por el ISP en los dos servidores antes mencionados:

- *tun-1.1-7.rh9.i386.rpm*: es el driver que implementa el dispositivo virtual de red punto a punto. Este dispositivo virtual es utilizado por cualquier aplicación de tunneling, tal como VTUN, la cual veremos a continuación.
- *vtun-2.6-2.rh9.i386.rpm*: es la aplicación que permite crear túneles virtuales sobre redes TCP/IP con encriptación y compresión. VTUN provee autenticación basada en desafío y encriptación BlowFish de 128bits.
- *lzo-1.08.tar.gz*: es la aplicación en la cual se basa VTUN para implementar compresión. Esta aplicación puede trabajar sobre TCP o UDP.

El ISP también proveyó el archivo de configuración necesario (*vtund.conf*), el cual debe ser copiado en el siguiente path<sup>31</sup>: */etc/*

En el archivo de configuración, únicamente deben cambiarse números IP, rutas y nombre de túnel empleados. El archivo de configuración se encuentra detallado en el Anexo C.

El componente servidor es iniciado con la siguiente línea de comandos<sup>32</sup>:

- *“vtun -s”*.

El componente cliente es iniciado con la siguiente línea de comandos:

- *“vtun -c nombre\_del\_tunel IP\_real\_servidor”*

En la siguiente figura se muestra el esquema de este enlace.

---

<sup>31/32</sup>KRASNYANSKY, Maxim. VTun - Virtual Tunnels over TCP/IP networks.

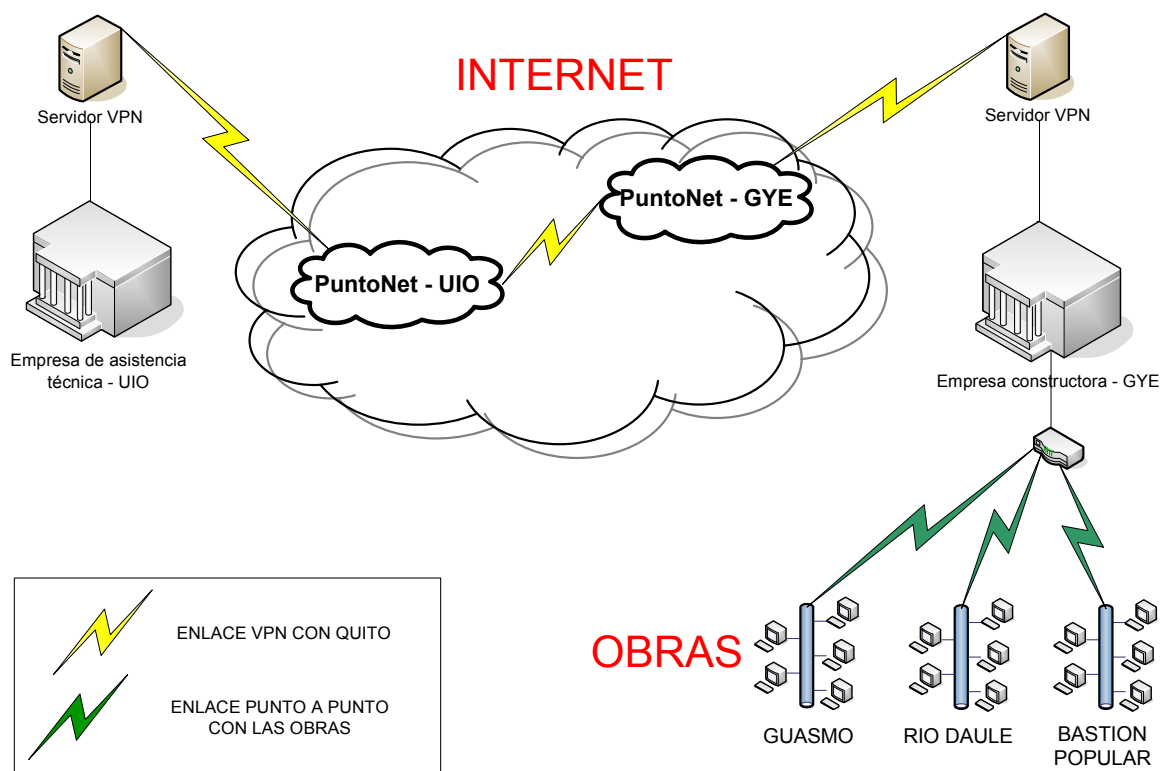


Figura 4.21. Esquema del enlace VPN entre las dos empresas y enlaces con obras.

En esta figura se incluyeron los enlaces punto a punto con las obras ya que la asistencia técnica remota también se realizará en las obras en construcción.

#### 4.5 PRUEBAS DE FUNCIONAMIENTO DE LA APLICACIÓN PARA CONTROL DE PRESUPUESTOS EN AMBIENTE E-BUSINESS.

Las pruebas realizadas mostradas en este trabajo se enfocan en la aplicación de control de presupuestos, e incluyen lo siguiente:

- Acceso a los sistemas de contabilidad y presupuestos.
- Creación de una obra.
- Creación del presupuesto licitatorio.
- Creación e importación de rubros en el presupuesto.
- Creación del presupuesto detallado inicial.

- Obtención de cronogramas.
- Obtención de reportes.
- Manejo de materiales, mano de obra y equipos en el módulo de mantenimiento.
- Integración con el sistema contable: creación de unidades de medida, creación automática de cuentas contables al licitar una obra.

A continuación se muestran las pantallas capturadas de las pruebas realizadas.

#### 4.5.1 ACCESO A LOS SISTEMAS DE CONTABILIDAD Y PRESUPUESTOS.

Las aplicaciones de contabilidad y control de presupuestos son accesibles mediante una interfaz común de autenticación.

Como se estableció en el numeral 2.2, la nueva aplicación implementará comunicaciones seguras a través de SSL; las zonas resaltadas en la siguiente figura muestran que entre la estación de trabajo del usuario y el servidor Web existen este tipo de comunicaciones.

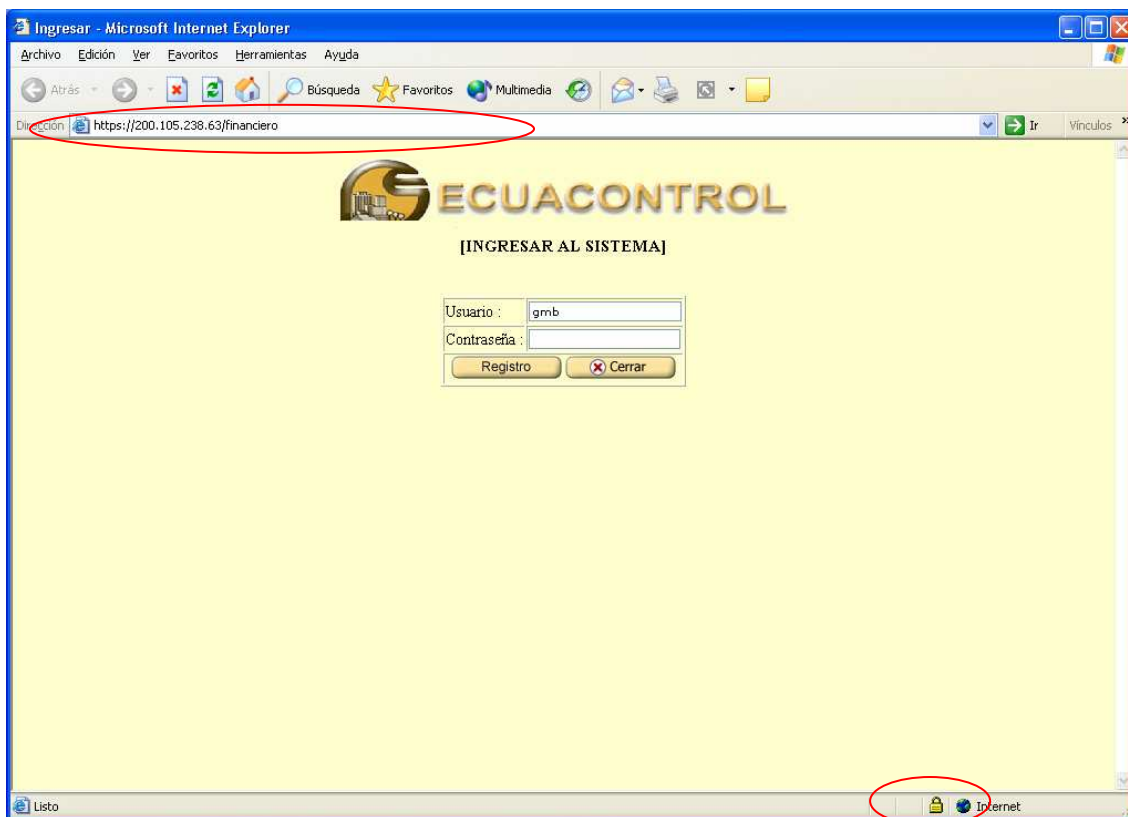


Figura 4.22 Pantalla de acceso común.

El usuario deberá escoger el sistema con el que desea trabajar.



Figura 4.23 Accesos a los sistemas de contabilidad y control de presupuestos.

Dependiendo del perfil del usuario uno de estos dos accesos a los sistemas puede estar deshabilitado.

El sistema de control de presupuestos tiene el siguiente aspecto:



Figura 4.24 Menú de la aplicación de control de presupuestos.

El sistema de contabilidad tiene el siguiente aspecto:



Figura 4.25 Menú de la aplicación de contabilidad.

#### 4.5.2 CREACIÓN DE UNA OBRA.

Una vez obtenidas las bases para concursar en una determinada licitación, los trabajos en oficina central comienzan con la creación de una obra.

Una obra es creada desde el menú *Mantenimiento y Parámetros, Actualización de Tablas, Obras*



Figura 4.26 Opción para creación de una obra.



A continuación se procede a crear la obra en sí. Los datos de una obra se clasifican en cuatro áreas: Generales, Costos Indirectos, Comparación y Parámetros.

En el área *Generales* se ingresan datos tales como: nombre de la obra, descripción, cliente, la ciudad, área de construcción, plazo, etc.

**ECUACONTROL**

[ OBRA - MANTENIMIENTO ]

Generales | Costos Indirectos | Comparación | Parámetros

Nuevo | Grabar

Código:  Campos Requeridos=\*

Nombre de Obra:

Descripción:

Cliente:

Dirección:

Ciudad:

Contratista:

Especificaciones:

Área de Construcción:  Licitación:

Plazo:

Creada:  Actualizada:

Tipo Obra:  Estado:

Fechas de la Obra

Presentación Licitación:  Inicio:  Terminación:

Figura 4.27 Datos generales de una nueva obra.

En la sección *Costos Indirectos* se ingresan los porcentajes de costos tales como garantías, promoción, seguros, prevención de accidentes, etc.

**ECUACONTROL**

[ OBRA - MANTENIMIENTO ]

Generales | Costos Indirectos | Comparación | Parámetros

Nuevo | Grabar

Escoger Costos Indirectos \*

Comando	Código	Nombre	%
Cancelar Actualizar	0001	Dirección de Obra	0.01
Eliminar Editar	0004	Vehículos	0.00
Eliminar Editar	0006	Promoción	0.00

Total Costos Indirectos: 0.00%

Figura 4.28 Porcentajes de costos indirectos.

En la sección *Comparación* se ingresan los valores de las propuestas de otras empresas.

En la sección *Parámetros* se ingresan valores asociados con el cálculo de mano de obra, materiales y equipos entre otras cosas.

Entonces se procede a guardar la obra mediante el botón *Grabar*.

#### 4.5.3 CREACIÓN DEL PRESUPUESTO LICITATORIO.

El presupuesto licitatorio incluye información general necesaria para concursar. Para crearlo se lo hace a través del menú *Preparación de Oferta, Presupuestar la Obra, Presupuesto Licitatorio*.



Figura 4.29 Menú de creación del presupuesto licitatorio.

Se obtiene un listado de obras creadas para seleccionar la que se desea presupuestar

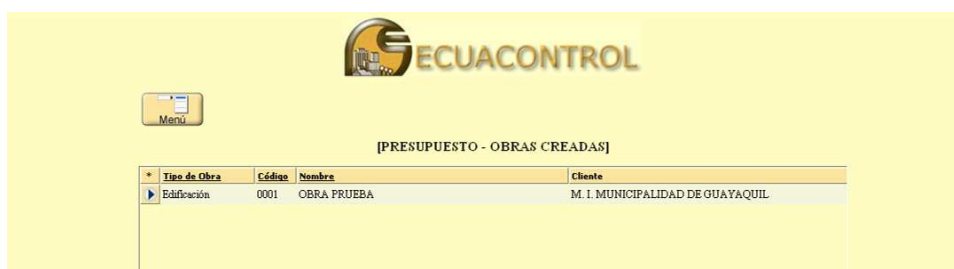


Figura 4.30 Selección de obra a ser presupuestada.

A continuación se obtienen sus datos generales y las opciones para importación de rubros: no importar, importar de la obra estándar e importar de otra obra según su código.

Figura 4.31 Datos generales de obra y opciones de importación de rubros.

Los rubros son los componentes o fases a seguirse en una obra en construcción, por ejemplo “Remoción de estructuras existentes”. Los rubros se organizan en una estructura de árbol. No se han importado rubros en el ejemplo de la siguiente figura



Figura 4.32 Obra sin rubros.

#### 4.5.4 CREACIÓN E IMPORTACIÓN DE RUBROS EN EL PRESUPUESTO.

El nodo del árbol lo ocupa el nombre de la obra, en segundo y tercer nivel de profundidad en el árbol pueden definirse nodos contenedores, los nodos hoja son los rubros en sí. En la siguiente figura consta la creación de un nodo contenedor, los cuales llevan el nombre *rubro título*.

**ECUACONTROL**

[PRESUPUESTO - AGREGAR TITULO]

Nombre:  Campos Requeridos=\*

Descripción:

No se ha especificado un nombre

Figura 4.33 Creación de un nodo contenedor de rubros.

La siguiente figura muestra los nodos contenedores de la obra estándar.

**ECUACONTROL**

[PRESUPUESTO - IMPORTAR RUBRO]

Código  Nombre

Todos

* Codigo	Nombre	Tipo	Cantidad	Unidad
<input type="checkbox"/> 0002	Desbroce, Deboscado y Limpieza(INC. Desalojo)	Rubro	6,0000	Hectáreas
<input type="checkbox"/> 0003	Excavación sin clasificar (INC. Desalojo)	Rubro	75000,0000	Metros Cúbicos
<input type="checkbox"/> 0004	Excavación en roca (INC. Desalojo) zona poblada	Rubro	28000,0000	Metros Cúbicos
<input type="checkbox"/> 0005	Material de prestamo local	Rubro	45000,0000	Metros Cúbicos
<input type="checkbox"/> 0006	Remoción de estructuras existentes	Rubro	800,0000	Metros Cuadrados
<input type="checkbox"/> 0008	Hormigón Estructural/Cem. Portl F/C=280 kg/cm2(INC. ENC)	Rubro	2381,0000	Metros Cúbicos
<input type="checkbox"/> 0009	Hormigón Estructural/Cem. Portl F/C=350 kg/cm2(INC. Enc)	Rubro	84,0000	Metros Cúbicos
<input type="checkbox"/> 0010	Hormigón Ciclopeo	Rubro	58,0000	Metros Cúbicos
<input type="checkbox"/> 0011	Geotextil NT1600	Rubro	3580,0000	Metros Cuadrados
<input type="checkbox"/> 0012	Material Filtrante	Rubro	48,0000	Metros Cúbicos

Figura 4.34 Nodos contenedores de rubros de la obra estándar.

#### 4.5.5 CREACIÓN DEL PRESUPUESTO DETALLADO INICIAL

Una vez ganado el concurso, al presupuesto licitatorio se le añaden más detalles y es convertido en el presupuesto detallado inicial mediante la opción *Licitat* de la lista de opciones que se encuentran en el lado izquierdo de la estructura de árbol.

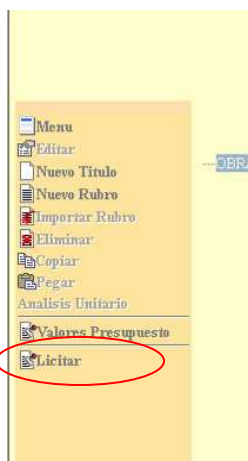


Figura 4.35 Conversión del presupuesto licitatorio al presupuesto detallado inicial.

#### 4.5.6 OBTENCIÓN DE CRONOGRAMAS.

La nueva aplicación ofrece la funcionalidad de exportación de cronogramas en formato de Microsoft Project. Los cronogramas pueden ser exportados desde el menú *Preparación de Oferta, Presupuestar la Obra*. En este caso se demuestra la exportación del cronograma de equipo.



Figura 4.36 Opción para exportación del cronograma de equipo.

Debe seleccionarse la obra de la cual se desea obtener el cronograma de equipo. Este cronograma se lo obtendrá tras aceptar que se desea ver el archivo.



Figura 4.37 Exportación del cronograma de equipo de una obra dada.

Lo que se obtiene es una ventana de Microsoft Project con los detalles del cronograma, tal como lo muestra la siguiente figura.

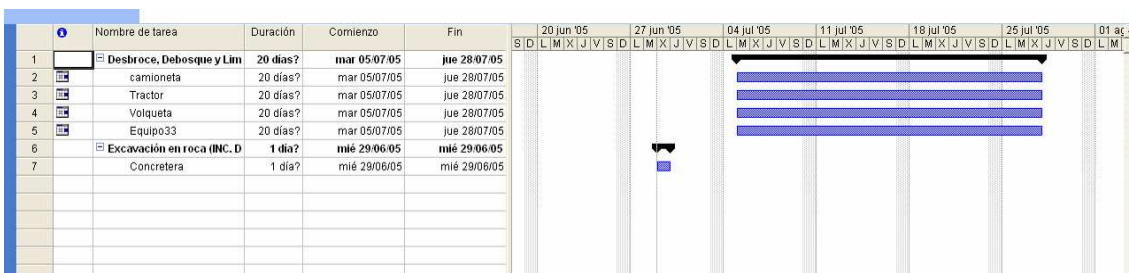


Figura 4.38 Detalles del cronograma de equipo exportado a Microsoft Project.

Al cerrar esta ventana, el sistema ofrece la posibilidad de guardar el cronograma como un archivo de Microsoft Project.

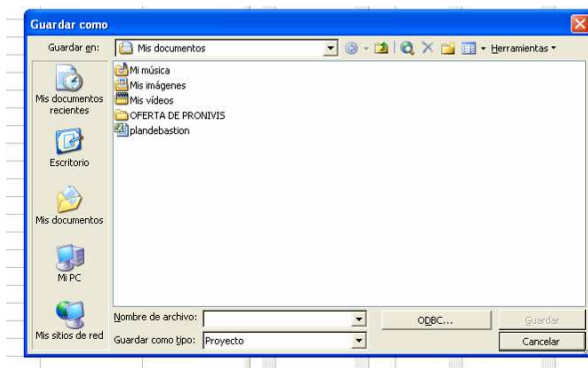


Figura 4.39 Selección de la ubicación del archivo.

#### 4.5.7 OBTENCIÓN DE REPORTES.

A través del menú *Informes* pueden obtenerse una variedad de reportes.



Figura 4.40 Menú de informes.

Como demostración se indicarán los siguientes reportes:

- Tabla de cantidades y precios.
- Resumen de Materiales, Mano de Obra, Equipo y Transporte.
- Detalle de Materiales.

Para obtener cada reporte primeramente se deberá escoger la obra deseada de una lista de obras.

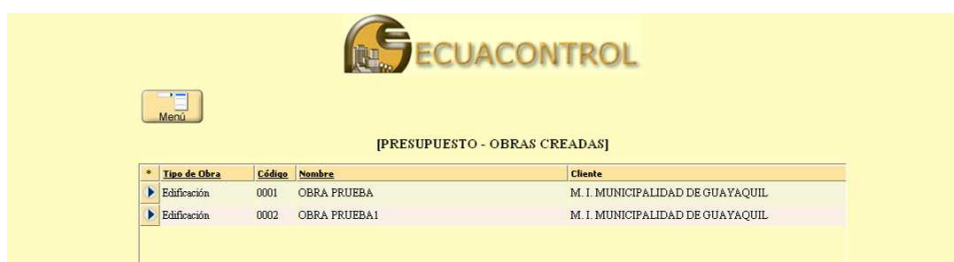


Figura 4.41 Listado de obras de las cuales se pueden obtener reportes.

La tabla de cantidades y precios ofrece un resumen, a la fecha, de los costos asociados a cada presupuesto de la obra.

NOMBRE DEL PROPONENTE: Ecuacostrucciones(Perez-Perazo)						FORMULARIO Nº 18
OBRA PRUEBA						
TABLA DE CANTIDADES Y PRECIOS						
CODIGO	RUBROS	UNIDAD	CANTIDAD	PRECIO UNITARIO	PRECIO PARCIAL US: \$ DOLAR	
<b>TITULO I</b>						
	Desbroce, Debroque Y Limpieza(INC. Desalojo)	HA	6.00	\$ 5,111.44	\$ 30,668.64	
	Excavación En Roca (INC. Desalojo) Zona Poblada	M3	28000.00	\$ 11.42	\$ 319,760.00	
<b>CIMENTACION</b>						
	Hormigon Estructural/Cem. Perfil F'c=250 Kg/Cm2(INC.Enc)	M3	447.00	\$ 0.00	\$ 0.00	
	Colocación De Arena	M3	480.00	\$ 0.00	\$ 0.00	
	Columnas	CJ	15.00	\$ 0.00	\$ 0.00	
				<b>SUMA TOTAL</b>	<b>\$ 350,428.64</b>	
				<b>IVA</b>	<b>\$ 42,051.44</b>	
				<b>TOTAL</b>	<b>\$ 392,480.00</b>	

SON: TRES CIENTOS NOVENTA Y DOS MIL CUATRO CIENTOS OCHENTA CON 0/100

Guayaquil 30 de Junio de 2005

**Ecuacostrucciones S.A. Y Asociado**  
Ing. Walter Egas Peña  
Administrador

Figura 4.42. Listado de costos por rubros y total.

El resumen de *Materiales, Mano de Obra, Equipo y Transporte* nos indica en términos generales los valores presupuestados para estos cuatro grupos.

PRESUPUESTO DE LA OBRA	
ECUAOCONSTRUCCIONES S.A & ASOCIADOS	
<b>FECHA:</b>	6/30/2005
<b>PAGINA:</b>	1
<b>OBRA:</b>	OBRA PRUEBA
PRESUPUESTO GENERAL	
PRESUPUESTO DE MATERIALES	235,727.98
PRESUPUESTO DE EQUIPOS	112,783.00
PRESUPUESTO DE MANO DE OBRA	69.90
PRESUPUESTO DE TRANSPORTE	0.00
<b>TOTAL COSTO DIRECTOS</b>	<b>348,580.88</b>

Figura 4.43 Valores generales de materiales, equipos, mano de obra y transporte.

El reporte *Detalle de Materiales* indica los valores asociados a cada material incluido en la construcción de la obra seleccionada (ver siguiente página).



powered by crystal

LISTADO GENERAL

6/30/2005 12:17:01AM 1

OBRA PRUEBA

Codigo	Nombre	Cantidad	Unidad	PrecioPromo	TotalDolar
0001	CEMENTO TIPO I	[Objeto de texto]4.00	SC	30.77	430.76
0002	CEMENTO BLANCO (50 KG)	10.00	SC	120.66	1,206.60
0003	CEMENTINA (25KG.)	12.23	SC	6.03	73.78
0004	AGUA	1.25	GLN	0.00	0.00
0007	ARENA HOMOGENIZADA	45.00	M3	132.73	5,972.67
0011	PIEDRA HOMOGENIZADA	45.00	M3	78.79	3,545.59
0114	AMPLIFICADOR DE POTENCIA	1.00	U	8,440.17	8,440.17
0118	MICROFONO SELECCIONABLE	1.00	U	3,619.80	3,619.80
0124	ATENUADOR DE VOLUMEN	1.00	U	162.89	162.89
0129	ALTAVOCES EMPOTRADOS	3.00	U	1,085.94	3,257.82
0133	ALTAVOCES EMPOTRADOS	2.00	U	1,550.48	3,100.96
0319	DIESEL	7.36	GLN	28,154.00	207,213.44
<b>TOTAL:</b>					<b>237,024.48</b>

Figura 4.44 Reporte detallado de materiales.

#### 4.5.8 MANEJO DE MATERIALES, MANO DE OBRA Y EQUIPOS EN EL MÓDULO DE MANTENIMIENTO.

El módulo de mantenimiento incluye el submódulo *Actualización de Tablas* y el submódulo *Estados de Obra*.



Figura 4.45 Módulo de mantenimiento.

##### 4.5.8.1 Manejo de materiales.

Desde la opción *Materiales* se obtiene un listado de todos los materiales que emplea la empresa constructora. Este listado se ordena en una estructura de árbol.

**ECUACONTROL**  
No esta seleccionada ninguna empresa.  
[ARTICULOS]

Código	<input type="text"/>	Nombre	<input type="text"/>
Precio Presupuestario:	<input type="text" value="0"/>	Grupo	AGREGADOS
Estado	ACTIVO	Unidad de medida princ.	SACO
Factor de conversión	<input type="text" value="1"/>	Unidad de medida sec.	SACO

- 001 - AGREGADOS
- 003 - MADERAS
- 004 - TABLEROS(CONTRACHAPADOS)TABLEROS PLYWOOD
- 005 - METALES Y FIJACIONES
- 006 - HORMIGON PREMEZCLADO
- 007 - ADITIVOS PARA EL HORMIGON
- 008 - ASFALTOS Y ADHESIVOS
- 009 - AISLANTES E IMPERMEABILIZANTES
- 010 - ELEMENTOS PREFABRICADOS
- 011 - LADRILLOS Y BLOQUES
- 012 - REVESTIMIENTOS
- 013 - ALUMINIO Y VIDRIO
- 014 - PUERTAS Y PASAMANOS
- 015 - CERRAJERIA
- 016 - PINTURAS Y PAPELES MURALES
- 017 - PAREDES Y CIELOS FALSOS
- 018 - ARTEFACTOS DE BAÑO Y COCINA
- 019 - MATERIALES DE ELÉCTRICOS
- 020 - MATERIAL SANITARIOS/TANQUES Y DESAGUES
- 021 - JARDINERIA
- 022 - SEÑALIZACIÓN
- 023 - VARIOS

Figura 4.46 Listado de materiales empleados por la empresa constructora.

Para crear un nuevo material, simplemente se escoge el nodo en el cual se lo incluirá y se ingresan sus detalles.

#### 4.5.8.2 Manejo de equipos

Desde la opción *Equipos* (ver figura 4.45) pueden editarse o crearse nuevos equipos.

Si se desean editar los detalles de un equipo, primero se lo debe seleccionar de un listado de todos los equipos empleados por la empresa constructora.



Figura 4.47 Listado de equipos.

Al obtener en pantalla sus detalles, se los puede modificar y guardar por medio del botón *Actualizar*.

[EQUIPO - MANTENIMIENTO]

Código: 0007 Campos Requeridos=\*

Nombre: Retroexcavadora

Descripción:

Marca: Caterpillar Estado: Activo

Unidad Tiempo: Hora Creado: 23/03/2005

Precio: 22 Actualizado: 25/03/2005

Nuevo Actualizar Eliminar

Figura 4.48 Detalles de un equipo.

También se pueden crear nuevos equipos

Figura 4.49 Confirmación de creación de un nuevo equipo.

#### 4.5.8.3 Manejo de Mano de Obra

El manejo de mano de obra es similar al manejo de equipos. Si se desea modificar los datos de una mano de obra específica, primero se la debe seleccionar de un listado de toda la mano de obra empleada por la empresa constructora.

Código	Nombre	S. Unificado	Jornal Real	Categoría
0001	Peon	151,56	10,81	Primera
0002	Guardian	153,64	11,67	Segunda
0003	Ayudante de Albañil	153,64	12,19	Segunda
0004	Ayudante de operador de equipo	142,79	10,57	Segunda
0005	Ayudante de Ferrero	153,64	10,95	Segunda
0006	Operador de Equipo Liviano	155,22	11,05	Tercera
0007	Pintor	155,22	11,05	Tercera
0008	Ealucador	155,22	11,05	Tercera
0009	Ferrero	155,22	11,05	Tercera
0010	Perforador	158,35	11,26	Cuarta
0011	Albañil	155,22	11,05	Tercera
0012	Carpintero	155,22	11,05	Tercera

Figura 4.50 Listado de mano de Obra.

Al obtener en pantalla sus detalles, se los puede modificar y guardar por medio del botón *Actualizar*.

También existe la opción de crear una nueva mano de obra.

[MANO DE OBRA - MANTENIMIENTO]

Código:  Campos Requeridos=\*

Nombre:

Descripción:

Categoría:

Sueldo Unificado:  Aporte Patronal:

Décimo Tercero:  Total Mensual:

Décimo Cuarto:  Jornal Real:

Fondo de Reserva:  Costo Horario:

Otros 1:  FSR:

Otros 2:  Creado:

Estado:  Actualizado:

Figura 4.51 Ingreso de datos correspondientes a una nueva mano de obra.

Basta con ingresar el valor del sueldo unificado para que se calculen automáticamente los valores del resto de componentes salariales.

[MANO DE OBRA - MANTENIMIENTO]

Código:  Campos Requeridos=\*

Nombre:

Descripción:

Categoría:

Sueldo Unificado:  Aporte Patronal:

Décimo Tercero:  Total Mensual:

Décimo Cuarto:  Jornal Real:

Fondo de Reserva:  Costo Horario:

Otros 1:  FSR:

Otros 2:  Creado:

Estado:  Actualizado:

Microsoft Internet Explorer  
DATOS GUARDADOS  
Aceptar

Figura 4.52 Confirmación de creación de una nueva mano de obra.


#### 4.5.9 INTEGRACIÓN CON EL SISTEMA CONTABLE: Y CREACIÓN AUTOMÁTICA DE CUENTAS CONTABLES AL LICITAR UNA OBRA.

Como demostración, se indicará la creación de unidades de medida y la creación automática de cuentas contables el licitar una obra.

##### 4.5.9.1 Creación de unidades de medida.

El módulo de manejo de unidades se encuentra implementado en el sistema de contabilidad. Al manejar unidades simplemente se utiliza un formulario del sistema contable. Al manejar proveedores existe también afectación contable como se verá a continuación.

Al seleccionar la opción *Unidades* (ver Figura 4.45) se obtiene un listado de todas la unidades utilizadas por la empresa constructora.



No esta seleccionada ninguna empresa.  
[UNIDADES DE MEDIDA]

	Cod. Unidad	Nombre	Sigla
<input type="checkbox"/>	0001	SACO	SC
<input type="checkbox"/>	0002	GALON	GLN
<input type="checkbox"/>	0003	METRO	M
<input type="checkbox"/>	0004	METRO LINEAL	ML
<input type="checkbox"/>	0005	METRO CUADRADO	M2
<input type="checkbox"/>	0006	METRO CUBICO	M3
<input type="checkbox"/>	0007	UNIDAD	U
<input type="checkbox"/>	0008	KILOGRAMO	KG
<input type="checkbox"/>	0009	GLOBAL	GBL
<input type="checkbox"/>	0010	LIBRA	LB
<input type="checkbox"/>	0011	CAJON	CA

Figura 4.53 Listado de unidades.

Se puede editar un ítem simplemente al seleccionarlo



No esta seleccionada ninguna empresa.  
[UNIDADES DE MEDIDA]

	Cod. Unidad	Nombre	Sigla
<input type="checkbox"/>	0001	SACO	SC
<input checked="" type="checkbox"/>	0002	GALON	GLN
<input type="checkbox"/>	0003	METRO	M
<input type="checkbox"/>	0004	METRO LINEAL	ML
<input type="checkbox"/>	0005	METRO CUADRADO	M2
<input type="checkbox"/>	0006	METRO CUBICO	M3
<input type="checkbox"/>	0007	UNIDAD	U
<input type="checkbox"/>	0008	KILOGRAMO	KG
<input type="checkbox"/>	0009	GLOBAL	GBL
<input type="checkbox"/>	0010	LIBRA	LB
<input type="checkbox"/>	0011	CAJON	CA

Figura 4.54 Edición de una unidad de medida.

Mediante el botón Nuevo pueden crearse nuevas unidades



**ECUACONTROL**  
No esta seleccionada ninguna empresa.  
[UNIDADES DE MEDIDA]

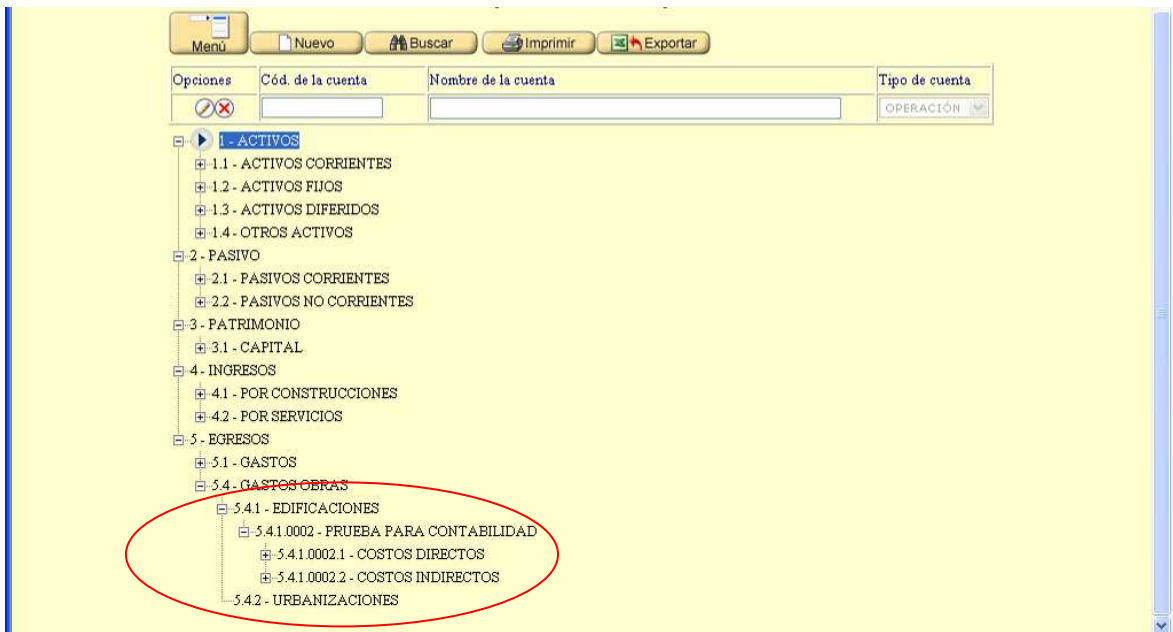
* /	Cod. Unidad	Nombre	Sigla
✓	0001	SACO	SC
✓	0002	GALON	GLN
✓	0003	METRO	M
✓	0004	METRO LINEAL	ML
✓	0005	METRO CUADRADO	M2
✓	0006	METRO CUBICO	M3
✓	0007	UNIDAD	U
✓	0008	KILOGRAMO	KG
✓	0009	GLOBAL	OBL
✓	0010	LIBRA	LB
✓	0011	CAJON	CA
✓	0012	KILOMETRO	KM

Figura 4.55 Agregación de “Kilómetro” dentro de las unidades.

#### 4.5.9.2 Creación automática de cuentas contables el licitar una obra.

Se indica en la siguiente figura un fragmento del plan de cuentas del sistema de contabilidad. Este plan se organiza en una estructura de árbol.

La empresa constructora clasifica sus obras en dos tipos: edificación y urbanización. Los códigos de sus cuentas contables respectivamente son: 5.1.4 y 5.4.2.



Opciones	Cód. de la cuenta	Nombre de la cuenta	Tipo de cuenta
1 - ACTIVOS			OPERACIÓN
1.1 - ACTIVOS CORRIENTES			
1.2 - ACTIVOS FIJOS			
1.3 - ACTIVOS DIFERIDOS			
1.4 - OTROS ACTIVOS			
2 - PASIVO			
2.1 - PASIVOS CORRIENTES			
2.2 - PASIVOS NO CORRIENTES			
3 - PATRIMONIO			
3.1 - CAPITAL			
4 - INGRESOS			
4.1 - POR CONSTRUCCIONES			
4.2 - POR SERVICIOS			
5 - EGRESOS			
5.1 - GASTOS			
5.4 - GASTOS OBRAS			
5.4.1 - EDIFICACIONES			
5.4.1.0002 - PRUEBA PARA CONTABILIDAD			
5.4.1.0002.1 - COSTOS DIRECTOS			
5.4.1.0002.2 - COSTOS INDIRECTOS			
5.4.2 - URBANIZACIONES			

Figura 4.56. Organización del plan de cuentas utilizado en el sistema contable.

Se puede observar que existe una sola cuenta dentro del grupo de edificaciones. A continuación se creará una obra nueva, se la licitará<sup>33</sup> y podrá observarse la inclusión automática de esta obra dentro del grupo de edificaciones.

El nombre de la obra a crearse es *SEGUNDA PRUEBA*.

En la siguiente figura se resalta la sección donde se elije el tipo, en este caso es *Edificación*.

Menú

[ OBRA - MANTENIMIENTO ]

Generales Costos Indirectos Comparación Parámetros

Nuevo Grabar

Código:  Campos Requeridos=\*

Nombre de Obra:

Descripción:

Cliente:

Dirección:

Ciudad:

Contratista:

Especificaciones:

Area de Construcción:  Licitación:

Plazo:

Creada:

Tipo Obra:

Actualizada:

Estado:

Fechas de la Obra

Presentación Licitación \* Inicio  Terminación

Figura 4.57. Creación de una nueva obra del tipo *Edificación*.

Para licitar la obra, se la debe seleccionar de un listado de obras que poseen únicamente el presupuesto licitatorio. La licitación se ejecuta mediante el botón *Aprobar*.

<sup>33</sup> Cambio de estado aplicado a una obra cuando la misma ha ganado el concurso de licitación.





Figura 4.58. Licitación de la obra.

La obra se encuentra dentro del grupo *Edificaciones*, con el código 5.4.1.007. De manera automática se crean las cuentas contables subordinadas requeridas para esta obra.

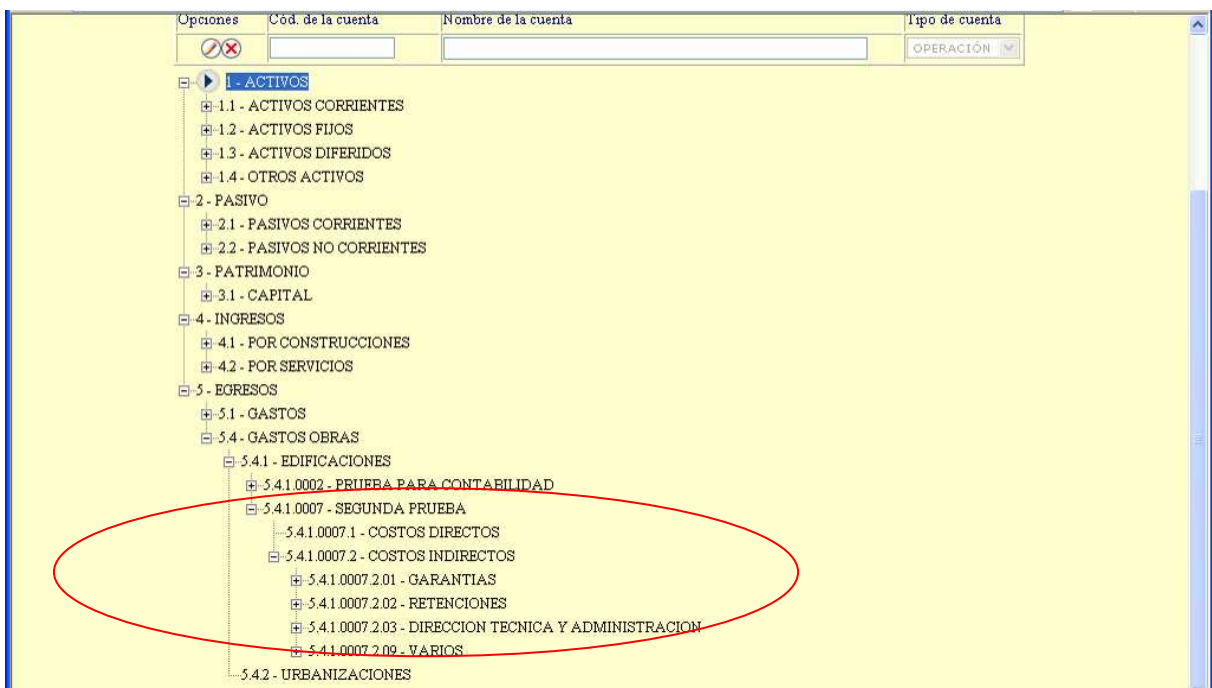


Figura 4.59. Creación automática de cuentas contables de una obra.

## **CAPITULO V**

### **5 CONCLUSIONES Y RECOMENDACIONES.**

#### **5.1 CONCLUSIONES**

La principal brecha de seguridad, aunque no lo parezca, es el propio recurso humano de la empresa, no solamente por una falta de conciencia en cuanto a seguridad informática sino también por falta de capacitación para la ejecución de sus tareas laborales.

En la implantación de cualquier esquema de seguridad informática se requiere la concientización y participación de todo el personal, especialmente del área directiva, ya que es responsabilidad de todos el lograr implantarla con éxito y mantenerla en el tiempo.

La concientización de todo el personal de una organización en temas de seguridad informática se la consigue por medio del entrenamiento en este tipo de temas y su comprometimiento al respecto.

La idea detrás de la implantación de cualquier esquema de seguridad consiste en alcanzar el mayor nivel de seguridad posible y evitar afectar o alterar los procesos empresariales; debe emplearse el adecuado equilibrio entre estos dos aspectos.

Es importante que todos los empleados de la empresa tomen conciencia sobre el manejo seguro de la información, ya que resulta inútil cualquier sistema de seguridad por complejo y completo que este sea, si los empleados, por ejemplo, facilitan su nombre de usuario y contraseña a otras personas y con esto dejan abierta la posibilidad de ataques o robo de información crítica de la empresa.

Mientras la edad del personal aumentaba, su experiencia o conocimiento en el manejo de los recursos informáticos iba en descenso.

No hubo resistencia por parte del personal a los cambios implantados producto del presente trabajo, por ejemplo, todo usuario se acopló inmediatamente al estilo de trabajo típico de un dominio.

Debido a que el acceso a la nueva aplicación de control de presupuestos y contabilidad se maneja mediante perfiles de usuarios, el área directiva de la empresa, subcontratistas de la empresa constructora y el dueño de la obra pueden revisar y constatar el avance cotidiano de la construcción de las obras desde cualquier lugar y a cualquier hora.

Ya que esta nueva aplicación es accesible vía web, así como el servicio de correo electrónico, no se requieren de estaciones de trabajo nuevas para su uso, permitiendo de este modo la utilización de las estaciones de trabajo anteriormente usadas en la oficina central (ver tabla 2.1) en las diferentes obras en construcción, concretándose de esta manera un ahorro para la empresa constructora.

La nueva aplicación antes mencionada permite contar con reportes actualizados y en línea de valores gastados y presupuestados, así como de otros temas relacionados a la construcción de una obra, lo que representa para el área directiva de la empresa constructora un valor añadido que aporta calidad y agilidad para una oportuna toma de decisiones.

La implantación del enlace VPN permanente con la empresa de asistencia técnica constituye una inversión clave cuyo beneficio representa asistencia técnica inmediata, disminuyendo el tiempo de inactividad de un determinado recurso informático que un desperfecto o daño pueda provocar.

El enlace VPN, además, permite que la empresa constructora enfoque todos sus esfuerzos en sus actividades de razón de ser, es decir, la construcción de obras civiles.

La segregación de usuarios que pueden acceder a Internet y la capacitación brindada en este tema, disminuyó considerablemente la incidencia de código malicioso en la intranet de la compañía.

El rediseño aplicado a la infraestructura existente permite la extensión de los servicios de asistencia técnica remota a las obras en construcción.

La infraestructura rediseñada es la base fundamental de apoyo de la nueva aplicación de presupuestos y contabilidad, para de esta manera poder contar con información actualizada del avance de una obra y comunicaciones permanentes con las obras en construcción mediante el servicio de correo electrónico.

## **5.2 RECOMENDACIONES**

Es necesario implantar un proceso de evaluación periódica de la seguridad informática para aplicar los cambios pertinentes, ya que con el avance del tiempo y de la tecnología, amenazas y vulnerabilidades cambiarán o aparecerán otras

En una próxima evaluación de la seguridad informática en la empresa constructora debe tomarse en cuenta la seguridad física de las instalaciones, del equipo informático y el recurso humano, no solamente las manifestaciones climáticas sino también acciones humanas perjudiciales.

En futuras evaluaciones del ambiente de seguridad informática, realizar un plan de contingencias, el cual resultará de utilidad para mejorar el tiempo y calidad de la respuesta ante daños ocasionados en los recursos informáticos.

Todo el personal debe conocer el contenido de las políticas, normas y procedimientos de seguridad, para normar el manejo que haga de los recursos informáticos y así evitar incidentes de seguridad.

En futuras evaluaciones del ambiente de seguridad informática incluir sanciones a aplicarse a quienes, sabiendo las políticas, normas y procedimientos de seguridad, no las utilicen en forma permanente.

Debido a que el único punto de separación entre la red corporativa y el mundo exterior lo constituye el servidor cortafuegos se lo debe monitorear semanalmente para realizar ajustes a las reglas de filtrado.

En futuras evaluaciones del ambiente de seguridad informática y conforme los recursos y la tecnología lo permitan, tomar en cuenta servicios de video conferencia y la posibilidad de extender el acceso a las aplicaciones corporativas a dispositivos móviles.

La empresa de asistencia técnica debe mantener a su personal en permanente actualización y entrenamiento en nuevas tecnologías, para ofrecer no solamente servicios de mejor calidad, sino también mejores y nuevas medidas de seguridad.

La empresa constructora también deberá mantener a su personal entrenado en el uso de nuevas tecnologías que se vayan incorporando con el paso del tiempo, para evitar brechas de seguridad.

Para mejorar la seguridad en los computadores debería instalarse software antispyware que implemente agentes de revisión permanente.

## **BIBLIOGRAFIA**

### **LIBROS Y MANUALES**

- ANONIMO. Microsoft Oficial Curriculum - Managing a Microsoft Windows 2000 Network Environment. 2daEd. USA. 2002.
- ANONIMO. Paso a Paso Microsoft Office Outlook 2003. 1eraEd. España McGraw-Hill. 2004.
- CORNER, Douglas. Redes de computadores, Internet e interredes. 1eraEd. Mexico. Prentice-Hall. 1997.
- PELTIER, Thomas. Effective Risk Analysis. 1eraEd. USA. Auerbach Publications. 2001.
- TOIGO, John. Disaster Recovery Planning Preparing for the Unthinkable. 3eraEd. USA. Prentice-Hall. 2003.

### **TESIS**

- CARRANZA, Ruperto; GUTIERREZ Luis. Políticas y estrategias de seguridad para la intranet de Petroecuador matriz. Septiembre 2004.
- HERNANDEZ Wilman; ORTIZ Efraín. Análisis y diseño de la infraestructura de un proveedor de servicios de Internet (ISP) para la provincia de Orellana. Noviembre 2003.

## E-BOOKS Y PAPERS

- ACADEMIA LATINOAMERICANA DE SEGURIDAD INFORMÁTICA. Modulo 1. 2005.
- ANONIMO. Seguridad. Sin año.
- GARCIA, Lledó. Seguridad en redes IP. Sin año.
- HERRERA, Juan. E-Business. Presentaciones de guías pedagógicas de la materia. 2004.
- HERRERA, Juan. Intranets – Extranets Presentaciones de guías pedagógicas de la materia. 2004.
- VILLALON, Antonio. Seguridad en Unix y Redes v2.1. 2002.

## DIRECCIONES ELECTRONICAS

- CARDENAS, Claudia. Indice de Seguridad en Tecnologías de Información. <http://www.monografias.com/trabajos16/tecnologias-informacion/tecnologias-informacion.shtml>. 2004.
- HEVIA, Mariano. Virtual Private Networks. <http://www.monografias.com/trabajos12/monvpn/monvpn.shtml>. 2003.
- KRASNYANSKY, Maxim. VTun - Virtual Tunnels over TCP/IP networks. <http://vtun.sourceforge.net>. 2003.
- MARTINEZ, Matías. Intranet. <http://www.monografias.com/trabajos16/intranet-o-internet/intranet-o-internet.shtml>. 2005.

- MICROSOFT. Internet Explorer 6 Service Pack 1.  
<http://www.microsoft.com/downloads/details.aspx?displaylang=es&FamilyID=1E1550CB-5E5D-48F5-B02B-20B602228DE6>. 2005.
- MICROSOFT. Requisitos del sistema para Outlook 2003.  
<http://www.microsoft.com/spain/office/products/outlook/sysreq.mspx>. 2005.
- NATIONAL CYBER SECURITY ALLIANCE. Top 8 Cyber Security Practices.  
<http://www.staysafeonline.info/practices/five.html>. 2005.
- UNIVERSIDAD DE VALENCIA. Red Privada Virtual.  
<http://www.uv.es/ciuv/cas/zxarxa/vpn.htm>. 2002.



## GLOSARIO

### **Antivirus.**

Son aplicaciones que pueden determinar cuándo un sistema ha sido infectado con un virus. Típicamente se ejecuta en segundo plano y revisa archivos siempre que sean descargados de Internet, recibidos como anexos en mensajes de correo electrónico, o modificados por otra aplicación que se ejecute en el sistema.

### **Clave o Contraseña.**

Palabra o frase que permite acceder a un sistema, encriptar información, determinar privilegios de usuario, etc.

### **Código Malicioso.**

Código desarrollado con el propósito de provocar daño al software o datos.

### **Cortafuegos o Firewall.**

Un cortafuegos es un mecanismo que sirve para controlar el flujo de tráfico IP entre dos redes. Los dispositivos cortafuegos funcionan habitualmente en el nivel 3 del modelo OSI, aunque algunos modelos también pueden funcionar a niveles superiores.

### **Encriptación de Clave Privada.**

Método de encriptación en el cual se emplea una sola clave para encriptar como para desencriptar.

### **Encriptación de Clave Pública.**

Método de encriptación en el cual se emplean dos claves, matemáticamente relacionadas, para encriptar como para desencriptar estableciendo lo siguiente: lo que la una encripta, la otra desencripta.

**Encriptar.**

Proceso para transformar información de modo que resulte inentendible a todos quienes puedan leerla con excepción de los verdaderos receptores quienes pueden desencriptarla.

**Desencriptar.**

Proceso de transformación de la información encriptada en información legible.

**Host.**

Cualquier dispositivo en una red TCP/IP que posea un número IP.

**ISP.**

(Internet Service Provider, Proveedor de servicios de Internet). Empresa que proporciona acceso servicios de Internet, como navegación, e-mail, ftp, chat, news, grupos de discusión, etc.

**Kbps.**

(Kilobits por segundo)

Unidad de medida de velocidad de transmisión.

**Mainframe.**

Término general para designar a grandes computadores de alto nivel que son capaces de realizar tareas computacionales demandantes.

**Navegador.**

Es un programa software que permite ver e interactuar con varios tipos de recursos de Internet disponibles en el World Wide Web.

**Número IP.**

Número que identifica de manera única una máquina dentro de la red que utiliza el protocolo IP.

**Presupuesto Detallado Inicial.**

Presupuesto preparado tras haberse ganado la licitación de una obra determinada. Consiste en añadir detalle al presupuesto licitatorio.

**Presupuesto Licitatorio.**

Presupuesto preparado para concursar en la licitación de una obra determinada. No lleva demasiado detalle.

**TCP/IP.**

(Transmission Control Protocol / Internet Protocol, Protocolo de control de transmisiones /Protocolo de Internet). Protocolos de red que identifican y definen a Internet. Aunque en su origen fue diseñado para UNIX, el software TCP/IP se encuentra ya disponible para los sistemas operativos más importantes.

**Rubro.**

Componente o fase a seguirse en una obra en construcción.

**Spyware.**

Tipo de código malicioso que se instala a sí mismo con el propósito de recolectar información personal sin el consentimiento del usuario y enviarla a través de Internet a su creador.

**SSL.**

(Secure Sockets Layer, Nivel de Sockets Seguro). Protocolo de seguridad para Internet e intranets que permite mantener la confidencialidad en las comunicaciones.

**Tunneling.**

Método de transporte de paquetes de un protocolo de red sobre otro protocolo de red diferente.

**Virus.**

Son programas que se autorepican y afectan principalmente los archivos ejecutables, a veces llegan a afectar a miles de computadoras.

**VNC.**

(Virtual Network Computing, Computación de Red Virtual)

Consola de administración remota desarrollada por AT&T utilizada para acceder remotamente a otras computadoras.

**VPN.**

(Virtual Private Network, Red Privada Virtual). Es un método para establecer conexiones de acceso remoto seguras sobre una insegura red pública de transporte, por ejemplo, Internet.

## ANEXO A - MATRIZ DE RIESGO

Esta técnica de análisis de riesgos, propuesta por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST por sus siglas en inglés), está compuesta por tres fases:

Primeramente se calcula el impacto de las amenazas sobre los activos.

El impacto permite determinar las consecuencias adversas que se obtienen como resultado de la ejecución exitosa de una amenaza al aprovechar una vulnerabilidad.

El impacto es evaluado cualitativamente en tres niveles: ALTO, MEDIO y BAJO. De esta manera, cada activo tiene una valoración de nivel de impacto por cada amenaza.

En la siguiente tabla se explican estos niveles de impacto.

Impacto	Definición
ALTO	La ejecución de la amenaza puede resultar en costos altos, pérdidas de activos tangibles y recursos, puede ocasionar violación, daños o impedir la misión de la organización, su reputación, intereses ; puede causar muertes o personas heridas.
MEDIO	La ejecución de la amenaza puede resultar en costos, pérdidas de activos tangibles o recursos; puede violar, dañar o impedir la misión de la organización, su reputación o interés; pueden resultar personas heridas.
BAJO	La ejecución de la amenaza puede resultar en costos bajos de activos tangibles o recursos, pueden afectar de alguna forma la misión de la organización su reputación o intereses.

Tabla A1. Definición de niveles de impacto.

En segundo lugar se calcula la probabilidad de ocurrencia de la amenaza sobre los activos.

Esta probabilidad es evaluada cualitativamente en tres niveles: ALTA, MEDIA y BAJA. De esta manera, cada activo tiene una valoración de probabilidad de ocurrencia de amenaza por cada amenaza.

En la siguiente tabla se explican estos niveles de probabilidad.

<b>Probabilidad</b>	<b>Definición</b>
Alto	El origen de la amenaza es alto, y los controles para prevenir la vulnerabilidad por el momento son ineficientes o no los hay.
Medio	El origen de las amenaza esta presente, pero los controles pueden impedir que las amenazas afecten realmente a la empresa.
Bajo	El origen de las amenazas pueden presentarse, pero existen controles que impiden que la amenaza afecte realmente a la empresa.

Tabla A2. Definición de probabilidad de ocurrencia de amenazas.

En tercer lugar se calcula el nivel de riesgo, el cual se obtiene al multiplicar los valores de cada celda de la matriz de impacto con el valor de la celda correspondiente en la matriz de probabilidad de ocurrencia de la amenaza.

Para lograr este cálculo se asignan cantidades a estos valores.

La siguiente tabla indica esta asignación de cantidades y la manera de obtener el resultado.

<b>Probabilidad de la Amenaza</b>	<b>Impacto</b>		
	<b>Bajo (10)</b>	<b>Medio (50)</b>	<b>Alto (100)</b>
<b>Alto (1.0)</b>	$10 * 1.0 = 10$	$50 * 1.0 = 50$	$100 * 1.0 = 100$
<b>Medio (0.5)</b>	$10 * 0.5 = 5$	$50 * 0.5 = 25$	$100 * 0.5 = 50$
<b>Bajo (0.1)</b>	$10 * 0.1 = 1$	$50 * 0.1 = 5$	$100 * 0.1 = 10$

Tabla A3. Matriz de nivel de riesgo.

Las cantidades obtenidas se las transforma a valores cualitativos de acuerdo a la siguiente tabla.

Nivel de riesgo	Definición
Alto	Si se encuentra entre 50 y 100 de acuerdo a los resultados de la matriz de riesgo. Si una observación es evaluada como de alto riesgo, existe una necesidad grande de tomar medidas correctivas. El sistema como tal puede seguir adelante, pero se debe tomar acciones correctivas para ser puestas en práctica tan pronto como sea posible.
Medio	Si se encuentra entre 10 y 50 de acuerdo a los resultados de la matriz de riesgo. Si una observación es evaluada como de riesgo medio, acciones correctivas son necesarias y un plan debe ser desarrollado para integrar estas acciones dentro de un período de tiempo razonable.
Bajo	Si se encuentra entre 1 y 10 de acuerdo a los resultados de la matriz de riesgo. Si una observación es evaluada como de riesgo bajo, el jefe, el personal y los directores deben decidir si acciones correctivas son necesarias o si se decide aceptar el riesgo.

Tabla A4. Definición de nivel de riesgo.

## ANEXO B - DIAGRAMA DE LA NUEVA RED

Tras la aplicación de políticas, normas y procedimientos, el esquema de la nueva red es el siguiente:

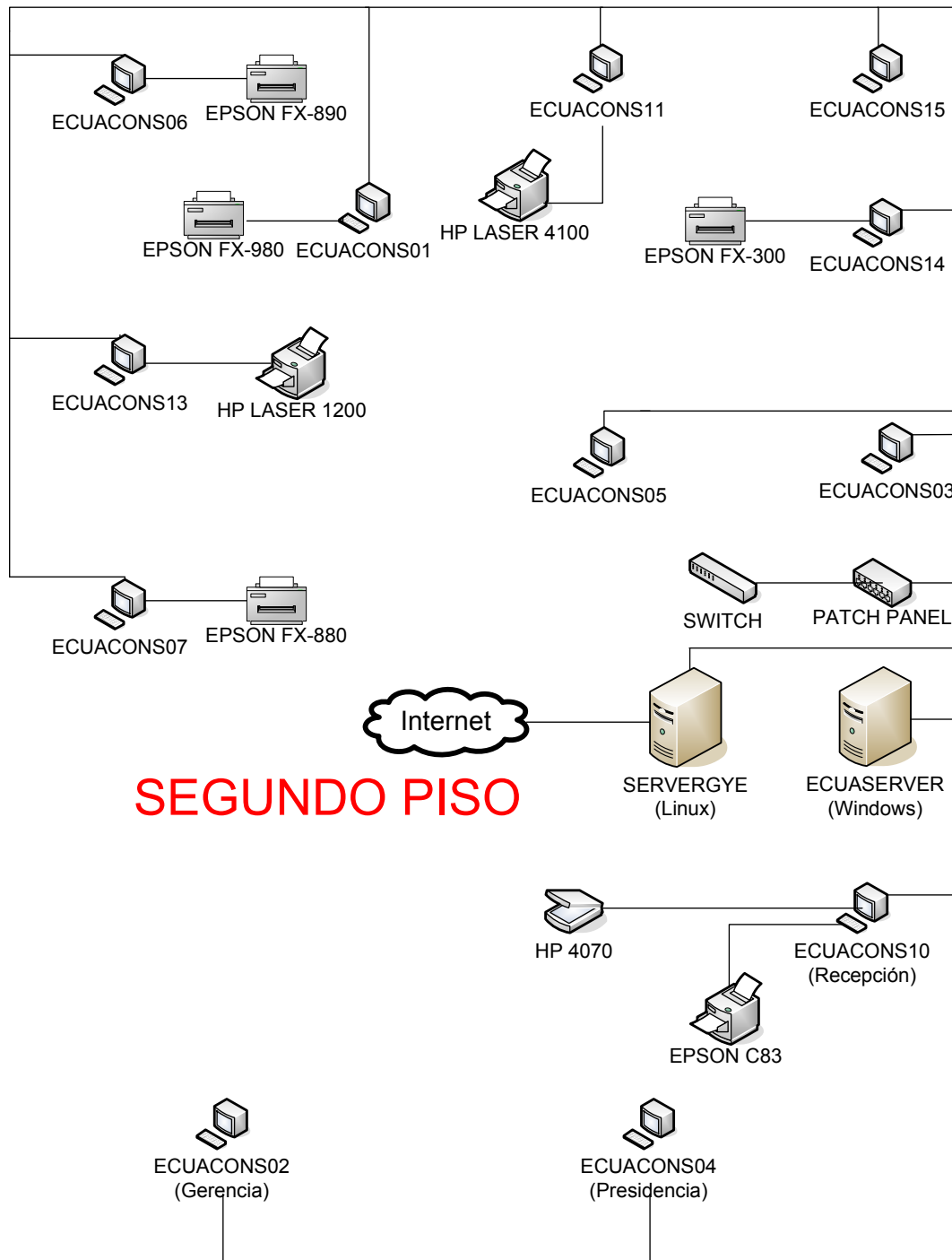


Figura B1. Diagrama de la nueva red – segundo piso.



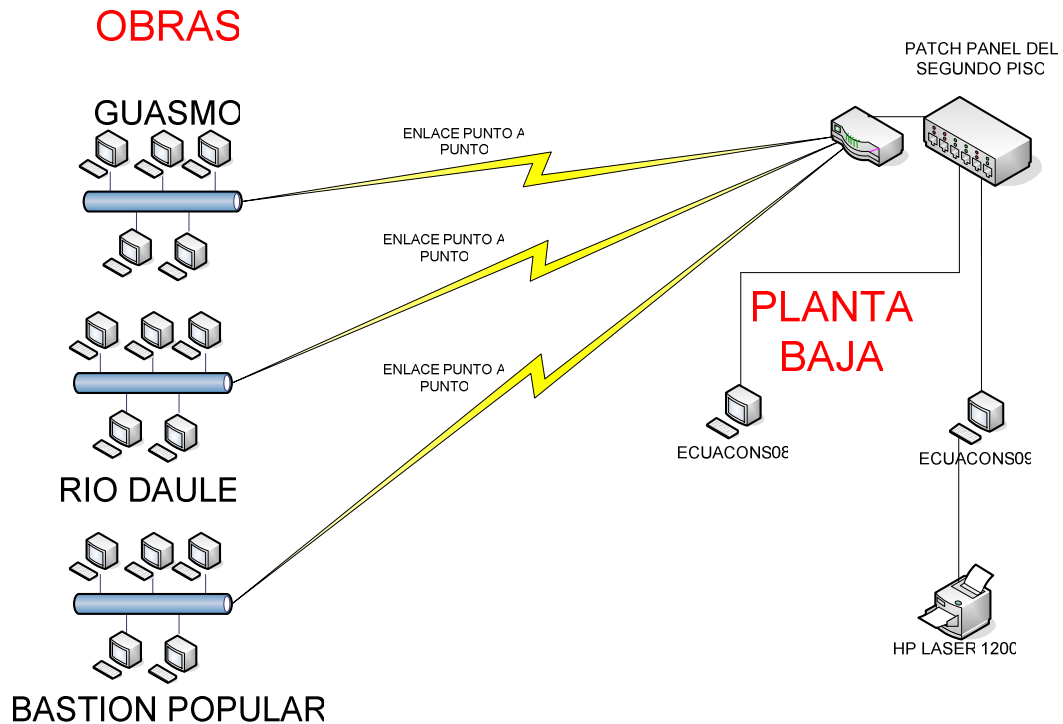


Figura B2. Diagrama de la nueva red – planta baja.

Los servidores son los siguientes:

- **SERVERGYE:** Es el servidor cortafuegos, servidor VPN, servidor de correo electrónico. El enlace SDSL a Internet se encuentra configurado en este servidor. Su sistema operativo es Red Hat v9.0.
- **ECUASERVER:** Es el servidor controlador de dominio, servidor de archivos.

## ANEXO C - ARCHIVO DE CONFIGURACION DEL ENLACE VPN

En el sitio oficial<sup>34</sup> de la aplicación empleada para implantar este enlace se encuentra un ejemplo del archivo de configuración, disponible para ser descargado. El nombre de esta aplicación es VTUN.

A continuación se incluye el contenido de este archivo utilizado para la implantación del enlace VPN permanente entre la empresa constructora y la empresa de asistencia técnica.

Para el componente servidor de esta aplicación se empleó la siguiente configuración:

```
options {
    port 5000;

    syslog    daemon;

    ppp       /usr/sbin/pppd;
    ifconfig  /sbin/ifconfig;
    route     /sbin/route;
    firewall  /sbin/ipchains;
    ip        /sbin/ip;
}

default {
    compress no;
    speed 0;
}
```

---

<sup>34</sup> <http://vtun.sourceforge.net/>

```

TUN0 {
    pass palosanto;
    type tun;
    prot udp;
    comp lzo:9;
    encr yes;
    keepalive yes;

    up {
        ifconfig "%% 10.0.0.1 pointopoint 10.0.0.2 mtu 1450";
        route "add -net 200.105.238.0 netmask 255.255.255.0 gw 10.0.0.2";
    };
}

```

Las secciones *options* y *default* no deben cambiarse ya que son las configuraciones por defecto de la aplicación.

La sección *TUN0* es la que debe ser modificada y su nombre puede ser arbitrario. *TUN0* es el nombre que la aplicación asigna a un túnel virtual específico.

Dentro de *TUN*: tenemos los siguientes componentes:

- *pass*: el password utilizado para encriptación del tráfico.
- *type*: el tipo de túnel a implantar; *tun* especifica que el túnel es IP.
- *prot*: el tipo de protocolo utilizado para implantar el túnel.
- *comp*: el algoritmo de compresión utilizado y el nivel de compresión aplicado.
- *encr*: si se utilizará o no encriptación.
- *keepalive*: si se creará automáticamente el túnel cuando el enlace caiga.

Dentro de la sección *up* los números 10.0.0.1 y 10.0.0.2 son los números IP asignados a los dispositivos virtuales de red punto a punto en el servidor y

cliente VPN respectivamente. El número IP de red 200.105.238.0 identifica la red en la cual se encuentra el número IP real asignado por el ISP al cliente VPN.

Para el componente cliente de esta aplicación se empleó la siguiente configuración:

```
options {  
    port 5000;  
  
    syslog    daemon;  
  
    ppp      /usr/sbin/pppd;  
    ifconfig /sbin/ifconfig;  
    route    /sbin/route;  
    firewall /sbin/ipchains;  
    ip       /sbin/ip;  
}  
  
default {  
    compress no;  
    speed 0;  
}  
  
TUN0 {  
    pass palosanto;  
    type tun;  
    prot udp;  
    comp lzo:9;  
    encr yes;  
    keepalive yes;
```

```
up {  
    ifconfig "%% 10.0.0.2 pointopoint 10.0.0.1 mtu 1450";  
    route "add -net 200.105.237.0 netmask 255.255.255.0 gw 10.0.0.1";  
};  
}
```

Como podrá observarse, el único cambio ocurrió en el contenido de la sección *up* dentro de la sección *TUN0*, donde las rutas fueron intercambiadas.

El servidor es iniciado con el siguiente comando:

```
vtund - s
```

El cliente es iniciado con el siguiente comando:

```
vtund - c TUN0 200.105.237.63
```

donde 200.105.237.63 es el número IP real asignado por el ISP al servidor VPN.

## ANEXO D - CONFIGURACION DE POLITICAS DE CONTRASEÑAS Y BLOQUEO DE CUENTAS DE USUARIO

### POLITICAS DE CONTRASEÑAS.

1. Abrir *Active Directory Users and Computers*

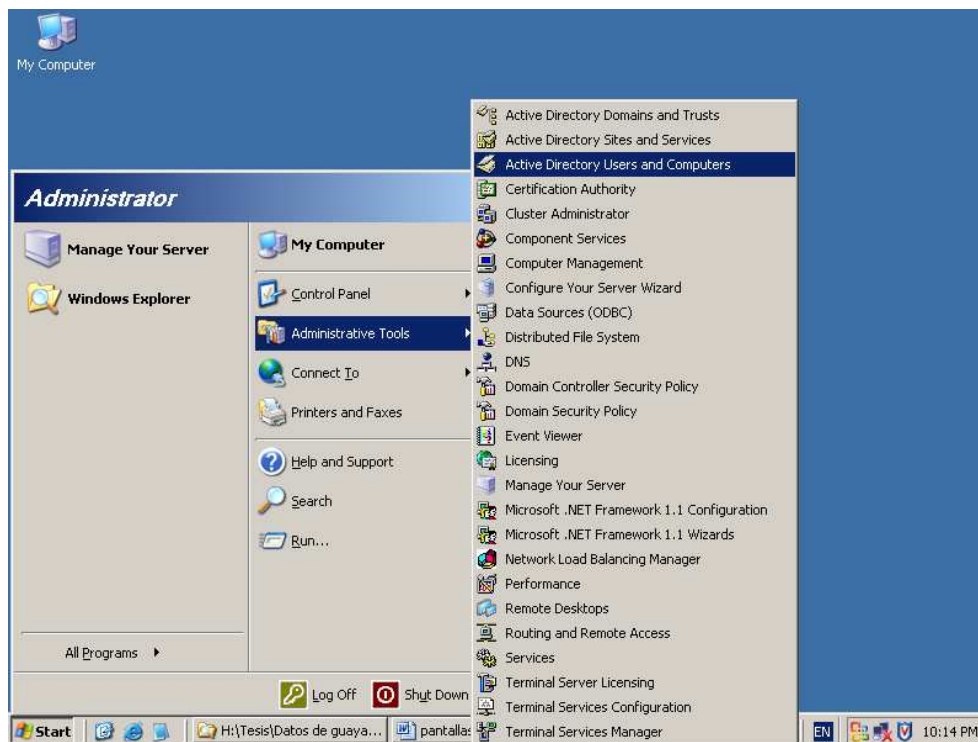


Figura D1. Seleccionar *Active Directory Users and Computers*.

Accesar a las propiedades del dominio, que en este caso lleva por nombre *ecuacons.int*.

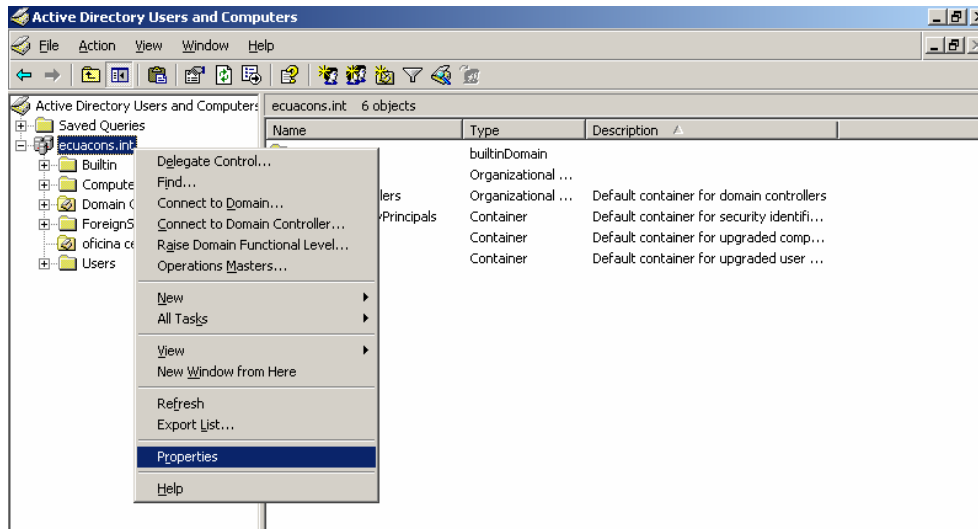


Figura D2. Acceso a las propiedades del dominio.

2. En la pestaña *Group Policy* hacer clic sobre el botón *Edit*.

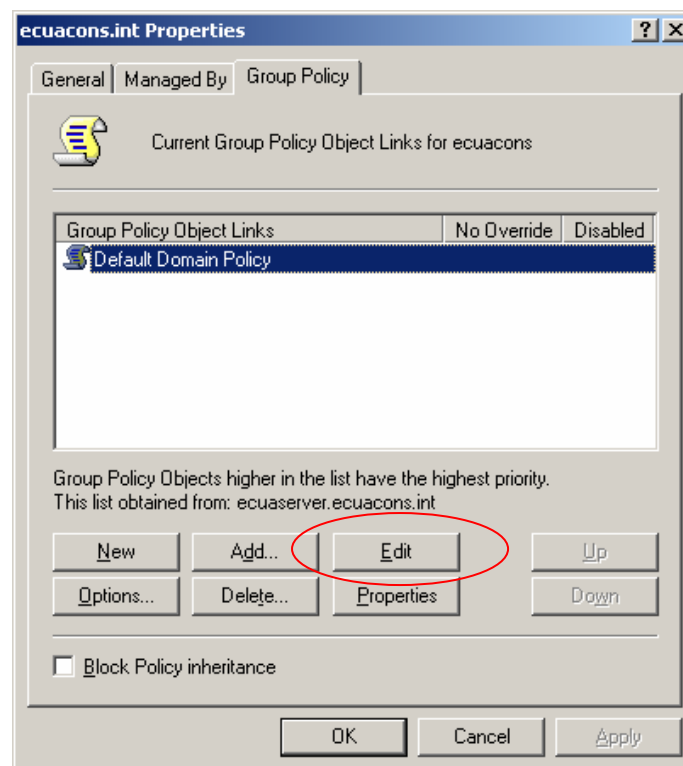


Figura D3. Edición de la política de dominio por defecto.

3. En la siguiente ventana dirigirse a *Computer Configuration, Windows Settings, Security Settings, Account Policies*

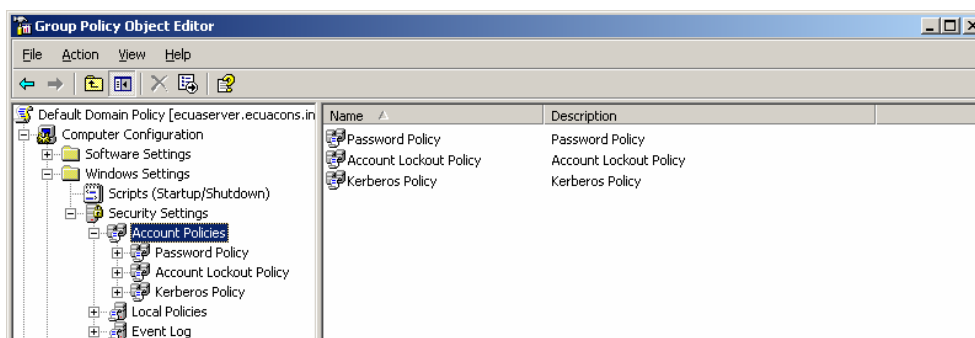


Figura D4. Acceso a las políticas de cuentas de usuario.

Dentro de *Password Policy* se configurará lo siguiente conforme a lo estipulado en las políticas de contraseñas del capítulo 3:

- El período de validez de una contraseña es de 90 días.
- Al ingresar una nueva contraseña, el sistema verificará que sea diferente a las tres últimas contraseñas utilizadas.
- El tamaño mínimo de la contraseña será de 8 dígitos.
- La contraseña debe contener al menos un carácter de tres de los siguientes grupos de caracteres:
  - Letras minúsculas
  - Letras mayúsculas
  - Dígitos
  - Caracteres especiales, por ejemplo: @, ¡, %, \$, etc.
- No emplear el mismo identificador de la cuenta de usuario.

Las siguientes políticas, incluidas en el capítulo 3, no las implementa el sistema operativo sino que las debe tomar en cuenta el usuario.

- No emplear fechas de nacimiento propia o de personas conocidas.
- No emplear palabras que se encuentren en el diccionario, ni siquiera escritas en sentido inverso.



Las políticas por defecto se indican en la siguiente figura.

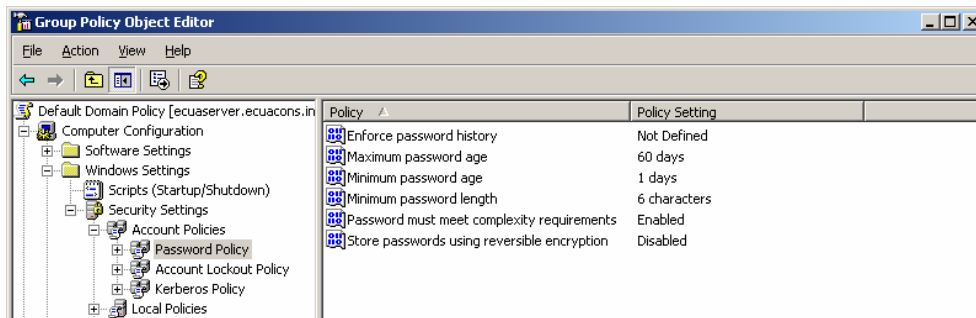


Figura D5. Valores por defecto para las políticas de contraseñas.

4. Cuando una contraseña se cambie, para evitar que sea la misma que las 3 anteriores contraseñas, se utiliza la política *Enforce Password History*.

Abrir la ventana de propiedades de la política haciendo doble clic sobre la misma, seleccionar *Define this policy setting* y colocar el valor 3 en la sección *Keep password history for*



Figura D6. Número de contraseñas recordadas.

5. En la política *Minimum password age* se establece el período de duración de una contraseña.

Colocar el valor 89 en la sección *Password can be changed after*



Figura D7. Período mínimo de validez.

Al presionar OK aparecerá la siguiente pantalla

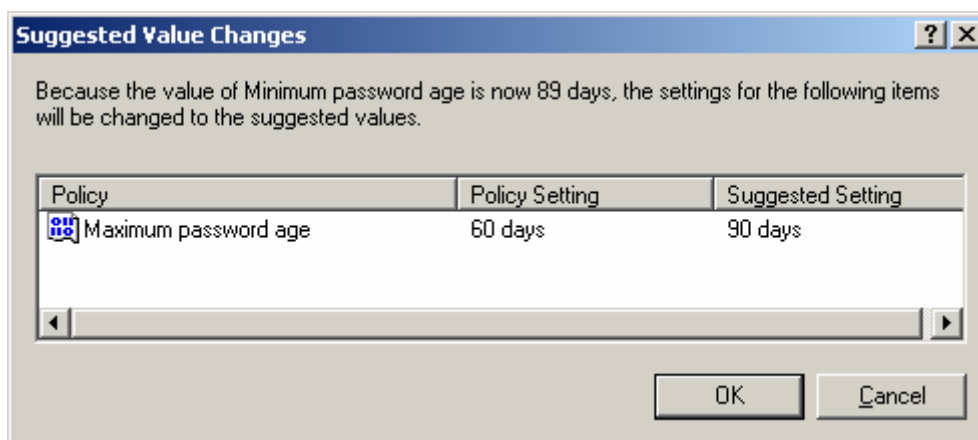


Figura D8. Configuración automática de la política *Maximum password age*.

La cual especifica que la política *Maximum password age* tendrá el valor de 90 días. Presionamos OK para aceptar.

De esta forma, un usuario podrá cambiar opcionalmente su contraseña a los 89 días pero deberá cambiarla obligatoriamente a los 90 días, tal como especifica la política de seguridad al respecto.

6. Con la política *Minimum password length* se establece la longitud mínima que debe poseer la contraseña

Colocar el valor 8 en la sección *password must be at least*.

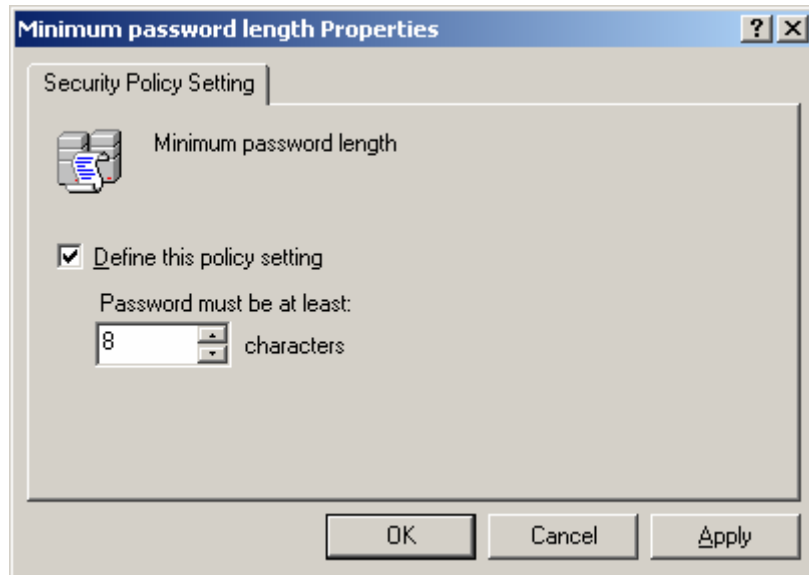


Figura D9. Longitud mínima de la contraseña

7. Con la política *password must meet complexity requirements* se establecen los requerimientos de complejidad, los cuales podemos obtener al dar clic derecho sobre la política y seleccionar Help

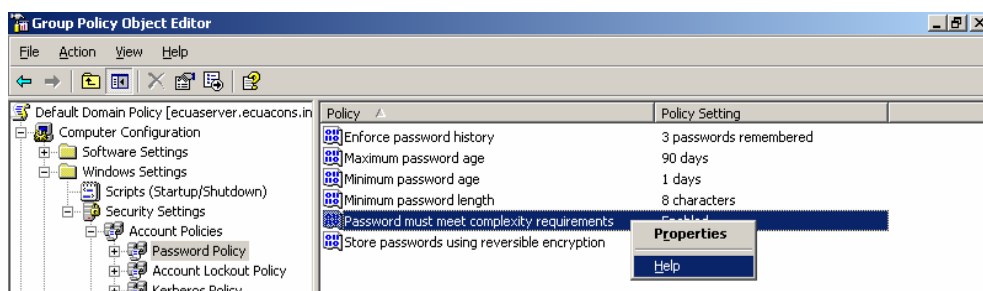


Figura D10. Obtener el contenido de los requerimientos de seguridad

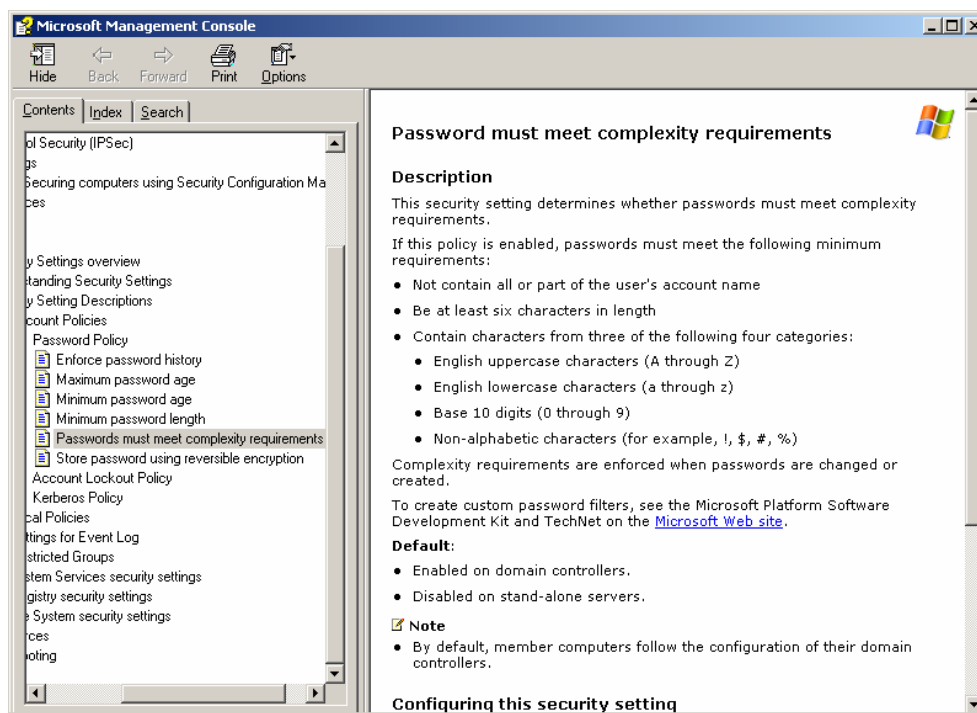


Figura D11. Detalle de la especificación de requerimientos de complejidad.

Los requerimientos de complejidad que implementa esta política son:

- El tamaño mínimo de la contraseña será de 8 dígitos.
- La contraseña debe contener al menos un carácter de tres de los siguientes grupos de caracteres:
  - Letras minúsculas
  - Letras mayúsculas
  - Dígitos
  - Caracteres especiales, por ejemplo: @, ¡, %, \$, etc.
- No emplear el mismo identificador de la cuenta de usuario.

Cabe recalcar que aunque esta política establezca que la longitud de la contraseña sea por lo menos de 6 caracteres, la política *Minimum password length* (la política anterior) tiene prioridad.

La política *password must meet complexity requirements* ya se encuentra habilitada por defecto.

## POLITICAS DE BLOQUEO DE CUENTAS DE USUARIO.

1. En el panel izquierdo seleccionar *Account Lockout Policy*

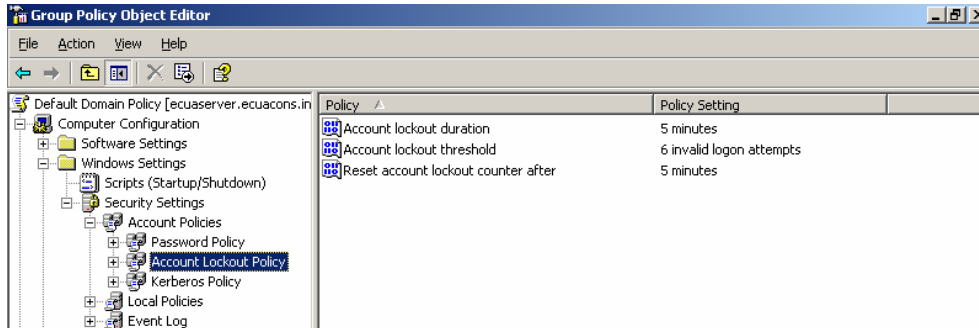


Figura D12. Políticas de bloqueo de cuentas.

2. En la política *Account lockout threshold* se establecerá el límite máximo permitido de intentos de acceso fallidos antes de que la cuenta sea bloqueada.

Abrir las propiedades de esta política y en la sección *Account will lockout after* colocar el valor 3.

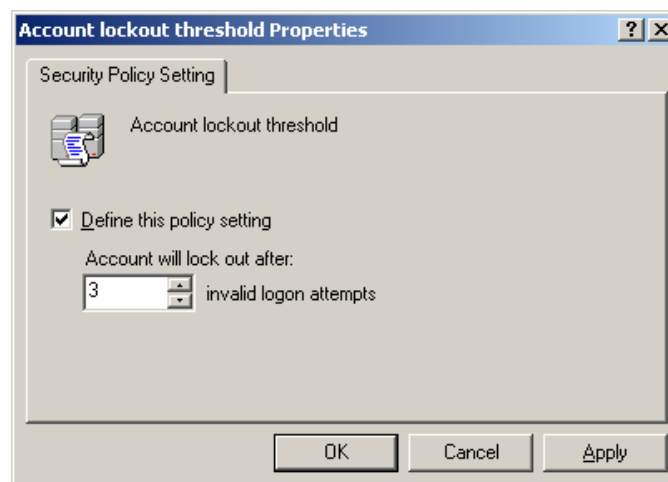


Figura D13. Número de intentos fallidos de acceso.

3. En la política *Account lockout duration* puede observarse que en la sección *Account is locked out for* se encuentra el tiempo en minutos que la cuenta permanecerá deshabilitada tras superarse el número máximo de intentos de acceso fallidos.

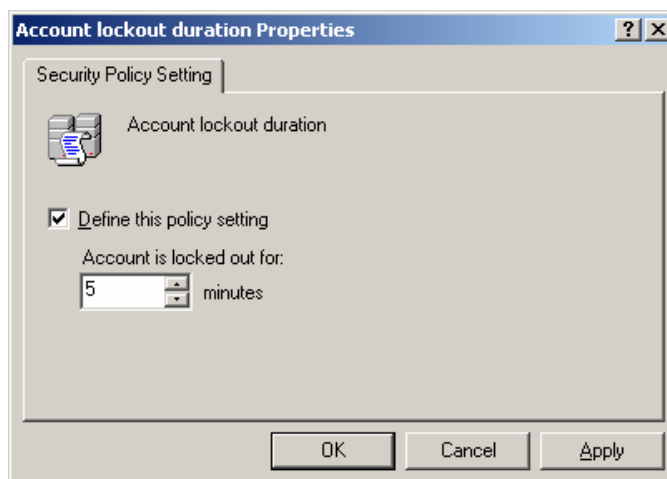


Figura D14. Tiempo durante el cual la cuenta permanecerá bloqueada.

Para cumplir con lo estipulado en las políticas de seguridad, se coloca 0 (cero), tras lo cual la sección *Account is locked out for* cambia a *Account is locked out until administrator unlocks it*.

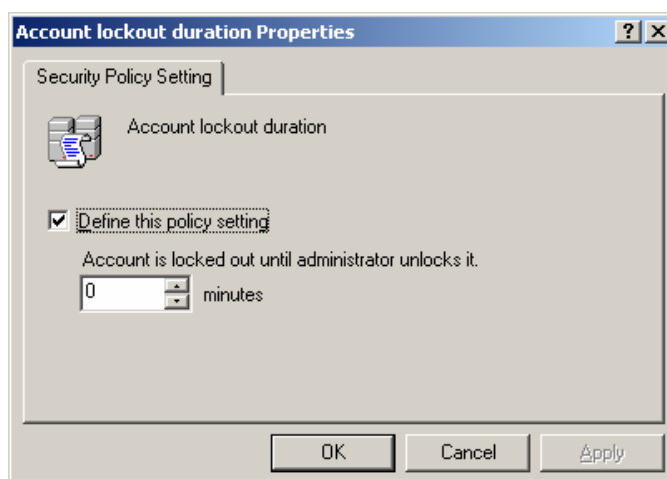


Figura D15. La cuenta permanecerá bloqueada hasta que el Administrador la desbloquee.