# ESCUELA SUPERIOR POLITECNICA DEL LITORAL


## Facultad de Ingeniería en Electricidad y Computación

"Diseño e Implementación de un Sitio Web Seguro y

Manual de Políticas de Seguridad aplicadas al Sitio"

## TESIS DE GRADO

Previa a la obtención del título de:

## LICENCIADO EN SISTEMAS DE INFORMACION

Presentado por:

Cruz del Rosario Candelario Vera

Sonnia Verónica Pinto Suárez

Grace Katiusca Viteri Guzmán

**GUAYAQUIL – ECUADOR**

**AÑO**

**2005**

# AGRADECIMIENTO

Agradecemos sinceramente a todas aquellas personas que han estado a nuestro lado brindándonos su apoyo incondicional en cada una de las etapas de esta carrera como son nuestras familias, compañeros de trabajo y amigos.

Rosario Candelario Vera

Sonnia Pinto Suarez

Grace Viteri Guzmán

# DEDICATORIA

Este trabajo significa un triunfo más en nuestras vidas y el único que ha hecho realidad este gran paso es DIOS, por lo que este proyecto va dedicado a ÈL por haber puesto en nuestro camino a todas esas personas que nos ayudaron con sus conocimientos y apoyo a culminarlo.

Rosario Candelario Vera

Sonnia Pinto Suarez

Grace Viteri Guzmán

## TRIBUNAL DE GRADUACION

Ing. Mónica Villavicencio

Coordinadora

Ing. Albert Espinal

Director de Tesis

## MIEMBROS PRINCIPALES

Ing. Jaime Lucero

Ing. Lorena Carló

## DECLARACION EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL"

Srta.Cruz del Rosario Candelario Vera

Anl. Sonnia Verónica Pinto Suárez

Anl. Grace Katiusca Viteri Guzmán

# RESUMEN

Este proyecto tiene como finalidad el desarrollo de un sitio web para esta institución y el establecimiento de seguridades ante posibles ataques a la información de la base de datos de la Comisión de Tránsito del Guayas.

Para esto se ha realizado un estudio de la situación actual que se lo detalla en el capítulo 1, se presenta antecedentes, la misión de la Comisión de Tránsito para conocer de una manera mejor su origen y para dónde se proyectan. Como lo que se desea con este trabajo es brindar un mejor servicio a toda la comunidad en los trámites más realizados disminuyendo la afluencia del público en las instalaciones de la institución, en este capítulo se detalla el procedimiento actual de trámites como la obtención de películas antisolares, cambio de propietario, denuncia por vehículo robado, consultas de pago de infracciones y de matrícula de vehículos.

Para establecer seguridad al sitio debemos conocer lo que la empresa posee en cuanto a hardware, software y políticas establecidas, en este capítulo también se presenta un diseño general de la red, los equipos y el software implementado y además las seguridades realizadas.

En el capítulo 2 se presenta una propuesta para la realización de este proyecto. Se detalla los requerimientos de hardware y software para implementar el sitio web,

tanto para la Comisión de Tránsito como para los usuarios que lo utilizarán. En este capítulo también se detallará los elementos que se les aplicará seguridad y que forman parte del sitio web.

En lo que se refiere al software en que se desarrolló el sitio es Visual .NET – ASP, de este lenguaje se explica el concepto y validación de la autenticación y autorización de los usuarios; el sistema operativo es Windows Server 2003 Standard Edition, de este se mencionan los beneficios, sus funciones principales y las diferentes ediciones y por qué se escogió Standard Edition; las seguridades que ofrece el IIS (Internet Information Services) y su evolución, esta herramienta está incluída en el sistema operativo; también incluye la definición del SSL (Secure Socket Layer), los requerimientos que se necesitan para su aplicación; con respecto a la base de datos se propone utilizar ORACLE por su gran soporte de almacenamiento de datos y la seguridad que ofrece en la protección de la información y actualmente la institución posee este manejador en sus sistemas informáticos.

Analizando la implementación del esquema de la red actual, proponemos la adición de ciertos componentes de seguridad para el sitio y por ende de toda la información de la institución, lo que causará una modificación en la estructura de la red como es la implementación de un servidor IDS (Servidor Detector de Intrusos), un servidor Revisor de Contenido, un servidor de Filtro de Correo y colocar un servidor para el

Firewall y otro para el Proxy. Y finalmente en este capítulo se muestran precios de los equipos y software que se necesitarán para la implementación de este proyecto.

En el capítulo 3 se realiza el diseño de las páginas del sitio web, se determina el estándar de cada uno de sus elementos: botones, colores y tipo de letras, banner, fondo, imágenes, etc. Se determina las opciones que tendrá el sitio y el objetivo de cada una de ellas: Historia, Misión y Visión, Leyes de Tránsito, Consulta en Línea, y Contáctenos. La opción "Consulta en Línea" tiene como objetivo brindar al usuario información acerca de sus deudas de infracciones y matrícula, e información de los trámites realizados; las demás opciones son páginas informativas. En este capítulo también se muestra el modelo entidad relación de la base de datos, el cual refleja la estructura de la información.

En el capítulo 4 se describe la configuración de cada uno de los elementos necesarios para proteger la información, estos fueron mencionados en el capítulo II. Para establecer seguridad al sitio web se debe tener instalado IIS 6.0 (Internet Information Services) o una versión mayor y tener un directorio virtual que va a contener el proyecto y para tener la confianza de que el usuario está verdaderamente usando el sitio de la institución en el IIS se configura el SSL (Secure Socket Layer) pero antes se debe certificar el sitio desde una empresa certificadora, para efectos de presentar este proyecto se consiguió en www.thawte.com un certificado de prueba. Cabe

recalcar que para emitir el certificado antes se debe tener un Domain Name (Nombre del sitio).

Con respecto a la protección de la base de datos se establece perfiles de acceso según el usuario, en este caso se establece a todos los que accesarán al sitio como usuario normal y para el acceso a la información (base de datos) desde la pantalla Login, se le pide al usuario su identificación el mismo que es el número de cédula y la contraseña que la institución le otorgará a cada cliente cuando se implemente el sitio web. Para tener un mejor control en cada página del sitio se ha escogido la autenticación basada en formulario y también se ha aplicado la escritura de los cookies, toda esta configuración en el Visual .NET. En fin cada detalle de las configuraciones de cada elemento lo podrá apreciar en este capítulo.

Pero las herramientas no son sólo técnicas. El software y el hardware utilizados son una parte importante, pero no la única. A ella se agrega lo que se denomina "políticas de seguridad internas", que cada empresa u organización debe generar, por lo que en el capítulo 5 se ha realizado un apartado para hablar sobre políticas que deben tomarse en cuenta en lo que se refiere a la Privacidad de la Información, al Acceso a la Información, Autenticación de Usuarios y Administración de la red.

# INDICE GENERAL

# INDICE DE TABLAS

**Pág.**


Tabla 2.1 La Evolución del IIS…….33
Tabla 2.2 Beneficios de Windows 2003……38
Tabla 2.3 Costos de Software……60
Tabla 2.4 Costos de Hardware…… ……..…..60
Tabla 2.5 Costos de Alojamiento del Sitio Web……60
Tabla 3.1 Detalle de Estilos de Letras……65

# INDICE DE FIGURAS


| | | Pág. |
|---|---|---|
| Figura 1.1 | Servidores | 9 |
| Figura 1.2 | Arquitectura de la Red | 11 |
| Figura 1.3 | Esquema General Actual de la Seguridad en la Red de la CTG | 17 |
| Figura 2.1 | Autenticación, Autorización y aplicaciones empresariales | 27 |
| Figura 2.2 | Secure Socket Layer SSL | 43 |
| Figura 2.3 | Ceritificado del SSL | 45 |
| Figura 2.4 | Autoridad de Certificación | 47 |
| Figura 2.5 | Esquema Propuesto de Seguridad en la ..red | 54 |
| Figura 3.1 | Diagrama jerárquici del Sitio Web | 61 |
| Figura 3.2 | Barra de Presentación de la Empresa | 64 |
| Figura 3.3 | Menú principal del Sitio Web | 64 |
| Figura 3.4 | Menú principal de la Consulta en Línea del Sitio Web | 64 |
| Figura 3.5 | Barra de Título | 65 |
| Figura 3.6 | Página Principal | 66 |
| Figura 4.1 | Creación de una aplicación web de ASP.NET | 70 |
| Figura 4.2 | Creación de un directorio virtual en IIS | 71 |
| Figura 4.3 | Activación del Acceso Anónimo. .. | 72 |
| Figura 4.4 | Ventana Inicial del servidor web | 79 |
| Figura 4.5 | Ventana del Wizard para la creación de un DNS | 80 |
| Figura 4.6 | Ventana de selección Tipo de Zona para un DNS | 81 |
| Figura 4.7 | Ventana de configuración de nombre de dominio | 82 |
| Figura 4.8 | Configuración del Activo de almacenamiento de datos del DNS | 83 |
| Figura 4.9 | Configuración de actualizaciones dinámicas | 84 |
| Figura 4.10 | Ventana de comando DOS | 85 |
| Figura 4.11 | Configuración del nombre del sitio web | 86 |
| Figura 4.12 | Configuración de la dirección IP para el sitio web | 87 |
| Figura 4.13 | Configuración de la ruta de almacenamiento del sitio web | 88 |
| Figura 4.14 | Ventana inicial para la creación del certificado | 89 |
| Figura 4.15 | Opciones para la instalación de un certificado | 90 |
| Figura 4.16 | Asociación con nombre del sitio web | 91 |
| Figura 4.17 | Configuración de información de la empresa dueña del certificado.. de seguridad. | 92 |
| Figura 4.18 | Asociación del nombre de dominio | 93 |
| Figura 4.19 | Configuración de información geográfica del sitio web | 94 |
| Figura 4.20 | Configuración de la ruta de almacenamiento del certificado de seguridad | 95 |
| Figura 4.21 | Configuración de información del sitio y de la empresa | 96 |
| Figura 4.22 | Ventana informativa del certificado | 97 |
| Figura 4.23 | Configuración final para la firma del certificado | 98 |
| Figura 4.24 | Configuración del certificado firmado en el IIS | 99 |
| Figura 4.25 | Asociación de la ruta de almacenamiento del certificado firmado | 100 |

Figura 4.26 Configuración del puerto TCP……...101
Figura 4.27 Ventana informativa del certificado firmado……102
Figura 4.28 Cuadro de diálogo Server (Request Security)……...106
Figura 4.29 Logón para la Conexión a la Base de Datos……110
Figura 4.30 Opción para crear usuarios……111

# INDICE GENERAL


**1. ANÁLISIS PARA EL DESARROLLO DE UN SITIO WEB SEGURO ..... 15**
**1.1 Antecedentes de la Empresa ..... 15**
**1.2 Misión y Visión de la Empresa ..... 18**
**1.3 Situación Actual ..... 19**
**1.3.1 Procedimiento Actual de Consultas ..... 19**
**1.3.2 Diseño General de la Red. ..... 22**
**1.3.2.1 Representación del diseño de red. ..... 22**
**1.3.2.2 Hardware ..... 27**
**1.3.2.3 Software ..... 30**
**1.3.2.4 Seguridad Implementada ..... 30**
**2. SITUACION PROPUESTA ..... 33**
**2.1 Justificación de la Implementación ..... 33**
**2.2 Objetivos ..... 34**
**2.3 Requerimientos Técnicos. ..... 35**
**2.3.1 CTG ..... 35**
**2.3.1.1 Hardware ..... 35**
**2.3.1.2 Software ..... 35**
**2.3.2 Usuarios ..... 36**
**2.3.2.1 Hardware ..... 36**
**2.3.2.2 Software ..... 36**
**2.4 Esquema General de las Seguridades a Implementar en el Sitio Web 36**
**2.4.1 Aplicación Web ..... 36**
**2.4.1.1 Autenticación ..... 37**
**2.4.1.2 Autorización ..... 39**
**2.4.2 Internet Information Services - IIS ..... 42**
**2.4.2.1 Seguridades en el IIS ..... 45**
**2.4.2.2 Evolución del IIS ..... 47**
**2.4.3 Sistema Operativo ..... 48**
**2.4.3.1 Funciones del Sistema Operativo ..... 49**
**2.4.3.2 Beneficios ..... 52**
**2.4.3.3 Ediciones del Sistema Operativo ..... 53**
**2.4.4 Secure Socket Layer - SSL ..... 56**
**2.4.4.1 Requerimientos ..... 57**
**2.4.4.2 Certificado de Autorización (CA) ..... 60**
**2.4.5 Base de Datos ..... 62**
**2.4.5.1 Definiciones de Seguridad ..... 63**
**2.4.5.2 Privilegios ..... 64**
**2.4.5.3 Roles ..... 65**
**2.4.5.4 Perfiles ..... 66**

**2.4.5.5 Accesos Autorizados desde el Sistema Operativo.....66**
**2.4.5.6 Niveles de Seguridad.....66**
**2.5 Esquema Propuesto de Seguridad de la Red.....69**
**2.5.1 Componentes del Esquema Propuesto.....69**
**2.5.2 Eventos en la Peticion de Información .....73**
**2.6 Costos Estimados.....74**
**2.6.1 Costos de Software.....74**
**2.6.2 Costos de Hardware .....75**
**2.6.3 Costos de Alojamento del Sitio Web.....75**
**3. DISEÑO DEL SITIO WEB SEGURO CTG ..... 76**
**3.1 Diseño de la Página.....76**
**3.1.1 Diagrama de Opciones.....76**
**3.1.1.1 Descripción de las Opciones del Sitio .....77**
**3.1.2 Estándares utilizados.....79**
**3.1.3 Página principal.....82**
**3.2 Diseño de la Base de Datos .....83**
**4. CONFIGURACION DE LOS ELEMENTOS QUE VAN A PROPORCIONAR SEGURIDAD AL SITIO..... 84**
**4.1 Aplicación Web .....84**
**4.1.1 Autenticación y Autorización .....87**
**4.2 Configuración del Certificado de Seguridad.....94**
**4.2.1 Creación Del Certificado Seguro Para Un Servidor Web.....94**
**4.2.1.1 Crear un Servidor DNS.....95**
**4.2.1.2 Creación de un Certificado Local. .....102**
**4.2.1.3 Firma Digital del Certificado.....112**
**4.3 Sistema Operativo .....119**
**4.4 Base De Datos.....127**
**4.4.1 Configuración de Perfiles de Usuarios .....127**
**4.4.2 Consideraciones de Seguridad.....129**
**5. POLITICAS DE SEGURIDAD..... 131**
**5.1 ¿Qué son las Políticas de Seguridad? .....131**
**5.2 Importancia para una Compañía.....131**
**5.3 Importancia de la Implementación para la CTG.....135**
**5.4 ¿Qué Datos se deben proteger en la CTG? .....135**
**5.5 Diseño de Políticas para la CTG.....136**

# CAPITULO 1

## 1. ANÁLISIS PARA EL DESARROLLO DE UN SITIO WEB SEGURO

### 1.1 Antecedentes de la Empresa

El 29 de enero de 1948, se crea la Comisión de Tránsito de la Provincia del Guayas mediante Decreto Ley de Emergencia No. 140 que se publicó en el Registro Oficial No. 112 del 30 de enero de 1948 cuando fue presidente de la República del Ecuador el Sr. Dr. Carlos Julio Arosemena Tola.

Al momento de su creación al igual que hoy la Institución Rectora del Tránsito ha respondido a las inquietudes y requerimientos puestos de manifiesto por los representantes del comercio, la industria, la banca, la agricultura, movimientos cívicos y en fin toda la colectividad.

Todos nos preguntamos ¿El por qué se celebra en el mes de junio el día del Vigilante de Tránsito?. En el mes de junio de cada año se celebra el mes del Vigilante los 31 días del mes.

Cuando se creó la CTG se llamó División de Tránsito de la Provincia del Guayas, en ese entonces no existían muchas calles y el tránsito lo integraban alrededor de 70 mil automotores.

Sus primeros miembros fueron: Ernesto Jouvín Cisneros, Gobernador y Presidente, Rafael Guerrero Valenzuela, Alcalde y Vocal; José Arosemena, Director Ejecutivo; Manuel Díaz Granados, Subjefe y Comandante de los nuevos Vigilantes.

Para seleccionar al personal que integraría al cuerpo de Vigilantes, fueron nombrados 4 oficiales: Eloy Moncayo Noboa, Luis Gonzaga Nieto, Raúl Yávar Robles y Alejandro García Intriago.

Se hizo un llamado por la prensa para que los ciudadanos interesados se presenten en el Cuartel de la Policía Municipal, ubicado en Chile entre Brasil y Cuenca. Después de un riguroso examen, se seleccionaron a 90 hombres que recibieron durante tres meses de entrenamiento militar y de tránsito.

Antes que existiera la CTG el servicio urbano de pasajeros en Guayaquil estaba formado por tranvías (carros eléctricos) cuyo pasaje costaba un medio y también se lo hacía en carros jalados por mulas. El propietario de esta empresa era el industrial guayaquileño Rodolfo Baquerizo Moreno. Posteriormente circularon las cooperativas de autobuses. Cuando se creó la CTG contaba con un bus, una camioneta, una grúa y 7 motos para controlar el tráfico.

Actualmente la Dirección Ejecutiva está bajo el cargo del Dr. Roberto Pólit, y la Subdirección Ejecutiva bajo la dirección del Crnl. Patricio Rivera.

En los últimos años la Comisión de Tránsito del Guayas se ha empeñado en brindar un mejor servicio, por lo que se han adquirido e implementado equipos tecnológicos de la época actual.

## 1.2 Misión y Visión de la Empresa

**Misión**

- Cumplir con lo dispuesto en el Art. 2[1] de la Ley Sustitutiva y para ello debemos construir una SÓLIDA FORMACIÓN DEL CUERPO DE VIGILANTES, además de reforzar y re-enfocar las áreas operativas de tránsito que posee la institución.

- Optimizar la calidad de nuestros servicios para poder obtener los ingresos por autogestión que nos permitan sostener permanentemente en el tiempo los gastos de la Institución.

**Visión**

- Nos queremos ver como una institución pública que controla el tránsito en la Provincia del Guayas, que se ha ganado la **CREDIBILIDAD** y **RESPETO** de la ciudadanía**,** por su actitud **preventiva** ante la problemática del tránsito y por la buena **calidad de los servicios** que ofrecemos.

[1] ART.2.- FINES.- La Comisión de Tránsito de la Provincia del Guayas tiene como finalidad regular, dirigir y controlar las actividades operativas y servicios de tránsito y el transporte terrestre en la jurisdicción de la provincia del Guayas. La planificación y organización de estas acciones podrán ser coordinadas: con las municipalidades de esta provincia.

## 1.3 Situación Actual

Actualmente las autoridades de la Comisión de Tránsito del Guayas, pensando en mejorar cada día, la funcionalidad y organización de la institución decidieron automatizar todos los procedimientos adquiriendo un nuevo sistema que en la actualidad se está implementando, el cual integra áreas como Control de Tránsito, Brevetación (Licencias), Recaudaciones de Infracciones y Matrícula, y otras más, en una base de datos más robusta en relación a la actual, como lo es ORACLE, el mismo que estamos seguros será un gran aporte que mejorará los procesos internos y de esta manera brindar un excelente servicio a la comunidad.

### 1.3.1 Procedimiento Actual de Consultas

**Consulta y Pago de Citaciones**

1. El usuario deberá acercarse a las ventanillas de Pago de Citaciones en cualquiera de los siguientes departamentos:
   - Atención al Usuario.
   - Brevetación (Norte y Centro).
   - Matriculación.
   - Banco.
2. La cajera/recaudadora consulta el valor de las deudas por infracciones.

3. El usuario cancela el valor por las deudas.
4. La cajera/recaudadora recauda el valor.

**Consulta y Pago de Matrícula**

1. El usuario se acerca a cualquier banco de la red de BANRED con la matrícula anterior.
2. La cajera le consulta el valor a cancelar.
3. La cajera recauda el valor y le da un recibo de pago.

**Películas Antisolares**

1. El usuario realiza un oficio con la petición dirigida a Dirección o Subdirección Ejecutiva, el mismo que demora un día y se lo efectúa en Atención al Usuario.
2. Si la autorización es favorable, el oficio regresa a Atención al Usuario, allí se entregan por parte del usuario los demás documentos los cuales son los siguientes:
   - Certificado Médico emitida por un dermatólogo.
   - La matrícula del vehículo.
   - La licencia del propietario del vehículo.
   - El valor correspondiente del trámite.

3. El trámite pasa al departamento de Jefatura, donde se encargan de realizar el respectivo permiso de circular con películas antisolares.
4. El documento pasa a las ventanillas de Atención al Usuario, lugar donde es retirado por el cliente.

**Cambio de Propietario**

1. Obtener el Certificado de No Poseer Gravamen en Atención al Usuario.
2. Cancelar en el SRI el impuesto del 1% del avalúo del vehículo.
3. Cancelar todas las deudas por infracciones de tránsito.
4. Revisión del vehículo por parte del departamento del OIAT (improntas).
5. El usuario deberá dirigirse a Matriculación y comprar la respectiva especie para este trámite y con los siguientes documentos:
   - Carta de Venta Notarizada.
   - Copia de Cédula del Comprador/Vendedor.
   - Copia de Matrícula del vehículo del año actual.
   - Certificado de No Poseer Gravamen (que se lo indica en el paso 1).
   - Comprobante de Pago del SRI (se lo indica en el paso 2).

6. La cajera/recaudadora realiza el cambio de propietario.

**Vehículos Robados**

1. El usuario deberá dirigirse al departamento del OIAT a reportar la denuncia del vehículo robado con los siguientes documentos:

- Copia de matrícula del vehículo.
- Copia de cédula de la persona que presenta la denuncia.

2. El secretario del departamento genera la denuncia por escrito y bloquea al vehículo para posibles trámites futuros.

## 1.3.2 Diseño General de la Red.

En esta sección explicaremos globalmente la conformación de la red de la institución, se mostrará de manera gráfica sus componentes y se mencionarán los departamentos a los cuales se ha implementado la red.

### 1.3.2.1 Representación del diseño de red.

Existen las siguientes subredes:

- 10.10.1.1
- 10.10.2.0
- (LAN).

- (MATRICULACION y TERMINAL TERRESTRE).

La WAN está conectada con TELCONET. El camino está formado por fibra óptica. Para enlazar los nodos se utiliza Frame Relay para Matriculación y así formar la WAN.

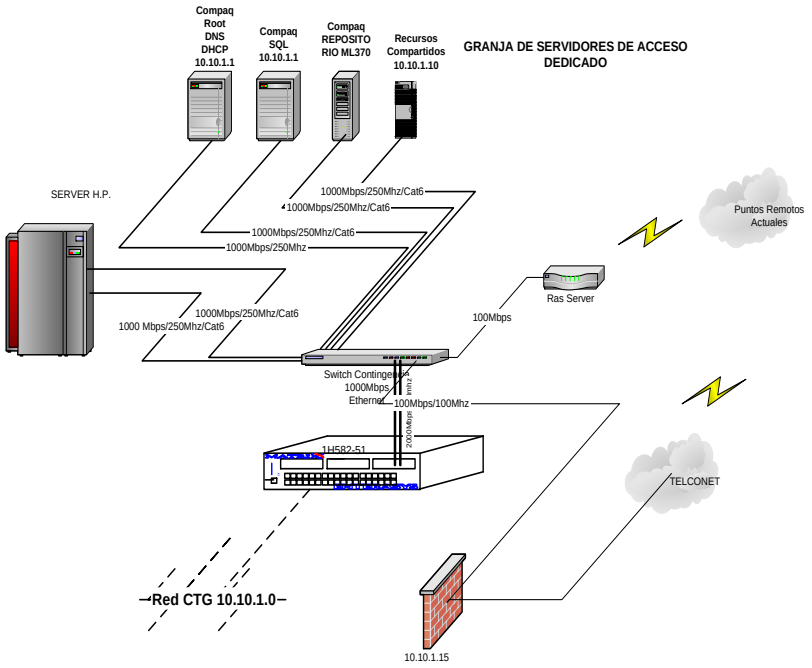



Figura 1.1 Servidores[2]

En la figura 1.1 se muestran los servidores que se encuentran en el Área deCómputo de la Dirección de Informática. La red es la 10.10.1.0, y está conformada por un router el cual tiene conectado un switch de donde están interconectados los siguientes componentes:

[2] FUENTE: Departamento de Redes de la Dirección de Informática de la CTG

- Un Ras Server (Vía teléfono) para comunicar a los host de los puntos remotos que existen como Playas, Salinas, el Empalme, Milagro, y otros puntos.
- El otro componente conectado al switch es un punto de TELCONET para comunicar el área de Matriculación.
- Los otros componentes que salen del switch son servidores los cuales tienen sus respectivas funciones como las mencionaremos a continuación:
  - Servidor de Red (LOGON).
  - Servidor de Base de Datos (SQL).
  - Servidor de Recursos Compartidos e Impresoras.
  - Servidor de Repositorio.
  - Servidor Web.
  - Servidor Exchange.
  - Servidor Intranet – Piloto.
  - Servidor Firewall/Proxi (conexión VPN).
  - Servidor Router CISCO 2610 XML para acceso remoto.

- Servidor HP, el cual contiene la base de datos ORACLE y todos los archivos fuentes y ejecutables del nuevo sistema AXIS.

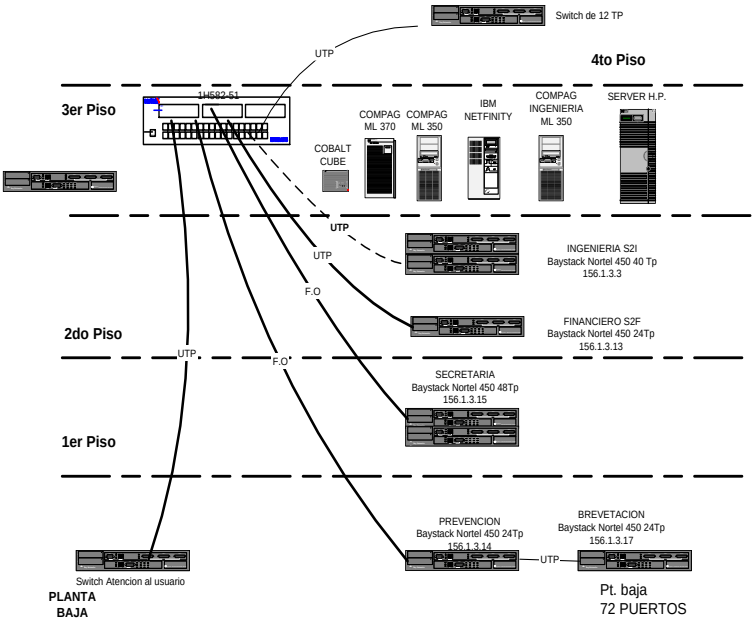



Figura 1.2 Arquitectura de la Red.[3]

En la figura 1.2 se detalla la arquitectura de red por departamentos especificando los dispositivos empleados para su constitución los cuales mencionaremos a continuación:

[3] FUENTE: Departamento de Redes de la Dirección de Informática de la CTG

- En el 3er. Piso en el departamento de Informática se encuentra un router del cual se conectan varios switch y baystack para la comunicación entre departamentos.
- Un Baystack para el departamento de Ingeniería conectado con cable UTP, de igual manera para el departamento Financiero los cuales se encuentran en el segundo piso.
- En el primero piso se encuentra un Baystack para el departamento de Secretaría conectado con fibra óptica.
- En la planta baja se encuentra conectado otro Baystack al router con fibra óptica para el departamento de Prevención el cual a su vez conecta por cable UTP un Baystack ubicado en el área de Brevetación (Licencias).
- En el departamento de Atención al Usuario el cual está en la planta baja se encuentra ubicado un switch conectado al router por cable UTP.

#### 1.3.2.2 Hardware

***Servidores:***

Los servidores se encuentran en el departamento de Informática, los cuales son los que se mencionan a continuación:

- Servidor de Red (LOGON).
- Servidor de Base de Datos (SQL).
- Servidor de Recursos Compartidos e Impresoras.
- Servidor de Repositorio.
- Servidor Web.
- Servidor Exchange.
- Servidor Intranet / Piloto.
- Servidor Firewall/Proxi (conexión VPN).
- Servidor Router CISCO 2610 XML para acceso remoto.
- Servidor Sistema AXIS.

**Características:**

Memoria: 1 GB

Velocidad: 2.4 GHZ Proliant RM 370.

Disco: 18 – 30 GB.

***Servidor de Base de Datos – ORACLE:***

**Características:**

| | |
|---|---|
| Modelo: | RISC 64 bits |
| Memoria: | 1 GB |
| Velocidad: | 2.8 GHZ Proliant. |
| Disco: | RAID5 de 7 discos de 36GB c/u. |
| S.O.: | HPUX 11i |

***Computadores:***

En el departamento de Informática se cuenta con 28 computadores.

**Características:**

| | |
|---|---|
| Memoria: | 256 MB. |
| Velocidad: | 2.4 GHZ. |
| Disco: | 40 GB. |
| Marca: | AOPEN |

***Impresoras:***

Existen 4 impresoras en el área de Informática: 3 tipo láser y 1 matricial.

**Características Impresora Láser:**

| | |
|---|---|
| Marca: | Lexmark |

Modelo: T630 para 80 columnas con servicio de copiado.

**Características Impresora Matricial:**

Marca: Lexmark

Modelo: 2381 para 132 columnas.

***Firewall:***

Este componente es un PC y PROXY al mismo tiempo (acceso a Internet).

**Características:**

Memoria: 512 MB.

Velocidad: 2.8 GHZ.

Disco: 40 GB.

***Router:***

**Características:**

Modelo: CISCO 2600

RAM: 28672k/4096k bytes of memory

ROM: vs.12.2

NVRAM: 32 Kb.

FLASH: 16384 Kb.

Procesador: CISCO 2610XM (MPC860P) Processor (revision 0x100).

I.O.S: Vs.12.2

Arch. Imagen: flash: c2600-i-mz.122-8.T5.bin

Interface: 1 FastEthernet/IEEE 802.3

#### 1.3.2.3 Software

- Sistema Operativo: Windows 2000 Server para el servidor, y para los PCs Windows 2000 Professional.
- Manejador de Base de Datos: SQL, Oracle 9i.
- Correo Interno: Outlook.
- Internet Explorer 6.0
- Firewall: ISA - Internet Security Aceleration de Microsoft

#### 1.3.2.4 Seguridad Implementada

- Los servidores se encuentran bloqueados, sólo los usuarios administradores pueden dar logon.
- Los servidores están protegidos ante hackers, virus por medio del firewall el cual la institución utiliza el ISA.
- Existen limitaciones de acceso según los usuarios a través de Windows 2000.

- Existe un Centro de cómputo privado donde se encuentran los servidores.

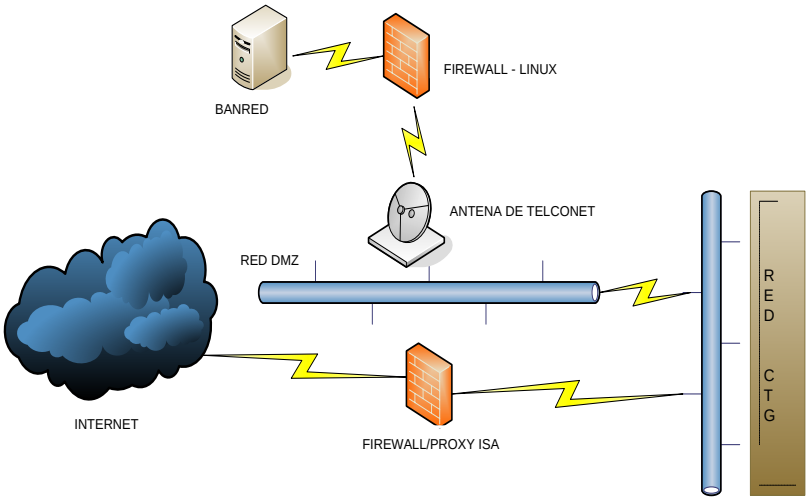



Figura 1.3 Esquema General Actual de la Seguridad en la Red de la CTG[4]

En la figura 1.3 se detalla el Esquema General Actual de la Seguridad en la red de la Comisión de Tránsito del Guayas especificando los dispositivos empleados para su constitución los cuales mencionaremos a continuación:

- En el esquema mostrado tenemos un firewall Linux que nos ayuda a proteger la información recibida de BANRED el mismo que se encuentra en el servidor que se menciona en la figura 1.3, y se tiene una antena de

[4] FUENTE: Creación Propia

Telconet para la conexión de Banred e Internet con la CTG.

- El FireWall/Proxy ISA: es un servidor que realiza las funciones de firewall y Proxy, controlando la información recibida desde la Internet hacia la red de la CTG, previniendo ataques de intrusos a la misma y almacenando información consultada con mayor frecuencia en Internet.

# CAPITULO 2

## 2. SITUACION PROPUESTA

### 2.1 Justificación de la Implementación

Debido al crecimiento del parque automotor y por ende a la cantidad de trámites que esta situación genera se propone crear un sitio Web Seguro cuya implementación permitirá a los usuarios obtener información de cada uno de los servicios que la CTG brinda, además podrá realizar un seguimiento de los trámites con mayor demanda reduciendo de esta manera la afluencia del público en las instalaciones de la institución.

Con el sitio web propuesto, el usuario podrá cómodamente desde su hogar o cualquier sitio con acceso al intenet obtener información de los trámites más requeridos en la institución como: permiso de películas antisolares,

vehículos robados, cambio de propietario y consulta de valores de deuda por infracciones y por matrícula.

## 2.2 Objetivos

Con el propósito de que la CTG mejore los servicios que brinda a la ciudadanía hemos resuelto implementarle un sitio web, el mismo que será de gran ayuda para sus usuarios en lo referente a Consultas de Trámites realizados en la institución, Consulta de Valores por infracciones y matrícula.

Entre los objetivos principales tenemos:

- Brindar a los usuarios una herramienta alternativa de consulta que les permitirá ahorrar tiempo conociendo el estado de sus trámites en todo momento y desde cualquier lugar.
- Evitar la aglomeración de personas en las instalaciones de la CTG, lo cual conlleva a una atención más rápida en los pagos.
- Establecer políticas de seguridad que permitirán realizar tareas para salvaguardar la información.
- Realizar un sitio web seguro de tal manera que el usuario tenga la confianza total de que sus datos están protegidos.

## 2.3 Requerimientos Técnicos

Debido al volumen de información que está almacenada en la base de datos y en base a estadísticas de transacciones que se procesan diariamente, se necesitan los siguientes recursos de hardware y software para la implementación del sitio web.

### 2.3.1 CTG

#### 2.3.1.1 Hardware

**Servidor para el Sitio Web**

***Características:***

Memoria: 1 GB

Velocidad: 2.4 GHZ Proliant RM 370.

Disco: 30 GB.

#### 2.3.1.2 Software

- Sistema Operativo Windows 2003 Server
- Internet Information Services 6.0
- Firewall con software ISA.
- Motor de Oracle 9i vs. 9.2.0.4
- Visual Basic .NET

### 2.3.2 Usuarios

#### 2.3.2.1 Hardware

**Computador**

***Características:***

Modelo: Pentium II de 500MHz

Memoria: 256 MB RAM

Disco: 10GB

Tarjeta Fax Módem

Conexión a Internet

#### 2.3.2.2 Software

- Sistema Operativo Windows 2000 o Windows XP
- Internet Explorer vs. 6.0

## 2.4 Esquema General de las Seguridades a Implementar en el Sitio Web.

### 2.4.1 Aplicación Web

Para el desarrollo de la página utilizaremos Visual Net con ASP.NET[5], el cual proporciona un mayor control para implementar la seguridad de la aplicación. La seguridad de ASP.NET trabaja

[5] FUENTEñ http://www.microsoft.com/spanish/msdn/articulos/archivo/020104/voices/vbnet10282003.asp

junto con la seguridad de Microsoft Internet Information Server (IIS) e incluye servicios de autenticación y autorización para implementar el modelo de seguridad de ASP.NET. ASP.NET incluye también una característica de seguridad basada en funciones que puede implementar para las cuentas de usuario, ya sean usuarios de Microsoft Windows o no.

#### 2.4.1.1 Autenticación

Es el proceso por el que se obtienen credenciales de identificación como el nombre y la contraseña de usuario y se validan dichas credenciales contra alguna autoridad.

ASP.NET proporciona cuatro proveedores de autenticación:

- Autenticación de Formularios.
- Autenticación de Windows.
- Autenticación de Passport.
- Autenticación predeterminada.

**Autenticación de Formularios**

La autenticación de formularios se refiere a un sistema en el que las solicitudes sin autenticar se redirigen a un

formulario de Lenguaje de marcado de hipertexto (HTML) en el que los usuarios escriben sus credenciales. Una vez que el usuario proporciona las credenciales y envía el formulario, la aplicación autentica la solicitud y el sistema emite un vale de autorización en forma de cookie. Esta cookie contiene las credenciales o una clave para volver a adquirir la identidad. Las solicitudes siguientes del explorador incluyen automáticamente la cookie.

**Autenticación de Windows**

En la autenticación de Windows, IIS realiza la autenticación y el símbolo autenticado se envía al proceso del trabajador de ASP.NET. La ventaja de usar la autenticación de Windows es que requiere una codificación mínima. Se recomienda la Autenticación de Windows para representar la cuenta de usuario que IIS autentica antes de entregar la solicitud a ASP.NET.

**Autenticación de Passport**

La autenticación de Passport es un servicio de autenticación centralizado que, proporcionado por Microsoft, ofrece un único inicio de sesión y servicios de

perfil principales para sitios miembros. Por lo general, la autenticación de Passport se usa cuando necesita la capacidad de inicio de sesión único a través de varios dominios.

**Autenticación Predeterminada**

La autenticación predeterminada se usa cuando no desea ninguna seguridad en su aplicación Web; se requiere acceso anónimo para este proveedor de seguridad. Entre todos los proveedores de autenticación, la autenticación predeterminada proporciona rendimiento máximo para la aplicación. Este proveedor de autenticación se usa también cuando utiliza su propio módulo de seguridad personalizado.

#### 2.4.1.2 Autorización

Autorización es el proceso que comprueba si el usuario autenticado tiene acceso a los recursos solicitados.

ASP.NET proporciona los proveedores de autorización siguientes:

- FileAuthorization.

- UrlAuthorization.

**FileAuthorization**

La clase **FileAuthorizationModule** realiza autorización de archivos y está activa cuando se usa la autenticación de Windows. **FileAuthorizationModule** se encarga de realizar comprobaciones en las Listas de control de acceso (ACL)[6] para determinar si un usuario debería tener acceso.

**UrlAuthorization**

La clase **UrlAuthorizationModule** realiza la autorización del Localizador de recursos universal (URL), que controla la autorización basada en el espacio de nombres de URI (Uniform Resourse Identifier).. Los espacios de nombres de URI pueden ser muy diferentes de las rutas de acceso físicas de las carpetas y los archivos que usan los permisos NTFS.

[6] ACL: Definición de permisos sobre el modo de acceso, el origen y los servicios a los que se permite acceder de una máquina.

**UrlAuthorizationModule.**

Implementa aserciones de autorización positiva y negativa; es decir, puede usar el módulo para permitir o denegar de manera selectiva el acceso a las partes arbitrarias de los espacios de nombres de URI para los usuarios, funciones (como directores, evaluadores y administradores) y verbos (como GET y POST).

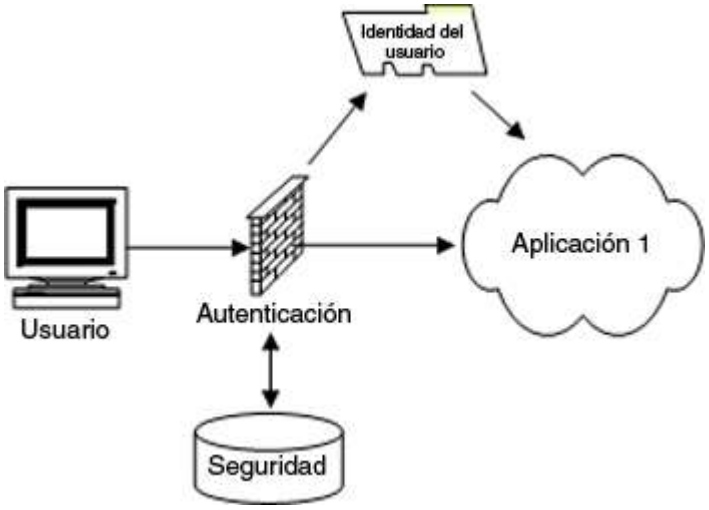



Figura 2.1 Autenticación, autorización y aplicaciones empresariales[7]

La figura 2.1 muestra el procedimiento de autenticación del usuario al ingresar al sitio web: el usuario ingresa su identificación y su contraseña las mismas que son

[7] FUENTE: http://www.microsoft.com/spanish/msdn/articulos/archivo/020104/voices/vbnet10282003.asp

comparadas con las existentes en la base de datos, y si es usuario registrado se le permite el acceso a la aplicación.

**Conclusión**

Sugerimos utilizar el método de Autenticación de Formularios por lo que nos provee un control de acceso por medio de un login donde el usuario colocará su identificación y contraseña que es validada con el servidor donde están los datos; y el tipo de autorización que se propone utilizar es FileAuthorization que nos permitirá configurar la restricción de accesos a la página.

### 2.4.2 Internet Information Services - IIS

El servidor web que se utilizará para la aplicación es el IIS (Internet Information Services). Internet Information Services (IIS) versión 6.0 es un poderoso servidor web que provee una alta confiabilidad, es manejable, y escalable para la infraestructura de una aplicación Web en todas las versiones de Windows Server 2003. IIS[8] ayuda a incrementar la configuración de sitios Web y a la disponibilidad de aplicaciones mientras los costos de sistemas de administración se

[8]FUENTE:http://www.microsoft.com/spain/technet/estudiantes/articulos/iis.mspx

reducen. IIS 6.0 soporta el Microsoft Dynamic Systems Initiative (DSI) con un monitoreo robusto y automatizado, procesos aislados y capacidades de administración mejoradas.

IIS 6.0 ofrece nuevas características incluyendo un proveedor de servicios de criptografía (Cryptographic Service Provider) seleccionable, la posibilidad de configurar la identidad de los Worker Process y deshabilitar extensiones desconocidas.

Cuando un sitio Web requiere SSL (Secure Socket Layer), se obtiene un mayor grado de seguridad a expensas del rendimiento debido al número de ciclos de CPU consumidos para encriptar el contenido. Afortunadamente, existen tarjetas aceleradoras basadas en hardware que permiten mover parte de este procesamiento al hardware. Esas aceleradoras implementan su propia versión de la Crypto API, y IIS 6.0 soporta proveedores de criptografía de terceros.

Una situación en la cual un ataque puede llegar a comprometer un sistema es cuando hay componentes ejecutándose como LocalSystem. Cualquier agujero en un componente de este tipo (como un desbordamiento de búfer) puede permitir al atacante tomar por completo el control de la máquina donde se está ejecutando. IIS

permite configurar la cuenta del sistema bajo la cual trabajará o trabajarán los Worker Process de las aplicaciones, controlando de ese modo el acceso a los recursos del sistema.

IIS permite también restringir la extensión de los ficheros que serán enviados al usuario. Una propiedad de la metabase permite servir solo ficheros con extensiones conocidas, mientras que solicitudes de ficheros con extensión desconocida recibirán un error de "acceso denegado" como respuesta.

Finalmente, existe un conjunto de nuevas características en IIS para hacer la vida del desarrollador Web y de los Webmasters mucho más fácil. Entre ellas se encuentran extensiones a las características FTP, soporte de UTF-8 y Unicode en ISAPIs, y soporte para transmitir vectores de búfers.

IIS 6.0 incrementa su soporte para FTP en dos importantes áreas. Primero, incluye una utilidad de aislamiento de usuarios FTP (FTP User Isolation), que permite restringir a los usuarios de FTP única y exclusivamente a su propio directorio FTP. Esto evita que un usuario vea y/o modifique los contenidos de otros usuarios. Segundo, IIS soporta ahora múltiples conjuntos de caracteres para FTP.

IIS 6.0 incluye soporte para Unicode y UTF-8 en nombres de fichero y URLs. ASP puede ahora trabajar con cualquier nombre de fichero usando el string en Unicode. Las peticiones de URLs en UTF-8 son convertidas a Unicode y luego entregadas a las páginas ASP.

Por último, gracias a una característica denominada VectorSend, IIS soporta la transmisión de listas ordenadas de búfers y manejadores de ficheros. Http.sys agrupa el búfer o bufers en un búfer de respuesta en el kernel y entonces lo envía. De este modo, IIS no tiene que hacer una reconstrucción de búfer o realizar múltiples escrituras al cliente.

#### 2.4.2.1 Seguridades en el IIS

Entre las seguridades que se aplicarán al servidor WEB tenemos:

- Cambiar la ubicación predeterminada del sitio Web de c:\inetpub\ a otra ubicación para que si el sistema estuviera en peligro de alguna manera, el atacante tendría problemas para explorar el árbol de directorios

sin verlo directamente, es decir el atacante no podría tener acceso a la unidad C escribiendo ..\como descripción de la ubicación.

- Eliminar los tipos de contenido dinámico que no se utilicen.
- Bloquear la solución para que utilice la cuenta de servicio local predeterminada de bajo privilegio (la cuenta ASPNET) para ejecutar el código ASP.NET con el fin de asignar sólo los privilegios estrictamente necesarios.
- Agregar la cuenta ASP.NET a un grupo que tenga privilegios limitados ya que originalmente pertenece al grupo "Usuarios" de dicho equipo, por lo tanto posee todos los privilegios asociados a este grupo y puede interactuar con todos los recursos a los que este grupo tiene acceso.
- Restringir el acceso a los directorios de registro de IIS para que los atacantes no puedan modificarlos para borrar sus huellas y ocultar información acerca de alguna vulnerabilidad explotada.

### 2.4.2.2 Evolución del IIS

| | IIS 4.0 | IIS 5.0 | IIS 5.1 | IIS 6.0 |
|---|---|---|---|---|
| **Plataforma** | Windows NT 4.0 | Windows 2000 | Windows XP Professional | Windows Server 2003 |
| **Arquitectura** | 32-bits | 32-bits | 32-bits | 32-bits y 64-bits |
| **Modelo de procesos** | TCP/IP en Kernel y DLL Host | TCP/IP en Kernel y DLL Host | TCP/IP en Kernel y múltiples DLL | HTTP.SYS en Kernel y múltiples Worker Process |
| **Representación de la Metabase** | Binaria | Binaria | Binaria | XML |
| **Seguridad** | Autenticación de Windows | Autenticación de Windows, Keberos y SSL | Autenticación de Windows, Kerberos, SSL y asistente para la seguridad | Autenticación de Windows, Kerberos, SSL, asistentes para la seguridad y Microsoft Passport |
| **Administración remota** | No soportada | HTMLA | Desaparece HTMLA y se introduce el soporte para Servicios de Terminal | Desaparece HTMLA, se introduce el soporte para los Servicios de Terminal y el Web Blade UI |
| **Soporte de cluster** | No disponible | Clustering de IIS | Usa el soporte de Windows | Usa el soporte de Windows |
| **Servicios de Web** | IIS en Windows NT 4.0 | Personal Web Manager en Windows 9x e IIS en Windows 2000 | Opción de IIS para Windows XP e IIS en Windows 2000 | IIS en Windows Server 2003 |

Tabla 2.1 La evolución de IIS[9]

[9] FUENTE: http://www.microsoft.com

En la tabla 2.1 se muestra las diferentes versiones del Internet Information Services y las mejoras en cada una de ellas.

**Conclusiones**

Claramente, la plataforma de elección para el futuro inmediato es Internet. Con tantos usuarios conectados a Internet, y con tantas nuevas aplicaciones en camino, los servidores Web experimentarán un incremento en su carga de trabajo. IIS 6.0 ha sido diseñado para atender esta demanda. Sus amplias mejoras benefician el rendimiento, la fiabilidad y la escalabilidad asegurando un hueco para IIS 6.0 y la plataforma .NET como plataforma de computación para el nuevo milenio.

### 2.4.3 Sistema Operativo

El Sistema Operativo empleado para esta aplicación es el Windows Server 2003 que es el nuevo sistema Operativo basado en la plataforma .NET también dedicado a entornos de servidores.

### 2.4.3.1 Funciones del Sistema Operativo

Tal como lo establece el articulo Presentación de la familia Windows Server 2003, Publicado en: 18 de noviembre del 2002[10], Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar una gran gama de funciones de servidor, en base a sus necesidades, tanto de manera centralizada como distribuida. Algunas de estas funciones del servidor son:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de transmisión de multimedia en tiempo real (Streaming).
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

[10] FUENTE: http://www.microsoft.com/latam/windowsserver2003/evaluation/overview/family.mspx

**.NET y los Servicios Web XML en Windows Server 2003**

Microsoft .NET está altamente integrado en la familia de Windows Server 2003. Permite un nivel sin precedentes de integración de software al usar servicios Web XML: aplicaciones discretas, con elementos básicos que se conectan entre sí - así como con otras aplicaciones más grandes - vía Internet.

Al implantar en los productos la estructura de la plataforma de Microsoft, .NET brinda la posibilidad de crear, alojar, implementar y usar rápida y fiablemente soluciones seguras y conectadas a través de servicios Web XML. La plataforma Microsoft proporciona una serie de herramientas de desarrollo, aplicaciones cliente, servicios Web XML y de servidores necesarios para participar en este mundo conectado.

Estos servicios Web XML proporcionan componentes reciclables construidos en base a los estándares de la

industria que integran capacidades de otras aplicaciones

- Aprovechar sus inversiones existentes. Las aplicaciones existentes basadas en Windows continuarán corriendo en Windows Server 2003 y pueden ser fácilmente empaquetadas como servicios Web XML.
- Escribir menos código y usar herramientas y lenguajes de programación que conozcan. Esto es posible por estar los servicios de aplicación creados en Windows Server 2003, tales como Microsoft ASP .NET, monitoreo de transacciones, mensajes en espera y acceso a datos.
- Usar monitoreo de procesos, reciclaje e instrumentación integrada para dar fiabilidad, disponibilidad y escalabilidad a sus aplicaciones.

Todos estos beneficios están en la infraestructura básica mejorada del servidor de Windows y forman la base de .NET.

### 2.4.3.2 Beneficios

Tal como se indica en la tabla 2.2, y de acuerdo a lo descrito en el documento[11] de **Héctor Gerson**, Windows Server 2003 cuenta con cuatro beneficios principales:

| Beneficio | Descripción |
|---|---|
| **Seguro** | Windows Server 2003 es el sistema operativo de servidor más rápido y más seguro que ha existido. Windows Server 2003 ofrece fiabilidad al:<br>➢ Proporcionar una infraestructura integrada que ayuda a asegurar que su información de negocios estará segura.<br>➢ Proporcionar fiabilidad, disponibilidad, y escalabilidad para que usted pueda ofrecer la infraestructura de red que los usuarios solicitan. |
| **Productivo** | Windows Server 2003 ofrece herramientas que le permiten implementar, administrar y usar su infraestructura de red para obtener una productividad máxima.<br>Windows Server 2003 realiza esto al:<br>➢ Proporcionar herramientas flexibles que ayuden a ajustar su diseño e implementación a sus necesidades organizativas y de red.<br>➢ Ayudarle a administrar su red proactivamente al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones.<br>➢ Ayudar a mantener bajos los gastos generales al permitirles a los usuarios trabajar más por su cuenta. |
| **Conectado** | Windows Server 2003 puede ayudarle a crear una infraestructura de soluciones de negocio para mejorar la conectividad con empleados, socios, sistemas y clientes.<br>Windows Server 2003 realiza esto al:<br>➢ Proporcionar un servidor Web integrado y un servidor de transmisión de multimedia en tiempo real para ayudarle a crear más rápido, fácil y seguro una Intranet dinámica y sitios de Internet.<br>➢ Proporcionar un servidor de aplicaciones integrado que le ayude a desarrollar, implementar y administrar servicios Web en XML más fácilmente.<br>➢ Brindar las herramientas que le permitan conectar servicios Web a aplicaciones internas, proveedores y socios. |
| **Mejor economía** | Windows Server 2003, cuando está combinado con productos Microsoft como hardware, software y servicios de los socios de negocios del canal brindan la posibilidad de ayudarle a obtener el rendimiento más alto de sus inversiones de infraestructura.<br><br>Windows Server 2003 lleva a cabo esto al:<br>➢ Proporcionar una guía preceptiva y de fácil uso para soluciones que permitan poner rápidamente la tecnología a trabajar.<br>➢ Ayudarle a consolidar servidores aprovechando lo último en metodologías, software y hardware para optimizar la |

[11]FUENTE: http://www.ilustrados.com/publicaciones/EpyVVZFykltyaFhnhS.php

| | |
|---|---|
| | implementación de su servidor.<br>➢ Bajar el coste total de propiedad (TCO) para recuperar rápido la inversión. |

Tabla 2.2 Beneficios de Windows 2003[12]

### 2.4.3.3 Ediciones del Sistema Operativo

Las ediciones del Sistema Operativo Windows Server 2003 son las siguientes:

- Microsoft Windows Server 2003 Standard Edition.

  El sistema operativo servidor fiable ideal para satisfacer las necesidades diarias de empresas de todos los tamaños, proporcionando la solución óptima para compartir archivos e impresoras, conectividad segura a Internet, implementación centralizada de aplicaciones y un entorno de trabajo que conecta eficazmente a empleados, socios y clientes. Soporta hasta 4 procesadores y 4 Gb de Memoria RAM.

- Microsoft Windows Server 2003 Enterprise Edition.

  La plataforma preferida tanto por las grandes compañías como por las de tamaño medio para implementar aplicaciones de forma segura, así como

[12] FUENTE: http://www.ilustrados.com/publicaciones/EpyVVZFykltyaFhnhS.php

servicios Web. Integrándose en infraestructuras aportando fiabilidad, mejores rendimientos y un elevado valor empresarial, se presenta tanto en 32 como en 64 bit. Soporta hasta 8 procesadores, hasta 64 Gb de memoria RAM y permite clustering de hasta 8 nodos.

- Microsoft Windows Server 2003 Datacenter Edition.

  Es el servidor escogido para aplicaciones críticas de negocio así como las consideradas de misión crítica, que exigen los más altos niveles de uptime, escalabilidad y fiabilidad. Sólo disponible a través del Datacenter Program de la mano de los fabricantes y proveedores de servicios líderes del mercado, se presenta en las versiones de 32 y 64 bit. y permite escalar por encima de las 8 vías o procesadores alcazando hasta 64 procesadores en paralelo.

- Microsoft Windows Server 2003 Web Edition.

  Optimizado específicamente para albergar y servir páginas web, manteniendo las funcionalidades esenciales que garantizan la fiabilidad, seguridad y facilidad de gestión características de Windows Server.

Es la edición adecuada para implementar servidores web dedicados a bajo coste.

**Conclusiones**

La edición del Sistema Operativo que se utilizará es la Windows Server 2003 Standard Edition por los beneficios que se mencionaron anteriormente y por lo que se menciona a continuación:

- Windows 2003 Server como servidor de ficheros es de un 100% a un 139% más rápido que Windows 2000 Server y un 200% más que Windows NT Server 4.0.
- Como servidor de impresión, es un 135% más eficiente que Windows NT Server 4.0.
- Como servidor web es de un 100% a un 165% más rápido que Windows 2000 Server.
- Las características mejoradas del Directorio Activo permiten realizar tareas más fácilmente, entre las que destacan la habilidad de renombrar dominios, la posibilidad de redefinir el esquema y una replicación más eficiente.
- Mayor disponibilidad a través del Windows System Resource Manager, de las actualizaciones del sistema

automáticas y gracias a un servidor cuyos parámetros le confieren la máxima seguridad por defecto.

- Ofrece la mejor conectividad, facilitando al máximo la configuración de enlaces entre delegaciones, acceso inalámbrico seguro y acceso remoto a aplicaciones a través de los Terminal Services, así como en su integración mejorada con dispositivos y aplicaciones.
- Combinado con Visual Studio .NET 2003, se convierte en la plataforma más productiva para implementar, ejecutar y gestionar aplicaciones conectadas mediante la nueva generación de servicios Web basados en XML. En una palabra, Microsoft Windows Server 2003 es productividad: más por menos.

### 2.4.4 Secure Socket Layer - SSL

El SSL (Secure Sockets Layer) originalmente desarrollado por Netscape Communications, es una tecnología de información para transmitir información de forma segura a través de Internet. El protocolo del SSL utiliza el cifrado para evitar el escuchar detrás de las puertas y el tratar de forzar los datos transmitidos, y se utiliza para asegurar la información pasada por un browser (tal como

número o contraseña de la tarjeta de crédito de un cliente) a un servidor web (tal como un almacén en línea).

Cuando se ingresa una tarjeta de crédito para realizar una compra en un sitio web, el número de tarjeta de crédito es transferida al sitio web del vendedor utilizando SSL, se puede comprobar que un sitio web es seguro porque su URL comienza con https: y si se muestra un candado que significa que SSL está habilitado, como lo muestra la figura 2.2.


Figura. 2.2 Socket Layer SSL[13]

### 2.4.4.1 Requerimientos

Para utilizar el SSL en un servidor web se requiere un certificado del SSL (también conocido como certificados del servidor web y asegurar certificados del servidor). Los certificados del SSL están instalados sobre el servidor web que recibe el sitio web particular y permiten el acceso a la funcionalidad de la seguridad del servidor web.

**¿Cómo un certificado del SSL está instalado sobre un servidor web?**

[13] FUENTE: http://www.microsoft.com

Cuando el SSL primero se activa en el servidor web, el servidor web requiere la información sobre la identidad del sitio web incluyendo los detalles del Nombre de dominio y de la compañía del sitio web.

El servidor web entonces crea dos llaves criptográficas - una llave privada y una llave pública. La llave privada es supuesta por una razón - esta llave debe seguir siendo privada y asegurar, solamente residiendo en el servidor web. La llave pública no necesita ser secreta y se coloca en una petición de la firma del certificado (CSR) - un fichero de datos que también contenga todas las credenciales del sitio web.

Utilizar las llaves privadas y públicas en el proceso del cifrado, para los datos que pasan entre el sitio web y el resto del browser del cliente confidencial y seguro.

El CSR generado se somete a las autoridades de la certificación durante el proceso de uso del certificado del SSL. La autoridad de la certificación después valida las credenciales del sitio web y publica un certificado del SSL

que contiene la identidad digital del sitio web, atando el Nombre de dominio a los detalles de la compañía.

El servidor web emparejará el certificado publicado del SSL a la llave privada asociada y permite que el servidor web establezca acoplamientos cifrados entre el sitio web y los browsers del cliente.

**A qué se parece un Certificado del SSL?**

Los certificados del SSL se pueden ver dando simplemente doble clic en el símbolo del padlock cuando están exhibidos en el browser. La figura 2.3 muestra un certificado típico que se emite al configurar el SSL.

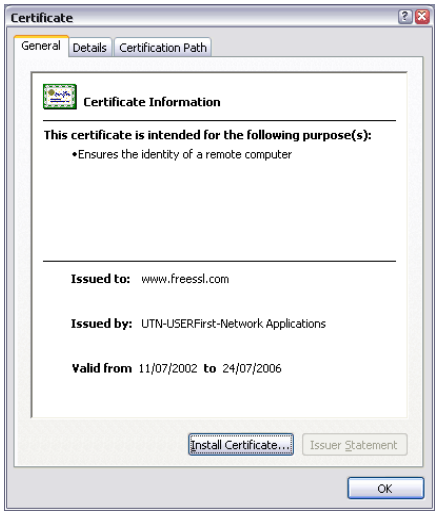



Figura. 2.3 Certificado del SSL[14]

[14] FUENTE: http://www.microsoft.com

Todos los certificados del SSL se publican a las compañías o a los individuos legalmente responsables. Los certificados del SSL contienen típicamente el Nombre de dominio, el nombre de la compañía, la ciudad de la dirección es decir, el estado y el país. También contendrá la fecha de vencimiento del certificado y de los detalles de la autoridad de la certificación responsable de la emisión del certificado.

Cuando un browser conecta con un sitio seguro que recuperará el certificado del SSL del sitio y que comprobará que no ha expirado, que ha sido publicado por una autoridad de la certificación las confianzas del browser y que está siendo utilizado por el sitio web para el cual se ha publicado. Si falla en uno de estos chequeos el browser exhibirá una advertencia al usuario del extremo.

#### 2.4.4.2 Certificado de Autorización (CA)

Las autoridades de la certificación, o CAs como se conocen comúnmente, pueden publicar certificados confiados en el SSL. No cualquiera puede publicar certificados confiados en SSL.

CAs han invertido generalmente en establecer las infraestructuras de la tecnología, de las ayudas, legales y comerciales asociadas a proporcionar certificados del SSL. Aunque CAs esencialmente ellos mismo se regulan, el más cercano a un cuerpo regulador es el programa del compliancy de WebTrust funcionado por AICPA/CICA. La mayoría de CAs se conforma a los principios de WebTrust, no obstante algunos CAs no tienen conformidad de WebTrust. Esos CAs que son exhibición obediente de WebTrust el sello de WebTrust, según lo visto abajo.


Figura. 2.4 Autoridad de Certificación.[15]

El sello de WebTrust mostrado en la figura 2.4 del aseguramiento para las autoridades de la certificación simboliza a los partidos que confían del potencial [e.g. al cliente del extremo] que un médico cualificado ha evaluado las prácticas y los controles de negocio de CA's de determinarse si están en conformidad con el AICPA/CICA

[15] FUENTE: http://www.microsoft.com

WebTrust para los principios y los criterios de las autoridades de la certificación. Una opinión incompetente del médico indica que tales principios se están siguiendo en conformidad con el WebTrust para los criterios de las autoridades de la certificación. Estos principios y criterios reflejan los estándares fundamentales para el establecimiento y la operación en curso de una organización o de una función de la autoridad de la certificación.

**Conclusiones**

Para este proyecto utilizaremos IIS, herramienta que nos provee el Windows Server 2003; y realizaremos la emisión del certificado de seguridad mediante la entidad certificadora www.thawte.com que nos ayudará con un documento de prueba para efectos de realizar este proyecto.

### 2.4.5 Base de Datos

En la Comisión de Tránsito del Guayas actualmente se está implementando un nuevo sistema, el mismo que está desarrollado en Oracle, lo cual es una plataforma robusta, estable y confiable para la información que se maneja en esta institución.

Para tener más claro sobre los puntos a considerar en la seguridad de la base de datos, se presenta a continuación definiciones de seguridad definidas por Oracle.[16]

### 2.4.5.1 Definiciones de Seguridad

**Usuarios**

- Deben tener una cuenta asignada a través de la cual entren en la base de datos y manipulen los objetos de la base.

**Privilegios**

- Permiso para realizar una operación determinada.
- Una mayor granularidad en la definición de privilegios en el sistema permite adaptarlo a las necesidades del trabajo.

**Roles**

- Grupos de privilegios agrupados bajo un nombre.
- Permiten realizar una administración más efectiva cuando existe un gran número de usuarios.

**Perfiles**

- Límites que permiten compartir recursos en la base de datos entre los usuarios.

[16] FUENTE: http://www.infor.uva.es/~jvegas/cursos/bd/oracledba/capitulo6.html

### 2.4.5.2 Privilegios

**A nivel de Objeto**

- El derecho a ejecutar una acción sobre una tabla, vista, secuencia, disparador o procedimiento almacenado específico.
- Puede incluir permisos para pasar privilegios de uno a otro usuario con la sentencia (grant).
- El propietario de un objeto adquiere automáticamente todos los privilegios sobre dicho objeto.
- Los privilegios son: alter, execute, delete, index, insert, references, select, update, all.

**A nivel de Sistema**

- Tiene derecho a ejecutar un tipo de comando sobre objetos de un esquema, objetos de un tipo especificado, sobre el sistema o sobre un usuario.
- El dba puede tener cualquier variedad de privilegios del sistema.
- Existen unos 80 privilegios distintos disponibles.

#### 2.4.5.3 Roles

- Grupo de privilegios que se concede a los usuarios o a otro rol.
- No son propiedad de nadie ni están en un esquema.
- Se puede dar acceso a cualquier usuario a un rol excepto a uno mismo (reflexiva).
- Pueden ser activados y desactivados, por usuarios autorizados (contraseña).
- Las definiciones de roles son almacenadas en el diccionario.
- Un rol puede decidir el acceso se usuario a un objeto, pero no puede permitir la creación de objetos.
- Guia para la creación de roles:
  - Crear un rol para cada aplicación (rol de aplicación).
  - Crear un rol para cada tipo de usuario (rol de usuario).
  - Se proporciona un grupo de roles predefinidos: connect, resource, dba, exp_full_database, imp_full_database.

#### 2.4.5.4 Perfiles

- Restringe la cantidad de recursos del sistema disponible para un usuario.
- Un usuario puede tener un perfil individual o utilizar los límites por defecto. En principio, todos los perfiles por defecto son ilimitados.

#### 2.4.5.5 Accesos Autorizados desde el Sistema Operativo

- Permite acceder a la base de datos sin introducir un nombre y contraseña Oracle a través de una cuenta autorizada del sistema operativo.
- El nombre de usuario Oracle se forma mediante la concatenación del prefijo definido en OS_AUTHENT_PREFIX al nombre de usuario SO.
- Este prefijo puede ser una cadena de caracteres vacía. Por defecto es OPS$.

#### 2.4.5.6 Niveles de Seguridad

Oracle pone al alcance del Administrador de la Base de Datos varios niveles de seguridad:

- Seguridad de Cuentas para la validación de Usuarios.

Para acceder a los datos en una base de datos Oracle, se debe tener acceso a una cuenta en esa base de datos. Cada cuenta debe tener una palabra clave o *password* asociada. Una cuenta en una BD puede estár ligada con una cuenta de sistema operativo. Los *passwords* son fijados cuando se crea un usuario y pueden ser alterados por el DBA o por el usuario mismo. La base de datos almacena una versión encriptada del *password* en una tabla del diccionario llamada `dba_users`. Si la cuenta en la base está asociada a una cuenta del sistema operativo puede evitarse la comprobación del *password*, dándose por válida la comprobación de la identidad del usuario realizada por el sistema operativo.

- Seguridad en el acceso a los objetos de la base de datos. El acceso a los objetos de la base de datos se realiza via privilegios. Estos permiten que determinados comandos sean utilizados contra determinados objetos de la base de datos. Esto se especifica con el comando `GRANT`, *conceder*. Los privilegios se pueden agrupar formando lo que se conoce por roles. La utilización de los roles simplifica la administración de los privilegios cuando

tenemos muchos usuarios. Los roles pueden ser protegidos con *passwords*, y pueden activarse y desactivarse dinámicamente, con lo que constituyen una capa más de seguridad en el sistema.

- Seguridad a nivel de sistema para la gestión de privilegios globales.

  Los roles se pueden utilizar para gestionar los comandos de sistema disponibles para los usuarios. Estos incluyen comandos como `CREATE TABLE` o `SELECT ANY TABLE`. Todos los usuarios que quieran acceder a la BD deben tener el rol `CONNECT`; aquellos que necesiten crear segmentos necesitaran el rol `RESOURCE`. Un usuario con el rol `DBA` tiene derecho para ver y manejar todos los datos de la BD. En Oracle `CONNECT`, `RESOURCE` y `DBA` son roles de sistema. Las acciones contra cada tipo de objeto son autorizadas por privilegios separados. Así, un usuario puede tener concedido el privilegio `CREATE TABLE`, pero no el `ALTER TABLE`.

## 2.5 Esquema Propuesto de Seguridad de la Red

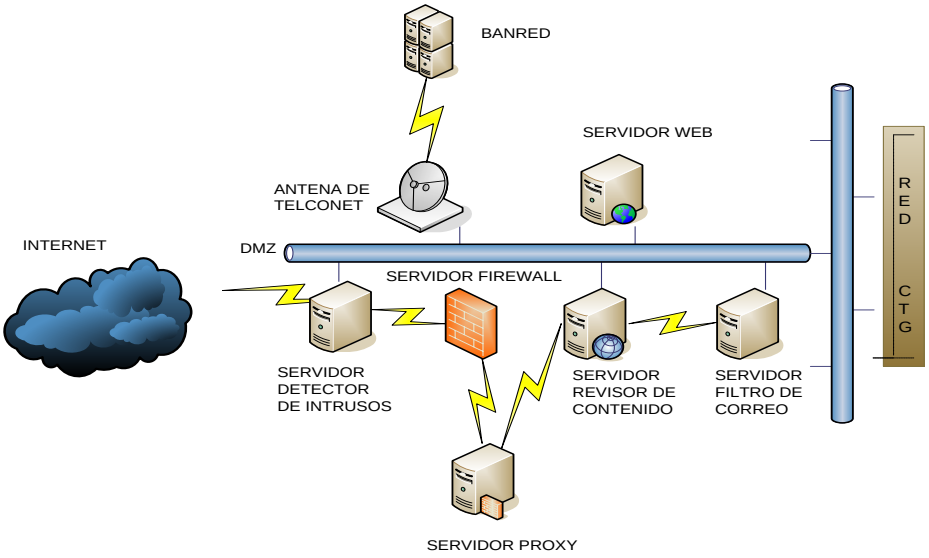



Figura. 2.5 Esquema Propuesto de Seguridad en la Red[17]

### 2.5.1 Componentes del Esquema Propuesto

A continuación se detalla los componentes que en la figura 2.5 se presentan:

- **Servidor para Detector de Intrusos**

  En este equipo se instalará un software llamado Intrusion Detection System (IDS) (sistema de detección de intrusos), el cual es similar a un sensor de movimiento o a una cámara de vigilancia que detecta actividad, activa alertas y genera una

[17] Fuente: Creación Propia

respuesta armada. El análisis es como un guardia de seguridad que controla y cierra las puertas o ventanas abiertas antes de que sean violadas.

- **Servidor para Firewall**

  Es este servidor se debe instalar el software ISA que la CTG ya lo posee, el mismo que sólo actuará como firewall, este sistema nos ayudará a prevenir algunos tipos de comunicaciones prohibidos por las políticas de red, las cuales se fundamentan en las necesidades del usuario.

- **Servidor para Proxy**

  Este equipo actuará como Proxy, y se utilizará para almacenar la información que es consultada con mayor frecuencia en páginas de Internet, por un período de tiempo, con el fin de aumentar la velocidad de acceso. Al mismo tiempo libera la carga de los enlaces hacia Internet.

- **Servidor para Revisor de Contenido**

  El software de revisor de contenidos se lo instalará en un servidor muy aparte de los demás, para que realice su función respectiva.

Este software que realiza la exploración de contenido se encuentra disponible como característica en soluciones más avanzadas de servidores de seguridad o como un componente de un servicio independiente, por ejemplo, el correo electrónico. La exploración de contenido analiza los datos que tienen permiso para entrar o salir de la red de la organización a través de los canales de datos válidos. Si se realiza en el correo electrónico, generalmente funciona con los servidores de correo electrónico para comprobar determinadas características del correo, como los archivos adjuntos. Esta técnica puede explorar e identificar contenido de software malintencionado en tiempo real a medida que los datos pasan a través del servicio. Microsoft colabora con distintos socios para ofrecer características de seguridad mejoradas, como la exploración de contenido antivirus en tiempo real, para Microsoft Exchange Server e ISA Server.

- **Servidor para Filtro de Correo**

En este servidor se colocará un software que nos ayudará a filtrar cuentas de correo que no se desea recibir, el cual permite bloquear correo a partir de una persona (por dirección de correo electrónico), de un sitio entero (por dominio), o de un dirección

IP. De esta manera también protegeríamos nuestra red de correos malintencionados.

- **Red Implementada en CTG**

  Es la red que actualmente está implementada en la institución, la misma que no se hará modificaciones, la misma que está detallada en la figura 1.1 y 1.2.

- **Red DMZ**

  Es un área de red de computadoras que está entre la red de computadoras interior de una organización y una red de computadoras exterior, generalmente la Internet. La zona desmilitarizada permite que servidores interiores provean la red exterior de servicios, mientras protege la red interior de intromisiones. En términos más simples es como una calle de sentido único. La red interior se permite iniciar conexiones a la exterior, pero no viceversa.

- **Servidor para el Sitio Web**

  En este servidor constará el sistio Web con todas las seguridades configuradas en el capítulo 4.

- **Servidor para Banred**

  Este servidor ya existe actualmente en la institución con los aplicativos de BANRED.

  A continuación se detalla el flujo de peticiones que desde la Internet se realizará hacia la CTG, y explicando la importancia de la implementación de cada hardware y software que se propone en la figura 2.5.

### 2.5.2 Eventos en la Peticion de Información

1. El usuario solicita una consulta en el sitio web;
2. Luego el IDS (servidor de Identificador de Intrusos) analiza los paquetes que el usuario envía y/o cualquier comportamiento sospechoso, como por ejemplo el scaneo de puertos o paquetes malformados, etc;
3. El firewall determina si el paquete IP cumple con las reglas definidas por el administrador del firewall;
4. Luego la petición llega al servidor Proxy, filtra el contenido en base a restricciones establecidas, si la información consultada no se encuentra en el servidor Proxy, el ISP hace la petición al sitio que corresponde;

5. El servidor donde se encuentra el revisor de contenido es el siguiente en realizar su función, que es la de verificar los datos que el usuario desea consultar;
6. Luego el software de Filtro de correo bloquea aquella correspondencia que no es permitida, y;
7. Finalmente los datos han pasado por todas las validaciones.

## 2.6 Costos Estimados

De acuerdo a nuestra investigación en el mercado local y luego de haber analizado los diferentes costos que implica la provisión del equipamiento de hardware y sofware propuesto, le presentamos unas tablas valuativas con los respectivos precios.

### 2.6.1 Costos de Software

| Artículo | Descripción | Precio |
|---|---|---|
| Windows Server 2003 Edición Estándar | Permite compartir impresoras y archivos, conectividad a internet más segura, administración centralizada de políticas para Pcs y soluciones web. Incorpora el IIS vs.6.0 | US$ 925.00 incluye 10 licencias |
| Visual Studio Net 2003 Professional Special Edition | Ofrece la herramienta ASP. | Versión Upgrade: US$ 310.00 Normal: US $799.00 |
| SSL123 | Ofrece certificado de seguridad. 128 bits de encripción. | US$ 149.00 1 año US$ 259.00 2 años |

Tabla 2.3 Costos de Software.[18]

[18] FUENTE: Windows Server 2003: http://cgi.ebay.es/ws/eBayISAPI.dll?ViewItem&category=80360&item=7163165138&rd=1&ssPageName=WD2V;

### 2.6.2 Costos de Hardware

| Artículo | Descripción | Precio |
|---|---|---|
| Servidor | Marca HP<br>Modelo proliant ml 350 G4<br>Velocidad procesador 3.2 GHZ<br>Ram 1GB<br>Disco duro 80GB | US$ 2,000.00 |
| | Marca HP<br>Modelo proliant ml 150 G2<br>Intel Xeon velocidad procesador 3 GHZ.<br>Ram 512 expandible hasta 8 GB<br>Disco duro 80 GB | US$ 1,825.00 |

Tabla 2.4 Costos de Hardtware.[19]

### 2.6.3 Costos de Alojamento del Sitio Web

En la tabla 2.5 se muestra una cotización de alojamiento de un sitio web, gasto que la Comisión de Tránsito no realizará por lo que ya posee un enlace con Telconet.

| Plan | Descripción | Precio |
|---|---|---|
| Webhosting Avanzado | 100 MB de almacenamiento<br>7 GB de transferencia de archivos<br>1 dominio incluído<br>5 cuenta de correo POP3<br>Acceso FTP - 24x7<br>Soporte para plataformas PERL, ASP y PHP<br>Soporte para base de datos en ACCESS, MySQL y SQL Server | US$ 560.00 anual |

Tabla 2.5 Costos de Alojamiento del Sitio.[20]

Visual Studio Net 2003: http://msdn.microsoft.com/howtobuy/vstudio/default.aspx; SSL123: http://WWW.thawte.com

[19] FUENTE: Empresa NOCSA

[20] FUENTE: http://www.telconet.net/espanol/productos/hosting.php

# CAPITULO 3

## 3. DISEÑO DEL SITIO WEB SEGURO CTG

### 3.1 Diseño de la Página

#### 3.1.1 Diagrama de Opciones

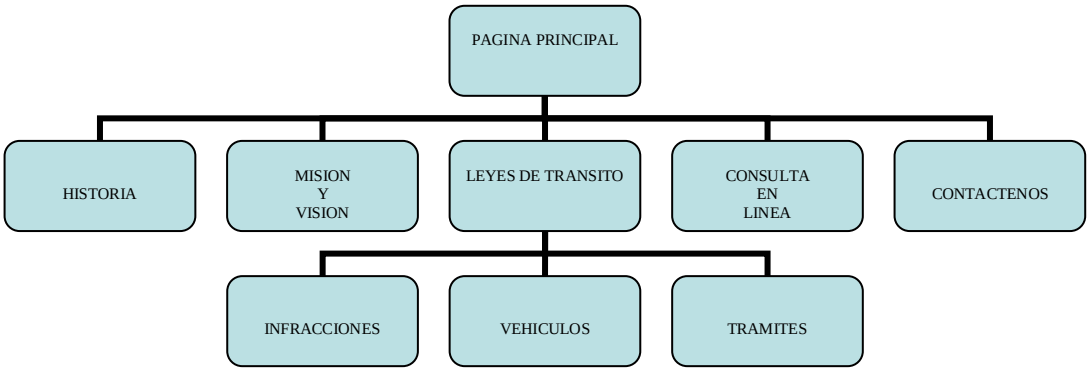



Figura 3.1 Diagrama Jerárquico del Sitio Web.[21]

[21] FUENTE: Creación propia

#### 3.1.1.1 Descripción de las Opciones del Sitio

La figura 3.1 muestra jerárquicamente la conformación del sitio web. A continuación describiremos cada una de sus opciones:

- **Historia**

  Esta página detalla una breve reseña de los inicios de la institución como: fecha de creación, bajo que gobierno fue creada, sus primeros miembros, etc.

- **Misión y Visión**

  En esta opción se indica los objetivos que conllevaron a su creación, y se expresa las metas presentes de la Comisión de Tránsito del Guayas.

- **Reglamentos de Tránsito**

  Esta opción transcribe los numerales de tránsito más notables y se muestra gráficamente las señales de tránsito más usuales.

- **Información de Requisitos de Trámites**

Esta opción tiene como objetivo presentar todos los requisitos necesarios para obtener un determinado trámite.

- **Consulta en Línea**

  "Consulta en Línea" permite al cliente con su número de licencia accesar al sitio web y revisar sus deudas como: infracciones, valores de matrícula; y realizar un seguimiento de los trámites efectuados, los cuales se detallan a continuación:

  - **Infracciones**

    En esta opción de "Infracciones", el sitio web visualizará las citaciones pendientes de pago del cliente.

  - **Vehículos**

    En la opción de "Vehículos", se le mostrará al cliente los valores de matrículas de todos los vehículos de su propiedad.

  - **Trámites**

    La opción "Trámites", permitirá al cliente realizar un seguimiento de los trámites que haya efectuado.

- **Contáctenos**

  Esta opción dará al cliente información dónde pueda contactarse y dejar sus sugerencias.

### 3.1.2 Estándares utilizados

**Barra de Presentación de Empresa**

Esta barra se encuentra en la parte superior de todas las páginas que conforman el sitio web. Su diseño es como se muestra en la figura 3.2.


Figura 3.2 Barra de Presentación de la empresa[22]

**Menús**

Los menús que tiene el sitio web están diseñados con botones como se aprecia en las figuras 3.3 y 3.4. y están ubicados en la parte izquierda de todas las páginas.

[22] FUENTE: Sitio Web de la CTG


Figura 3.3 Menú Principal del Sitio Web.[23]


Figura 3.4 Menú Principal de la Consulta en Línea del Sitio Web.[24]

## Barra de Títulos

La barra de títulos que indicará en que menú se encuentra navegando se encuentra ubicada en la parte superior de todas las páginas debajo de la barra de presentación de la empresa. (Vea figura 3.5)


Figura 3.5 Barra de Títulos[25]

[23] FUENTE: Sitio Web de la CTG

[24] FUENTE: Sitio Web de la CTG

[25] FUENTE: Sitio Web de la CTG

## Estilos de Letras

El estilo utilizado en el sitio web es el siguiente:

| Descripción | Tipo | Tamaño | Estilo |
|---|---|---|---|
| Contenido Normal | Tahoma | 12 px | normal |
| Subtítulos | Tahoma | 1 | Título |
| Títulos | Tahoma | 2 | Mayúscula negrita |

Tabla 3.1 Detalle de estilos de letras.
El color que tienen todas las letras es azul marino.[26]

[26] FUENTE: Creación Propia

### 3.1.3 Página principal

La figura 3.6 muestra el diseño de la página principal del Sitio Web, el cual tiene todos los componentes que se mencionan anteriormente: barra de presentación de la empresa, barra de títulos en la parte superior; la barra de menú en la parte vertical izquierda; y el contenido el resto de la pantalla restante.


Figura 3.6 Página Principal[27]

[27] FUENTE: Sitio Web de la CTG

## 3.2 Diseño de la Base de Datos

El diseño de la base de datos es fundamental en la implementación de todo proyecto en donde se desea manejar información dinámica. Para el desarrollo del sitio web hemos determinado que se utilizará el mismo diseño que se está implementando en el nuevo sistema Axis que la Comisión de Tránsito de la Provincia del Guayas obtuvo con el convenio que realizó con la ESPOL.

Ver anexo # 1

# CAPITULO 4

## 4. CONFIGURACION DE LOS ELEMENTOS QUE VAN A PROPORCIONAR SEGURIDAD AL SITIO

### 4.1 Aplicación Web

De acuerdo a lo descrito en el manual[28] para que funcione una aplicación Web de ASP.Net se debe tener en el Servidor Web lo siguiente:

- Tener instalado IIS 5.0 ó superior en el servidor Web y configurar un directorio virtual asociado a la aplicación Web.
- Tener instalado en el servidor Web .Net Framework.
- Los archivos .aspx correspondientes a las páginas Web.

[28] FUENTE:http://www.microsoft.com/spanish/msdn/articulos/archivo/140303/voices/openhack.asp

- Un archivo de ensamblado (DLL) situado en la carpeta Bin de la aplicación Web, que contiene el código de servidor que necesitan las páginas aspx.
- Un archivo llamado Global.asax que sirve para el control general de la aplicación durante su ejecución.
- Un archivo llamado Web.config donde se establece la configuración de la aplicación. Aunque este fichero es opcional se necesita cuando se quieren establecer parámetros de configuración que no sean los de por defecto.
- De manera adicional también puede aparecer en la carpeta Web otro tipo de archivos como:
  - Archivos .ascx (controles personalizados de usuario de ASP.Net)
  - Archivos .asmx (servicios Web XML de ASP.Net).
  - Páginas .htm ó .html (páginas Web estáticas)
  - Páginas .asp (páginas activas de servidor)
  - Archivos .css (hojas de estilo CSS, Cascade Style Sheet).
  - Documentos, imágenes, etc.

Para terminar, se va a crear una aplicación Web de tipo ASP.Net y a instalarla en un servidor Web con IIS. El primer paso es crear la aplicación Web, para ello se entra en Visual Studio .Net y en el menú 'Archivo' se selecciona 'Nuevo proyecto'. Aquí se debe elegir uno de los lenguajes

disponibles y seleccionar 'Aplicación Web ASP.Net' como lo señala la figura 4.1.

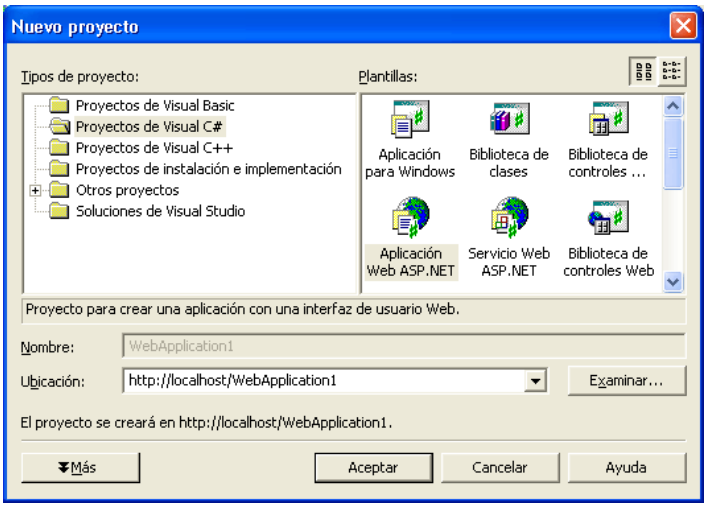



Figura 4.1. Creación de una aplicación Web de ASP.Net

Esta figura muestra la Ventana inicial para elegir la clase de proyecto.[29]

De forma automática, al crear un nuevo proyecto Web, Visual Studio .Net crea un directorio virtual en el IIS y lo asocia con la aplicación Web. Si se ha instalado IIS con la configuración por defecto, el sitio Web predeterminado (localhost) será 'c:\inetpub\wwwroot'.

En el caso de que tuviéramos una aplicación Web de ASP.Net ya creada y se desee instalar en un servidor Web, se debe copiar la carpeta con la aplicación en el servidor Web y asociarla manualmente a un directorio virtual. Para ello, dentro de IIS se selecciona el elemento de 'Sitio Web predeterminado' y pulsando con el botón derecho se selecciona la opción:

[29] FUENTE : http://www.microsoft.com/spanish/msdn/articulos/archivo/140303/voices/openhack.asp

'Nuevo' > 'Directorio virtual' donde mediante un asistente se asocia la carpeta de la aplicación Web a un directorio virtual en el servidor, tal como se muestra en la figura 4.2.

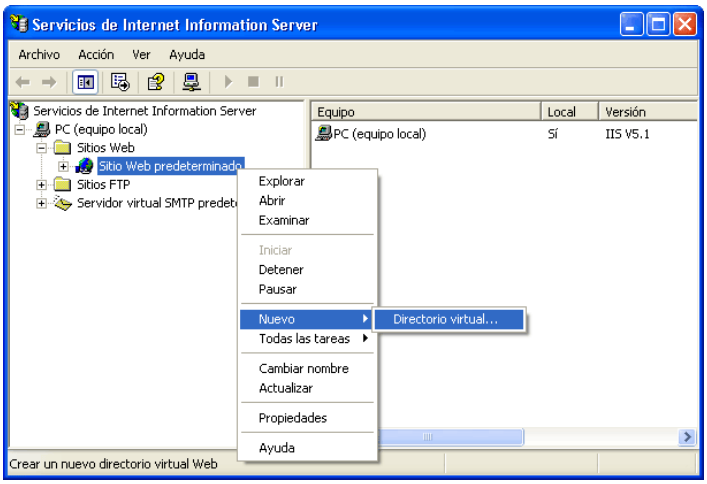



Figura. 4.2. Creación de un directorio virtual en IIS

Para probar que la aplicación Web funciona correctamente se debe compilar primero en Visual Studio .Net y posteriormente acceder a la aplicación mediante el navegador como se muestra a continuación:

http://[Nombre_del_servidor]/[directorio_virtual]/[página]

Por ejemplo, http://localhost/MiWeb/webform1.aspx

### 4.1.1 Autenticación y Autorización

**Uso de la Autenticación basada en Formularios.**

Aunque la autenticación de Windows es fácil de utilizar, en muchas ocasiones no resulta práctica para las aplicaciones Web. La mayoría

de las aplicaciones Web proporcionan servicios a usuarios que no disponen de cuentas en nuestro dominio o Active Directory, por lo que es necesario implementar un esquema de seguridad personalizado.

La característica de autenticación basada en formularios que incorpora ASP.NET proporciona una solución cómoda, aunque como veremos no trata automáticamente todos los detalles.

La autenticación formulario es un servicio de autenticación ASP.NET que permite que las aplicaciones proporcionen su propia interfaz de sesión y que realicen comprobación de credenciales personalizada. Con autenticación mediante formularios, ASP.NET autentica los usuarios y a continuación, redirigir a usuarios no autenticados a la página de sesión especificada por el atributo **loginurl** del elemento **<forms>** en el archivo Web.config. Cuando proporciona credenciales a través del formulario de sesión, la aplicación autentica la solicitud y a continuación, el sistema emite una clase **FormsAuthenticationTicket** en el formulario de un cookie. La clase **FormsAuthenticationTicket** se pasa como un cookie como respuesta a solicitudes posteriores Web del cliente autenticado.

Para utilizar la autenticación basada en formularios, IIS debe permitir el acceso anónimo a nuestro sitio Web. Éste es el comportamiento predeterminado para una nueva raíz virtual y se puede establecer en la consola de administración de IIS. La figura 4.3 muestra la ventana de diálogo para configurar el modo de autenticación por formularios.

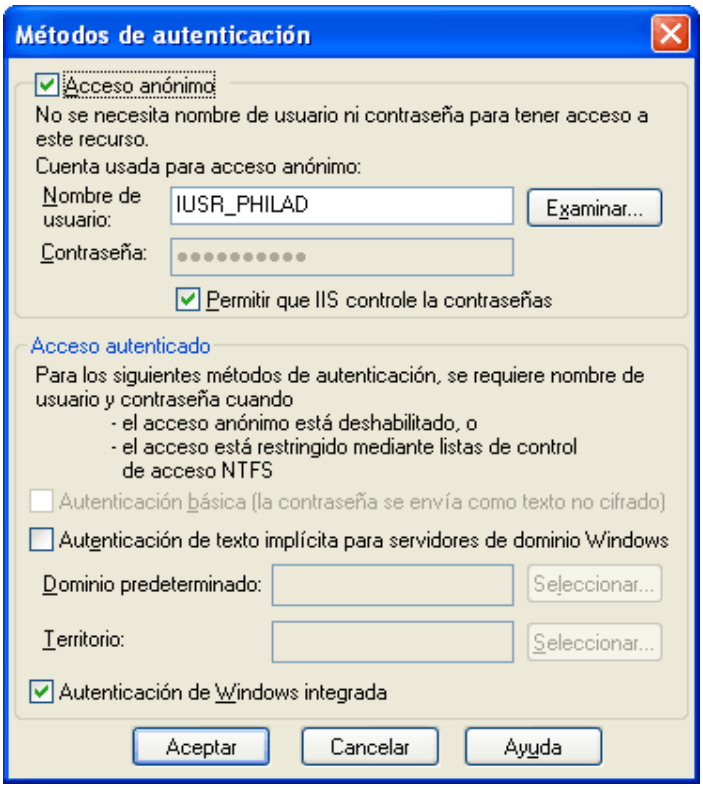



Figura 4.3 Activación del acceso anónimo[30]

A continuación, necesitamos configurar en nuestro archivo web.config que la aplicación utilice la seguridad basada en

[30] FUENTE: http://www.microsoft.com/spanish/msdn/articulos/archivo/140303/voices/openhack.asp

formularios. Para ello, tenemos que cambiar los elementos <authentication> y <authorization> del archivo:

```
    <authentication mode="Forms">
       <forms name="login"
         loginUrl="login.aspx" protection="All"
         timeout="60" />
    </authentication>

 <authorization>
   <deny users="?" /><!-- Block unauthorized users -->
 </authorization>
```

En el elemento <forms>, especificamos un atributo **loginUrl**, que apunta a una página Web específica de nuestra aplicación. Esta página Web se encargará de solicitar al usuario las credenciales y autenticar al usuario teniendo en cuenta estas credenciales. Mientras que no se haya autenticado al usuario, ASP.NET dirigirá automáticamente al usuario a esta página de inicio de sesión siempre que se realice un acceso a nuestro sitio.

Por tanto, es necesario implementar login.aspx. Esta página debe solicitar las credenciales al usuario, normalmente un nombre de usuario y una contraseña. A continuación, utilizará dicha información para autenticar al usuario. Tenga en cuenta que los

datos enviados desde el explorador a nuestro servidor Web se pasarán como texto sin cifrar, por lo que deberá utilizar SSL para proteger esta página y cifrar la contraseña del usuario antes de que se envíe desde el explorador hasta nuestro servidor.

**Depuración con la identidad ASPNET**

Al depurar un servicio Web XML, la llamada a éste se realiza con la identidad ASPNET, si se determinó esta opción en el archivo machine.config. De forma predeterminada, la identidad ASPNET no es un miembro del grupo Usuarios del depurador (consulte la sección siguiente, "Mecanismos de seguridad en el entorno de desarrollo de Visual Studio .NET"), de modo que no se puede obtener acceso al código del servicio Web XML durante la depuración. Para depurar un servicio Web XML, abra el código del servicio y establezca un punto de interrupción.

Se recomienda llevar a cabo la depuración en un equipo de prueba y no en el de implementación. Este tema se describe en la sección siguiente, "Mecanismos de seguridad en el entorno de desarrollo de Visual Studio .NET".

Para obtener más información sobre cómo configurar la identidad de proceso, consulte ASP.NET Process Identity y ASP.NET Impersonation (en inglés).

**Mecanismos de seguridad en el entorno de desarrollo de Visual Studio .NET**

Además de proteger el servidor, es necesario proteger el equipo de desarrollo del ataque de código malintencionado y datos dañados. Existen varios mecanismos en el entorno de desarrollo que se pueden aprovechar para garantizar la seguridad de los servidores de desarrollo:

**Depuradores y Programadores de VS** Estos dos grupos de cuenta se agregan durante la instalación de Visual Studio .NET. El grupo Programadores de VS dispone de los permisos de IIS, recurso compartido y archivo necesarios para crear y desarrollar aplicaciones Web en un servidor. El grupo Depuradores tiene la capacidad de depurar procesos en un equipo determinado, ya sea de forma local o remota. Los dos grupos son usuarios eficaces del servidor, ya que disfrutan del acceso a la mayoría de los recursos. Para obtener más información, consulte Web Application Security at Design Time in Visual Studio (en inglés).

**Depuración**

Se recomienda llevar a cabo la depuración en un equipo de prueba y no en el de implementación. Si debe realizar la depuración en un servidor de implementación, instale sólo el componente de depuración remota y desinstálelo cuando haya finalizado el proceso. Deje al servidor sin conexión mientras realiza la depuración. Para obtener más información, consulte Introduction to Web Application Debugging (en inglés).

**Implementación**

La mayoría de las aplicaciones sólo necesitan que .NET Framework se encuentre instalado en el servidor. Si instala Visual Studio .NET o sus componentes de servidor en el equipo de implementación, aparecerán en éste los grupos Depuradores y Programadores de VS, y deberá restringir los miembros de sus usuarios. Asimismo, es aconsejable deshabilitar el descubrimiento dinámico.

**Advertencia** Se recomienda no instalar Visual Studio en el servidor de implementación.

En la característica de copia de proyectos de Visual Studio .NET se incluye una opción que permite implementar una aplicación con un archivo de configuración (Web.config) diferente al utilizado durante

el desarrollo. Es probable que la depuración esté habilitada en el archivo de desarrollo y, si éste se implementa, permitiría a los usuarios examinar la pila de llamadas al originarse una excepción. Se recomienda llevar a cabo la implementación con un archivo de configuración independiente que no permita la depuración.

## 4.2 Configuración del Certificado de Seguridad

### 4.2.1 Creación Del Certificado Seguro Para Un Servidor Web Utilizando Internet Information Services.

Un certificado seguro (Secure Certificate) nos permitirá cifrar la información que viaja desde y hacia el servidor web para de esta manera evitar fraudes, robo o uso indebido de información confidencial por terceras partes. Para poder utilizar un certificado seguro éste deberá ser manejado a nivel del servidor por un componente llamado SECURE SOCKET LAYER que es quien establece la conexión segura para que el certificado entre en funcionamiento. Sin embargo, antes de generar un certificado seguro, usted debe asegurarse de que el nombre calificado de Internet (DNS) del servidor web ya exista porque cada certificado depende de éste nombre.

Hay dos etapas en la creación de un certificado seguro que se deben tener en cuenta, la primera es asegurarse que hay un servidor DNS funcionando y la segunda parte es la creación del certificado como tal en el Internet Information Services y alguna compañía de Emisión de certificados autorizados como por ejemplo THAWTE.

#### 4.2.1.1 Crear un Servidor DNS

Si aún no ha definido un DNS en su servidor web, es conveniente que realice este paso antes que nada. Por favor siga los siguientes pasos para que vea el proceso completo de definir un DNS y luego como adquirir e instalar un certificado seguro en el servidor web IIS.

Un certificado seguro (Secure Certificate) nos permitirá cifrar la información que viaja desde y hacia el servidor web para de esta manera evitar fraudes, robo o uso indebido de información confidencial por terceras partes. Para poder utilizar un certificado seguro éste deberá ser manejado a nivel del servidor por un componente llamado SECURE SOCKET LAYER que es quien establece la conexión segura para que el certificado entre en funcionamiento. Sin embargo, antes de generar un

certificado seguro, usted debe asegurarse de que el nombre calificado de Internet (DNS) del servidor web ya exista porque cada certificado depende de éste nombre.

**Paso 1:** Deberá escoger en las herramientas administrativas la opción de administrar o crear un DNS y deberá llegar a la pantalla donde le pregunta que tipo de zona es con la que desea trabajar. Expanda el árbol donde se encuentra el nombre del equipo, seleccione "forward lookup zone" haga clic con el botón derecho y seleccione la opción "new zone" como muestra la figura 4.4.

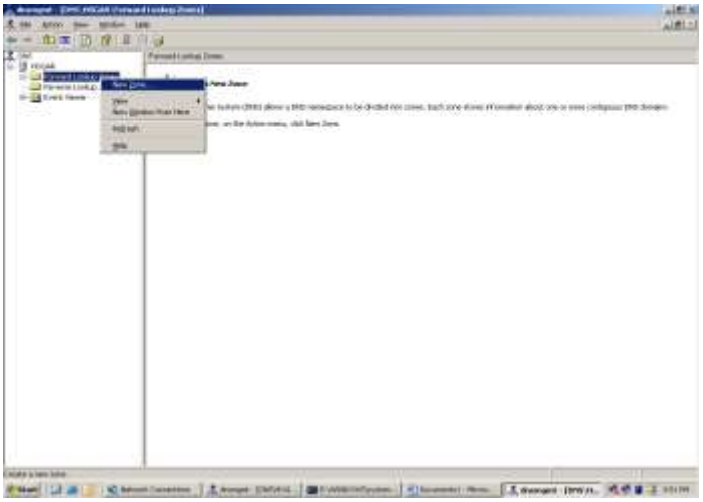


Figura 4.4 Ventana Inicial del Servidor Web[31]

[31] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003

**Paso 2:** En la creación del DNS, se muestra la siguiente pantalla del wizard como muestra la figura 4.5.


Figura 4.5 Ventana del Wizard para la creación de un DNS[32]

**Paso 3:** Deberá seleccionar el tipo de zona que su servidor DNS va a manejar. En este caso es una zona primaria que se actualizará y se le dará mantenimiento directamente en este servidor así que escoja la primera opción tal cual muestra la figura 4.6.

[32] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003

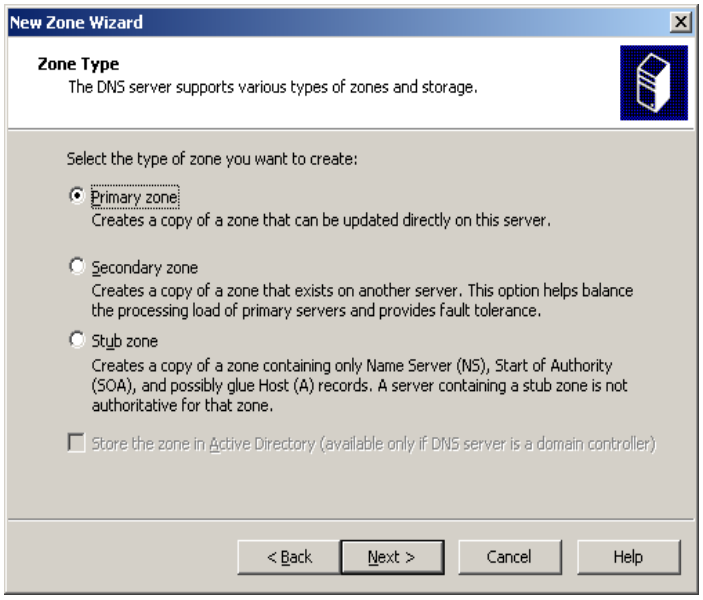



Figura 4.6 Ventana de selección Tipo de Zona para un DNS[33]

**Paso 4**: En este paso debemos seleccionar el calificativo o nombre de dominio con el que su servidor será conocido en el mundo exterior del Internet. Recuerde que los certificados se crean en base a este nombre pues parte de la codificación del mismo incluye en algún lugar este nombre. Una vez creado el certificado con este nombre ya no hay marcha atrás y si desea cambiar el nombre de su servidor tendrá que generar y obtener otro certificado. El ejemplo de la figura 4.7 muestra el

[33] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003

nombre de Internet con el que este servidor será conocido, para este caso escogimos “ctg.gov.ec”.

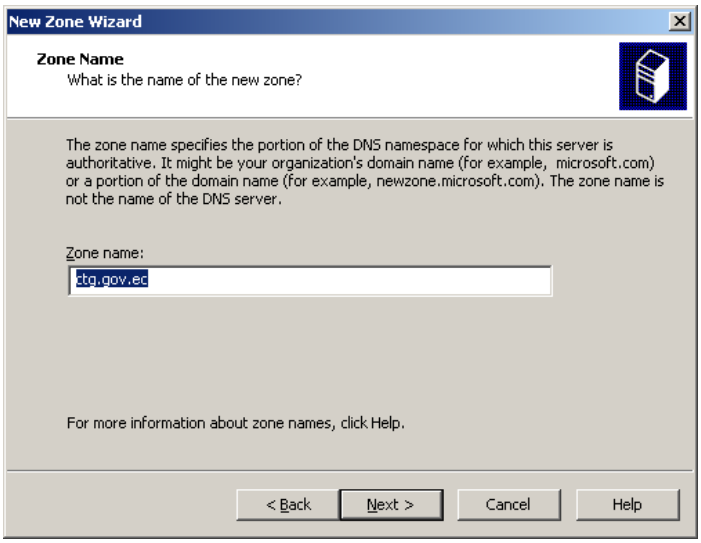



Figura 4.7 Ventana de Configuración de nombre de dominio[34]

**Paso 5:** Todo DNS maneja los datos de la zona que administra en un archivo que se almacena localmente en un disco duro del servidor. Para efectos de recordar de qué zona es el archivo que se está manejando, el wizard propone como nombre de almacenamiento el mismo nombre DNS del servidor web con la extensión “.dns”. Es recomendable dejarlo así como el asistente sugiere. Ver figura 4.8.

[34] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003

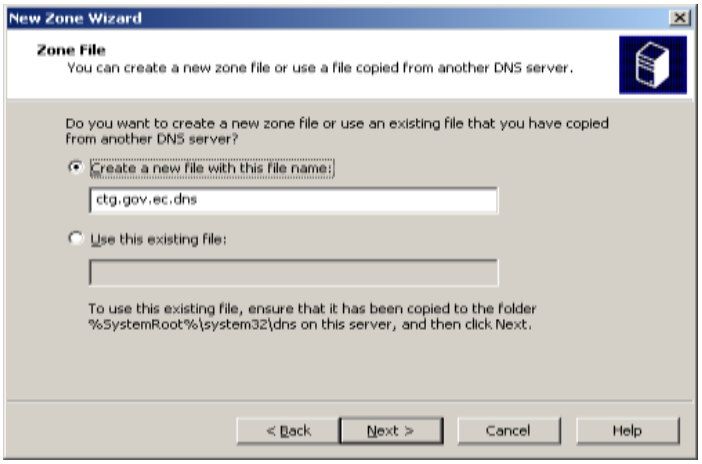



Figura 4.8 Configuración del Archivo de almacenamiento de datos del DNS[35]

**Paso 6:** Un servidor DNS puede tener múltiples maneras de actualización pero por razones de seguridad no es conveniente que se actualice de cualquier fuente que se encuentre en la red interna o en el Internet y que pueda significar permitir a intrusos tomar control del servidor y causar daños, por lo tanto lo más recomendable es no permitir actualizaciones dinámicas tal cual muestra la figura 4.9.

[35] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003

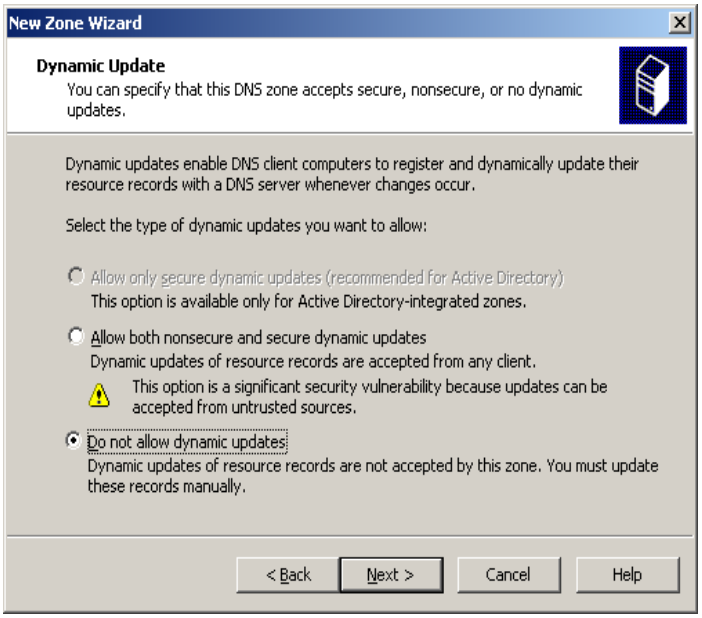



Figura 4.9 Configuración de Actualizaciones dinámicas[36]

**Paso 7:** Una vez que hemos creado nuestro DNS podemos hacer una prueba utilizando el comando "PING" para ver si la dirección IP del servidor quedó asociada al mombre o calificativo de Internet que le asignamos en pasos anteriores. Para esto vaya a "START" luego "RUN" y escriba "PING www.ctg.gov.ec" y deberá obtener una respuesta como en la figura 4.10.

[36] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003

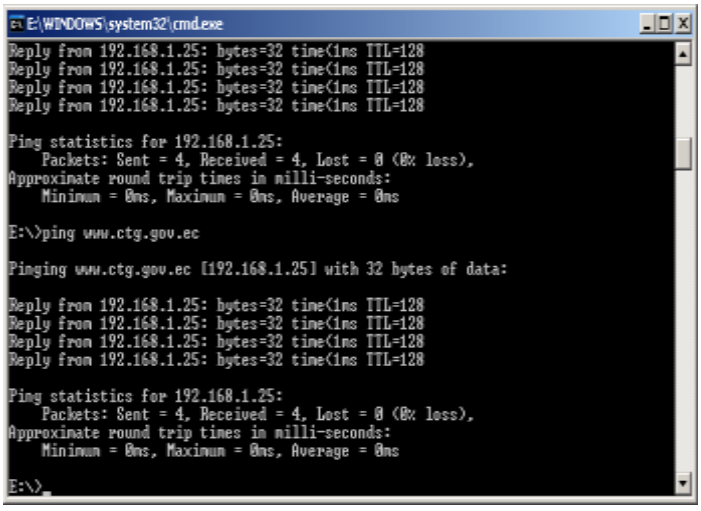



Figura 4.10 Ventana de Comando DOS[37]

#### 4.2.1.2 Creación de un Certificado Local.

El primer paso es crear un certificado inicial en el IIS para luego pasarlo a una entidad autorizada de creación de certificados y firmarlo digitalmente para ser usado posteriormente. Aquí detallamos los pasos para crear el certificado base o inicial generado en el mismo servidor:

**Paso 1:** Escoja el nombre del Sitio Web que va a funcionar en este servidor tal como muestra el ejemplo de la figura 4.11.

[37] FUENTE: Ventana de Comandos de DOS

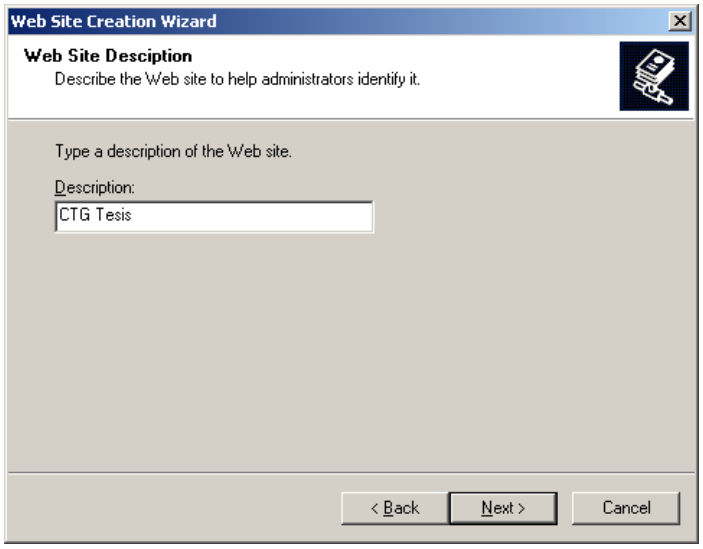



Figura 4.11 Configuración del nombre del sitio web[38]

**Paso 2:** Tal cual muestra la figura 4.12, usted deberá seleccionar una dirección IP para el servidor donde funcionará el sitio web que en este caso toma por defecto la asignada en la configuración de red para el servidor. Luego pregunta por el puerto TCP que atenderá las peticiones de quien quiera acceder al sitio el cual debería dejarse como muestra por defecto en 80 que es el que normalmente se usa cuando se navega por Internet. Luego hay que poner el nombre de dominio de Internet que le hemos asignado al

[38] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003

servidor el cual debería ser el mismo que se configuró en la parte de DNS anteriormente.

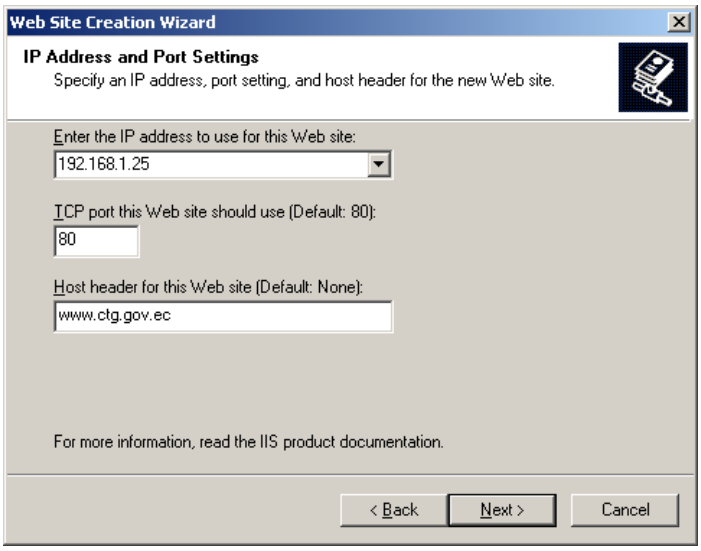



Figura 4.12 Configuración de la dirección IP para el sitio web[39]

**Paso 3:** Todo sitio web debe tener físicamente una ruta en el disco duro donde se almacenarán las páginas, scripts, gráficos y demás archivos que formarán parte del mismo, para esto, usted deberá seleccionar la carpeta donde va a almacenar toda esta información. La figura 4.13 muestra un ejemplo de la selección de una ruta para el sitio y adicionalmente pregunta si usted desea que el acceso a esa ruta en la Internet sea accesible anónimamente o si en su defecto se requiere

[39] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003

autentificación para poder hacerlo. Todo depende de las necesidades de cada administrador pero generalmente un sitio web debería ser accesible por todos así que la opción de que los anónimos puedan ver el sitio estándar debería estar habilitada.

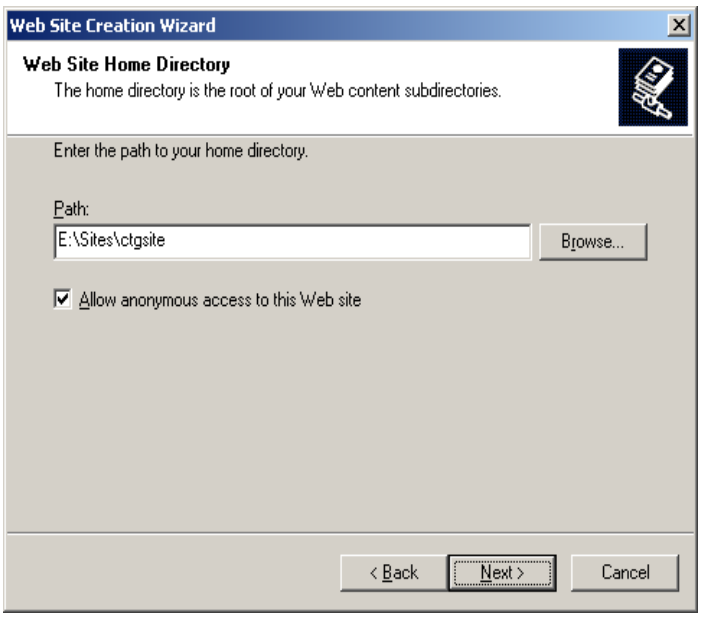



Figura 4.13 Configuración de la ruta de almacenamiento del sitio web[40]

**Paso 4:** La siguiente pantalla que se muestra en la figura 4.14 sirve para empezar la creación del certificado a nivel del servidor local.

[40] FUENTE: Servidor Web de Herramientas Administrativas de Windows Serwver 2003


Figura 4.14 Ventana inicial para la creación del certificado[41]

**Paso 5:** Existen varias opciones para instalar un certificado en el servidor web como muestra la figura 4.15 pero en este caso lo que interesa es crear uno nuevo porque el sitio web también es nuevo.

[41] FUENTE: Internet Informations Services

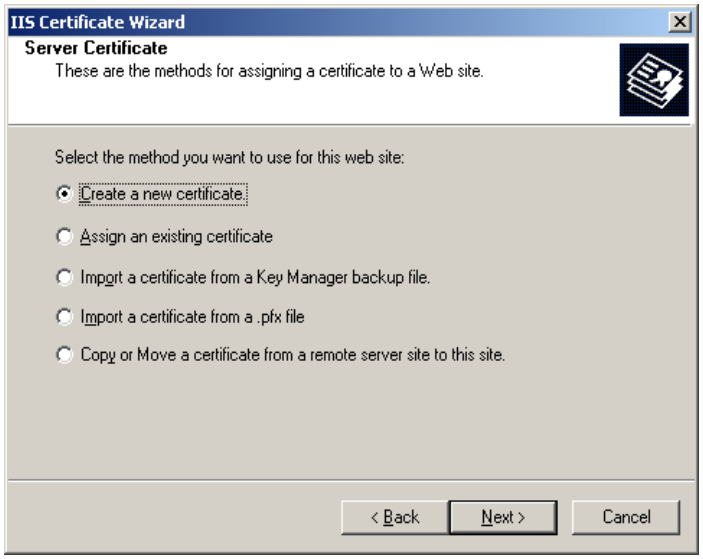



Figura 4.15 Opciones para la instalación de un certificado[42]

**Paso 6:** Todo certificado debe estar asociado al nombre del sitio web al cual pertenece para su posterior firmado digital. Adicionalmente se debe escoger el nivel de cifrado para hacerlo más o menos fuerte en cuanto a su capacidad de inviolabilidad, sin embargo, tenga en cuenta que mientras más grande sea la longitud de bits que escoja para hacer el cifrado, usted sacrifica rendimiento pero gana mucho más en seguridad. Lo recomendado es usar una longitud de bits de 1024 bytes como muestra la figura 4.16.

[42] FUENTE: Internet Informations Services

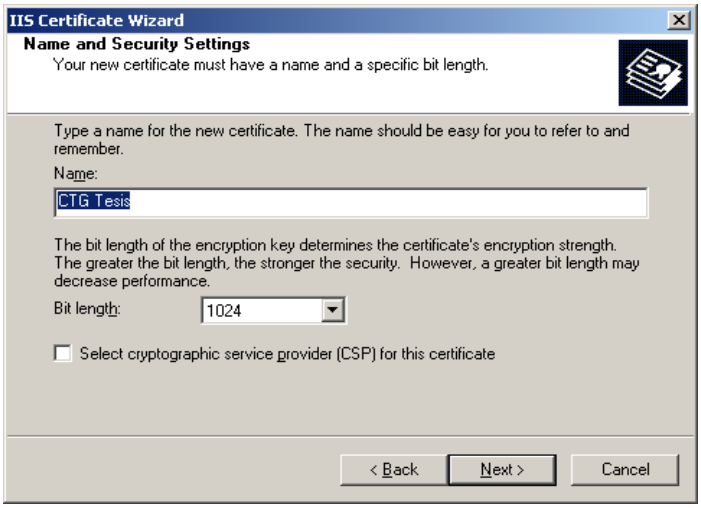



Figura 4.16 Asociación con nombre del sitio web[43]

**Paso 7:** La figura 4.17 muestra una pantalla que pide ingresar información adicional sobre la organización a la cual pertenece el certificado. Esto es importante ya que cuando alguien en Internet consulta a su certificado para ver la procedencia y a nombre de quién está firmado, los datos de la empresa u organización aparecen allí y es lo que generará la confianza del usuario a hacer transacciones seguras con usted. La organización es el nombre de su empresa y la unidad organizacional es el departamento de la empresa que solicita el certificado.

[43] FUENTE: Internet Informations Services

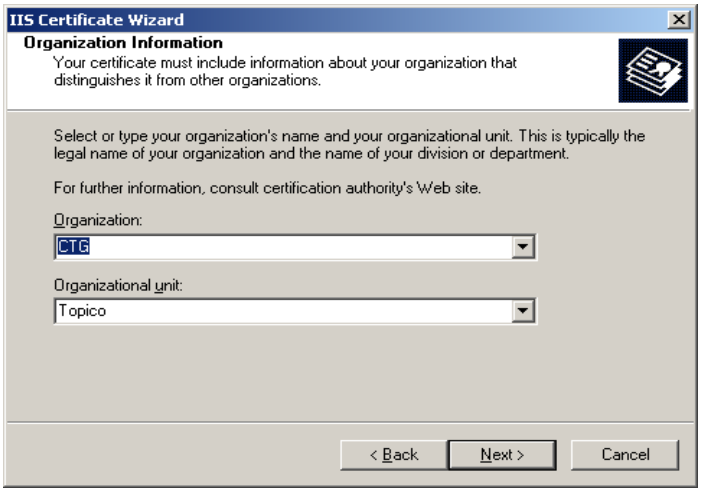



Figura 4.17 Configuración de información de la empresa dueña del certificado de seguridad[44]

**Paso 8:** La pantalla de la figura 4.18 nos indica que debemos ingresar el nombre calificado de Internet que le hemos asignado al servidor web. La creación de este nombre ya fue especificado en pasos anteriores.

[44] FUENTE: Internet Informations Services

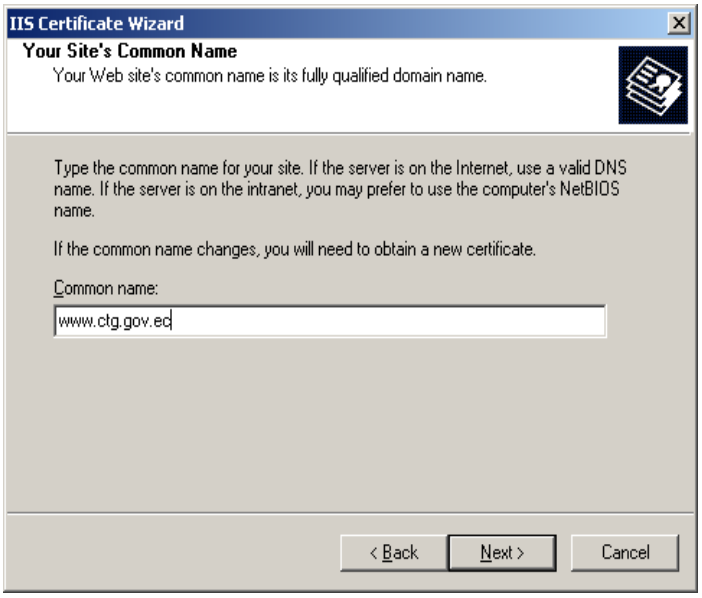



Figura 4.18 Asociación del nombre de dominio[45]

**Paso 9:** Al igual que en la figura 4.19, el certificado requiere de más información sobre quién solicita el certificado, en este caso es información geográfica de la ubicación del sitio web. La figura nos ilustra sobre como ingresar estos datos:

[45] FUENTE: Internet Informations Services

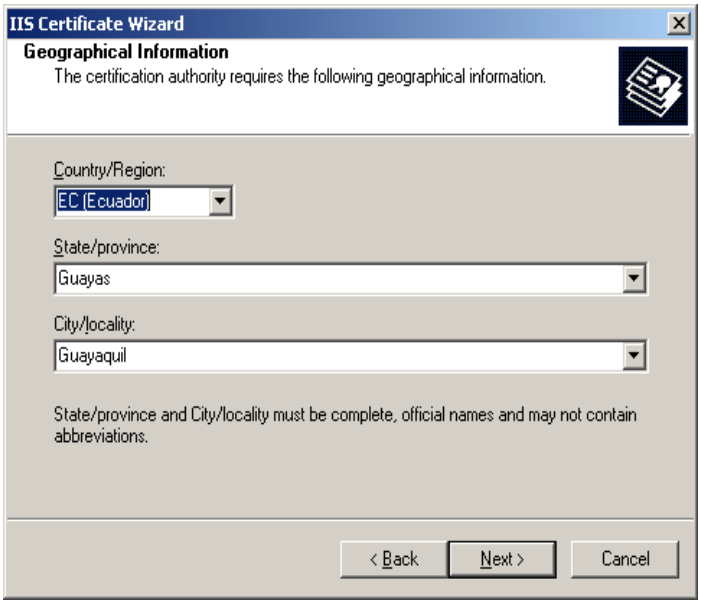



Figura 4.19 Configuración de información geogr.áfica del sitio web[46]

**Paso 10:** La figura 4.20 muestra una pantalla con la ruta donde usted desea almacenar el certificado a nivel local de su servidor que está creando. Una vez hecho esto se grabará en el disco duro un certificado local y ahora puede proceder a firmarlo digitalmente conectándose con una compañía emisora de certificados autorizada.

[46] FUENTE: Internet Informations Services

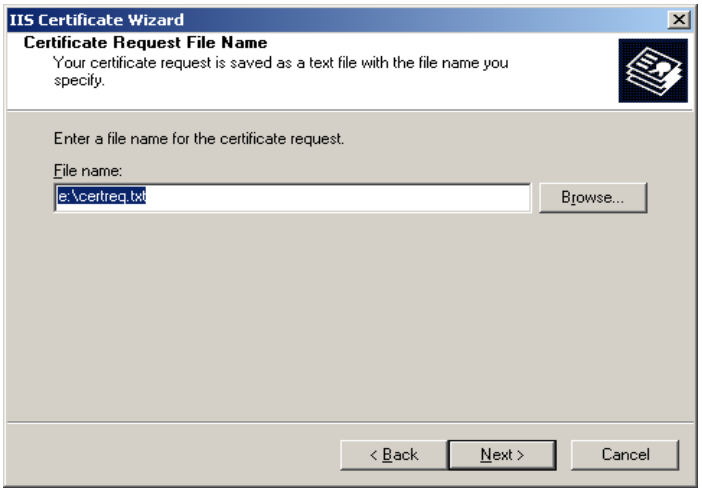



Figura 4.20 Configuración de la ruta de almacenamiento del certificado de seguridad[47]

### 4.2.1.3 Firma Digital del Certificado

Como se indicó anteriormente, es necesario que el certificado local sea firmado digitalmente por una compañía emisora de certificados autorizada. Para este servidor web se escogió a la compañía THAWTE INC. (http://www.thawte.com). A continuación se datallan los pasos para firmar digitalmente el certificado que fue generado localmente en el servidor:

**Paso 1:** Al visitar el sitio web de Thawte, usted encontrará entre las opciones del menú una para emitir certificados gratis por un tiempo limitado sólo

[47] FUENTE: Internet Informations Services

para efectos de prueba. Eso esta en el menú “trial” → “Free trial certificate” lo cual lo llevará a una pantalla que le preguntará datos acerca de usted y su sitio web. Proceda a llenar toda la información como se muestra en la figura 4.21 y asegúrese que todo lo que ingresa en esta página sea fidedigna porque una vez generada la firma digital ya no hay marcha atrás.

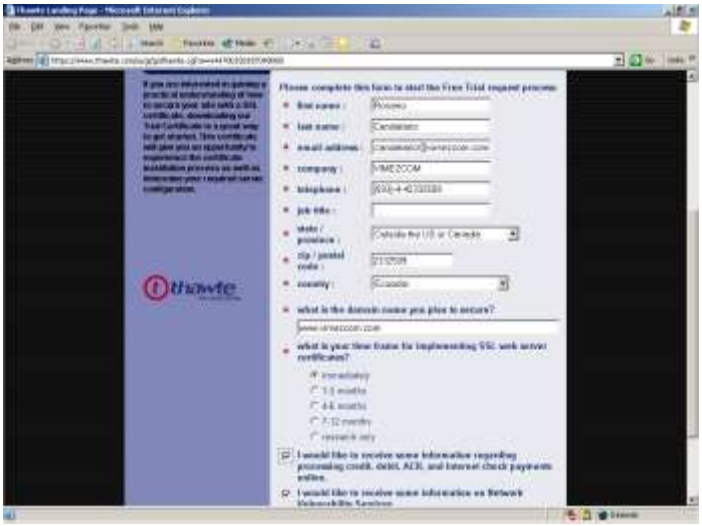


Figura 4.21 Configuración de información del sitio y de la empresa[48]

**Paso 2:** Al poner Siguiente (next) en la pantalla anterior, Thawte mostrará una pantalla previa a la firma de su certificado a fin de generar posteriormente el

[48] FUENTE : sitio web de Thawte http://www.thawte.com

certificado raíz final ya firmado digitalmente para su sitio web. Esta pantalla le informa acerca de qué es un certificado raíz, como funciona y cómo generarlo. Una vez que haya leído esta información haga click en el botón “NEXT” como muestra la figura 4.22.

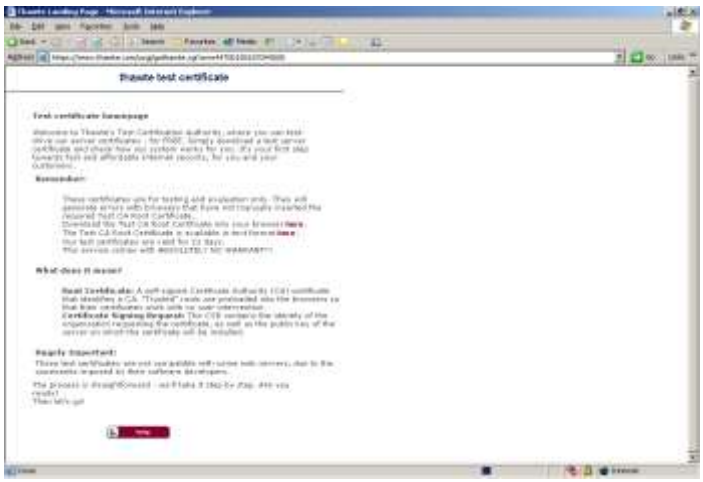



Figura 4.22 Ventana informativa del certificado [49]

**Paso 3:** En esta parte usted deberá buscar el archivo donde generó el certificado local en su disco duro, paso que realizamos antes de ingresar a Thawte.com. Por favor abra este archivo y luego haga un copiar y pegar en la parte inferior de la pantalla como muestra la figura 4.23. Debe incluir el contenido

[49] FUENTE : sitio web de Thawte http://www.thawte.com

del archivo que está entre las líneas “BEGIN NEW CERTIFICATE REQUEST” y “END NEW CERTIFICATE REQUEST” inclusive, es decir, estas dos etiquetas también deberán ser copiadas y pegadas. Una vez realizado esto se hace click en el botón “NEXT” y Thawte firmará digitalmente su certificado el cual se mostrará en la pantalla y usted deberá almacenar en su disco duro con la extensión “.CER”

Figura 4.23 Configuración final para la firma del certificado[50]

**Paso 4:** Regrese al IIS luego de que el certificado fue exitosamente firmado y el servidor le indicará que hay una solicitud de firma de certificado

[50] FUENTE : sitio web de Thawte http://www.thawte.com

pendiente por lo cual le presente dos alternativas, procesar e instalar un certificado ya firmado o eliminar el requerimiento que está pendiente. Como usted ya ha firmado el certificado que estaba pendiente deberá escoger que desea que se procese tal como muestra la figura 4.24.

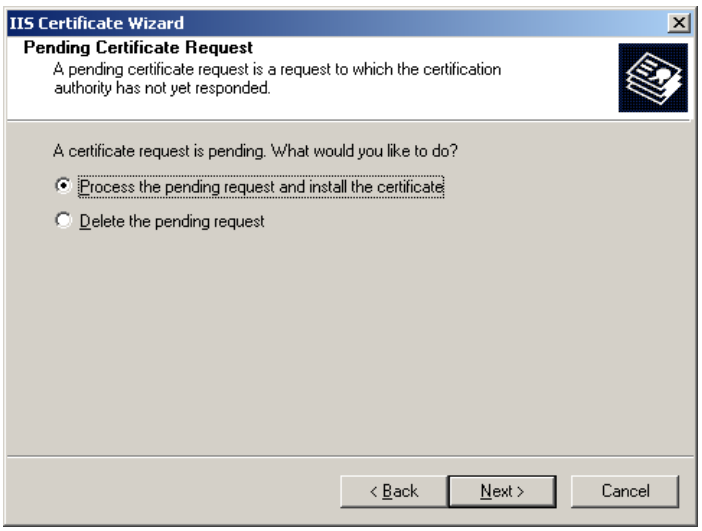



Figura 4.24 Configuración del certificado firmado en el IIS[51]

**Paso 5:** Al hacer click en el botón "NEXT" de la pantalla anterior, el IIS le preguntará dónde usted almacenó el archivo del certificado ya firmado con la extensión ".CER" que usted grabó cuando Thawte firmó su certificado y le pidió que lo guarde en su disco duro. Ubique el archivo como

[51] FUENTE: Internet Informations Services

en la figura 4.25 y después haga click en el botón "NEXT".

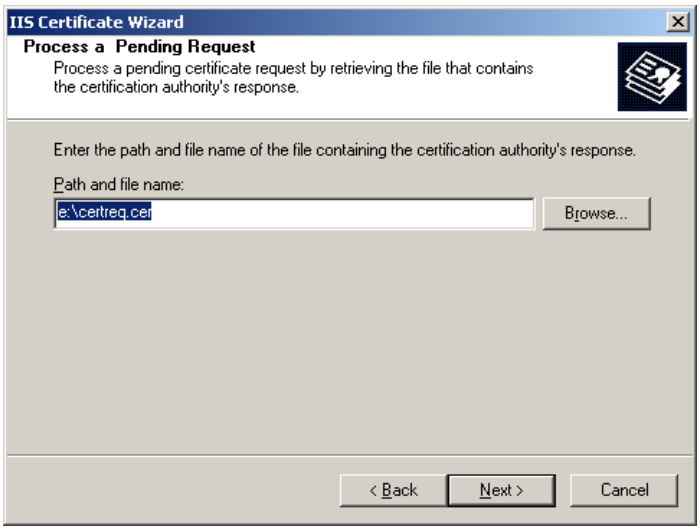



Figura 4.25 Asociación de la ruta de almacenamiento del certificado firmado[52]

**Paso 6:** Si el certificado es válido para el IIS (él hace una comprobación interna de esta situación) le pedirá que ingrese el puerto TCP donde los requerimientos para obtener una conexión segura de su sitio web serán escuchados y de esa manera usar SSL junto con su certificado para que las transacciones se hagan de manera cifrada y le de a su web la seguridad que necesita. (Observar Figura 4.26)

[52] FUENTE: Internet Informations Services

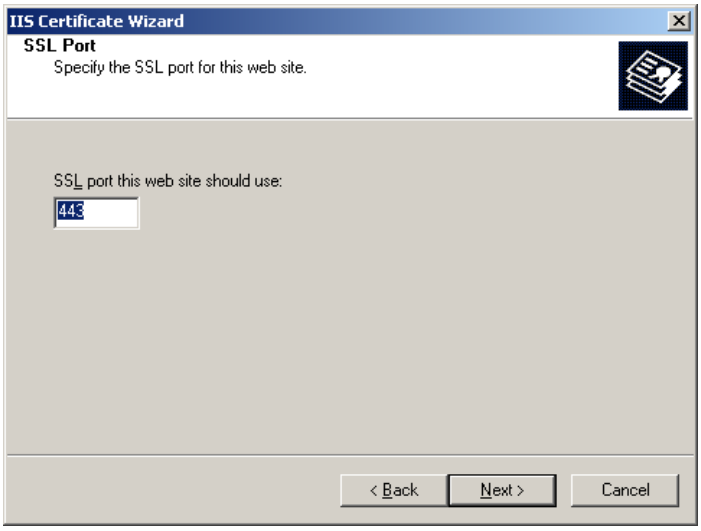



Figura 4.26 Configuración del puerto TCP[53]

**Paso 7:** Finalmente se le mostrará una pantalla como en la figura 4.27 en donde usted podrá ver la información detallada de su certificado y un último botón "NEXT" para instalarlo en su servidor web. Una vez instalado habrá una pantalla final que no se muestra en donde le informará que el certificado se instaló con éxito y que presione el botón de TERMINAR (FINISH).

[53] FUENTE: Internet Informations Services

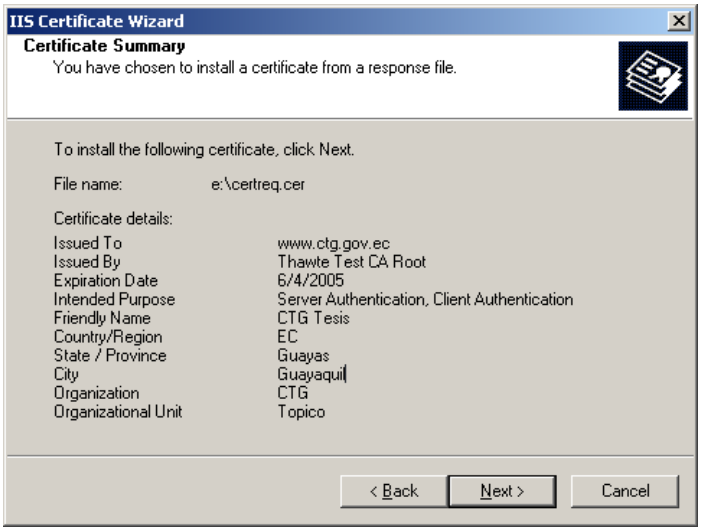



Figura 4.27 Ventana informativa del certificado firmado[54]

## 4.3 Sistema Operativo

Para la configuración de la seguridad del sistema operativo se ha tomado referencia el texto mostrado.[55]

1. Instalar todas las revisiones de seguridad (en inglés) es decir el último parche actualizado. Una de las prácticas más adecuadas, fundamental consiste en estar al día en lo que se refiere a las revisiones de seguridad más recientes.

2. Una vez instaladas estas actualizaciones, se debe desactivar todos los servicios del sistema operativo que no sean necesarios. Ésta es también

[54] FUENTE: Internet Informations Services

[55] FUENTE : http://www.microsoft.com/spanish/msdn/articulos/archivo/140303/voices/openhack.asp

otra de las prácticas más adecuadas en todo momento. Al desactivarse estos servicios, se pueden liberar recursos del sistema y reducir el área de la superficie expuesta a los ataques. Los servicios específicos que se pueden desactivar dependen de las necesidades de cada solución concreta. Messenger, Alerter y ClipBook son sólo algunos ejemplos.

3. A continuación, se debe realizar las pruebas apropiadas para asegurarse de que la aplicación puede funcionar perfectamente sin ellos. Por último, se debe desactivar estos servicios cambiando su estado de inicio a desactivado.

4. También se debe utilizar el Editor del Registro (Regedit.exe) para cambiar cuatro valores del registro con el fin de aumentar la seguridad. Todos ellos se recomiendan como prácticas más adecuadas, siempre que no se necesiten las funciones que se están desactivando.

**Crear valor de registro: nolmhash**

Ubicación: HKLM\System\CurrentControlSet\Control\LSA

Objetivo: evita que el sistema operativo almacene las contraseñas de usuarios en formato hash LM. Este formato en realidad sólo se utiliza con los clientes de Windows 3.11 que no admiten NTLM o Kerberos. El peligro de crear y conservar este hash LM radica en que si un atacante consigue descifrar las contraseñas almacenadas de esta

manera, podrá volver a utilizar dichas contraseñas en otros equipos de la red.

**Crear valor de registro: NoDefaultExempt**

Ubicación: HKLM\System\CurrentControlSet\Services\IPSEC

Objetivo: de manera predeterminada, IPSec permitirá que el tráfico entrante cuyo puerto de origen sea 88 pueda consultar al servicio IPSec acerca de información sobre cómo conectar con el equipo, independientemente de las directivas IPSec que haya establecido. Al definir este valor, no se permitirá ninguna comunicación entre los puertos excepto las que permitan los filtros de IPSec que se hayan configurado, como se describe en la sección Directivas IPSec.

**Crear valor de registro: DisableIPSourceRouting**

Ubicación:

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

Objetivo: evita que los paquetes TCP determinen explícitamente la ruta hacia el destino final, requiriendo que el servidor determine la mejor ruta. Se trata de un nivel de protección frente a ataques a través de intermediarios, en los que el atacante dirige los paquetes a través de sus servidores, los cuales investigan el contenido a medida que éste los atraviesan.

**Crear valor de registro: SynAttackProtect**

Ubicación:

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

Objetivo: esta clave protege al sistema operativo de ciertos ataques mediante inundación de paquetes SYN limitando los recursos asignados a las solicitudes entrantes. Es decir, esto ayuda a bloquear los intentos de utilizar solicitudes de paquetes SYN, o de sincronización, entre un cliente y el servidor para realizar ataques de negación de servicio.

Además, aunque no está directamente relacionado con la prevención de ataques, se activaron varios registros de auditoría que cubrieran los eventos de inicio y de fin de sesión, la administración de cuentas, el cambio de directivas y los eventos del sistema.

**Directivas de Estándares de Seguridad IP (IPSec)**

A partir de Windows 2000, Microsoft permite administrar la autenticación y el cifrado del tráfico de protocolo de Internet (IP) mediante los estándares de seguridad IP (IPSec), una extensión del protocolo IPv4. La figura 4.28 que aparece a continuación muestra la directiva predeterminada correspondiente al cuadro de diálogo Server (Request Security).

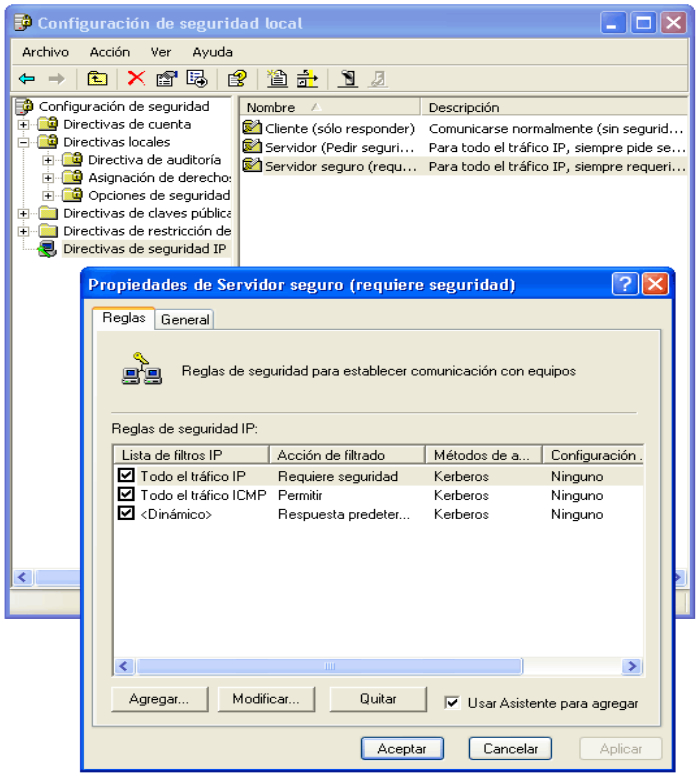



Figura 4.28. Cuadro de diálogo Server (Request Security)[56]

Las reglas IPSec se configuraron utilizando el complemento MMC (Microsoft Management Console) de configuración de seguridad local (anterior). Estas directivas tuvieron un importante papel en la implementación y la protección de las comunicaciones permitidas entre servidores OpenHack. Estas reglas nos han permitido implementar la práctica más adecuada del menor privilegio:

- Obligando a que todo el tráfico necesario para ejecutar y administrar la aplicación se especifique de manera explícita y única en la directiva IPSec de cada sistema.

[56] FUENTE: http://www.microsoft.com/spanish/msdn/articulos/archivo/140303/voices/openhack.asp

- Haciendo que las comunicaciones entre sistemas se autentiquen mediante certificados.
- Obligando a que las comunicaciones con fines administrativos se autentiquen mediante certificados y se cifren.
- Denegando todo el tráfico que no esté expresamente permitido para la aplicación o la administración del sistema, incluyendo el tráfico ICMP e IP (la regla "denegar de forma predeterminada").

Las reglas IPSec tienen tres componentes principales: el filtro que identifica el tráfico que va a tratar IPSec, la acción que hay que llevar a cabo cuando el filtro detecta este tráfico y el mecanismo de autenticación que se utilizará para establecer una asociación de seguridad. Si dos sistemas que están intentando comunicarse no tienen reglas que identifiquen el tráfico, así como un mecanismo de autenticación común entre ellos, no podrán establecer una conexión.

El primer paso para bloquear la solución mediante IPSec es conocer perfectamente las rutas de comunicación entre los diferentes sistemas para poder generar los filtros IPSec adecuados. Es necesario permitir que el servidor Web se comunique con la base de datos; el servidor de acceso remoto debía permitir a los administradores utilizar una red privada virtual (VPN) para tener acceso al segmento de administración de la red; el servidor de administración debía conceder a los clientes VPN la posibilidad de crear

sesiones de cliente de Servicios de Terminal Server de Windows 2003 (éstos permiten tener acceso a aplicaciones que se estén ejecutando en el escritorio de un equipo remoto), así como tener acceso y copiar archivos en los recursos compartidos del servidor de administración; todos los sistemas tenían que permitir que el servidor de administración pudiese generar una sesión de Servicios de Terminal Server para su interfaz privada; por último, todos los sistemas tenían que tener acceso a determinados recursos compartidos de archivos del sistema de administración. Una vez que la conectividad necesaria entre los sistemas se planeó en función de cada puerto, se crearon filtros IPSec en cada uno de los diferentes sistemas.

A continuación, hubo que determinar cómo se trataría el tráfico cuando lo identificasen los filtros del sistema. Para OpenHack 4, se definieron las cuatro posibles acciones que se podrían llevar a cabo (denominadas "acciones de filtros"):

- Bloquear el tráfico.
- Permitir el tráfico.
- "Autenticar y firmar": autentica el origen del tráfico mediante certificados y establece una asociación de seguridad mediante firma de paquetes.

- "Autenticar, firmar y cifrar": autentica el origen del tráfico mediante certificados y establece una asociación de seguridad mediante cifrado y firma de paquetes.

La regla de bloquear sencillamente retira el paquete. Esta regla funciona como la regla "denegar de manera predeterminada", es decir, "si no se ha permitido expresamente el tráfico, no se debe permitir". La regla de permitir consiente el tráfico independientemente del origen. Se utilizó para permitir el acceso público a la aplicación Web.

Aunque para la autenticación del tráfico mediante certificados fue necesario generar y distribuir certificados IPSec desde una autoridad de certificados (CA) común, mejoró notablemente la integridad de la capacidad de los sistemas de comunicarse con seguridad. Hay que señalar que se utilizó una autoridad de certificados independiente. Una vez otorgados todos los certificados, se retiró la autoridad de certificados de la red. Si la autoridad de certificados ya no es necesaria en el momento de la producción, es sin duda aconsejable hacerlo así, es otra buena manera de reducir el área de la superficie de la solución.

Mediante los certificados IPSec, se pudo comprobar la identidad de los sistemas de origen y destino, incluyendo los administradores remotos que tenían acceso al servidor de acceso remoto. IPSec procesa las reglas dando

mayor prioridad a las reglas más específicas. Por tanto, todos los sistemas comenzarán con las dos reglas siguientes:

- Bloquear todo el tráfico IP.
- Bloquear todo el tráfico ICMP.

A continuación, se generaron las reglas específicas de cada sistema. A las comunicaciones entre el servidor Web y el servidor de la base de datos se les asignó una acción de filtro "Autenticar y firmar"; a las comunicaciones con el servidor de administración se les asignó una acción de filtro "Autenticar, firmar y cifrar"; asimismo, se estableció un acceso público al sitio Web para que se pudiera tener acceso a él.

## 4.4 Base De Datos

### 4.4.1 Configuración de Perfiles de Usuarios

Para configurar los perfiles de los usuarios que accesarán a la base de datos se debe ingresar como usuario DBA a la base de datos como se muestra a continuación en la figura 4.29.

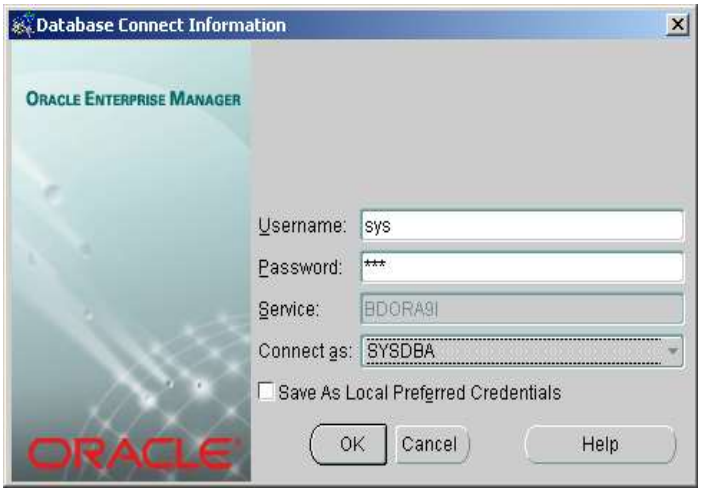



Figura 4.29 Logón para la Conexión a la Base de Datos[57]

Para proteger los datos de intrusos se ha creado un usuario, el mismo que utilizaremos para realizar la conexión a la base de datos como se muestra en la figura 4.30. Este usuario tiene permisos exclusivamente para consultar información de todas las tablas que conforman la opción de "Consulta en Línea" del Sitio Web, y se le restringió permisos de ingreso, actualización y borrado de datos.

[57] FUENTE: Motor de Oracle 9i

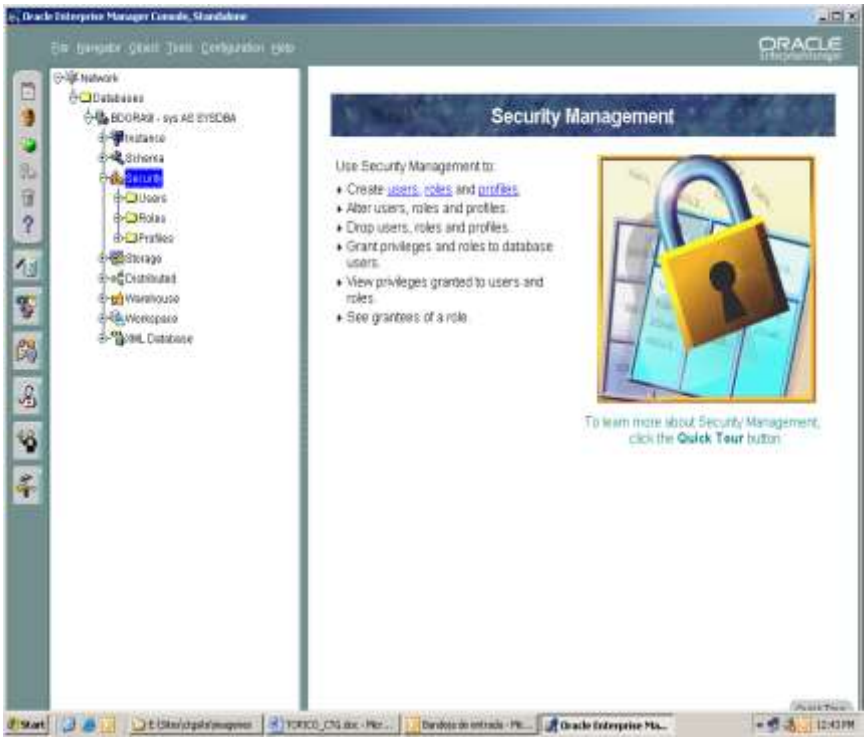



Figura 4.30 Opción para crear usuarios[58]

### 4.4.2 Consideraciones de Seguridad

- Para obtener información de la base de datos se está utilizando paquetes, los cuales son llamados desde la aplicación en Visual .NET.
- En el sitio web se realizó una opción para accesar a la información de la base de datos donde el usuario deberá colocar su identificación (número de cédula) y la contraseña (dada por la institución) para accesar a la opción “Consulta en Línea”, de este

[58] FUENTE: Motor de Oracle 9i

modo protegemos la privacidad de la información y sólo obtendrán acceso los usuarios que tengan licencia en la Comisión de Tránsito del Guayas.

- Internamente el logón que el usuario da para conectarse a la base de datos desde el sitio web junto con la contraseña la cual será enviada encriptada al momento de verificar si tiene acceso o no a la opción “Consulta en Línea” del sitio web.

# CAPITULO 5

## 5. POLITICAS DE SEGURIDAD

### 5.1 ¿Qué son las Políticas de Seguridad?

Políticas de seguridad son los documentos que describen, principalmente, la forma adecuada de uso de los recursos de un sistema de cómputo, las responsabilidades y derechos tanto de usuarios como administradores, describe lo que se va a proteger y lo que se esta tratando de proteger. Las políticas son parte fundamental de cualquier esquema de seguridad eficiente.[59]

### 5.2 Importancia para una Compañía

Encontramos muy importante la aplicación de políticas en una empresa por los siguientes puntos[60]:

[59] FUENTE: http:// www.isaca.org/art6a.htm
[60] FUENTE: http://www.monografias.com/trabajos11/seguin/seguin.shtml

- **Porque aseguran la aplicación correcta de las medidas de seguridad con la ilusión de resolver los problemas de seguridad expeditamente**. Una empresa necesita de documentación sobre políticas, definiciones de responsabilidades, directrices, normas y procedimientos para que se apliquen las medidas de seguridad, los mecanismos de evaluación de riesgos y el plan de seguridad. Las políticas y una estimación preliminar de los riesgos son el punto de partida para establecer una infraestructura organizativa apropiada, es decir, son los aspectos esenciales desde donde se derivan los demás.

- **Porque guían el proceso de selección e implantación de los productos de seguridad.**

  La mayoría de las organizaciones no tiene los recursos para diseñar e implantar medidas de control desde cero. Por tal razón a menudo escogen soluciones proporcionadas por los fabricantes de productos de seguridad y luego intentan adaptar esos productos a las políticas, procedimientos, normas y demás esfuerzos de integración dentro de la organización. Esto se realiza a menudo sin conocer o entender suficientemente los objetivos y las metas de seguridad. Como resultado, los productos de seguridad escogidos y su aplicación pueden no resultar adecuados a las verdaderas necesidades de la organización.

Las políticas pueden proporcionar la comprensión y la guía adicional que el personal necesita para actuar como desearía la gerencia en lo que a seguridad se refiere. De manera que tales políticas pueden ser una manera de garantizar de que se está apropiadamente seleccionando, desarrollando e implantando los sistemas de seguridad.

- **Por que demuestran el apoyo de la Presidencia y de la Junta Directiva.**

  La mayoría de las personas no está consciente de la gravedad de los riesgos relativos a la seguridad y por eso no se toma el tiempo para analizar estos riesgos a fondo. Además, como no tiene la experticia suficiente, no es capaz de evaluar la necesidad de ciertas medidas de seguridad. Las políticas son una manera clara y definitiva para que la alta gerencia pueda mostrar que:

  1. La seguridad de los activos de información es importante
  2. El personal debe prestar la atención debida a la seguridad.

  Las políticas pueden entonces propiciar las condiciones para proteger los activos de información. Un ejemplo muy frecuente involucra a los gerentes a nivel medio que se resisten a asignar dinero para la seguridad en sus presupuestos. Pero si las políticas que han sido emitidas por la Junta Directiva o la alta gerencia, entonces los gerentes a nivel medio no podrán continuar ignorando las medidas de seguridad.

- **Para evitar responsabilidades legales.**

  Se presentan cada vez más casos judiciales en los cuales se encuentra responsables a empleados, y particularmente a gerentes, de no actuar apropiadamente bien en lo referente a seguridad informática. La razón puede ser atribuida a: negligencia, violación de confianza, fallas en el uso de medidas de seguridad, mal práctica, etc. Estos casos se usan a menudo con éxito para llamar la atención de la gerencia y para lograr apoyo para los esfuerzos en seguridad informática.

- **Para lograr una mejor seguridad.**

  Uno de los problemas más importantes en el campo de seguridad informática representa los esfuerzos fragmentados e incoherentes. A menudo un departamento estará a favor de las medidas de seguridad, mientras que otro dentro de la misma organización se opondrá o será indiferente. Si ambos departamentos comparten recursos informáticos (por ejemplo una LAN o un servidor), el departamento que se opone pondrá en riesgo la seguridad del otro departamento y de la organización completa. Aunque no es ni factible ni deseable que todas las personas en una organización se familiaricen con las complejidades de la seguridad informática, es importante que todas ellas se comprometan con mantener algún nivel mínimo de protección. Las políticas pueden usarse para definir el nivel de esta protección mínima, a veces llamada línea de base.

## 5.3 Importancia de la Implementación para la CTG

- Debido a que la información y los equipos informáticos son recursos importantes y vitales no solo de la CTG sino también de la ciudadanía cuyos datos residen en la institución.
- Con la correcta aplicación de las políticas se pueden evitar o disminuir en gran medida riesgos tales como fraude, espionaje, violación de la privacidad, intrusos, hackers, interrupción del servicio, etc.
- Se concientiza al personal sobre la importancia de aplicar las políticas de seguridad y las consecuencias de la violación o no aplicación de las mismas.
- Se pueden evitar problemas legales por demandas debido a la violación de la privacidad de los datos personales.
- La implementación de políticas obliga a los responsables del diseño y aplicación de las mismas a actualizar contínuamente sus conocimientos sobre los riesgos y los recursos que se deben utilizar para combatirlos.

## 5.4 ¿Qué Datos se deben proteger en la CTG?

La información almacenada en la base de datos de la CTG proviene de diferentes fuentes y por lo tanto es primordial clasificarlos a fin de aplicar medidas de seguridad de acuerdo a su importancia, entre ellos tenemos los siguientes datos:

- Información de los vehículos, registro de matrículas, registro de licencias, registro de infracciones, y todas las transacciones realizadas diariamente.
- Reglamentos de la CTG.
- Contabilidad, Nómina, Inventarios, Cuentas por Cobrar y Cuentas por Pagar.
- Información Estadística.

## 5.5 Diseño de Políticas para la CTG

En la realización del diseño de las políticas se tomó como referencia el manual de guia[61]. Antes de describir las políticas es necesario establecer los entes que deberían ser responsables de la seguridad en la CTG.

Se recomienda crear un Comité de Seguridad Informática compuesto por los representantes de los distintos departamentos de la CTG, así como por el Director de Informática, el Jefe de Telecomunicaciones, y el abogado o representante legal de la CTG. Este comité estará encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a la seguridad en Informática y Telecomunicaciones. También será responsable

[61] FUENTE: http:// www.monografias.com/trabajos11/seguin/seguin.shtml

de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres.

En los anexos 2, 3 y 4 se incluyen como ejemplo de implementación de políticas de seguridad las siguientes:

- Polícas de seguridad para el uso y el acceso de Información.
- Políticas de seguridad para la utilización de recursos informáticos.
- Políticas de seguridad para las comunicaciones
- Políticas de seguridad para redes.

Los empleados serán responsables de cumplir con todas las políticas de seguridad expuestas en los anexos.

# CONCLUSIONES

El propósito de este proyecto realizado para la Comisión de Tránsito de la Provincia del Guayas es el siguiente:

1. Implementar un sitio web que permita dar información de deudas, de trámites e información general de la institución.

2. Aplicación de políticas de seguridad al sitio y por ende a la institución, algo que cada organización debe generar, como es la privacidad de la información, el acceso a la información, autenticación de los usuarios y administración de la red.

# RECOMENDACIONES

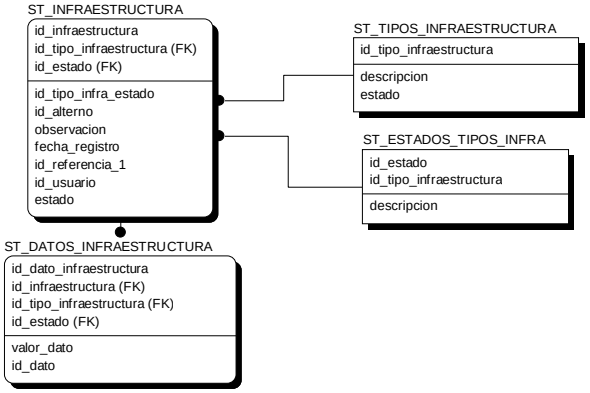
Las configuraciones de Seguridad que se han implementado en el Sitio web no son para ser establecidas una sóla vez en la vida, se deben revisar objetivamente cada 6 o 12 meses y realizar los ajustes necesarios en beneficio de la información.

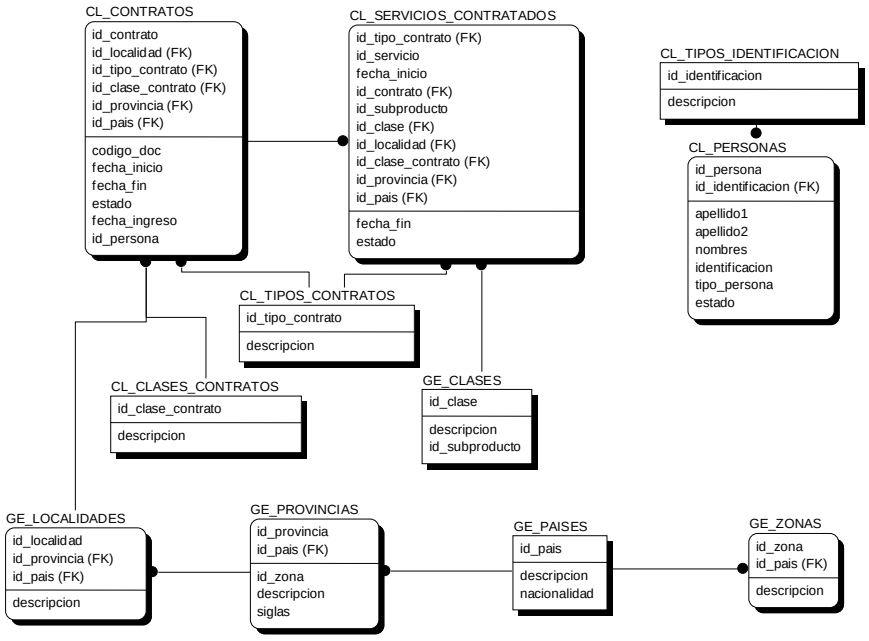
Cabe recalcar que así como las amenazas a la seguridad y la tecnología nunca se detienen, el aprendizaje de los empleados involucrados tampoco debe estancarse. Se debe promover la formación en seguridad, lo cual podría hacerse ofreciendo entrenamiento al personal, asistiendo a conferencias o trayendo al lugar de trabajo educadores externos de seguridad.

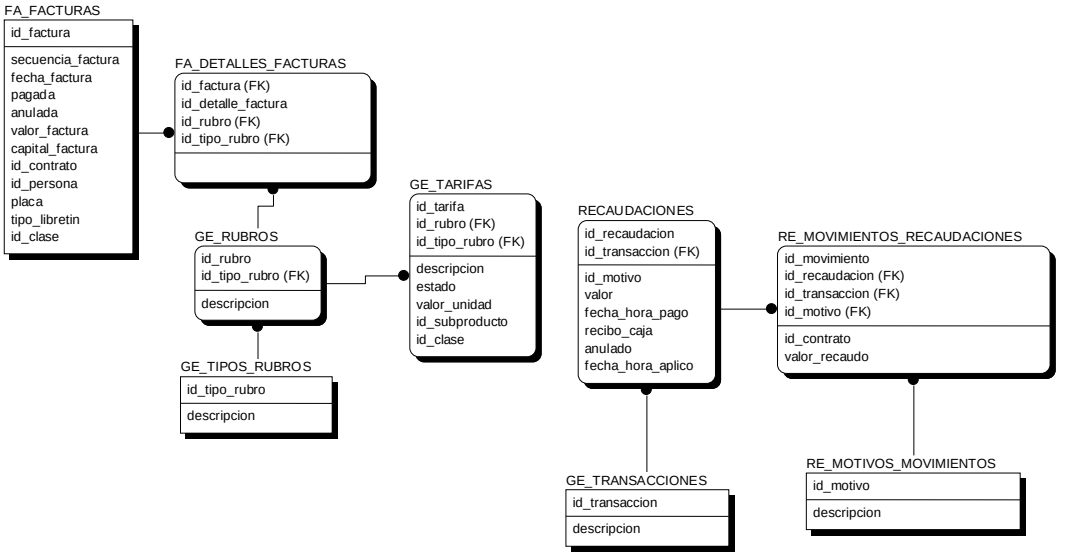
# ANEXOS

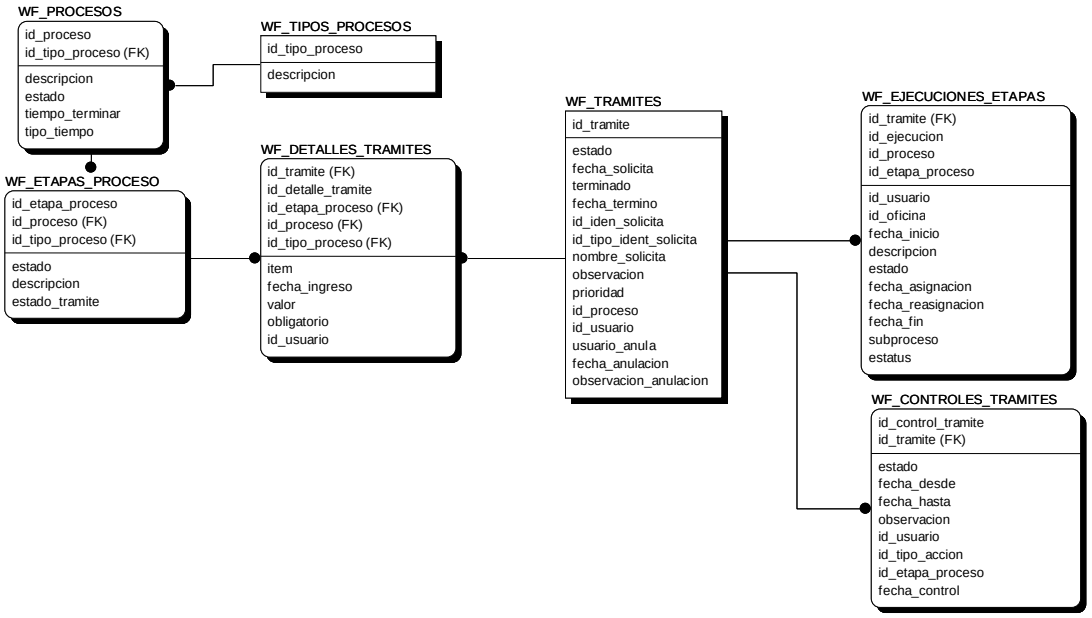
# ANEXO 1

# DISEÑO DE LA BASE DE DATOS




FA_FACTURAS
id_factura
secuencia_factura
fecha_factura
pagada
anulada
valor_factura
capital_factura
id_contrato
id_persona
placa
tipo_libretin
id_clase
FA_DETALLES_FACTURAS
id_factura (FK)
id_detalle_factura
id_rubro (FK)
id_tipo_rubro (FK)
GE_RUBROS
id_rubro
id_tipo_rubro (FK)
descripcion
GE_TIPOS_RUBROS
id_tipo_rubro
descripcion
GE_TARIFAS
id_tarifa
id_rubro (FK)
id_tipo_rubro (FK)
descripcion
estado
valor_unidad
id_subproducto
id_clase
RECAUDACIONES
id_recaudacion
id_transaccion (FK)
id_motivo
valor
fecha_hora_pago
recibo_caja
anulado
fecha_hora_aplico
GE_TRANSACCIONES
id_transaccion
descripcion
RE_MOVIMIENTOS_RECAUDACIONES
id_movimiento
id_recaudacion (FK)
id_transaccion (FK)
id_motivo (FK)
id_contrato
valor_recaudo
RE_MOTIVOS_MOVIMIENTOS
id_motivo
descripcion


WF_PROCESOS
id_proceso
id_tipo_proceso (FK)
descripcion
estado
tiempo_terminar
tipo_tiempo
WF_TIPOS_PROCESOS
id_tipo_proceso
descripcion
WF_ETAPAS_PROCESO
id_etapa_proceso
id_proceso (FK)
id_tipo_proceso (FK)
estado
descripcion
estado_tramite
WF_DETALLES_TRAMITES
id_tramite (FK)
id_detalle_tramite
id_etapa_proceso (FK)
id_proceso (FK)
id_tipo_proceso (FK)
item
fecha_ingreso
valor
obligatorio
id_usuario
WF_TRAMITES
id_tramite
estado
fecha_solicita
terminado
fecha_termino
id_iden_solicita
id_tipo_ident_solicita
nombre_solicita
observacion
prioridad
id_proceso
id_usuario
usuario_anula
fecha_anulacion
observacion_anulacion
WF_EJECUCIONES_ETAPAS
id_tramite (FK)
id_ejecucion
id_proceso
id_etapa_proceso
id_usuario
id_oficina
fecha_inicio
descripcion
estado
fecha_asignacion
fecha_reasignacion
fecha_fin
subproceso
estatus
WF_CONTROLES_TRAMITES
id_control_tramite
id_tramite (FK)
estado
fecha_desde
fecha_hasta
observacion
id_usuario
id_tipo_accion
id_etapa_proceso
fecha_control

# ANEXO 2

# POLITICAS DE SEGURIDAD PARA EL USO Y ACCESO DE INFORMACION

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas.
- No divulgar información confidencial de la CTG a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la CTG a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la CTG.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la CTG y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

# ANEXO 3

# POLÍTICAS DE SEGURIDAD PARA UTILIZACION DE RECURSOS INFORMATICOS

- Los computadores de la CTG sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
- Los equipos de la CTG sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática.
- No se permite fumar, comer o beber mientras se está usando un PC.
- Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.
- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la CTG se requiere una autorización escrita.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.
- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad.
- Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.
- Si un PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
- No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la CTG.
- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la CTG está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
- Los usuarios no deben copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de la CTG, sin la aprobación previa de la gerencia.
- No pueden extraerse datos fuera de la sede de la CTG sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan computadoras portátiles o están conectados a redes como Internet.
- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente

peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

- Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos.
- Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la CTG.
- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.
- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Informática.
- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.
- No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la CTG a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
- Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba

de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de CTG debe guardarse en otra sede, lejos del edificio.

- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).
- La información de la CTG clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Gerencia de Informática.
- No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.
- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.
- Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad.

Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la CTG.

- No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la CTG.
- El personal que utiliza un computador portátil que contenga información confidencial de la CTG, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

# ANEXO 4

# POLÍTICAS DE SEGURIDAD PARA LAS COMUNICACIONES

## Políticas de Propiedad de la información

- Con el fin de mejorar la productividad, la CTG promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la CTG y no propiedad de los usuarios de los servicios de comunicación.

## Políticas para el Uso de los Sistemas de Comunicación

- Los sistemas de comunicación de la CTG generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la CTG.
- Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la CTG y en tal sentido deben usarse las horas no laborables.

## Políticas de Confidencialidad y Privacidad

- Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que esté cifrada. Para tal fin debe utilizarse Outolook, Outlook Express u otros productos previamente aprobados por la Gerencia de Informática.
- Los empleados y funcionarios de la CTG no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La CTG se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.
- Es política de la CTG no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoría. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.
- De manera consistente con prácticas generalmente aceptadas, la CTG procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

**Política de Reenvío de Mensajes**

- Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la CTG, se debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la CTG sin la debida aprobación.

**Política de Borrado de Mensajes**

- Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

# ANEXO 5

# POLÍTICAS DE SEGURIDAD PARA REDES

## Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la CTG al estar conectada a redes de computadoras.

## Alcance

Esta política se aplica a todos los empleados, contratistas, consultores y personal temporal de la CTG.

## Aspectos generales

Es política de la CTG prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

### Políticas de Modificaciones

- Todos los cambios en la central telefónica (PABX) y en los servidores y equipos de red de la CTG, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y

debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

**Políticas de Cuentas de Usuarios**

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.
- No debe concederse una cuenta a personas que no sean empleados de la CTG a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
- Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo

más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

- Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix no deben entrar inicialmente como "root", sino primero empleando su propio ID y luego mediante "set userid" para obtener el acceso como "root". En cualquier caso debe registrarse en la bitácora todos los cambios de ID.
- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.
- Cuando un empleado es despedido o renuncia a la CTG, debe desactivarse su cuenta antes de que deje el cargo.

**Políticas de Contraseñas y el Control de Acceso**

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o

substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

- Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.
- Para el acceso remoto a los recursos informáticos de la CTG, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.

- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).
- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la CTG, pudiendo ser causal de despido.
- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
- Los archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

- Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

# BIBLIOGRAFIA


1. http://www.monografias.com
2. http://www.thawte.com
3. http://www.microsoft.com
4. http://www.oracle.com
5. http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGSO00.htm#Políticas
6. http://www.microsoft.com/windowsserver2003/evaluation/features/guidedtour/default.mspx
7. http:// www.isaca.org/art6a.htm
8. http:// www.monografias.com/trabajos11/seguin/seguin.shtml

# GLOSARIO DE TÉRMINOS

**CORTAFUEGOS (FIREWALL):**

Sistema (o router) diseñado para manejar de forma segura la conexión entre la red interna protegida y redes inseguras, públicas o sub-redes de la propia empresa. FTP: Protocolo de Transferencia de Activos (File Transfer Protocol). Método estándar para mover Activos de gran volumen usando Internet. FTP utiliza una arquitectura Cliente/Servidor en la que los usuarios pueden cargar y descargar Activos de Información.

**DIRECCIÓN IP (IP ADDRESS)**

La dirección física de un sistema Internet, expresada en el formato siguiente: xxxx.xxxx.xxxxx.xxxxx. Cada sistema tiene una única dirección IP.

**GATEWAY:**

Referido al contexto de la interconexión de redes se asimila a un Router.

**INTERNET:**

Red de comunicaciones mundial basada en el protocolo TCP/IP y originalmente fundada por la Agencia de Proyectos de Investigación Avanzados de la Defensa, la cual es parte del Departamento de Defensa de los EE.UU. Internet ha aceptado recientemente el tráfico de operaciones comerciales y de negocio.

**ROUTER:**

Es un procesador de redes interconectadas que encamina paquetes de datos entre dos, o más, redes conectadas. El router IP encamina datagramas entre redes directamente conectadas o adyacentes.

**SERVIDOR FTP ANÓNIMO (ANONYMOUS FTP SERVER):**

Un sistema de Internet que permite el acceso público a Activos disponibles y su transferencia mediante FTP. IP: Protocolo Internet (Internet Protocol). El nivel de red requerido para conectarse con Internet.

**TCP/IP:**

Protocolo de Control de Transmisión/Protocolo Internet (Transmission Control Protocol/Internet Protocol). El protocolo de comunicaciones original de Internet y su espina dorsal. Es el más utilizado en el mundo de las comunicaciones y fue desarrollado bajo las directrices del Departamento de Defensa de los EE.UU.

**TELNET:**

Una aplicación que sirve para conectarse a Sistemas que, a su vez, están conectados a Internet. SERVIDOR TELNET: Aquel que permite el acceso Telnet.

**WWW (WORLD WIDE WEB):**

También llamado Web o W3. Una aplicación Internet cliente/servidor que permite a los usuarios navegar por Internet usando documentos de hipertexto. Requiere un cliente llamado popularmente 'browser'.