ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UNA INFRAESTRUCTURA DE CLAVES PÚBLICAS JERÁRQUICA CON CERTIFICADOS DIGITALES X.509 Y SU APLICACIÓN EN REDES 802.11 CON EL ESTÁNDAR 802.1X

TOMO II

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

SHIRMA DAYUMA ORTIZ BOADA

DIRECTOR: ING. PABLO HIDALGO

Quito, Octubre de 2006

ÍNDICE DE CONTENIDO

TOMO I

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 6

ANEXOS

GLOSARIO DE ACRÓNIMOS

Capítulo 5

SOLUCIÓN PARA UNA RED LAN INALÁMBRICA SEGURA CON EAP-TLS

5. SOLUCIÓN PARA UNA RED LAN INALÁMBRICA SEGURA CON EAP-TLS

En este capítulo se presenta una solución para la implementación de seguridad en redes inalámbricas utilizando el protocolo EAP-TLS como mecanismo para el intercambio de credenciales digitales dentro del proceso de autenticación; para la emisión de certificados digitales se utiliza la PKI diseñada en el capítulo anterior.

5.1. GENERALIDADES DE LA SOLUCIÓN CON EAP-TLS

EAP-TLS provee autenticación mutua entre cliente y servidor con un alto nivel de seguridad mediante el uso de certificados digitales, por lo tanto necesita una infraestructura que permita administrar los certificados; su implementación demanda de una inversión superior a la requerida por otras soluciones de seguridad para WLANs, por lo que su uso es recomendable en dos tipos de escenarios:

- WLANs corporativas con gran número de usuarios.
- WLANs donde se requiera un alto nivel de seguridad.

EAP-TLS debe implementarse dentro de un dominio; para su implementación se requieren los siguientes elementos:

- Una AC-SUB por sucursal o área[1].
- Un AP (*Access Point*) compatible con 802.1x, por cada 150 m^2 (aproximadamente).
- Un servidor RADIUS compatible con 802.1x.

[1] La AC subordinada emite certificados digitales para los usuarios y el servidor.

- NICs compatibles con 802.1x.
- *Software* cliente compatible con EAP-TLS.

5.2. DESCRIPCIÓN DEL PROBLEMA

La inseguridad inherente a los medios inalámbricos se torna crítica en empresas con un gran número de usuarios móviles o en organizaciones que transmiten por sus redes datos sensibles; en estos casos, se debe implementar mecanismos que provean un alto nivel de escalabilidad y seguridad.

Para adaptar la solución planteada a un ambiente real, de la misma manera que en el capítulo anterior, se enfoca la implementación en un entorno empresarial, esto es, se toma como modelo la empresa ficticia ACSW.

Perfil General de la Empresa ACSW	
Característica	**Descripción**
	La empresa ACSW está dedicada a la investigación y desarrollo de nuevos productos.
Directrices	La información transmitida a través de sus WLANs está relacionada con datos de clientes y socios, estrategias comerciales, propiedad intelectual de carácter industrial y hasta patentes.
Valor de la Información	Sobre el 20% del capital total de la Empresa.
Usuarios WLAN que manejan información crítica.	Sobre el 20% del total de usuarios.
Servicios de Seguridad requeridos	Comunicaciones seguras a través de la WLAN, éstas deben garantizar: - Privacidad de la Información que se transmite a través de la WLAN. - Integridad de la Información que se transmite a través de la WLAN. - Autenticación de la Información que se transmite a través de la WLAN. - Autenticación de los usuarios que acceden a la WLAN.
Número de Sucursales	Mínimo 2.

Tabla 5.1 Perfil General de la Empresa ACSW

La solución EAP-TLS con una PKI jerárquica es ideal para redes corporativas con un perfil general semejante al expuesto en la tabla 5.1, pues esta solución brinda un alto nivel de seguridad, proporcionando escalabilidad mediante la implementación de una AC subordinada por sucursal como se muestra en la figura 5.1.

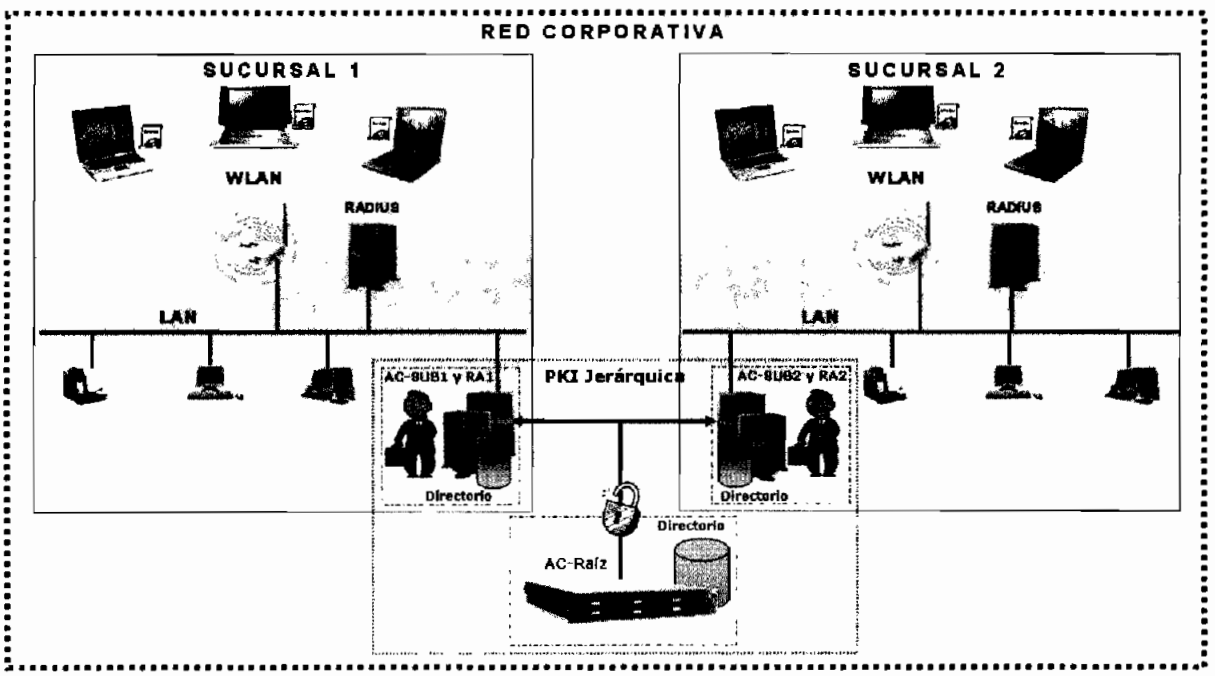


Figura 5.1 Red Corporativa Típica para una Implementación EAP-TLS

Esta solución se adapta perfectamente dentro de organizaciones con 2 o más áreas estratégicas; sin embargo, se puede aplicar también en empresas con una sucursal, pues proporciona flexibilidad ante una expansión de la organización.

Es importante considerar el área de cobertura de la red; ésta puede requerir de uno o más APs como se muestra en la figura 5.2. En espacios con poca interferencia y diseñados con estructuras modulares un AP puede cubrir hasta 150 m^2. El incremento del número de APs dentro de la WLAN no implica aumento en el número de servidores, a menos que el esquema funcional de la organización así lo requiera.

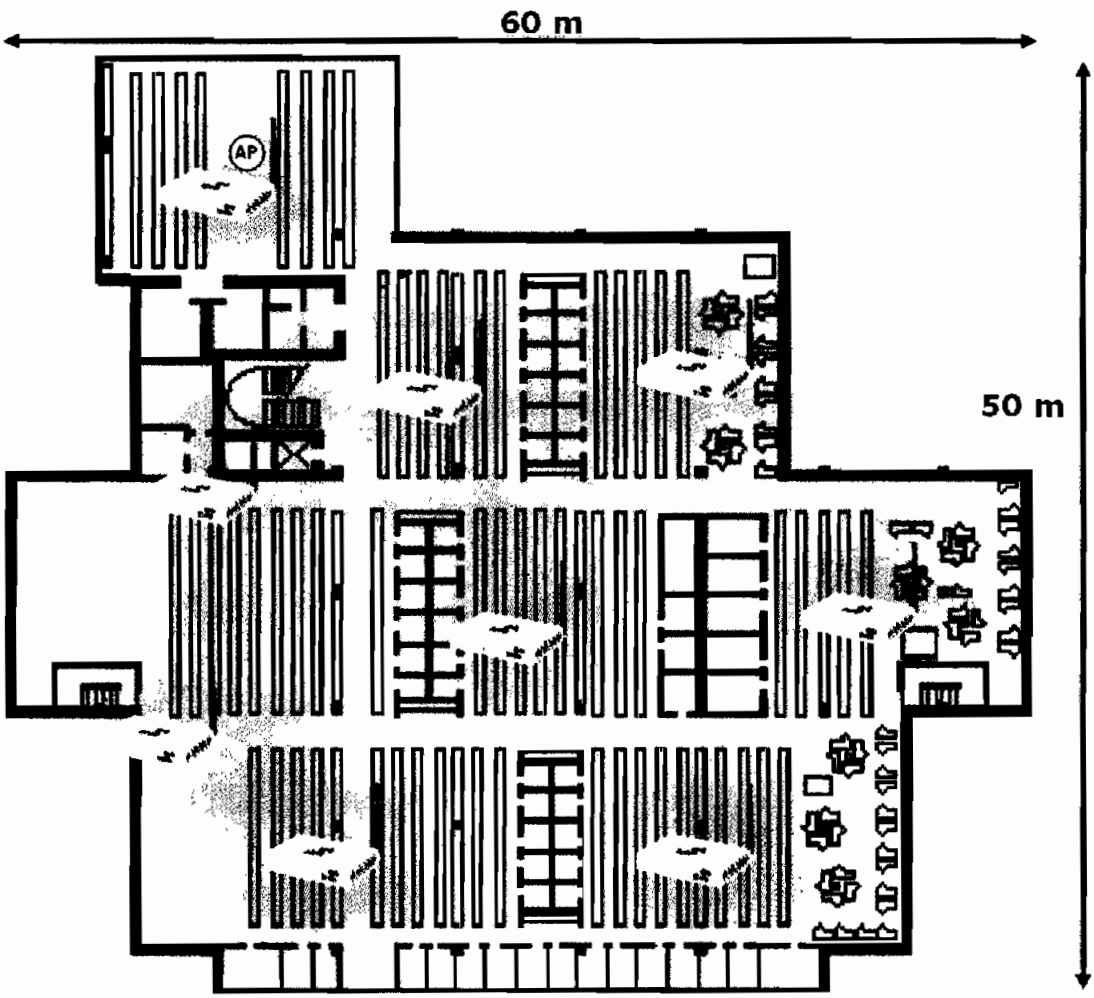


Figura 5.2 Área WLAN

5.3. BOSQUEJO DE LA SOLUCIÓN

En la figura 5.3 se muestra un bosquejo general de la solución planteada, en el gráfico se incluye el servidor de certificados y el servidor RADIUS individualmente para distinguir la función que cada uno cumple dentro de la red.

Las características técnicas de cada elemento son las siguientes:

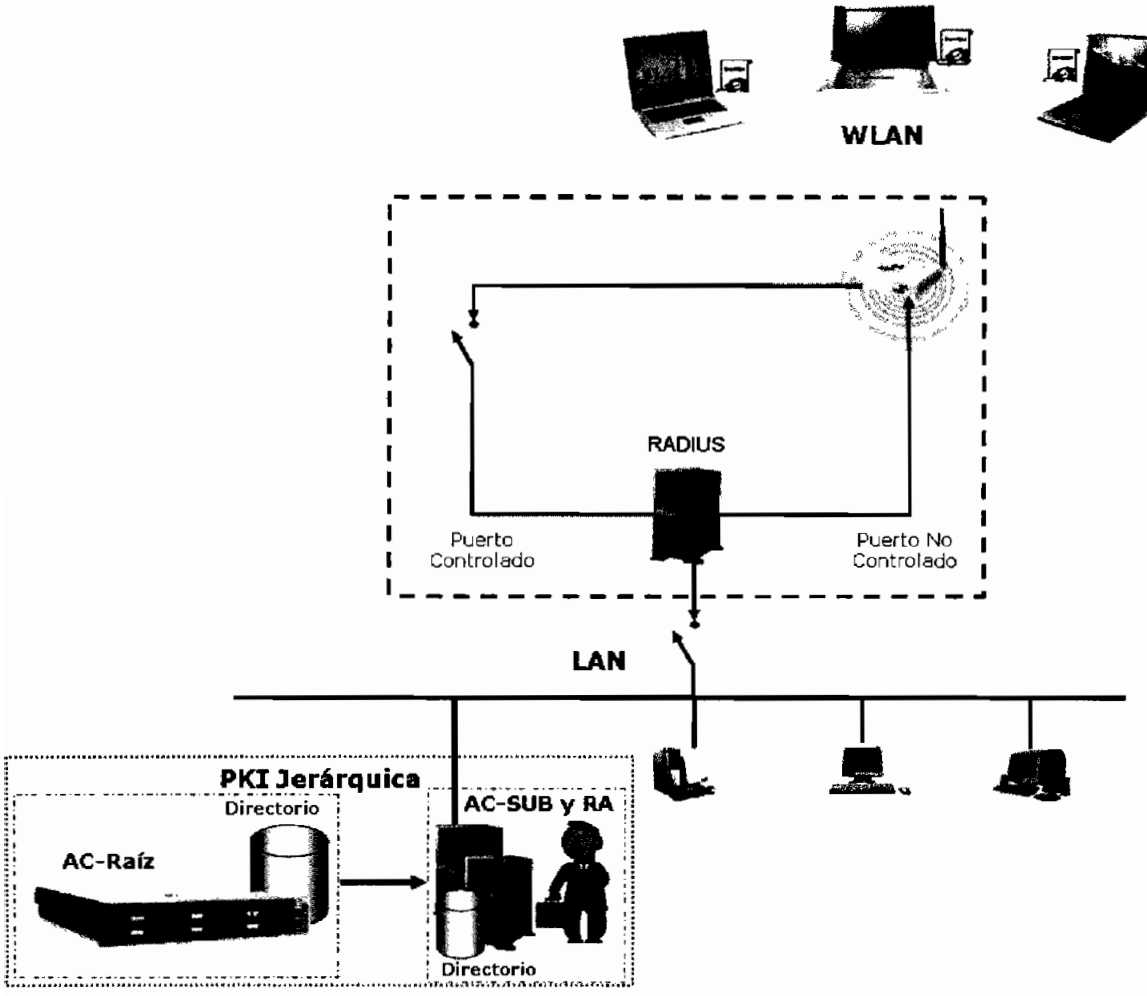


Figura 5.3 Esquema general: EAP-TLS

- **Servidor de Certificados**.- El servidor de certificados utiliza como plataforma el sistema operativo *Windows 2003 Server Enterprise*. Los certificados emitidos cumplen el estándar X509v3 y las CRLs están basadas en la versión 2 especificada en el estándar X509. Para el registro de los usuarios y el establecimiento de directivas se utiliza *Active Directory*.

- **AP**.- Por disponibilidad de equipos, para la implementación se utiliza el AP *3Com Office Connect Wireless 108 Mbps 11g PoE* mostrado en la figura 5.4, el cual soporta 802.1x. En la tabla 5.2 se especifican las características técnicas del AP.

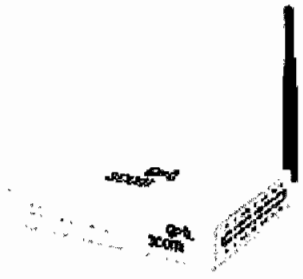


Figura 5.4 AP 3Com Office Connect Wireless 108 Mbps 11g PoE[1]

Característica	Descripción
Número de Antenas	Una antena dipolar omnidireccional.
Potencia de la señal	18 dBm (63.096 mW).
Estándares IEEE	802.11b y 802.11g.
Velocidad de transmisión máxima	Con 802.11g hasta 54 Mbps y en modo turbo hasta 108 Mbps.
Número de usuarios WLAN.	Hasta 64 por AP.
Características de seguridad	- WEP - WPA - 802.1x - Filtrado MAC

Tabla 5.2 Características del AP

- **Servidor RADIUS**.- Para la implementación se utiliza IAS (*Internet Authentication Service*), ésta es la solución proporcionada dentro de la plataforma *Windows 2003 Server*; IAS está basado en los RFCs 2865 y 2866.

  IAS provee los servicios de autenticación y control de acceso, soportando el uso de certificados digitales para la autenticación dentro de redes cableadas o inalámbricas. Para los procesos de autenticación utiliza por defecto el puerto UDP 1812.

- **NICs**.- Las tarjetas de red inalámbricas deben ser compatibles con 802.1x; dentro de la implementación no se utiliza un modelo o proveedor específico.

[1] http://www.3com.com/products/en_US/detail.jsp?pathtype=purchase&tab=features&sku=3CRGPOE10075.

- ***Software* cliente**.- Para la configuración en los clientes se utiliza el paquete proporcionado por *Juniper Networks*, OAC[1] v4.51. OAC soporta el manejo de certificados digitales para la autenticación EAP-TLS sobre plataformas *Windows XP/2000/98/Me*, siendo compatible con NICs fabricadas por diferentes proveedores; además, su interfaz es amigable para los usuarios.

  El paquete OAC ha sido seleccionado debido a que su versión OAC 4.51 se puede utiliza bajo la modalidad de *software* de prueba. Como alternativa se puede considerar el cliente *SecureConnect* de *Meetinghouse*, pero por el momento, la versión de prueba[2] de este *software* no está disponible; en otros casos las NICs WLAN poseen *software* especializado, como es el caso del ACU[3] de *Cisco*.

5.4. CONFIGURACIÓN DEL SERVIDOR RADIUS

Esta sección contiene todos los procedimientos necesarios para la implementación del servidor RADIUS para la autenticación EAP-TLS. Como se dijo en la sección anterior, se utilizará como servidor de acceso remoto a IAS, éste se configurará en el mismo servidor que la AC-SUB.

5.4.1. GRUPOS Y USUARIOS EN *ACTIVE DIRECTORY*

Se debe crear un grupo de seguridad relacionado con el servidor RADIUS, de esta manera solo un usuario miembro del grupo podrá autenticarse ante el servidor para

---

[1] *Odyssey Access Client.*

[2] El 29 de Julio de 2006, *Meetinghouse* fue adquirida por *Cisco Systems*, por el momento no se encuentra disponible la modalidad de prueba del *software* cliente *SecureConnect*. http://newsroom.cisco.com/dlls/2006/corp_081606.html.

[3] *Aironet Client Utility.*

establecer una comunicación por medios inalámbricos; esto permite una mejor administración de los usuarios WLAN.

5.4.1.1. Creación del Grupo de Seguridad

Para crear el grupo de seguridad se ingresa en **Usuarios y equipos de *Active Directory***; luego, se ingresa a la carpeta ***Users*** y en la barra de herramientas se da un clic sobre el botón **Crear un nuevo grupo en el contenedor actual** como se muestra en la figura 5.5.

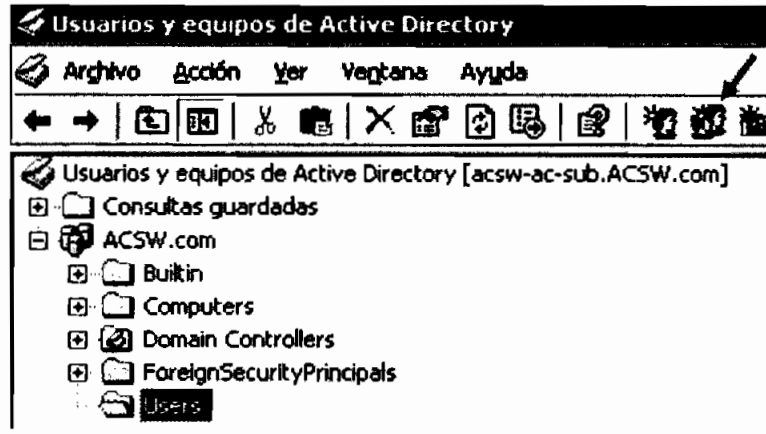


Figura 5.5 Creación del Nuevo Grupo

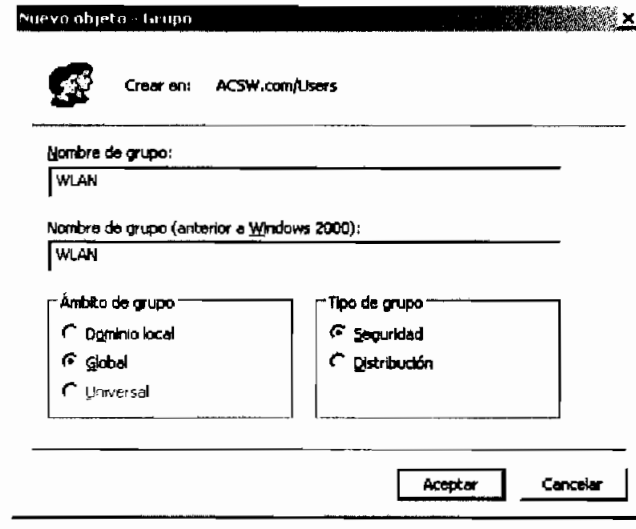


Figura 5.6 Propiedades del Nuevo Grupo

En la pantalla siguiente, se ingresa como nombre de grupo WLAN como se muestra en la figura 5.6 y se da un clic en **Aceptar**. El ámbito de grupo **Global** permite definir directivas para el control de los usuarios dentro del dominio *acsw.com*; por otra parte, el tipo **Seguridad** permite asignar permisos y privilegios a los usuarios del grupo para el acceso a los recursos dentro de la red.

5.4.1.2. Creación de un Perfil de Usuario

Se requiere crear un tipo de usuario miembro del grupo WLAN, éste servirá como plantilla para la creación de nuevos usuarios WLAN; para crear el usuario se realiza el procedimiento indicado en la sección Añadir Usuarios al Dominio del capítulo 4, estableciendo como nombre de usuario: Usuario_wlan.

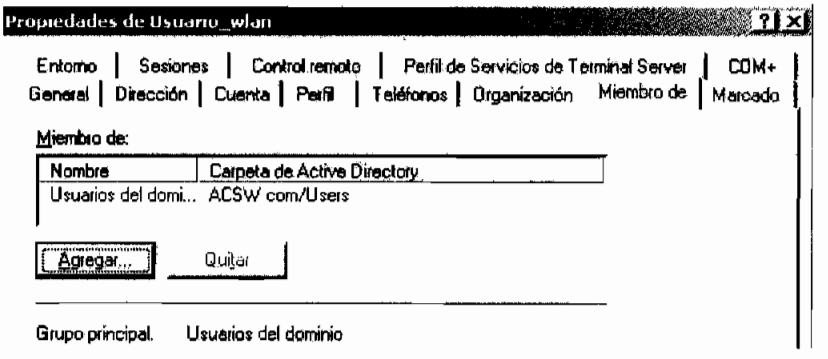


Figura 5.7 Miembro de en Propiedades de Usuario_wlan

Cuando el nuevo usuario ha sido creado, se da un clic con el botón derecho del *mouse* sobre éste y en el menú emergente se selecciona la opción **Propiedades**. En el cuadro de diálogo de propiedades, se selecciona la pestaña **Miembro de** como se muestra en la figura 5.7, ahí se da un clic en el botón **Agregar**.

En el cuadro de diálogo que se presenta se ingresa el nombre WLAN y se da un clic en el botón **Comprobar nombres**, si el nombre corresponde a un grupo existente,

éste es marcado como se muestra en la figura 5.8, cuando se ha terminado se da un clic en **Aceptar**.

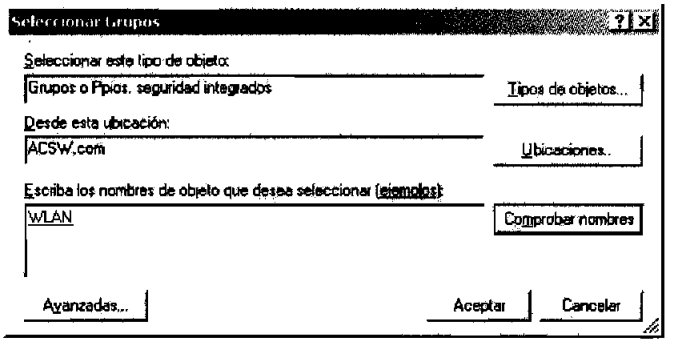


Figura 5.8 Inclusión del Nuevo Usuario en el Grupo WLAN

5.4.2. CONFIGURACIÓN DE ACTUALIZACIÓN AUTOMÁTICA DE LA INFORMACIÓN DE CERTIFICADOS PARA USUARIOS

Para que los usuarios WLAN puedan obtener información de la PKI de forma automática, se ingresa a **Usuarios y equipos de *Active Directory***, en el dominio *acsw.com* se da clic con el botón derecho del *mouse* y en el menú emergente se selecciona la opción **Propiedades**.

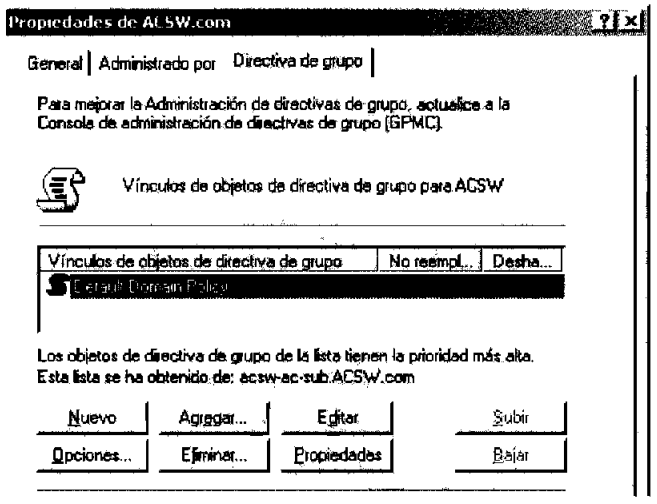


Figura 5.9 Directiva de Grupo

En la pantalla de propiedades se selecciona la pestaña **Directiva de Grupo** como se muestra en la figura 5.9, ahí se da un doble clic sobre ***Default Domain Policy*** o se da un clic sobre el botón **Editar** para ingresar en **Editor de objetos de directiva de Grupo**.

En el Editor de directivas dentro de la **Configuración del usuario** se selecciona la carpeta **Directiva de claves públicas** como se muestra en la figura 5.10 y en la parte derecha de la pantalla se da un doble clic sobre **Configuración de inscripción automática**.

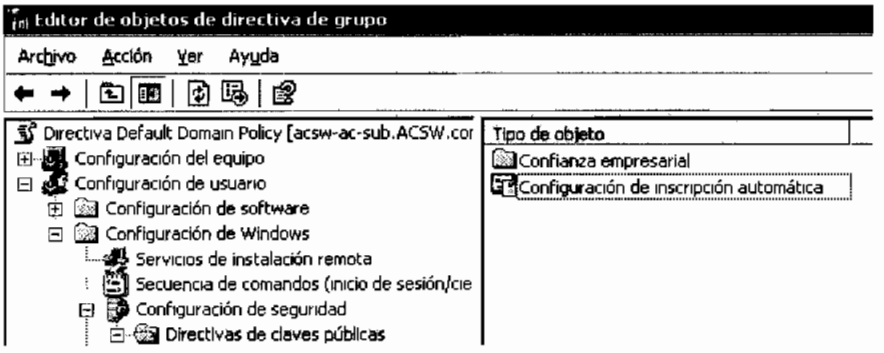


Figura 5.10 Editor de Objetos de Directiva de Grupo

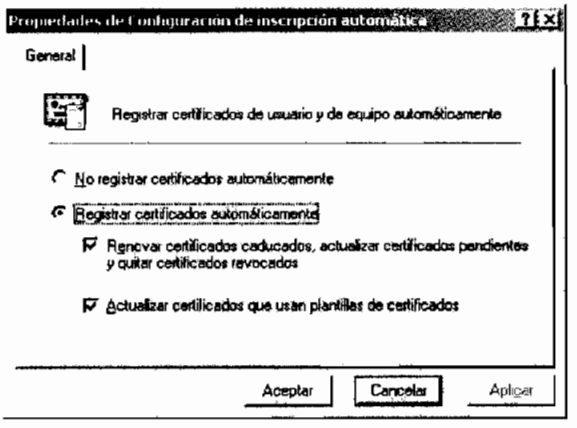


Figura 5.11 Registro de Certificados Automática

En el cuadro de diálogo que se presenta se activa la opción **Registrar certificados automáticamente** y luego se eligen las dos opciones permitidas como se muestra en la figura 5.11; finalmente se da un clic en **Aceptar**.

5.4.3. CONFIGURACIÓN DE DIRECTIVAS DE RED INALÁMBRICA

Para configurar las directivas de red inalámbrica dentro del dominio se ingresa al **Editor de objetos de directiva de Grupo**; en **Configuración del equipo** se da un clic con el botón derecho del *mouse* sobre la carpeta **Directiva de red inalámbrica** y en el menú emergente se selecciona la opción **Crear directiva de red inalámbrica** como se muestra en la figura 5.12.

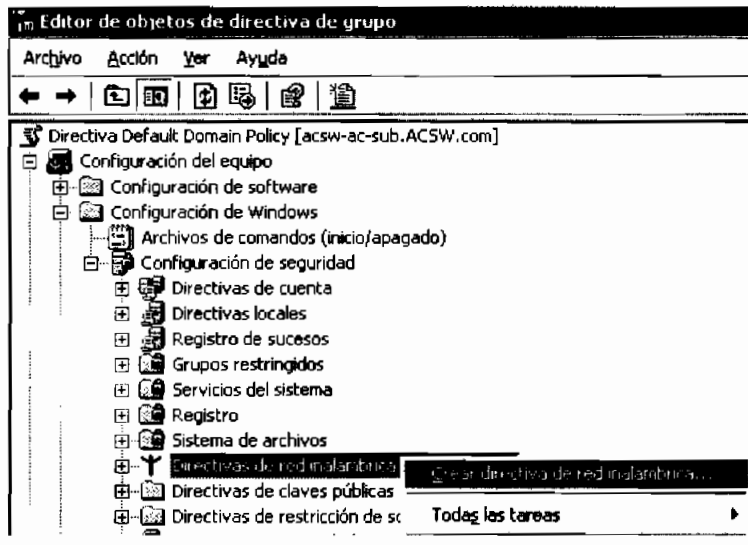


Figura 5.12 Creación de Directiva para Red Inalámbrica

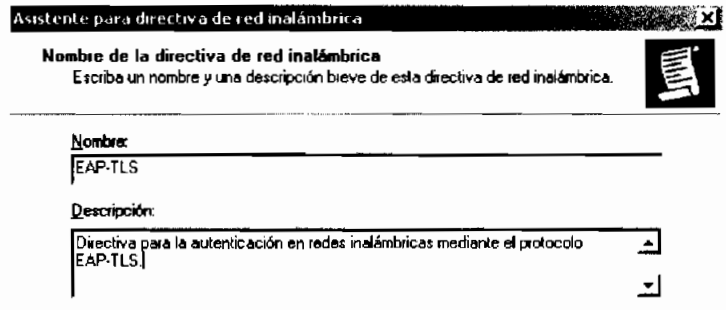


Figura 5.13 Identificación de Directiva para Red Inalámbrica

En la pantalla del asistente se da un clic en **siguiente**. En la pantalla que se presenta a continuación se ingresa el nombre de la directiva y una descripción, tal como se

muestra en la figura 5.13, luego se da un clic en **siguiente**. En la pantalla siguiente se da un clic en **finalizar**.

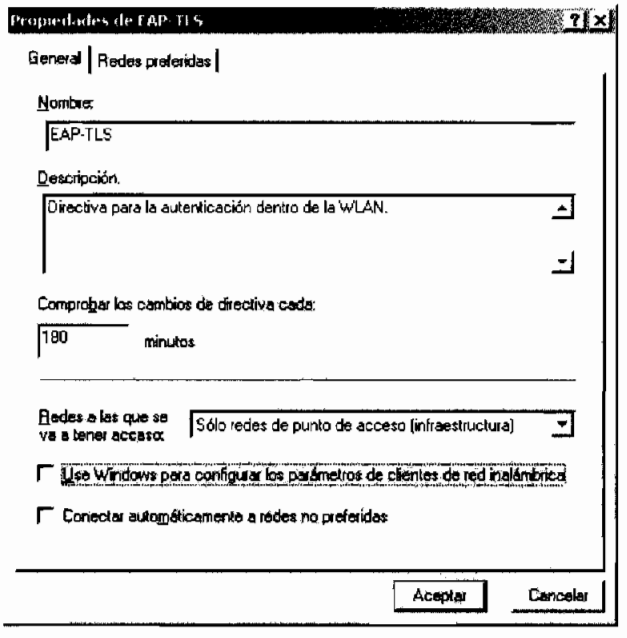


Figura 5.14 Redes a las que se va a Tener Acceso

Entonces se presenta un cuadro de diálogo que permite configurar las propiedades de la nueva directiva; en la pestaña **General** en el campo **Redes a las que se va a tener acceso** se selecciona la opción **Solo redes de punto de acceso** como se muestra en la figura 5.14.

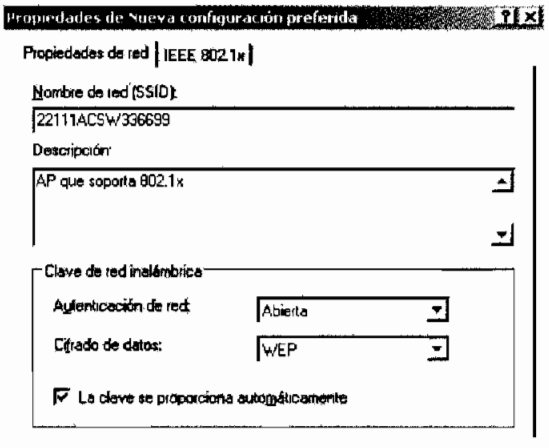


Figura 5.15 Parámetros de Red Inalámbrica

Luego, se desactiva la opción **Use *Windows* para configurar los parámetros de clientes de red inalámbrica**, para permitir que diferentes plataformas de sistemas operativos y *hardware* puedan acceder a la red.

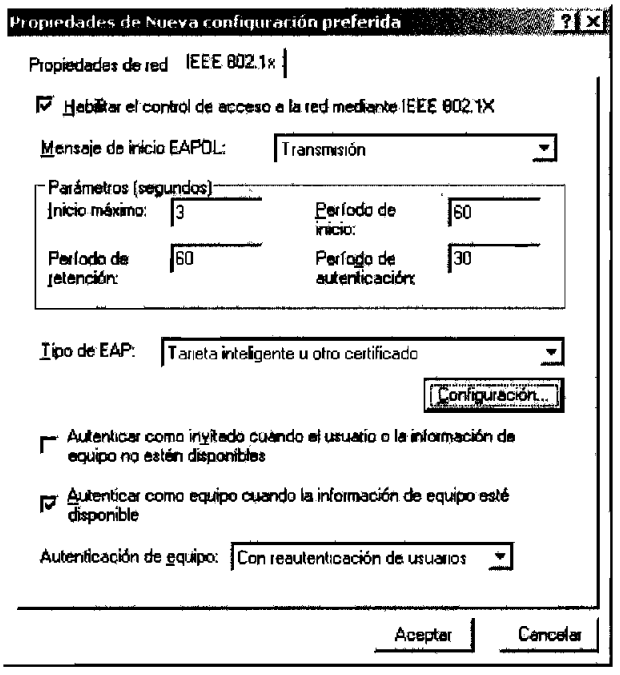


Figura 5.16 Parámetros de 802.1x

En la pestaña **Redes preferidas** (figura 5.14) se da un clic sobre el botón **Agregar**; y en la pestaña **Propiedades de red** del cuadro de diálogo que se presenta se ingresa el SSID de la red, manteniendo la configuración proporcionada por defecto como se muestra en la figura 5.15.

Luego se selecciona la pestaña **IEEE 802.1x** y se activa el campo **Habilitar el control de acceso a la red mediante IEEE 802.1x** como se muestra en la figura 5.16 y se da un clic en el botón **Aceptar**.

Al terminar con este procedimiento, la red configurada se muestra en la pestaña **Redes preferidas** de la directiva de redes inalámbricas como se muestra en la figura 5.17; entonces de da un clic en **Aceptar**.

Para actualizar las directivas configuradas, se ingresa al **Inicio** de *Windows* y se selecciona la opción **Ejecutar**, en el cuadro de diálogo se ingresa el comando *gpupdate* y se da un clic en **Aceptar**.

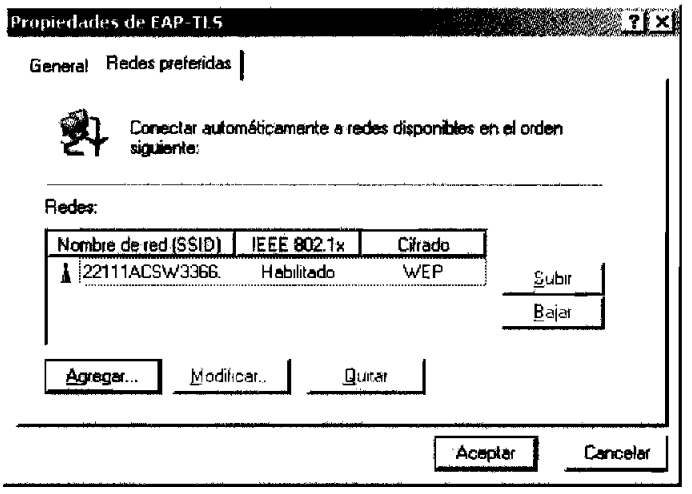


Figura 5.17 Redes Preferidas

5.4.4. INSTALACIÓN DE IAS

Para instalar IAS, en el **Panel de control** se ingresa en **Agregar o quitar programas**, y se selecciona **Agregar o quitar componentes de *Windows***.

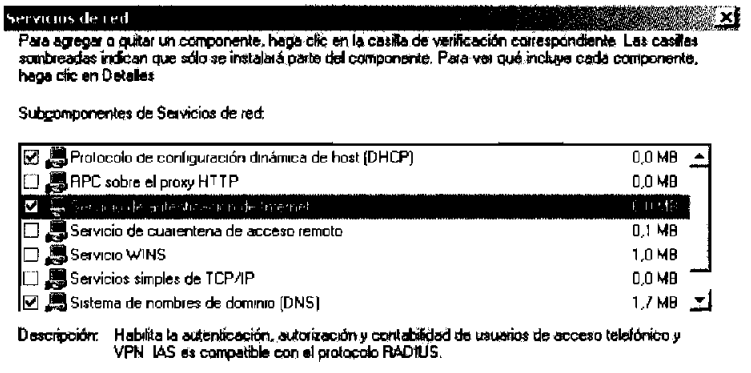


Figura 5.18 Instalación de IAS

En el **Asistente para componentes de *Windows*** se selecciona **Servicios de red** y se da un clic sobre el botón **Detalles**; en el cuadro de diálogo que se presenta se selecciona **Servicio de autenticación de Internet** como se muestra en la figura 5.18 y se da un clic en **Aceptar**.

Finalmente, en el **Asistente para componentes de *Windows*** se da un clic en **siguiente** y en la siguiente pantalla se da un clic en **finalizar**.

5.4.5. CONFIGURACIÓN DE IAS

Para configurar el servidor de acceso remoto para la autenticación EAP-TLS se requiere de un certificado para el servidor; cuando el certificado ha sido emitido, se puede modificar la directiva de acceso en el servidor.

5.4.5.1. Configuración de la Plantilla de Certificado

Para permitir que el servidor IAS pueda solicitar un certificado basado en plantillas, se ejecuta *certtmpl.msc*. En la pantalla de plantillas de certificados se da un clic con el botón derecho del *mouse* sobre la plantilla **Servidor RAS e IAS** y en el menú emergente se selecciona **Propiedades** como se muestra en la figura 5.19.

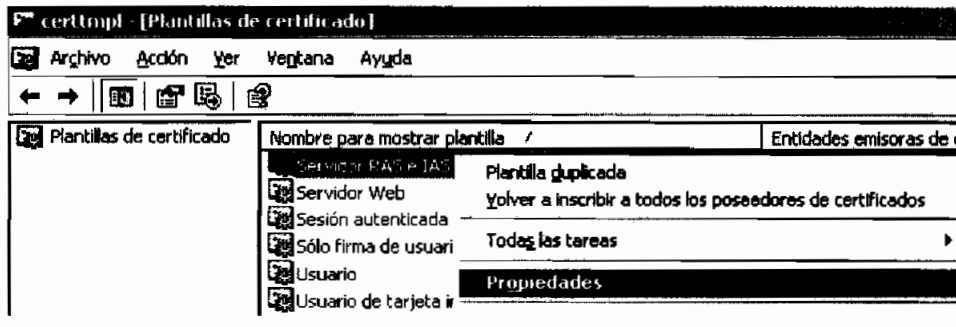


Figura 5.19 Plantilla de Certificado para Servidor IAS

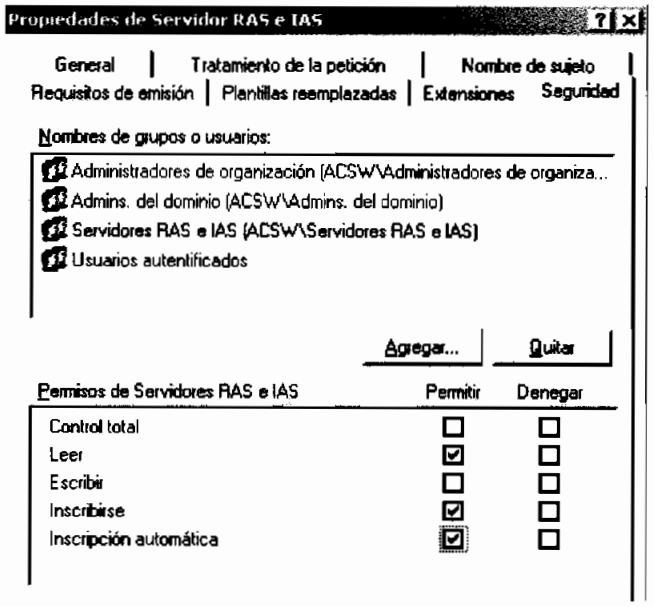


Figura 5.20 Permisos para Inscripción de Certificados

En la pantalla de **Propiedades** se selecciona la ficha **Seguridad**, y en el campo **Nombres de grupos o usuarios** se selecciona el grupo **Servidores RAS e IAS**; luego, en el campo **Permisos de Servidores RAS e IAS** se selecciona las opciones **Leer**, **Inscribirse** e **Inscribirse Automáticamente** como se muestra en la figura 5.20.

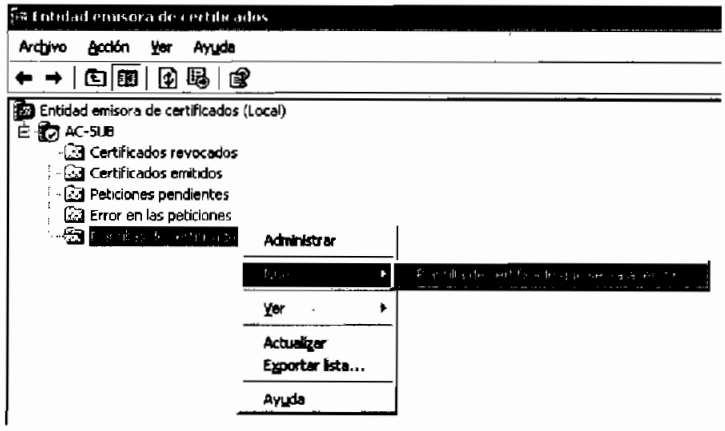


Figura 5.21 Nueva Plantilla de Certificados en la AC-SUB

Cuando el proceso de modificación de la plantilla se ha terminado, se ingresa a la AC-SUB, ahí se da un clic con el botón derecho del *mouse* sobre la carpeta

Plantillas de certificados y en el menú emergente se selecciona la opción **Nuevo** y luego **Plantilla de certificado que se va a emitir** como se muestra en la figura 5.21.

En el cuadro de diálogo que se presenta se selecciona la plantilla **Servidor RAS e IAS** como se muestra en la figura 5.22 y se da un clic en el botón **Aceptar**.

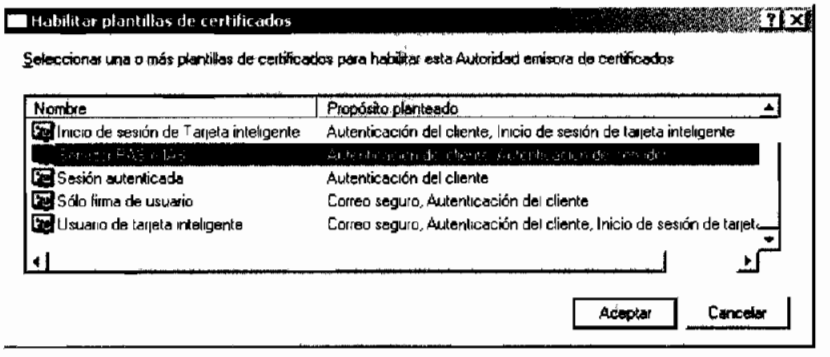


Figura 5.22 Plantilla para Servidor RAS e IAS

Después de la emisión del certificado del servidor IAS, se debe desactivar la Inscripción e Inscripción automática para los servidores de acceso remoto en la plantilla **Servidores RAS e IAS**, debido a que si permanecen activadas, otro servidor podría solicitar un certificado de manera ilícita.

5.4.5.2. Asignación y Actualización Automática de Certificados e Información de la PKI

Para que el servidor IAS pueda obtener su certificado digital e información de la PKI de forma automática, se ingresa a **Usuarios y equipos de *Active Directory***, ahí se da clic con el botón derecho del *mouse* sobre el dominio *acsw.com* y en el menú emergente se selecciona la opción **Propiedades**.

En la pantalla de propiedades se selecciona la pestaña **Directiva de Grupo**, ahí se da un doble clic sobre ***Default Domain Policy*** para ingresar en **Editor de objetos de directiva de Grupo**.

En el Editor de directivas dentro de la **Configuración del equipo** se selecciona la carpeta **Directiva de claves públicas** mostrada en la figura 5.23 y en la parte derecha de la pantalla se da un doble clic sobre **Configuración de inscripción automática**.

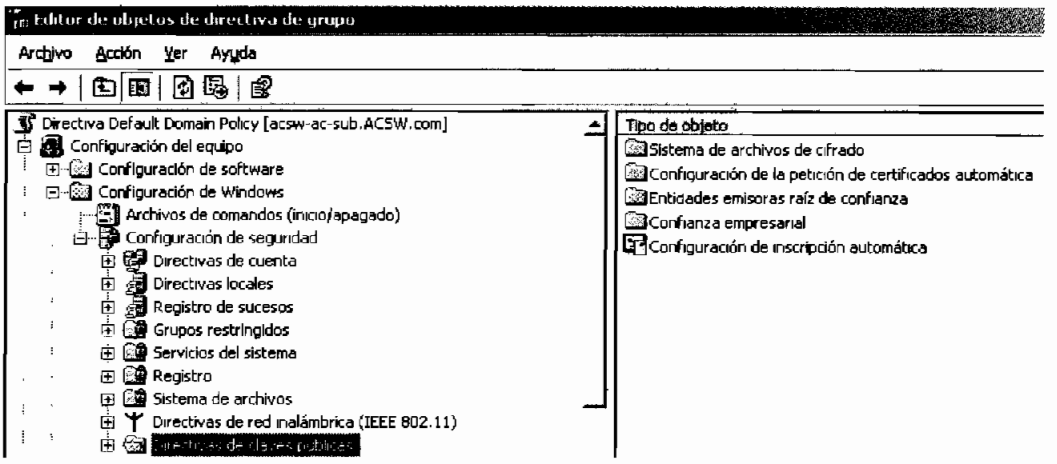


Figura 5.23 Editor de Objetos de Directiva de Grupo

En el cuadro de diálogo que se presenta se selecciona la opción **Registrar certificados automáticamente** y luego se elige las dos opciones permitidas como se muestra en la figura 5.24; finalmente se da un clic en **Aceptar**.

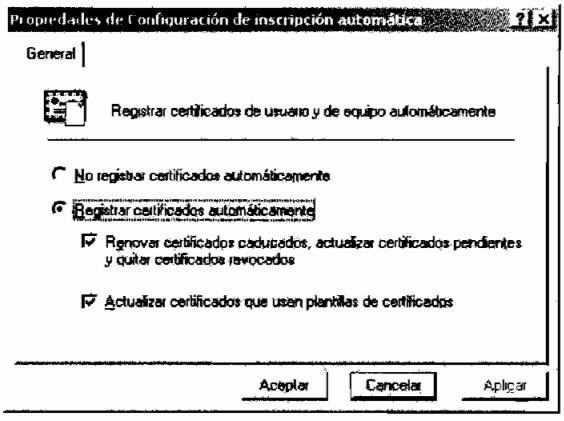


Figura 5.24 Registro de Certificados Automática

A continuación, se da un clic con el botón derecho del *mouse* sobre la carpeta **Configuración de la petición de certificados automática** y en el menú emergente

se selecciona la opción **Nuevo** y luego **Petición de certificados automática** como se muestra en la figura 5.25.

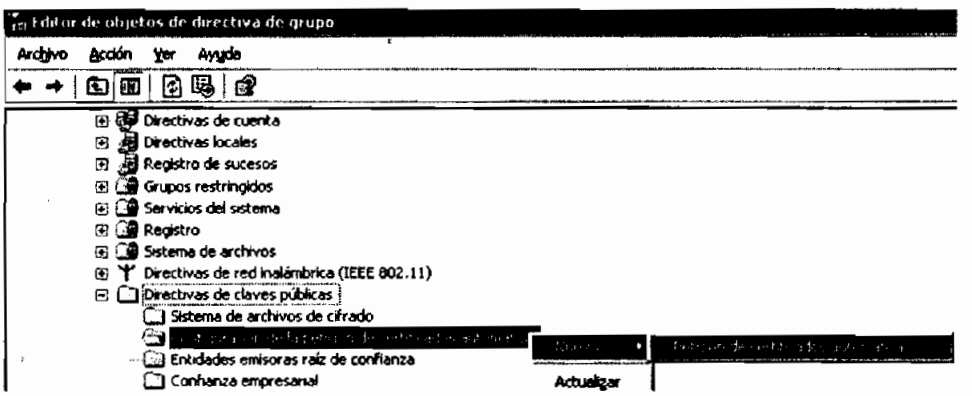


Figura 5.25 Configuración de Certificados Automática

En la pantalla del Asistente se da un clic en **siguiente**. En la siguiente pantalla se selecciona la plantilla **Equipo** como se muestra en la figura 5.26 y se da un clic en **siguiente**; en la última pantalla se da un clic en **Finalizar**.

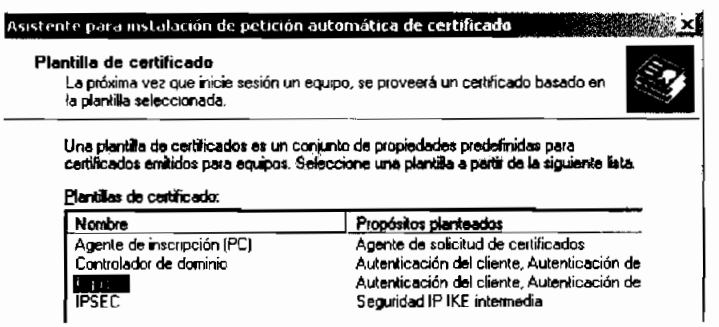


Figura 5.26 Configuración de Certificados Automática para Equipos

5.4.5.3. Registro de IAS en el Domino

Para que el servidor IAS pueda leer las cuentas registradas en *Active Directory* se ingresa al **Inicio** de *Windows* y se selecciona la opción **Herramientas administrativas**, luego se da un clic sobre **Servicio de autenticación de Internet**.

En la pantalla que se presenta se da un clic sobre el botón **Acción** del menú principal y en el menú emergente se selecciona la opción **Registrar servidor en *Active Directory*** como se muestra en la figura 5.27.

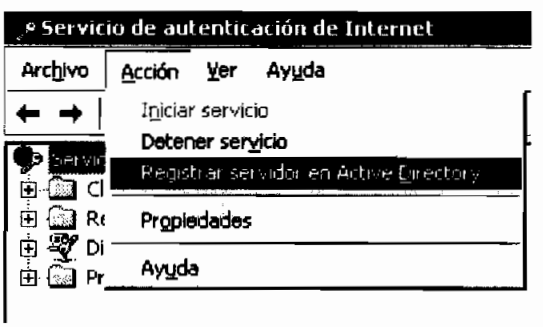


Figura 5.27 Registro de IAS en el Dominio

A continuación se presentan dos mensajes, en el primero se pregunta si se desea que el servidor esté autorizado para leer las propiedades de acceso de los usuarios del dominio, se da un clic en **Aceptar**; el segundo mensaje indica que el equipo ha sido autorizado para leer las propiedades de acceso, para finalizar se da un clic en **Aceptar**.

5.4.5.4. Creación de la Directiva de Acceso Remoto

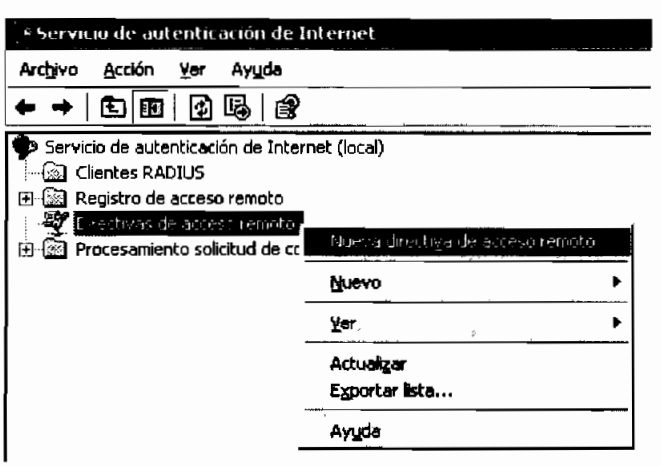


Figura 5.28 Nueva Directiva de Acceso Remoto

Para crear una nueva directiva para el acceso en el servidor IAS, se da un clic con el botón derecho del *mouse* sobre la opción **Directivas de acceso remoto** y en el menú emergente se selecciona la opción **Nueva directiva de acceso remoto** como se muestra en la figura 5.28.

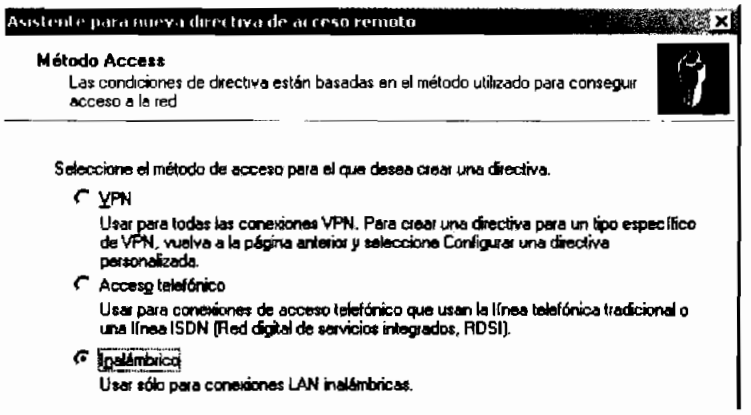


Figura 5.29 Método de Acceso

En la pantalla del Asistente de creación de directivas se da un clic en el botón **siguiente**. En la pantalla que se presenta a continuación se ingresa EAP-TLS como nombre de la nueva directiva y se da un clic en **siguiente**. Posteriormente se selecciona como método de acceso el **Inalámbrico** como se muestra en la figura 5.29 y se da un clic en **siguiente**.

En la pantalla que se presenta en la opción **Grupo** se da un clic en el botón **Agregar** y se ingresa el grupo WLAN; cuando el grupo ha sido agregado, se da un clic en **siguiente**.

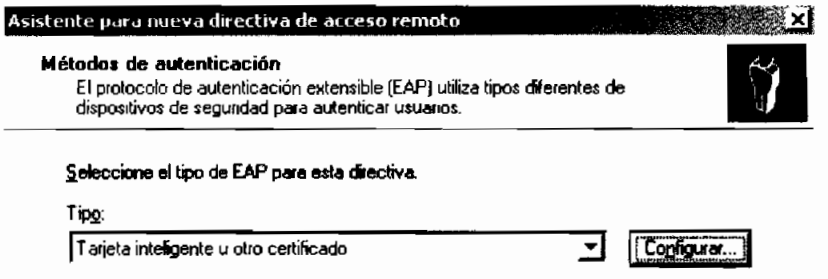


Figura 5.30 Selección del Método de Autenticación

En la pantalla que se presenta a continuación se selecciona dentro del campo **Tipo** la opción **Tarjeta inteligente u otro certificado** y se da un clic en el botón **Configurar** como se muestra en la figura 5.30.

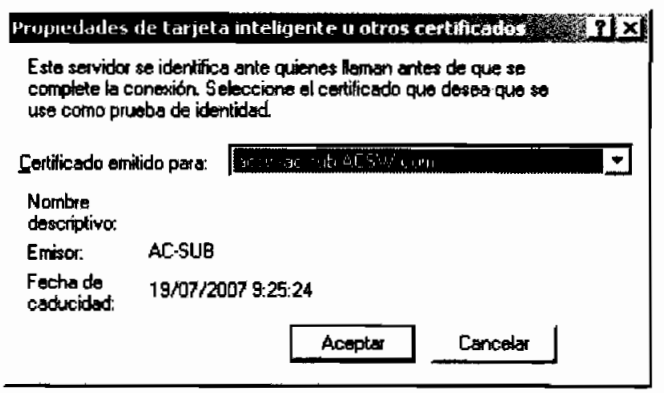


Figura 5.31 Selección del Certificado del Servidor IAS

En el cuadro de diálogo que se presenta se selecciona el certificado del servidor IAS como se muestra en la figura 5.31; entonces se da un clic en el botón **Aceptar** y en la pantalla de **Métodos de autenticación** mostrada en la figura 5.30 se da un clic en **siguiente**. En la última pantalla se da un clic en el botón **finalizar**.

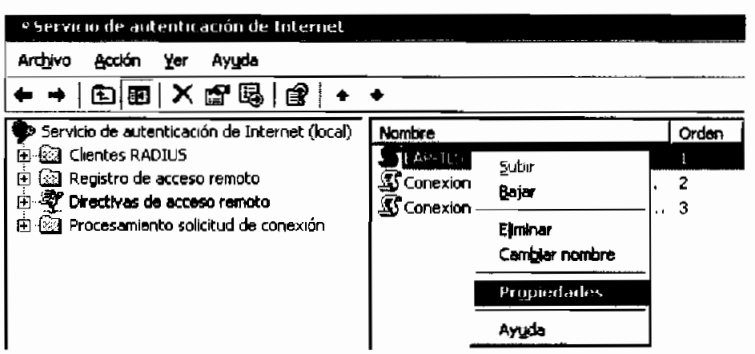


Figura 5.32 Modificación de la Nueva Directiva

La nueva política aparece en el lado derecho de la pantalla del servidor IAS como se muestra en la figura 5.32; para modificarla se da un clic con el botón derecho del *mouse* sobre ésta y en el menú emergente se selecciona la opción **Propiedades**.

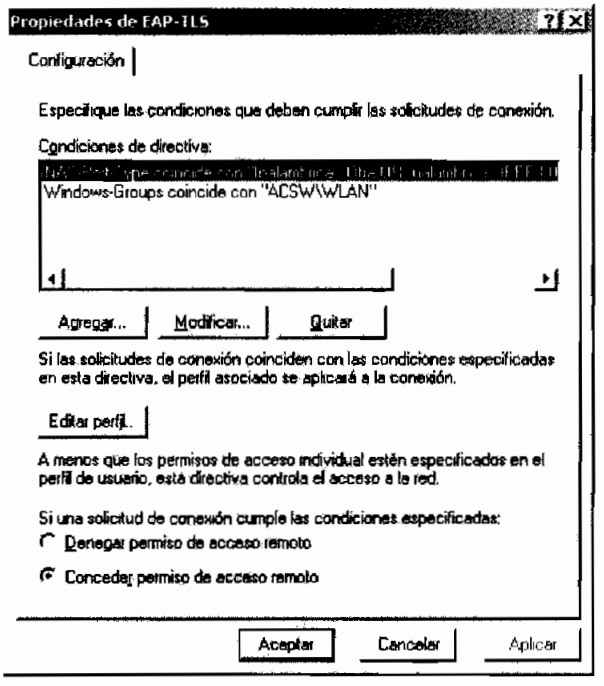


Figura 5.33 Propiedades de la Nueva Directiva

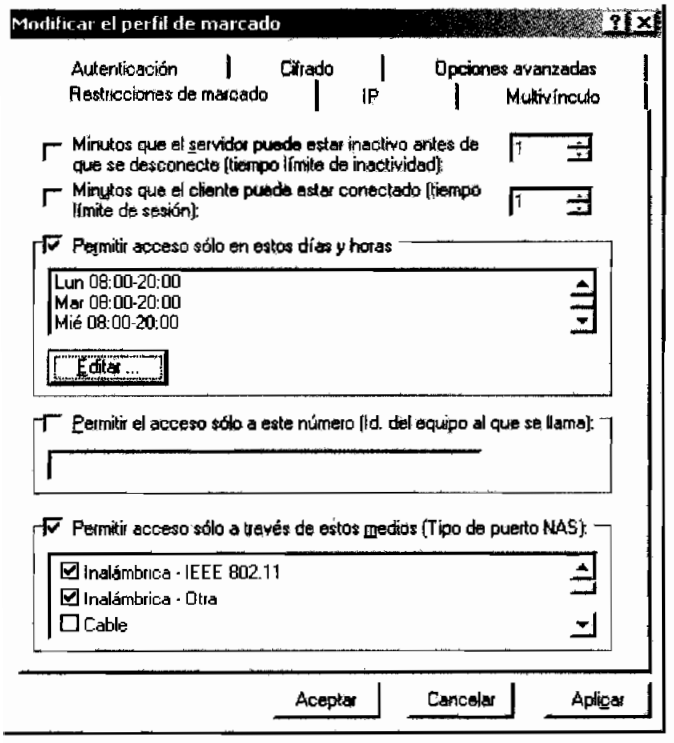


Figura 5.34 Restricciones de Marcado

En el cuadro de diálogo de **Propiedades** se da un clic sobre el botón **Editar perfil** y en el cuadro de diálogo que se presenta se selecciona la pestaña **Restricciones de marcado** y se habilita la opción **Permitir acceso solo en estos días y horas** como se muestra en la figura 5.34.

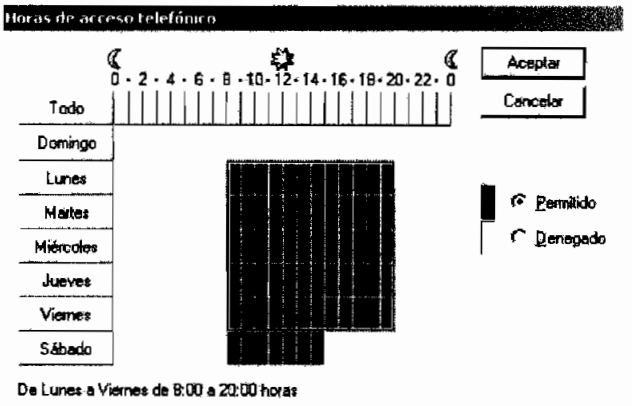


Figura 5.35 Horario de Acceso Permitido

Para modificar el horario establecido por defecto se da un clic sobre el botón **Editar** y se selecciona el horario permitido como se muestra en la figura 5.35; entonces se da un clic en **Aceptar**.

Finalmente, para definir qué medio físico se utilizará para el acceso a la red se habilita el campo **Permitir acceso sólo a través de estos medios** y en la parte inferior se selecciona las opciones **Inalámbrica – IEEE 802.11** e **Inalámbrica – Otra** como se muestra en la figura 5.34.

5.4.5.5. Creación de un Nuevo Cliente RADIUS

El AP es el cliente RADIUS que funcionará como autenticador dentro del proceso de intercambio de credenciales entre un usuario y el servidor IAS; para registrar el AP, se da un clic con el botón derecho del *mouse* sobre la carpeta **Clientes RADIUS** y en el menú emergente se selecciona la opción **Nuevo cliente RADIUS** como se muestra en la figura 5.36.

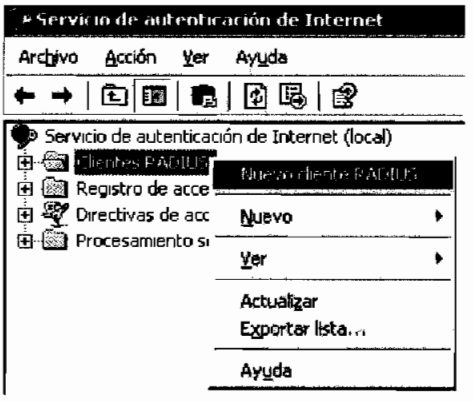


Figura 5.36 Creación de un Nuevo Cliente RADIUS

En el cuadro de diálogo que de presenta se ingresa el nombre del AP en los campos **Nombre descriptivo** y **Dirección del cliente** como se muestra en la figura 5.37; luego se da un clic en el botón **Comprobar** para verificar la conectividad con el AP. Si el AP es localizado correctamente como se muestra en la figura 5.38, se da un clic en **Aceptar** en el cuadro de diálogo **Comprobar cliente** y luego en **Siguiente**.

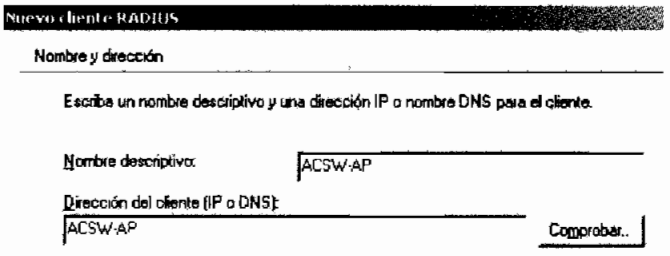


Figura 5.37 Creación de un Nuevo Cliente RADIUS

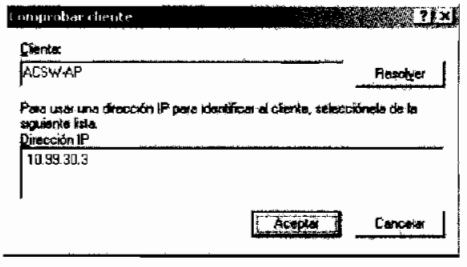


Figura 5.38 Creación de un Nuevo Cliente RADIUS

La pantalla que luego se presenta se utiliza para configurar parámetros específicos de la red como se muestra en la figura 5.39; en el campo **Cliente proveedor** se

selecciona la opción *3Com*; para finalizar con la instalación se ingresa y confirma el secreto compartido y se da un clic en el botón **Finalizar**.

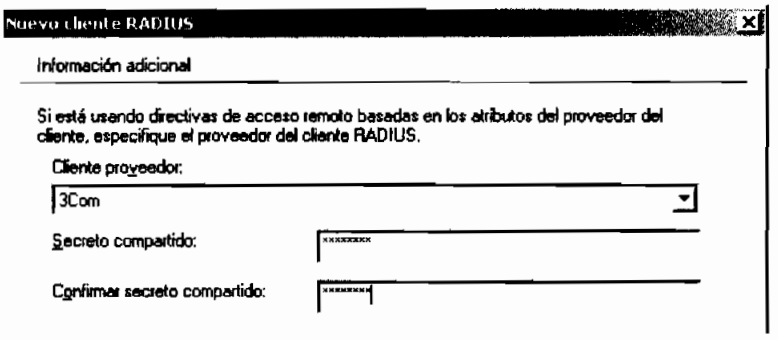


Figura 5.39 Parámetros del Cliente RADIUS

5.5. CONFIGURACIÓN DEL *ACCESS POINT*

Características Generales	
Característica	Descripción
Marca	3Com
Modelo	*Office Connect Wireless 108 Mbps 11g PoE Access Point*
Serie	3CRGPOE10075
Firmware	Versión : 2.1 *Release* : 03 Estado : No actualizado
Estándares Compatibles	802.11b y 802.11g
Dirección MAC	00:0F:CB:C1:85:80
Valores de la Configuración por Defecto	
Característica	Descripción
Dirección IP por defecto	192.168.0.228
Máscara	255.255.255.0
Nombre	SCC18580
Usuario	*admin*
Contraseña	*password*
SSID	3Com
Autenticación	Desactivada
Broadcast de SSID	Activado
SNMP	Desactivado

Tabla 5.3 Características del AP

Para la WLAN se utiliza un AP 3Com, las características generales de este equipo están resumidas en la tabla 5.3.

5.5.1. CONFIGURACIÓN BÁSICA

Dentro de la configuración básica se debe considerar los siguientes aspectos: actualización del *firmware*, direccionamiento IP, parámetros WLAN, filtrado de direcciones MAC y modificación de parámetros de administración. En la tabla 5.4 se encuentran resumidas las características de configuración básica que se aplicarán en el AP.

Configuración Establecida		
Característica	Descripción	
Firmware	Versión :	2.1
	Release :	036
	Estado :	Actualizado[1]
Nombre	ACSW-AP	
Dirección IP	10.99.30.3	
Máscara	255.255.0.0	
Gateway	10.99.30.250	
DNS	10.99.30.250	
Estándares Compatibles	802.11b y 802.11g	
Modo de trabajo	*Root*	
Brodcast de SSID	Desactivado	
Canal	Automático	
Filtrado MAC	Habilitada	
Usuario	Adminaap	
Contraseña	kasas*2799	
Administración	HTTP	Deshabilitado
	HTTPS[2]	Habilitado
	Telnet	Deshabilitado
Respaldos	Almacenados	
SNMP	Deshabilitado	

Tabla 5.4 Parámetros Configurados en el AP

[1] http://www.3com.com/products/en_US/result.jsp?selected=all&sort=effdt&sku=3CRGPOE10075&order =desc.

[2] *Secure* HTTP.

5.5.1.1. Actualización del *Firmware*

Al ingresar a la página *Web* oficial de 3Com se encuentra que la última versión de *firmware* para el AP *Office Connect Wireless 108 Mbps 11g PoE* es la v2.106; por lo tanto es necesario realizar una actualización en el AP antes de empezar su configuración.

Para actualizar el *firmware* se ingresa a la página *Web* http://192.168.0.228. En el menú de la parte izquierda de la Pantalla se selecciona la opción ***Management***; en el campo ***Upgrade File*** de la pestaña ***Upgrade Firmware*** se da un clic sobre el botón **Examinar** y se selecciona la ubicación del nuevo *firmware* como se muestra en la figura 5.40; luego se da un clic en el botón ***Upgrade***.

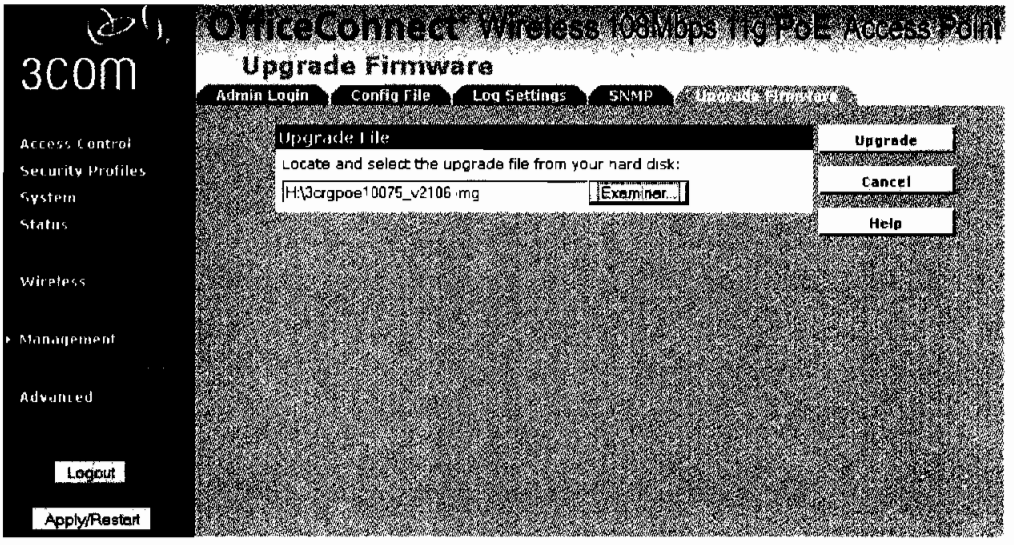


Figura 5.40 Selección del Firmware

Entonces se presenta en pantalla el avance del proceso de almacenamiento del *firmware* como se muestra en la figura 5.41; cuando éste ha concluido se presenta un mensaje indicando que para realizar la actualización se debe reiniciar el AP, para lo cual se da un clic en el botón ***Apply/Restart*** ubicado en la parte inferior izquierda de la pantalla.

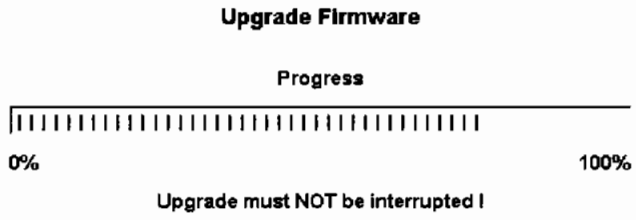


Figura 5.41 Proceso de la Actualización del Firmware

En la figura 5.42 se muestra el estado del AP después de reiniciar, como se puede observar, en la Pestaña ***Status*** del menú ***Status*** se encuentra registrada versión de *firmware* 2.1 *Release* 06.

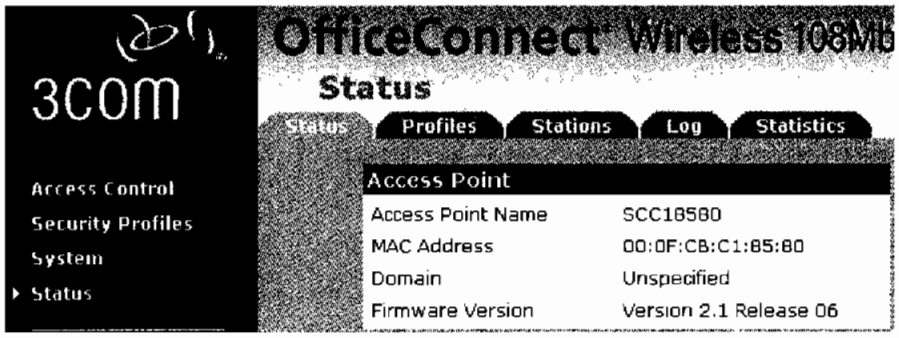


Figura 5.42 Firmware Actualizado

5.5.1.2. Direccionamiento IP

Después de la actualización del *firmware* se modifican los valores de la configuración por defecto. Para modificar la dirección IP del AP se ingresa a la página Web http://192.168.0.228.

En el menú de la parte izquierda de la Pantalla se selecciona la opción ***System***. En el campo ***Identification*** se ingresa el nombre del AP como se muestra en la figura 5.43; en el campo ***Country or Domain*** se mantiene la opción ***United States*** debido a que si se cambia este parámetro se desactiva la compatibilidad con 802.11g.

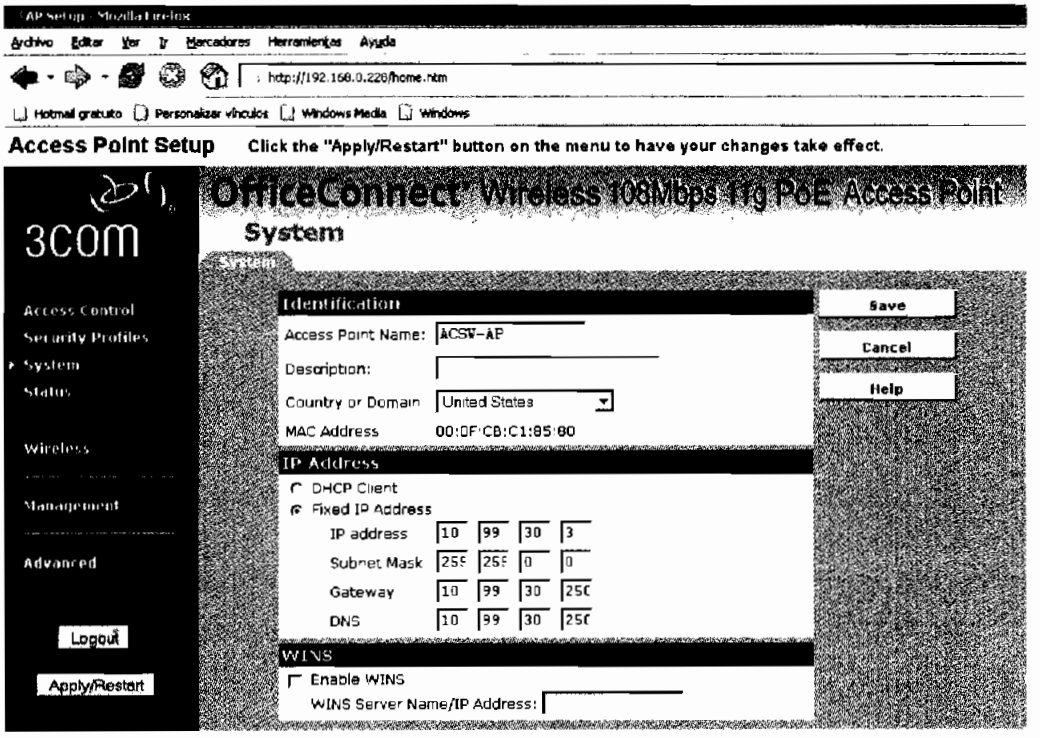


Figura 5.43 Configuración IP del AP

En el campo ***IP Address*** se selecciona la opción ***Fixed IP Address*** y se ingresan los parámetros de configuración IP, como se observa en la figura 5.43; al terminar se da un clic en el botón ***Save***. En la parte superior de la pantalla se presenta un mensaje indicando que para aplicar los cambios se debe reiniciar el equipo, para esto se da un clic en el botón ***Apply/Restart***.

5.5.1.3. Parámetros de la WLAN

Para modificar los parámetros de configuración inalámbrica se ingresa a la página http://10.99.30.3, en el menú principal se selecciona la opción ***Wireless*** y en el campo ***Operation*** se realizan los siguientes cambios:

- En la opción ***Wireless Mode*** se selecciona 802.11b y 802.11g.
- En la opción **AP Mode** se elige ***Access Point*** (*root*).
- Se deshabilita el *Broadcast* de SSID.

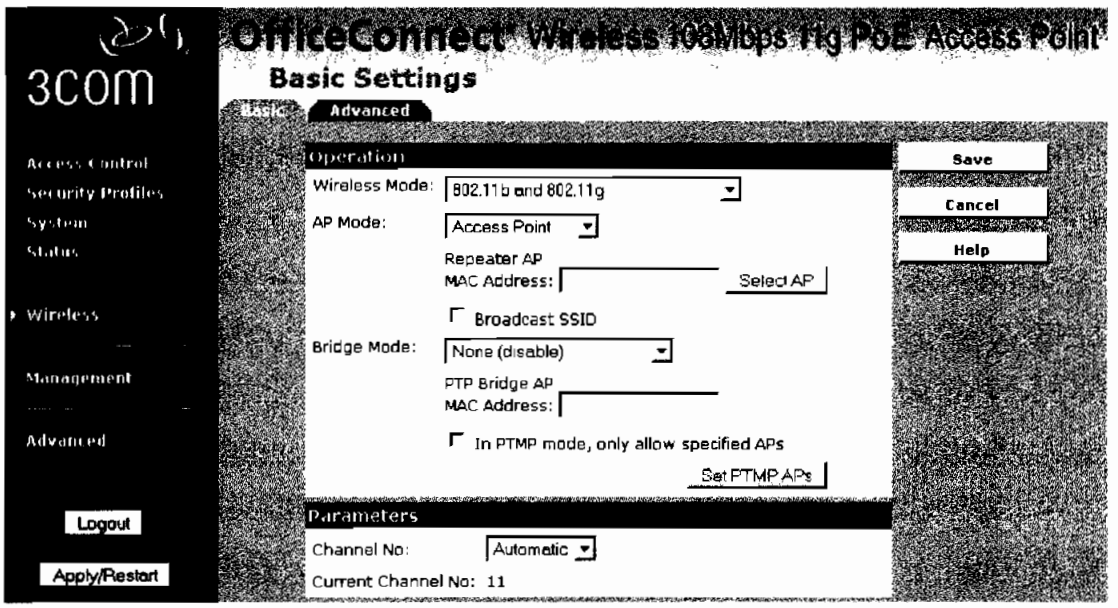


Figura 5.44 Configuración de Parámetros Wireless en el AP

Finalmente, en la opción ***Channel Nº*** del campo ***Parameters*** se selecciona ***Automatic***. Cuando se han realizado todos los cambios mencionados se da un clic sobre el botón ***Save*** y luego en el botón ***Apply/Restart***, la configuración realizada se muestra en la figura 5.44.

5.5.1.4. Habilitación del Filtrado de Direcciones MAC

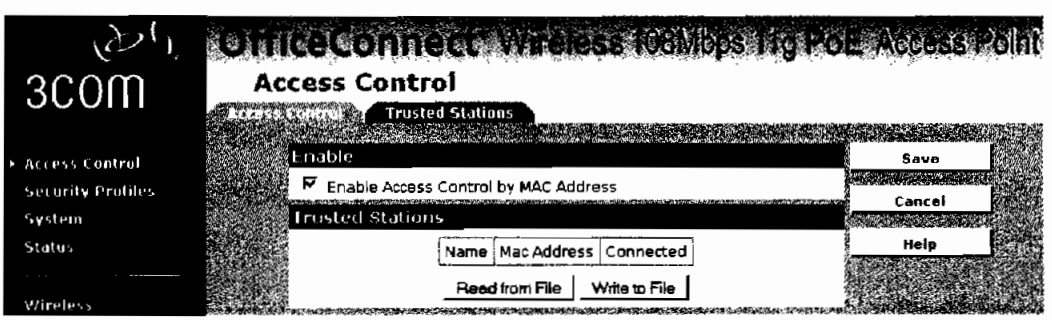


Figura 5.45 Configuración de Filtrado MAC

Para habilitar el filtrado de direcciones MAC, se selecciona en el menú principal la opción ***Access Control*** y en la primera pestaña se selecciona la opción ***Enable***

Access Control by MAC Address como se muestra en la figura 5.45; luego se da un clic en ***Save*** y en ***Apply/Restart***.

Para agregar direcciones MAC válidas se selecciona la pestaña ***Trusted Station***, se llena los campos ***Name*** y ***Address*** como se muestra en la figura 5.46 y se da un clic en ***Add***; para guardar los cambios se da un clic en ***Apply/Restart***. Si se requiere retirar una dirección del grupo de confianza se selecciona la dirección y se da un clic en el botón señalado con la flecha en la figura 5.46 y se aplican los cambios.

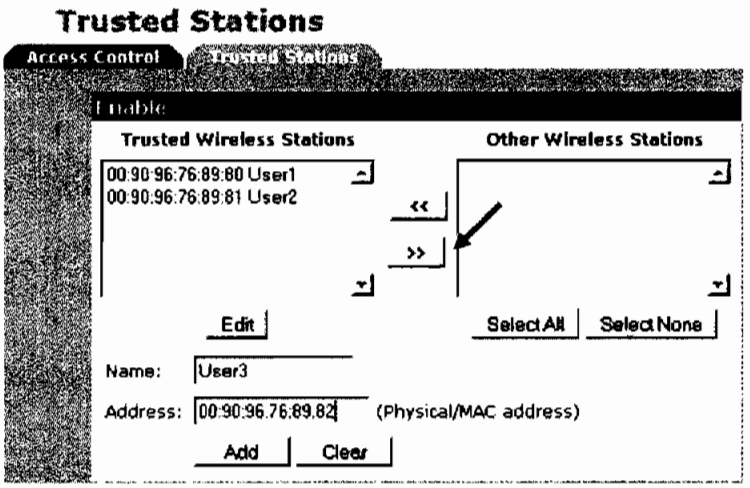


Figura 5.46 Introducción de direcciones MAC de Confianza

5.5.1.5. Modificación de Parámetros de Administración

Para modificar los parámetros de administración, se selecciona en el menú principal la opción ***Management***. En la primera pestaña dentro del campo ***Login*** se modifica el nombre de usuario y la contraseña. En el campo ***Admin Connections*** se deshabilita las opciones HTTP y ***Telnet***, como se muestra en la figura 5.47; luego se da un clic en ***Save*** y en ***Apply/Restart***.

Para volver a ingresar a la configuración del AP, se debe acceder a la página *Web* https://10.99.30.3, como se muestra en la figura 5.48.

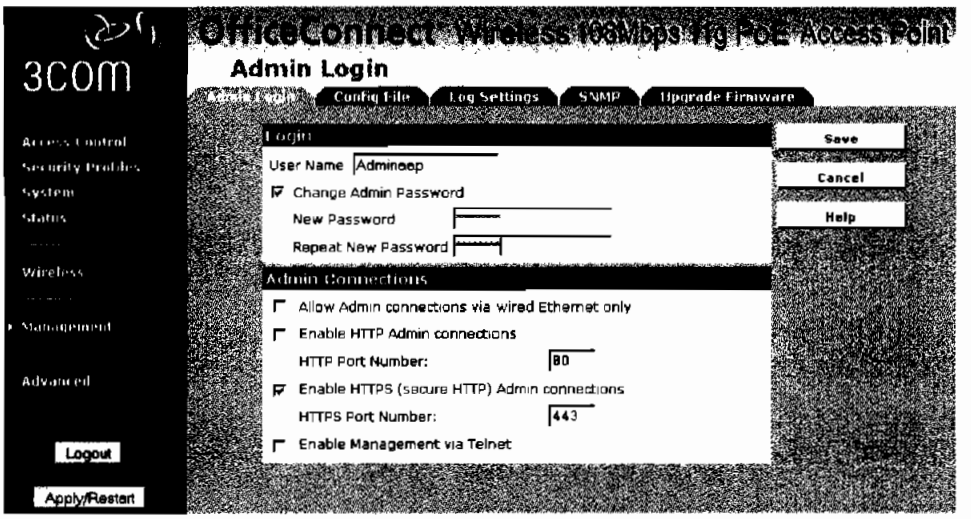


Figura 5.47 Modificación de Parámetros de Administración

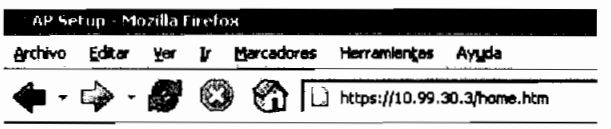


Figura 5.48 Administración con Conexión Segura

La configuración para monitoreo del equipo por medio del protocolo SNMP por defecto está deshabilitada; por lo tanto, se ha terminado la configuración básica del AP.

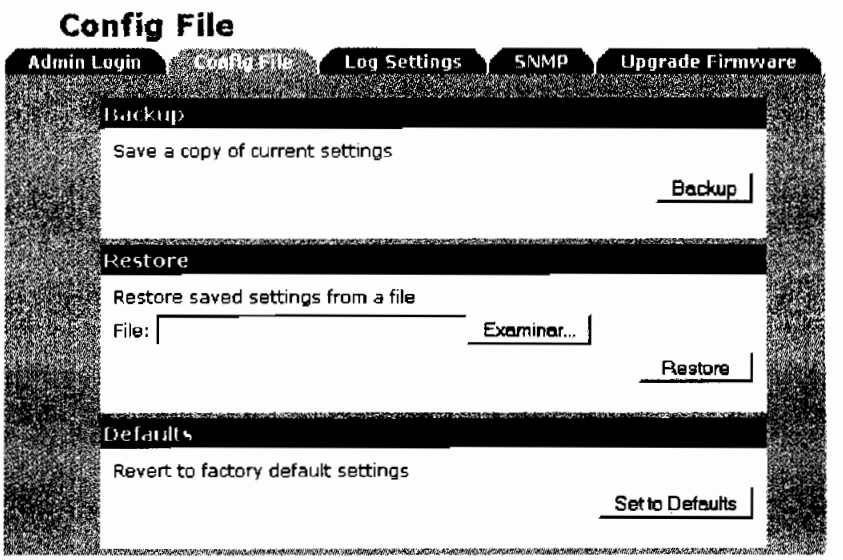


Figura 5.49 Respaldos de la Configuración

Para sacar respaldos de la configuración se selecciona la pestaña ***Config File*** y dentro del campo ***Backup*** se da un clic sobre el botón ***Backup*** mostrado en la figura 5.49 y se guarda el archivo *ap11g.cfg* en disco.

Como se puede observar en la figura 5.49, dentro de la pestaña ***Config File*** se puede respaldar la configuración actual, restablecer una configuración mediante un archivo .cfg o volver a la configuración por defecto a través de la opción ***Set to Defaults***.

5.5.2. CONFIGURACIÓN EAP-TLS

Para habilitar la autenticación EAP-TLS se ingresa en el menú ***Security Profiles***, como se observa en la figura 5.50, en la parte derecha de la pantalla se muestran los perfiles disponibles en el AP; para modificar un perfil, se selecciona y se da un clic en el botón ***Configure***.

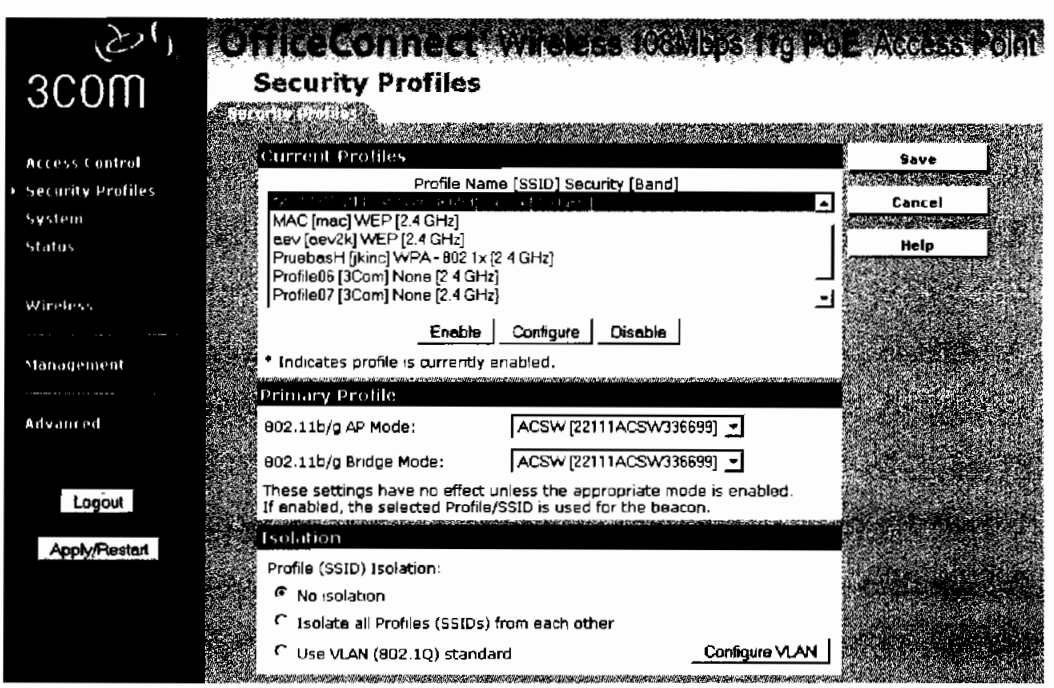


Figura 5.50 Selección del Perfil a Modificar

En la pantalla que se presenta se ingresa el nombre del perfil y el SSID de la red; luego en el campo ***Wireless Security System*** se selecciona la opción **802.1x**. Para la encripción se define como tamaño de la clave WEP 128 *bits* y se habilita la opción ***Dynamic WEP key***, modificando el tiempo de vida de la clave a 120 minutos como se muestra en la figura 5.51.

Finalmente, en la sección ***Primary Profile*** del menú ***Security Profiles*** se activa el perfil configurado en los campos AP y *Bridge* como se muestra en la figura 5.50. Cuando se ha terminado, se da un clic en el botón ***Save*** para guardar el perfil y en el botón ***Apply/Restart*** para almacenar la configuración.

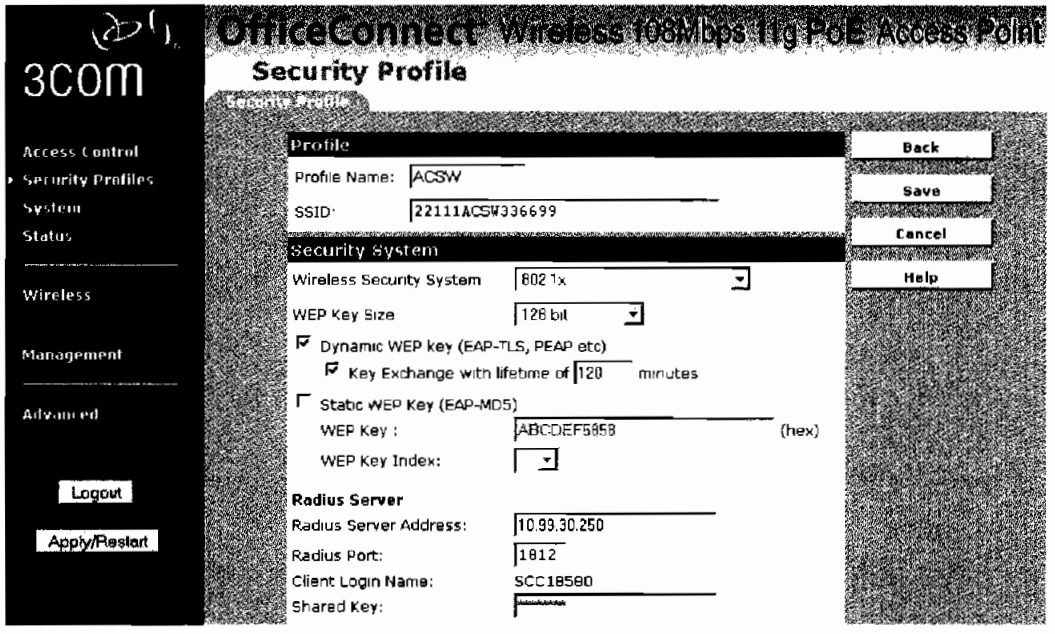


Figura 5.51 Configuración del Perfil EAP-TLS

5.6. CONFIGURACIÓN DEL USUARIO

La versión de prueba (*trial*) del OAC 4.51 está disponible en la página *Web* http://www.juniper.net/customers/support/products/aaa_802/oac_client_user.jsp. La

instalación del cliente OAC es sencilla, basta con seguir el asistente de instalación y marcar la opción de 30 días de prueba como se muestra en la figura 5.52.

Para iniciar la configuración del cliente WLAN, primero se debe agregar el equipo al dominio, cuando el equipo ha sido agregado al dominio, el usuario puede ingresar a la red para descargar su certificado digital; este proceso se realiza a través de la LAN cableada.

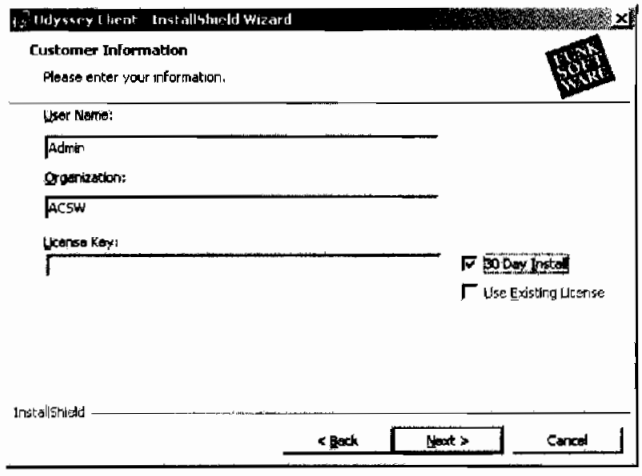


Figura 5.52 Instalación del Cliente Odyssey

5.6.1. CONFIGURACIÓN DEL PERFIL DE AUTENTICACIÓN

Después de que el usuario ha descargado su certificado digital, se ingresa al **Inicio** de *Windows*, ahí se da un clic sobre la opción **Todos los programas** y se selecciona la opción ***Funk Software***, luego se da un clic sobre ***Odyssey Client*** para seleccionar la opción ***Odyssey Client Manager***.

En el menú de la parte izquierda del OAC mostrado en la figura 5.53, se selecciona la opción ***Profiles*** y se elimina el perfil por defecto, entonces se da un clic en el botón ***Add***; en el campo ***Profile Name*** del cuadro de diálogo ***Add Profile*** se ingresa el nombre *acsw* como se muestra en la figura 5.54.

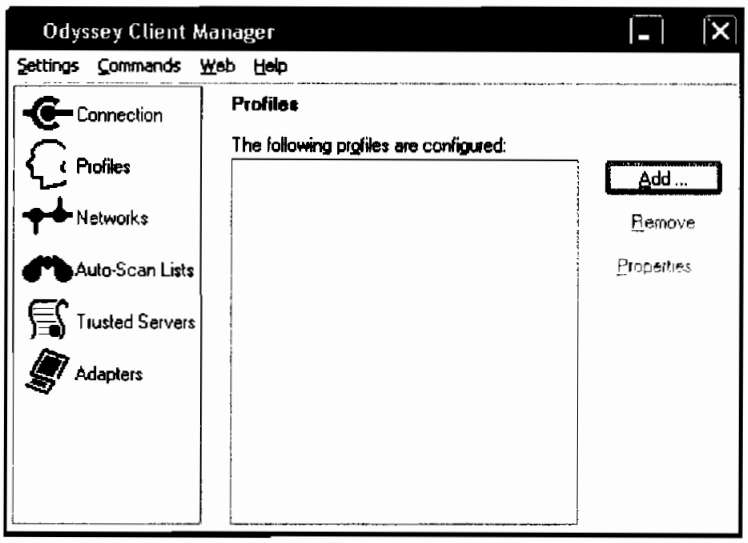


Figura 5.53 Odyssey Client Manager

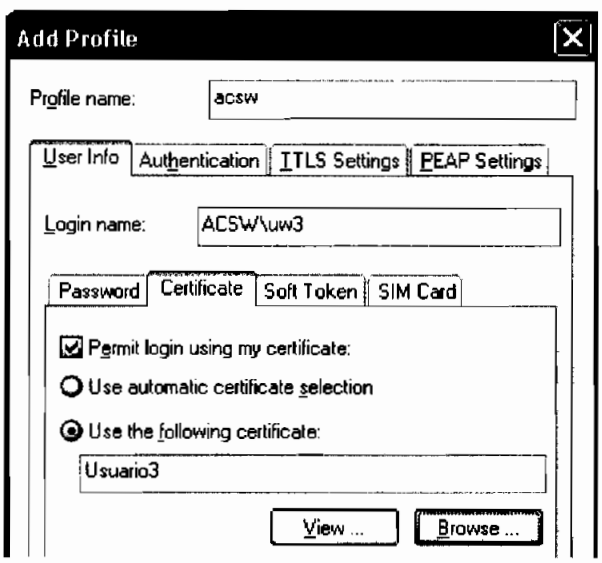


Figura 5.54 Configuración del Perfil de Autenticación Odyssey

Luego en la pestaña ***User Info*** se selecciona la subpestaña ***Certificate*** y se activa el campo ***Permit login using my certificate*** con la opción ***Use the following certificate*** y se da un clic en el botón ***Browse*** para seleccionar el certificado.

Después se selecciona la pestaña ***Authentication*** y en el campo ***Authentication protocols*** se elimina la opción EAP-TTLS y se agrega EAP-TLS, activando la opción

Validate server certificate como se muestra en la figura 5.55; finalmente, se da un clic en el botón ***Ok***.

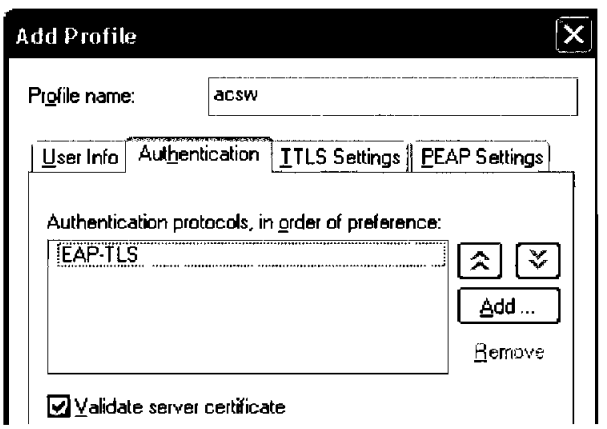


Figura 5.55 Configuración del Perfil EAP-TLS

5.6.2. CONFIGURACIÓN DE LA RED

Para configurar los parámetros de la WLAN en el menú principal se selecciona la opción ***Networks*** como se muestra en la figura 5.56, entonces se elimina la opción ***any*** y se da un clic sobre el botón ***Add***.

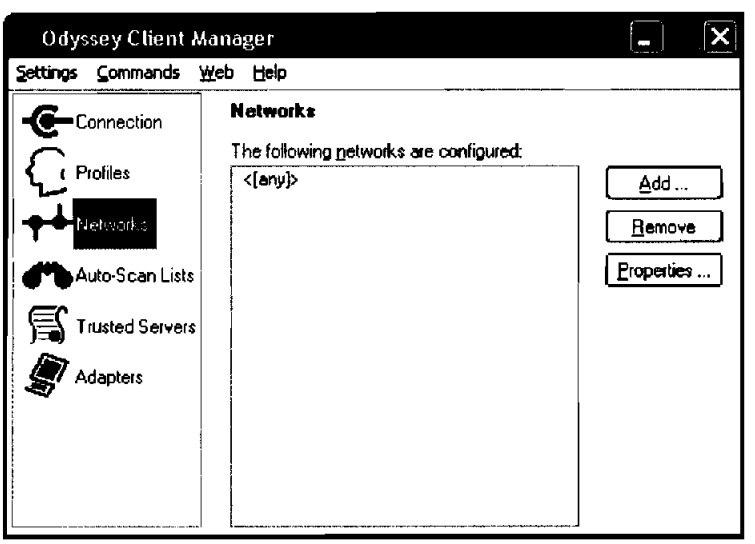


Figura 5.56 Configuración del Perfil de Red Odyssey

En el cuadro de diálogo ***Add Network*** se ingresa el SSID 22111ACSW336699 dentro del campo ***Network name*** y en el campo ***Encryption method*** se elige WEP; luego en el campo ***Authentication*** se habilita la opción ***Authenticate using profile*** y se selecciona el perfil *acsw* creado en la sección anterior.

Finalmente, se activa la opción ***Keys will be generated automatically for data privacy*** como se muestra en la figura 5.57 y se da un clic en ***Ok***.

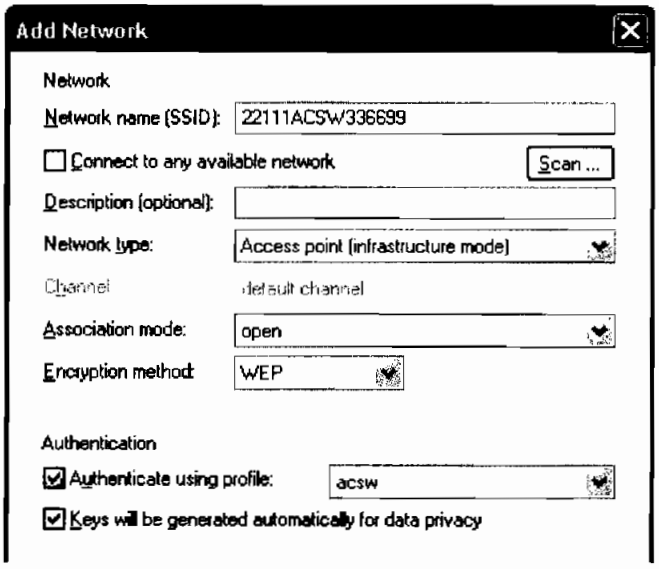


Figura 5.57 Configuración de los Parámetros de Red

5.6.3. SELECCIÓN DE LA RED

Después de la configuración de los parámetros de red, se selecciona en el menú principal la opción ***Connection*** y se activa el campo ***Connect to network*** asignando la red 22111ACSW336699 como se indica en la figura 5.58.

Como se puede observar en la figura 5.58, al inicio de la conexión el estado del campo ***Status*** es ***waiting to authenticate***; entonces se presenta en pantalla el cuadro de diálogo mostrado en la figura 5.59, éste muestra la ruta de certificación del

certificado del servidor IAS. Para agregar el servidor a la lista de confianza se activa la opción ***Add the trusted server to the database*** y se da un clic en ***Yes***.

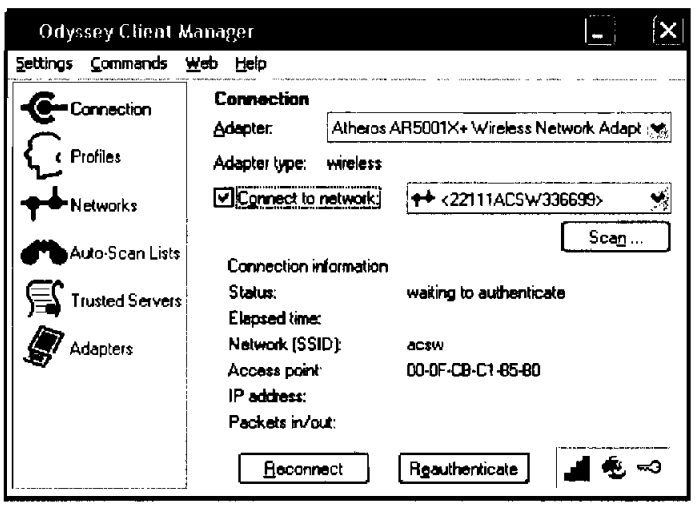


Figura 5.58 Selección de la Red

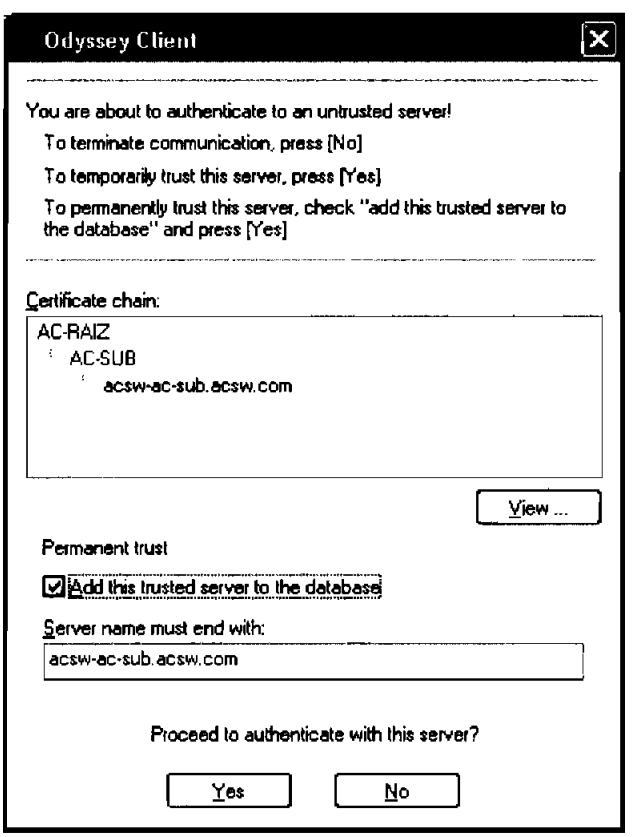


Figura 5.59 Ruta de Certificación del Certificado del Servidor IAS

5.7. POLÍTICAS PARA EL ACCESO A LA RED

Dentro de las políticas para el acceso a la red se establecen los siguientes lineamientos:

- **Usos Permitidos de Certificados**.- De acuerdo a la CP y CPS de la PKI-ACSW, el uso de los certificados está restringido para el intercambio de claves simétricas con el fin de asegurar la WLAN; siendo así, los usuarios pueden utilizar sus certificados únicamente bajo este esquema.

- **Usos Permitidos de los Medios Inalámbricos**.- El uso de los medios inalámbricos está restringido a comunicaciones con entidades miembro de la red ACSW, queda prohibido el establecimiento de redes ***Ad Hoc*** o con un SSID distinto al establecido (22111ACSW336699).

- **Protección de la Clave Privada**.- La clave privada debe permanecer bajo custodia de su titular; para su protección se debe establecer durante la creación del certificado digital la seguridad alta. La contraseña que protege a la clave debe cumplir una longitud y aleatoriedad adecuadas.

- **Horario Permitido para el Acceso a la Red**.- El horario de acceso a la red está limitado de ocho a veinte horas para los días laborables y los días sábados de ocho a catorce horas. Los días domingos no se permite el acceso.

- **Usuarios con autorización para utilizar medios inalámbricos**.- Solo los usuarios miembro del grupo WLAN están autorizados y cuentan con los privilegios para acceder a la red por medios inalámbricos.

- **Disponibilidad de la información**.- Toda la información relacionada con CP, CPS, rutas de confianza, certificados de las ACs y CRLs, debe estar disponible en horario establecido en la página *Web* http://acsw.com.

Para el cumplimiento efectivo de las políticas de acceso a la red los usuarios deben ser capacitados antes de interactuar con la infraestructura; además, deben conocer el contenido de la CP y CPS antes de firmar el contrato de certificación (Anexo 6).

5.8. INTERACCIÓN CON PKI

La interacción entre un usuario de la WLAN y la PKI empieza desde el momento en que éste se somete al proceso de identificación realizado por el personal de recursos humanos.

Cuando los datos presentados por el usuario han sido verificados, el usuario debe informarse en detalle del contenido de la CP y CPS (Anexo 5 y 6, respectivamente), luego de lo cual debe llenar el formulario incluido en el Anexo 6 y firmar el contrato de certificación.

Después de un proceso de identificación exitoso, el personal de recursos humanos entrega los datos del usuario al Administrador de AC de la sucursal, para que éste sea agregado en *Active Directory* como miembro de los usuarios del grupo WLAN dentro del dominio.

El proceso final del registro del usuario se lleva a cabo vía *Web*; para esto el usuario debe ingresar al portal de descarga de certificados de la AC-SUB, en éste el usuario podrá concluir su registro y descargar su certificado digital.

La dirección del sitio *Web* de descarga de certificados de la AC-SUB es: http://acsw-ac-sub.acsw.com/certsrv. Para ingresar a este portal el usuario debe autenticarse con el nombre de usuario y la clave registrados en *Active Directory* como se muestra en la figura 5.60.

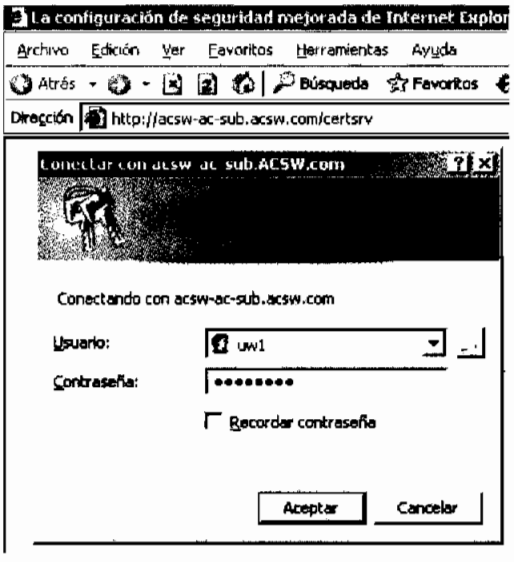


Figura 5.60 Autenticación ante el Portal de la AC-SUB

Si la información proporcionada durante la autenticación por el usuario es correcta, el usuario puede acceder a la página mostrada en la figura 5.61; en ésta puede encontrar el certificado de la AC-SUB, la CRL, etc. Para iniciar con el proceso de emisión del certificado digital se da un clic sobre la opción **Solicitar un certificado**.

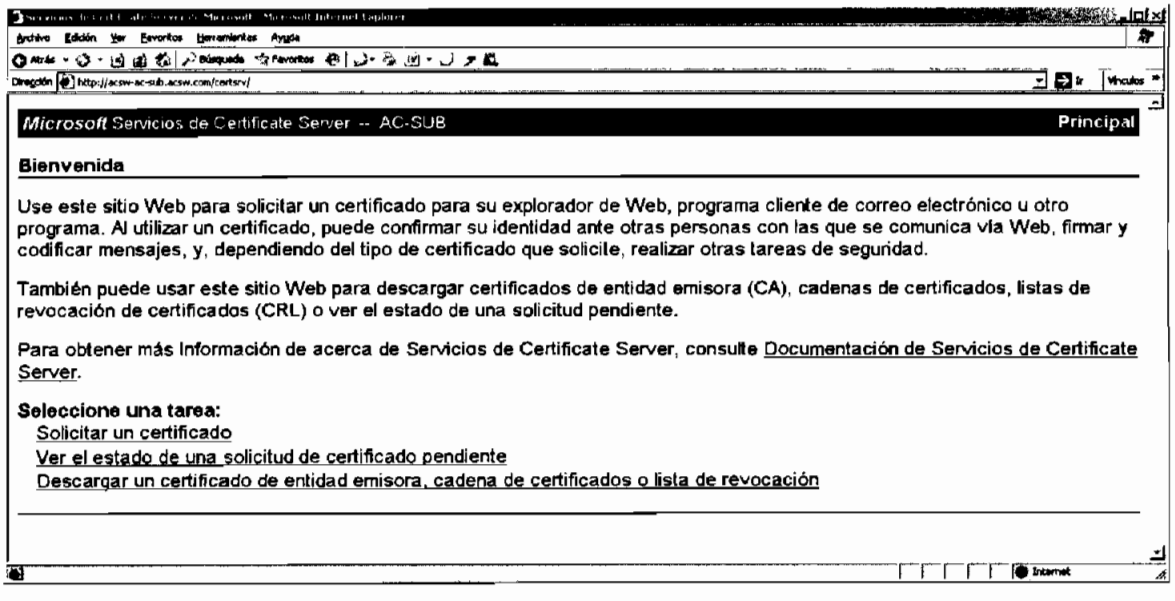


Figura 5.61 Página de Bienvenida del Portal de la AC-SUB

La figura 5.62 muestra la página que se presenta a continuación, en ésta se selecciona la opción **Certificado de usuario**. En la siguiente página se activa el campo **Más opciones** para acceder a la página de opciones adicionales.

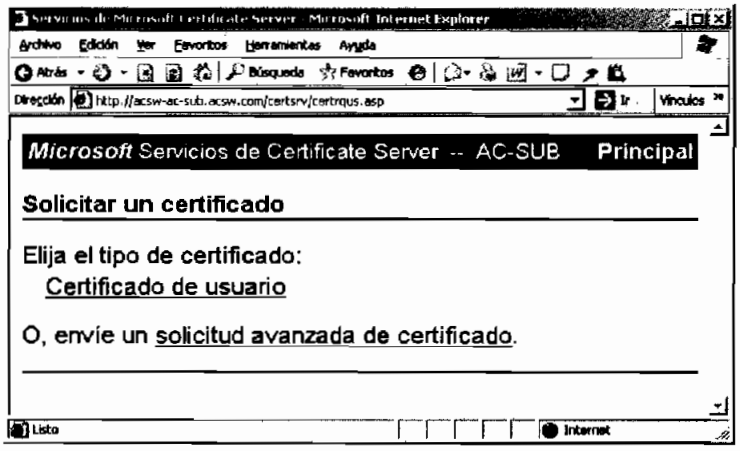


Figura 5.62 Página de Solicitud de Certificados de Usuario del Portal de la AC-SUB

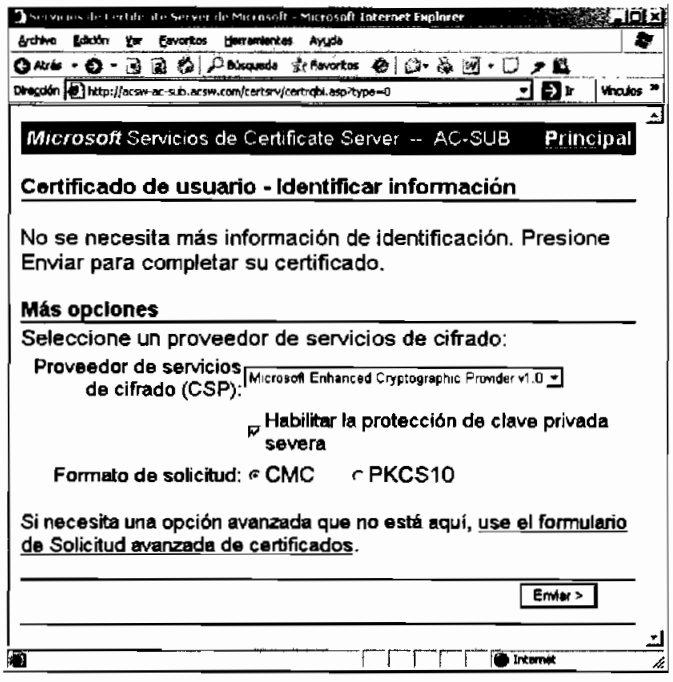


Figura 5.63 Página de Opciones Adicionales de Solicitud

En la página de opciones adicionales, se activa la opción **Habilitar la protección de clave privada severa** como se muestra en la figura 5.63 y luego se da un clic en el

botón **Enviar**. Entonces se presenta un mensaje solicitando autorización para que el sitio *Web* solicite un certificado personal para el usuario, se da un clic en **Sí**.

Antes de enviar la solicitud a la AC-SUB, se presenta el asistente para protección de claves mostrado en la figura 5.64, entonces se da un clic en el botón **Nivel de Seguridad**; y en el cuadro de diálogo que se presenta se selecciona **Alto** y se da un clic en **siguiente**.

Figura 5.64 Asistente para Seguridad de la Clave

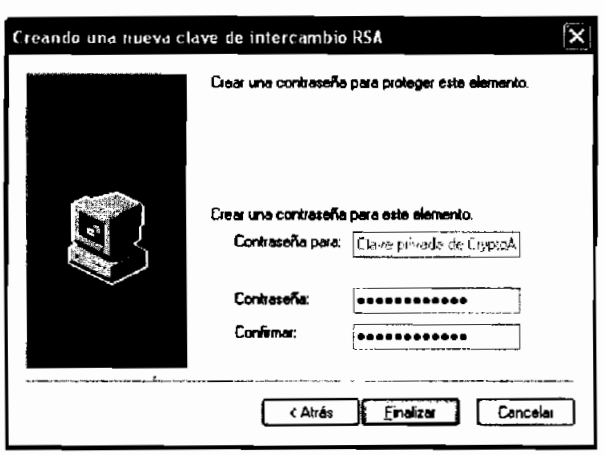


Figura 5.65 Contraseña para Seguridad de la Clave

El nivel de seguridad Alto requiere del establecimiento de mecanismos de seguridad para proteger la clave privada; para esto el asistente de generación de claves solicita una contraseña como se muestra en la figura 5.65. Después de ingresar y confirmar

la contraseña se da un clic en **finalizar** en el cuadro de diálogo de protección de clave y se selecciona **Aceptar** en el cuadro de diálogo de generación de claves.

Si la generación del certificado tuvo éxito, se presenta la pantalla mostrada en la figura 5.66, ahí se da un clic en **Instalar certificado**; entonces se presenta un mensaje solicitando autorización para que el sitio *Web* instale el certificado personal, se da un clic en **Sí**.

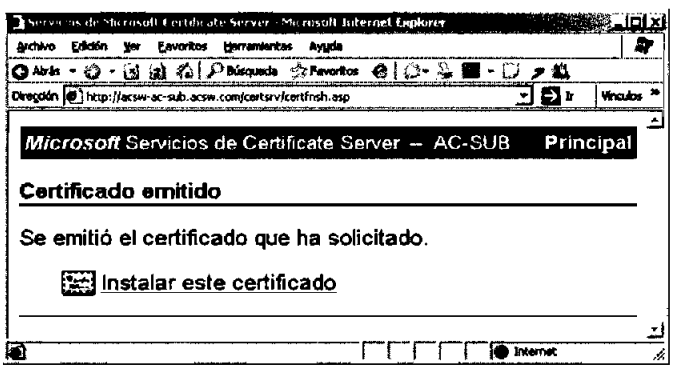


Figura 5.66 Instalación del Certificado

Sí el certificado se instaló correctamente se presenta la pantalla mostrada en la figura 5.67; desde este momento el usuario puede ingresar a la aplicación *certmgr.msc* para administrar su certificado personal como se vio en la sección Configuración del usuario PKI del capítulo 4.

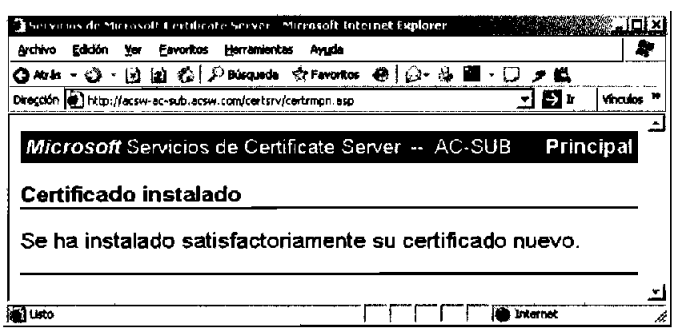


Figura 5.67 Certificado Instalado Exitosamente

5.9. PRUEBAS DE FUNCIONAMIENTO

En la figura 5.68 se muestra un esquema general del ambiente de pruebas, el mismo que cuenta con los siguientes elementos: una AC-Raíz, una AC subordinada, un servidor RADIUS[1], un AP y tres clientes WLAN[2].

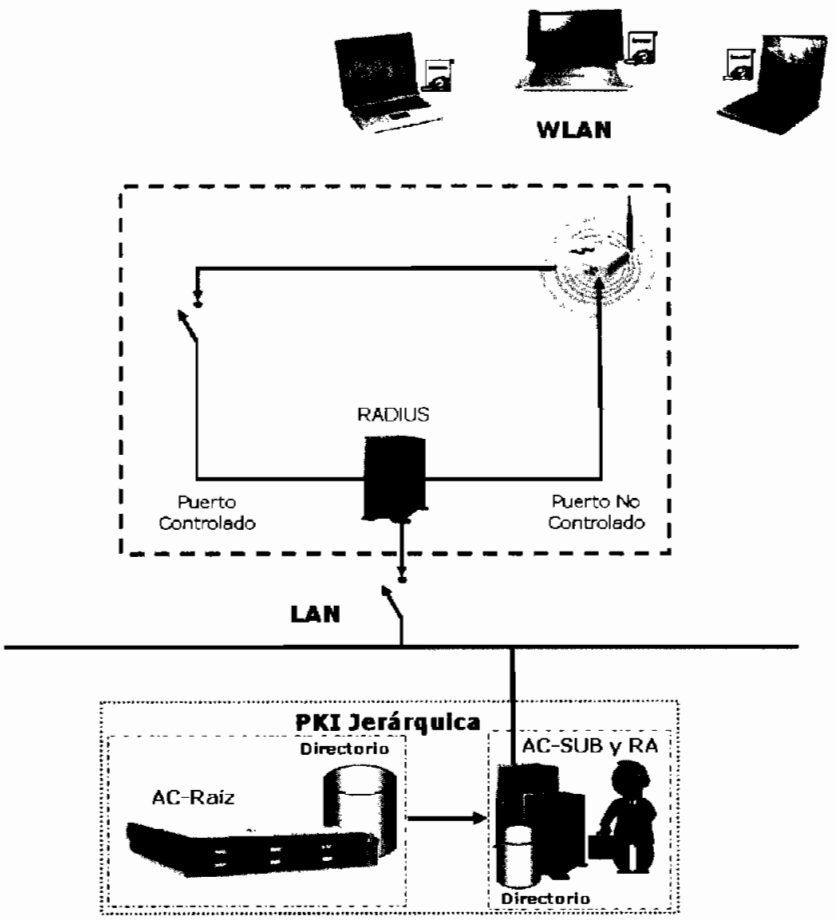


Figura 5.68 Esquema general: Ambiente de pruebas

[1] Instalado en el mismo servidor que la AC subordinada.

[2] No se especifica una marca o modelo, debido a que la solución está destinada a brindar autenticación con EAP-TLS para plataformas de *hardware* que soporten el estándar 802.1x; además, la configuración del cliente OAC es la misma para cualquier cliente *Windows XP Professional*.

5.9.1. REGISTRO DE USUARIOS

Este proceso se inicia registrando los datos del usuario en *Active Directory*, en la figura 5.69 se muestra el cuadro de diálogo de **Propiedades** de un usuario. Como se puede observar, *Active Directory* permite registrar todos los datos personales y corporativos de un usuario.

Cuando el usuario está debidamente registrado en *Active Directory*, puede finalizar el proceso de registro con la PKI ingresando al sitio *Web* de la AC-SUB: http://acsw-ac-sub.acsw.com/certsrv, como se vio en la sección 5.8 de este Capítulo.

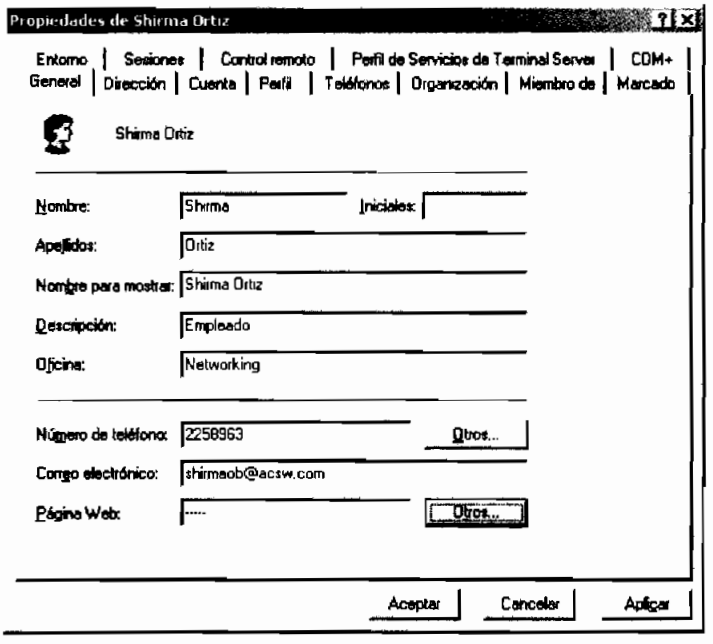


Figura 5.69 Registro de Usuario en Active Directory

5.9.2. CONTENIDO DEL CERTIFICADO DE UN USUARIO

En la figura 5.70 se muestra el certificado digital del Usuario1. Como se puede observar, la pestaña **General** muestra los propósitos para los cuales fue creado el certificado, su período de validez y el emisor (AC-SUB).

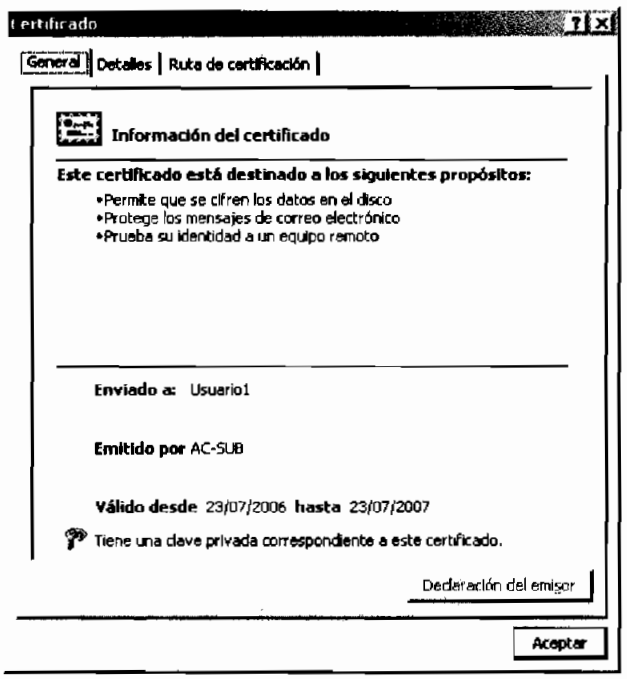


Figura 5.70 Certificado Usuario

Cuando se selecciona la pestaña **Detalles** se puede identificar cada campo del certificado. Para verificar los parámetros de configuración del certificado se da un clic en la opción **Mostrar** y se selecciona **Solo campos versión 1** como se muestra en la figura 5.71.

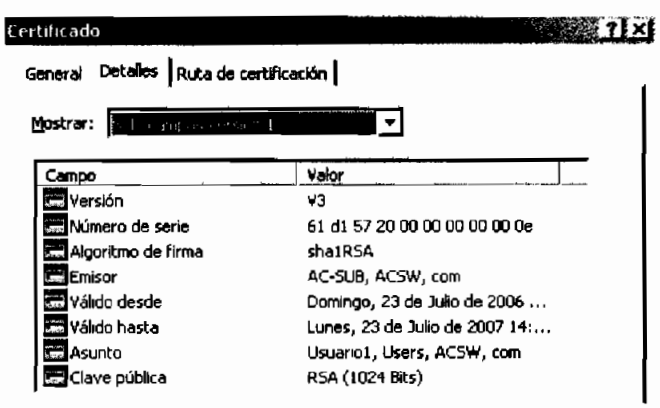


Figura 5.71 Parámetros del Certificado

En la opción **Sólo campos versión 1** mostrada en la figura 5.71 se pueden verificar los siguientes parámetros:

- Versión X.509: v3.
- Número de serie: 61 d1 57 20 00 00 00 00 00 0e.
- El algoritmo *hash*: SHA-1.
- El algoritmo de firma digital: RSA.
- El emisor del certificado: AC-SUB, ACSW, com.
- El propietario del certificado: Usuario1, *User*, ACSW, com.
- Fecha de emisión del certificado: 23 de julio de 2006.
- Fecha de expiración del certificado: 23 de julio de 2007.
- Longitud de la clave: 1024 *bits*.

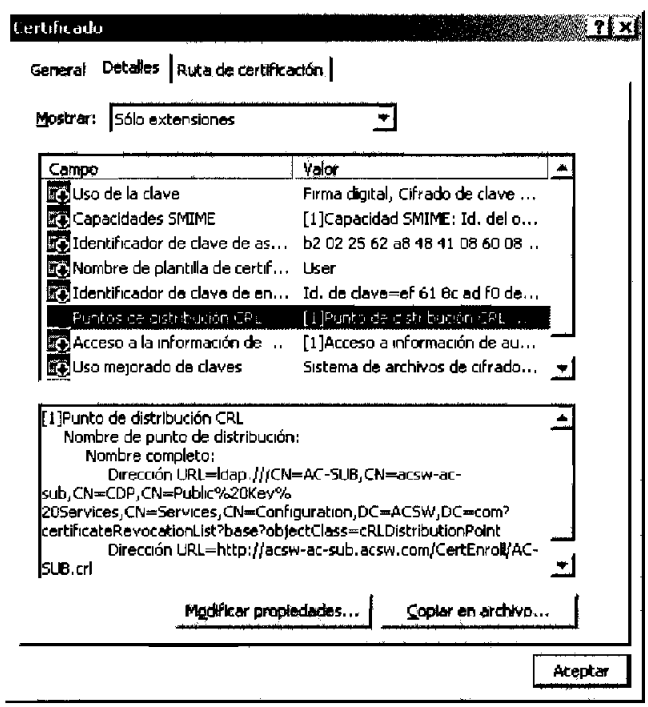


Figura 4.72 Extensiones del Certificado

Para verificar los parámetros relacionados con las extensiones del certificado, se da un clic en la opción **Mostrar** de la pestaña **Detalles** y se selecciona **Solo extensiones** como se muestra en la figura 5.72, como se puede observar, esta sección posee información relacionada con los puntos de distribución e información de la AC-SUB. El certificado de Usuario no posee extensiones críticas.

En la pestaña **Ruta de certificación** mostrada en la figura 5.73, se observa que se trata del certificado de usuario emitido por la AC-SUB, en la parte inferior de la pantalla se comprueba que el certificado es válido.

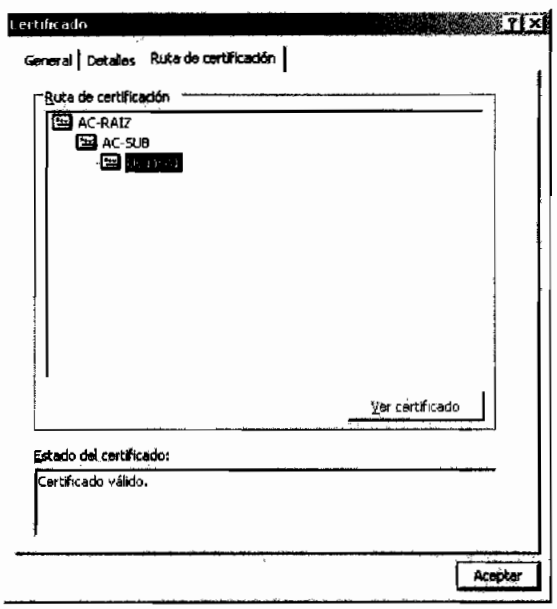


Figura 5.73 Ruta de Certificación

Si se desea acceder a los certificados de las ACs, se selecciona uno y luego se da un clic en el botón **Ver Certificado**.

5.9.3. PUNTO DE DISTRIBUCIÓN

El punto de distribución de la PKI es el sitio *Web*: http://acsw.com, mostrado en la figura 5.74, en este portal los usuarios pueden descargar: la CPS y CP de la PKI, la ruta de confianza de la AC-SUB, CRLs y certificados de la AC-Raíz y de la AC-SUB.

Para descargar una de las opciones disponibles en el punto de distribución, se da un clic sobre su *link*; en el caso de las opciones: Declaración de Prácticas de Certificación, Política de Certificación, Ruta de Confianza, Certificado AC-SUB y

Certificado AC-Raíz, se presenta un cuadro de diálogo como el que se muestra en la figura 5.75, en estos casos se da un clic en el botón **Guardar** y se descarga el archivo a la estación de trabajo.

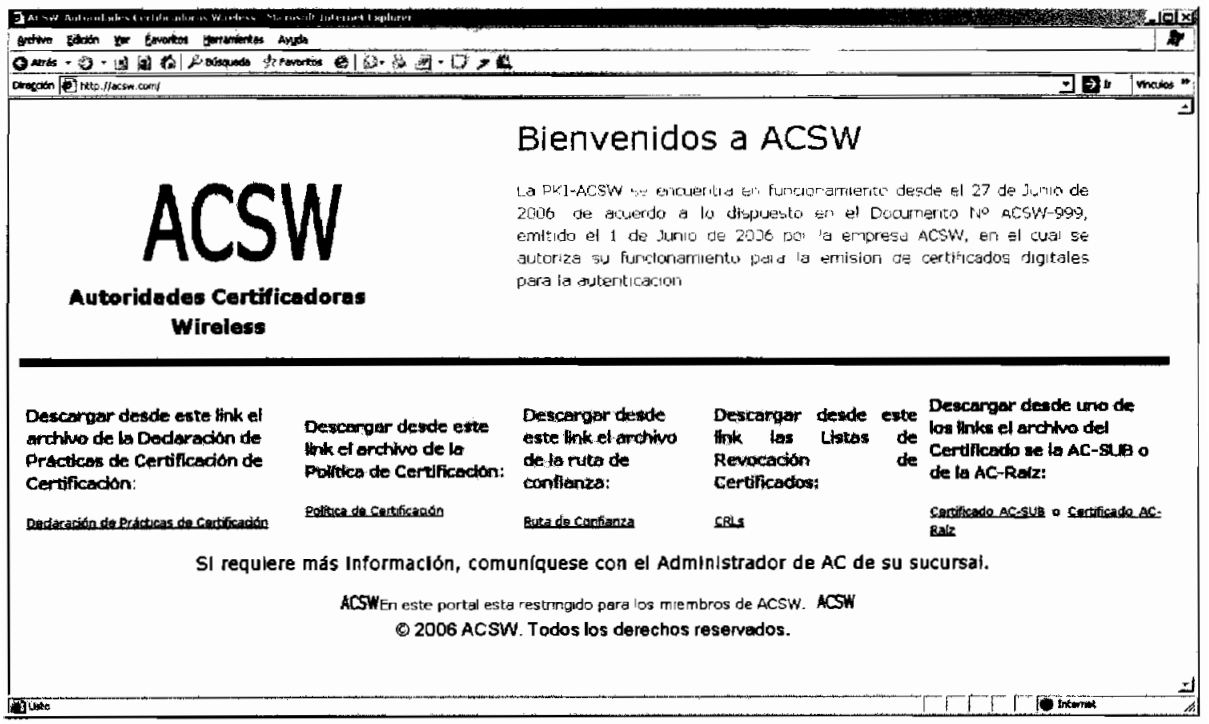


Figura 5.74 Punto de distribución de la PKI-ACSW

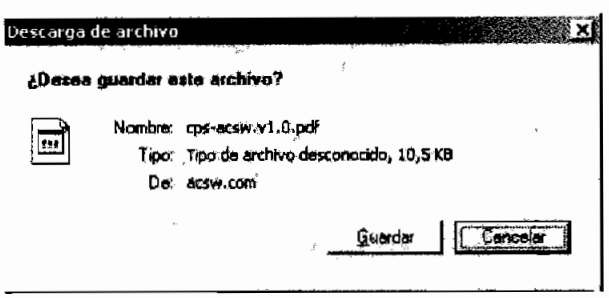


Figura 5.75 Cuadro de diálogo de Descarga de Archivos

Los archivos de la CPS y CP se encuentran en formato pdf, los nombres de los archivos son: *cps-acsw.v1.0.pdf* y *cp-acsw.v1.0.pdf*, respectivamente. La ruta de confianza de la AC-SUB se encuentra contenida en un archivo PKCS#7 con el nombre de *ruta.p7b*.

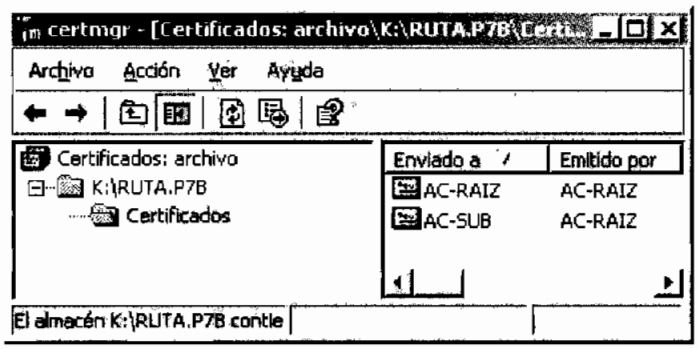


Figura 5.76 Contenido del Archivo ruta.p7b

En la figura 5.76 se muestra el contenido del archivo *ruta.p7b*. Como se puede observar, el archivo contiene el directorio en que se encuentra almacenado y los certificados digitales de la AC-Raíz y de la AC-SUB.

Los archivos de los certificados digitales de la AC-SUB y de la AC-Raíz, respetan el formato X.509, los nombres de los archivos son: *acsw-ac-sub.acsw.com_AC-SUB.cer* y *acsw-ac-raiz.acsw.com_AC-RAIZ.cer*, respectivamente.

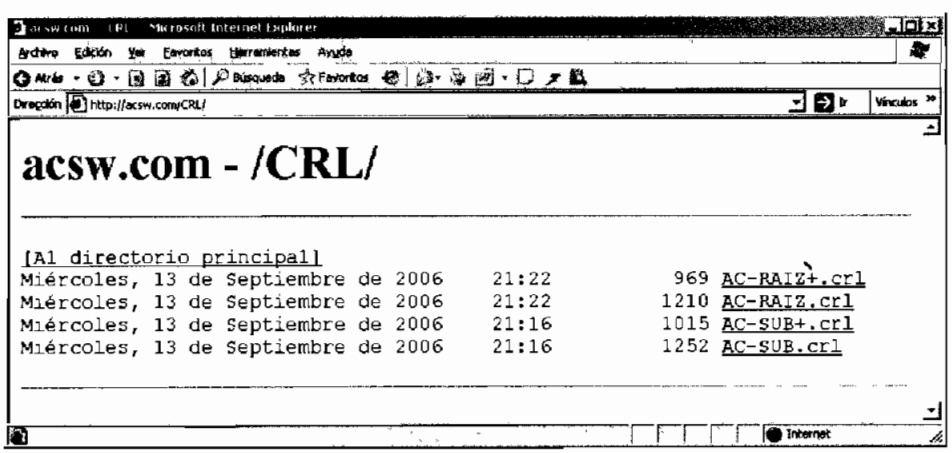


Figura 5.77 http://ascw.com/CRL

Cuando un usuario da un clic sobre la opción CRLs del punto de distribución, accede al portal mostrado en la figura 5.77; éste contiene las listas de revocación de certificados completas (.crl) y *delta* (+.crl) de la AC-Raíz y de la AC-SUB. Para descargar una CRL, por ejemplo, la CRL completa publicada por la AC-SUB, se da

un clic en el *link* AC-SUB.crl y en el cuadro de diálogo que se presenta se da un clic en el botón **Guardar**.

En la figura 5.78 se muestra la CRL AC-SUB; en la pestaña **General** se pueden verificar los siguientes parámetros:

- Versión CRL: v2.
- Emisor: AC-SUB, ACSW, com.
- El propietario del certificado: Usuario1, *User*, ACSW, com.
- Fecha de emisión: 13 de Septiembre de 2006.
- Próxima actualización: 12 de Octubre de 2006.
- El algoritmo *hash*: SHA-1.
- El algoritmo de firma digital: RSA.
- Id. de clave: ef 61 8c ad f0 de 44 6e 34 ce 79 c2 d4 87 5c ed cb 88 5d a7.
- Número de CRL: 11.

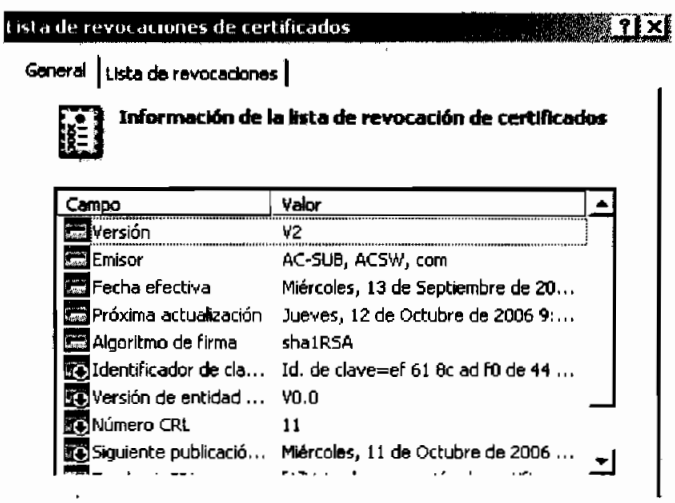


Figura 5.78 CRL AC-SUB

Si se desea verificar la validez de un certificado, se selecciona la pestaña **Lista de revocaciones** mostrada en la figura 5.79. Al seleccionar un certificado dentro de la

lista, en la parte inferior del cuadro de diálogo se presenta información de la revocación.

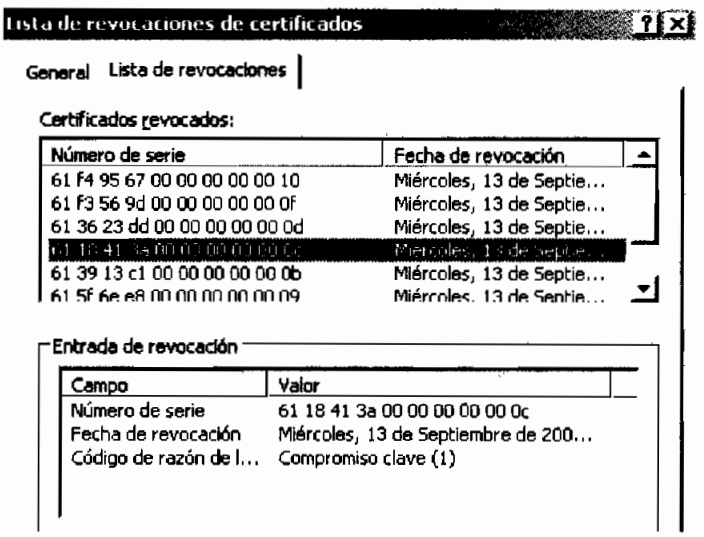


Figura 5.79 Lista de revocaciones de la CRL AC-SUB

5.9.4. ACCESO A LA WLAN

Cuando un usuario WLAN enciende su equipo, el proceso de autenticación inicia después de que éste ingresa su nombre de cuenta y contraseña; entonces el cliente OAC intenta acceder a la clave privada, y la aplicación de protección de claves solicita la contraseña que protege la clave tal como se muestra en la figura 5.80.

Como se puede ver en la figura 5.80, el icono de la conexión WLAN indica el inicio del proceso de negociación para la autenticación; y el icono del cliente OAC se encuentra en estado *disconnected*.

Después de ingresar la contraseña y permitir el acceso a la clave privada se inicia el intercambio de credenciales y parámetros TLS. Para verificar el proceso, se ingresa en el menú ***Status*** del AP y se selecciona la pestaña ***Log*** como se muestra en la figura 5.81.

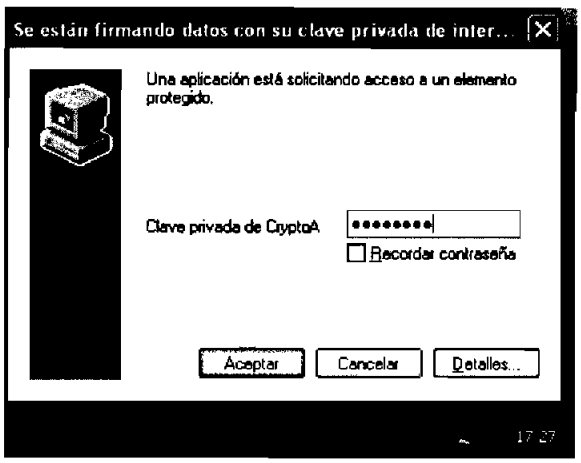


Figura 5.80 Acceso a la Clave Privada

El proceso registrado en la figura 5.81 indica que para iniciar el proceso, el AP se conecta con el servidor RADIUS; luego verifica que la dirección MAC del equipo esté registrada dentro de su lista de direcciones de confianza. Si la autenticación MAC es exitosa el equipo queda asociado y puede continuar con la autenticación EAP-TLS, caso contrario el equipo queda desasociado del AP.

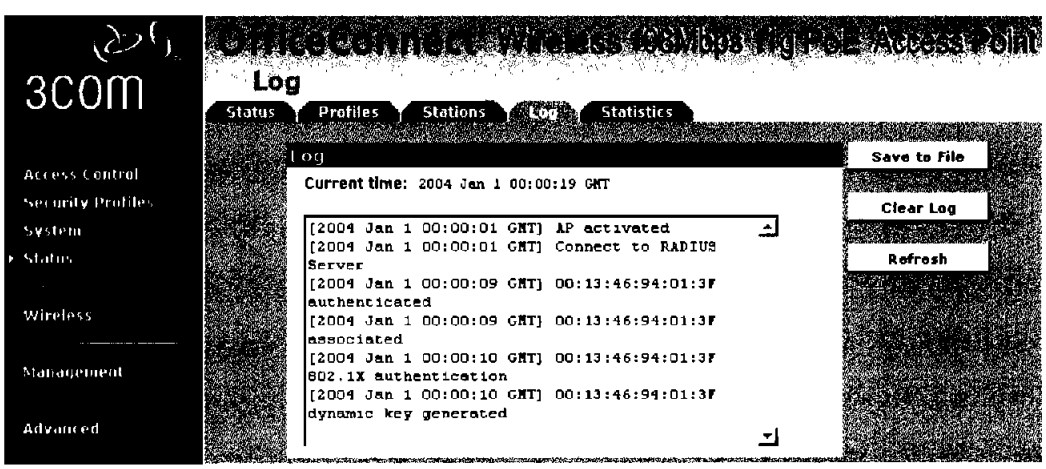


Figura 5.81 Registro AP

Durante el proceso de negociación para la autenticación se genera una clave dinámica para cifrar la comunicación. El servidor DHCP sólo asigna una dirección después que las credenciales del usuario han sido validadas exitosamente.

Figura 5.82 Cliente OAC después de una Autenticación Exitosa

En la barra de tareas de *Windows* se puede verificar el estado de la comunicación; en la figura 5.82 se muestra al cliente OAC en estado *open and authenticated* y en la figura 5.83 se muestra el estado de la conexión WLAN.

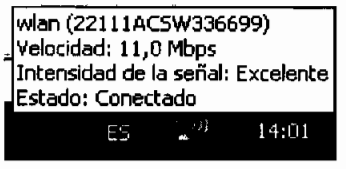


Figura 5.83 Estado de la Conexión después de una Autenticación Exitosa

También se puede verificar el estado de la comunicación a través de la aplicación *Odyssey Client Manager*, como se muestra en la figura 5.84. En la parte inferior derecha de la aplicación se muestra el estado de la comunicación de acuerdo a las siguientes especificaciones:

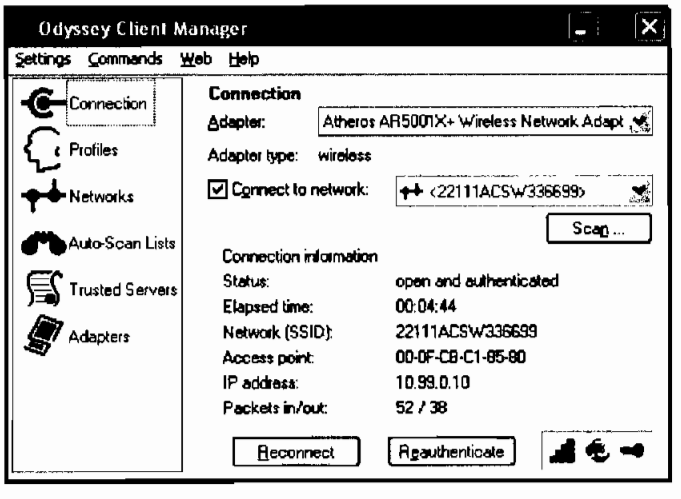


Figura 5.84 Estado de la Conexión después de una Autenticación Exitosa

- ***Signal Power***.- El icono en verde representa la calidad de la señal, en este caso, se tiene una señal excelente; si éste se torna gris indica que el equipo no se encuentra dentro del área de cobertura de la red.

- ***Last authentication results***.- El icono intermedio representa el resultado del último intento de autenticación, el color gris indica que el equipo está desconectado de la red, en tanto que el color rojo indica que la autenticación ha fallado. Si la autenticación ha sido exitosa, el icono se torna azul.

En la figura 5.85 se muestra una autenticación EAP-TLS exitosa, en el campo *Cipher suite* se muestran los algoritmos utilizados para establecer los servicios de autenticación, confidencialidad e integridad, respectivamente.

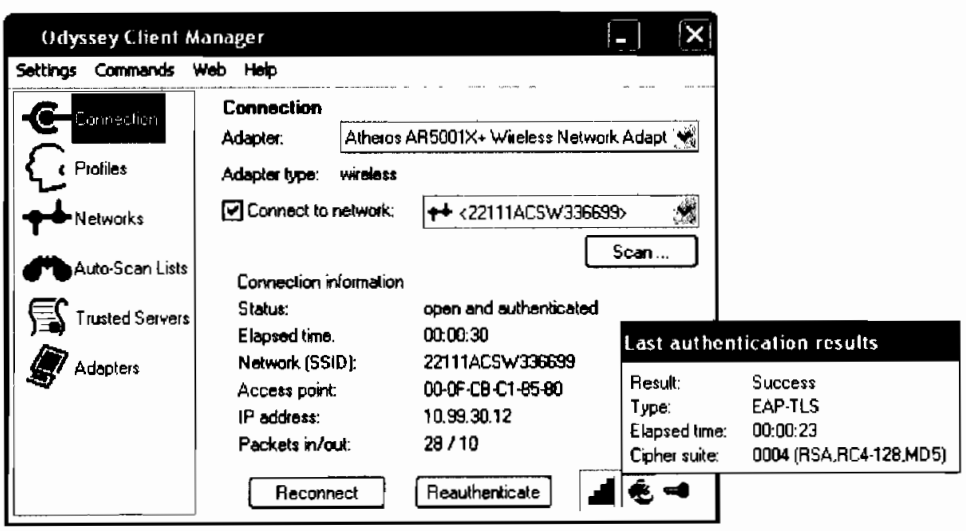


Figura 5.85 Autenticación Exitosa

En la figura 5.86 se muestra el resultado de un intento de autenticación fuera del horario establecido; como se puede observar, la conexión fue rechazada por el servidor.

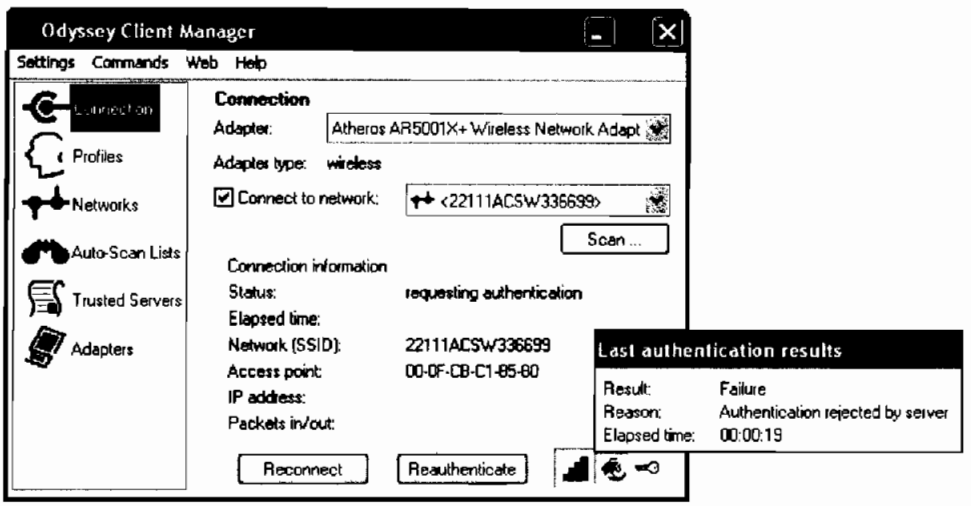


Figura 5.86 Autenticación Rechazada debido a Incumplimiento en el Horario Permitido

Finalmente, en la figura 5.87 se muestra el resultado de un intento de autenticación con un certificado revocado; como se puede observar, la conexión fue rechazada por el servidor.

Figura 5.87 Autenticación Rechazada por Certificado Revocado

- ***Encryption***.- Este icono está representado por la llave, si se torna azul indica que se está cifrando las comunicaciones como se muestra en la figura 5.88; de lo contrario el icono se muestra gris.

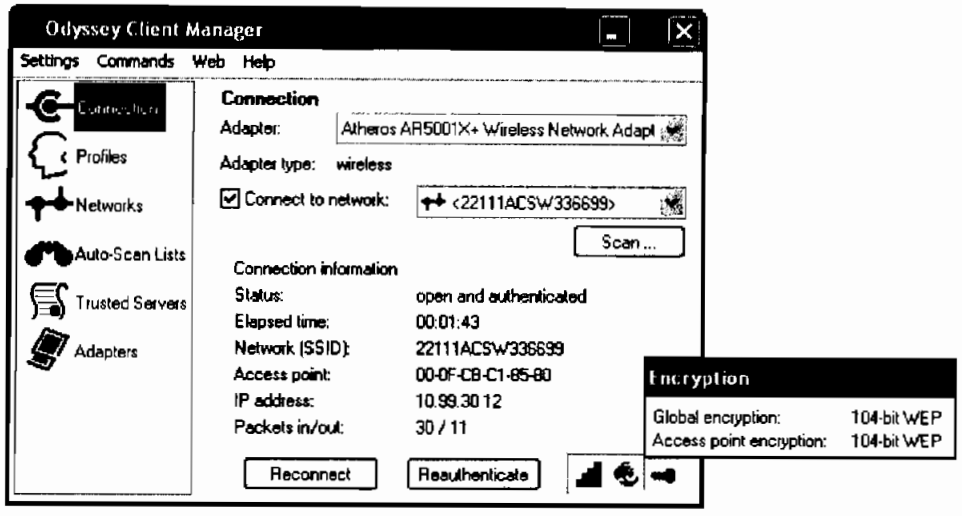


Figura 5.88 Autenticación Rechazada por Certificado Revocado

5.10. PRESUPUESTO REFERENCIAL

La implementación de una solución de seguridad en WLANs con EAP-TLS y una PKI jerárquica requiere de la adquisición de los siguientes equipos: una AP por cada 150 m^2 (aproximadamente) y servidores para la PKI jerárquica y el servidor RADIUS. Además se requiere licencias del sistema operativo *Windows 2003 Server Enterprise* y de los clientes OAC.

La solución planteada contempla la instalación de una PKI jerárquica de dos niveles, la cual está formada por una AC-Raíz y una AC subordinada; el servidor RADIUS funcionará en el mismo equipo que la AC subordinada. Todas las características técnicas de este servidor se encuentran registradas en la sección Presupuesto Referencial del capítulo 4.

El servidor AC-SUB/RADIUS incluido en el primer literal (PKI jerárquica) del presupuesto consta de 25 licencias CALs, por lo tanto, puede atender a 25 entidades; sin embargo, sus características técnicas le permiten atender hasta 75 usuarios simultáneamente.

En la tabla 5.5 se muestra un desglose del presupuesto final de la solución de seguridad en WLANs con EAP-TLS y una PKI jerárquica de dos niveles; el presupuesto considera la compra de licencias, servidores, un AP y los costos de mano de obra por la instalación y configuración de los equipos.

La implementación de esta solución para una sucursal adicional incrementa el presupuesto en 7263,39 dólares (no se contemplan paquetes OAC adicionales); por otro lado, si se requiere que más clientes accedan a los servicios del servidor AC-SUB/RADIUS, un paquete adicional con 20 CALs, tiene un costo de 799 dólares.

SOLUCIÓN EAP-TLS[1]					
#	Tipo	Descripción	Cantidad	Precio Unitario	Precio Total
1	PKI Jerárquica	PKI diseñada en Capítulo 4	1	$ 13001	$ 13001
2	AP	*Access Point* 3Com 3CRGPOE10075	1	$ 155.39[2]	$ 155.39
3	Configuración del AP	Configuración básica de seguridad y parámetros 802.1x.	2 HT	$ 50	$ 100
4	Cliente OAC	Paquete con 25 licencias *Odyssey Access Client* v4.51; compatibles con *Windows* 98/98SE/2000/Me/XP.	1	$ 1089.95[3]	$ 1089.95
5	Configuración RADIUS	Configuración del servidor RADIUS para el control de autenticación EAP-TLS.	2 HT	$ 50	$ 100
6	Configuración de usuarios.	Instalación de *software cliente* y configuración de EAP-TLS en usuarios de la WLAN.	2 HT (5 usuarios)	$ 100	$ 100
7	Instalación de Equipos	Instalación de servidor y AP	1 HT	$ 50	$ 50
				TOTAL:	**$ 14596.34**

Tabla 5.5 Presupuesto final para una WLAN con autenticación EAP-TLS[4]

En el presupuesto referencial no se incluyen los equipos clientes, debido a que la solución EAP-TLS puede brindar servicios para cualquier cliente WLAN que soporte 802.1x.

---

[1] Este presupuesto no incluye los equipos clientes.

[2] www.amazon.com.

[3] http://accessories.gateway.com/AccessoryStore/Software_316896/AntiVirus+_A1_+Utilities_316962/Security_316968/12643804_ProdDetail.

[4] Este presupuesto no incluye impuestos ni transporte.

La implementación de esta solución demanda de una inversión superior a la requerida por otras soluciones de seguridad para WLANs; sin embargo se justifica plenamente por el nivel de seguridad entregado. Además, puede funcionar como un proyecto piloto en el que los usuarios se familiaricen con el uso de herramientas criptográficas, después de lo cual puede aplicarse dentro de otras áreas.

Según *CSO Magazine*[1], en el año 2003 el 70 % de las empresas de estados unidos sufrió un ataque; las pérdidas ocasionadas por estos ataques alcanzaron un monto total de 666 millones de dólares.

Estas cifras hacen referencia al conjunto de redes cableadas e inalámbricas; sin embargo, debido a que las redes inalámbricas son más susceptibles a ataques en comparación con las redes cableadas; la inversión en mecanismos de seguridad en este tipo de red es primordial.

[1] http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_4563.html.

Capítulo 6

CONCLUSIONES Y RECOMENDACIONES

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

El avance tecnológico y la creciente tendencia al comercio electrónico, han logrado que las empresas estén obligadas a compartir información a través de sus redes corporativas y del Internet. Bajo estas circunstancias, cada empresa debe encontrar estrategias de seguridad que permitan un acceso máximo a la información y recursos para los usuarios lícitos y que restrinjan el acceso para otros usuarios; para seleccionar una estrategia adecuada se debe considerar los siguientes aspectos:

- Requerimientos de seguridad.
- Presupuesto.
- Aplicabilidad.
- Incremento en los procesos administrativos.

Una WLAN está expuesta a todos los ataques aplicables a una LAN cableada, con una diferencia, en este tipo de redes su medio de transmisión está expuesto. Siendo así, es indispensable la introducción de una política de seguridad elemental, que garantice niveles aceptables de operación; si la WLAN está ligada a una LAN cableada, durante la creación de la política de seguridad, se debe considerar los requerimientos de la WLAN y las condiciones de la red LAN y sus puntos críticos.

Antes de seleccionar una técnica de autenticación, se debe estimar el nivel de seguridad requerido y los recursos disponibles para su implementación. Durante la operación del sistema de autenticación, hay que considerar que el nivel de seguridad obtenido no solo depende de la cantidad de recursos invertidos, sino también de la forma en que se aplica y protege el método seleccionado.

Los sistemas de autenticación basados en EAP-TLS proveen un alto nivel de seguridad siempre que la clave privada se encuentre protegida. Para la protección de la clave privada, se debe establecer un método que garantice la auto-autenticación de su propietario. Adicionalmente, es necesario capacitar y concientizar a los usuarios, y en algunos casos se puede requerir la adición de un contrato, en el que el usuario se comprometa a respetar la política establecida dentro de la empresa.

El uso de encripción asimétrica y PKI no tuvo una expansión significativa hasta el aparecimiento del comercio electrónico; éste ha logrado que se incremente el número de transacciones realizadas a través de redes corporativas e Internet, a través de aplicaciones basadas en certificados digitales, estos certificados están ligados a la confianza proporcionada por PKI. El creciente uso de tecnologías PKI marca una nueva etapa en la evolución de las herramientas de encripción asimétrica; en pocos años, se podría utilizar esta técnica para reemplazar los sistemas actuales de facturación, contratación e incluso de sufragio.

PKI basa su funcionamiento en la confianza que los usuarios tienen sobre los certificados emitidos por una determinada AC. En el caso de una PKI corporativa, los niveles de confianza en ésta son elevados, debido a que los usuarios se encuentran directamente relacionados con la AR y el Administrador de AC, y tienen la certeza de que los certificados digitales son emitidos por una AC de la PKI para un usuario lícito.

La Ley 67 y su reglamento brindan flexibilidad para la introducción de tecnologías que involucren el uso de medios electrónicos (neutralidad tecnológica). Además, reconocen los derechos y obligaciones de los usuarios y proveedores de servicios basados en estas tecnologías. En el caso de PKI, la Ley abarca de forma limitada a cada una de sus entidades; en cada caso, define flexiblemente su ámbito de operación, dejando abierta la posibilidad de establecer lineamientos claros a partir de resoluciones emitidas por el CONATEL. Sin embargo, la resolución 584 emitida por

el CONATEL, restringe la operación de una PKI e introduce trámites burocráticos innecesarios, limitando la autonomía de la infraestructura.

La PKI del BCE cuenta con una infraestructura tecnológica que cumple con un nivel satisfactorio de seguridad para la autenticación ante las aplicaciones del SNP. De acuerdo a los resultados encontrados durante el estudio de mercado, se puede concluir lo siguiente:

- Los usuarios y responsables de certificados perciben niveles adecuados de seguridad y confiabilidad dentro de cada proceso.
- El soporte técnico brindado por los Administradores de la PKI mantiene niveles aceptables de satisfacción.
- Es necesario concientizar a los usuarios y responsables sobre: protección de claves privadas, manejo de códigos de activación, procedimientos, etc.
- Es necesario crear una CPS en la que se establezca de manera clara los procedimientos utilizados dentro de la PKI.

Para la implementación de una PKI jerárquica, la solución presentada por *Windows* resulta apropiada, pues contiene herramientas que permiten la generación de ACs raíces y subordinadas, estableciendo mecanismos para la administración de certificados y CRLs; además, admite la distribución de certificados de confianza a través de *Active Directory* de manera transparente para los usuarios dentro del dominio.

Dentro de la operación de una PKI, es importante considerar que aunque los certificados hayan caducado, su ciclo de vida legal puede ser más largo[1]; por ejemplo: una firma digital, se puede validarse incluso si el certificado o las claves relacionadas con ésta han caducado.

---

[1] Esto no se aplica al ambiente EAP-TLS, debido a que la pareja de claves es utilizada para el intercambio de claves simétricas.

La seguridad obtenida con un sistema de autenticación basado en EAP-TLS, depende de la creación de una CP y CPS adecuadas; además, se debe verificar su cumplimiento y funcionamiento, en caso de encontrar falencias, se debe replantear políticas y procedimientos.

6.2. RECOMENDACIONES

Es importante considerar que la implementación de una PKI requiere de una participación adecuada de los usuarios. En muchos casos, esto no se logra tan solo con capacitación, pues el comportamiento de los usuarios está relacionado con aspectos culturales; siendo así, es recomendable la implementación de un proyecto piloto en el que se pueda medir en la práctica la aplicabilidad de la estrategia.

La administración adecuada de un AP es importante para brindar seguridad al sistema, logrando un mejor funcionamiento. A continuación se presenta una lista de prácticas recomendadas:

- Analizar el nivel de seguridad requerido y de acuerdo a esto, determinar: capacidades, funcionalidades y nivel de compatibilidad de los equipos.
- Cambiar los parámetros configurados por defecto.
- Realizar un análisis de los servicios que debe brindar el AP; los servicios que no sean necesarios deben desactivarse.
- Mantener habilitado SNMP si se cuenta con un monitoreo que permita envío de mensajes SNMP versión 3; de lo contrario, se recomienda crear listas de acceso con permisos de solo lectura.
- Evitar que el identificador de la comunidad SNMP y el SSID proporcionen información de la red.
- Deshabilitar el *broadcast* de SSID dentro de las tramas *beacon*.
- Para la configuración de los APs, se debe crear usuarios con perfiles de lectura-escritura y para el monitoreo con perfiles de solo lectura.

- Configurar RADIUS en un AP sólo si se requiere este servicio.
- Mantener actualizado el *firmware* de los Aps y las tarjetas inalámbricas.
- Capacitar a los usuarios para que no introduzcan malas prácticas.
- Cifrar la información crítica.
- De ser posible, establecer un sistema de administración y autenticación centralizado.
- Limitar el acceso físico a los APs.
- Proporcionar a los usuarios información sobre:
    - El uso adecuado de los adaptadores inalámbricos.
    - Manejo del SSID.
    - Protección de la clave privada y de la contraseña relacionada con ésta.
    - Acceso a redes desconocidas, etc.

Si se posee recursos suficientes, es recomendable instalar el servidor RADIUS en un equipo independiente de la AC-SUB, debido a que los clientes WLAN interactúan con éste de manera constante, mientras que requieren acceder a la AC-SUB sólo para solicitudes o renovaciones de certificados, y estos eventos se presentan en contadas ocasiones.

Para la implementación PKI deben tomarse en cuenta las siguientes recomendaciones:

- La AC-Raíz debe conectarse a la red sólo cuando se haya planificado un evento de actualización de CRLs o emisión de certificados.
- En el caso de la AC-Raíz, es recomendable eliminar los permisos de solicitud de certificado para los administradores, cuando no se tenga planeada la emisión de certificados para ACs subordinadas, debido a que los certificados de administrador no tienen restricciones de uso.
- Se debe evitar el acceso directo a la carpeta *CertEnroll*, debido a que los usuarios no están familiarizados con el ambiente y en el inicio de la implementación no distinguirán una CRL de un certificado.

- Es recomendable renovar un certificado inmediatamente después de su revocación, para que el certificado revocado se retire del directorio del dominio.

Es importante tomar en cuenta que las políticas de seguridad, CPs y CPSs son documentos legales; por lo tanto, deben ser revisados por el departamento jurídico de la organización antes de su publicación, con el fin de asegurar que los documentos sean aplicables y transmitan con fidelidad su propósito. Cuando la CP y la CPS revelan demasiada información del funcionamiento de la PKI, es recomendable crear un PDS[1], este documento contiene un resumen que proporciona sólo información general del funcionamiento de la PKI.

Número de usuarios (n)	OAC[2] [$]	*Entrust IdentyGuard*[2] [$]	*Token RSA SecurID*[3] [$]
n=25	1089,34	----	----
n=350	15.259,00	22.805,00	45.590,00
n=1000	43.598,00	49.304,00	95.946,00
n=10000	435.980,00	99.209,00	694.989,00

Tabla 6.1 Comparación de Costos entre Clientes Basados en Software y Hardware

En la tabla 6.1 se incluye la variación de los precios de clientes WLAN basados en *software* y *hardware* de acuerdo al número de usuarios. De acuerdo a estos datos, el uso del cliente OAC, es recomendable para redes WLAN corporativas con un número de usuarios menor o igual a 350. Para redes con un número de usuarios entre 350 y 1000, la decisión puede basarse en los requerimientos de seguridad de la empresa, si éstos son elevados, será más recomendable el uso de clientes *hardware*. Finalmente, en el caso de redes corporativas con un número de usuarios superior a 1000, es recomendable el uso de *tokens* o tarjetas inteligentes, debido a que éstos proporcionan mayor seguridad y al ser adquiridos a gran escala no introducen una diferencia considerable en el monto final de inversión.

---

[1] *PKI Disclosure Statement.*

[2] http://accessories.gateway.com/AccessoryStore/Software_316896/AntiVirus+_A1_+Utilities_316962/Security_316968/12643804_ProdDetail.

[3] http://www.entrust.com/strong-authentication/identityguard/calculator.cfm#results.

Bibliografía

BIBLIOGRAFÍA

APUNTES

Apuntes de clase de Redes LAN, Ing. Pablo Hidalgo. (Escuela de Ingeniería – EPN).

Apuntes de Clase, Seguridad en Redes, Ing. Nelson Ávila. (Escuela de Ingeniería – EPN).

Apuntes de Clase, Muestreo, Mat. Carlos Echeverría (Escuela de Ciencias – EPN).

Apuntes de Clase, Generación de Empresas, Ing. Jaime Cadena (Escuela de Ciencias – EPN).

LIBROS

LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS. Abril 2002.

NASH, Andrew. PKI-Infraestructura de Claves Públicas. Primera Edición. Osborne McGraw-Hill, Bogota, 2002.

KOMAR, Brian. Windows Server 2003 PKI Certificate Security. Microsoft Press. Estados Unidos. 2004.

KAUFMANN, Russ. MCSA/MCSE: Windows® Server 2003 Network Security Administration, Study Guide. SYBEX. Estados Unidos. 2004.

TANENBAUM, Andrew. Redes de Computadoras. Cuarta Edición. Prentice Hall. México. 2003.

GAST, Mattbew. 802.11 Wireless Networks. Primera Edición. O'REILLY. Estados Unidos. Abril-2002.

Libro Técnico de CISCO. Certified Wireless Network Administrator. Planet3 Wireless. 2002.

CHOUDHURY, Suranjan. Public Key Infrastructure, Implementation and Design. Primera Edición. Professional Mindware. Estados Unidos. 2003.

RAINA, Kapil. PKI, Security Solutions for the Enterprise. Primera Edición. Professional Mindware. Estados Unidos. 2003.

MARTÍNEZ, Ciro. Estadística y muestreo. Onceava Edición. Ecocediciones. Bogota. 2002.

MARTÍNEZ, Ciro. Estadística Básica Aplicada. Segunda Edición. Ecocediciones. Bogota. Marzo 2002.

Ferguson, Bill. Designing Security™ for a Windows® Server™ 2003 Network Exam Cram™ 2 (Exam 70-298). Microsoft Press. Mayo 2004.

DAVIES, Joseph. Microsoft Windows Server 2003, TCP/IP Protocols and Services. Microsoft Press. 2003.

ARTÍCULOS

BCE

REFORMAS DEL SISTEMA DE PAGOS. 2003.

3COM

OfficeConnect® Wireless 11b/g PoE Access Point User Guide. Diciembre 2004.

OfficeConnect® Wireless 11b/g PoE Access Point Data Sheet. Abril 2006.

Foundry Networks

802.1X AUTHENTICATION & EXTENSIBLE AUTHENTICATION PROTOCOL (EAP). Mayo 2003.

802.1X PORT AUTHENTICATION WITH MICROSOFT'S ACTIVE DIRECTORY. Marzo 2003.

DirecTrust

Polítca de Certificación (PC) para certificados de Clave Pública (PKC). 2005.

NetFocus
Declaración de Prácticas de Certificación (DCP), para Certificados de Clave Pública (PKSs). 2005.

Gartner
LINUX HAS A FIGHT ON ITS HANDS IN EMERGING PC MARKETS. Septiembre 2004.
Costs and Benefits Still Favor Windows Over Linux Among Midsize Businesses. Octubre 2005.

Cultural Santa Ana
Etapas del Proceso Investigador. 2005.

ESI (*European Software Institute*)
Infraestructura de Clave Pública. 2005.

UNA y CNC (Universidad Nacional de Asunción y Centro Nacional de Computación – Paraguay)
Infraestructura para la Criptografía de Clave Pública. 2004.

Universidad Politécnica de Cataluña
Cryptographic Message Sintax. Diciembre 2005.

eTOKEN
Firma Digital-Soluciones Seguras. 2005.

Network Logistics Company
Wireless LAN Security & Manageability. 2005.

IETF (Internet Engineering Task Force)
RFC 3748 Extensible Authentication Protocol (EAP). Junio 2004.
RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Enero 1999.
RFC 3647. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Noviembre 2003.

RFC 2716 PPP EAP TLS Authentication Protocol. Octubre 1999.
RFC 3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. Septiembre 2003.
RFC 4210. Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). Septiembre 2005.
RFC 2797. Certificate Management Messages over CMS. Abril 2000.
RFC 4211. Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF). Septiembre 2005.
RFC 2560. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Junio 1999.
RFC 3852. Cryptographic Message Syntax (CMS). Julio 2004.
RFC 2196. Site Security Handbook. Septiembre 1997.
draft-ietf-pkix-scvp-23. Standard Certificate Validation Protocol (SCVP). Marzo 2006.
The SSL Protocol Version 3.0. Noviembre 1996.
draft-ietf-tls-rfc2246-bis-13. nternet Public Key Infrastructure; Part VI: Notary Protocols. Julio 1997.
draft-ietf-pkix-ipki6np-00. The TLS Protocol Version 1.1. Junio 2005.
TWG-98-59. Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations. Septiembre 1998.

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission)
Text of ISO/IEC FDIS 17799: 2005-02-11-Information techniques- Security techniques-Code of practice for information security management (2nd edition). Febrero 2005.

PCWorld
Safari tecnológico-guía de compras. Diciembre 2004.

PGP
The OpenPGP Standard & PGP Products. Mayo 2005.

RSA (Rivest, Shamir, Adleman**) Laboratories**
RSA Data Security. 1998.
A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Septiembre 1997.

PKCS #1 v2.1: RSA Cryptography Standard. Junio 2002.
Bulletin 13. A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths. Abril 2000.

UIT-T (Unión Internacional de Telecomunicaciones: Sector de Normalización de las Telecomunicaciones)
X.509: Series X: Data Networks, Open System Communications And Security. Agosto 2005.
Q.817: Serie Q: Conmutación Y Señalización, Interfaz Q3. Certificados digitales de la infraestructura de claves públicas de la red de gestión de las telecomunicaciones y perfiles de listas de revocación de certificados. Enero 2001.
Grupo de Trabajo 17. ITU-T The leader on ASN.1 Standards. Mayo 2006.

IEEE (Institute of Electrical and Electronics Engineers)
IEEE Standard for Local and Metropolitan Area Networks: Standard for Port based Network Access Control. IEEE 802.1x. 2001.
802.11i Overview. Febrero 2005.
IEEE Information Theory Society Newsletter. Marzo 2004.

NMC Research
Algoritmo NMC Stream, Descripción y Formalización. Febrero 2004.

ETSI (European Telecommunications Standards Institute)
ETSI SR 002 176 V1.1.1: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures. Marzo 2003.

NIST (National Institute of Standards and Technology)
FIPS (*Federal Information Processing Standards*) PUB 46-3 : Data Encryption Standard (DES). Octubre 1999.
FIPS PUB 197 : Advanced Encryption Standard (AES). Noviembre 2001.

Mugino Saeki
Elliptic Curve Cryptosystems. Febrero 1997.

Yankee Group
2005 North American Linux and Windows TCO Comparison, Part 1. Abril 2005.

2005 North American Linux and Windows TCO Comparison Report, Part 2: Hardening Security Is Key to Reducing Risk and TCO. Julio 2005.

Ideas Custom Consulting Services
Microsoft Windows Server vs. Red Hat Enterprise Linux: Costs of Acquisition and Support – A Comparison. Agosto 2005.

ANSI/TIA/EIA (*American National Standards Institute /Telecomunications Industries Association/ Electronics Industries Association*)
Technical Information: ANSI/TIA/EIA-569-A. 2005.

DIRECCIONES ELECTRÓNICAS

Airgo
Airgo.
http://www.airgonetworks.com/

PCWorld
First Draft-N Routers Don't Impress.
http://www.pcworld.com/article/id,125634-page,1/article.html

PCMag
Draft-N Fails to Deliver.
http://www.pcmag.com/article2/0,1895,1977784,00.asp

Wi-FiPlanet
802.11n Draft Approved.
http://www.wi-fiplanet.com/news/article.php/3578886

Entrust
Entrust IdentityGuard Price Comparison Calculator.
http://www.entrust.com/strong-authentication/identityguard/calculator.cfm#results

Advento Networks

Estándares para el entorno de la gestión de las redes inalámbricas bajo la denominación 802.11.

http://www.e-advento.com/tecnologia/estandares.php

Intel

Wireless LAN Products-Wireless Security – 802.1x and EAP Types.

http://support.intel.com/support/wireless/wlan/sb/cs-008413.htm

IEEE

Official IEEE 802.11 Working Group Project Timelines - 09/01/06.

http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

Cisco

Cisco Systems Completes Acquisition of Meetinghouse Data Communications

http://newsroom.cisco.com/dlls/2006/corp_081606.html

Microsoft

Installing Windows Server 2003 R2.

http://www.microsoft.com/windowsserver2003/R2/trial/installinstruct.mspx

Windows Server 2003: Guía CAL.

http://www.microsoft.com/latam/softlegal/sam/lic_cal_win2003_server.mspx

Windows Server 2003 R2 Pricing.

http://www.microsoft.com/windowsserver2003/howtobuy/licensing/pricing.mspx

Windows vs. Linux, Mitos y Realidades.

http://www.microsoft.com/spanish/msdn/comunidad/mtj.net/voices/art184.asp#ref01

Descripción de la característica Protección de archivos de Windows.

http://support.microsoft.com/?kbid=222193

Objete que identificadores asociaron a criptografía de Microsoft.

http://support.microsoft.com/?id=287547

How CA Certificates Work.

http://technet2.microsoft.com/WindowsServer/f/?en/Library/0e4472ff-fe9b-4fa7-b5b1-9bb6c5a7f76e1033.mspx

How Certificates Work.

http://technet2.microsoft.com/WindowsServer/en/Library/fb3df0cd-0aae-472b-9e9c-bb8ca878bc341033.mspx?mfr=true
How Certificate Services Works.
http://technet2.microsoft.com/WindowsServer/en/Library/2d98e8a9-b019-44eb-9558-d081590bce871033.mspx?mfr=true

RSA Security
RSA Laboratories.
http://www.rsasecurity.com/rsalabs/node.asp?id=2153

NetworkWorld
802.11h helps WLANs share spectrum.
http://www.networkworld.com/news/tech/2004/071904techupdate.html

Alvestrand Data
Authenticode Microsoft OIDs.
http://www.alvestrand.no/objectid/1.3.6.1.4.1.311.2.html

Hewlett-Packard
Server buying guide.
http://www.hp.com/cgi-bin/sbso/buyguides/tsg_product_select.cgi

IBM
Tower servers.
http://www-03.ibm.com/systems/x/tower/index.html
Rack-optimized servers.
http://www-03.ibm.com/systems/x/rack/index.html

Sun Microsystems
Sum store US.
http://store.sun.com/

Amazon
3COM Corp OFFICECONNECT WRLS 108MBPS 11G (3CRGPOE10075-US).
http://www.amazon.com

IETF

PKIX.

http://www.ietf.org/ids.by.wg/pkix.html

Public-Key Infrastructure (X.509) (pkix).

http://www.ietf.org/html.charters/pkix-charter.html

Banco Central del Ecuador

Emisión de certificados Digitales Del Banco Central Del Ecuador.

https://sas.bcepki.bce.fin.ec/enroll/

IWORLD

SET a fondo Secure Electronic Transaction.

http://www.idg.es/iworld/impart.asp?id=103068

ENIAC

Factoring & Gestión de Pagos.

http://www.eniac.com/productos/download/FACTORING.pdf

Universidad de Málaga

Servicios de notarización electrónica.

http://www.revistasic.com/revista45/pdf_45/SIC_45_agora.PDF

El Universo

Los trámites notariales se harán por vía electrónica en Internet.

http://www.eluniverso.com/2006/03/01/10/ceb25996b6b0469d9ebc10a4c056e702.html?EUID=

Votobit

El DNI electrónico y la firma-e.

http://www.votobit.org/articulos/dni.html

mi2g

Windows regains mantle of most vulnerable OS.

http://www.mi2g.co.uk/cgi/mi2g/press/140802.php

Linux

Certificate Management.

http://howtos.linux.com/howtos/SSL-Certificates-HOWTO/c118.shtml

SourceForge

Security project.

http://sourceforge.net/softwaremap/trove_list.php?form_cat=43

EJBCA

EJBCA - The J2EE Certificate Authority.

http://ejbca.sourceforge.net/

DEBIAN

Comunicado conjunto sobre la seguridad de GNU/Linux.

http://www.us.debian.org/News/2004/20040406.es.html

Macuarium

Mac OS X se defiende bien.

http://www.macuarium.com/macuarium/actual/noticias/2002_11_03_solidasanosx.shtml

MeetingHouse

Free Trial Download.

http://www.mtghouse.com

Gateway

Funk Software ODYSSEY.

http://accessories.gateway.com/AccessoryStore/Software_316896/AntiVirus+_A1_+Utilities_316962/Security_316968/12643804_ProdDetail

DIRECCIONES ELECTRÓNICAS PKI

Autoridad Certificadora Raíz de ICP-Brasil (Infraestructura de Clave Pública-Brasil).

http://www.iti.br/

Información PKI Brasil.

http://www.icpbrasil.gov.br/

Oficina Nacional de Gobierno Electrónico e Informática: Perú.
http://www.pcm.gob.pe/portal_ongei/ongei2.asp

Entidad encargada de la acreditación de ACs: Chile.
http://www.entidadacreditadora.cl/

Agenda de Conectividad: Colombia.
http://www.agenda.gov.co/

Cámara Nacional de Comercio y Servicios del Uruguay: Uruguay.
http://www.cncs.com.uy/

Gobierno en Línea: Venezuela.
http://www.gobiernoenlinea.ve/

Gobierno Bolivia.
http://www.bolivia.gov.bo/

Agencia para el Desarrollo de la Sociedad de la Información en Bolivia.
http://www.adsib.gob.bo/

Consejo de Comercio Exterior e Inversiones: Ecuador.
http://www.comexi.gov.ec/

CORPECE (Coorporación Ecuatoriana de Comercio Electrónico): Ecuador.
http://www.corpece.org.ec/

Federal PKI Policy Authority: Estados Unidos.
http://www.cio.gov/fpkipa/

The Nation's Professional Notary Organization: Estados Unidos.
http://www.nationalnotary.org/eNotarization/

Anexo 1

Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento

A.1. LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS Y SU REGLAMENTO

A.1.1. LEY DE COMERCIO ELECTRONICO, FIRMAS Y MENSAJES DE DATOS

Ley No. 67. R.O. Suplemento 557 de 17 de Abril del 2002.

El H. CONGRESO NACIONAL

Considerando:

Que el uso de sistemas de información y de redes electrónicas, incluida la Internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado;

Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos;

Que se debe generalizar la utilización de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura;

Que a través del servicio de redes electrónicas, incluida la Internet, se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una ley especializada sobre la materia;

Que es indispensable que el Estado Ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales; y,
En ejercicio de sus atribuciones, expide la siguiente:

LEY DE COMERCIO ELECTRONICO, FIRMAS ELECTRONICAS Y MENSAJES DE DATOS

TITULO PRELIMINAR

Art. 1.- Objeto de la ley.- Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

CAPITULO I
PRINCIPIOS GENERALES

Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento.

Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Art. 4.- Propiedad intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.

Art. 6.- Información escrita.- Cuando la ley requiera u obligue que la

información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que este contenga sea accesible para su posterior consulta.

Art. 7.- Información original.- Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

Se considera que un mensaje de datos permanece integro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación.

Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente.

Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

Art. 8.- Conservación de los mensajes de datos.- Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

a. Que la información que contenga sea accesible para su posterior consulta;
b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.
No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Art. 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en

contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguiente casos:

a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,
b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado.

Art. 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

a) Momento de emisión del mensaje de datos.- Cuando el mensaje de datos ingrese cuan sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto;
b) Momento de recepción del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,
c) Lugares de envío y recepción.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos.

Art. 12.- Duplicación del mensaje de datos.- Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

TITULO II

DE LAS FIRMAS ELECTRONICAS, CERTIFICADOS DE FIRMA ELECTRONICA, ENTIDADES DE CERTIFICACION DE INFORMACION, ORGANISMOS DE PROMOCION DE LOS SERVICIOS ELECTRONICOS, Y DE REGULACION Y CONTROL DE LAS ENTIDADES DE CERTIFICACION ACREDITADAS

CAPITULO I
DE LAS FIRMAS ELECTRONICAS

Art. 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba enjuicio.

Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular;

b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y,
e) Que la firma sea controlada por la persona a quien pertenece.

Art. 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas, en dicho mensaje de datos, de acuerdo a lo determinado en la ley.

Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;
b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
d) Verificar la exactitud de sus declaraciones;
e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;
f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
g) Las demás señaladas en la ley y sus reglamentos.

Art. 18.- Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Art. 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por:

a) Voluntad de su titular;
b) Fallecimiento o incapacidad de su titular;
c) Disolución o liquidación de la persona jurídica, titular de la firma; y,
d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

CAPITULO II
DE LOS CERTIFICADOS DE FIRMA ELECTRONICA

Art. 20.- Certificado de firma electrónica.- Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Art. 21.- Uso el certificado de firma electrónica.- El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta ley y su reglamento.

Art. 22. - Requisitos del certificado de firma electrónica.- El Certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:

a) Identificación de la entidad de certificación de información;
b) Domicilio legal de la entidad de certificación de información;

c) Los datos del titular del certificado que permitan su ubicación e identificación;
d) El método de verificación de la firma del titular del certificado;
e) Las fechas de emisión y expiración del certificado;
f) El número único de serie que identifica el certificado;
g) La firma electrónica de la entidad de certificación de información;
h) Las limitaciones o restricciones para los usos del certificado; y,
i) Los demás señalados en esta ley y los reglamentos.

Art. 23.- Duración del certificado de firma electrónica.- Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta ley.

Art. 24.- Extinción del certificado de firma electrónica.- Los certificados de firma electrónica, se extinguen, por las siguientes causas:

a) Solicitud de su titular;
b) Extinción de la firma electrónica, de conformidad con lo establecido en el artículo 19 de esta ley; y,
c) Expiración del plazo de validez del certificado de firma electrónica.

La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Art. 25.- Suspensión del certificado de firma electrónica.- La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:

a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley;
b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,
c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica.
La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

La entidad de certificación de información deberá levantar la suspensión temporal una vez desvanecidas las causas que la originaron, o cuando mediare resolución del Consejo Nacional de Telecomunicaciones, en cuyo caso, la entidad de certificación de información está en la obligación de habilitar de inmediato el certificado de firma electrónica.

Art. 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta ley, cuando:

a) La entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,
b) Se produzca la quiebra técnica de la entidad de certificación judicialmente declarada.

La revocatoria y sus causas deberán ser inmediatamente notificadas al titular del certificado.

Art. 27.- Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el

respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

La entidad de certificación de información será responsable por los perjuicios que ocasionare la falta de comunicación, de publicación o su retraso.

Art. 28.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el reglamento correspondiente para la aplicación de este artículo.

Las firmas electrónicas creadas en el extranjero, para el reconocimiento de su validez en el Ecuador se someterán a lo previsto en esta ley y su reglamento.

Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho.

Salvo aquellos casos en los que el Estado, en virtud de convenios o tratados internacionales haya pactado la utilización de medios convencionales, los tratados o convenios que sobre esta materia se suscriban, buscarán la armonización de normas respecto de la regulación de mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico, la protección a los usuarios de estos sistemas, y el reconocimiento de los certificados de firma electrónica entre los países suscriptores.

CAPITULO III
DE LAS ENTIDADES DE CERTIFICACION DE INFORMACION

Art. 29.- Entidades de certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

Art. 30.- Obligaciones de las entidades de certificación de información acreditadas.- Son obligaciones de las entidades de certificación de información acreditadas:

a) Encontrarse legalmente constituidas, y estar registradas en Consejo Nacional de Telecomunicaciones;
b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;
c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información,
d) Mantener sistemas de respaldo de la información relativa a los certificados;
e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en esta ley;
f) Mantener una publicación del estado de los certificados electrónicos emitidos;
g) Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;
h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las

operaciones que garanticen sus certificados; e,
i) Las demás establecidas en esta ley y los reglamentos.

Art. 31.- Responsabilidades de las entidades de certificación de información acreditadas.- Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.

Cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio.

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Art. 33.- Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

El Conejo Nacional de Telecomunicaciones, establecerá los términos bajo los cuales las Entidades de Certificación de Información podrán prestar sus servicios por medio de terceros.

Art. 34.- Terminación contractual.- La terminación del contrato entre las entidades de certificación acreditadas y el suscriptor se sujetará a las normas previstas en la Ley Orgánica de Defensa del Consumidor.

Art. 35.- Notificación de cesación de actividades.- Las entidades de certificación de información acreditadas, deberán notificar al Organismo de Control, por lo menos con noventa días de anticipación, la cesación de sus actividades y se sujetarán a las normas y procedimientos establecidos en los reglamentos que se dicten para el efecto.

CAPITULO IV

DE LOS ORGANISMOS DE PROMOCION Y DIFUSION DE LOS SERVICIOS ELECTRONICOS, Y DE REGULACION Y CONTROL DE LAS ENTIDADES DE CERTIFICACION ACREDITADAS

Art. 36.- Organismo de promoción y difusión.- Para efectos de esta ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior.

Art. 37.- Organismo de regulación, autorización y registro de las entidades de certificación acreditadas.- El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas. En su calidad de organismo de autorización podrá además:

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas, previo informe motivado de la Superintendencia de Telecomunicaciones;
b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; y
c) Las demás atribuidas en la ley y en los reglamentos.

Art. 38.- Organismo de control de las entidades de certificación de información acreditadas.- Para efectos de esta ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas.

Art. 39.- Funciones del organismo de control.- Para el ejercicio de las atribuciones establecidas en esta ley, la Superintendencia de Telecomunicaciones tendrá las siguientes funciones:

a) Velar por la observancia de las disposiciones constitucionales y legales sobre la promoción de la competencia y las prácticas comerciales restrictivas, competencia desleal y protección al consumidor, en los mercados atendidos por las entidades de certificación de información acreditadas;
b) Ejercer el control de las entidades de certificación de información acreditadas en el territorio nacional y velar por su eficiente funcionamiento;
c) Realizar auditorías técnicas a las entidades de certificación de información acreditadas;
d) Requerir de las entidades de certificación de información acreditadas, la información pertinente para el ejercicio de sus funciones;
e) Imponer de conformidad con la ley sanciones administrativas a las entidades de certificación de información acreditadas, en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio;
f) Emitir los informes motivados previstos en esta ley;
g) Disponer la suspensión de la prestación de servicios de certificación para impedir el cometimiento de una infracción; y,
h) Las demás atribuidas en la ley y en los reglamentos.

Art. 40.- Infracciones administrativas.- Para los efectos previstos en la presente ley, las infracciones administrativas se clasifican en leves y graves.

Infracciones leves:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por el organismo de control; y,
2. Cualquier otro incumplimiento de las obligaciones impuestas por esta ley y sus reglamentos a las entidades de certificación acreditadas.

Estas infracciones serán sancionadas, de acuerdo a los literales a) y b) del artículo siguiente.

Infracciones graves:

1. Uso indebido del certificado de firma electrónica por omisiones imputables a la entidad de certificación de información acreditada;
2. Omitir comunicar al organismo de control, de la existencia de actividades presuntamente ilícitas realizada por el destinatario del servicio;
3. Desacatar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción;
4. El incumplimiento de las resoluciones dictadas por los Organismos de Autorización Registro y Regulación, y de Control; y,
5. No permitir u obstruir la realización de auditorías técnicas por parte del organismo de control.

Estas infracciones se sancionarán de acuerdo a lo previsto en los literales c) y d) del artículo siguiente.

Las sanciones impuestas al infractor, por las infracciones graves y leves, no le eximen del cumplimiento de sus obligaciones.

Si los infractores fueren empleados de instituciones del sector público, las sanciones podrán extenderse a la suspensión, remoción o cancelación del cargo del infractor, en cuyo caso deberán observarse las normas previstas en la ley.

Para la cuantía de las multas, así como para la gradación de las demás sanciones, se tomará en cuenta:

a) La gravedad de las infracciones cometidas y su reincidencia;
b) El daño causado o el beneficio reportado al infractor; y,
c) La repercusión social de las infracciones.

Art. 41.- Sanciones.- La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

a) Amonestación escrita;
b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;
c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y,
d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica;

Art. 42.- Medidas cautelares, En los procedimientos instaurados por infracciones graves.- Se podrá solicitar a los órganos judiciales competentes, la adopción de las medidas cautelares previstas en la ley que se estimen necesarias, para asegurar la eficacia de la resolución que definitivamente se dicte.

Art. 43.- Procedimiento.- El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones.

TITULO III

DE LOS SERVICIOS ELECTRONICOS, LA CONTRATACION ELECTRONICA Y TELEMATICA, LOS DERECHOS DE LOS USUARIOS, E INSTRUMENTOS PUBLICOS

CAPITULO I
DE LOS SERVICIOS ELECTRONICOS

Art. 44.- Cumplimiento, de formalidades.- Cualquier actividad, transacción mercantil, financiera o de servicios, que se realice con mensajes de datos, a través de redes electrónicas, se someterá a los requisitos y solemnidades establecidos en la ley que las rija, en todo lo que fuere aplicable, y tendrá el mismo valor y los mismos efectos jurídicos que los señalados en dicha ley.

CAPITULO II
DE LA CONTRATACION ELECTRONICA Y TELEMATICA

Art. 45.- Validez de los contratos electrónicos.- Los contratos podrán ser instrumentados mediante mensajes de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos.

Art. 46.- Perfeccionamiento y aceptación de los contratos electrónicos.- El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.

La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

Art. 47.- Jurisdicción.- En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio el del consumidor o usuario.

Para la identificación de la procedencia de un mensaje de datos, se utilizarán los medios tecnológicos disponibles, y se aplicarán las disposiciones señaladas en esta ley y demás normas legales aplicables.

Cuando las partes pacten someter las controversias a un procedimiento arbitral en la formalización del convenio de arbitraje como en su aplicación, podrán emplearse medios telemáticos y electrónicos, siempre que ello no sea incompatible con las normas reguladoras del arbitraje.

CAPITULO III
DE LOS DERECHOS DE LOS USUARIOS O CONSUMIDORES DE SERVICIOS ELECTRONICOS

Art. 48.- Consentimiento para aceptar mensajes de datos.- Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

El usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

Art. 49.- Consentimiento para el uso de medios electrónicos.- De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:

a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,
b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:

1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;
2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;
3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,
4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

Art. 50.- Información al consumidor.- En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de

conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento.

Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.

La publicidad, promoción e información de servicios electrónicos, por redes electrónicas de información, incluida la Internet, se realizará de conformidad con la ley, y su incumplimiento será sancionado de acuerdo al ordenamiento jurídico vigente en el Ecuador.

En la publicidad y promoción por redes electrónicas de información, incluida la Internet, se asegurará que el consumidor pueda acceder a toda la información disponible sobre un bien o servicio sin restricciones, en las mismas condiciones y con las facilidades disponibles para la promoción del bien o Servicio de que se trate.

En el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la presente ley.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.

CAPITULO IV
DE LOS INSTRUMENTOS PUBLICOS

Art. 51.- Instrumentos públicos electrónicos.- Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente.

Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables.

TITULO IV
DE LA PRUEBA Y NOTIFICACIONES ELECTRONICAS

CAPITULO I
DE LA PRUEBA

Art. 52.- Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

Art. 53.- Presunción.- Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

Art. 54.- Práctica de la prueba.- La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;
b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados; y,
c) El facsímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

Art. 55.- Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Art. 56.- Notificaciones Electrónicas.- Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo electrónico, de un abogado legalmente inscrito, en cualquiera de los Colegios de Abogados del Ecuador.

Las notificaciones a los representantes de las personas jurídicas del sector público y a los funcionarios del Ministerio Público que deben intervenir en los juicios, se harán en las oficinas que estos tuvieren o en el domicilio judicial electrónico en un correo electrónico que señalaren para el efecto.

TITULO V
DE LAS INFRACCIONES INFORMATICAS

CAPITULO I
DE LAS INFRACCIONES INFORMATICAS

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:

"Art...- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y

multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art...- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Art. 59.- Sustitúyase el artículo 262 por el siguiente:

"Art...- 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo".

Art. 60.- A continuación del artículo 353, agréguese el siguiente artículo innumerado:

"Art....- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
4.- El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.".

Art. 61.- A continuación del artículo 415 del Código Penal, inclúyanse los siguientes artículos innumerados:

"Art...- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art...- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho

meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.".

Art. 62.- A continuación del artículo 553 del Código Penal, añádanse los siguientes artículos innumerados:

"Art...- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art...- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

"... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

DISPOSICIONES GENERALES

Primera.- Los certificados de firmas electrónicas, emitidos por entidades de certificación de información extranjeras y acreditados en el exterior, podrán ser revalidados en el Ecuador siempre que cumplan con los términos y condiciones exigidos por la ley. La revalidación se realizará a través de una entidad de certificación de información acreditada que garantice en la misma forma que lo hace con sus propios certificados, dicho cumplimiento.

Segunda.- Las entidades de certificación de información acreditadas podrán prestar servicios de sellado de tiempo. Este servicio deberá, ser acreditado técnicamente por el Consejo Nacional de Telecomunicaciones. El reglamento de aplicación de la ley recogerá los requisitos para este servicio.

Tercera.- Adhesión.- Ninguna persona está obligada a usar o aceptar mensajes de datos o firmas electrónicas, salvo que se adhiera voluntariamente en la forma prevista en esta ley.

Cuarta.- No se admitirá ninguna exclusión, restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en la presente ley y su reglamento.

Quinta.- Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor.

Sexta.- El Consejo Nacional de Telecomunicaciones tomará las medidas necesarias, para que no se afecten los derechos del titular del certificado o de terceros, cuando se produzca la revocatoria del certificado, por causa no atribuible al titular del mismo.

Séptima.- La prestación de servicios de certificación de información por parte de entidades de certificación de información acreditadas, requerirá de autorización previa y registro.

Octava.- El ejercicio de actividades establecidas en esta ley, por parte de instituciones públicas o privadas, no requerirá de nuevos requisitos o requisitos adicionales a los ya establecidos, para garantizar la eficiencia técnica y seguridad jurídica de los procedimientos e instrumentos empleados.

Novena.- Glosario de términos.- Para efectos de esta ley, los siguientes términos serán entendidos conforme se definen en este artículo:

Mensaje de datos: Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos.

Red electrónica de información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.
Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Servicio electrónico: Es toda actividad realizada a través de redes electrónicas de información.

Comercio electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley.

Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Certificado electrónico de información: Es el mensaje de datos que contiene información de cualquier tipo.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

Dispositivo de emisión: Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.
Emisor: Persona que origina un mensaje de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos.

Signatario: Es la persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Quiebra técnica: Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta ley y su reglamento.

Factura electrónica: Conjunto de registros lógicos archivados en soportes susceptibles de ser leídos por equipos electrónicos de procesamiento de datos que documentan la transferencia de bienes y servicios, cumpliendo los requisitos exigidos por las Leyes Tributarias, Mercantiles y más normas y reglamentos vigentes.

Sellado de tiempo: Anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación.

Décima.- Para la fijación de la pena en los delitos tipificados mediante las presentes, reformas al Código Penal, contenidas en el Título V de esta ley, se tomarán en cuenta los siguientes criterios: el importe de lo defraudado, el quebranto económico causado, los medios empleados y cuantas otras circunstancias existan para valorar la infracción.

DISPOSICIONES TRANSITORIAS

Primera.- Hasta que se dicte el reglamento y más instrumentos de aplicación de esta ley, la prestación del servicio de sellado de tiempo, deberá cumplir con los requisitos de seguridad e inalterabilidad exigidos para la firma electrónica y los certificados electrónicos.

Segunda.- El cumplimiento del artículo 56 sobre las notificaciones al correo electrónico se hará cuando la infraestructura de la Función Judicial lo permita, correspondiendo al organismo competente de dicha Función organizar y reglamentar los cambios que sean necesarios para la aplicación de esta ley y sus normas conexas.

Para los casos sometidos a Mediación o Arbitraje por medios electrónicos, las notificaciones se efectuarán obligatoriamente en el domicilio judicial electrónico en un correo electrónico señalado por las partes.

DISPOSICION FINAL

El Presidente de la República, en el plazo previsto en la Constitución Política de la República, dictará el reglamento a la presente ley.

La presente ley entrará en vigencia a partir de su publicación en el Registro Oficial.

A.1.2. REGLAMENTO GENERAL A LA LAY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

No. 3496

Gustavo Noboa Bejarano
PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Considerando:

Que mediante Ley No. 67, publicada en el Registro Oficial Suplemento No. 557 de 17 de Abril del 2002 se expidió la Ley de Comercio Electrónico, Firmas y Mensajes de Datos;

Que la disposición final de la citada ley dispone que el Presidente de la Republica debe expedir el correspondiente reglamento; y,

En ejercicio de la facultad prevista en el artículo 171 numeral 5 de la Constitución Política de la República,

Decreta:

Expedir el siguiente:

REGLAMENTO GENERAL A LA LAY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

Art. 1.- Incorporación de archivos o mensajes adjuntos.- La incorporación por remisión a la que se refiere el artículo 3 de la Ley 67, incluye archivos y mensajes incorporados por remisión o como anexo en un mensaje de datos a cuyo contenido se accede indirectamente a partir de un enlace electrónico directo incluido en el mismo mensaje de datos y que forma parte del mismo.

La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación. En el caso de contenido incorporado por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación e expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos.
En las relaciones con consumidores, es responsabilidad del proveedor asegurar la disponibilidad de los remitidos o anexos para que sean accedidos por un medio aceptable para el consumidor cuando éste lo requiera. En las relaciones de otro tipo las partes podrán acordar la forma y accesibilidad de los anexos y remitidos.

Los anexos o remisiones referidas a garantías, derechos, obligaciones o información al consumidor deberán observar lo establecido en la Ley Orgánica de Defensa del Consumidor y su reglamento.

Toda modificación a un anexo o remitido en un mensaje de datos se comunicará al receptor del mismo, a través de un mensaje de datos o por escrito, resaltando las diferencias entre el texto original y el modificado. En el texto modificado se deberá incluir en lugar visible y claramente accesible un enlace al contenido anterior. La comunicación al consumidor acerca de modificaciones no constituye indicación de aceptación de las mismas por su parte. Dicha aceptación deberá ser expresa y remitida por cualquier medio, ya sea éste físico o electrónico.

Cuando las leyes así lo determinen, cierto tipo de información deberá estar directamente incluida en el mensaje de datos y no como anexo o remitido.

Art. 2.- Accesibilidad de la información.- Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Art. 3.- Información escrita.- Se entiende que la información contenida

en un mensaje de datos es accesible para su posterior consulta cuando:

a) Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,

b) Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente el mensaje de los datos a fin de garantizar el posterior acceso al mismo.

Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensaje de datos.

Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito.

Art. 4.- Información original y copias certificadas.- Los mensajes de datos de los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.

Los documentos desmaterializados se considerarán para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Art. 5.- Desmaterialización.- El acuerdo expreso para desmaterializar documentos deberá constar en un documento físico o electrónico con las firmas de las partes aceptando tal desmaterialización y confirmado que el documento original y que el documento desmaterializado son idénticos. En caso que las partes lo acuerden o la ley lo exija, las partes acudirán ante Notario o autoridad competente para que certifique electrónicamente que el documento desmaterializado corresponde al documento original que se acuerda desmaterializar. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica del Notario o autoridad competente.

Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la única diferencia que el documento desmaterializado tendrá con el documento original.

En el caso de documentos que contengan obligaciones, se entiende que tanto el documento original cono el desmaterializado son la expresión de un mismo acuerdo de las partes intervinientes y por tanto no existe duplicación de obligaciones. De existir multiplicidad de documentos desmaterializados y originales con la misma información u obligación, se entenderá que se trata del mismo, salvo prueba en contrario.

La desmaterialización de los documentos de identificación personal estará sujeta a las disposiciones especiales y procedimiento que las entidades competentes determinen.

Art. 6.- Integridad de un mensaje de datos.- La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no

constituye parte sustancial de la información.

Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

Art. 7.- Procedencia e identidad de un mensaje de datos.- La verificación de la concordancia entre el emisor del mensaje de datos y su firma electrónica se realizará comprobando la vigencia y los datos del certificado de firma electrónica que la respalda. En otros tipos de firmas o sistemas de identificación y autentificación, esta verificación se realizará mediante la verificación de los registros acordados o requeridos.

El aviso de un posible riesgo sobre la vulnerabilidad o inseguridad de una firma, su certificado o el mensaje de datos y los anexos relacionados podrá ser realizado por el titular de los mismos, mediante cualquier tipo de advertencia que permita, de manera inequívoca a quien realiza la verificación o recibe un mensaje de datos, tomar las precauciones necesarias para evitar perjuicios y prevenir fallas de seguridad. Este aviso deberá ser realizado antes de iniciar cualquier proceso de transacción comercial negociación o contratación electrónica

De acuerdo a las leyes, se podrá recurrir a peritos para determinar la procedencia y otro tipo de relaciones de un mensaje de datos con quien lo remite de modo directo o indirecto.

Art. 8.- Responsabilidad por el contenido de los mensajes de datos.- La prestación de servicios electrónicos de cualquier tipo por parte de terceros, relacionados con envío y recepción de comunicaciones electrónicas, alojamiento de sitios en medios electrónicos o servicios similares o relacionados, no implica responsabilidad sobre el contenido de los mensajes de datos por parte de quien presta estos servicios, siendo la responsabilidad exclusivamente del propietario de la información.
De acuerdo a la ley y por orden de la autoridad competente, el órgano regulador podrá ordenar la suspensión del acceso a cualquier información en redes electrónicas que se declare ilegal y/o que atente contra las leyes o la seguridad nacionales. El proveedor de servicios electrónicos deberá cumplir con la orden de suspender el acceso al contenido en forma inmediata, y en caso de no hacerlo será sancionado con sujeción a la ley por el CONELEC.

Art. 9.- Prestación de servicios de conservación de mensajes de datos.- La conservación, incluido el almacenamiento y custodia de mensajes de datos, podrá realizarse a través de terceros, de acuerdo a lo que establece el Art. 8 de la Ley 67. los sistemas, políticas y procedimientos que permiten realizar las funciones de conservación de mensajes de datos se denominan Registro Electrónico de Datos. Una vez cumplidos los requisitos establecidos en las leyes, cualquier persona puede prestar servicios de Registro Electrónico de Datos que incluyen:

a) Conservación, almacenamiento y custodia de la información en formato electrónico con las debidas seguridades;
b) Preservación de la integridad de la información conservada;
c) Administración del acceso a la información y la reproducción de la misma cuando se requiera;
d) Respaldo y recuperación de información; y,
e) Otros servicios relacionados con la conservación de los mensajes de datos.

La prestación de servicios de Registro de Dato se realizará bajo el régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios, podrán determinar las condiciones que regulan su relación.

La prestación del servicio de Registro Electrónico de Datos deberá observar todas las normas contempladas en la

Ley 67, este reglamento y demás disposiciones legales vigentes.
En los procesos de conservación de los mensajes de datos, se debe garantizar la integridad de los mismos al menos por el mismo tiempo que las leyes y reglamentos exijan su almacenamiento.

Por orden de autoridad competente, podrá ordenarse a los proveedores de servicios de Registro Electrónico de Datos mantener en sus sistemas respaldos de los mensajes de datos que tramite por el tiempo que se considere necesario.

Art. 10.- Elementos de la infraestructura de firma electrónica.- La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no registren la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento.

Los principios y elementos que respaldan a la firma electrónica son:

a) No-discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada;
b) Practicas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente;
c) El soporte lógico o conjunto de instrucciones para los equipos de computo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b);
d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios; y,
e) Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.

Art. 11.- Duración del certificado de firma electrónica.- La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firmas electrónicas se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes.

Art. 12.- Listas de revocación.- Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al artículo 26 de la Ley 67. Cuando la verificación de la validez de los certificados de firma electrónica no sea posible de realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos.

Los periodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente.

Art. 13.- Revocación del certificado de firma electrónica.- Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades.

La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado.

La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la ley 67 y este reglamento.

Art. 14.- De la notificación por extinción, suspensión o revocación del certificado de firma electrónica.- La notificación inmediata al titular del certificado de firma electrónica, de acuerdo al articulo 26 de la Ley 67, se hará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio, luego de la extinción, suspensión o revocación del certificado.

Art. 15.- Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.- La publicación a la que se refiere el artículos 27 de la Ley 67, se deberá hacer por cualquiera de los siguientes medios:

a) Siempre a la página electrónica determinada por el CONELEC en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y,
b) Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un Directorio electrónico o por cualquier procedimiento por el cual se consulta los datos del certificado de firma electrónica.

Opcionalmente en caso de que la entidad certificadora o la entidad de registro relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública.

Art. 16.- Reconocimiento internacional de certificados de firma electrónica.- Los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en Ecuador, una vez obtenida la revalidación respectiva emitida por el CONELEC, el deberá comprobar el grado de fiabilidad de los certificados y la solvencia técnica de quien los emite.

Art. 17.- Régimen de acreditación de entidades de certificación de información.- Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONELEC.

Los certificados de firma electrónica emitidos por las entidades de certificación de información que, además de registrarse, se acrediten voluntariamente en el CONELEC, tienen carácter probatorio.

Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acreditan en el CONELEC, tendrán la calidad de entidades de certificación de información no acreditadas y están obligados a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten.

Art. 18.- Responsabilidades de las entidades de certificación de información.- Es responsabilidad de la entidad certificadora de información o de la entidad de Registro que actúe en su nombre, verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica.

El CONATEL, podrá requerir en cualquier momento de la entidad de

certificación de información, de la entidad de Registro que actúe en su nombre, o del titular del certificado de firma electrónica los documentos de respaldo que confirmen la autenticidad y exactitud de los datos que contiene.

Art. 19.- Obligaciones del titular de firma electrónica.- A más de las consideradas en la Ley 67 y su reglamento, serán las mismas previstas en las leyes por el empleo de la firma manuscrita.

El órgano que ejerce las funciones de control previsto en la Ley 67, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control.

Art. 20.- Información al usuario.- La información sobre los programas o equipos que se requiere para acceder a registros o mensajes de datos deberá ser proporcionada mediante medios electrónicos o materiales. En el caso de uso de medios electrónicos se contará con la confirmación de recepción de la información por parte del usuario, cuando se usen medios materiales, los que formarán parte de la documentación que se le deberá entregar al usuario.

Para demostrar el acceso a la información el usuario deberá manifestar expresamente que conoce la información objeto de su consentimiento y que sus sistemas le permiten el acceso tecnológico a la misma.

Art. 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo al acceso a los sistemas o a la información de instruir claramente sobre los posibles riesgos en que pueden incurrir por la falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidos en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

Art. 22.- Envió de mensajes de datos no solicitados.- El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

a) Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y de suscripción;
b) Se deberá incluir una nota indicando el derecho del receptor a solicitar se le deje de enviar información no solicitada;
c) Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos;
d) A solicitud del destinatario se deberá eliminar toda información que de él se tenga en bases de

datos o en cualquier otra fuente de información empleada para el envió de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos; y,

e) Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente.

Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino.

Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envió periódico de mensajes de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada.

Art. 23.- Sellado de tiempo.- Para la prestación de los servicios de sellado de tiempo, el mensaje de datos debe ser enviado a través de la entidad certificadora o un tercero debidamente registrado en el CONELEC para prestar este servicio.

El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por el CONELEC; y la fecha y hora exacta en dicho mensaje de datos fue entregado al destinatario.

Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano.

La prestación de servicios de sellado de tiempo se realizará en régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios podrán determinar las condiciones que regulen su relación.

Articulo Final.- El presente reglamento entrará en vigencia a partir de su publicación en el Registro oficial.

Dado en el Palacio Nacional, en Quito, a 12 de Diciembre del 2002.

f.) Gustavo Noboa Bejarano, Presidente Constitucional de la República.

Es fiel copia del original.- Lo certifico.

f.) Marcelo Santos Vera, Secretario General de la Administración Pública.

Anexo 2

Formato de Entrevista y Entrevista Aplicada al Administrador de la PKI del Banco Central del Ecuador

A.2. FORMATO DE ENTREVISTA Y ENTREVISTA APLICADA AL ADMINISTRADOR DE LA PKI DEL BANCO CENTRAL DEL ECUADOR

A.2.1. FORMATO DE ENTREVISTA APLICADA AL ADMINISTRADOR DE LA PKI DEL BANCO CENTRAL DEL ECUADOR

OBJETIVO DE LA ENTREVISTA

Recolectar información del funcionamiento de la PKI del Banco Central, los servicios que brinda, su inserción en el mercado; para evaluar el progreso alcanzado.

Objetivos específicos

- Determinar el alcance y limitaciones de la PKI del Banco Central del Ecuador.
- Determinar la arquitectura y plataforma utilizadas por la PKI del Banco Central del Ecuador.
- Identificar el nivel de seguridad de los procedimientos empleados dentro de la PKI del Banco Central del Ecuador.
- Establecer la existencia de políticas de certificación de la PKI del Banco Central del Ecuador.
- Determinar que tipo soporte técnico se brinda a los clientes por parte de la PKI del Banco Central del Ecuador.

CÁLCULOS DE LA MUESTRA

La entrevista se realiza el 18 de Noviembre de 2005 al Ing. Marcelo Balarezo, Administrador de la PKI del Banco Central, por tratarse de una entrevista no se necesita realizar un cálculo de muestra.

FORMATO DE ENTREVISTA APLICADA AL ADMINISTRADOR DE LA PKI DEL BANCO CENTRAL DEL ECUADOR.

Esta entrevista ha sido realizada con fines investigativos, por parte de la Srta. Shirma Ortiz Boada, estudiante de la Carrera de Ingeniería Electrónica y Redes de Información de la Escuela Politécnica Nacional.

I ALCANCE Y LIMITACIONES:

1 ¿Qué productos de seguridad utiliza el BCE para el funcionamiento de su PKI?

---

2 ¿Qué tipo de certificados puede expedir la PKI del BCE?

- ☐ Certificados Auto-firmados.
- ☐ Certificados para Autoridad Certificadora
- ☐ Certificados para Entidad Destino

3 ¿A qué sector está destinado el servicio de la PKI del BCE?

---

4 ¿Cuál es el número máximo de certificados digitales que puede expedir la PKI del BCE? ¿En qué período?

---

5 ¿Cuántos certificados digitales ha expedido la PKI del BCE para el Sistema Nacional de Pagos desde el inicio de su funcionamiento?

De estos certificados cuantos han sido destinados a:

Sistema de Pagos Interbancario (SPI)_____
Sistema de Pagos en Línea (SPL) _____
Sistema de Cobros Interbancario _____
Otro (especifique)_____

6 ¿Cuál es el período de validez del certificado de la Autoridad Certificadora de la PKI del BCE?

II ARQUITECTURA Y PLATAFORMA

1 La arquitectura que se tiene en la PKI del BCE es:

---

2 ¿Qué plataforma se utiliza para la infraestructura?

III NIVEL DE SEGURIDAD

General

1 ¿El PKI del BCE tiene definida una Declaración de Prácticas de Certificación?

☐ Si ☐ No

Operación de la Autoridad Certificadora

1 ¿Dónde se encuentran los servidores PKI?

---

2 En una escala de 1 a 10, siendo 10 el mayor nivel protección de los servidores utilizados para la operación de PKI y 1 el menor. ¿Qué puntuación daría usted al PKI del BCE?

1	2	3	4	5	6	7	8	9	10

3 ¿Quiénes tienen acceso a los servidores?

---

4 ¿Qué tipo de control de autenticación se tiene para el acceso a los servidores? (señale los que aplican)

---

5 ¿Se realizan copias de seguridad para recuperación de los servidores?

☐ Si ☐ No

Si la respuesta es Si, ¿cada cuánto se realizan los respaldos?

---

6 ¿Existen sistemas redundantes dentro de la infraestructura?

---

7 ¿La información almacenada en los servidores está cifrada?

☐ Si ☐ No

Si la respuesta es Si, ¿qué tipo de cifrado?

Manejo de los Certificados Digitales

1 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para el establecimiento de identidades utilizado por la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

2 ¿Quién realiza la confirmación de las identidades de los usuarios?

---

3 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado por la PKI del BCE para la entrega del Número de referencia y el Código de Autorización utilizado?

1	2	3	4	5	6	7	8	9	10

4 ¿Cuál es el período de duración del Número de referencia y el Código de Autorización?

---

5 El código de Autorización se emite para el procedimiento de generación de:

- ☐ Cada certificado personal
- ☐ Todos los certificados de una Institución

6 ¿Cuál es la longitud de las claves pública/privada?

_____

7 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted las reglas determinadas por la PKI del BCE para la elección del *password* para la utilización de los certificados personales?

1	2	3	4	5	6	7	8	9	10

9 ¿Se dan recomendaciones para el manejo del *password* y certificado a los usuarios finales?

☐ Si ☐ No

8 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la recuperación del certificado utilizado por la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

7 ¿Cuál es el período de validez de los certificados personales emitidos?

_____

8 ¿Cuál es el período de actualización de las Listas de Certificados Revocados?

_____

I V SOPORTE TÉCNICO

1 La información disponible sobre el funcionamiento de la PKI del BCE es:

- ☐ Pública
- ☐ Acceso restringido
- ☐ Solo para usuarios de Certificados

2 ¿Cuál es la disponibilidad del soporte técnico?

- ☐ Horario de oficina
- ☐ 24 horas
- ☐ Otro (especifique)_____

3 La asistencia se realiza:

- ☐ Telefónicamente
- ☐ Personalmente
- ☐ Por medio de correo electrónico
- ☐ Otro (especifique)_____

¡Gracias por su colaboración!

A.2.2. ENTREVISTA APLICADA AL ADMINISTRADOR DE LA PKI DEL BANCO CENTRAL DEL ECUADOR

Esta entrevista ha sido realizada con fines investigativos, por parte de la Srta. Shirma Ortiz Boada, estudiante de la Carrera de Ingeniería Electrónica y Redes de Información de la Escuela Politécnica Nacional.

I ALCANCE Y LIMITACIONES:

1 ¿Qué productos de seguridad utiliza el BCE para el funcionamiento de su PKI?

El PKI del Banco Central del Ecuador utiliza los siguientes productos:

Sofware* PKI / *Entrust	
Cantidad	**Descripción**
1	*Infrastructure Entrust Authority Security Manager* (AC)
1	*TruePass Server* (Autenticación robusta)
1	*Roaming Server* (Movilidad para el acceso de certificados)
1	*Self Administration Server* (Emisión de certificados vía Web)
1	*GetAccess Server* (Control de Acceso)
250	*Entrust TruePass ID's Funtions* (Licencias de Certificados Digitales)

Tabla A2.1 Productos de seguridad utilizados por la PKI del BCE

2 ¿Qué tipo de certificados puede expedir la PKI del BCE?

- ☐ Certificados Auto-firmados.
- ☐ Certificados para Entidad Destino

3 ¿A qué sector está destinado el servicio de la PKI del BCE?

Exclusivamente a las instituciones del Sistema Financiero Nacional como bancos, tarjetas de crédito y mutualistas.

4 ¿Cuál es el número máximo de certificados digitales que puede expedir la PKI del BCE? ¿En qué período?

Actualmente puede expedir hasta un máximo de 250 certificados en un período máximo de 20 años contados desde el año 2004.

5 ¿Cuántos certificados digitales ha expedido la PKI del BCE para el Sistema Nacional de Pagos desde el inicio de su funcionamiento?

180 certificados (5 de para pruebas, 175 para usuarios)

De estos certificados cuantos han sido destinados a:

Sistema de Pagos Interbancario (SPI)	**80 %**
Sistema de Pagos en Línea (SPL)	**15%**
Sistema de Cobros Interbancario	**5%**

6 ¿Cuál es el período de validez del certificado de la Autoridad Certificadora de la PKI del BCE?

20 años

II ARQUITECTURA Y PLATAFORMA

1 La arquitectura que se tiene en la PKI del BCE es:

El Banco Central del Ecuador actúa como Autoridad Certificadora raíz pero no puede jerarquizar su servicio por no existir la necesidad ni el licenciamiento correspondiente.

2 ¿Qué plataforma se utiliza para la infraestructura?

Solaris y Windows

III NIVEL DE SEGURIDAD

Operación de la Autoridad Certificadora

1 ¿Dónde se encuentran los servidores PKI?

En el centro de Computo dentro de una zona protegida por un *Firewall.*

2 En una escala de 1 a 10, siendo 10 el mayor nivel protección de los servidores utilizados para la operación de PKI y 1 el menor. ¿Qué puntuación daría usted al PKI del BCE?

1	2	3	4	5	6	7	8	9	10

3 ¿Quiénes tienen acceso a los servidores?

Solo personal de seguridad informática.

4 ¿Qué tipo de control de autenticación se tiene para el acceso a los servidores? (señale los que aplican)

Híbrido la puerta principal se accede con *password* y lectura de la huella dactilar.

5 ¿Se realizan copias de seguridad para recuperación de los servidores?

Si

Si la respuesta es Si, ¿cada cuánto se realizan los respaldos?

Una vez al mes, incrementales y se guarda una copia total una vez por año.

6 ¿Existen sistemas redundantes dentro de la infraestructura?

No, pero es imprescindible el contar con este tipo de esquemas de Alta Disponibilidad en sistemas críticos de seguridad.

7 ¿La información almacenada en los servidores está cifrada?

Si

Si la respuesta es Si, ¿qué tipo de cifrado?

Cifrado Asimétrico RSA

Manejo de los Certificados Digitales

1 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para el establecimiento de identidades utilizado por la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

2 ¿Quién realiza la confirmación de las identidades de los usuarios?

A través de un procedimiento de verificación el Administrador de la PKI del Banco Central del Ecuador realiza la confirmación, básicamente se utiliza un formulario de inscripción del usuario y se le llama telefónicamente preguntando nombres completos, dirección de correo, teléfono celular y lugares donde estudió la primaria y secundaria de acuerdo a lo registrado en el formulario.

3 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado por la PKI del BCE para la entrega del Número de referencia y el Código de Autorización utilizado?

1	2	3	4	5	6	7	8	9	10

4 ¿Cuál es el período de duración del Número de referencia y el Código de Autorización?

- Si no se ha utilizado, caduca automáticamente en 21 días.
- Inmediata luego del ingreso de los códigos para la creación o recuperación del certificado.

5 El código de Autorización se emite para el procedimiento de generación de:

Cada certificado personal

6 ¿Cuál es la longitud de las claves pública/privada?

RSA 1024 bits

7 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted las reglas determinadas por la PKI del BCE para la elección del *password* para la utilización de los certificados personales?

1	2	3	4	5	6	7	8	9	10

Se cumplen reglas estrictas para la definición de un *password* robusto.

8 ¿Se dan recomendaciones para el manejo del *password* y certificado a los usuarios finales?

Si

9 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la recuperación del certificado utilizado por la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

Para la recuperación del certificado se siguen procedimientos de seguridad como la verificación del usuario quien solicita la recuperación del certificado y la entrega de nuevos códigos de autorización, le pongo un 8 porque hay procedimientos más estrictos que entrarían en la categoría de clase mundial.

10 ¿Cuál es el período de validez de los certificados personales emitidos?

2 años de acuerdo a la Ley de Comercio Electrónico

11 ¿Cuál es el período de actualización de las Listas de Certificados Revocados?

La actualización de los certificados revocados es casi inmediata se demora 15 minutos en actualizar las CRL'S.

IV SOPORTE TÉCNICO

1 La información disponible sobre el funcionamiento de la PKI del BCE es:

Acceso restringido

2 ¿Cuál es la disponibilidad del soporte técnico?

Horario de oficina

3 La asistencia se realiza:

- ☐ Telefónicamente
- ☐ Personalmente
- ☐ Por medio de correo electrónico

¡Gracias por su colaboración!

Anexo 3

Formato, Tabulación y Resultados de Encuesta
Aplicada a los Responsables de los Certificados de cada
Institución que forma parte del SNP

A.3. FORMATO, TABULACIÓN Y RESULTADOS DE ENCUESTA APLICADA A LOS RESPONSABLES DE LOS CERTIFICADOS DE CADA INSTITUCIÓN QUE FORMA PARTE DEL SNP

A.3.1. FORMATO DE ENCUESTA APLICADA A LOS RESPONSABLES DE LOS CERTIFICADOS DE CADA INSTITUCIÓN QUE FORMA PARTE DEL SNP

OBJETIVO DE LA ENCUESTA

Recolectar información del desempeño de los Responsables de los Certificados de cada institución que forma parte del SNP (Sistema Nacional de Pagos).

Objetivos específicos

- Determinar el nivel de seguridad que se tiene en el manejo de códigos de autorización.
- Determinar el nivel de seguridad que se tiene en el manejo de certificados digitales.
- Identificar el nivel de cumplimiento de los procedimientos recomendados por los Administradores de la PKI del Banco Central del Ecuador.
- Determinar la calidad del soporte técnico que reciben los Responsables de los Certificados por parte de la PKI del Banco Central del Ecuador.

CÁLCULOS DE LA MUESTRA

La encuesta se realiza utilizando como método de muestreo el censo: es decir, se va ha encuestado a todos los responsables de certificados digitales (24) de las instituciones participantes dentro de la PKI del Banco Central del Ecuador. Las encuestas se realizaron[1] telefónicamente entre el 30 de Enero de 2006 y el 3 de Marzo de 2006.

---

[1] La realización de las encuestas fue aprobada por el Director de Informática del Banco Central Del Ecuador el 30 de Noviembre de 2005; los responsables de los certificados digitales de cada institución fueron informados de la realización del estudio de mercado el 23 de Enero del 2006.

FORMATO DE ENCUESTA APLICADA A LOS RESPONSABLES DE LOS CERTIFICADOS DE CADA INSTITUCIÓN QUE FORMA PARTE DEL SNP

Esta encuesta ha sido realizada con fines investigativos, por parte de la Srta. Shirma Ortiz Boada, estudiante de la Carrera de Ingeniería Electrónica y Redes de Información de la Escuela Politécnica Nacional.

GENERAL

1 Que aplicación o aplicaciones utiliza su institución en el Sistema Nacional de Pagos: (seleccione las que aplican)

- ☐ Sistema de Pagos Interbancario (SPI)
- ☐ Sistema de Pagos en Línea (SPL)
- ☐ Sistema de Cobros Interbancario
- ☐ Otro (especifique)_____

2 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la solicitud de certificados digitales utilizado por la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

3 En una escala de 1 a 10, siendo 10 el mayor nivel de confiabilidad y 1 el menor. ¿Qué puntuación daría usted al nivel de confianza de la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

I MANEJO DE CÓDIGOS DE AUTORIZACIÓN:

1 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la entrega de los Códigos de Autorización utilizado por la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

2 ¿Sabe Ud. cuál es el período de duración del Código de Autorización?

☐ 5 días ☐ 21 días ☐ Otro (especifique)_____

3 Los códigos de autorización se han guardado en: (seleccione las que aplican).

- ☐ Correo electrónico
- ☐ Escrito en un Papel
- ☐ En un documento en la computadora
- ☐ Otro (especifique)_____

4 ¿Ha revelado los códigos de autorización a otra persona?

☐ Si ☐ No

¿Por qué?_____

II MANEJO DE CERTIFICADOS DIGITALES:

1 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la generación de los certificados digitales utilizado por la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

2 ¿Sabe Ud. cuál es el período de duración de un Certificado Digital?

☐ 1 año ☐ 2 años ☐ Otro (especifique)_____

3 Dentro de su institución, los certificados digitales se almacenan en: (seleccione las que aplican).

☐ Disquete/CD/Otro dispositivo extraíble
☐ Disco duro
☐ Otro (especifique)_____

4 ¿Se permite que diferentes usuarios tengan acceso a los certificados digitales?

☐ Si ☐ No

5 ¿Cuántos certificados ha expedido la PKI del BCE para su institución?

III CUMPLIMIENTO DE POLÍTICAS

1 ¿Se han dado recomendaciones sobre el manejo de: códigos de autorización y certificados digitales por parte de los Administradores de la PKI del BCE?

☐ Si ☐ No

Si la respuesta es Si:

¿Se dio una explicación del por qué de estas recomendaciones?

☐ Si ☐ No ☐ Parcialmente

¿Se han cumplido estas recomendaciones?

☐ Si ☐ No ☐ Parcialmente

2 ¿Se han establecido normas y políticas de seguridad para el manejo de los *códigos de autorización* y certificados digitales por parte de su institución?

☐ Si ☐ No

Si la respuesta es Si:

¿Se dio una explicación del por qué de estas normas y políticas a los usuarios?

☐ Si ☐ No ☐ Parcialmente

¿Se han cumplido estas normas y políticas?

☐ Si ☐ No ☐ Parcialmente

3 ¿En cuáles de las siguientes situaciones reportaría un suceso al Administrador de la PKI del BCE? (seleccione las que aplican).

☐ El usuario sale de vacaciones
☐ El usuario sufre un accidente
☐ El usuario deja de trabajar en la Institución
☐ El *password* se ve comprometido
☐ El certificado se ve comprometido
☐ Otro (especifique)_____

I V SOPORTE TÉCNICO

1 ¿Ha utilizado el soporte técnico brindado por la PKI del BCE?

☐ Si ☐ No

Si la respuesta es si:

La información disponible sobre el funcionamiento de la PKI del BCE es:

☐ Pública
☐ Acceso restringido
☐ Solo para usuarios de Certificados

¿Cuál es la disponibilidad del Soporte Técnico?:

☐ Horario de oficina
☐ 24 horas
☐ Otro (especifique)_____

La asistencia se realiza:

☐ Telefónicamente
☐ Personalmente
☐ Por medio de correo electrónico
☐ Otro (especifique)_____

2 En una escala de 1 a 10, siendo 10 el mayor nivel de calidad del soporte técnico y 1 el menor. ¿Qué puntuación daría usted al soporte técnico brindado por los administradores de la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

¡Gracias por su colaboración!

A.3.2. TABULACIÓN DE LAS ENCUESTAS APLICADAS A LOS 24 RESPONSABLES DE LOS CERTIFICADOS DE CADA INSTITUCIÓN QUE FORMA PARTE DEL SNP

SECCIÓN GENERAL

Nº	1 Que aplicación o aplicaciones utiliza su institución en el Sistema Nacional de Pagos: (seleccione las que aplican)			
	SPI	SPL	SCI	Otro
1	1		1	
2	1	1		
3	1			
4	1			
5	1			
6	1		1	
7	1			
8	1		1	
9	1			
10	1			
11	1			
12		1		
13	1			
14	1			
15	1	1		
16	1			
17	1			
18	1			
19		1		
20	1			
21	1			
22	1			
23	1			SPN
24	1	1		
T	22	5	3	1
%	91,67	20,83	12,5	4,17

1- Otro		
Respuesta	#	%
SPN	1	4,17
Total:	1	4,17

Nº	2 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la solicitud de certificados digitales utilizado por el PKI del BCE?									
	1	2	3	4	5	6	7	8	9	10
1										1
2								1		
3										
4										1
5								1		
6										1
7									1	
8		1								
9										1
10									1	
11										1
12									1	
13									1	
14										1
15									1	
16								1		
17									1	
18								1		
19								1		
20										1
21									1	
22									1	
23								1		
24					1					
T	0	1	0	0	1	0	0	6	8	7
%	0	4,17	0	0	4,17	0	0	25	33,33	29,17

Menor:	2
Mayor:	10
Moda:	9
Promedi	8,57

Nº	3 En una escala de 1 a 10, siendo 10 el mayor nivel de confiabilidad y 1 el menor. ¿Qué puntuación daría usted al nivel de confianza del PKI del BCE?									
	1	2	3	4	5	6	7	8	9	10
1										1
2									1	
3									1	
4										1
5								1		
6										1
7									1	
8		1								
9										1
10									1	
11										1
12									1	
13										1
14										1
15										1
16								1		
17										1
18								1		
19										1
20										1
21									1	
22									1	
23									1	
24										1
T	0	1	0	0	0	0	0	3	8	12
%	0	4,17	0	0	0	0	0	12,5	33,33	50

Menor:	2
Mayor:	10
Moda:	10
Promedio	9,08

Sigla	Significado
SCI	Sistema Cobros Interbancario
SPI	Sistema de Pagos Interbancario
SPL	Sistema de Pagos en Línea
SPN	Sistema de Pagos por valores Netos
☐	El encuestado no contestó la pregunta.

Tabla A3.1 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección General

SECCIÓN MANEJO DE CÓDIGOS DE AUTORIZACIÓN

Nº	1 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la entrega de los Códigos de Autorización utilizado por el PKI del BCE?									
	1	2	3	4	5	6	7	8	9	10
1									1	
2								1		
3										
4									1	
5							1			
6									1	
7								1		
8			1							
9										1
10									1	
11										1
12							1			
13										1
14										1
15										1
16									1	
17									1	
18									1	
19										1
20									1	
21									1	
22								1		
23								1		
24								1		
T	0	0	1	0	0	0	2	5	9	6
%	0	0	4,17	0	0	0	8,33	20,83	37,5	25

Menor:	3
Mayor:	10
Moda:	9
Promedio	8,61

Nº	2 ¿Sabe Ud. cuál es el período de duración del Código de Autorización?		
	5 días	21 días	Otro
1		1	
2			NS
3			
4			1a
5			NS
6			NS
7			NS
8			NS
9			1a
10			NS
11			NS
12			1a
13			I
14			NS
15			NS
16			NS
17			30d
18			1a
19			1a
20			4d
21			NS
22			1a
23	1		
24			1a
T	1	1	21
%	4,17	4,17	87,5

2- Otro		
Respuesta	#	%
I	1	4,17
NS	11	45,83
4d	1	4,17
30d	1	4,17
1a	7	29,17
Total:	21	87,50

Nº	3 Los códigos de autorización se han guardado en (seleccione las que aplican).			
	Correo	Papel	Doc PC	Otro
1				D
2			1	
3				
4			1	
5		1		
6				c/p
7				CF
8				B
9			1	
10				BC
11	1			
12				CF
13		1	1	
14	1			
15				B
16				BC
17			1	
18				BC
19				DE
20		1	1	
21				CF
22				CF
23	1			
24		1		
T	3	4	6	12
%	12,5	16,67	25	50

3- Otro		
Respuesta	#	%
B	2	8,33
BC	3	12,50
CF	4	16,67
c/p	1	4,17
D	1	4,17
DE	1	4,17
Total:	12	50,00

Nº	4 ¿Ha revelado los códigos de autorización a otra persona?		
	Si	No	Por qué?
1		1	
2		1	
3			
4		1	
5		1	
6		1	
7		1	
8		1	
9		1	
10		1	
11		1	
12		1	
13		1	
14		1	
15		1	
16		1	
17	1		M1
18		1	
19		1	
20		1	
21		1	
22		1	
23	1		M2
24		1	
T	2	21	0
%	8,33	88	0

Sigla	Significado
B	Bóveda
BC	Bajo Custodia
CF	Caja fuerte
c/p	Depende de cada persona
D	Destruido
DE	Dispositivo extraíble
I	Indefinido
M1	Existe una persona del departamento de *helpdesk* encargada de instalar los certificados.
M2	Se reveló el código de autorización para la descarga de los certificados en las sucursales.
NS	No sabe
#a	# años (# significa número de años; por ejemplo dos años)
#d	# días (# significa número de días; por ejemplo treinta días)
[ ]	El encuestado no contestó la pregunta.

Tabla A3.2 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Manejo de Códigos de Autorización

SECCIÓN MANEJO DE CERTIFICADOS DIGITALES (primera parte)

Nº	1 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la generación de los certificados digitales utilizado por el PKI del BCE?									
	1	2	3	4	5	6	7	8	9	10
1									1	
2									1	
3										
4									1	
5									1	
6									1	
7								1		
8		1								
9									1	
10									1	
11										1
12									1	
13										1
14										1
15									1	
16									1	
17									1	
18								1		
19								1		
20										1
21								1		
22									1	
23									1	
24					1					
T	0	1	0	0	1	0	0	4	13	4
%	0	4,17	0	0	4,17	0	0	16,67	54,17	16,67

Menor:	2
Mayor:	10
Moda:	9
Promedio:	8,52

Nº	2 ¿Sabe Ud. cuál es el período de duración de un certificado digital?		
	1 año	2 años	Otro
1	1		
2			NS
3			
4	1		
5	1		
6			NS
7	1		
8	1		
9	1		
10			NS
11	1		
12	1		
13			I
14	1		
15	1		
16	1		
17	1		
18	1		
19	1		
20	1		
21	1		
22			NS
23			I
24	1		
T	17	0	6
%	70,83	0	25

2- Otro		
Respuesta	#	%
I	2	8,33
NS	4	16,67
Total:	6	25,00

Sigla	Significado
I	indefinido
NS	No sabe
☐	El encuestado no contestó la pregunta.

Tabla A3.3 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Manejo de Certificados Digitales

SECCIÓN MANEJO DE CERTIFICADOS DIGITALES (segunda parte)

Nº	3 Dentro de su institución, los certificados digitales se almacenan en: (seleccione las que aplican).		
	Dispositivo extraíble	Disco duro	Otro
1		1	
2		1	
3			
4		1	
5		1	
6			NS
7			B
8		1	
9		1	
10		1	
11		1	
12	1		
13		1	
14		1	
15		1	
16	1		
17		1	
18			BC
19	1		
20		1	
21		1	
22		1	
23	1	1	
24		1	
T	4	17	3
%	16,67	70,833	12,5

Nº	4 ¿Se permite que diferentes usuarios tengan acceso a los certificados digitales?	
	Si	No
1		1
2	1	
3		
4		1
5		1
6		1
7		1
8		1
9		1
10		1
11		1
12		1
13		1
14		1
15		1
16		1
17		1
18		1
19		1
20		1
21		1
22		1
23		1
24		1
T	1	22
%	4,17	91,67

Nº	5 ¿Cuántos certificados ha expedido el PKI del BCE para su institución?		
	#	Porcentaje %	L
1	5	2,86%	G
2	10	5,71%	Q
3			G
4	2	1,14%	Q
5	2	1,14%	G
6	3	1,71%	L
7	3	1,71%	Q
8	2	1,14%	G
9	1	0,57%	Q
10	2	1,14%	G
11	NR		G
12	1	0,57%	Q
13	12	6,86%	Q
14	5	2,86%	Q
15	2	1,14%	Q
16	1	0,57%	Q
17	3	1,71%	Q
18	2	1,14%	Q
19	2	1,14%	C
20	5	2,86%	Q
21	2	1,14%	Q
22	6	3,43%	G
23	2	1,14%	Q
24	4	2,29%	Q
T	77	44%	
%	44	44%	

3- Otro		
Respuesta	#	%
B	1	4,17
BC	1	4,17
NS	1	4,17
Total:	3	12,50

Sigla	Significado
B	Bóveda
BC	Bajo Custodia
C	Cuenca
G	Guayaquil
L	Loja
NR	No recuerda
NS	No sabe
Q	Quito
□	El encuestado no contestó la pregunta.

Tabla A3.4 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Manejo de Certificados Digitales

SECCIÓN CUMPLIMIENTO DE POLÍTICAS (primera parte)

Nº	1 ¿Se han dado recomendaciones sobre el manejo de: códigos de autorización y certificados digitales por parte de los Administradores del PKI del BCE?	
	Si	No
1	1	
2	1	
3	1	
4	1	
5	1	
6	1	
7	1	
8	1	
9	1	
10	1	
11	1	
12		1
13		1
14	1	
15	1	
16	1	
17	1	
18	1	
19		1
20	1	
21	1	
22	1	
23	1	
24	1	
T	21	3
%	87,5	12,5

Nº	1.1 Si la respuesta es Si: ¿Se dio una explicación del por qué de estas recomendaciones?		
	Si	No	Parcialmente
1	1		
2	1		
3	1		
4	1		
5			1
6	1		
7	1		
8	1		
9		1	
10	1		
11	1		
12			
13			
14	1		
15	1		
16	1		
17	1		
18			1
19			
20	1		
21			1
22		1	
23	1		
24			1
T	15	2	4
%	71,43	9,52	19,05

Nº	¿Se han cumplido estas recomendaciones?		
	Si	No	Parcialmente
1	1		
2	1		
3	1		
4	1		
5	1		
6	1		
7	1		
8	1		
9	1		
10	1		
11	1		
12			
13			
14			NS
15	1		
16	1		
17	1		
18	1		
19			
20	1		
21	1		
22	1		
23			1
24			1
T	18	0	2
%	85,71	0	9,52

Nº	2 ¿Se han establecido normas y políticas de seguridad para el manejo de los códigos de autorización y certificados digitales por parte de su institución?	
	Si	No
1	1	
2		1
3	1	
4	1	
5	1	
6		1
7	1	
8		1
9	1	
10	1	
11		1
12	1	
13	1	
14		1
15	1	
16		1
17	1	
18	1	
19		1
20	1	
21	1	
22	1	
23	1	
24	1	
T	17	7
%	70,83	29,17

Sigla	Significado
NS	No sabe
☐	El encuestado no contestó la pregunta.

Tabla A3.5 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Cumplimiento de Políticas

SECCIÓN CUMPLIMIENTO DE POLÍTICAS (segunda parte)

2.1 Si la respuesta es Si.								3 ¿En cuáles de las siguientes situaciones reportaría un suceso al Administrador del PKI del BCE? (seleccione las que aplican).					
Nº	¿Se dio una explicación del por qué de estas normas y políticas a los usuarios?			Nº	¿Se han cumplido estas normas y políticas?			Nº	vac.	acc.	deja trab.	pass. comp.	cert. comp.	Otro
	Si	No	Parcialmente		Si	No	Parcialmente							
1	1			1	1			1	1	1	1	1	1	
2				2				2			1	1		
3	1			3	1			3	1			1	1	
4	1			4	1			4					1	
5	1			5	1			5			1			
6				6				6	1	1	1	1	1	FT
7	1			7	1			7			1	1		
8				8				8			1	1		
9	1			9	1			9		1				
10	1			10	1			10	1		1			
11				11				11						
12		1		12	1			12	1	1	1	1	1	
13	1			13	1			13			1			
14				14				14			1			
15	1			15	1			15			1		1	CC
16				16				16						
17	1			17	1			17			1	1		
18	1			18	1			18			1	1	1	
19				19				19			1			DU
20	1			20	1			20	1	1	1	1	1	
21	1			21	1			21			1			DU
22	1			22	1			22			1	1	1	
23	1			23	1			23	1		1	1	1	
24	1			24	1			24			1			
T	16	1	0	T	17	0	0	T	7	5	19	12	10	4
%	94,12	5,88	0	%	100	0	0	%	29,17	20,83	79,17	50	41,67	16,67

3- Otro		
Respuesta	#	%
CC	1	4,17
DU	2	8,33
FT	1	4,17
Total:	4	16,67

Sigla	Significado
CC	Cambio de Cargo (funciones del empleado)
DU	Se desconfía del usuario
FT	Falla técnica en el Sistema de la PKI
□	El encuestado no contestó la pregunta.

Tabla A3.6 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Cumplimiento de Políticas

SECCIÓN SOPORTE TÉCNICO

Nº	1 ¿Ha utilizado el soporte técnico brindado por el PKI del BCE?	
	Si	No
1	1	
2	1	
3		1
4	1	
5	1	
6		1
7		1
8	1	
9	1	
10	1	
11	1	
12		1
13	1	
14	1	
15	1	
16	1	
17	1	
18	1	
19	1	
20	1	
21	1	
22	1	
23	1	
24		1
T	19	5
%	79,17	20,83

1.1 Si la respuesta es Si

Nº	La información disponible sobre el funcionamiento con PKI del BCE es		
	Púb.	Rest.	Usu. de Cert.
1			1
2		1	
3			
4			1
5		1	
6			
7			
8			1
9			1
10			1
11	1		
12			
13			1
14	1		
15	1		
16			1
17			1
18			1
19			1
20	1		
21			1
22			1
23			1
24			
T	4	2	13
%	21,05	10,53	68,42

Nº	¿Cual es la disponibilidad del soporte técnico?			
	Hor. Ofic.	24 horas	Otro	
1	1			
2	1			
3				
4	1			
5	1			
6				
7				
8	1			
9	1			
10	1			
11			NS	
12				
13	1			
14	1			
15	1			
16	1			
17			NS	
18	1			
19			NE	
20	1			
21	1			
22	1			
23	1			
24				
T	18	0	3	
%	84,21	0	15,79	

1.1.1 - Otro		
Respuesta	#	%
NE	1	5,26
NS	2	10,53
Total:	3	15,79

Nº	La asistencia se realiza (seleccione los que aplican)			
	Tlf.	Pers.	Correo	Otro
1	1		1	
2			1	
3				
4	1			
5	1		1	
6				
7				
8		1	1	
9	1	1		
10	1			
11	1		1	
12				
13	1			
14	1			
15	1		1	
16	1			
17	1		1	
18	1			
19	1			
20	1	1	1	
21	1			
22	1		1	
23	1	1		
24				
T	17	4	9	0
%	89,47	21,05	47,37	0

Nº	En una escala de 1 a 10, siendo 10 el mayor nivel de calidad del soporte técnico y 1 el menor, ¿Que puntuación da usted al soporte técnico brindado por los administradores de PKI del BCE?									
	1	2	3	4	5	6	7	8	9	10
1								1		
2									1	
3										
4									1	
5						1				
6										
7										
8								1		
9										1
10									1	
11									1	
12										
13									1	
14									1	
15										1
16									1	
17										1
18								1		
19				1						
20										1
21								1		
22								1		
23									1	
24										
T	0	0	0	1	0	1	0	5	8	4
%	0	0	0	5,26	0	5,26	0	26,3	42,1	21,1

Menor:	5
Mayor:	10
Moda:	9
Promedio:	8,53

Sigla	Significado
NE	No es estable
NS	No sabe
☐	El encuestado no contestó la pregunta.

Tabla A3.7 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Soporte Técnico

A.3.3. RESULTADOS DE LAS ENCUESTAS APLICADAS A LOS 24 RESPONSABLES DE LOS CERTIFICADOS DE CADA INSTITUCIÓN QUE FORMA PARTE DEL SNP

A continuación se exponen los resultados encontrados al evaluar mediante el encuestamiento a los 24 responsables de los certificados digitales de cada institución que forma parte del Sistema Nacional de Pagos.

SECCIÓN GENERAL

Sigla	Significado
NC	No contesta
SCI	Sistema Cobros Interbancario
SPI	Sistema de Pagos Interbancario
SPL	Sistema de Pagos en Línea
SPN	Sistema de Pagos por valores Netos

Tabla A3.8 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección General

1. Que aplicación o aplicaciones utiliza su institución en el Sistema Nacional de Pagos: (seleccione las que aplican)

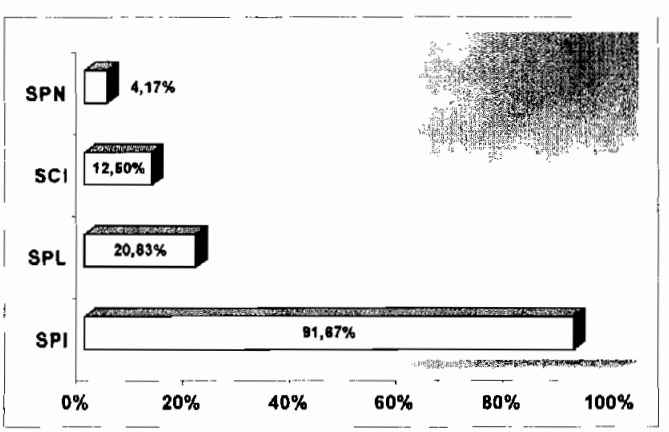
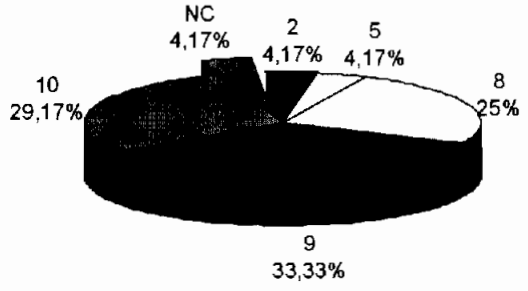


Figura A3.1 Resultados pregunta 1 – sección General

2. En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la solicitud de certificados digitales utilizado por la PKI del BCE?

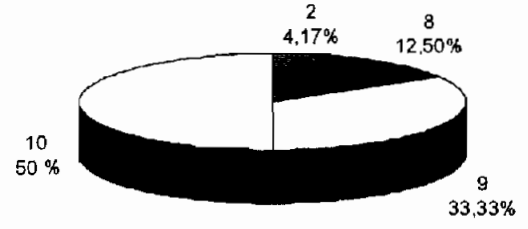


Menor:	2
Mayor:	10
Moda:	9
Promedio:	8,57

Figura A3.2 Resultados pregunta 2 – sección General

Las puntuaciones con los valores: 1, 3, 4, 6 y 7 no se muestran en el gráfico por tener un valor del cero por ciento (0%).

3. En una escala de 1 a 10, siendo 10 el mayor nivel de confiabilidad y 1 el menor. ¿Qué puntuación daría usted al nivel de confianza de la PKI del BCE?



Menor:	2
Mayor:	10
Moda:	10
Promedio:	9,08

Figura A3.3 Resultados pregunta 3 – sección General

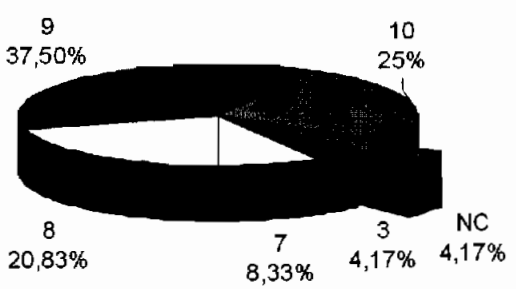
Las puntuaciones con los valores: 1, 3, 4, 5, 6 y 7 no se muestran en el gráfico por tener un valor del cero por ciento (0%).

SECCIÓN I: MANEJO DE CÓDIGOS DE AUTORIZACIÓN

Sigla	Significado
B	Bóveda
BC	Bajo Custodia
CF	Caja fuerte
c/p	Depende de cada persona
D	Destruido
DE	Dispositivo extraíble
I	Indefinido
NS	No sabe
#a	# años (# significa número de años; por ejemplo dos años)
#d	# días (# significa número de días; por ejemplo treinta días)

Tabla A3.9 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Manejo de Códigos de Autorización

1. En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la entrega de los Códigos de Autorización utilizado por la PKI del BCE?



Menor:	3
Mayor:	10
Moda:	9
Promedio:	8,61

Figura A3.4 Resultados pregunta 1 – sección Manejo de Códigos de Autorización

Las puntuaciones con los valores: 1, 2, 4, 5 y 6 no se muestran en el gráfico por tener un valor del cero por ciento (0%).

2. ¿Sabe Ud. cuál es el período de duración del Código de Autorización?

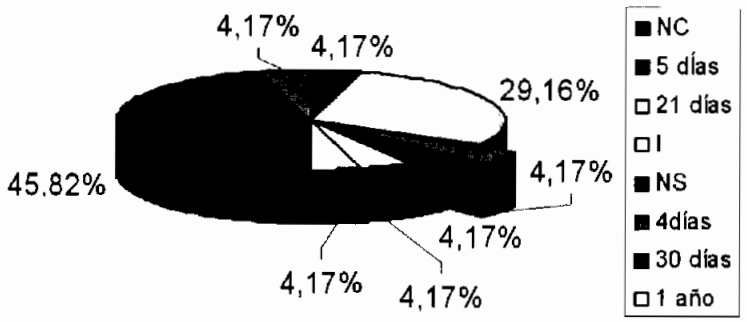


Figura A3.5 Resultados pregunta 2 – sección Manejo de Códigos de Autorización

3. Los códigos de autorización se han guardado en: (seleccione las que aplican).

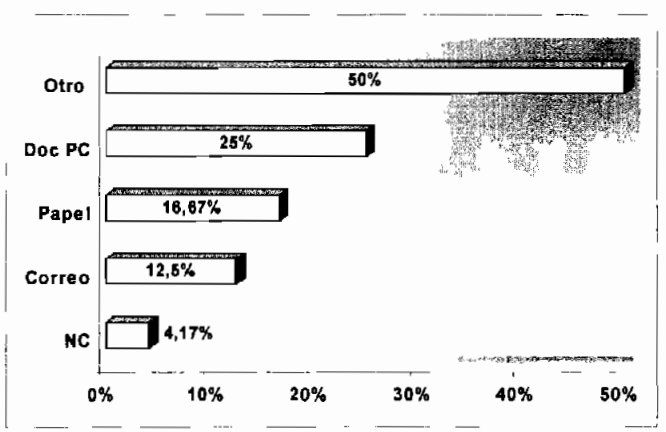


Figura A3.6 Resultados pregunta 3 – sección Manejo de Códigos de Autorización

4. ¿Ha revelado los códigos de autorización a otra persona?

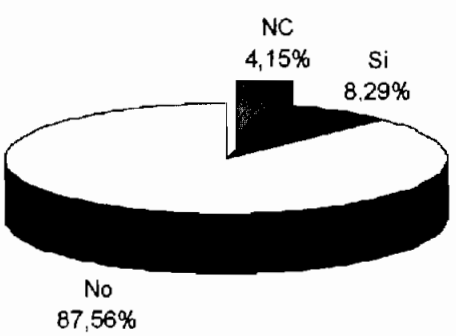


Figura A3.7 Resultados pregunta 4 – sección Manejo de Códigos de Autorización

a. ¿Por qué?

M1: Existe una persona del departamento de helpdesk encargada de instalar los certificados.

M2: Se reveló el código de autorización para la descarga de los certificados en las sucursales.

SECCIÓN II: MANEJO DE CERTIFICADOS DIGITALES

Sigla	Significado
B	Bóveda
BC	Bajo Custodia
I	indefinido
NC	No contesta
NR	No recuerda
NS	No sabe

Tabla A3.10 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Manejo de Certificados Digitales

1. En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la generación de los certificados digitales utilizado por la PKI del BCE?

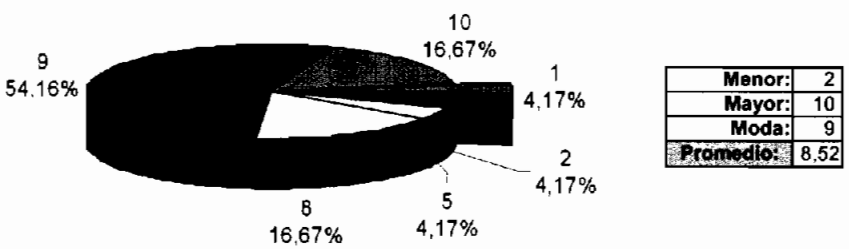


Figura A3.8 Resultados pregunta 1 – sección Manejo de Certificados Digitales

Las puntuaciones con los valores: 1, 3, 4, 6 y 7 no se muestran en el gráfico por tener un valor del cero por ciento (0%).

2. ¿Sabe Ud. cuál es el período de duración de un Certificado Digital?

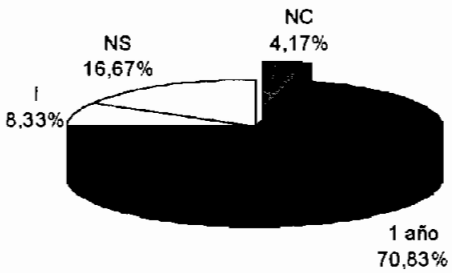


Figura A3.9 Resultados pregunta 2 – sección Manejo de Certificados Digitales

El valor de 2 años no se muestra en el gráfico por tener un valor del cero por ciento (0%).

3. Dentro de su institución, los certificados digitales se almacenan en: (seleccione las que aplican).

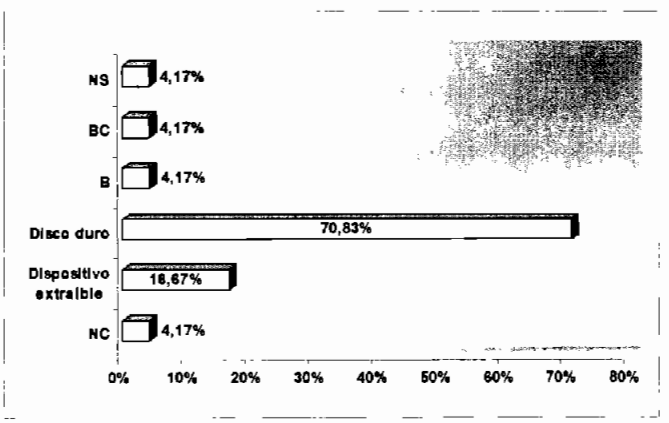


Figura A3.10 Resultados pregunta 3 – sección Manejo de Certificados Digitales

4. ¿Se permite que diferentes usuarios tengan acceso a los certificados digitales?

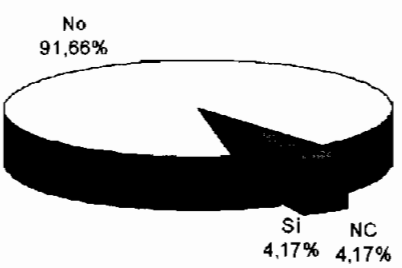
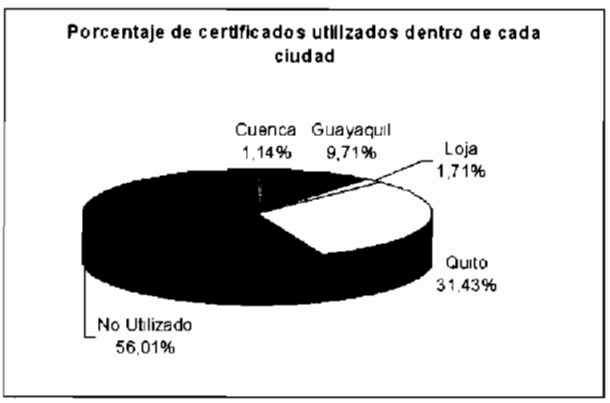


Figura A3.11 Resultados pregunta 4 – sección Manejo de Certificados Digitales

5. ¿Cuántos certificados ha expedido la PKI del BCE para su institución?

Nº	5 ¿Cuántos certificados ha expedido el PKI del BCE para su institución?		
	#	Porcentaje %	L
1	5	2,86%	G
2	10	5,71%	Q
3			G
4	2	1,14%	Q
5	2	1,14%	G
6	3	1,71%	L
7	3	1,71%	Q
8	2	1,14%	G
9	1	0,57%	Q
10	2	1,14%	G
11	NR	-	G
12	1	0,57%	Q
13	12	6,86%	Q
14	5	2,86%	Q
15	2	1,14%	Q
16	1	0,57%	Q
17	3	1,71%	Q
18	2	1,14%	Q
19	2	1,14%	C
20	5	2,86%	Q
21	2	1,14%	Q
22	6	3,43%	G
23	2	1,14%	Q
24	4	2,29%	Q
T	77	44%	
%	44	44%	



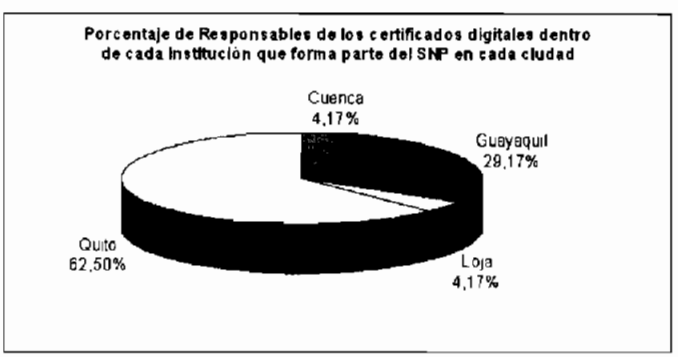


Figura A3.12 Resultados pregunta 5 – sección Manejo de Certificados Digitales

SECCIÓN III: CUMPLIMIENTO DE POLÍTICAS

1. ¿Se han dado recomendaciones sobre el manejo de: códigos de autorización y certificados digitales por parte de los Administradores de la PKI del BCE?

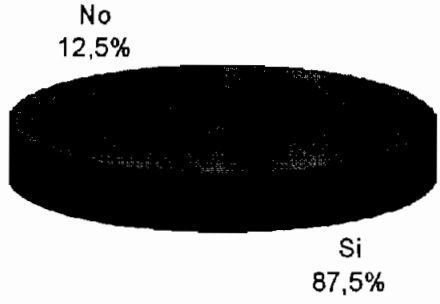


Figura A3.13 Resultados pregunta 1 – sección Cumplimiento de Políticas

a. Si la respuesta es Si:

i. ¿Se dio una explicación del por qué de estas recomendaciones?

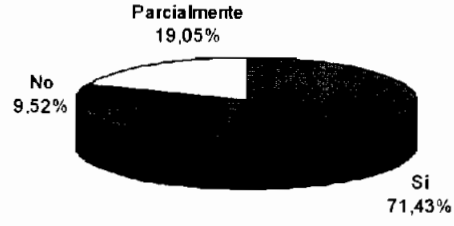


Figura A3.14 Resultados pregunta 1.1 – sección Cumplimiento de Políticas

ii. ¿Se han cumplido estas recomendaciones?

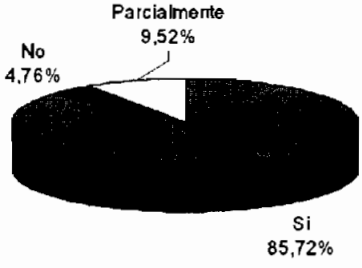


Figura A3.15 Resultados pregunta 1.2 – sección Cumplimiento de Políticas

2. ¿Se han establecido normas y políticas de seguridad para el manejo de los códigos de autorización y certificados digitales por parte de su institución?

Figura A3.16 Resultados pregunta 2 – sección Cumplimiento de Políticas

a. Si la respuesta es Si:

i. ¿Se dio una explicación del por qué de estas normas y políticas a los usuarios?

Figura A3.17 Resultados pregunta 2.1 – sección Cumplimiento de Políticas

ii. ¿Se han cumplido estas normas y políticas?

Figura A3.18 Resultados pregunta 2.2 – sección Cumplimiento de Políticas

3. ¿En cuáles de las siguientes situaciones reportaría un suceso al Administrador de la PKI del BCE? (seleccione las que aplican).

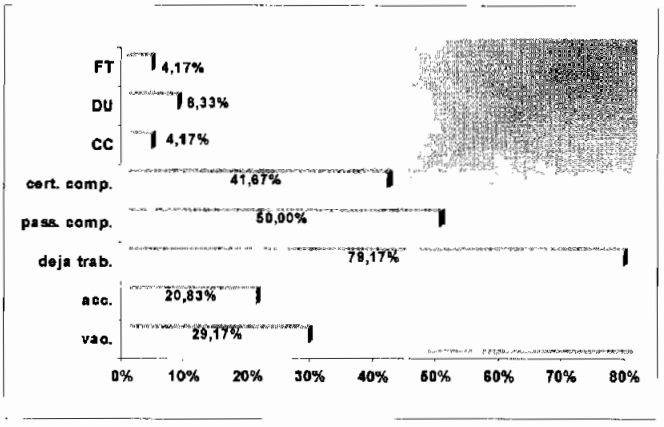


Figura A3.19 Resultados pregunta 3 – sección Cumplimiento de Políticas

Sigla	Significado
CC	Cambio de Cargo (funciones del empleado)
DU	Se desconfía del usuario
FT	Falla técnica en el Sistema de la PKI

Tabla A3.11 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Cumplimiento de Políticas

SECCIÓN I V: SOPORTE TÉCNICO

1. ¿Ha utilizado el soporte técnico brindado por la PKI del BCE?

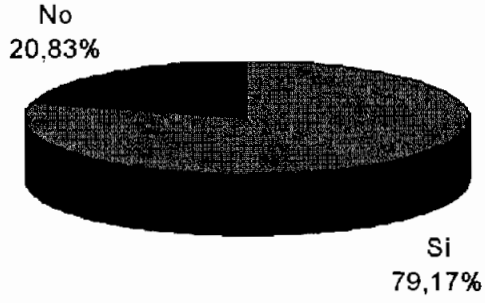


Figura A3.20 Resultados pregunta 1 – sección Soporte Técnico

a. Si la respuesta es si:

i. La información disponible sobre el funcionamiento de la PKI del BCE es:

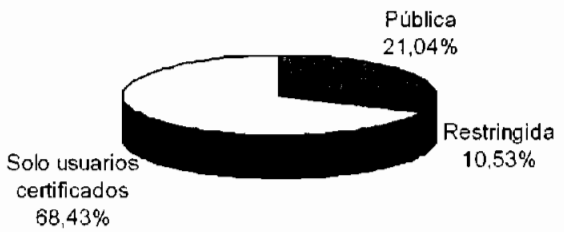


Figura A3.21 Resultados pregunta 1.1 – sección Soporte Técnico

ii. ¿Cuál es la disponibilidad del Soporte Técnico?:

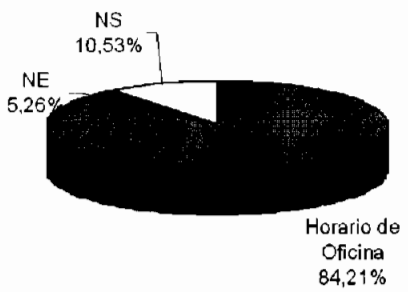


Figura A3.22 Resultados pregunta 1.2 – sección Soporte Técnico

Sigla	Significado
NE	No es estable
NS	No sabe

Tabla A3.12 Siglas para la tabulación de las encuestas realizadas a los responsables de los certificados de cada institución que forma parte del SNP – sección Soporte Técnico

iii. La asistencia se realiza:

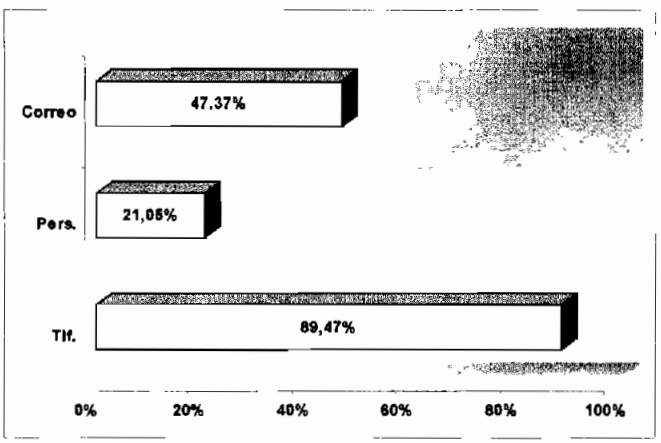
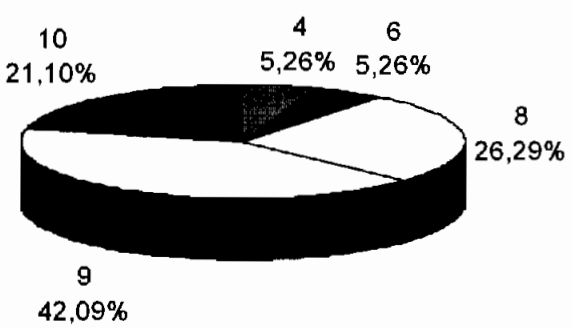


Figura A3.23 Resultados pregunta 1.3 – sección Soporte Técnico

iv. En una escala de 1 a 10, siendo 10 el mayor nivel de calidad del soporte técnico y 1 el menor. ¿Qué puntuación daría usted al soporte técnico brindado por los administradores de la PKI del BCE?



Menor:	5
Mayor:	10
Moda:	9
Promedio:	8,53

Figura A3.24 Resultados pregunta 1.4 – sección Soporte Técnico

Las puntuaciones con los valores: 1, 2, 3, 5 y 7 no se muestran en el gráfico por tener un valor del cero por ciento (0%).

Anexo 4

Formato, Tabulación y Resultados de Encuesta Aplicada a los Usuarios de los Certificados de las Instituciones que forman parte del SNP

A.4. FORMATO, TABULACIÓN Y RESULTADOS DE ENCUESTA APLICADA A LOS USUARIOS DE LOS CERTIFICADOS DE LAS INSTITUCIONES QUE FORMAN PARTE DEL SNP

A.4.1. FORMATO DE ENCUESTA APLICADA A LOS USUARIOS DE LOS CERTIFICADOS DE LAS INSTITUCIONES QUE FORMAN PARTE DEL SNP

OBJETIVO DE LA ENCUESTA

Recolectar información del desempeño de los Usuarios de los Certificados de las instituciones que forman parte del SNP (Sistema Nacional de Pagos).

Objetivos específicos

- Determinar el nivel de seguridad que se tiene en el manejo del número de referencia.
- Determinar el nivel de seguridad que se tiene en el manejo de certificados digitales.
- Identificar el nivel de cumplimiento de los procedimientos recomendados por los Administradores de la PKI del Banco Central del Ecuador.
- Determinar la calidad del soporte técnico que reciben los Usuarios de los Certificados por parte de la PKI del Banco Central del Ecuador.

CÁLCULOS DE LA MUESTRA

Las encuestas se realizaron[1] telefónicamente entre el 30 de Enero y el 17 de Febrero de 2006; utilizando como método el muestreo aleatorio simple; debido a que este método es adecuado para poblaciones pequeñas, compuestas por elementos homogéneos; como es el caso de los usuarios de certificados del SNP.

Hasta el 30 de Enero de 2006, la PKI del BCE ha expedido 175 certificados digitales para usuarios dentro del SNP; sin embargo, no todos los certificados digitales se encuentran en uso actualmente. Con el fin de determinar la población real que al momento hace uso del SNP, se

[1] La realización de las encuestas fue aprobada por el Director de Informática del Banco Central Del Ecuador el 30 de Noviembre de 2005; los responsables de los certificados digitales de cada institución fueron informados de la realización del estudio de mercado el 23 de Enero del 2006.

analizó los registros[1] de los accesos de los usuarios que se almacenan diariamente dentro del sistema *TruePass*[2] de *Entrust*.

Como resultado de este análisis, se determinó que 83 usuarios accedieron al SNP durante el periodo de almacenamiento de los registros examinados; por este motivo, se toma como población total 83 usuarios. Los datos considerados para la determinación de la muestra y del error de muestreo se encuentran en la tabla A4.1 y los resultados correspondientes en la tabla A4.2. Para el cálculo del cálculo del error de muestreo se utiliza la fórmula A4.1.

Datos para cálculo del tamaño de la muestra y el error de estimación	
Parámetro	**Valor**
i: Inicio.	1
N: Población total.	83
Z: Grado de confiabilidad.	1.81 (94%)
p: Probabilidad de que un usuario A sea encuestado dentro del proceso de encuestamiento.	0.5
1-p (q): Probabilidad de que un usuario A sea encuestado dentro del proceso de encuestamiento.	0.5[3]

Tabla A4.1 Datos para el cálculo del tamaño de la muestra y el error de muestreo

Resultados	
Parámetro	**Valor**
N: Muestra a encuestar.	20.75 (21)[4]
B: Error de muestreo[5]	17,3%

Tabla A4.2 Resultados del cálculo del tamaño de la muestra y el error de muestreo

$$B = Z\sqrt{\frac{pq(N-n)}{n(N-1)}}$$

Fórmula A4.2 Cálculo del error de estimación[6]

Como resultado se tiene una muestra de 21 usuarios de certificados digitales con un grado de confiabilidad del 94% y un 17,3% de error de muestreo.

---

[1] Los registros analizados se almacenaron entre el 1 de diciembre de 2005 y el 4 de Enero del 2006.

[2] Autenticación robusta.

[3] Cuando no se tiene datos reales de la población, p y q toman el valor máximo (0.5) para considerar la situación más desfavorable.

[4] Debido al control de Seguridad de la PKI del Banco Central, la muestra tomada se limita al 25% de la población total.

[5] Falta de coincidencia entre los datos reales de la población y los obtenidos al realizar la encuesta sobre una muestra; es decir, es el error introducido cuando se utilizan muestras en lugar de la población total.

[6] Mat. Carlos Echeverría (Escuela de Ciencias – EPN).

FORMATO DE ENCUESTA APLICADA A LOS USUARIOS DE LOS CERTIFICADOS DE LAS INSTITUCIONES QUE FORMAN PARTE DEL SNP

Esta encuesta ha sido realizada con fines investigativos, por parte de la Srta. Shirma Ortiz Boada, estudiante de la Carrera de Ingeniería Electrónica y Redes de Información de la Escuela Politécnica Nacional.

GENERAL

1 Que aplicación usa dentro del Sistema Nacional de Pagos: (seleccione las que aplican)

- ☐ Sistema de Pagos Interbancario (SPI)
- ☐ Sistema de Pagos en Línea (SPL)
- ☐ Sistema de Cobros Interbancario
- ☐ Otro (especifique)_____

2 En una escala de 1 a 10, siendo 10 el mayor nivel de confiabilidad y 1 el menor. ¿Qué puntuación daría usted al nivel de confianza de la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

I MANEJO DE NÚMERO DE REFERENCIA:

1 ¿Cómo obtuvo el número de referencia para la generación de su certificado personal?

- ☐ Correo electrónico
- ☐ Telefónicamente
- ☐ Personalmente
- ☐ Otro (especifique)_____

2 ¿Sabe Ud. cuál es el período de duración del Número de Referencia?

☐ 5 días ☐ 21 días ☐ Otro (especifique)_____

3 ¿Sabe usted para qué sirve el número de referencia?

☐ Si ☐ No

4 El número de referencia se han guardado en: (seleccione las que aplican).

- ☐ Correo electrónico
- ☐ Escrito en un Papel
- ☐ En un documento en la computadora
- ☐ Otro (especifique)_____

5 ¿Ha revelado el número de referencia a otra persona?

☐ Si ☐ No

¿A qué persona?_____

II MANEJO DE CERTIFICADOS DIGITALES:

1 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la generación de los certificados digitales utilizado por la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

2 ¿Cuál es el período de duración de su Certificado Digital?

☐ 1 año ☐ 2 años ☐ Otro (especifique)_____

3 Su certificado digital se ha almacenado en: (seleccione las que aplican).

☐ Disquete/CD/Otro dispositivo extraíble
☐ Disco duro
☐ Otro (especifique)_____

4 ¿Ha permitido que otra persona tenga acceso a su certificado digital?

☐ Si ☐ No

III CUMPLIMIENTO DE POLÍTICAS

1 ¿Se han establecido normas y políticas de seguridad para el manejo de los *números de referencia* y certificados digitales por parte de su institución?

☐ Si ☐ No

Si la respuesta es Si:

¿Se dio una explicación del por qué de estas normas y políticas?

☐ Si ☐ No ☐ Parcialmente

¿Se han cumplido estas normas y políticas?

☐ Si ☐ No ☐ Parcialmente

I V SOPORTE TÉCNICO

1 ¿Ha utilizado el soporte técnico brindado por la PKI del BCE?

☐ Si ☐ No

Si la respuesta es si:

¿Sabe Ud. cuál es la disponibilidad del Soporte Técnico?:

☐ Horario de oficina
☐ 24 horas
☐ Otro (especifique)_____

La asistencia se realiza:

- ☐ Telefónicamente
- ☐ Personalmente
- ☐ Por medio de correo electrónico
- ☐ Otro (especifique) _____

2 En una escala de 1 a 10, siendo 10 el mayor nivel de calidad del soporte técnico y 1 el menor. ¿Qué puntuación daría usted al soporte técnico brindado por los administradores de la PKI del BCE?

1	2	3	4	5	6	7	8	9	10

¡Gracias por su colaboración!

A.4.2. TABULACIÓN DE LAS ENCUESTAS APLICADAS A 21 USUARIOS DE LOS CERTIFICADOS DE LAS INSTITUCIONES QUE FORMA PARTE DEL SNP

SECCIÓN GENERAL

Nº	1 ¿Qué aplicación usa dentro del Sistema Nacional de Pagos? (seleccione las que aplican).			
	SPI	SPL	SCI	Otro
1	1	1		
2	1		1	
3	1			
4	1		1	
5	1		1	
6	1			SPN
7	1			
8	1			
9	1			
10	1			
11	1			
12	1			
13	1			
14	1			
15				SPN
16	1			
17	1			
18	1			
19	1	1		
20		1		
21	1	1		
T	19	4	3	2
%	90,48	19,05	14,29	9,52

1- Otro		
Respuesta	#	%
SPN	2	9,52
Total:	2	9,52

Nº	2 En una escala de 1 a 10, siendo 10 el mayor nivel de Confiabilidad y 1 el menor. ¿Qué puntuación darla usted al nivel de confianza del PKI del BCE?									
	1	2	3	4	5	6	7	8	9	10
1										1
2										1
3									1	
4										1
5									1	
6										1
7										1
8									1	
9										1
10										1
11									1	
12						1				
13										1
14										1
15								1		
16									1	
17										1
18										1
19								1		
20										1
21										1
T	0	0	0	0	0	1	0	2	5	13
%	0	0	0	0	0	4,76	0	9,52	23,81	61,90

Menor:	6
Mayor:	10
Moda:	10
Promedio:	9,38

Sigla	Significado
SCI	Sistema Cobros Interbancario
SPI	Sistema de Pagos Interbancario
SPL	Sistema de Pagos en Línea
SPN	Sistema de Pagos por valores Netos
☐	El encuestado no contestó la pregunta.

Tabla A4.3 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección General

SECCIÓN MANEJO DE NÚMERO DE REFERENCIA (primera parte)

Nº	1 ¿Cómo obtuvo el número de referencia para la generación de su certificado personal?			
	Correo	Tlf.	Pers.	Otro
1	1	1		
2		1		
3		1		
4		1		
5			1	
6		1		
7			1	
8			1	
9				
10	1			
11				
12	1			
13	1			
14			1	
15	1			
16			1	
17	1			
18				NR
19			1	
20			1	
21	1			
T	7	5	7	1
%	33,33	23,81	33,33	4,76

Nº	2 ¿Sabe Ud. cuál es el período de duración del número de referencia?		
	5 días	21 días	Otro
1		1	
2			NS
3			NS
4			NS
5			NS
6			NS
7		1	
8			NS
9			
10	1		
11			
12			NS
13			NS
14			NS
15	1		
16			1M
17			1A
18			1M
19			NS
20			NS
21			NS
T	2	2	15
%	9,52	9,52	71,43

1- Otro		
Respuesta	#	%
NR	1	4,76
Total:	1	4,76

2- Otro		
Respuesta	#	%
NS	12	57,14
1m	2	9,52
1a	1	4,76
Total:	15	71,43

Sigla	Significado
NR	No Recuerda
NS	No sabe
#a	# años (# significa número de años; por ejemplo dos años)
#m	# meses (# significa número de meses; por ejemplo dos meses)
□	El encuestado no contestó la pregunta.

Tabla A4.4 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección Manejo de Números de Referencia

SECCIÓN MANEJO DE NÚMERO DE REFERENCIA (segunda parte)

Nº	3 ¿Sabe usted para qué sirve el número de referencia?	
	Si	No
1	1	
2		1
3		1
4	1	
5		1
6	1	
7		1
8		1
9		
10	1	
11		
12		1
13		1
14		1
15		1
16		1
17	1	
18	1	
19	1	
20	1	
21	1	
T	9	10
%	42,86	47,62

Nº	4 El número de referencia se ha guardado en: (seleccione las que aplican).			
	Correo	Papel	Doc PC	Otro
1	1			
2		1		
3		1		
4		1		
5			1	
6		1		
7		1		
8			1	
9				
10				M
11				
12		1		
13			1	
14				NS
15				NS
16		1		
17		1		
18				M
19			1	
20				M
21				D
T	1	8	4	6
%	4,76	38,10	19,05	28,57

Nº	5 ¿Ha revelado el número de referencia a otra persona?		
	Si	No	¿A qué persona?
1		1	
2		1	
3	1		PS
4		1	
5		1	
6	1		PS
7		1	
8		1	
9			
10		1	
11			
12		1	
13		1	
14	1		PS
15		1	
16		1	
17		1	
18		1	
19		1	
20		1	
21		1	
T	3	16	-
%	14,29	76,19	-

4- Otro		
Respuesta	#	%
M	3	14,29
NS	2	9,52
D	1	4,76
Total:	6	28,57

[1]

Sigla	Significado
D	Destruido
M	Memorizado
NS	No sabe
PS	Personal de sistemas
☐	El encuestado no contestó la pregunta.

Tabla A4.5 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección Manejo de Números de Referencia

[1] Dos de los usuarios (9,52%) NO RESPONDEN: Los usuarios que corresponden a las encuestas con numeración 9 y 11 no descargaron directamente su certificado; en sus instituciones es el personal de sistemas el encargado del procedimiento e instalación de los certificados, por lo tanto, no se encuentran familiarizados con el procedimiento.

SECCIÓN MANEJO DE CERTIFICADOS DIGITALES (primera parte)

Nº	1 En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la generación de los certificados digitales utilizado por el PKI del BCE?									
	1	2	3	4	5	6	7	8	9	10
1										1
2										1
3								1		
4									1	
5									1	
6								1		
7								1		
8									1	
9									1	
10										1
11										1
12						1				
13									1	
14										1
15								1		
16								1		
17										1
18										1
19									1	
20									1	
21									1	
T	0	0	0	0	0	1	0	5	8	7
%	0	0	0	0	0	4,76	0	23,81	38,10	33,33

Menor:	6
Mayor:	10
Moda:	9
Promedio:	8,95

Nº	2 ¿Sabe Ud. cuál es el período de duración de un certificado digital?		
	1 año	2 años	Otro
1			NS
2			NS
3	1		
4			NS
5	1		
6			NS
7	1		
8			NS
9			NS
10		1	
11			NS
12			NS
13	1		
14			NS
15			NS
16	1		
17	1		
18			NS
19			NS
20			NS
21	1		
T	7	1	13
%	33,33	4,76	61,9

2- Otro		
Respuesta	#	%
NS	13	61,9
Total:	13	61,9

Sigla	Significado
NS	No sabe

Tabla A4.6 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección Manejo de Certificados Digitales

SECCIÓN MANEJO DE CERTIFICADOS DIGITALES (segunda parte)

Nº	3 Dentro de su institución, los certificados digitales se almacenan en: (seleccione las que aplican).		
	Disquete/CD/Otro dispositivo extraíble	Disco duro	Otro
1		1	
2		1	
3		1	
4		1	
5		1	
6		1	
7		1	
8		1	
9		1	
10		1	
11		1	
12		1	
13		1	
14		1	
15		1	
16		1	
17		1	
18		1	
19		1	
20			B
21		1	
T	0	20	1
%	0	95,24	4,762

Nº	4 ¿Ha permitido que otra persona tenga acceso a su certificado digital?	
	Si	No
1		1
2		1
3		1
4		1
5		1
6		1
7		1
8		1
9	1	
10		1
11		1
12		1
13		1
14	1	
15		1
16		1
17		1
18		1
19		1
20		1
21		1
T	2	19
%	9,52	90,48

3- Otro		
Respuesta	#	%
B	1	4,76
Total:	1	4,76

Sigla	Significado
B	Bóveda

Tabla A4.7 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección Manejo de Certificados Digitales

SECCIÓN CUMPLIMIENTO DE POLÍTICAS

Nº	1 ¿Se han establecido normas y políticas de seguridad para el manejo de los números de referencia y certificados digitales por parte de su institución?	
	Si	No
1	1	
2	1	
3	1	
4		1
5	1	
6	1	
7	1	
8		1
9	1	
10	1	
11	1	
12	1	
13	1	
14		1
15	1	
16		1
17	1	
18	1	
19	1	
20		1
21	1	
T	16	5
%	76,19	23,81

1.1 Si la respuesta es Si:								
Nº	¿Se dio una explicación del por qué de estas normas y políticas?			Nº	¿Se han cumplido estas normas y políticas?		
	Si	No	Parcialmente		Si	No	Parcialmente
1	1			1	1		
2	1			2	1		
3	1			3	1		
4				4			
5	1			5	1		
6	1			6	1		
7	1			7	1		
8				8			
9	1			9	1		
10	1			10	1		
11	1			11	1		
12	1			12	1		
13		1		13	1		
14				14			
15			1	15			1
16				16			
17	1			17	1		
18	1			18	1		
19	1			19	1		
20				20			
21	1			21	1		
T	14	1	1	T	15	0	1
%	87,5	6,25	6,25	%	93,75	0	6,25

Sigla	Significado
☐	El encuestado no contestó la pregunta.

Tabla A4.8 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – – sección Cumplimiento de Políticas

SECCIÓN SOPORTE TÉCNICO

Nº	1 ¿Ha utilizado el soporte técnico brindado por el PKI del BCE?	
	Si	No
1	1	
2	1	
3		1
4		1
5	1	
6	1	
7	1	
8	1	
9		1
10	1	
11	1	
12	1	
13		1
14		1
15		1
16	1	
17	1	
18	1	
19	1	
20	1	
21	1	
T	15	6
%	71,43	28,57

1.1 Si la respuesta es Si:			
Nº	1 1 1 ¿Sabe Ud. cuál es la disponibilidad del soporte técnico?		
	Hor. Ofic.	24 horas	Otro
1	1		
2	1		
3			
4			
5	1		
6			NS
7		1	
8	1		
9			
10	1		
11	1		
12	1		
13			
14			
15			
16	1		
17	1		
18	1		
19	1		
20	1		
21	1		
T	13	1	1
%	86,67	6,67	6,67

1.1 Si la respuesta es Si:				
Nº	1 1 2 La asistencia se realiza: (seleccione las que aplican)			
	Tlf.	Pers.	Correo	Otro
1	1		1	
2	1			
3				
4				
5	1		1	
6	1			
7			1	
8	1			
9				
10	1		1	
11	1		1	
12	1			
13				
14				
15				
16	1		1	
17	1	1	1	
18	1			
19	1			
20	1			
21	1			
T	14	1	7	0
%	93,33	6,67	46,67	0

1.1 Si la respuesta es Si:										
Nº	1 1 3 En una escala de 1 a 10, siendo 10 el mayor nivel de calidad del soporte técnico y 1 el menor ¿Qué puntuación daría usted al soporte técnico brindado por los administradores del PKI del BCE?									
	1	2	3	4	5	6	7	8	9	10
1										1
2										1
3										
4										
5							1			
6									1	
7									1	
8									1	
9										
10									1	
11								1		
12					1					
13										
14										
15										
16							1			
17										1
18									1	
19								1		
20										1
21									1	
T	0	0	0	0	1	0	2	2	6	4
%	0	0	0	0	6,67	0	13,33	13,33	40	26,67

Menor:	5
Mayor:	10
Moda:	9
Promedio:	8,6

1.1.1 - Otro		
Respuesta	#	%
NS	1	6,67
Total:	1	6,67

Sigla	Significado
NS	No sabe
□	El encuestado no contestó la pregunta.

Tabla A4.9 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección Soporte Técnico

A.4.3. RESULTADOS DE LAS ENCUESTAS APLICADAS A 21 USUARIOS DE LOS CERTIFICADOS DE LAS INSTITUCIONES QUE FORMAN PARTE DEL SNP

A continuación se exponen los resultados encontrados al evaluar mediante el encuestamiento a 21 usuarios de los certificados digitales de las instituciones que forman parte del Sistema Nacional de Pagos.

SECCIÓN GENERAL

Sigla	Significado
NC	No contesta
SCI	Sistema Cobros Interbancario
SPI	Sistema de Pagos Interbancario
SPL	Sistema de Pagos en Línea
SPN	Sistema de Pagos por valores Netos

Tabla A4.10 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección General

1. Que aplicación usa dentro del Sistema Nacional de Pagos: (seleccione las que aplican)

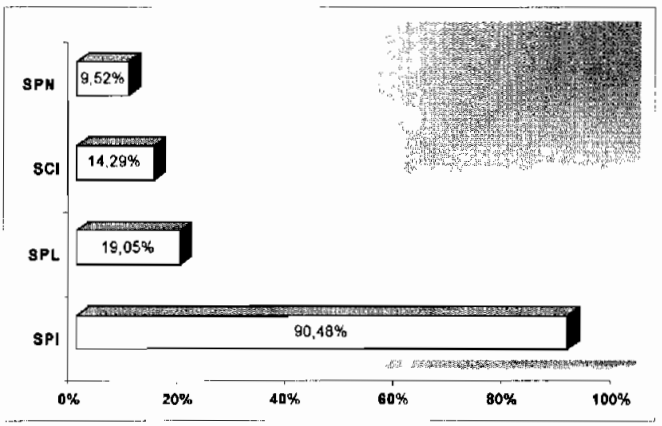
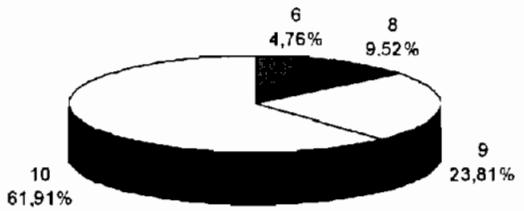


Figura A4.1 Resultados pregunta 1 – sección General

2. En una escala de 1 a 10, siendo 10 el mayor nivel de confiabilidad y 1 el menor. ¿Qué puntuación daría usted al nivel de confianza de la PKI del BCE?



Menor:	6
Mayor:	10
Moda:	10
Promedio:	9,38

Figura A4.2 Resultados pregunta 1 – sección General

Las puntuaciones con los valores: 1, 2, 3, 4, 5 y 7 no se muestran en el gráfico por tener un valor del cero por ciento (0%).

SECCIÓN I: MANEJO DE NÚMERO DE REFERENCIA

Sigla	Significado
D	Destruido
M	Memorizado
NC	No contesta
NR	No recuerda
NS	No sabe
#a	# años (# significa número de años; por ejemplo dos años)
#d	# días (# significa número de días; por ejemplo treinta días)
#m	# meses (# significa número de meses; por ejemplo dos meses)

Tabla A4.11 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección Manejo de Códigos de Autorización

1. ¿Cómo obtuvo el número de referencia para la generación de su certificado personal?

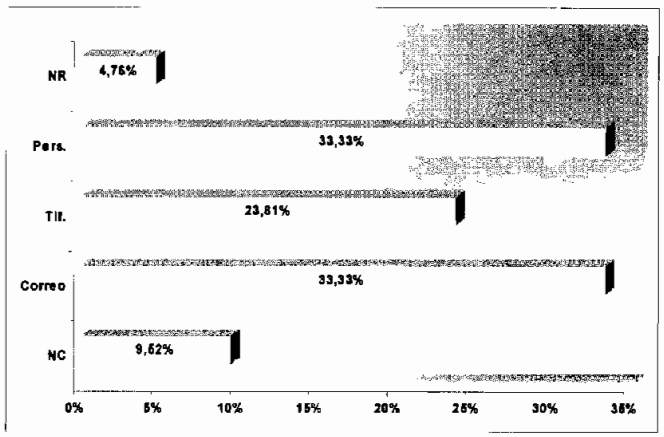


Figura A4.3 Resultados pregunta 1 – sección Manejo de Número de Referencia

2. ¿Sabe Ud. cuál es el período de duración del Número de Referencia?

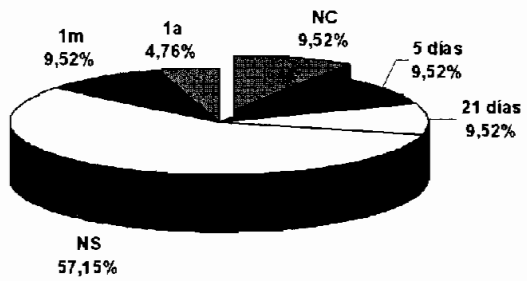


Figura A4.4 Resultados pregunta 2 – sección Manejo de Número de Referencia

3. ¿Sabe Ud. para qué sirve el Número de Referencia?

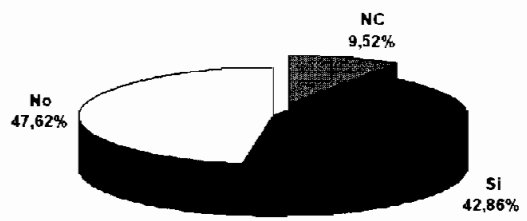


Figura A4.5 Resultados pregunta 3 – sección Manejo de Número de Referencia

4. Los números de referencia se han guardado en: (seleccione las que aplican).

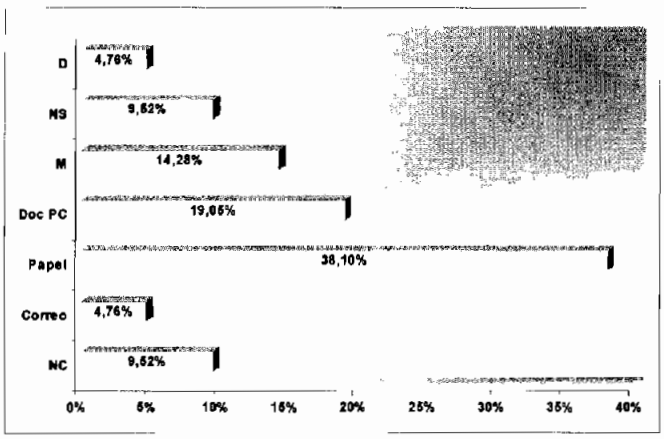


Figura A4.6 Resultados pregunta 4 – sección Manejo de Número de Referencia

5. ¿Ha revelado el número de referencia a otra persona?

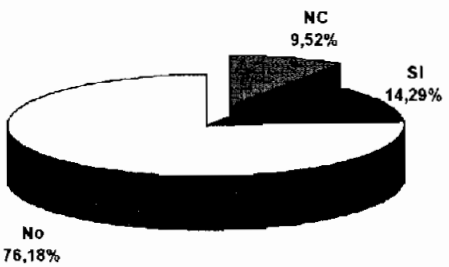


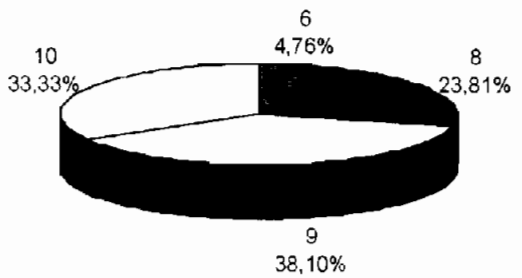
Figura A4.7 Resultados pregunta 5 – sección Manejo de Número de Referencia

a. ¿A qué persona?

   Dentro del proceso se ha detectado que el 14.29 % de usuarios que admitió haber revelado su número de referencia a otra persona; lo hizo debido a que dentro de sus instituciones el encargado de la descarga e instalación de los certificados digitales es el personal de sistemas.

SECCIÓN II: MANEJO DE CERTIFICADOS DIGITALES

1. En una escala de 1 a 10, siendo 10 el mayor nivel de Seguridad y 1 el menor. ¿Qué puntuación daría usted al procedimiento realizado para la generación de los certificados digitales utilizado por la PKI del BCE?



Menor:	6
Mayor:	10
Moda:	9
Promedio:	8,95

Figura A4.8 Resultados pregunta 1 – sección Manejo de Certificados Digitales

Las puntuaciones con los valores: 1, 3, 4, 6 y 7 no se muestran en el gráfico por tener un valor del cero por ciento (0%).

2. ¿Sabe Ud. cuál es el período de duración de un Certificado Digital?

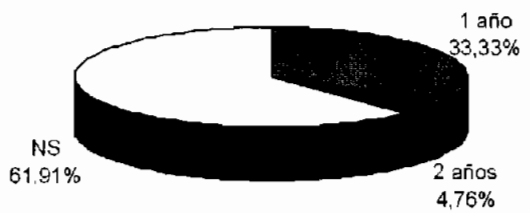


Figura A4.9 Resultados pregunta 2 – sección Manejo de Certificados Digitales

Sigla	Significado
B	Bóveda
NS	No sabe

Tabla A4.12 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección Manejo de Certificados Digitales

3. Su certificado digital se ha almacenado en: (seleccione las que aplican).

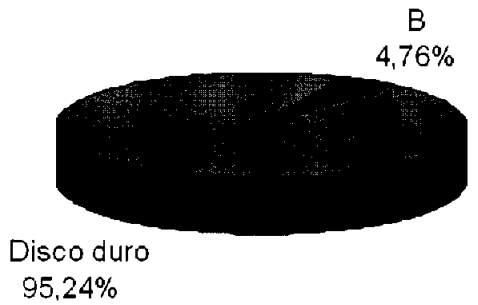


Figura A4.10 Resultados pregunta 3 – sección Manejo de Certificados Digitales

4. ¿Ha permitido que otra persona tenga acceso a su certificado digital?

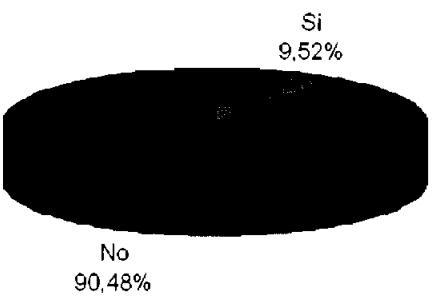


Figura A4.11 Resultados pregunta 4 – sección Manejo de Certificados Digitales

SECCIÓN III: CUMPLIMIENTO DE POLÍTICAS

1. ¿Se han establecido normas y políticas de seguridad para el manejo de los números de referencia y certificados digitales por parte de su institución?

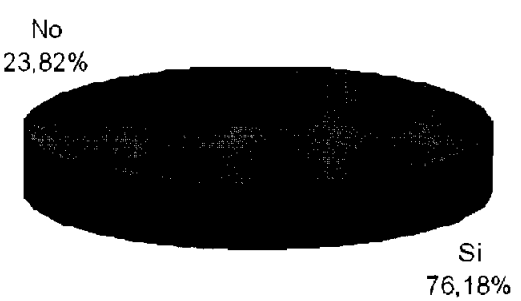


Figura A4.12 Resultados pregunta 1 – sección Cumplimiento de Políticas

a. Si la respuesta es Si:

i. ¿Se dio una explicación del por qué de estas normas y políticas?

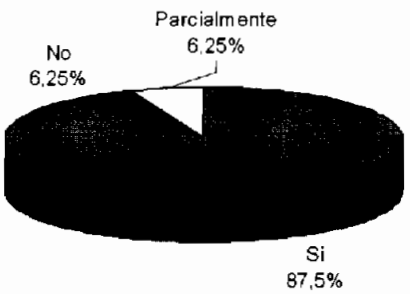


Figura A4.13 Resultados pregunta 1.1 – sección Cumplimiento de Políticas

ii. ¿Se han cumplido estas normas y políticas?

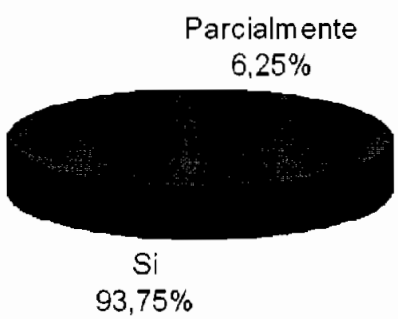


Figura A4.14 Resultados pregunta 1.2 – sección Cumplimiento de Políticas

SECCIÓN I V: SOPORTE TÉCNICO

Sigla	Significado
NS	No sabe

Tabla A4.13 Siglas para la tabulación de las encuestas realizadas a los usuarios de los certificados de las instituciones que forman parte del SNP – sección Soporte Técnico

1. ¿Ha utilizado el soporte técnico brindado por la PKI del BCE?

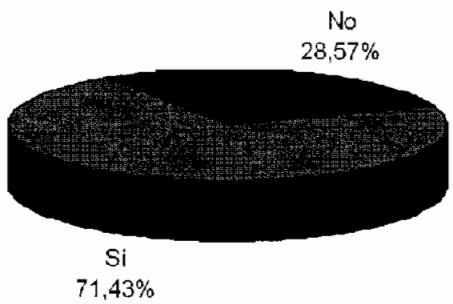


Figura A4.15 Resultados pregunta 1 – sección Soporte Técnico

a. Si la respuesta es si:

i. ¿Sabe Ud. cuál es la disponibilidad del Soporte Técnico?:

Figura A4.16 Resultados pregunta 1.1 – sección Soporte Técnico

ii. La asistencia se realiza:

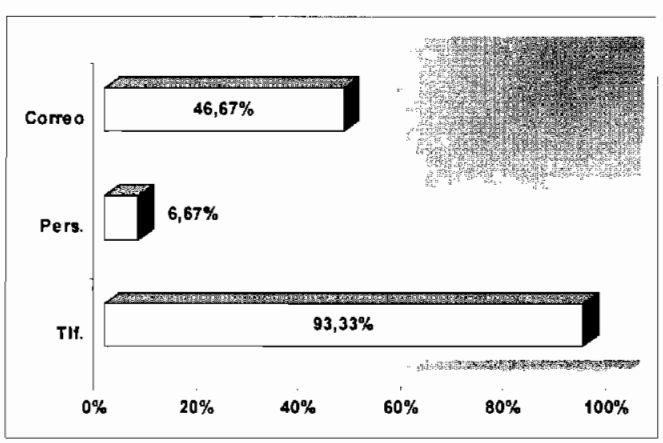
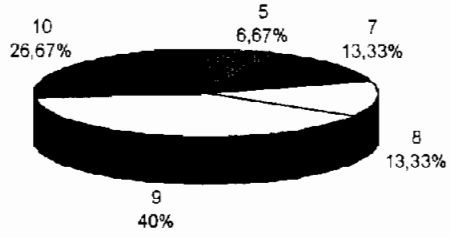


Figura A4.17 Resultados pregunta 1.2 – sección Soporte Técnico

iii. En una escala de 1 a 10, siendo 10 el mayor nivel de calidad del soporte técnico y 1 el menor. ¿Qué puntuación daría usted al soporte técnico brindado por los administradores de la PKI del BCE?



Menor:	5
Mayor:	10
Moda:	9
Promedio:	8,6

Figura A4.18 Resultados pregunta 1.3 – sección Soporte Técnico

Las puntuaciones con los valores: 1, 2, 3, 4 y 6 no se muestran en el gráfico por tener un valor del cero por ciento (0%).

Anexo 5

Política de Certificación

A.5. POLÍTICA DE CERTIFICACIÓN

Autoridades Certificadoras *Wireless*

ACSW

Política de Certificación para Certificados de Entidades Subordinadas y Usuarios Finales de ACSW

CP-ACSW	
Fecha: 27/06/2006	Versión: 1.0
Estado: APROBADO	Nº de páginas:
OID: 1.3.6.1.4.1.311.21.8.**0.0.0.2.1.0.**1.402	CLASIFICACIÓN: RESTRINGIDO
Archivo: cp-acsw.v1.0.pdf	
Preparado por: ACSW	

Tabla A5.1 Información CP

ÍNDICE

1. INTRODUCCIÓN

1.1. RESUMEN

La PKI-ACSW se encuentra en funcionamiento desde el 27 de Junio de 2006, de acuerdo a lo dispuesto en el Documento Nº ACSW-999, emitido el 1 de Junio de 2006[1] por la empresa ACSW, en el cual se autoriza su funcionamiento para la emisión de certificados digitales para la autenticación.

El presente documento contiene la Política de Certificación o CP de la PKI-ACSW; esta CP es el marco de referencia para el funcionamiento y la interacción de todas las ACs y entidades que forman parte de la PKI.

Esta CP se utilizará para la emisión de certificados reconocidos por ACSW y sus miembros, los certificados relacionados con esta CP son expedidos para ACs subordinadas a la AC-RAÍZ, y para los certificados que las ACs subordinadas a su vez emitan para asegurar las comunicaciones dentro de la WLAN de ACSW.

La CP está basada en el RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*", emitido por la IETF para el desarrollo de CPs y CPSs. Todos los términos especificados en el RFC que no se aplican a la estructura de la PKI han sido omitidos.

La CPS relacionada con esta CP es la Declaración de Prácticas de Certificación para Certificados de Entidades Subordinadas y Usuarios Finales de ACSW, los documentos que contienen la CP y CPS son complementarios.

[1] Estas fechas al igual que todos los nombres de organizaciones o eventos citados a lo largo de este documento son ficticios, son mencionados como una guía para el desarrollo de la CP, no hacen referencia a eventos o entidades reales.

1.2. IDENTIFICACIÓN DE LA CP

CP-ACSW	
Nombre de la CP	Política de Certificación para Certificados de Entidades Subordinadas y Usuarios Finales de ACSW
Calificador de la CP	Certificado reconocido dentro de ACSW para la emisión de certificados digitales de entidades subordinadas a la AC-RAÍZ y usuarios finales dentro de la PKI-ACSW.
Versión	1.0
Estado	Aprobado
OID	1.3.6.1.4.1.311.21.8.**0.0.0.2.1.0**.1.402[1]
Fecha de Expedición	27 de Junio de 2006
Fecha de Expiración	27 de Junio de 2011
CPS relacionada	Declaración de Practicas de Certificación para Certificados de Entidades Subordinadas y Usuarios Finales de ACSW. Versión 1.0. OID: 1.3.6.1.4.1.311.21.8.**0.0.0.3.1.0**.1.402[2]
Ubicación	Esta CP se encuentra almacenada en: http://acsw.com

Tabla A5.2 Identificación CP

1.3. COMUNIDAD Y APLICABILIDAD

Esta sección hace referencia a todas las entidades relacionadas con la AC-RAÍZ y sus ACs subordinadas dentro de la PKI-ACSW.

1.3.1. AUTORIDADES DE CERTIFICACIÓN

La autoridad certificadora raíz encargada de emitir certificados bajo está CP es la AC-RAÍZ de la PKI-ACSW, ésta está destinada a emitir certificados para ACs subordinadas dentro de la PKI empresarial. El certificado relacionado con la AC-RAÍZ es valido desde el 27 de Junio de 2006 hasta el 27 de Junio de 2016.

En este documento se denominará AC-SUB a toda AC que haya solicitado un certificado a la AC-RAÍZ de la PKI-ACSW, una AC-SUB está destinadas a emitir certificados para entidades destino dentro de la PKI empresarial. El certificado relacionado con cada AC-SUB es valido desde el 27 de Junio de 2006 hasta el 27 de Junio de 2008.

1.3.2. AUTORIDADES DE REGISTRO

La autoridad de registro encargada de la identificación de una AC-SUB bajo está CP está representada por el Administrador del departamento de IT[3] de la empresa ACSW, en conjunto con el servidor que realiza las funciones de controlador de dominio.

---

[1] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.0.0.0.**cp-acsw.v1.0**.assurance.high.*
[2] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.0.0.0.**cps-acsw.v1.0**.assurance.high.*
[3] *Information technology.*

Por otro lado, la autoridad de registro encargada de la identificación de usuarios finales bajo está CP está representada por personal del Departamento de Recursos Humanos y el Administrador de AC de cada sucursal de la empresa ACSW, en conjunto con el servidor que realiza las funciones de controlador de dominio.

1.3.3. USUARIOS FINALES

1.3.3.1. Entidad Destino

Puede considerarse como una entidad destino relacionada directamente con la AC-RAÍZ a cualquier AC subordinada debidamente registrada. Además, se considera como una entidad destino relacionada directamente con una AC-SUB a cualquier usuario que requiera de un certificado para autenticarse dentro de la WLAN por medio del protocolo EAP-TLS.

1.3.3.2. Entidad Confiante

Se limita el derecho de confiar en los certificados emitidos por la AC-RAÍZ o una AC-SUB, de acuerdo a la presente política a las entidades que requieran verificar la identidad de otra entidad durante el proceso de autenticación dentro de la red.

1.4. USO DE LOS CERTIFICADOS

1.4.1. USOS PERMITIDOS

Los certificados emitidos por la AC-RAÍZ de la PKI-ACSW bajo esta CP, pueden utilizarse para la emisión de certificados digitales de usuarios finales de ACSW. Los certificados emitidos por una AC-SUB de la PKI-ACSW bajo esta CPS, pueden utilizarse para el intercambio de claves simétricas, con el fin de asegurar las comunicaciones dentro de la WLAN de ACSW.

1.4.2. USOS PROHIBIDOS

Los certificados pueden ser utilizados únicamente dentro del ámbito establecido en el literal anterior, todos los usos diferentes a éste quedan prohibidos.

1.5. POLÍTICA DE ADMINISTRACIÓN DE LA PKI-ACSW

1.5.1. ESPECIFICACIÓN DE ACSW

Especificaciones de ACSW	
Nombre:	Autoridades Certificadoras *Wireless*-ACSW
e-mail:	acsw@acsw.com.ec
Dirección:	Isla Fernandina N42-45
Teléfono:	593-2-2257089

Tabla A5.3 Especificaciones de ACSW

1.5.2. PERSONA DE CONTACTO

Especificaciones de Persona de Contacto ACSW	
Nombre:	Administrador de IT - ACSW
e-mail:	admin@acsw.com.ec
Dirección:	Isla Fernandina N42-45
Teléfono:	593-2-2257089 Ext.: 503

Tabla A5.4 Especificaciones Persona de contacto

1.5.3. COMPETENCIA PARA DETERMINAR LA ADECUACIÓN DE LA CPS A LA CP

El departamento de IT de ACSW es el ente encargado de determinar la adecuación de esta CP a su CPS, de acuerdo a lo establecido en el Documento Nº ACSW-999.

1.6. ACRÓNIMOS Y DEFINICIONES

Según lo establecido en la CPS.

2. PUBLICACIÓN DE INFORMACIÓN Y DIRECTORIO

Según lo establecido en la CPS.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. REGISTRO DE NOMBRES

Según lo establecido en la CPS.

3.2. IDENTIFICACIÓN

3.2.1. MÉTODOS DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA

Según lo establecido en la CPS.

3.2.2. IDENTIFICACIÓN DE UNA ENTIDAD

La identificación del servidor de certificados de una AC subordinada estará a cargo del Administrador del departamento de IT de la empresa ACSW, la identificación se llevará a cabo mediante la presentación del código y los datos asignados al equipo.

En cambio, la identificación de la identidad de un usuario final estará a cargo del personal del Departamento de Recursos Humanos de ACSW, la identificación se llevará a cabo mediante la presentación de la Cédula de Ciudadanía y toda la documentación requerida por la empresa ACSW.

3.3. IDENTIFICACIÓN PARA RENOVACIÓN

3.3.1. IDENTIFICACIÓN PARA UNA RENOVACIÓN RUTINARIAS

La renovación del certificado de una AC dentro de la PKI-ACSW se realizará únicamente con el fin de mantener un lapso de sobreposición en el cual el certificado actual y el nuevo sean validos dentro del dominio, esta renovación implicará siempre un cambio de la pareja de claves.

La renovación del certificado de una AC se llevará a cabo 2 meses antes de que su certificado actual pierda validez.

En el caso de una renovación de certificados de entidades destino relacionadas con una AC-SUB, bastará con una actualización de los datos de la entidad destino en caso de que estos hayan cambiado.

3.3.2. IDENTIFICACIÓN PARA UNA RENOVACIÓN DESPUÉS DE UNA REVOCACIÓN – CLAVE NO COMPROMETIDA

La renovación del certificado de la AC-RAÍZ por revocación implicará una revisión del evento que causó el compromiso de la pareja de claves; luego de esto se aplicará los correctivos necesarios.

En el caso de la renovación del certificado de una AC-SUB por revocación, la AR encargada verificará el evento bajo el cual se dio la revocación, luego de lo cual se realizará una actualización de los datos de la AC-SUB en caso de que estos hayan cambiado.

Cuando se trate de una renovación de certificados de usuarios por revocación, la entidad custodia del certificado se presentará personalmente ante la AR correspondiente, para la verificación del evento causante de la revocación, luego de lo cual se realizará una actualización de los datos de la entidad destino en caso de que estos hayan cambiado.

3.4. IDENTIFICACIÓN PARA SOLICITUDES DE REVOCACIÓN

En general, la petición de una revocación de certificado se llevará a cabo por la AR correspondiente o por la entidad destino de manera personal o telefónica; sin embargo, cualquier entidad que forme parte de la PKI-ACSW está obligada a solicitar la revocación de un certificado si tuviera la presunción del compromiso de la clave privada relacionada con éste u otro hecho en particular.

4. EL CICLO DE VIDA DE LOS CERTIFICADOS

Según lo establecido en la CPS.

5. CONTROLES DE SEGURIDAD FÍSICA Y DE GESTIÓN Y OPERACIÓN

Según lo establecido en la CPS.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. GENERACIÓN E INSTALACIÓN DE LA PAREJA DE CLAVES

Las disposiciones determinadas en esta sección de la CP hacen referencia exclusivamente a las claves generadas para la creación de certificados dentro de la PKI-ACSW y bajo esta política.

6.1.1. GENERACIÓN DE LA PAREJA DE CLAVES

Las claves son generadas a partir del modulo RSA provisto por *Windows* para la generación de claves, éste está basado en *software*.

6.1.2. ENTREGA DE LA CLAVE PRIVADA A LA ENTIDAD DESTINO

Las claves son entregadas por medio de paquetes PKCS#12[1], estos paquetes son cifrados y se eliminan del sistema después de la creación del certificado; el certificado creado está ligado a la clave privada.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA A LA AC

La clave es enviada por CMP (*Certificate Management Protocol*), a través de un paquete CMS[2], también se puede utilizar un paquete PKCS #10.

6.1.4. ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LOS USUARIOS

La clave pública se vincula al certificado digital de una AC, éste de distribuye a los usuarios a través de *Active Directory* o por medio del portal http://acsw.com.

6.1.5. TAMAÑO DE LAS CLAVES

El tamaño de las calves para certificados emitidos por la AC-RAÍZ es de 2048 *bits* a excepción de su certificado auto-firmado, éste tiene relacionada una clave con un tamaño de 4096 *bits*. El tamaño de las calves para certificados emitidos por una AC subordinada es de 1024 *bits*.

6.1.6. PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA

Los parámetros seleccionados se basan en las especificaciones ETSI SR 002 176 V1.1.1[3], por lo cual se limita como parámetros validos para la emisión de certificados a los mostrados en la tabla A5.5.

Parámetros para la Emisión de Certificados	
ID	ETSI SR 002 176 V1.1.1: 002
Algoritmo de Firma Digital	RSA
Parámetros Del Algoritmo (longitud de clave/*MinModLen*[4]=1020)	1024 *bits* (mínima)
Algoritmo de Generación de Clave	rsagen1
Método de relleno	EMSA-PASS[5]
Función *hash*	SHA-1

Tabla A5.5 Parámetros para la emisión de certificados

[1] Estándar diseñado por RSA *Laboratories*, define la sintaxis general para mensajes de intercambio de información personal que incluyen elementos criptográficos como: información personal, claves, certificados, extensiones, etc.
[2] *Cryptographic Message Syntax*.
[3] ETSI: *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures*.
[4] Longitud mínima de clave = 1020.
[5] *Encoding Methods for Signatures with Appendix/ Probabilistic Signature Scheme*. Método de codificación para la operación de funciones *hash* desarrollado por RSA.

6.1.7. COMPROBACIÓN DE LA CALIDAD DE LOS PARÁMETROS

Dentro de las especificaciones ETSI SR 002 176 V1.1.1 categoría 002, se define un tamaño mínimo de clave de 1020 bits, esta CP respeta las especificaciones y determina la utilización de claves con una longitud mínima de 1024 *bits*.

6.1.8. *HARDWARE/SOFTWARE* DE GENERACIÓN DE CLAVES

Las claves son generadas bajo el modulo de *software* basado en algoritmos RSA provisto por *Microsoft*.

6.1.9. FINES DEL USO DE LA CLAVE

Las claves relacionadas con los certificados emitidos por una AC serán utilizadas bajo las mismas condiciones de usos permitidos y prohibidos de certificados indicados en el literal 1.4 de esta CP.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA

6.2.1. CONTROL MULTIPERSONA DE LA CLAVE PRIVADA

Las claves privadas deben ser accesadas y utilizadas únicamente por su propietario, éstas serán protegidas con un nivel Alto de seguridad, para esto se establecerá la auto-autenticación de su propietario a través de contraseñas.

6.2.2. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La activación de la clave privada se dará después de la auto-autenticación de su propietario a través de contraseñas.

6.2.3. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Las claves de ACs se desactivarán cuando la AC se encuentre fuera de funcionamiento, las claves de usuarios se desactivarán cuando el usuario suspenda o termine la sesión.

6.3. OTROS ASPECTOS DE LA GESTIÓN DE LA PAREJA DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

Según lo establecido en la CPS.

6.3.2. PERIODO DE USO PARA LAS CLAVES PÚBLICAS Y PRIVADAS

Esta CP determina que el certificado de una AC subordinada y la pareja de claves relacionadas con éste, tendrá una duración de 2 años a partir de su emisión; en el caso de la AC-RAÍZ, sus claves tendrán una duración de 10 años a partir de su emisión.

En el caso de certificados de usurario, esta CP determina que el certificado de una entidad destino y la pareja de claves relacionadas con éste, tendrá una duración de 1 año a partir de su emisión.

6.4. DATOS DE ACTIVACIÓN

Esta sección es aplicable solo a certificados emitidos por AC-SUBs para usuarios dentro de la red ACSW.

6.4.1. GENERACIÓN Y ACTIVACIÓN DE LOS DATOS DE ACTIVACIÓN

El usuario que ingrese al sistema por primera vez, deberá cambiar obligatoriamente la contraseña proporcionada por el Administrador de AC cuando inicie una sesión.

6.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

El propietario del certificado es responsable de guardar la reserva de la contraseña que protege su clave privada.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

Según lo establecido en la CPS.

7. PERFILES DE CERTIFICADOS Y CRLs

7.1. PERFIL DE CERTIFICADO

7.1.1. NÚMERO DE VERSIÓN

Esta CP define la expedición de dos tipos de certificado, los dos cumplen con el estándar X.509v3; el primero está destinado a la firma y emisión de certificados de ACs. El

segundo está destinado al intercambio de claves simétricas para asegurar las comunicaciones dentro de una WLAN.

7.1.2. EXTENSIONES DEL CERTIFICADO

Se utiliza las siguientes extensiones:

- [PolicyExtension]: Lista las políticas definidas por el usuario.
- [AuthorityInformationAccess].- Especifica los puntos de acceso de la información de la AC.
- [CRLDistributionPoint].- Indica los puntos de distribución de CRLs.
- [BasicConstraintsExtension]: Restricción de Ruta del Certificado.

7.1.3. IDENTIFICADOR DE OBJETO (OID) DE LOS ALGORITMOS

El identificador del algoritmo para la generación de certificados es:

SHA1withRSAEncryption = 1.2.840.113549.1.1.5[1].

7.1.4. FORMATOS DE NOMBRES

Los certificados contienen el nombre distinguido del emisor y propietario en los capos Emitido por y Enviado a, respectivamente. En el caso de los certificados de AC, el campo CN del emisor y propietario debe mantener mayúsculas en su totalidad.

7.1.5. RESTRICCIONES DE LOS NOMBRES

Se restringen todos los nombres que no concuerden con los establecidos en el literal anterior.

7.1.6. IDENTIFICADOR DE OBJETO (OID) DE LA POLÍTICA DE CERTIFICACIÓN

El OID para identificar la presente CP es el siguiente:

1.3.6.1.4.1.311.21.8.**0.0.0.2.1.0.**1.402[2]

---

[1] *iso.member.usa.rsadsi.pkcs.pkcs-1.*
[2] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.0.0.0.**cp-acsw.v1.0**.assurance.high.*

7.2. PERFIL DE CRL

7.2.1. NÚMERO DE VERSIÓN

El formato de CRLs utilizado dentro de la PKI-ACSW está definido por la versión 2 establecida dentro del estándar X.509.

7.2.2. CRL Y EXTENSIONES

Se utiliza CRLs establecidas en el estándar X.509.

8. AUDITORÍA DE CONFORMIDAD

Según lo establecido en la CPS.

9. REQUISITOS COMERCIALES Y LEGALES

Según lo establecido en la CPS.

Anexo 6

Declaración de Prácticas de Certificación

A.6. DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

Autoridades Certificadoras *Wireless*

ACSW

Declaración de Prácticas de Certificación para Certificados de Entidades Subordinadas y Usuarios Finales de ACSW

CPS-ACSW	
Fecha: 27/06/2006	Versión: 1.0
Estado: APROBADO	Nº de páginas:
OID: 1.3.6.1.4.1.311.21.8.**0.0.0.3.1.0.**1.402	CLASIFICACIÓN: RESTRINGIDO
Archivo: cps-acsw.v1.0.pdf	
Preparado por: ACSW	

Tabla A6.1 Información CP

ÍNDICE

1. INTRODUCCIÓN

1.1. RESUMEN

La PKI-ACSW se encuentra en funcionamiento desde el 27 de Junio de 2006, de acuerdo a lo dispuesto en el Documento Nº ACSW-999, emitido el 1 de Junio de 2006[1] por la empresa ACSW, en el cual se autoriza su funcionamiento para la emisión de certificados digitales para la autenticación.

El presente documento contiene la Declaración de Prácticas de Certificación o CPS de la PKI-ACSW; esta CPS contiene todas las normas y condiciones bajo las cuales se brindan los servicios de certificación por parte de la PKI-ACSW, esto hace referencia a todos los procesos involucrados en el ciclo de vida de certificados y claves.

La CPS especifica además las condiciones bajo las cuales se realizarán los procesos de solicitud, registro, expedición, uso, suspensión, reactivación y revocación de los certificados emitidos; contiene también medidas de seguridad requeridas para asegurar la operación de la infraestructura.

Esta CPS está basada en el RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*", emitido por la IETF para el desarrollo de CPs y CPSs. Todos los términos especificados en el RFC que no se aplican a la estructura de la PKI han sido omitidos.

1.2. IDENTIFICACIÓN DE LA CP

CPS-ACSW	
Nombre de la CP	Declaración de Prácticas de Certificación para Certificados de Entidades Subordinadas y Usuarios Finales de ACSW
Versión	1.0
Estado	Aprobado
OID	1.3.6.1.4.1.311.21.8.**0.0.0.3.1.0.**1.402[2]
Fecha de Expedición	27 de Junio de 2006
Fecha de Expiración	27 de Junio de 2011
Ubicación	Esta CP se encuentra almacenada en: http://acsw.com

Tabla A6.2 Identificación CPS

[1] Estas fechas al igual que todos los nombres de organizaciones o eventos citados a lo largo de este documento son ficticios, son mencionadas como una guía para el desarrollo de la CPS, no hacen referencia a eventos o entidades reales.

[2] *iso.org.dod.intenet.private.enterprises.microsoft.certsrv.oidenterprisesroot.0.0.0.**cps-acsw.v1.0**.assurance.high.*

1.3. COMUNIDAD Y APLICABILIDAD

Esta sección hace referencia a todas las entidades relacionadas con la AC-RAÍZ y sus ACs subordinadas dentro de la PKI-ACSW.

1.3.1. AUTORIDADES DE CERTIFICACIÓN

La PKI-ACSW está compuesta por una infraestructura jerárquica con dos niveles, las autoridades de certificación que componen PKI-ACSW son:

- **AC-RAÍZ**.- Ésta emite certificados para un nivel inferior de ACs subordinadas y no para entidades destino, esto permite que ésta se mantenga desconectada de la red y almacenada bajo custodia para lograr un alto nivel de seguridad.

  La AC-RAÍZ se encuentra en el primer nivel de la jerarquía; por lo tanto es el ancla de confianza de la Infraestructura. Esta AC emite un certificado auto-firmado para si misma, la clave pública relacionada con este certificado escrita en hexadecimal es:

```
30 82 02 0a 02 82 02 01 00 cd c1 b1 fb 6f 38 d5 7e 4f 27 02 47 6c cd 90 68 25 05 ee
20 1e ab 77 4f 72 e0 00 44 ca 76 cf 9a 30 bc cd 45 d6 2c d3 90 d5 f8 10 ba 9c 1d e2
69 ea 9e da 53 4a e0 ed 81 e5 ab 50 a4 58 40 e9 21 68 ed 01 74 26 a0 b6 5f 1b 67 c0
fe 66 c8 b1 cb a1 08 a9 06 2e fa 8a b7 5c 7e f9 e3 07 53 de e7 8b ee 01 89 73 4c 3f
7b dc fe 9c 16 98 b5 75 d9 79 7d f4 d8 d8 cb 4a 0b d1 f7 d2 0b 6e 65 a3 82 01 6a dc
d2 22 2c f4 1e 69 3d 1c d3 2e 2e 77 dd eb d3 ba 7c 89 03 20 34 9d e1 41 77 58 e6 18
88 60 c0 6a 8e 86 8a 40 1d 91 70 a2 7c e2 9f a0 3d db 83 87 c7 6a c4 5a be 13 d6 64
54 1c ff e4 a6 cc b4 9b ef 6b 04 ae 7c 40 57 37 67 59 1b 2f 50 7d 86 7b 13 82 2d 43
19 17 e0 10 9a 4c bc ff 44 1e 1c 66 f5 11 9b c7 66 0d 4d e0 6e 8e f2 50 b0 12 dd 7e
c4 cc 2b cf f0 07 11 7e 18 12 c0 47 9f 4a 49 21 1a c5 b8 aa ba 66 2f 01 36 05 1d 6d
12 a0 d5 84 cb f0 54 3e df ad fc 3d a2 84 04 bd 82 1a 9b d4 68 5a 77 fc c3 c0 d6 46
df 80 79 43 8b 01 29 31 e5 55 2e ee d5 be c0 c4 02 f0 b7 3f c2 11 1c cd 3e a7 71 8a
7f 68 47 b6 86 5a 8c a3 74 5e db 40 3a 84 41 fe 86 9f 47 68 e0 11 0a 10 d8 5d 17 9f
f6 37 f6 71 90 18 9e 98 04 f0 11 cc 24 ff e8 cf b5 f1 12 b7 57 61 6a 88 d8 bf b7 97
fb 85 85 7e a0 72 1f 5e 0a ed 16 a9 1b b7 fb a8 17 ab 7e 83 b8 f5 29 e2 bc 4a 41 6f
57 1c 16 2e 01 23 d7 d0 1c 5e 77 04 40 a7 d3 56 a8 9d cb 31 69 46 ae e8 19 3e ff 70
53 c9 bd 85 54 f1 79 4e 6c 3f 70 85 40 b1 aa 71 fa 0d 9d 1c 86 c4 85 4f 75 f7 29 da
3c 13 26 bf 82 31 f1 07 7a e6 33 a3 54 03 16 56 81 a6 26 3d d8 1d 3c f0 4c ed c2 f0
         e3 4a 01 c1 60 df fb d3 bf 17 14 2b a8 cc 98 3b cf 02 03 01 00 01
```

  El certificado relacionado con la AC-RAÍZ es valido desde el 27 de Junio de 2006 hasta el 27 de Junio de 2016.

- Una AC subordinada dentro la PKI solo podrá expedir certificados de entidad destino; estos certificados estarán vinculados a claves destinadas para el intercambio de claves simétricas con el fin de lograr comunicaciones seguras dentro de una WLAN. El certificado relacionado con cada AC-SUB es valido desde el 27 de Junio de 2006 hasta el 27 de Junio de 2008.

1.3.2. AUTORIDADES DE REGISTRO

La autoridad de registro encargada de la identificación de una AC-SUB, está representada por el Administrador del departamento de IT[1] de la empresa ACSW, en conjunto con el servidor que realiza las funciones de controlador de dominio.

Por otro lado, la autoridad de registro encargada de la identificación de usuarios finales está representada por personal del Departamento de Recursos Humanos y el Administrador de AC de cada sucursal de la empresa ACSW, en conjunto con el servidor que realiza las funciones de controlador de dominio.

Cualquier autoridad de registro tiene las siguientes obligaciones:

- Realizar la identificación de cualquier entidad que solicite un certificado digital a la PKI-ACSW.
- Verificar la veracidad de la información proporcionada por el solicitante de un certificado.
- Entregar a la AC correspondiente los datos que le permitan emitir un certificado después de la aprobación de una solicitud.

1.3.3. USUARIOS FINALES

1.3.3.1. Solicitante

Es cualquier persona que solicita para si mismo o para otra entidad la emisión de un certificado digital a una AC de la PKI-ACSW.

1.3.3.2. Entidad Destino

La entidad destino está definida por el titular del certificado digital, éste es el custodio de la clave privada ligada a su certificado; queda prohibida la transferencia del certificado a otra entidad.

---

[1] *Information technology.*

Puede considerarse como una entidad destino relacionada directamente con la AC-RAÍZ a cualquier AC subordinada debidamente registrada. Además, se considera como una entidad destino relacionada directamente con una AC-SUB a cualquier usuario que requiera de un certificado para autenticarse dentro de la WLAN por medio del protocolo EAP-TLS.

1.3.3.3. Entidad Confiante

Se limita el derecho de confiar en los certificados emitidos por la AC-RAÍZ o una AC-SUB, de acuerdo a la presente declaración de prácticas de certificación a las entidades que requieran verificar la identidad de otra entidad durante el proceso de autenticación dentro de la red de ACSW.

1.4. USO DE LOS CERTIFICADOS

1.4.1. USOS PERMITIDOS

Los certificados emitidos por la AC-RAÍZ de la PKI-ACSW bajo esta CPS, pueden utilizarse para la emisión de certificados digitales de usuarios finales de ACSW. Los certificados emitidos por una AC-SUB de la PKI-ACSW bajo esta CPS, pueden utilizarse para el intercambio de claves simétricas, con el fin de asegurar las comunicaciones dentro de la WLAN de ACSW.

1.4.2. USOS PROHIBIDOS

Los certificados pueden ser utilizados únicamente dentro del ámbito establecido en el literal anterior, todos los usos diferentes a éste quedan prohibidos.

1.5. POLÍTICA DE ADMINISTRACIÓN

1.5.1. ESPECIFICACIÓN DE ACSW

Especificaciones de ACSW	
Nombre:	Autoridades Certificadoras *Wireless*-ACSW
e-mail:	acsw@acsw.com.ec
Dirección:	Isla Fernandina N42-45
Teléfono:	593-2-2257089

Tabla A6.3 Especificaciones de ACSW

1.5.2. PERSONA DE CONTACTO

Especificaciones de Persona de Contacto ACSW	
Nombre:	Administrador de AC sucursal # - ACSW
e-mail:	admin.ac.suc#@acsw.com.ec
Dirección:	Isla Fernandina N42-45
Teléfono:	593-2-2257089 Ext.: 503

Tabla A6.4 Especificaciones Persona de contacto

1.5.3. COMPETENCIA PARA DETERMINAR LA ADECUACIÓN DE LA CPS A LA CP

El departamento de IT de ACSW es el ente encargado de determinar la adecuación de esta CPS a la CP, de acuerdo al Documento Nº ACSW-999.

1.6. ACRÓNIMOS Y DEFINICIONES

1.6.1. ACRÓNIMOS

- AC.- Autoridad de Certificación.
- AC.- Autoridad de Certificación.
- ACSW.- Autoridades de Certificación *Wireless*.
- AR.- Autoridad de Registro.
- CP.- Política de Certificación (*Certificate Policy*).
- CPS.- Declaración de Prácticas de Certificación (*Certification Practice Statement*).
- CRL.- Lista de Revocación de Certificados (*Certificate Revocation List*).
- EAP-TLS.- *Extensible Authentication Protocol-Transport Layer Security*.
- PKI.- Infraestructura de Claves Públicas (*Public Key Infrastructure*).
- RSA.- Rivest, Shamir, Adelman.
- SHA.- *Secure Hash Algorithm*.
- WLANs.- Redes inalámbricas de área local (*Wireless Local Area Networks*).

1.6.2. DEFINICIONES

- **AC**.- La AC es un tercero de confianza que emite los certificados digitales de manera segura, para esto requiere de la implementación de un servidor de certificados; además, la AC tiene la obligación de administrar los certificados, lo que implica la expedición, suspensión, reactivación y revocación de éstos.
- **AR**.- Entidad encargada de garantizar el servicio de identificación dentro de PKI; es responsable de la interacción entre los usuarios de certificados y la AC; acepta solicitudes de creación de certificados, valida los datos y finalmente envía la información necesaria a la AC.
- **Ancla De Confianza**.- Punto que utiliza un usuario como referente de confianza.
- **Autenticación**.- Es un proceso en el cual una autoridad apoyándose en credenciales o información presentadas por una entidad verifica su identidad; requiere que otra autoridad haya expedido previamente las credenciales presentadas o que la información relacionada con la entidad se encuentre registrada y sea factible su verificación.

- **Certificado Digital**.- Los certificados son credenciales digitales que contienen una clave pública y el nombre de su propietario.
- **CRL**.- Una lista de revocación de certificados contiene información sobre certificados que han dejado de ser validos, ya sea por suspensión o revocación.
- **CPS**.- Define como se va a implementar y dar soporte a las CPs, contiene toda la información de los procedimientos necesarios para la expedición, suspensión, reactivación y revocación de certificados, así como también la forma en que se va a realizar los diferentes procesos dentro de la PKI.
- **Directivas**.- Las directivas son las reglas que rigen una PKI, están compuestas por políticas de certificación y una declaración de prácticas de certificación.
- **Directorios**.- Dentro de una PKI los directorios son la base para el sistema de distribución de certificados y listas de revocación. Dentro de algunas implementaciones los certificados son distribuidos a los usuarios personalmente; en la mayor parte de casos, se los distribuye por medio de directorios.
- **EAP-TLS**.- Protocolo creado por Microsoft, se encuentra registrado en el RFC 2716, provee autenticación con el más alto nivel de seguridad por medio de certificados digitales dentro de WLANs.
- **Ecripción**.- Es la técnica que permite cifrar un mensaje de datos mediante el uso de algoritmos.
- **Entidad Confiante**.- En general, es cualquier entidad que utiliza un certificado digital perteneciente a otra entidad; es decir, ésta valida un certificado para verificar una identidad; cuando el certificado queda validado, la entidad confiante asume la autenticidad de la credencial electrónica.
- **Entidad Destino**.- La entidad destino está representada por el propietario del certificado, éste puede ser una persona, un equipo o cualquier entidad que requiera autenticarse ante un sistema o usuario utilizando certificados digitales.
- **Firma Digital**.- En general, se dice que un usuario firma un mensaje de datos cuando lo cifra con su clave privada.
- **Función *hash***.- Es aquella que toma como entrada un mensaje y entrega como resultado un resumen conocido como valor *hash*, éste identifica de manera única al mensaje.
- **Identificación**.- Es el proceso mediante el cual se establece la identidad de un individuo en particular.
- **Políticas de Certificación (CP)**.- Una política de certificación o CP define pautas para el manejo de la información, procesos y principales usos de las herramientas de criptografía pública dentro de una organización.
- **RSA**.- Algoritmo que permite cifrar mensajes y realizar firmas digitales.

- **SHA-1**.- Algoritmo que toma mensajes con un tamaño menor a 2^{64} bits y entrega un valor *hash* con una longitud de 160 bits.
- **Vulnerabilidad**.- Una vulnerabilidad es una debilidad (interna) de un sistema, se produce por fallas en su diseño, implementación o administración, haciendo que éste sea frágil y se vea expuesto ante amenazas. Cada parte del sistema puede tener sus propias vulnerabilidades.
- **WLAN**.- Las redes inalámbricas de área local cubren áreas pequeñas como oficinas, edificios, bibliotecas, etc., su cobertura está limitada a segmentos locales.

2. PUBLICACIÓN DE INFORMACIÓN Y DIRECTORIO

2.1. DIRECTORIO DE CERTIFICADOS

El servicio de directorio de certificados estará disponible para los usuarios bajo un esquema restringido al horario de oficina extendido (8:00 a 20:00) durante los días laborables, si se presenta una falla en el sistema, el directorio se restaurará en el menor tiempo posible.

La información registrada en el directorio está restringida para el conjunto de miembros de ACSW, y está disponible en el portal: http://acsw.com.

2.2. PUBLICACIÓN

Las ACs pertenecientes a la PKI-ACSW están obligadas a publicar toda la información relacionada con: CP y CPS, certificados, CRLs completas y deltas. La información publicada por una AC tiene el carácter de restringida y está disponible para los usuarios en el portal: http://acsw.com.

Además, los certificados digitales y las CRLs son publicados en el directorio de *Active Directory* de manera automática después de su emisión.

2.3. ACTUALIZACIONES

La CP y CPS (v1.0) tienen una vida útil de 5 años a partir del 27 de Junio de 2006; cumplido este periodo se realizará una revisión de su estructura, con el fin de adaptarlas al entorno existente en ese momento. Cundo una CP o CPS ha caducado, se incrementará la fracción entera de su versión a su inmediato superior (v2.0).

Sin embargo, si durante la vida útil de una CP o CPS se requiere de una actualización, ésta será publicada incrementando la fracción decimal de su versión al inmediato superior (v1.1). Cada vez que se realice modificaciones en la estructura de una CP o CPS, éstas se publicarán de manera inmediata.

Las CRLs emitidas por la AC-RAÍZ serán publicadas normalmente cada año y las CRLs delta se publicarán cada cuatro semanas; sin embargo, el compromiso de la clave privada de una AC-SUB causará la publicación inmediata de una CRL completa. Se realizaran publicaciones de las CRLs emitidas por una AC-SUB, cada cuatro semanas y las CRLs delta serán publicadas cada semana.

2.4. CONTROL DE ACCESO

Se permite el acceso de lectura y examen de directorios para toda la información del directorio http://acsw.com de la PKI-ACSW. Sólo el Administrador de Dominio está autorizado a modificar, sustituir o eliminar información de este directorio.

El directorio relacionado con Active Directory está restringido a la administración del grupo de Administradores del departamento de IT de ACSW.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. REGISTRO DE NOMBRES

Todas las entidades finales requieren un nombre distintivo basado en el estándar X.500, éste se incluye en el campo CN (*Common Name*) y corresponde con el nombre registrado en el servidor de dominio.

3.1.1. TIPOS

Se aceptan los nombres de directorio (*DirectoryName*) y UPN (*User Principal Name*). Los nombres registrados en los certificados deben tener sentido.

3.1.2. UNICIDAD

Los nombres registrados en los certificados deben ser únicos, evitando cualquier ambigüedad.

3.2. IDENTIFICACIÓN

3.2.1. MÉTODOS DE PRUEBA DE POSESIÓN DE LA CLAVE PRIVADA

Cuando la pareja de claves se genera en el equipo de la entidad destino, el paquete enviado por *Windows* como solicitud se firma con la clave privada relacionada con la clave pública. Este proceso está a cargo del sistema *CriptoAPI* que genera la pareja de claves y no del usuario.

3.2.2. IDENTIFICACIÓN DE UNA ENTIDAD

La identificación del servidor de certificados de una AC subordinada estará a cargo del Administrador del departamento de IT de la empresa ACSW, la identificación se llevará a cabo mediante la presentación del código y los datos asignados al equipo.

En cambio, la identificación de la identidad de un usuario solicitante estará a cargo del personal del Departamento de Recursos Humanos de ACSW, la identificación se llevará a cabo mediante la presentación de la Cédula de Ciudadanía y toda la documentación requerida por la empresa ACSW.

3.3. IDENTIFICACIÓN PARA RENOVACIÓN

3.3.1. IDENTIFICACIÓN PARA UNA RENOVACIÓN RUTINARIA

La renovación del certificado de una AC dentro de la PKI-ACSW se realizará únicamente con el fin de mantener un lapso de sobreposición en el cual el certificado actual y el nuevo sean validos dentro del dominio, esta renovación implicará siempre un cambio de la pareja de claves.

La renovación del certificado de una AC se llevará a cabo 2 meses antes de que su certificado actual pierda validez. En el caso de una renovación de certificados de entidades destino relacionadas con una AC-SUB, bastará con una actualización de los datos de la entidad destino en caso de que estos hayan cambiado.

3.3.2. IDENTIFICACIÓN PARA UNA RENOVACIÓN DESPUÉS DE UNA REVOCACIÓN – CLAVE NO COMPROMETIDA

En el caso de la renovación del certificado de una AC-SUB por revocación, la AR encargada verificará el evento bajo el cual se dio la revocación, luego de lo cual se realizará una actualización de los datos de la AC-SUB en caso de que estos hayan cambiado.

Cuando se trate de una renovación de certificados de usuarios por revocación, la entidad custodia del certificado se presentará personalmente ante la AR correspondiente, para la verificación del evento causante de la revocación, luego de lo cual se realizará una actualización de los datos de la entidad destino en caso de que estos hayan cambiado.

3.4. IDENTIFICACIÓN PARA SOLICITUDES DE REVOCACIÓN

En general, la petición de una revocación de certificado se llevará a cabo por la AR correspondiente o por la entidad destino de manera personal o telefónica; sin embargo, cualquier entidad que forme parte de la PKI-ACSW está obligada a solicitar la revocación de un certificado si tuviera la presunción del compromiso de la clave privada relacionada con éste u otro hecho en particular.

4. CICLO DE VIDA DE LOS CERTIFICADOS

4.1. SOLICITUD DE CERTIFICADOS

Un equipo de ACSW que esté destinado a funcionar como servidor de certificados dentro de la red ACSW, será habilitado después de la presentación de una solicitud por parte del administrador de AC de cada sucursal, esta solicitud será validada por la AR correspondiente.

Un empleado de ACSW que requiera autenticarse ante la red ACSW por medios inalámbricos, deberá presentar la solicitud de certificado utilizando el formulario ACSW-1 (Anexo 1 de esta CPS) a la AR correspondiente.

La AR está encargada de la identificación del usuario solicitante; además, debe verificar los datos contenidos en el formulario y la firma registrada por parte del usuario en el contrato provisto en el Anexo 2 de esta CPS.

4.2. TRAMITACIÓN DE LA SOLICITUD DE CERTIFICADOS

Cuando el proceso de registro ha terminado exitosamente, la AR notifica a la AC que el proceso de registro ha concluido exitosamente. En caso de que durante el proceso de registro de usuarios se halle irregularidades, la solicitud será negada.

4.3. EMISIÓN DE CERTIFICADOS

La emisión del certificado de una AC-SUB se realizará de acuerdo a eventos planificados; durante estos eventos la AC-RAÍZ será conectada a la red y recibirá las solicitudes correspondientes de manera manual. El servidor de certificados de la AC-RAÍZ marcará como pendiente cualquier otra solicitud.

En el caso de los usuarios finales, cuando la AR notifica a la AC la identificación exitosa de una entidad, la emisión de certificados se realiza después del registro de los datos del usuario en el servidor de dominio. La AC subordinada recibirá las solicitudes y emitirá certificados de forma automática cuando la información registrada concuerde con la solicitud recibida.

4.4. ENTREGA DE CERTIFICADOS

Un certificado será entregado automáticamente desde el servidor de certificados al equipo destinado a almacenar dicho certificado.

4.5. USO DE LA PAREJA DE CLAVES Y DEL CERTIFICADO

Las parejas de claves deben ser utilizadas de acuerdo a las restricciones impuestas en la sección 1.4 de esta CPS para el uso de certificados.

4.6. RENOVACIÓN DE CERTIFICADOS

La renovación del certificado de una AC dentro de la PKI-ACSW se realizará únicamente con el fin de mantener un lapso de sobreposición en el cual el certificado actual y el nuevo sean validos dentro del dominio, esta renovación implicará siempre un cambio de la pareja de claves.

La renovación del certificado de una AC se llevará a cabo 2 meses antes de que su certificado actual pierda validez.

En el caso de una renovación de certificados de entidades destino relacionadas con una AC-SUB, bastará con una actualización de los datos de la entidad destino en caso de que estos hayan cambiado.

4.7. RENOVACIÓN DE CLAVES

Las claves serán renovadas bajo las mismas condiciones y durante el mismo proceso de la renovación del certificado.

4.8. REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS

4.8.1. CIRCUNSTANCIAS PARA LA REVOCACIÓN

La revocación de un certificado es definitiva; es decir, éste queda inhabilitado hasta que termine su periodo de validez. Una revocación se puede presentar por las siguientes razones:

- Compromiso de la Clave Privada relacionada con el propietario del certificado.
- Compromiso de la Clave Privada relacionada con el certificado de la AC que emitió el certificado.
- El certificado ha sido actualizado por otro.
- El usuario deja de pertenecer la Sistema que requiere del uso de un certificado para la autenticación; esto se puede dar por cambio de funciones o desvinculación entre la empresa y el usuario.
- Irregularidades encontradas en la información presentada por el usuario final a la AR.

4.8.2. ENTIDAD QUE PUEDE SOLICITAR LA REVOCACIÓN

En general, la petición de una revocación de certificado se llevará a cabo por la AR correspondiente o por la entidad destino de manera personal o telefónica; sin embargo, cualquier entidad que forme parte de la PKI-ACSW está obligada a solicitar la revocación de un certificado si tuviera la presunción del compromiso de la clave privada relacionada con éste u otro hecho en particular.

4.8.3. PROCEDIMIENTO DE SOLICITUD DE REVOCACIÓN

La AC-RAÍZ acepta solicitudes de revocación realizadas por el Administrador de AC de cualquier sucursal de ACSW, estas solicitudes pueden realizarse de manera personal o telefónicamente. El Administrador de la AC-RAÍZ revocará el certificado y publicará la CRL correspondiente inmediatamente.

La AR encargada verificará el evento causante de la revocación, luego de lo cual se realizará una evaluación para corregir las vulnerabilidades causantes del compromiso.

Una AC-SUB acepta solicitudes de revocación realizadas por el propietario del certificado, la AR correspondiente o cualquier miembro de ACSW, estas solicitudes pueden realizarse de manera personal o telefónicamente.

4.8.4. TIEMPO DE ESPERA DESPUÉS DE UNA SOLICITUD DE REVOCACIÓN

Cuando una solicitud se realice personalmente por el propietario de certificado o la AR, la revocación se realizará inmediatamente.

En caso de los certificados de usuario, si la solicitud se realiza telefónicamente o por un tercero, el Administrador de la AC suspenderá el certificado hasta verificar las condiciones que causaron el compromiso; sí el evento lo amerita, procederá a la revocación del certificado involucrado y la publicación de la CRL.

4.8.5. CIRCUNSTANCIAS PARA LA SUSPENSIÓN

La suspensión para el certificado de la AC-Raíz no está permitida.
La suspensión se puede declarar únicamente por la AC que emitió el certificado, en el caso del certificado de una AC-SUB, ésta se dará cuando el Administrador de AC o una entidad equivalente comuniquen un evento planificado de mantenimiento de *software* o *hardware* que lo amerite o en caso de problemas técnicos.

La suspensión de un certificado emitido por una AC-SUB se dará cuando su propietario o la AR correspondiente notifiquen la ausencia temporal del propietario dentro de la empresa; durante el periodo de suspensión del certificado, el equipo que almacena el certificado será colocado bajo custodia.

4.8.6. ENTIDAD QUE PUEDE SOLICITAR LA SUSPENSIÓN

La suspensión de un certificado se puede solicitar por su propietario o por la AR correspondiente.

4.8.7. PROCEDIMIENTO PARA LA SOLICITUD DE SUSPENSIÓN

La entidad que requiera la suspensión de un certificado debe solicitarla al Administrador del departamento de IT en el caso del certificado de una AC-SUB; cuando se requiera la suspensión de un certificado de usuario final, la solicitud será presentada al Administrador de AC de la sucursal correspondiente.

4.8.8. LÍMITES DEL PERÍODO DE SUSPENSIÓN

Los límites se determinarán de acuerdo al evento que motivó la suspensión.

4.8.9. EMISIÓN DE CRLs

Las CRLs emitidas por la AC-RAÍZ serán publicadas normalmente cada año y las CRLs delta se publicarán cada cuatro semanas; sin embargo, el compromiso de la clave privada de una AC-SUB causará la publicación inmediata de una CRL completa. Se realizaran publicaciones de las CRLs emitidas por una AC-SUB, cada cuatro semanas y las CRLs delta serán publicadas cada semana.

4.9. SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS

Las CRLs publicadas por las ACs de la PKI-ACSW estarán disponibles para la verificación del estado de un certificado bajo un esquema restringido al horario de oficina extendido (8:00 a 20:00) durante los días laborables.

4.10. REACTIVACIÓN

La reactivación se llevará acabo cuando haya concluido el evento que motivó la suspensión del certificado.

5. CONTROLES DE: SEGURIDAD FÍSICA, GESTIÓN Y OPERACIÓN

5.1. CONTROLES DE SEGURIDAD FÍSICA

5.1.1. UBICACIÓN Y CONSTRUCCIÓN

El servidor de la AC-RAÍZ se encuentra bajo custodia en la bóveda de la empresa. Los servidores de certificados de las ACs subordinadas se ubican en el Centro de Seguridad Informática de cada sucursal de ACSW; la construcción de estos locales se ha realizado guardando niveles adecuados solidez en la cimentación. Adicionalmente se mantiene un régimen de vigilancia 24x7.

5.1.2. ACCESO FÍSICO

El servidor de la AC-RAÍZ se encuentra bajo custodia en la bóveda de la empresa; por lo tanto, solo está disponible durante eventos planificados.

La red de cada sucursal está dividida en diferentes perímetros de seguridad; cada perímetro mantiene niveles razonables de seguridad de acuerdo a sus características y requerimientos.

El servidor de certificados de una AC-SUB, está ubicado en el perímetro con mayor nivel de seguridad, para acceder a éste se requiere de una autenticación biométrica acompañada de una contraseña, solo los administradores poseen un perfil válido.

5.1.3. ALIMENTACIÓN ELÉCTRICA Y AIRE ACONDICIONADO

La instalación de los sistemas de alimentación está diseñada para brindar servicio de manera ininterrumpida, en caso de presentarse problemas en el sistema principal de alimentación, se activa un UPS[1] independiente, éste puede mantenerse en funcionamiento por un período de aproximadamente 2 horas. Además del UPS, se dispone de un sistema de puesta a tierra para proteger los equipos frente a fluctuaciones de eléctricas.

El sistema de de ventilación tiene la capacidad de suministrar niveles de temperatura y humedad óptimos para la operación de los sistemas.

5.1.4. EXPOSICIÓN AL AGUA

Los Centros de Seguridad Informática están dotados de detectores de inundación, si éstos detectan anomalías en el medio, activan una alarma.

5.1.5. PROTECCIÓN Y PREVENCIÓN DE INCENDIOS

Todos los Centros de Seguridad Informática están dotados de armarios ignífugos y un sistema a prueba de incendios; de presentarse un siniestro, el sistema activa una alarma.

5.1.6. *BACKUP*

El respaldo de la base de datos de la AC-RAÍZ se realiza después de cada evento planificado; las bases de datos de las ACs subordinadas son respaldadas una vez por semana, este procedimiento está a cargo del Administrador de AC de cada sucursal.

---

[1] *Uninterrupted Power Supply.*

5.2. CONTROLES DE PROCEDIMIENTOS

Para proteger la operación de los sistemas de la PKI-ACSW, la información relacionada con los controles de procedimiento se mantiene bajo estricta confidencialidad, esta sección presenta un esquema elemental de la solución empleada.

5.2.1. PAPELES DE CONFIANZA

Se tiene definidos dos tipos de roles para el control y la gestión de los servicios de certificación, estos son: Administrador de IT y Administrador de AC.

- **Administrador del Departamento de IT**.- Es el encargado de la operación de la AC-RAÍZ, esto implica la planificación de eventos de emisión de certificados y CRLs para las ACs subordinadas; también se encarga de respaldar la base de datos de la AC-RAÍZ.
- **Administrador de AC**.- Está encargado de la operación de la AC-SUB de una sucursal, hace las funciones de solicitante ante el Administrador de IT cuando se requiere la generación de un certificado para la AC-SUB a su cargo.
  Por otro lado, realiza parte de las funciones de registro de los usuarios finales. También se encarga de la emisión de certificados y CRLs, manteniendo los respaldos de la base de datos y claves de la AC-SUB.
  Se encarga de realizar las auditorías internas, debe verificar la disponibilidad de la información y la correspondencia entre ésta y los procedimientos empleados.

5.3. CONTROLES DE SEGURIDAD DE PERSONAL

El personal encargado del desempeño de los roles expuestos en el literal anterior debe contar con el conocimiento y la experiencia adecuados para realizar sus funciones; esto implica un dominio sobre todos los temas relacionados con los servicios de certificación y sus implicaciones legales.

Además, todo miembro del equipo de Administradores debe actualizar sus conocimientos de manera periódica, con el fin de brindar un soporte seguro y confiable. Si se llega a introducir un cambio tecnológico, el personal será capacitado con suficiente anterioridad.

Para verificar el cumplimento de la CP y CPS, se efectuará un control periódico, si se detecta irregularidades causadas por un desempeño negligente o malintencionado, se suspenderá el

acceso a las instalaciones del o los involucrados de manera inmediata. El departamento jurídico de la empresa ACSW tomará las acciones pertinentes.

5.4. RECUPERACIÓN EN CASO DE COMPROMISO DE UNA CLAVE O DE DESASTRE

5.4.1. ALTERACIÓN DE LOS RECURSOS *HARDWARE*, *SOFTWARE* Y/O DATOS

En caso de percibir comportamientos anómalos del *software* o *hardware* que solventan el funcionamiento de la PKI, se respaldará la base de datos y las claves de la AC afectada. Cuando todos los respaldos estén protegidos, se realizará una inspección para localizar la falla y corregirla. Si luego de las reparaciones se considera necesaria la reinstalación de la AC, se procederá de inmediato.

5.4.2. LA CLAVE PÚBLICA DE UNA ENTIDAD SE REVOCA

Si se llega a revocar un certificado de AC, se generará y publicará la CRL correspondiente, luego se detendrá la ejecución de la AC y se procederá a la instalación de una nueva AC relacionada con una pareja de claves diferente, de ser necesario el nombre de AC comprometida puede ser reutilizado.

Las CRLs publicadas por la AC eliminada permanecerán en el directorio hasta que todos los certificados registrados en éstas hayan cumplido su período de validez, luego de esto serán retiradas del directorio.

5.4.3. LA CLAVE DE UNA ENTIDAD SE COMPROMETE

Si se compromete la clave privada de una AC, se realizará el proceso indicado en el literal anterior; luego de lo cual se informará a todas las entidades relacionadas con la PKI-ACSW. Todos los certificados emitidos por la AC o sus subordinadas serán revocados antes de revocar el certificado de la AC, la AR correspondiente es la responsable de notificar a todos los usuarios afectados.

5.5. CESE DE UNA AC

Una AC puede cesar en funciones por los siguientes motivos:

- Compromiso de su clave privada.

- Cese de la PKI-ACSW, por decisión de sus autoridades.

El cese de funciones de una AC se será comunicado previamente a todos los afectados, luego de lo cual se revocará todos los certificados emitidos por ésta. Toda la información relacionada con la AC o los certificados emitidos por ésta serán almacenados bajo custodia, garantizando el derecho a la intimidad de los usuarios involucrados.

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. GENERACIÓN E INSTALACIÓN DE LA PAREJA DE CLAVES

Las disposiciones determinadas en esta sección hacen referencia exclusivamente a las claves generadas para la creación de certificados dentro de la PKI-ACSW y bajo la CP relacionada con esta CPS.

6.1.1. GENERACIÓN DE LA PAREJA DE CLAVES

Las claves son generadas a partir del modulo RSA provisto por *Windows* para la generación de claves, éste está basado en *software*.

6.1.2. ENTREGA DE LA CLAVE PRIVADA A LA ENTIDAD DESTINO

Las claves son entregadas por medio de paquetes PKCS#12[1], estos paquetes son cifrados y se eliminan del sistema después de la creación del certificado; el certificado creado está ligado a la clave privada.

6.1.3. ENTREGA DE LA CLAVE PÚBLICA A LA AC

La clave pública es enviada por CMP (*Certificate Management protocol*), a través de un paquete CMS[2], también se puede utilizar un paquete PKCS #10.

6.1.4. ENTREGA DE LA CLAVE PÚBLICA DE LA AC A LOS USUARIOS

La clave pública se vincula al certificado digital de la AC, éste de distribuye a los usuarios a través de *Active Directory* o por medio del portal http://acsw.com.

---

[1] Estándar diseñado por RSA *Laboratories*, define la sintaxis general para mensajes de intercambio de información personal que incluyen elementos criptográficos como: información personal, claves, certificados, extensiones, etc.
[2] *Cryptographic Message Syntax*.

6.1.5. TAMAÑO DE LAS CLAVES

El tamaño de las claves para certificados emitidos por la AC-RAÍZ es de 2048 *bits* a excepción de su certificado auto-firmado, éste tiene relacionada una clave con un tamaño de 4096 *bits*. El tamaño de las calves para certificados emitidos por una AC subordinada es de 1024 *bits*.

6.1.6. PARÁMETROS DE GENERACIÓN DE LA CLAVE PÚBLICA

Los parámetros seleccionados se basan en las especificaciones ETSI SR 002 176 V1.1.1[1], por lo cual se limita como parámetros validos para la emisión de certificados a los mostrados en la tabla A6.5.

Parámetros para la Emisión de Certificados	
ID	ETSI SR 002 176 V1.1.1: 002
Algoritmo de Firma Digital	RSA
Parámetros Del Algoritmo (longitud de clave/*MinModLen*[2]=1020)	1024 bits
Algoritmo de Generación de Clave	rsagen1
Método de relleno	EMSA-PASS[3]
Función *hash*	SHA-1

Tabla A6.5 Parámetros para la emisión de certificados

6.1.7. COMPROBACIÓN DE LA CALIDAD DE LOS PARÁMETROS

Dentro de las especificaciones ETSI SR 002 176 V1.1.1 categoría 002, se define un tamaño mínimo de clave de 1020 bits, esta CP respeta las especificaciones y determina la utilización de claves con una longitud mínima de 1024 bits.

6.1.8. *HARDWARE/SOFTWARE* DE GENERACIÓN DE CLAVES

Las claves son generadas bajo el modulo de *software* basado en algoritmos RSA provisto por *Microsoft*.

6.1.9. FINES DEL USO DE LA CLAVE

Las claves relacionadas con los certificados emitidos por una AC serán utilizadas bajo las mismas condiciones de usos permitidos y prohibidos de certificados.

---

[1] ETSI: *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.*
[2] Longitud mínima de clave = 1020.
[3] *Encoding Methods for Signatures with Appendix/ Probabilistic Signature Scheme.* Método de codificación para la operación de funciones *hash* desarrollado por RSA.

6.2. PROTECCIÓN DE LA CLAVE PRIVADA

6.2.1. CONTROL MULTIPERSONA DE LA CLAVE PRIVADA

Las claves privadas deben ser accesadas y utilizadas únicamente por su propietario, éstas serán protegidas con un nivel Alto de seguridad, para esto se establecerá la auto-autenticación de su propietario a través de contraseñas.

6.2.2. MÉTODO DE ACTIVACIÓN DE LA CLAVE PRIVADA

La activación de la clave privada se dará después de la auto-autenticación de su propietario a través de contraseñas.

6.2.3. MÉTODO DE DESACTIVACIÓN DE LA CLAVE PRIVADA

Las claves de ACs se desactivarán cuando la AC se encuentre fuera de funcionamiento, las claves de usuarios se desactivarán cuando el usuario suspenda o termine la sesión.

6.3. OTROS ASPECTOS DE LA GESTIÓN DE LA PAREJA DE CLAVES

6.3.1. ARCHIVO DE LA CLAVE PÚBLICA

Se almacena todos los certificados emitidos para usuarios finales durante un período de 2 años, los certificados de ACs subordinadas se almacenan por 3 años y el certificado de la AC-RAÍZ por 12 años.

6.3.2. PERIODO DE USO PARA LAS CLAVES PÚBLICAS Y PRIVADAS

Esta CP determina que el certificado de una AC subordinada y la pareja de claves relacionadas con éste, tendrá una duración de 2 años a partir de su emisión; en el caso de la AC-RAÍZ, sus claves tendrán una duración de 10 años a partir de su emisión.

En el caso de certificados de usurario, esta CP determina que el certificado de una entidad destino y la pareja de claves relacionadas con éste, tendrá una duración de 1 año a partir de su emisión.

6.4. DATOS DE ACTIVACIÓN

Esta sección es aplicable solo a certificados emitidos por AC-SUBs para usuarios dentro de la red ACSW.

6.4.1. GENERACIÓN Y ACTIVACIÓN DE LOS DATOS DE ACTIVACIÓN

El usuario que ingrese al sistema por primera vez, deberá cambiar obligatoriamente la contraseña proporcionada por el Administrador de AC cuando inicie una sesión.

6.4.2. PROTECCIÓN DE LOS DATOS DE ACTIVACIÓN

El propietario del certificado es responsable de guardar la reserva de la contraseña que protege su clave privada.

6.5. CONTROLES DE SEGURIDAD INFORMÁTICA

ACSW garantiza que el acceso a los Centros de Seguridad Informática está limitado a personal autorizado, entre las medidas que se han tomado para garantizar el control de acceso se tiene:

- Identificación adecuada del personal.
- Administración de los perfiles de usuarios.
- Separación entre el Centro de Seguridad Informática y otras secciones de red de ACSW.
- Restricción del acceso al directorio únicamente dentro del dominio de ACSW.

7. PERFILES DE CERTIFICADOS Y CRLs

7.1. PERFIL DE CERTIFICADO

7.1.1. NÚMERO DE VERSIÓN

Esta CPS define la expedición de dos tipos de certificado, los dos cumplen con el estándar X.509v3; el primero está destinado a la firma y emisión de certificados de entidades subordinadas. El segundo está destinado al intercambio de claves simétricas para asegurar las comunicaciones dentro de una WLAN.

7.1.2. EXTENSIONES DEL CERTIFICADO

Se utiliza las extensiones:

- [*PolicyExtension*]: Lista las políticas definidas por el usuario.
- [*AuthorityInformationAccess*].- Especifica los puntos de acceso de la información de la AC.
- [*CRLDistributionPoint*].- Indica los puntos de distribución de CRLs.
- [*BasicConstraintsExtension*]: Restricción de Ruta del Certificado.

7.1.3. IDENTIFICADOR DE OBJETO (OID) DE LOS ALGORITMOS

El identificador del algoritmo para la generación de certificados es SHA1withRSAEncryption = 1.2.840.113549.1.1.5[1].

7.1.4. FORMATOS DE NOMBRES

Los certificados contienen el nombre distinguido del emisor y propietario en los capos Emitido por y Enviado a, respectivamente. El campo CN del emisor debe mantener mayúsculas en su totalidad.

7.1.5. RESTRICCIONES DE LOS NOMBRES

Se restringen todos los nombres que no concuerden con los establecidos en el literal anterior.

7.1.6. IDENTIFICADOR DE OBJETO (OID) DE LA POLÍTICA DE CERTIFICACIÓN

El OID para identificar la CP es el siguiente: 1.3.6.1.4.1.311.21.8.0.0.0.2.1.0.1.402.

7.2. PERFIL DE CRL

7.2.1. NÚMERO DE VERSIÓN

El formato de CRLs utilizado dentro de la PKI-ACSW está definido por la versión 2 establecida dentro del estándar X.509.

7.2.2. CRL Y EXTENSIONES

Se utiliza CRLs establecidas en el estándar X.509.

---

[1] *iso.member.usa.rsadsi.pkcs.pkcs-1*.

8. AUDITORÍA DE CONFORMIDAD

8.1. FRECUENCIA DE LOS CONTROLES DE CONFORMIDAD PARA CADA ENTIDAD

Un proceso de Auditoría será realizado cada año para verificar el cumplimento de la CP y CPS; después de la evaluación se realizará una reestructuración para corregir omisiones en el cumplimento de la directiva.

8.2. IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR

La entidad auditora será seleccionada entre las empresas que brinden este servicio en el área de funcionamiento de la PKI-ACSW.

8.3. RELACIÓN ENTRE EL AUDITOR Y LA ENTIDAD AUDITADA

La independencia entre la entidad que realiza la auditoría es necesaria para evitar conflictos de intereses que puedan afectar los resultados.

8.4. TÓPICOS CUBIERTOS POR EL CONTROL DE CONFORMIDAD

La entidad auditora deberá verificar el cumplimiento de los siguientes aspectos:

- Publicación de CP y CPS.
- Publicación de certificados y CRLs.
- Protección de los datos entregados por los solicitantes.
- Disponibilidad del servicio.
- Procedimientos de Identificación y Autenticación.
- Control de Acceso a los Centros de Seguridad Informática.

8.5. ACCIONES A TOMAR COMO RESULTADO DE UNA DEFICIENCIA

Si los resultados obtenidos revelan no-conformidades, se tomarán las medidas pertinentes para su eliminación en el menor tiempo posible. En el caso de encontrarse una deficiencia grave, la PKI-ACSW suspenderá temporalmente sus funciones hasta la aplicación de medidas correctivas.

8.6. COMUNICACIÓN DE RESULTADOS

La entidad auditora comunicará los resultados de la auditoría a las Autoridades de la empresa ACSW y a los Administradores y ARs de las sucursales en las que se detecten no-conformidades.

9. REQUISITOS COMERCIALES Y LEGALES

9.1. TARIFAS

Debido a que los certificados emitidos serán utilizados únicamente por entidades miembro de ACSW, no se aplica ninguna tarifa por emisión y mantenimiento.

9.2. POLÍTICA DE CONFIDENCIALIDAD

9.2.1. INFORMACIÓN CONFIDENCIAL

Está prohibida la divulgación o uso de información confidencial. Se considera información confidencial a la siguiente:

- Claves privadas de las ACs de la PKI-ACSW.
- Claves privadas de los certificados emitidos para entidades destino.
- Información relacionada con la operación de la PKI-ACSW.
- Información de mecanismos de control de acceso, seguridad, auditoría, etc.
- Información proporcionada por los solicitantes de certificado.
- Secretos comerciales.
- Información sobre estudios de patentes.

9.2.2. INFORMACIÓN NO CONFIDENCIAL

Se considera información no confidencial pero restringida a la siguiente:

- CP y CPS de la PKI-ACSW.
- Información registrada en certificados emitidos por una AC dentro de la PKI-ACSW.
- Listas de revocación de certificados.

Se permite el acceso a la información considerada no confidencial, únicamente a los miembros de la empresa ACSW.

9.3. DERECHOS DE PROPIEDAD INTELECTUAL

Todos los elementos de propiedad intelectual creados por la PKI-ACSW forman parte del patrimonio de la empresa ACSW, esto incluye: certificados y CRLs, CP, la presente CPS, etc.

9.4. OBLIGACIONES Y RESPONSABILIDAD CIVIL

9.4.1. OBLIGACIONES DE LA AC

Toda AC perteneciente a la PKI-ACSW está obligada a cumplir con los siguientes aspectos:

- Emisión de certificados bajo la CP y la presente CPS respetando el formato X.509v3.
- Protección de su clave privada.
- Publicación de su certificado y CRLs de manera oportuna.
- Suspensión, reactivación y revocación de certificados bajo la CP y la presente CPS.
- Notificar de manera oportuna en caso de compromiso de su clave privada.
- Publicar la CP y la presente CPS en el directorio.
- Colaborar con las auditorias internas y externas.
- Garantizar la disponibilidad del directorio.
- Conservar los respaldos de bases de datos.
- Notificar de manera oportuna en caso de cese en sus funciones.

9.4.2. OBLIGACIONES DE LA AR

Toda AR perteneciente a la PKI-ACSW está obligada a cumplir con los siguientes aspectos:

- Identificación de los usuarios que requieren la emisión de un certificado bajo la CP y la presente CPS.
- Almacenar de forma segura la información proporcionada por un solicitante.
- Verificar la firma del contrato para el acceso a certificados dentro de la PKI-ACSW por parte de la entidad destino.
- En caso de que una solicitud sea negada, debe comunicar a la entidad correspondiente los motivos que produjeron la negación.
- Informar a la AC correspondiente de la aprobación de solicitudes.
- Solicitar la suspensión o revocación de un certificado cuando sea necesario.
- Colaborar con las auditorias internas y externas.

9.4.3. OBLIGACIONES DE LAS ENTIDADES DESTINO

Toda entidad destino perteneciente a la PKI-ACSW está obligada a cumplir con los siguientes aspectos:

- Tener conocimiento de la CP y la presente CPS.
- Proporcionar a la AR correspondiente información fiable, veraz y oportuna.
- Limitar el uso de su certificado a lo estipulado en la CP y la presente CPS.
- Proteger su clave privada.
- Solicitar la revocación de su certificado inmediatamente después de la sospecha o confirmación del compromiso de su clave privada.

9.4.4. OBLIGACIONES DE LAS ENTIDADES CONFIANTES EN LOS CERTIFICADOS EMITIDOS POR LA PKI-ACSW

Toda entidad confiante perteneciente a la PKI-ACSW está obligada a realizar la validación de un certificado según la CP y la presente CPS; además deberá limitar la confianza en un certificado en base a los datos suscritos en éste.

9.4.5. OBLIGACIONES DEL DIRECTORIO

Todo directorio perteneciente a la PKI-ACSW está obligado a mantener la disponibilidad de directivas, certificados y CRLs.

9.5. LEGISLACIÓN APLICABLE

En el Ecuador está vigente la 67 (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos) y su respectivo reglamento. Adicionalmente, el CONATEL ha expedido la Resolución 584 compuesta por "Reglamento Para Acreditación De Servicios De Comercio Electrónico".

9.6. CONFORMIDAD CON LA LEY APLICABLE

Debido a que en el Ecuador no se ha acreditado hasta el momento una AC con título hablitante, el funcionamiento de la PKI-ACSW se sustenta en el artículo 28 de la Ley 67, que establece que "Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho".

ANEXO 6-1: FORMULARIO ACSW-1

ACSW

FORMULARIO UNICO PARA SOLICITAR LA CREACIÓN DE UN CERTIFICADO PARA LA AUTENTICACIÓN EAP-TLS DENTRO DE LA WLAN DE ACSW

DATOS DEL USUARIO SOLICITANTE

Nombre:
Cedula de Ciudadanía:
Dirección:
Teléfono Fijo:
Teléfono Móvil:
e-mail personal:

Firma
CC:

Uso Exclusivo par las Autoridades Encargadas del Registro

DATOS DE LA AR de Recursos Humanos

Nombre:
Teléfono Móvil:
e-mail corporativo:

DATOS DE LA AR de IT

Nombre:
Teléfono Móvil:
e-mail corporativo:

Respuesta a la Solicitud

Fecha:
Número de Formulario:
Estado: Aprobado: ☐ Negado: ☐

Firma AR Recursos Humanos
CC:

Firma AR Dep. IT
CC:

ANEXO 6-2: CONTRATO DE CERTIFICACIÓN

ACSW

Contrato de Certificación-OID 1.3.6.1.4.1.311.21.8.**0.0.0.2.1.0.**1.402

En Quito, hoy **dd/mm/aa**, celebran el presente contrato de certificación, por una parte, como Proveedor de Servicios de Certificación, la empresa ACSW (en adelante ACSW), legalmente representada por el (la) señor(a) **Nombre Administrador de AC**, en su calidad de Administrador de AC de la Sucursal Nº **#**, y por otra parte en calidad de usuario propietario de certificado (en adelante Usuario), el (la) señor(a) **Nombre del Usuario**, portador de la Cédula de ciudadanía Nº **xxxxxxxxx-x**; sus propios y personales derechos, mayores de edad y legalmente capaces para contratar, quienes libre y voluntariamente convienen en celebrarlo, de conformidad con las siguientes estipulaciones.

Primera.- El **Usuario** suscribe el siguiente contrato de certificación asociado con la Política de Certificación con OID: 1.3.6.1.4.1.311.21.8.0.0.0.2.1.0.1.402 y la Declaración de Prácticas de Certificación con OID: 1.3.6.1.4.1.311.21.8.0.0.0.2.1.0.1.402 emitidas por ACSW.

Segunda.- El **Usuario** declara conocer y aceptar los términos y reglamentaciones determinados en la Política de Certificación y Declaración de Prácticas de Certificación relacionadas con el uso de certificados digitales emitidos por ACSW; asimismo, declara que los datos entregados al Departamento de Recursos Humanos de ACSW para su identificación son ciertos.

Tercera.- El **Usuario** se obliga a mantener la confidencialidad y reserva debida en los asuntos que por razón de su relación con la PKI de ACSW llegue a conocer. Esta obligación se mantendrá aún después de terminado el Contrato.

Firma Usuario	Firma Administrador
CC:	CC:

Anexo 7

Código del sitio Web ACSW

A.7. CÓDIGO DEL SITIO *WEB* ACSW

```
<html>
<head>
<title>ACSW-Autoridades Certificadoras Wireless</title>
<style>
<!--
 /* Font Definitions */
 @font-face
        {font-family:Verdana;
        panose-1:2 11 6 4 3 5 4 4 2 4;
        mso-font-charset:0;
        mso-generic-font-family:swiss;
        mso-font-pitch:variable;
        mso-font-signature:536871559 0 0 0 415 0;}
 /* Style Definitions */
h1
        {mso-margin-top-alt:auto;
        margin-right:0cm;
        mso-margin-bottom-alt:auto;
        margin-left:0cm;
        text-align:justify;
        line-height:150%;
        mso-pagination:widow-orphan;
        mso-outline-level:1;
        font-size:24.0pt;
        font-family:Verdana;
        font-weight:bold;}
p
        {mso-margin-top-alt:auto;
        margin-right:0cm;
        mso-margin-bottom-alt:auto;
        margin-left:0cm;
        text-align:justify;
        line-height:150%;
        mso-pagination:widow-orphan;
        font-size:12.0pt;
```

```
        font-family:Verdana;
        mso-fareast-font-family:"Times New Roman";
        mso-bidi-font-family:"Times New Roman";}
-->
</style>
</head>
<body bgcolor="#FFF3F8">
<table width="117%" border=1 cellpadding=0 cellspacing=0 class=MsoTableGrid
 style='background:#EBEAD1;border-collapse:collapse;border:none;mso-border-bottom-alt:
 solid maroon 6.0pt;mso-yfti-tbllook:480;mso-padding-alt:0cm 5.4pt 0cm 5.4pt;
 mso-border-insideh:.5pt solid windowtext;mso-border-insidev:.5pt solid windowtext'>
 <tr>
  <td width=442 valign=top style='width:333.0pt;border:none;border-bottom:solid maroon 6.0pt;
  padding:0cm 5.4pt 0cm 5.4pt'>
  <h1 align=center style='margin-right:31.65pt;text-align:center'><span
  style='font-size:16.0pt;mso-bidi-font-size:24.0pt;line-height:150%'>        <img        width=274
height=160
  src="iisstart_archivos/image004.jpg"><o:p></o:p></span></h1>
  <h1 align=center style='margin-right:31.65pt;text-align:center'><span
  style='font-size:16.0pt;mso-bidi-font-size:24.0pt;line-height:150%'><u2:p></u2:p>Autoridades
  Certificadoras <br>Wireless</span></i><span style='font-size:28.0pt;
  mso-bidi-font-size:24.0pt;line-height:150%'><o:p></o:p></span></h1>
  </td>
  <td width=598 valign=top style='width:450.3pt;border:none;border-bottom:solid maroon 6.0pt;
  padding:0cm 5.4pt 0cm 5.4pt'>
  <p style='margin-right:22.2pt'><span style='font-size:26.0pt;mso-bidi-font-size:
  12.0pt;line-height:150%;color:#71A05E'>Bienvenidos a ACSW<o:p></o:p></span></p>
     <p><span    style='font-size:12.0pt;line-height:150%;color:#71A05E'><font    face="Verdana,
Arial, Helvetica, sans-serif">La
                PKI-ACSW se encuentra en funcionamiento desde el 27 de Junio de 2006,
       de acuerdo a lo dispuesto en el Documento Nº ACSW-999, emitido el 1 de
       Junio de 2006 por la empresa ACSW,
       en el cual se autoriza su funcionamiento para la emisión de certificados
       digitales para la autenticación.</font></span></p></td>
 </tr>
</table>
<br>
```

```
<table width="100%" border="1" align="center" cellpadding="4" cellspacing="1"
bordercolor="#FFFFFF" bgcolor="#D5EEFB">
        <tr>
          <td height="177"><p align="left"><strong>Descargar desde este link
       el archivo de la Declaración de Prácticas de Certificación:</strong></p>
      <p align="left"> <a href="./Policy/cps-acsw.v1.0.pdf"><font size="2">Declaración
       de Prácticas de Certificación</font></a> </p>
      </td>
          <td><p class=MsoNormal align=left style='text-align:left'><strong>Descargar
       desde este link el archivo de <st1:PersonName ProductID="la Política" w:st="on">la
       Política</st1:PersonName> de Certificación</strong>:</p>

        <p class=MsoNormal><span style='font-size:9.0pt;line-height:150%'><a
    href="./Policy/cp-acsw.v1.0.pdf"><font size="2">Política de
          Certificación</font></a><font size="2"><o:p></o:p><o:p></o:p></font><font
size="3"><o:p></o:p></font><font size="2"><o:p></o:p></font><font
size="7"><o:p></o:p></font><o:p></o:p></span></p>
          </td>
          <td><p align="left"><strong>Descargar desde este link las Listas de
       Revocación de Certificados: </strong></p>
      <p align="left"><span style='font-size:9.0pt;
    line-height:150%'><a href="./CRL/"><span
    class=SpellE> CRLs</span> </a></span></p></td>
          <td><p class=MsoNormal align=left style='text-align:left'><strong>Descargar
       desde uno de los links el archivo del Certificado se <st1:PersonName
    ProductID="la AC-SUB" w:st="on">la AC-SUB</st1:PersonName> o de <st1:PersonName
    ProductID="la AC-Raíz" w:st="on">la AC-Raíz</st1:PersonName>:</strong></p>
            <p class=MsoNormal><span style='font-size:9.0pt;line-height:150%'><a
    href="./CertSub/acsw-ac-sub.ACSW.com_AC-SUB.crt">Certificado
            AC-SUB</a></span><span
    style='font-size:10.0pt;line-height:150%'> o </span><span style='font-size:
    9.0pt;line-height:150%'><a href="./CertRaiz/acsw-ac-raiz.ACSW.com_AC-RAIZ.crt">Certificado
            AC-Raíz</a></span></p> </td>
        </tr>
       </table>

<table width="100%" border="0">
```

```
  <tr>
    <td><div align="center"><font face="Verdana, Arial, Helvetica, sans-serif"><span style='font-
size:14.0pt;
line-height:150%'>Si requiere más información, comuníquese con el Administrador
       de AC de su sucursal.</span></font></div></td>
  </tr>
  <tr>
    <td></td>
  </tr>
  <tr>
    <td><div align="center"><font face="Verdana, Arial, Helvetica, sans-serif"><span
style='font-size:16.0pt;mso-bidi-font-size:12.0pt;line-height:150%'><img width=52 height=30
src="iisstart_archivos/image008.jpg"></span><span
style='font-size:11.0pt;mso-bidi-font-size:9.0pt;line-height:150%;color:black'>En
       este portal está restringido para los miembros de ACSW.</span><span
style='font-size:16.0pt;mso-bidi-font-size:12.0pt;line-height:150%'><img width=52 height=30
src="iisstart_archivos/image008.jpg"></span></font></div></td>
  </tr>
  <tr>
    <td></td>
  </tr>
  <tr>
    <td><div align="center"><font size="2" face="Arial, Helvetica, sans-serif">&copy;
       2006 ACSW. Todos los derechos reservados. </font></div></td>
  </tr>
</table>
</body>
</html>
```

Anexo 8

Instalación de Servicios

A.8. INSTALACIÓN DE SERVICIOS

A.8.1. Servicios de Servidor Principal

Antes de empezar con la instalación se debe insertar el disco de instalación de *Windows 2003 Server*. En el cuadro de diálogo **Administre su servidor** se da un clic en el botón **Agregar o quitar función** como se muestra en la figura A.8.1; la pantalla que luego se presenta indica que todas las tarjetas de red o *modems* deben estar conectados antes de empezar con la instalación, se da un clic en **siguiente.**

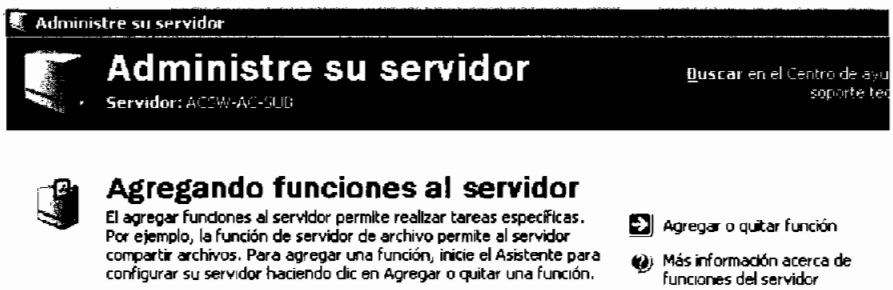


Figura A.8.1 Aplicación para Administrar el Servidor

En el cuadro de diálogo **Opciones de configuración**, se selecciona **Configuración típica para un servidor principal** y se da un clic en **siguiente**. En la pantalla siguiente se ingresa el nombre del nuevo dominio (ACSW.com), como se muestra en la figura A.8.2 y se da un clic en **siguiente**; a continuación, en la pantalla de configuración del nombre de *NetBios*, se mantiene el nombre ACSW y se da un clic en **siguiente**.

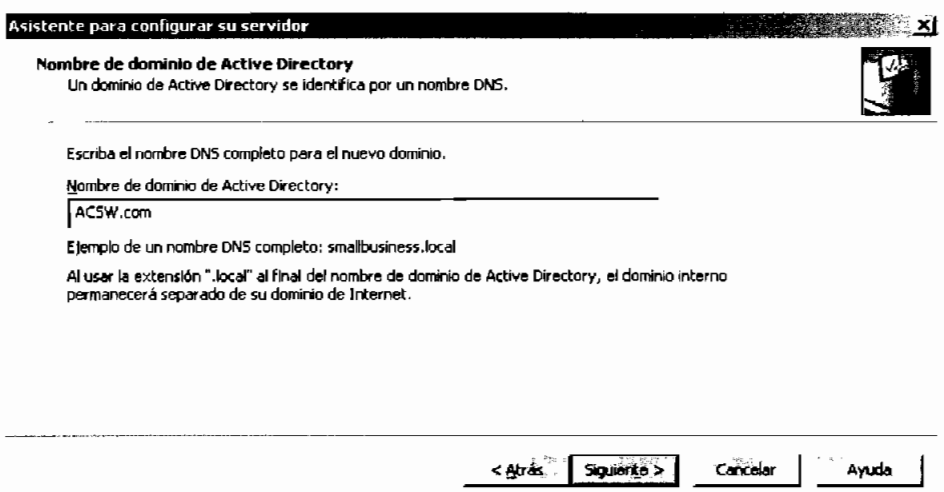


Figura A.8.2 Nombre del Dominio

En la pantalla que sigue, se consulta si es necesario reenviar consultas a un Servidor DNS (*Domain Name System*); el servidor DNS se instalará en el mismo servidor de *Active Directory*, por lo tanto se selecciona **No reenviar consultas** y se da un clic en **siguiente**.

Antes de iniciar con el proceso de instalación se presenta en pantalla el resumen de las opciones seleccionadas para la instalación del dominio como se muestra en la figura A.8.3, si los datos mostrados son correctos, se da un clic en **siguiente**.

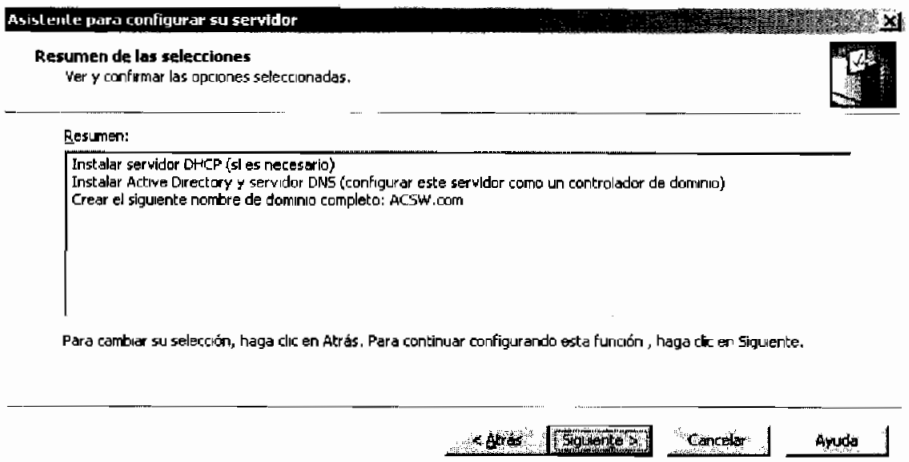


Figura A.8.3 Resumen de Elementos seleccionados para la Instalación

Entonces se presenta un cuadro de diálogo que indica que es posible que el equipo deba reiniciarse durante el proceso de instalación, se da un clic en **Aceptar**.

Cuando la instalación ha concluido, el equipo debe reiniciarse. Al iniciar nuevamente el sistema, se muestra en pantalla un resumen de las instalaciones realizadas, entre éstas se encuentran: *Active Directory*, DNS y DHCP como se muestra en la figura A.8.4; se da un clic en **siguiente** y en la pantalla que sigue se da un clic en **finalizar**.

A.8.1.1. Definir el Espacio de Direcciones IP

Se ingresa al **Inicio** de *Windows* y se selecciona la opción **Herramientas administrativas** y luego **DHCP** como se muestra en la figura A.8.5.

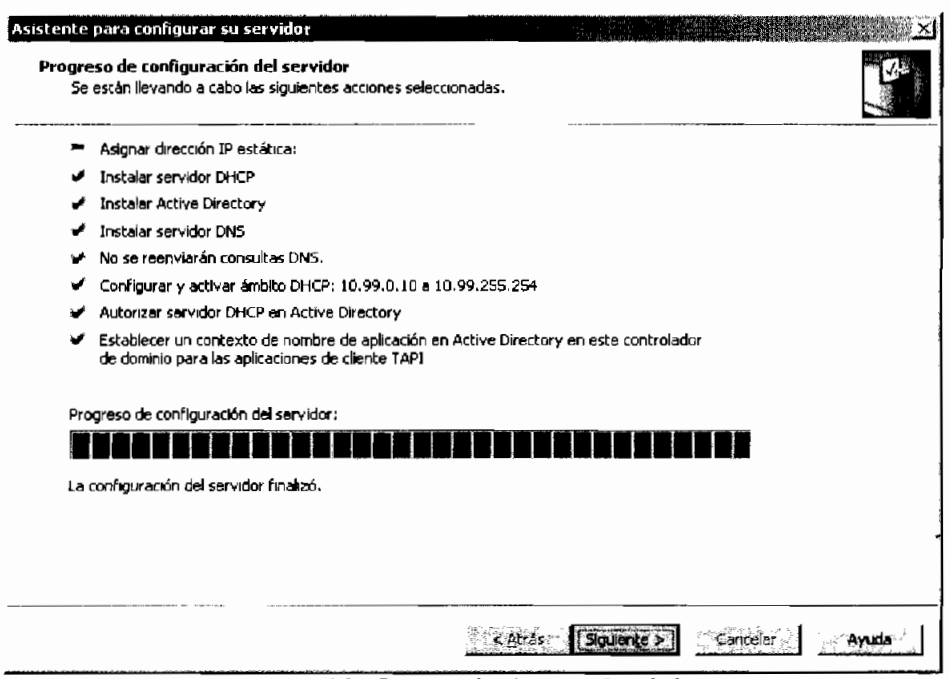


Figura A.8.4 Resumen de Elementos Instalados

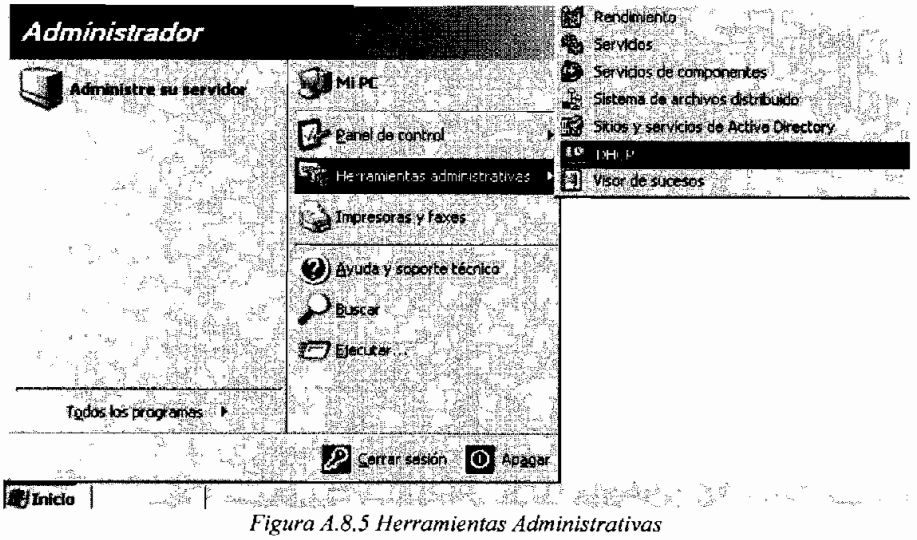


Figura A.8.5 Herramientas Administrativas

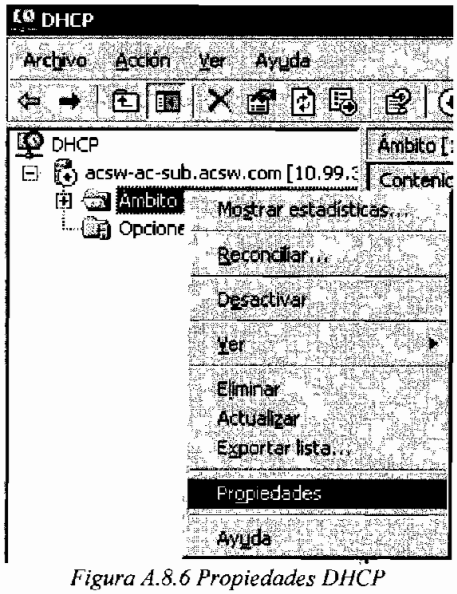


Figura A.8.6 Propiedades DHCP

En la pantalla de administración de DHCP, se da un clic con el botón derecho de *mouse* sobre la carpeta **Ámbito** y en el menú emergente se selecciona la opción **Propiedades**, tal como se muestra en la figura A.8.6.

En la pestaña **General**, de la pantalla **Propiedades de Ámbito**, se cambia el nombre del ámbito por ACSW, la dirección IP inicial por 10.99.30.51 y la dirección IP final por 10.99.30.150; adicionalmente se limita la duración de la concesión de direcciones a 10 días, como se muestra en la figura A.8.7, cuando se ha concluido se da un clic en **Aceptar**.

A.8.1.2. Añadir Usuarios al Dominio

Se ingresa al **Inicio** de *Windows* y se selecciona la opción **Herramientas administrativas** y luego ***Usuarios y equipos de Active Directory***, en la pantalla de administración de usuarios se selecciona el dominio **ACSW.com** y luego la carpeta ***Users*** como se muestra en la figura A.8.8.

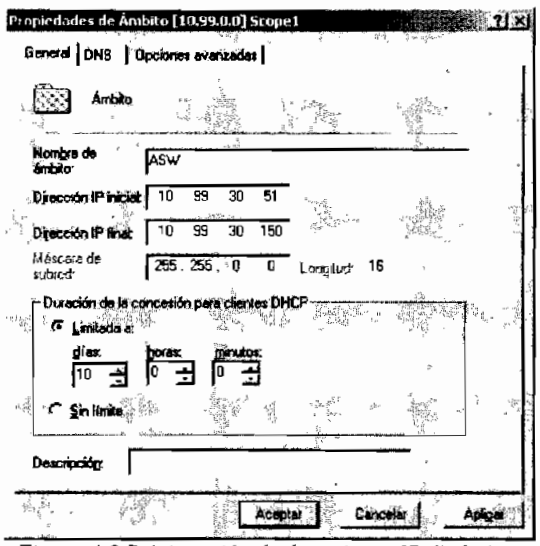


Figura A.8.7 Asignación de direcciones IP dinámicas

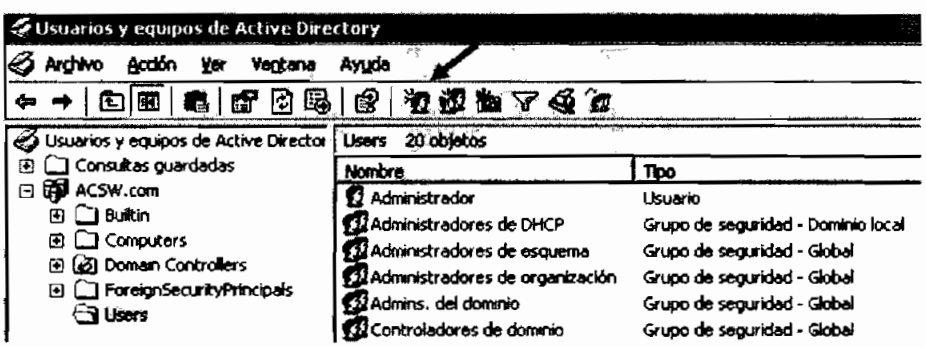


Figura A.8.8 Agregar usuarios y equipos

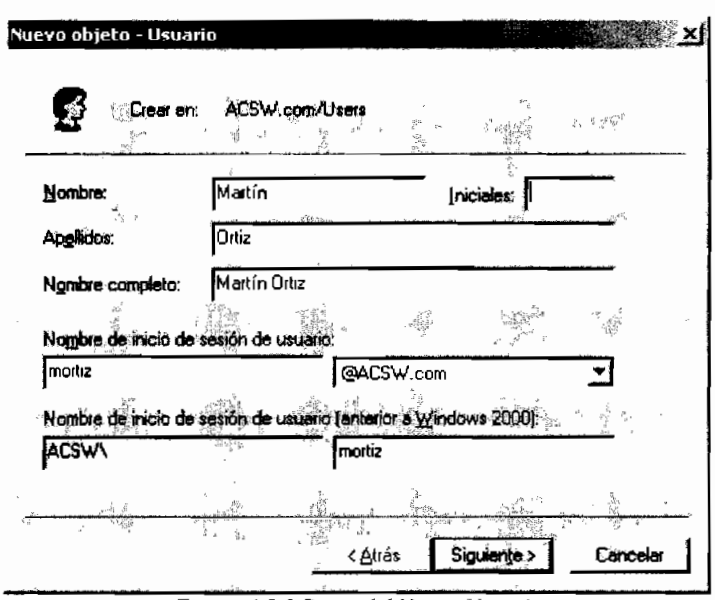


Figura A.8.9 Datos del Nuevo Usuario

Para crear un usuario con perfil de **Usuario** se selecciona en la barra de herramientas de *Active Directory* el botón **Crear un nuevo usuario** señalado con la flecha en la figura A.8.8; en la pantalla **Nuevo objeto** se llena el Nombre, Apellido y nombre de sesión como se muestra en la figura A.8.9. Cuando se ha concluido se da un clic en **siguiente**.

En la pantalla siguiente se ingresa y confirma una contraseña; luego, se selecciona la opción **El usuario debe cambiar la contraseña al iniciar una sesión de nuevo** y se da un clic en **siguiente**; luego se presenta un resumen con los datos del nuevo usuario, si los datos son correctos, se da un clic en **finalizar**.

Para crear un nuevo usuario con perfil de Administrador se da un clic con el botón derecho de *mouse* sobre el usuario predeterminado como Administrador y en el menú emergente se selecciona **Copiar** como se muestra en la figura A.8.10; luego se sigue el proceso indicado anteriormente para la creación de nuevos usuarios.

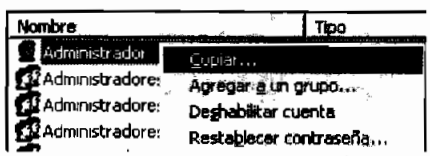


Figura A.8.10 Agregar Usuario con Perfil de Administrador

A.8.1.3. Añadir Equipos al Dominio

Se selecciona el botón **Inicio**, se da un clic con el botón derecho del *mouse* sobre **Mi PC** y en el menú emergente se elige **Propiedades**; en la pantalla de **Propiedades del Sistema**, se selecciona la pestaña **Nombre de equipo** como se muestra en la figura A.8.11 y luego se da un clic en **Cambiar**.

En la opción **Miembro de** del cuadro de diálogo **Cambios en el nombre de equipo** se selecciona **Dominio** y se escribe ACSW.com como se muestra en la figura A.8.12; luego, se da un clic en **Aceptar**.

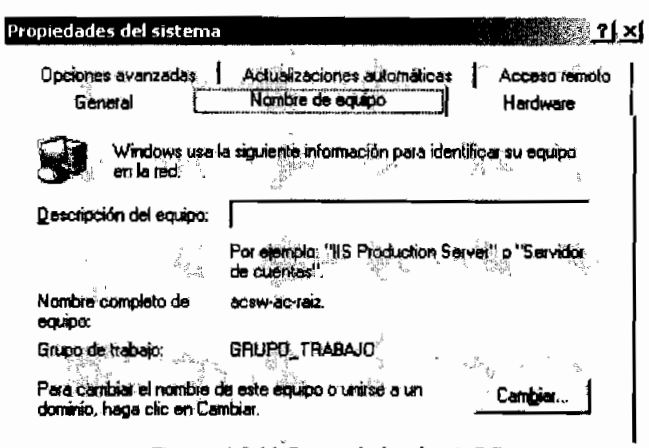


Figura A.8.11 Propiedades de Mi PC

Entonces se presenta un cuadro de diálogo que requiere la autenticación del usuario dentro del dominio, se ingresa el nombre de usuario y su contraseña y se da un clic en **Aceptar**, si el equipo se registró exitosamente se presentará el mensaje mostrado en la figura A.8.13, luego de lo cual se da un clic en **Aceptar** y se reinicia el equipo para que los cambios tengan efecto.

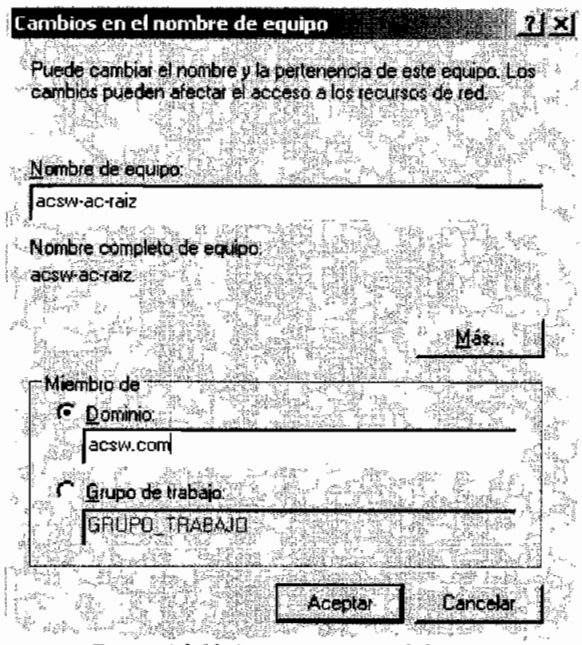


Figura A.8.12 Agregar equipos al dominio

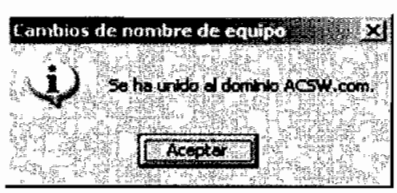


Figura A.8.13 Equipo agregado

A.8.2. IIS

En el cuadro de diálogo **Administre su servidor** se da un clic en el botón **Agregar o quitar función.** La pantalla que se presenta inicialmente indica los pasos preliminares antes de realizar una instalación; se da un clic en **siguiente**. En el cuadro de diálogo **Funciones del Servidor** se selecciona la opción **Servidor de Aplicaciones** y se da un clic en **siguiente.**

El siguiente cuadro de diálogo muestra herramientas adicionales soportadas por IIS para el desarrollo de aplicaciones *Web*, éstas no son requeridas para la implementación de la PKI, por lo tanto se da un clic en **siguiente**.

La siguiente pantalla muestra un resumen de las opciones seleccionadas para la instalación, si los datos mostrados son correctos, se da un clic en **siguiente**; cuando la instalación ha concluido, se da un clic en **finalizar**.

Finalmente, en el directorio *C:\Inetpub\wwwroot* del servidor de certificados de la AC subordinada se crea las carpetas *Policy*, *CertRaíz*, *CertSub* y CRL; éstas tienen la siguiente finalidad:

- *Policy*: Se utilizará para almacenar la CP y CPS de la empresa.
- *CertRaíz*: Se utilizará para almacenar el Certificado de la AC-Raíz.
- *CertSub*: Se utilizará para almacenar el Certificado de la AC-SUB.
- CRL: Se utilizará para almacenar las CRLs.

A.8.3. Herramientas de Administración y Supervisión

Para instalar las herramientas de administración se da un clic en el **Inicio** de *Windows* y se selecciona **Panel de control** y luego **Agregar o quitar programas**; en la pantalla que se presenta se da un clic sobre **Agregar o quitar componentes de *Windows***.

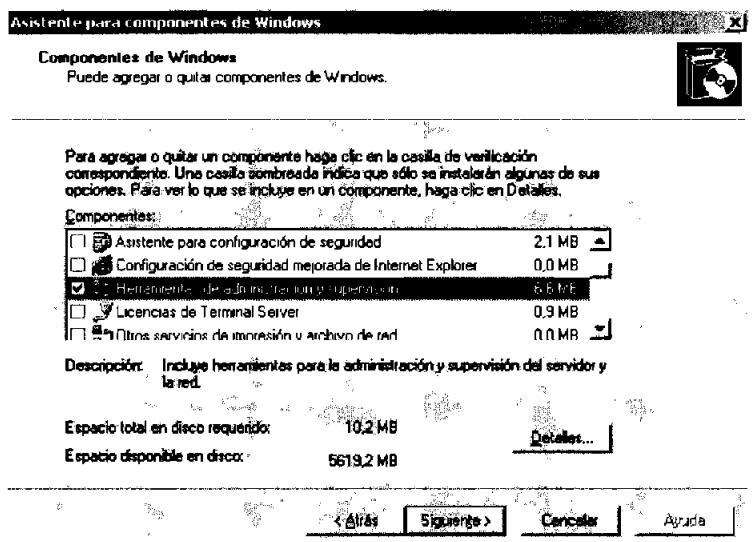


Figura A.8.14 Instalación de Herramientas de Administración y supervisión

En el **Asistente para componentes de *Windows*** se selecciona **Herramientas de administración y supervisión** como se muestra en la figura A.8.14; se presenta un mensaje indicando que deben detenerse temporalmente los servicios de IIS para continuar con la instalación, se da un clic en **Sí**. En el cuadro de diálogo del Asistente se da un clic en **siguiente** y en la pantalla que sigue se da un clic en **finalizar**.

A.8.3.1. Activar Auditorías de Objetos

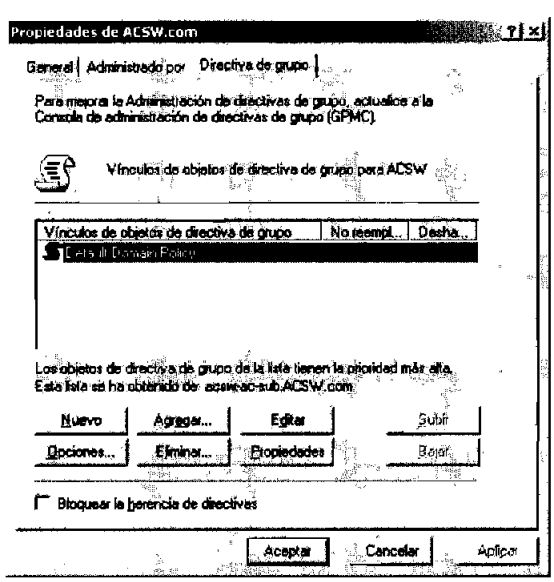


Figura A.8.15 Propiedades de ACSW.com

Para registrar los eventos que causen errores en los servidores de certificados, es necesario activar las auditorías de objetos; para esto se da un clic en el **Inicio** de *Windows*, se selecciona **Herramientas administrativas** y después a **Usuarios y equipos de *Active Directory***.

En la pantalla de *Active Directory* se da un clic con el botón derecho del *mouse* sobre el dominio ACSW.com y en el menú emergente se selecciona **Propiedades**; en el cuadro de diálogo de Propiedades se selecciona la pestaña **Directiva de Grupo** como se muestra en la figura A.8.15, ahí se da un doble clic sobre ***Default Domain Policy*** para ingresar en **Editor de objetos de directiva de Grupo**.

En el Editor de directivas dentro de la **Configuración del equipo** se selecciona la carpeta **Directiva de Auditoría** mostrada en la figura A.8.16 y en la parte derecha de la pantalla se da un doble clic sobre **Auditar el acceso a objetos**.

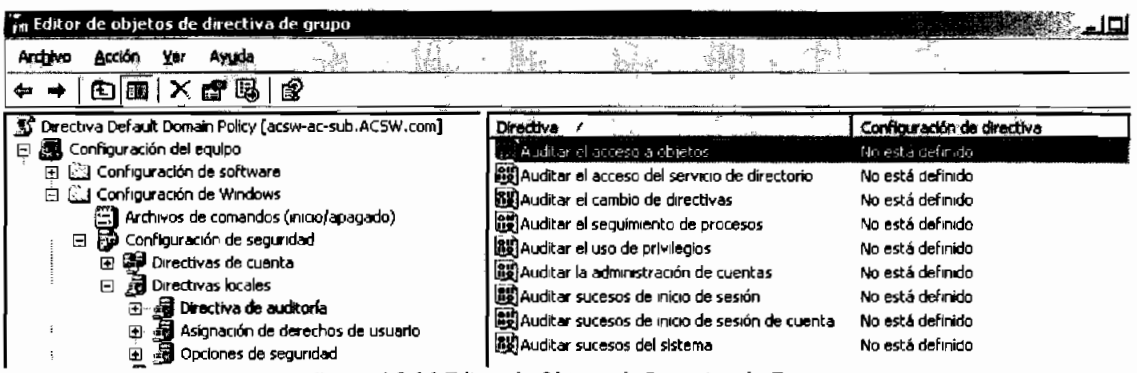


Figura A.8.16 Editor de Objetos de Directiva de Grupo

En el cuadro de diálogo que se presenta se selecciona la opción **Definir esta configuración de directiva** y luego se elige la opción **Error** como se muestra en la figura A.8.17; finalmente se da un clic en **Aceptar**.

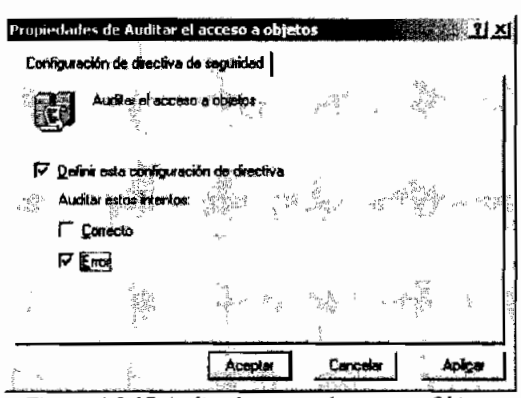


Figura A.8.17 Auditorías para el acceso a Objetos

Todos los eventos que produzcan error al acceder a objetos dentro de los servidores serán registrados en el **Visor de sucesos** de *Windows* en cada equipo.

Glosario de Acrónimos

GLOSARIO DE ACRÓNIMOS

#a: número de años

#d: número de días

#m: número de meses

3-DES: triple DES

AAA: Authentication, Authorization and Accounting

ABA: American Bar Association

AC: Autoridad Certificadora

ACS: Access Control Server

ACSW: Autoridades Certificadoras Wireless

ACU: Aironet Client Utility

AECOC: Asociación Española de Codificación Comercial

AES: Advanced Encryption Standard

AES-CCMP: AES in Counter Mode with CBC-MAC Protocol

AH: Authentication Header

ANSI: American National Standards Institute

AP: Access Point

AR: Autoridad de Registro

ASN.1: Abstract Syntax Notation One

B: Bóveda

B2B: Business-to-Business

BC: Bajo Custodia

BCE: Banco Central del Ecuador

BER: Bit Error Rate

BSS: Basic Service Set

c/p: Depende de cada persona

C:Cuenca

C4CA: Citizen and Commerce Class Common Certification Authority

CAL: Client Access License

CAST: Carlisle Adams and Strafford Travares

CC: Cambio de Cargo (funciones del empleado)

CDP: Cisco Discovery Protocol

CEN: Comité Europeo de Normalización

CF: Caja fuerte

CHAP: Challenge Authentication Protocol

CIOC: Chief Information Officers Council

CMC: Certificate Management Messages over CMS

CMP: Certificate Management Protocol

CMS: Cryptographic Message Syntax

CNUDMI: Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

COMEXI: Consejo de Comercio Exterior e Inversiones

CONATEL: Consejo Nacional de Telecomunicaciones

CP: Certificate Policy

CPFCA: Common Policy Framework Certification Authority

CPS: Certification Practice Statement

CRC-32: Código de Redundancia Cíclica-32 bits

CRL: Certificate Revocation List

CSMA/CA: Carrier Sense Multiple Access/Collision Avoidance

CSP: Cryptographic Service Provider

D: Destruido

DAP: Directory Access Protocol

DE: Dispositivo extraíble

DES: Data Encryption Standard

DFIR: Diffuse Infrared

DFS: Dynamic Frequency Selection

DHCP: Dynamic Host Configuration Protocol

DLL: Dynamic Linking Library

DNI: Documento Nacional de Identidad

DNS: Domain Name Service

DoD: Department of Defense

DS: Distribution System

DSA: Digital Signature Algorithm

DSS: Digital Signature Standard

DSSS: Direct Sequence Spread Spectrum

DU: Se desconfía del usuario

EAP: Extensible Authentication Protocol

EAP-FAST: EAP-Flexible Authentication via Secure Tunneling

EAPOL: EAP over LANs

EAP-SIM: EAP-Subscriber Identity Module

EAP-TLS: EAP-Transport Layer Security

EAP-TTLS: EAP-Tunneled TLS

EAPW: EAP over WLAN

ECC: Elliptic Curve Cryptosystems

EDCA: Enhanced Distributed Channel Access

EEPROM: Electrically Erasable Programmable Read-Only Memory

EIA: Electronics Industries Association

EJBCA: Enterprise JavaBeans Certificate Authority

EMV: Europay, MasterCard, and Visa

ESP: Encapsulating Security Payload

ESS: Extended Service Set

ETS: European Telecommunication Standard

ETSI: European Telecommunications Standards Institute

FBCA: Federal Bridge Certification Authority

FCD: Función de Coordinación Distribuida

FCP: Función de Coordinación Puntual

FHSS: Frequency Hopping Spread Spectrum

FIPS: Federal Information Processing Standards

FPKI: Federal Public Key Infrastructure

FT: Falla técnica en el Sistema de la PKI

FTP: File Transfer Protocol

G: Guayaquil

GNU: GNU's not UNIX

GPG: GNU Privacy Guard

GPL: General Public Licence

GTA: Global Trust Authority

GTC: Generic Token Card

GUID: Globally Unique Identifier

HCCA: HCF Controlled Channel Access

HCF: Hybrid Coordination Function

HiperLAN: HIgh PErformance Radio LAN

HMAC: Hash MAC

HP: Hewlett-Packard

HR/DSSS: High-Rate/DSSS

HTTP: Hypertext Transfer Protocol

HTTPS: Secure HTTP

I: Indefinido

IANA: Internet Assigned Numbers Authority

IAS: Internet Authentication Service

IBM: International Business Machines

ICMP: Internet Control Message Protocol

I-D: Internet Draft

IDEA: International Data Encryption Algorithm

IE: Internet Explorer

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

IIS: Internet Information Server

IP: Internet Protocol

IPSec: Internet Protocol Security

ISA: Internet Security and Acceleration

ISM: Industrial, Científica y Médica

ISO/IEC: International Organization for Standardization/International Electrotechnical Commission

IT: Information Technology

ITI: Instituto Nacional de Tecnologías de Información

J2EE: Java 2 Platform, Enterprise Edition

KCK: Key Confirmation Key

KEK: Key Encryption Key

KMF: Key Mixing Function

L: Loja

LDAP: Lightweight DAP

LEAP: Lightweight EAP

M: Memorizado

M1: Mensaje 1

M2: Mensaje 2

MAC: Media Access Control

MAC: Message Authentication Code

MD#: Message Digest # (MD2, MD4 y MD5)

MIC: Message Integrity Check

MIMO: Multiple-Input/Multiple-Output

MMC: Microsoft Management Console

MSCHAP: Microsoft version of the CHAP

MSCHAPv2: Microsoft version of the CHAP- version 2

MTA: Master Trust Authority

NA: Notary Authority

NC: No contesta

NDS: Novell Directory Services

NE: No es estable

NIC: Network Interface Card

NIST: National Institute of Standards and Technology

NMC: Néstor Marroquín Carrera

NR: No recuerda

NS: No sabe

NSA: National Security Agency

NTP: Network Time Protocol

OAC: Odyssey Access Client

OCSP: Online Certificate Status Protocol

OFDM: Orthogonal Frequency Division Multiplexing

OID: Object Identifiers

OSI: Open System Interconnection

OTP: One Time Password

PAC: Protected Access Credential

PAE: Port Access Entity

PAP: Password Authentication Protocol

PEAP: Protected EAP

PGP: Pretty Good Privacy

PIN: Personal Identification Number

PKCS: Public-Key Cryptography Standards

PKI: Public Key Infrastructure

PKIX: PKI X509

PLCP: Physical Layer Convergence Procedure

PMD: Physical Medium Dependent

PMK: Pairwise Master Key

PPP: Point to Point Protocol

PRF: Pseudo-Random Function

PS: Personal de sistemas

Q: Quito

QoS: Quality of Service

RADIUS: Remote Access Dial-In User Server

RAM: Random Access Memory

RC4: Rivest Cipher 4 o Ron's Code 4

RFC: Request for Comment

ROM: Read-Only Memory

RPM: RPM Package Manager

RSA: Rivest, Shamir and Adelman

RTGS: Real Time Gross Settlement

S/MIME: Secure/ Multipurpose Internet Mail Extensions

SATA: Serial Advanced Technology Attachment

SCI: Sistema de Cobros Interbancario

SCVP: Standard Certificate Validation Protocol

SENATEL: Secretaría Nacional de Telecomunicaciones

SET: Secure Electronic Transaction

SFN: Sistema Financiero Nacional

SHA: Secure Hash Algorithm

SNMP: Simple Network Management Protocol

SNP: Sistema Nacional de Pagos

SP: Service Pack

SPI: Sistema de Pagos Interbancario

SPL: Sistema de Pagos en Línea

SPN: Sistema de Pagos por valores Netos

SRI: Servicio de Rentas Internas

SSID: Service Set Identifier

SSL: Secure Sockets Layer

STA: Scheme Trust Authority

TCP: Transmission Control Protocol

TIA: Telecomunications Industries Association

TK: Temporal Key

TKIP: Temporal Key Integrity Protocol

TLS: Transport Layer Security

TPC: Transmit Power Control

TSA: Time Stamp Authority

TTP: Trusted Third Party

UDP: User Datagram Protocol

UIT-T: Unión Internacional de Telecomunicaciones: Sector de Normalización de las Telecomunicaciones

UTC: Universal Time Coordinated

VI: Vector de Inicialización

VLAN: Virtual LAN

VPN: Virtual Private Network

WECA: Wireless Ethernet Compatibility Alliance

WEP: Wired Equivalent Privacy

WFP: Windows File Protection

Wi-Fi: Wireless Fidelity

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Networks

WPA: Wi-Fi Protected Access

WPAN: Wireless Personal Area Networks

WWAN:Wireless Wide Area Networks

XOR: Exclusive OR