

# **ESCUELA POLITECNICA DEL EJERCITO**

**Carrera de Ingeniería de  
Sistemas e Informática**

**Desarrollo de una aplicación  
Sign – On en Smart Cards**

**Vinicio Ramirez M.**

# SEGURIDAD INFORMÁTICA

La Seguridad Informática debe vigilar principalmente por los siguientes elementos:

- **INTEGRIDAD**

Los componentes del sistema permanecen intactos a menos que sean modificados por los usuarios autorizados.

- **DISPONIBILIDAD**

Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

- **PRIVACIDAD**

Los componentes del sistema son accesibles sólo por los usuarios autorizados.

# SEGURIDAD INFORMÁTICA

- **CONTROL**

Solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

- **AUTENTICIDAD**

Definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

- **NO REPUDIO**

Evita que cualquier entidad que envíe o reciba información niegue que lo hizo.

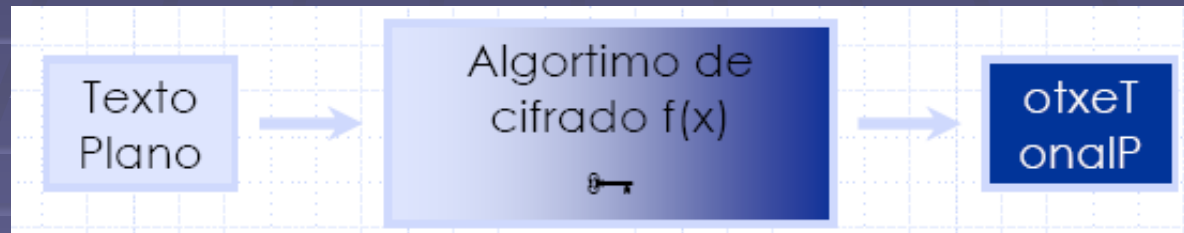
- **AUDITORIA**

Determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema.

# SEGURIDAD INFORMÁTICA

## CRIPTOGRAFIA

Transformar un mensaje legible en otro cifrado, mediante la utilización de claves, que solo el emisor y receptor conocen.



Utilidades:

- Genera certificados digitales
- Genera firmas digitales
- Protege información
- Protege tráfico
- Almacena credenciales localmente de una manera muy segura

# SEGURIDAD INFORMÁTICA

## MÉTODOS CRIPTOGRÁFICOS

- SIMÉTRICOS O DE CLAVE PRIVADA

Se emplea la misma clave para cifrar y descifrar.  
El emisor y receptor deben conocerlas.

- ASIMÉTRICOS O DE CLAVE PÚBLICA

Se emplea una clave privada y una clave pública.  
Una de ellas es utilizada para cifrar y la otra para descifrar.  
El emisor conoce una y el receptor la otra.  
Cada clave no puede obtenerse a partir de la otra.

# SEGURIDAD INFORMÁTICA

## FIRMA DIGITAL

Verifica que la información no ha sido modificada (integridad) desde su generación.

## CERTIFICADOS DIGITALES

Certifican que quien firma un documento electrónico, es quien dice ser, para lo cual se generan previamente la clave pública y privada del remitente.

# TARJETAS INTELIGENTES

Tarjetas de plástico similares a las tarjetas de crédito.

Poseen un circuito integrado.

Este circuito puede ser de sola memoria o contener un microprocesador (CPU) con un sistema operativo que le permite:

- Almacenar
- Encriptar información
- Leer y escribir datos, como un ordenador.



# TARJETAS INTELIGENTES

## CLASIFICACIÓN POR EL TIPO DE CONTACTO

### Tarjetas inteligentes de Lectores con Contacto

- Poseen chip y una placa de contactos
- Necesitan lector/grabador para comunicarse con el exterior

### Tarjetas inteligentes de Lectores sin Contacto

- Poseen chip y antena para realizar transacciones
- Transacciones rápidas

### Tarjetas inteligentes Híbridos (Ambos Lectores )

- Combinación de las anteriores.



# TARJETAS INTELIGENTES

## CLASIFICACIÓN POR EL TIPO DE MICROCHIP

### Tarjetas de Memoria Simple:

- Chip integrado
- Ventaja:
  - Almacenamiento más seguro de la información
- Desventaja:
  - Sólo almacenar información no la procesa

# TARJETAS INTELIGENTES

## CLASIFICACIÓN POR EL TIPO DE MICROCHIP

### Tarjetas de memoria inteligente con Lógica de Seguridad:

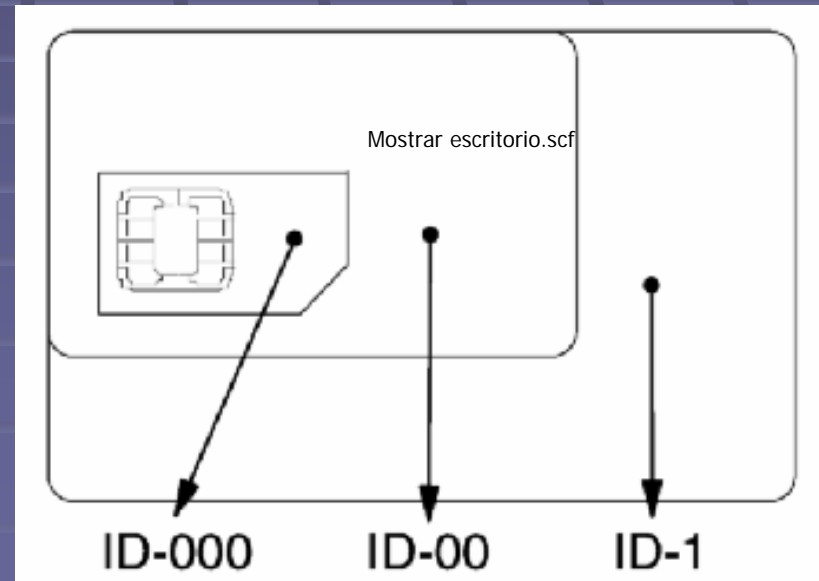
#### Tarjetas microprocesadores

- Ventajas:
  - Dispositivo seguro por definición
  - Capaces de procesar información (además de almacenarla)
  - Pueden ser programadas.
  - Multiaplicación (monedero electrónico, información bancaria, telefonía, etc)
- Desventajas:
  - Lenguajes de programación de tarjetas dependientes del hardware.
  - Programación de las tarjetas en ensamblador.
  - Aplicaciones desarrolladas por el proveedor de la tarjeta.

# TARJETAS INTELIGENTES

## Tamaños de tarjetas ISO 7816-1

- ID-1 (es el más habitual)
- ID-00
- ID-000 (GSM)



# PROTOCOLOS DE AUTENTICACIÓN: KERBEROS

- Protocolo de seguridad
- Utiliza criptografía de claves simétricas para validar usuarios
- Evita el envío de contraseñas a través de la red.

Kerberos puede proporcionar tres servicios de seguridad:

- **Autenticación:** Probar que usted es quien dice ser.
- **Integridad:** Asegurar que los datos no son modificados en su tránsito.
- **Privacidad:** Asegurar que los datos no son leídos por personas ajenas.

# PROTOSCOLOS DE AUTENTICACIÓN: KERBEROS

## VENTAJAS

- Autenticación segura: mezcla de números aleatorios y marcas de tiempo
- Eliminar la transmisión a través de la red de información de autenticación.
- Confidencialidad de datos: Flujo seguro mediante cifrado con claves de sesión

## DESVENTAJAS

- Gran centralización del sistema, si el servidor Kerberos falla, no habrá autenticación y por tanto no se podrá prestar ningún servicio que requiera autenticación
- Casi toda la seguridad reside en el servidor de la base de datos, y si esta se ve amenazada, lo estará la red
- Necesarias aplicaciones “kerberizadas” en todos los participantes

# ARQUITECTURA AAA

## AUTENTICACION (Authentication)

- Comprobación de que el usuario es quien dice ser

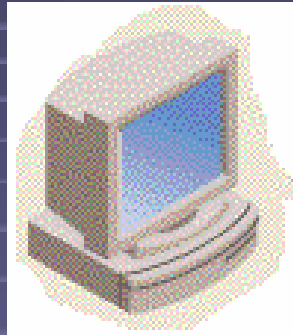
## AUTORIZACIÓN (Authorization)

- Verificación de las tareas autorizadas

## CONTABILIDAD (Accounting)

- Medición del consumo de recursos recursos

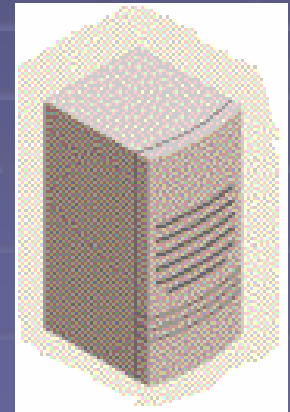
# SIGN ON



Agente  
certificador



Cliente



Servidor



# INSTALACIÓN DE ACTIVE DIRECTORY - DHCP

**Asistente para configurar su servidor**

**Nombre de dominio de Active Directory**  
Un dominio de Active Directory se identifica por un nombre DNS.

Escriba el nombre DNS completo para el nuevo dominio.

Nombre de dominio de Active Directory:

Ejemplo de un nombre DNS completo: smallbusiness.local

Al usar la extensión ".local" al final del nombre de dominio de Active Directory, el dominio interno permanecerá separado de su dominio de Internet.

< Atrás    Siguiente >    Cancelar    Ayuda

**Asistente para configurar su servidor**

**Resumen de las selecciones**  
Ver y confirmar las opciones seleccionadas.

Resumen:

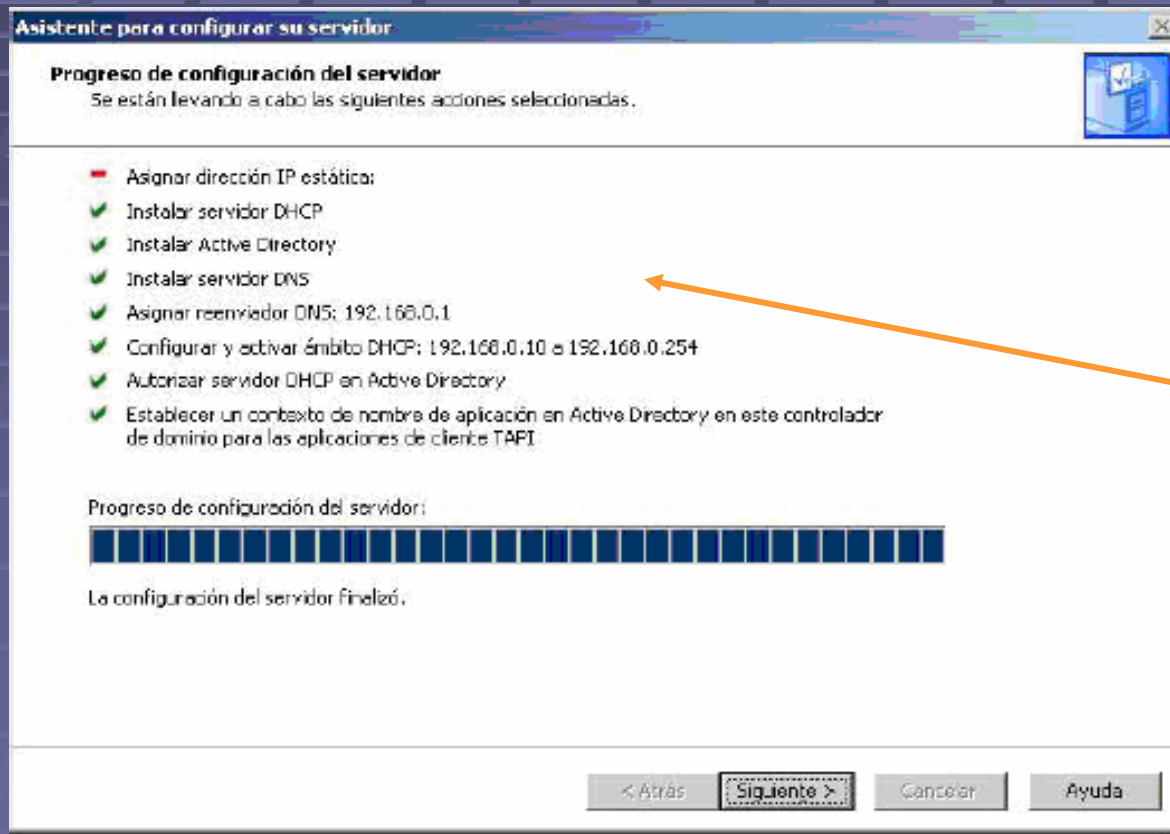
- Instalar servidor DHCP (si es necesario)
- Instalar Active Directory y servidor DNS (configurar este servidor como un controlador de dominio)
- Crear el siguiente nombre de dominio completo: minfin.gov.ec
- Enviar consultas DNS sin resolver al siguiente servidor: 192.168.0.1

Para cambiar su selección, haga clic en Atrás. Para continuar configurando esta función, haga clic en Siguiente.

< Atrás    **Siguiente >**    Cancelar    Ayuda

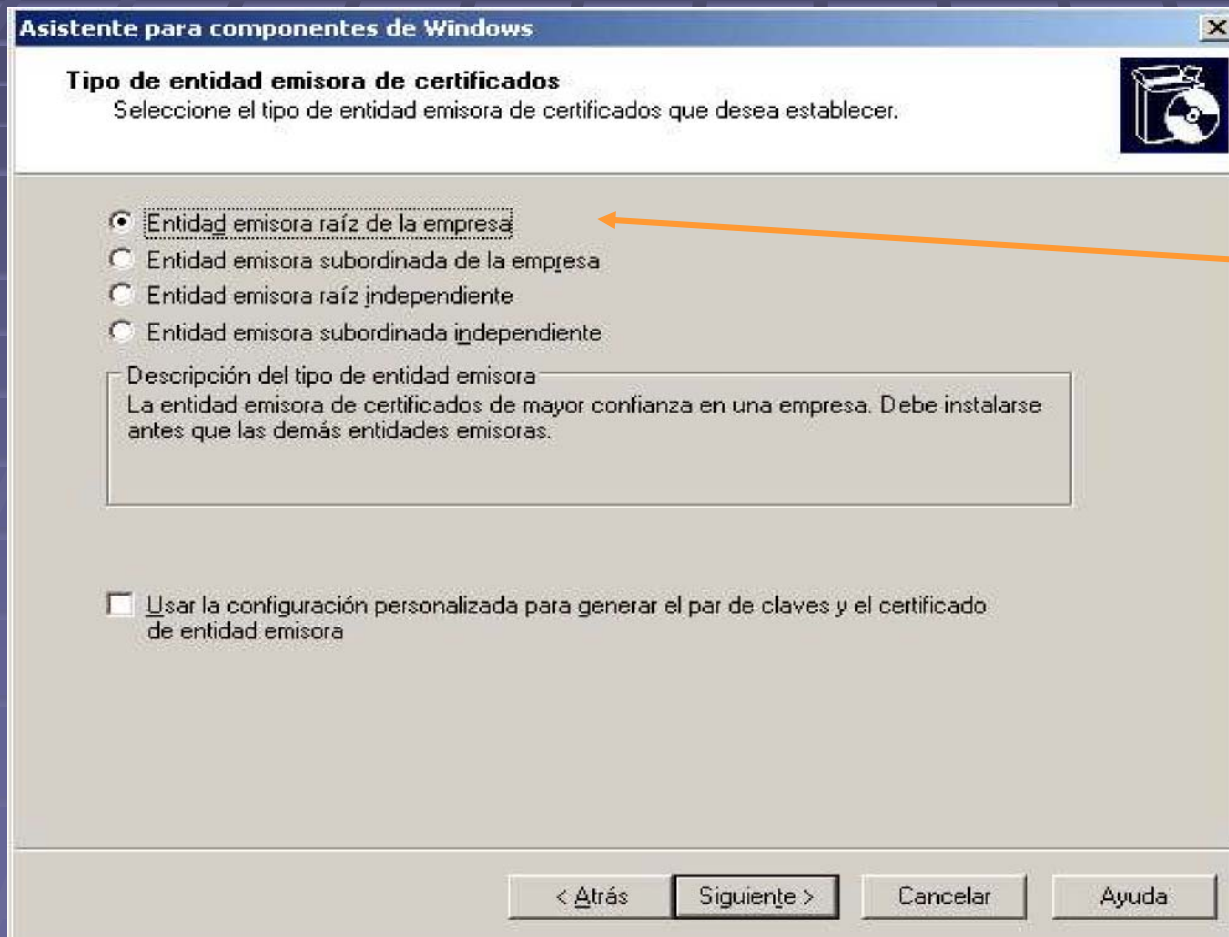


# INSTALACIÓN DE ACTIVE DIRECTORY - DHCP



Finalización  
De la Instalación  
Active Directory  
DHCP, etc

# INSTALACIÓN DE LA ENTIDAD EMISORA DE CERTIFICADOS



Entidad  
emisora raíz  
de la empresa

# INSTALACIÓN DE LA ENTIDAD EMISORA DE CERTIFICADOS

**Asistente para componentes de Windows**

**Configuración de la base de datos de certificados**  
Escriba la ubicación para la base de datos de certificados, el registro de la base de datos y la información de configuración.

Base de datos de certificados:  
 Examinar...

Registro de la base de datos de certificados:  
 Examinar...

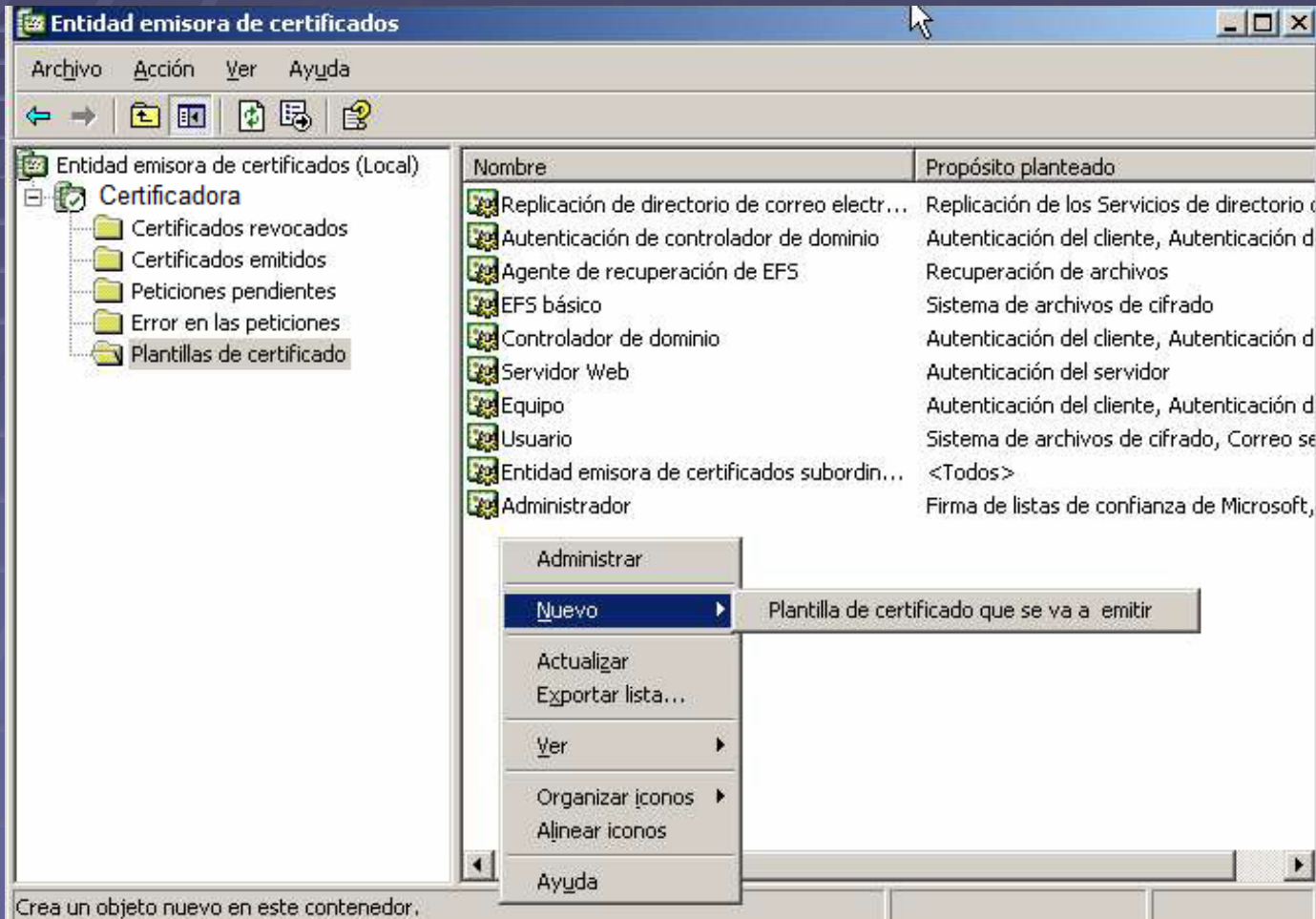
Almacenar la información de configuración en una carpeta compartida  
Carpeta compartida:  
 Examinar...

Conservar la base de datos de certificados existente

< Atrás    Siguiente >    Cancelar    Ayuda

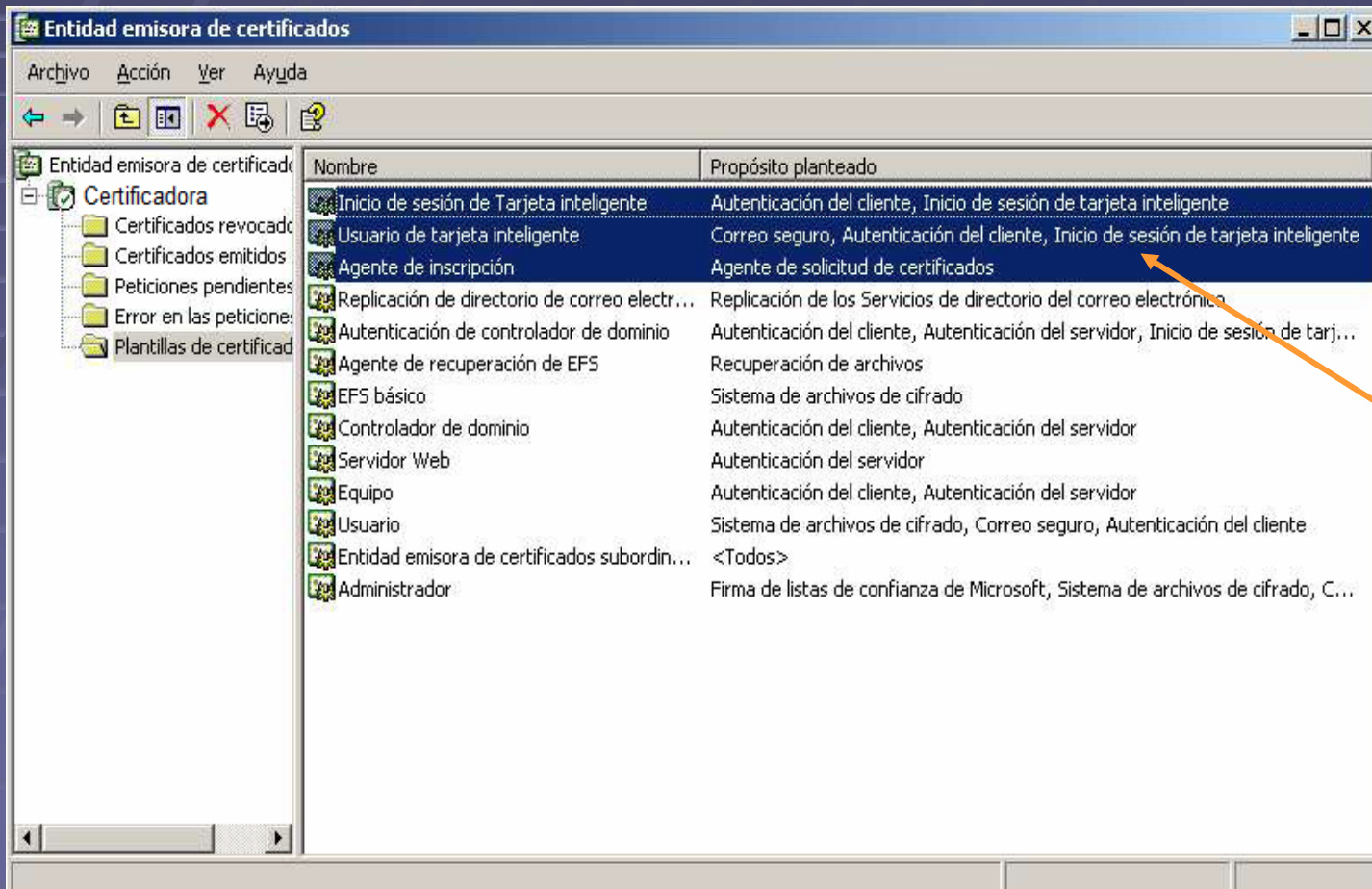
Almacenamiento de los certificados

# CONFIGURACIÓN DE ENTIDAD EMISORA DE CERTIFICADOS



Seleccionar  
Plantillas

# CONFIGURACIÓN DE ENTIDAD EMISORA DE CERTIFICADOS



Seleccionar plantillas a ser emitidas

# GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN

**Solicitar un certificado**

Servicios de Certificate Server de Microsoft - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Ir Vínculos >>

Dirección http://192.168.0.1/certsrv/

Microsoft Servicios de Certificate Server -- Certificadora **Principal**

**Bienvenida**

Use este sitio Web para solicitar un certificado para su explorador de Web, programa cliente de correo electrónico u otro programa. Al utilizar un certificado, puede confirmar su identidad ante otras personas con las que se comunica vía Web, firmar y codificar mensajes, y, dependiendo del tipo de certificado que solicite, realizar otras tareas de seguridad.

También puede usar este sitio Web para descargar certificados de entidad emisora (CA), cadenas de certificados, listas de revocación de certificados (CRL) o ver el estado de una solicitud pendiente.

Para obtener más información de acerca de Servicios de Certificate Server, consulte [Documentación de Servicios de Certificate Server](#).

**Seleccione una tarea:**

- [Solicitar un certificado](#)
- [Ver el estado de una solicitud de certificado pendiente](#)
- [Descargar un certificado de entidad emisora, cadena de certificados o lista de revocación](#)

http://192.168.0.1/certsrv/certraqd.asp Sitios de confianza

# GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN

Servicios de Microsoft Certificate Server - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Ir Vínculos >>

Dirección <http://192.168.0.1/certsrv/certrqad.asp>

Microsoft Servicios de Certificate Server -- Certificadora Principal

## Solicitud de certificado avanzada

La directiva de la entidad emisora (CA) determina los tipos de certificados que puede solicitar. Haga clic en una de las siguientes opciones para:

- [Crear y enviar una solicitud a esta CA.](#)
- [Enviar una solicitud de certificados usando un archivo cifrado de base64 CMC o PKCS #10 o una solicitud de renovación usando un archivo cifrado de base64 PKCS #7.](#)
- [Solicitar un certificado para una tarjeta inteligente de otro usuario usando la Estación de inscripción de certificados para tarjetas inteligentes.](#)

Nota: Debe tener un agente de inscripción de certificados para enviar una solicitud de otro usuario.

<http://192.168.0.1/certsrv/certrqma.asp> Sitios de confianza

Crear y Enviar  
una Solicitud a  
esta CA

# GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN

Servicios de Microsoft Certificate Server - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Dirección http://192.168.0.1/certsrv/certrqma.asp

Microsoft Servicios de Certificate Server -- Certificadora Principal

### Solicitud de certificado avanzada

Plantilla de certificado: Agente de inscripción

Opciones de clave:

Crear conjunto de claves nuevo  Usar el conjunto de claves establecido

Proveedor de servicios de cifrado (CSP): Microsoft Enhanced Cryptographic Provider v1.0

Uso de clave:  Firma

Tamaño de la clave: 1024 Min.: 384 (tamaños de clave comunes: 512 1024 2048 4096 8192 16384) Máx.: 16384

Nombre automático de contenedor de claves  Nombre de contenedor de claves especificado por el usuario

Marcar claves como exportables

Habilitar la protección de clave privada de alta seguridad

Almacenar el certificado en el almacén de certificados del equipo local  
*Almacena el certificado en el almacén del equipo local en lugar del almacén de certificados del usuario. No instala el certificado de la entidad emisora raíz. Debe ser un administrador para generar o usar una clave en el almacén local del equipo.*

Opciones adicionales:

Formato de solicitud:  CMC  PKCS10

Algoritmo hash: SHA-1  
*Sólo usado para solicitud de firmas.*

Guardar solicitud en un archivo

Atributos:

Nombre descriptivo:

Enviar >

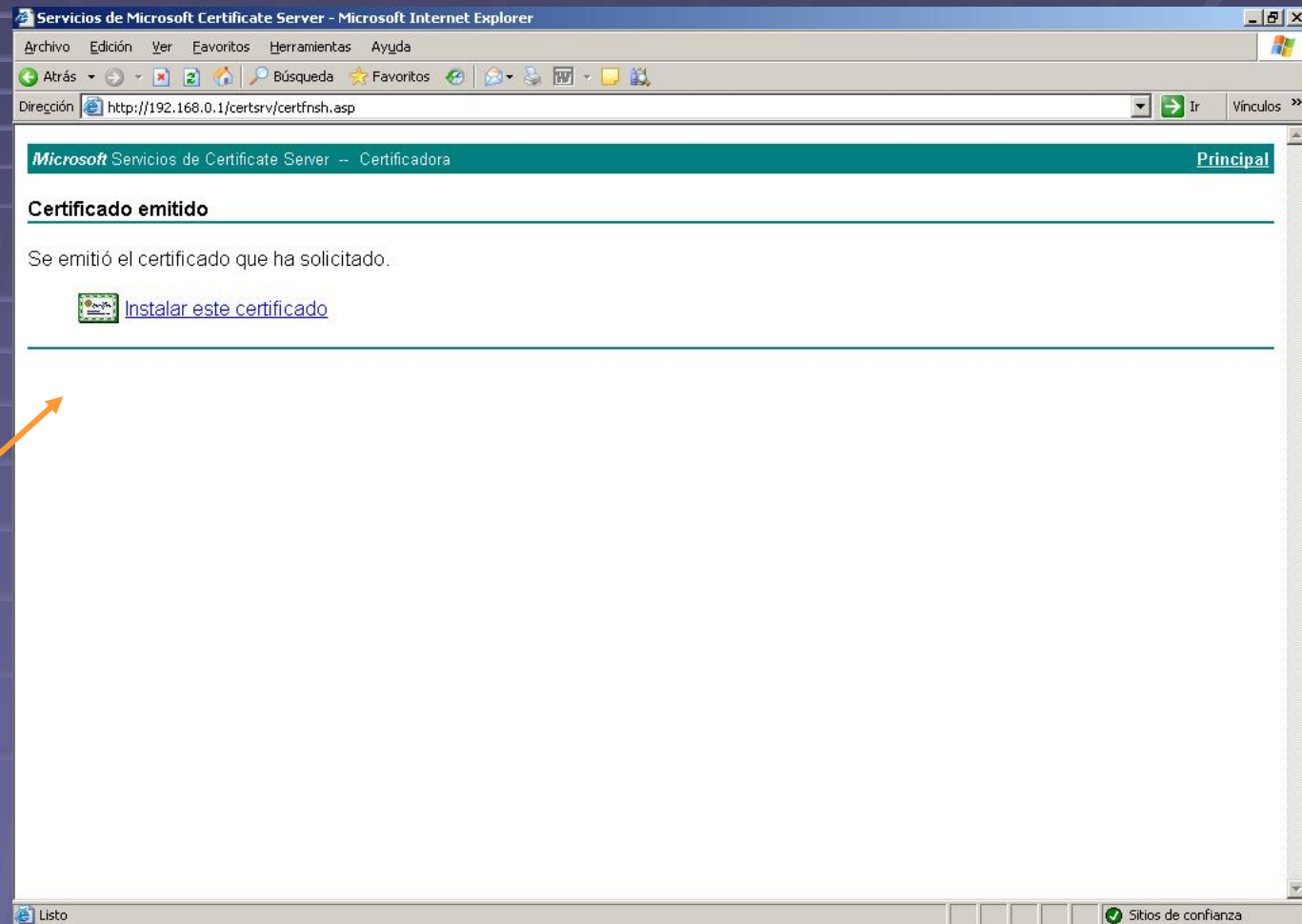
Listo Sitios de confianza

Seleccionar la Opción de Agente de Inscripción

Enviar solicitud

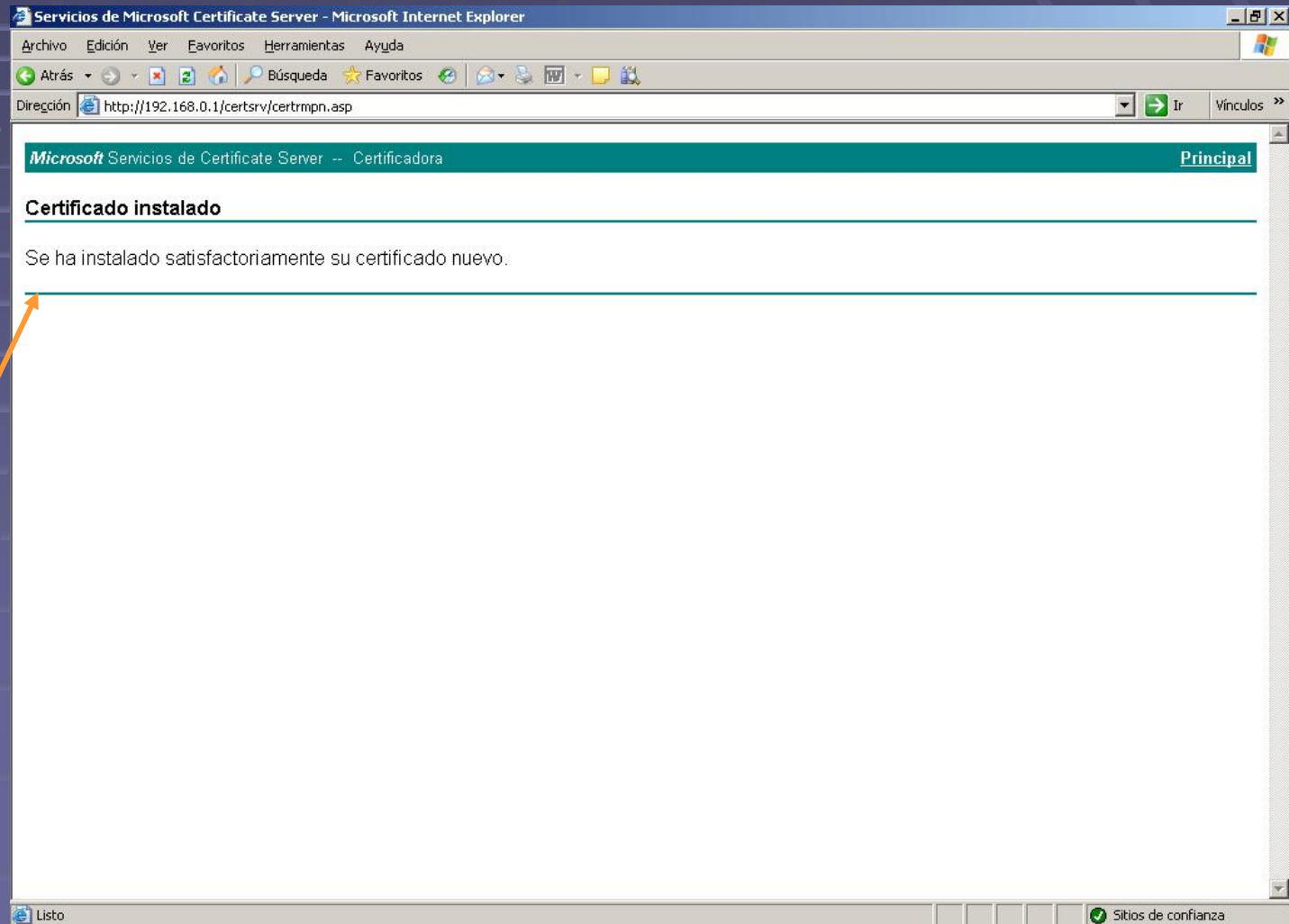


# GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN



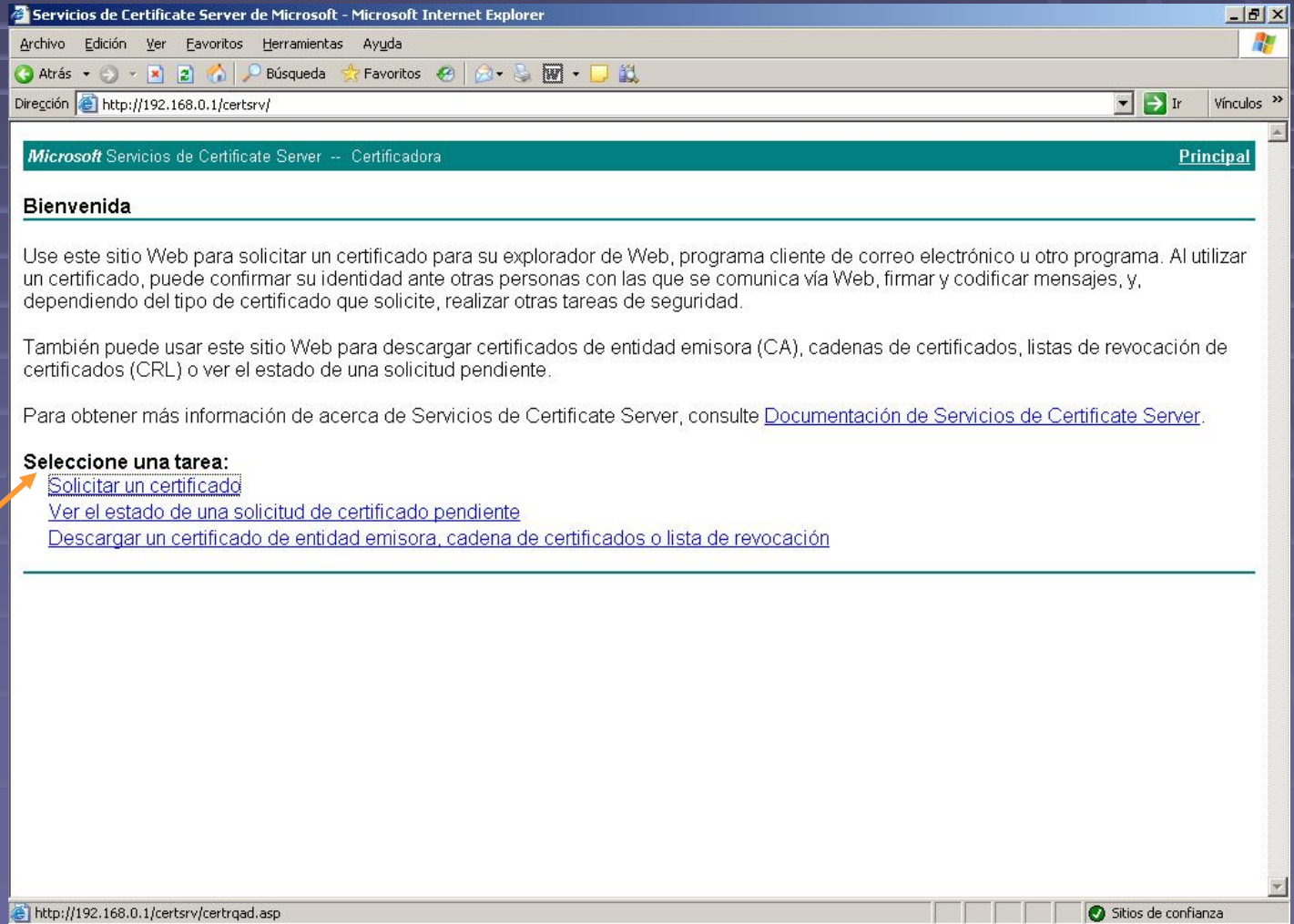
Instalar  
certificado

# GENERACIÓN DEL CERTIFICADO DEL AGENTE DE INSCRIPCIÓN



Finalización  
Configuración  
del Agente  
Certificador

# GENERACIÓN DE CERTIFICADOS PARA USUARIOS



Solicitar un certificado para usuario

# GENERACIÓN DE CERTIFICADOS PARA USUARIOS

Servicios de Microsoft Certificate Server - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Ir Vínculos >>

Dirección <http://192.168.0.1/certsrv/certrqad.asp>

Microsoft Servicios de Certificate Server -- Certificadora Principal

## Solicitud de certificado avanzada

La directiva de la entidad emisora (CA) determina los tipos de certificados que puede solicitar. Haga clic en una de las siguientes opciones para:

- [Crear y enviar una solicitud a esta CA.](#)
- [Enviar una solicitud de certificados usando un archivo cifrado de base64 CMC o PKCS #10 o una solicitud de renovación usando un archivo cifrado de base64 PKCS #7.](#)
- [Solicitar un certificado para una tarjeta inteligente de otro usuario usando la Estación de inscripción de certificados para tarjetas inteligentes.](#)

Nota: Debe tener un agente de inscripción de certificados para enviar una solicitud de otro usuario.

<http://192.168.0.1/certsrv/certsces.asp> Sitios de confianza

Solicitar un certificado para tarjeta inteligente

# GENERACIÓN DE CERTIFICADOS PARA USUARIOS

Estación de inscripción de la tarjeta inteligente de Microsoft - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Ir Vinculos

Dirección http://192.168.0.1/certsrv/certsces.asp

Servicios de **Microsoft** Certificate Server **Principal**

### Estación de inscripción de certificados para tarjetas inteligentes

**Opciones de inscripción:**

Plantilla de certificado: [v]  
Entidad emisora de certificados: [v]  
Proveedor de servicios de cifrado: [v]  
Certificado de firma de administrador: (Certificado...)

**Usuario que se inscribirá:**

(Usuario n...)

**Estado:**

Espera un momento. Cargando control ActiveX.

Internet Explorer

Un control ActiveX de esta página podría no ser seguro al interactuar con otras partes de la página. ¿Desea permitir esta interacción?

Sí No

Aceptar la solicitud

# GENERACIÓN DE CERTIFICADOS PARA USUARIOS

Estación de inscripción de la tarjeta inteligente de Microsoft - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Ir Vínculos >>

Dirección http://192.168.0.1/certsrv/certsces.asp

Servicios de **Microsoft** Certificate Server Principal

### Estación de inscripción de certificados para tarjetas inteligentes

**Opciones de inscripción:**

Plantilla de certificado: Inicio de sesión de Tarjeta inteligente

Entidad emisora de certificados: Certificadora

Proveedor de servicios de cifrado: CeresCSP

Certificado de firma de administrador: Administrador

**Usuario que se inscribirá:**

(Usuario no seleccionado)

**Estado:**

Seleccione un usuario para la inscripción.

Sitios de confianza

Seleccionar la opción de...

Seleccionar usuario desde Active Directory

# GENERACIÓN DE CERTIFICADOS PARA USUARIOS

Estación de inscripción de la tarjeta inteligente de Microsoft - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Ir Vinculos

Dirección http://192.168.0.1/certsrv/certsces.asp

Servicios de Microsoft Certificate Server Principal

## Estación de inscripción de certificados para tarjetas inteligentes

**Opciones de inscripción:**

Plantilla de certificado: Inicio de sesión de Tarjeta inteligente

Entidad emisora de certificados: Certificadora

Proveedor de servicios de cifrado: CeresCSP

Certificado de firma de administrador: Administrador

**Usuario que se inscribirá:**

yramirez@minfin.gov.ec

**Estado:**

Inserte la tarjeta inteligente del usuario en el lector y después presione 'Inscribir'.

Sitios de confianza

Inscribir la tarjeta

# GENERACIÓN DE CERTIFICADOS PARA USUARIOS

Estación de inscripción de la tarjeta inteligente de Microsoft - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Ir Vínculos

Dirección <http://192.168.0.1/certsrv/certsces.asp>

Servicios de **Microsoft** Certificate Server Principal

## Estación de inscripción de certificados para tarjetas inteligentes

**Opciones de inscripción:**

Plantilla de certificado:

Entidad emisora de certificados:

Proveedor de servicios de cifrado:

Certificado de firma de administrador:

**Usuario que se inscribirá:**

**Estado:**

Esperando mientras el usuario se inscribe...

**Verificación de PIN**

**Introducir PIN**

XXXX

OK Cancel

Seleccionar certificado...

Seleccionar usuario...

Ingresar Código de la Smart Card

Inscribiendo... SitiOS de confianza



# GENERACIÓN DE CERTIFICADOS PARA USUARIOS

Estación de inscripción de la tarjeta inteligente de Microsoft - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Dirección <http://192.168.0.1/certsrv/certsces.asp> Ir Vínculos >>

Servicios de **Microsoft** Certificate Server Principal

## Estación de inscripción de certificados para tarjetas inteligentes

**Opciones de inscripción:**

Plantilla de certificado:

Entidad emisora de certificados:

Proveedor de servicios de cifrado:

Certificado de firma de administrador:

**Usuario que se inscribirá:**

**Estado:**

La tarjeta inteligente está lista. Presione 'Ver certificado' para asegurarse de que el certificado contiene la información personal correcta acerca del usuario.

Verificar Certificado en Smart Card

# GENERACIÓN DE CERTIFICADOS PARA USUARIOS



Certificado en  
Smart Card

# INICIO DE SESIÓN CON TARJETA INTELIGENTE



Cliente listo para  
log on con smart  
card

# INICIO DE SESIÓN CON TARJETA INTELIGENTE

Iniciar sesión en Windows



Microsoft®  
**Windows 2000  
Professional**  
Basado en tecnología NT

Microsoft®

NIP:

Iniciar sesión usando una conexión de acceso telefónico

Ingresa Pin de  
Smart Card

**GRACIAS**