INSTRUCTIVO ALTA, REHABILITACIÓN Y BAJA DE USUARIOS SLU / MCC

INTRODUCCIÓN

El presente documento tiene como objetivo definir el instructivo de alta (A), rehabilitación (R) y baja (B) de usuarios en el dominio de la aplicación SLU (Sidif Local Unificado) y su habilitación en el sistema MCC perteneciente a la Oficina Nacional de Contrataciones.

ALCANCE

El presente instructivo está destinado a los usuarios del sistema SLU y a los responsables de la administración del sistema SLU en el organismo. Este instructivo permite:

- Conocer qué datos son necesarios para realizar un pedido de ABR.
- Conocer qué formulario utilizar y cómo completarlo.
- Conocer qué autorizaciones son necesarias para que el pedido tome curso.
- Conocer los sectores encargados de recibirlo y hacerlo efectivo.
- Conocer los conceptos básicos de Firma Digital.
- Conocer cómo solicitar, renovar o revocar un certificado digital.
- Conocer cómo instalar, utilizar y verificar un certificado digital.

REQUERIMIENTOS

Para poder solicitar el alta (A), rehabilitación (R) y baja (B) de usuarios en el dominio de la aplicación SLU es necesario que cada una de las personas responsables de la administración del sistema SLU en el organismo obtenga un Certificado Digital, el cual deberán instalar en su computadora. Para hacer efectivo este requerimiento siga las instrucciones detalladas en el Anexo A.

SOLICITUD DE ALTA(A), REHABILITACIÓN(R) Y BAJA(B)

Para solicitar un alta (A), rehabilitación (R) y/o baja (B) de usuarios el responsable de la administración del sistema SLU en el organismo deberá enviar a la Mesa de Ayuda de la Unidad Informática de la Secretaría de Hacienda un mail firmado a la cuenta mesa@mecon.gov.ar, adjuntando una copia del Formulario de Solicitud de Accesos al sistema SLU, que deberá ser bajado desde

(http://uninfo.mecon.gov.ar/Docs/Formularios/Formulario_Pedido_Acceso_SLU.doc) o solicitado por mail a la Mesa de Ayuda de la Unidad Informática (mesa@mecon.gov.ar).

El responsable de la administración del SLU en el organismo deberá completar en el Formulario de Solicitud de Accesos al sistema SLU los datos marcados como obligatorios, a saber:

2.1 Para el caso de ***Alta*** de usuario indicar:

- **A**lta
- Sistema **SLU y/o MCC**
- Repartición a la que pertenece
- Nombre y Apellido completos
- Documento, Tipo y Número
- Dirección IP de la PC (*)
- Nombre de la impresora que utiliza para imprimir (*)
- Nombre del driver de la impresora que utiliza.(*)

(*) Se explica como obtener estos datos en la guía de relevamiento técnico, que se entrega al inicio de las réplicas.

2.2 Para el caso de ***Rehabilitación*** de usuario indicar:

- **R**ehabilitación
- Repartición a la que pertenece
- Cuenta (login) del usuario que necesita rehabilitación

2.3 Para el caso de ***Baja*** de usuario indicar:

- **B**aja
- Repartición a la que pertenece
- Cuenta (login) del usuario a dar de baja

3. El sector Mesa de Ayuda abrirá un pedido interno y enviará un mail al solicitante indicando el número de pedido correspondiente.

4. Una vez realizado el pedido, el sector Mesa de Ayuda enviará un mail al responsable de la administración del sistema SLU que originó el pedido, con la solución del mismo en un archivo **adjunto**. Este archivo adjunto contendrá un mail **firmado y cifrado** por los administradores de las cuentas en la Unidad Informática y contendrá los datos necesarios para acceder al sistema SLU/MCC. Luego, el sector Mesa de Ayuda cerrará el pedido y deberá mantener una copia (impresa o digital) del mail enviado.

5. El responsable de la administración del sistema SLU efectuará una copia impresa del documento recibido y la entregará al Usuario correspondiente, previa confirmación de la identidad del mismo y haciéndole firmar el documento de registro de entregas y las normas sobre uso de claves, que deberán ser archivadas. El responsable deberá mantener una copia (impresa o digital) del documento recibido vía mail.

ANEXO A - CERTIFICADO DIGITAL

INTRODUCCIÓN

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, permitiendo que estos gocen de una característica que únicamente era propia de los documentos en papel.

Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. La firma digital no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

La firma digital es un instrumento con características técnicas y normativas, esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

SOLICITUD DE CERTIFICADO DIGITAL PERSONAL

Para obtener un Certificado Digital deberá realizar el trámite a través de la **Subsecretaría de la Gestión Pública (SGP),** la cual, según el Decreto N° 409/2005, es la autoridad de aplicación del régimen normativo que establece la infraestructura de firma digital establecida en la Ley N° 25.506.

Para ello deberá acceder vía WEB al sitio http://ca.pki.gov.ar y cumplimentar el inicio del trámite, siguiendo los pasos establecidos en el mismo sitio.

Posteriormente deberá terminar el trámite presentándose personalmente, ante la Autoridad Certificante correspondiente (http://ca.pki.gov.ar/RARR.html).

El trámite es muy sencillo y totalmente asistido, contando también con soporte técnico brindado por la **Infraestructura de Firma Digital** (http://www.pki.gov.ar).

RENOVACIÓN DE CERTIFICADOS

Todos los certificados emitidos tienen un período de validez, por cuestiones de seguridad. Por esto, cada una de las personas responsables de la administración del sistema SLU en el organismo que se encuentren dentro de este período de

validez y su certificado no haya sido revocado, deberá renovar su certificado accediendo vía WEB al sitio http://ca.pki.gov.ar y cumplimentar los pasos ahí previstos para Renovación de Certificado Digital.

REVOCACIÓN DE CERTIFICADOS

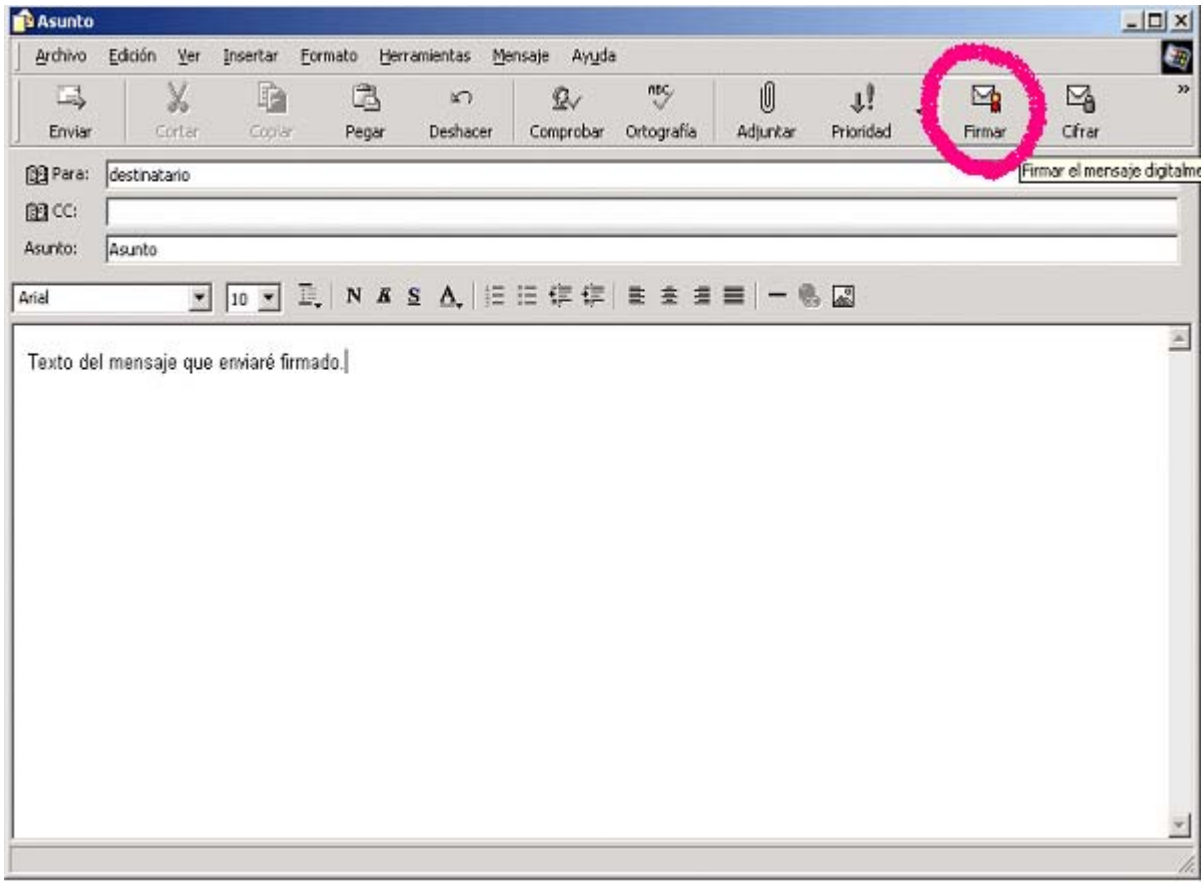
En el caso de que el período de validez del certificado haya sido cumplido, la persona responsable de la administración del sistema SLU en el organismo (suscriptor) deberá solicitar a la Autoridad Certificante la revocación de su certificado, accediendo vía WEB al sitio http://ca.pki.gov.ar y cumplimentar los pasos ahí previstos para Revocación de Certificado Digital.

INSTALACIÓN Y USO DEL CERTIFICADO DIGITAL

A continuación se describe cómo configurar su cliente de correo de modo que pueda utilizar el Certificado Digital. Las configuraciones varían dependiendo del producto que se esté utilizando, por lo tanto utilice las instrucciones que correspondan a su cliente de correo:

Outlook Express 5 / 5.5 / 6
Ingrese al menú [Herramientas] → [Cuentas...]. Seleccione en la solapa [Correo] el nombre de su cuenta de correo y luego presione [Propiedades]. Acceda a la solapa [Seguridad] y seleccione [Usar identificador digital ...]. Luego presione en [Identificador digital...] y seleccione su Certificado de Clave Pública y luego presione [Aceptar]. Cierre las pantallas presionando [Aceptar] y [Cerrar].

Para firmar digitalmente un correo electrónico redactar un mensaje y antes de enviarlo hacer un click en el menú de [Herramientas] y luego hacer click en el ítem [Firmar Digitalmente]. De esta forma se está indicando al cliente de correo que antes de enviar el mensaje lo firme digitalmente. Otra forma de firmar un mensaje es haciendo click antes de enviarlo en el ícono [Firmar] como se indica en la figura:



Si desea que por defecto todos los correos que se envíen salgan firmados, acceda al menú [Herramientas] → [Opciones...] y luego en la solapa de [Seguridad] seleccione [Firmar digitalmente todos los mensajes salientes]. Para finalizar presione [Aceptar].

Outlook 2000

Acceda al menú [Herramientas] → [Opciones...]. Accediendo a la solapa [Seguridad], seleccione [Cambiar configuración...] y luego en la sección [Certificados y algoritmos] presione [Elegir...]. Seleccione su Certificado de Clave Pública y luego presione [Aceptar]. Cierre las pantallas presionando [Aceptar].

Si desea que por defecto todos los correos que envíe salgan firmados, acceda al menú [Herramientas] → [Opciones...] y luego en la solapa de [Seguridad] seleccione [Agregar firma digital a los mensajes salientes]. Para finalizar presione [Aceptar].

Outlook XP

Acceda al menú [Herramientas] → [Opciones...]. Accediendo a la solapa [Seguridad], seleccione [Configuración...] y luego en la sección [Certificados y algoritmos] presione [Elegir...]. Seleccione su Certificado de Clave Pública y luego presione [Aceptar]. Cierre las pantallas presionando [Aceptar].

Si desea que por defecto todos los correos que envíe salgan firmados, acceda al menú [Herramientas] → [Opciones...] y luego en la solapa de [Seguridad] seleccione [Agregar firma digital a los mensajes salientes]. Para finalizar presione [Aceptar].

Netscape Messenger

Abra Netscape Navigator y utilizando la barra de navegación acceda a [Seguridad]. En la pantalla [Información sobre seguridad] seleccione [Messenger] de la lista que aparece en la parte izquierda. En la parte derecha seleccione [Certificado para sus mensajes firmados y cifrados] su certificado de clave pública. Si desea indicarle al cliente de correo que todos los correos que envíe salgan firmados seleccione la opción [Firmar mensajes de correo, cuando sea posible]. Cierre la pantalla presionando [Aceptar].

Para indicarle a Netscape que firme un mensaje digitalmente redacte un mensaje nuevo y una vez que el mensaje está listo para ser enviado, presione el botón [Opciones] y haga click en la opción [Firmado]. De esta forma, cuando envíe su correo electrónico éste va a salir firmado.

VERIFICACIÓN DE UNA FIRMA DIGITAL

La persona que recibe un mensaje firmado digitalmente podrá verificar la autenticidad de la firma siempre que cuente con un cliente de correo electrónico que soporte el manejo de certificados X.509 versión 3 (por ejemplo, Outlook Express 5 / 5.5 / 6 / 2000 / XP, Netscape Messenger 4.x / 7.0, Mozilla 1.5).

El procedimiento realizado por el cliente de correo al recibir un mensaje firmado es el siguiente: el receptor recibirá el mensaje en claro junto con la firma digital y el certificado de clave pública del firmante. El cliente de correo descifrará la firma digital utilizando la clave pública extraída del certificado en cuestión y obtendrá el valor de hash que calculó el emisor al momento de enviar el mensaje.
Por otra parte, utilizando el mismo algoritmo de hash que utilizó el emisor se lo aplicará al documento recibido y obtendrá otro valor de hash. Si ambos números de hash no coincidieran, entonces el mensaje ha sido alterado y el cliente de correo sabrá de esta situación informando al usuario mediante un mensaje de advertencia; si los números de hash coincidieran entonces el mensaje será íntegro.

La autoría del mensaje se corrobora gracias a que para poder obtener el número de hash calculado por el emisor fue necesario descifrar la firma digital con la clave pública que se corresponde con la única clave privada capaz de producir esa firma. Por lo tanto el propietario de esa clave pública, que es el que figura en el certificado recibido, es la única persona capaz de haber producido esa firma, ya que la vinculación entre la clave pública y el propietario está certificada por la Autoridad Certificante que emitió el certificado recibido.

Cabe aclarar que todos estos pasos son transparentes para el usuario, el cliente de correo los hace automáticamente.