PROCEDIMIENTO
ALTA, BAJA, REHABILITACION y DESBLOQUEO DE USUARIOS EN SISTEMAS ESIDIF, BI, SLU, UEPEX, BUDI, MCC, SIRHU DE LA SECRETARÍA DE HACIENDA

(PG-U-T-01 Rev.07)

INDICE

DESCRIPCIÓN....3

SOLICITUD POR COMUNICACIÓN OFICIAL (SISTEMA GDE)....3

REQUISITOS....3
PASOS PARA ENVIAR SOLICITUD POR COMUNICACIÓN OFICIAL (SISTEMA GDE)....3
- *ALTA DE USUARIO*....3
- *BAJA DE USUARIO*....3
- *REHABILITACIÓN DE USUARIO (CUENTA SISTEMA Ó CITRIX)*....3
- *DESBLOQUEO DE USUARIO (CUENTA SISTEMA Ó CITRIX)*....3

SOLICITUD POR CORREO ELECTRÓNICO....5

REQUISITOS....5
PASOS PARA ENVIAR SOLICITUD POR CORREO ELECTRÓNICO....5
- *ALTA DE USUARIO*....5
- *BAJA DE USUARIO*....5
- *REHABILITACIÓN DE USUARIO (CUENTA SISTEMA Ó CITRIX)*....5
- *DESBLOQUEO DE USUARIO (CUENTA SISTEMA Ó CITRIX)*....5

INSTRUCTIVO PARA COMPLETAR EL FORMULARIO DE SOLICITUD DE ACCESO....6

ALTA DE USUARIO....6
BAJA DE USUARIO....7
REHABILITACIÓN (CUENTA SISTEMA O CITRIX)....8
DESBLOQUEO (CUENTA SISTEMA O CITRIX)....10

ANEXO A - CERTIFICADO DIGITAL....12

INTRODUCCIÓN....12
SOLICITUD DE CERTIFICADO DIGITAL PERSONAL....12
RENOVACIÓN DE CERTIFICADOS....12
REVOCACIÓN DE CERTIFICADOS....12
INSTALACIÓN Y USO DEL CERTIFICADO DIGITAL....13
Outlook Express 5 / 5.5 / 6....13
Outlook 2000....14
Outlook XP....14
Mozilla Thunderbird....14
Verificación de una Firma Digital....14

Descripción
Procedimiento para solicitar el alta, baja, rehabilitación y desbloqueo de usuarios en el dominio de las aplicaciones: ESIDIF, BI, SLU, UEPEX, BUDI, MCC, SIRHU pertenecientes a la Dirección General de Sistemas Informáticos de Administración Financiera (DGSIAF) de la Secretaría de Hacienda y su habilitación en el sistema MCC perteneciente a la Oficina Nacional de Contrataciones (ONC)

Solicitud por Comunicación Oficial (Sistema GDE)

Requisitos
• El Director General de Administración ó Administrador Local en el Organismo/Institución debe tener **acceso al Sistema GDE** y **el Token USB** para la firma digital certificada (Más información), caso contrario deberá enviar la Solicitud vía correo electrónico al Centro de Atención a Usuarios de la DGSIAF. • Para poder validar los documentos PDF firmados digitalmente por el Sistema GDE, se requiere que el Acrobat Reader de los usuarios tenga instalado el certificado de la Autoridad certificante Raíz de la República Argentina.

Pasos para enviar Solicitud por Comunicación Oficial (Sistema GDE)

1 Para enviar una solicitud de alta, baja, rehabilitación y desbloqueo de usuarios en Sistemas de Administración Financiera, deberá descargarse el Formulario de solicitud correspondiente:

Formulario de Solicitud de Acceso a ESIDIF, BI, SLU, UEPEX, BUDI, MCC, SIRHU
Formulario de Solicitud de Acceso a UEPEX

2 Completar el Formulario ingresando los datos requeridos para cada tipo de acceso:

- ***Alta de usuario***
- ***Baja de usuario***
- ***Rehabilitación de usuario (cuenta Sistema ó citrix)***
- ***Desbloqueo de usuario (cuenta Sistema ó citrix)***

Nota: Diferentes tipos de Solicitudes de Acceso (alta, baja, rehabilitación, desbloqueo) pueden ser enviados en el mismo Formulario.

3 Ingresar al **Sistema GDE – Módulo CCOO**, y confeccionar una **NOTA (NO)**, indicando:

- **Referencia**: Solicitud Acceso Usuarios <OR | SAFxxx | UExxx>
- **Mensaje:** Informar un texto aclaratorio que describa el pedido.
- **Archivo embebido**: Añadir el Formulario con los datos requeridos en función al tipo de acceso.
- **Destinatario**: personal del Centro de Atención de Ayuda: Dirección de Ayuda a Usuarios (DAYAU#MHA), a saber:
  Juan Carlos Araujo, Marisol Moure, Diego Lavandera, Consuelo Gonzalo, Uriel

Pinieiro

Para facilitar el ingreso de los destinatarios puede copiar y pegar el listado de usuarios:
JCARAU,MMOURE,DLAVAN,CONGONZALO,UPINIE

4 El Director General de Administración o Administrador Local en el Organismo/Institución debe **firmar la Nota con Token USB**.

5 El Centro de Atención de Ayuda de la DGSIAF, ingresará un pedido en el Sistema de Gestión de Requerimientos, asociado a la solicitud e informará al solicitante el estado del pedido cuando sea requerido y al finalizar el mismo.

Ante algún inconveniente, informará al requirente los motivos por los cuales no es posible tramitar la solicitud.

Para dar respuesta a una nota enviada por el Centro de Atención de Ayuda, se recomienda continuar ésta última para que la nueva nota de respuesta quede asociada a la solicitud original.

6 Resueltas las solicitudes de alta y rehabilitación, el Director General de Administración o Administrador Local en el Organismo/Institución deberá ingresar a la aplicación Entrega de Claves para retirarlas.

Solicitud por correo electrónico

Requisitos
El Director General de Administración o Administrador Local en el Organismo/Institución: • Debe tener el Certificado de Firma Digital para firmar correos electrónicos, el cual deberá ser instalado en la computadora. Para hacer efectivo este requerimiento siga las instrucciones detalladas en el Anexo A - Certificado Digital. • No debe tener **acceso al Sistema GDE.**

Pasos para enviar Solicitud por correo electrónico

1 Para enviar una solicitud de alta, baja, rehabilitación y desbloqueo de usuarios en Sistemas de Administración Financiera, deberá descargarse el Formulario correspondiente:

Formulario de Solicitud de Acceso a ESIDIF, BI, SLU, UEPEX, BUDI, MCC, SIRHU
Formulario de Solicitud de Acceso a UEPEX

2 Completar el Formulario ingresando los datos requeridos para cada tipo de acceso:

- ***Alta de usuario***
- ***Baja de usuario***
- ***Rehabilitación de usuario (cuenta Sistema ó citrix)***
- ***Desbloqueo de usuario (cuenta Sistema ó citrix)***

Nota: Diferentes tipos de Solicitudes de Acceso (alta, baja, rehabilitación, desbloqueo) pueden ser enviados en el mismo Formulario.

3 Enviar al Centro de Atención de Ayuda de la DGSIAF un correo electrónico a la cuenta mesa@mecon.gov.ar. El correo debe enviarse con el Formulario adjunto y firmado digitalmente por el Director General de Administración o Administrador Local en el Organismo/Institución.

4 El Centro de Atención de Ayuda de la DGSIAF, ingresará un pedido en el Sistema de Gestión de Requerimientos, asociado a la solicitud e informará al solicitante el estado del pedido cuando sea requerido y al finalizar el mismo.

Ante algún inconveniente, informará al requirente los motivos por los cuales no es posible tramitar la solicitud.

5 Resueltas las solicitudes de alta y rehabilitación, el Director General de Administración o Administrador Local en el Organismo/Institución deberá ingresar a la aplicación Entrega de Claves para retirarlas.

Instructivo para completar el Formulario de Solicitud de Acceso

Alta de usuario

Descargar el Formulario correspondiente:

Formulario de Solicitud de Acceso a ESIDIF, BI, SLU, UEPEX, BUDI, MCC, SIRHU
Formulario de Solicitud de Acceso a UEPEX

Nota: Diferentes tipos de Solicitudes de Acceso (alta, baja, rehabilitación, desbloqueo) pueden ser enviados en el mismo Formulario.

ESIDIF, BI, SLU, BUDI, MCC, SIRHU

Tipo de Solicitud	Informar Alta para un **usuario final**, o Alta Admin para un **usuario administrador**.
Sistema	Informar el Sistema ESIDIF, BI, SLU, BUDI, MCC, SIRHU en el que se solicita el alta de usuario.
Organismo / SAF Nro./ Dominio Especial	Informar Organismo/SAF Nro./Dominio Especial al que pertenece el usuario
Nombre y Apellido	Informar nombre y apellido completo del usuario
Cuenta Usuario	No informar
Teléfono	Informar teléfono incluyendo interno
Correo electrónico	Informar una cuenta de correo electrónico
Tipo y Nº de documento	Informar Tipo y Nº de documento
VPN	Indicar **SI | NO** para conectarse al Sistema a través de Internet

UEPEX

Tipo de Solicitud	Informar Alta para un **usuario final**, o Alta Admin para un **usuario administrador**.
UEPEX Nº	Informar número de Uepex.
Tipo y Nº de proyecto	Informar Tipo y número de Proyecto
Nombre y Apellido	Informar nombre y apellido completo del usuario
Cuenta Usuario	En caso de pertenecer a otro Proyecto indicar la cuenta de usuario (uexxxyyy)
Teléfono	Informar teléfono incluyendo interno
Correo electrónico	Informar una cuenta de correo electrónico
Tipo y Nº de documento	Informar Tipo y Nº de documento
VPN	Indicar **SI | NO** para conectarse al Sistema a través de Internet

Baja de usuario

Descargar el Formulario correspondiente:

Formulario de Solicitud de Acceso a ESIDIF, BI, SLU, UEPEX, BUDI, MCC, SIRHU
Formulario de Solicitud de Acceso a UEPEX

Nota: Diferentes tipos de Solicitudes de Acceso (alta, baja, rehabilitación, desbloqueo) pueden ser enviados en el mismo Formulario.

ESIDIF, BI, SLU, BUDI, MCC, SIRHU

Tipo de Solicitud	Informar Baja para un **usuario final**, o Baja Admin para un **usuario administrador**.
Sistema	Informar el Sistema ESIDIF, BI, SLU, BUDI, MCC, SIRHU en el que se solicita la baja de usuario.
Organismo / SAF Nro./ Dominio Especial	Informar Organismo/SAF Nro./Dominio Especial al que pertenece el usuario
Nombre y Apellido	Informar nombre y apellido completo del usuario
Cuenta Usuario	Informar la cuenta a dar de baja. (Ejemplo sxxxyyy)
Teléfono	No informar
Correo electrónico	No informar
Tipo y Nº de documento	Informar Tipo y Nº de documento
VPN	No informar

UEPEX

Tipo de Solicitud	Informar Baja para un **usuario final**, o Baja Admin para un **usuario administrador**.
UEPEX Nº	Informar número de UEPEX.
Tipo y Nº de proyecto	Informar Tipo y número de Proyecto
Nombre y Apellido	Informar nombre y apellido completo del usuario
Cuenta Usuario	Informar la cuenta a dar de baja (uexxxyyy)
Teléfono	No informar
Correo electrónico	No informar
Tipo y Nº de documento	Informar Tipo y Nº de documento
VPN	No informar

Rehabilitación (cuenta Sistema o Citrix)

Descargar el Formulario correspondiente:

Formulario de Solicitud de Acceso a ESIDIF, BI, SLU, UEPEX, BUDI, MCC, SIRHU
Formulario de Solicitud de Acceso a UEPEX

Nota: Diferentes tipos de Solicitudes de Acceso (alta, baja, rehabilitación, desbloqueo) pueden ser enviados en el mismo Formulario.

ESIDIF, BI, SLU, BUDI, MCC, SIRHU

Tipo de Solicitud	Informar Rehabilitación para un **usuario final**, o Rehabilitación Admin para un **usuario administrador**.
Sistema	Informar el Sistema ESIDIF, BI, SLU, BUDI, MCC, SIRHU si se requiere rehabilitar la cuenta de acceso al sistema. Informar Citrix si se requiere rehabilitar la cuenta citrix.
Organismo / SAF Nro./ Dominio Especial	Informar Organismo/SAF Nro./Dominio Especial al que pertenece el usuario
Nombre y Apellido	Informar nombre y apellido completo del usuario
Cuenta Usuario	Informar la cuenta a rehabilitar (Ejemplo sxxxyyy)
Teléfono	No informar
Correo electrónico	No informar
Tipo y Nº de documento	No informar
VPN	No informar

UEPEX

Tipo de Solicitud	Informar Rehabilitación si se solicita la rehabilitación de un **usuario final**. Informar Rehabilitación Admin si se solicita la rehabilitación de un **usuario administrador**.
UEPEX Nº	Informar número de UEPEX.
Tipo y Nº de proyecto	Informar Tipo y número de Proyecto
Nombre y Apellido	Informar nombre y apellido completo del usuario
Cuenta Usuario	Informar la cuenta a rehabilitar (uexxxyyy)
Teléfono	No informar
Correo electrónico	No informar
Tipo y Nº de documento	No informar
VPN	No informar

Más información

La **rehabilitación** de una cuenta genera una nueva clave de acceso.

La **rehabilitación de cuentas** (de acceso al Sistema ó cuenta Citrix) **de usuarios SLU ó Uepex** debe ser realizada por el administrador local SLU o Uepex activo. Si no hay administrador local activo entonces se deberá enviar la solicitud al Centro de Atención de Ayuda de la DGSIAF.

La **rehabilitación de la cuenta de acceso Sistema eSidif** la realiza el Administrador Local, excepto la rehabilitación de la cuenta propia del Administrador Local eSidif

La **rehabilitación de la cuenta de acceso Sistema eSidif** la realiza el Administrador Local. La **rehabilitación de un administrador local eSidif** la puede realizar otro administrador local. Si no hay administrador local activo entonces se deberá enviar la solicitud al Centro de Atención de Ayuda de la DGSIAF.

Desbloqueo (cuenta Sistema o Citrix)

Descargar el Formulario correspondiente:

Formulario de Solicitud de Acceso a ESIDIF, BI, SLU, UEPEX, BUDI, MCC, SIRHU
Formulario de Solicitud de Acceso a UEPEX

Nota: Diferentes tipos de Solicitudes de Acceso (alta, baja, rehabilitación, desbloqueo) pueden ser enviados en el mismo Formulario.

ESIDIF, BI, SLU, BUDI, MCC, SIRHU

Tipo de Solicitud	Informar Desbloqueo para un **usuario final**, o Desbloqueo Admin para un **usuario administrador**.
Sistema	Informar el Sistema ESIDIF, BI, SLU, BUDI, MCC, SIRHU si se requiere desbloquear la cuenta de acceso al sistema. Informar Citrix si se requiere rehabilitar la cuenta citrix.
Organismo / SAF Nro./ Dominio Especial	Informar Organismo/SAF Nro./Dominio Especial al que pertenece el usuario
Nombre y Apellido	Informar nombre y apellido completo del usuario
Cuenta Usuario	Informar la cuenta a desbloquear (Ejemplo sxxxyyy)
Teléfono	No informar
Correo electrónico	No informar
Tipo y Nº de documento	No informar
VPN	No informar

UEPEX

Tipo de Solicitud	Informar Desbloqueo para un **usuario final**, o Desbloqueo Admin para un **usuario administrador**.
UEPEX Nº	Informar número de UEPEX.
Tipo y Nº de proyecto	Informar Tipo y número de Proyecto
Nombre y Apellido	Informar nombre y apellido completo del usuario
Cuenta Usuario	Informar la cuenta a desbloquear (uexxxyyy)
Teléfono	No informar
Correo electrónico	No informar
Tipo y Nº de documento	No informar
VPN	No informar

Más información
Una cuenta se bloquea por superar la cantidad de intentos fallidos permitidos. El **desbloqueo** de la cuenta no altera la clave actual del usuario. El **desbloqueo de cuentas** (de acceso al Sistema ó cuenta Citrix) **de usuarios SLU ó Uepex** debe ser realizada por el administrador local SLU o Uepex activo. Si no hay administrador local activo entonces se deberá enviar la solicitud al Centro de Atención de Ayuda de la DGSIAF. El **desbloqueo de la cuenta de acceso Sistema eSidif** la realiza el Administrador Local, excepto el desbloqueo de la cuenta propia del Administrador Local eSidif El **desbloqueo de la cuenta de acceso Sistema eSidif** la realiza el Administrador Local. El **desbloqueo de un administrador local eSidif** la puede realizar otro administrador local. Si no hay administrador local activo entonces se deberá enviar la solicitud al Centro de Atención de Ayuda de la DGSIAF.

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 **Secretaría 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 https://pki.jgm.gov.ar/app/ 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.

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 https://pki.jgm.gov.ar/app/ y cumplimentar los pasos ahí previstos para Renovación de Certificado Digital.

Revocación de Certificados

De acuerdo con lo establecido en la política de Certificación de la Autoridad Certificante de la ONTI, un suscriptor debe solicitar la inmediata revocación de su certificado en los siguientes casos:

a) Cuando se produzcan cambios en la información que el certificado contiene o ésta se desactualice.
b) Cuando la clave privada asociada al certificado de clave pública, o el medio en que se encuentre almacenada, se encuentren comprometidos o corran peligro de estarlo.
c) Cuando cese su vínculo laboral con el organismo, dependencia o institución.

Para esto, el titular del certificado deberá solicitar a la Autoridad Certificante la revocación de su certificado, accediendo vía WEB al sitio https://pki.jgm.gov.ar/app/ y cumplimentar los pasos ahí previstos para Revocación de Certificado Digital.

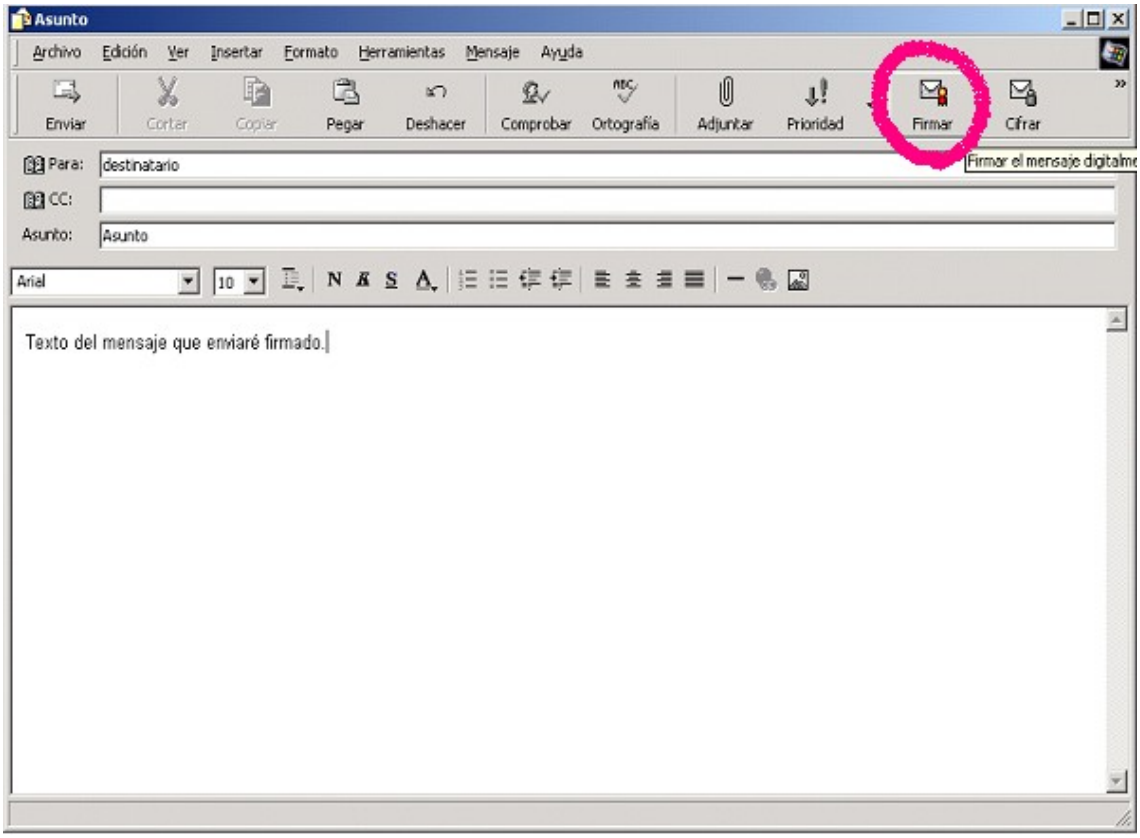
Instalación y Uso del Certificado Digital

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].

Mozilla Thunderbird

Primero debe tramitar el certificado desde su navegador (ya sea Internet Explorer, firefox u otro) y exportarlo en formato #pkcs12. Hecho esto, en Thunderbird debe ir al menú [Herramientas] → [Opciones...], acceder a la solapa [Certificados] y elegir la opción [Ver Certificados]. En esa opción, elegir [Certificados Propios] -> [Importar] y luego indicar la carpeta en la que almaceno el certificado (y la clave privada) que exportó desde el navegador.
Una vez que importó su certificado en su cliente de correo Mozilla Thunderbird, debe configurar este último para poder enviar sus e-mails firmados digitalmente con el certificado recién importado. Para ello debe acceder al menú [Herramientas] / [Tools] y luego al ítem [Cuentas] / [Account settings]. Se abrirá un cuadro de diálogo y sobre el panel izquierdo encontrará escrita la cuenta de correo que está configurando, presionando el nodo con el signo [+] que está a la izquierda se desplegarán una serie de categorías. Seleccione el ítem [Seguridad] / [Security], sobre la derecha podrá visualizar un área de configuración con la leyenda [Firma Digital] / [Digital Signing], dentro de esa area presione el botón con el rótulo [Seleccionar] / [Select]. Al presionar el botón se abrirá un cuadro de diálogo con un cuadro de lista con la leyenda [Certificado] / [Certificate] el cual le permitirá seleccionar el certificado que desea utilizar. Elija el certificado y presione [Aceptar] / [OK], luego vuelva a presionar [Aceptar] / [OK] para salir del cuadro de configuración.
Para enviar un mail firmado digitalmente, redacte el mail y antes de enviarlo, sobre la parte superior del cuadro de redacción podrá visualizar un ícono con un candado con el rótulo [Seguridad] / [Security], presione la flecha que está sobre la derecha del ícono, aparecerá un menú contextual con varias opciones. Seleccione la opción [Firma digitalmente] / [Digitally Sign This Message] para enviar el mail firmado digitalmente, por último presione [Enviar] / [Send] para enviar el mensaje.

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, Mozilla Thunderbird 2.x).

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 realiza automáticamente.