PROCEDIMIENTO ALTA, BAJA Y REHABILITACIÓN DE ADMINISTRADORES

EN SISTEMAS SLU, ESIDIF y GESUS

DE LA SECRETARÍA DE HACIENDA

(PG-U-T-01 Rev.09)

ÍNDICE

Descripción
Procedimiento para solicitar el alta, baja y rehabilitación de Administradores en el dominio de las aplicaciones SLU, ESIDIF (Administración Local de ESIDIF, BI y Aplicaciones del Portal DGSIAF) y GESUS (Administración de usuarios VPN y CITRIX), pertenecientes a la Dirección General de Sistemas Informáticos de Administración Financiera (DGSIAF) de la Secretaría de Hacienda.

Solicitud por Comunicación Oficial (Sistema GDE)

Requisitos
• El Director General de Administración, su equivalente, o el Administrador Local vigente 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 (Más información).

Pasos para enviar Solicitud por Comunicación Oficial (Sistema GDE)

1 Para enviar una solicitud de alta, baja y/o rehabilitación de Administradores en los Sistemas de Administración Financiera, deberá descargarse el Formulario de solicitud correspondiente: **Formulario de Solicitud de Acceso a Sistemas Informáticos de Administración Financiera.**

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

- Alta de Administrador
- Baja de Administrador
- Rehabilitación de Administrador (cuenta Sistema y/o Citrix)

Nota: Diferentes tipos de Solicitudes de Acceso (alta, baja, rehabilitación) 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 a Usuarios de la Dirección de Análisis y Atención a Usuarios (DAYAU#MEC), a saber:
  Uriel Piñeiro, María Paula Alvarez, Laura Apat, Diego Lavandera, Consuelo Gonzalo, María Paz Sagardoy, Cecilia María Giusti, Lucas Casagrande, María Graciela Pollio, María Soledad Sammartino, Romina Apat, Juan Carlos Rodilla, Silvana Amadeo.

  Para facilitar el ingreso de los destinatarios puede copiar y pegar el listado de usuarios:
  UPINIE, MPALVA, LAPAT, DLAVAN, CONGONZALO, MPSAGA, CGIUSTI, LCASAG, GPOLLI, MSAMMARTINO, RAPAT, JRODILL, SILAMADEO

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

5 El Centro de Atención a Usuarios 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 a Usuarios, 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, su equivalente, o el 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, su equivalente, o el Administrador Local vigente en el Organismo/Institución:

- No tiene implementado el Sistema GDE o éste se encuentra caído.
- Debe tener instalado en su computadora el Certificado de Firma Digital para firmar correos electrónicos. Para hacer efectivo este requerimiento siga las instrucciones detalladas en el Anexo A - Certificado Digital.

Pasos para enviar Solicitud por correo electrónico

1 Para enviar una solicitud de alta, baja y/o rehabilitación de Administradores en los Sistemas de Administración Financiera, deberá descargarse el Formulario de solicitud correspondiente:
Formulario de Solicitud de Acceso a Sistemas Informáticos de Administración Financiera.

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

- Alta de Administrador
- Baja de Administrador
- Rehabilitación de Administrador (cuenta Sistema y/o Citrix)

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

3 Enviar al Centro de Atención a Usuarios 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, su equivalente, o el Administrador Local vigente en el Organismo/Institución.

4 El Centro de Atención a Usuarios 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, su equivalente, o el 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 Administrador

Descargar el Formulario correspondiente:

Formulario de Solicitud de Acceso a Sistemas Informáticos de Administración Financiera.

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

SLU, ESIDIF, GESUS

Tipo de Solicitud	Informar Alta Admin.
Sistemas	Informar los Sistemas (SLU, ESIDIF/GESUS o UEPEX/GESUS) en los que se solicita la administración
Organismo | SAF Nro. | Dominio Acceso Especial	Informar Organismo, Nro. SAF o Dominio especial
Tipo y Nº de Proyecto UEPEX	Informar Tipo y N° de Proyecto UEPEX para Alta Admin. UEPEX/GESUS
Nombre y Apellido	Informar nombre y apellido completo del usuario
DNI	Informar Tipo y N° de documento sin puntos
Teléfono e interno	Informar teléfono laboral, incluyendo interno
Correo electrónico	Informar una cuenta de correo electrónico institucional
CUIL/CUIT/CDI	Informar CUIL/CUIT/CDI para Alta Administrador ESIDIF

Baja de Administrador

Descargar el Formulario correspondiente:

Formulario de Solicitud de Acceso a Sistemas Informáticos de Administración Financiera.

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

SLU, ESIDIF, GESUS

Tipo de Solicitud	Informar Baja Rol Admin. ó Baja total Admin. según si se requiere sólo quitar el rol de Administrador o la baja total como usuario
Sistemas	Informar los Sistemas (SLU, ESIDIF/GESUS o UEPEX/GESUS) en los que se solicita la baja
Organismo | SAF Nro. | Dominio Acceso Especial	Informar Organismo, Nro. SAF o Dominio especial
Tipo y Nº de Proyecto UEPEX	Informar Tipo y N° de Proyecto UEPEX para Baja Admin. UEPEX/GESUS
Nombre y Apellido	Informar nombre y apellido completo del usuario
DNI	Informar Tipo y N° de documento sin puntos
Teléfono e interno	No informar
Correo electrónico	No informar
CUIL/CUIT/CDI	No informar

Rehabilitación (cuenta Sistema y/o Citrix)

Descargar el Formulario correspondiente:

Formulario de Solicitud de Acceso a Sistemas Informáticos de Administración Financiera.

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

SLU, ESIDIF, VPN/CITRIX

Tipo de Solicitud	Informar Rehabilitación Admin.
Sistemas	Informar el Sistema y/o acceso (SLU, ESIDIF y/o VPN/Citrix) en el que se solicita la rehabilitación
Organismo | SAF Nro. | Dominio Acceso Especial	Informar Organismo, Nro. SAF o Dominio especial
Tipo y Nº de Proyecto UEPEX	Informar Tipo y N° de Proyecto UEPEX para Rehabilitación Admin. UEPEX/GESUS
Nombre y Apellido	Informar nombre y apellido completo del usuario
DNI	Informar Tipo y N° de documento sin puntos
Teléfono e interno	Informar teléfono laboral, incluyendo interno
Correo electrónico	Informar una cuenta de correo electrónico institucional
CUIL/CUIT/CDI	Informar CUIL/CUIT/CDI para Rehabilitación Administrador ESIDIF

Más información

La **rehabilitación** de una cuenta genera una nueva clave de acceso, mientras que el **desbloqueo** no la modifica.

El **alta, baja, rehabilitación y desbloqueo de usuarios** en los Sistemas ESIDIF o SLU debe ser realizado por el administrador local activo del organismo **desde dichos sistemas**. Si no hay administrador local activo, se deberá enviar la solicitud al Centro de Atención a Usuarios de la DGSIAF.

Tanto la **rehabilitación de cuentas Citrix y VPN,** como la asignación de **íconos de los sistemas** debe ser realizado por el administrador local activo desde la aplicación **GESUS**.

La **rehabilitación y/o desbloqueo de un administrador local** en el Sistema ESIDIF y/o el acceso Citrix puede ser realizado por otro administrador local activo del organismo, desde ESIDIF y/o GESUS, respectivamente. Si no hay administrador local activo, se deberá enviar la solicitud al Centro de Atención a Usuarios de la DGSIAF.

El **alta, rehabilitación y/o desbloqueo de un Administrador SLU** puede ser realizado por otro Administrador SLU. Si no hay Administrador SLU activo en el organismo, se deberá enviar la solicitud al Centro de Atención a Usuarios de la DGSIAF.

Quedará automáticamente **inhabilitado** por el sistema el usuario que no ingrese al mismo en un período de **60 días corridos**. A los **90 días** de producirse la inhabilitación, de no haberse realizado la **rehabilitación**, el usuario se dará de baja.

Asimismo, se **bloqueará** el usuario que no haya cambiado su clave durante el período máximo sugerido (**90 días**) y el usuario que tenga **cinco** intentos de ingreso fallidos consecutivos (en este caso se desbloqueará automáticamente a los **15 minutos**).

Los pedidos de alta, baja, modificación y rehabilitación de usuarios en el sistema **SCG** (Sidif Central Gráfico), deben solicitarse a la Dirección de Normas y Sistemas de la CONTADURÍA GENERAL DE LA NACIÓN enviando una copia del Formulario de Solicitud de Accesos al SIDIF mediante nota o correo electrónico a la cuenta sapicgn@mecon.gov.ar. Ver sitio de la Contaduría General de la Nación, Normativas, Disposición Número 5 de 2003.

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 2010

Acceda al menú [Archivo] → [Opciones...]. Accediendo a la solapa [Centro de confianza], seleccione [Configuración del Centro de confianza...], luego en la pestaña [Seguridad del Correo Electrónico] presione [Configuración...]. Seleccione un nombre para identificar el certificado y presione [Elegir]. Seleccione su Certificado y luego presione [Aceptar] en todas las ventanas abiertas. Ver instructivo AQUI.

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 2010 y Thunderbird).

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.