



Banco de la República
Bogotá D. C., Colombia

Subgerencia de Informática
Unidad de Protección y Continuidad Informática

NOVEDADES Y ADMINISTRACION DE USUARIOS SEBRA
UPCI-CDS-GI-3

31 de Octubre de 2007
Versión 1.0



TABLA DE CONTENIDO

1	INTRODUCCIÓN	3
2	ADMINISTRACIÓN DE USUARIOS	4
3	DILIGENCIAMIENTO DEL FORMATO “NOVEDADES USUARIOS SEBRA”.....	6
3.1	INFORMACIÓN BÁSICA DE LA ENTIDAD AUTORIZADA SOLICITANTE	7
3.2	NOVEDADES DE USUARIO	7
3.3	NOVEDADES DE TOKEN OTP.....	8
3.4	OBSERVACIONES.....	10
3.5	INFORMACIÓN OBLIGATORIA	10
3.6	RECOMENDACIONES	10
3.7	ESPACIO RESERVADO PARA EL CENTRO DE SOPORTE INFORMÁTICO.....	10
4	CONDICIONES PARA EL ENVÍO DE SOLICITUDES CON PKI.....	11
4.1	NOVEDADES DE USUARIO SISTEMA SEBRA.....	11
4.1.1	Firma Digital	11
4.1.2	Formato del archivo	11
4.1.3	Nombre del archivo.....	11
4.1.4	Envío del archivo	12
4.1.5	Información del archivo.....	12
4.2	AUTORIZACIÓN DE RETIRO DE TOKEN OTP.....	12
4.2.1	Firma Digital	12
4.2.2	Formato del archivo	12
4.2.3	Nombre del archivo.....	13
4.2.4	Envío del archivo	13
4.2.5	Entrega de Token OTP	13
5	CONSIDERACIONES ADICIONALES DEL SERVICIO	14
5.1	RESPUESTA A LA SOLICITUD Y ENTREGA DE TOKEN OTP	14
5.1.1	Validación de condiciones de solicitud y firma digital	14
5.1.2	Pruebas de Ingreso	14
5.2	ENTREGA DE TOKEN OTP	15
5.3	PÉRDIDA DE TOKEN.....	15
5.4	COBRO DE TOKEN OTP	16



1 INTRODUCCIÓN

Con el propósito de brindar un servicio ágil, eficiente y seguro en cuanto a la administración de los servicios electrónicos del Banco de la República - SEBRA, el presente documento describe los requisitos que deben cumplir las solicitudes que realizan las Entidades Autorizadas a través de su delegado con responsabilidad administrativa por medio de PKI para el trámite de novedades, tales como: incluir, modificar, retirar usuarios y/o servicios, adicionar servicio, reasignar Token OTP¹, blanqueo de PIN, revisión Token, solicitud de PIN manual y reposición por pérdida.

Cada una de las Entidades Autorizadas que desee hacer uso de los servicios a los que puede acceder a través del sistema SEBRA, deberá definir los usuarios para cada servicio (personas naturales) a los cuales se les asignará un nombre de usuario y un Token OTP (dispositivo de seguridad, personal e intransferible, que le permitirá autenticarse al ingreso del sistema).

¹ OTP: One Time Password



2 ADMINISTRACIÓN DE USUARIOS

Para dar trámite a cualquier solicitud de novedades de usuario, la Entidad Autorizada debe enviar, a través del delegado PKI nombrado por el representante legal de la Entidad Autorizada, el formato denominado “NOVEDADES DE USUARIOS SEBRA”; debidamente diligenciado, el cual se encuentra disponible en la página web² del Banco. La solicitud deberá enviarse por medio de correo electrónico firmado (no encriptado) con certificado PKI al buzón de correo electrónico novedadsebra@banrep.gov.co.

Las novedades que puede solicitar una Entidad Autorizada son:

1. Novedades de Usuario:

- Incluir Usuario
- Retiro Definitivo de Usuario
- Modificar Servicio
- Retirar Servicio
- Adicionar Servicio

2. Novedades de Token OTP:

- Blanqueo de Pin
- Revisión

² http://www.banrep.gov.co/sistema-financiero/seb_sebra.htm#Formatos



- Reasignación
- Reposición por pérdida

Es importante aclarar que a un mismo usuario se le puede asociar más de un servicio. Así mismo, se debe tener en cuenta que los servicios y perfiles, NO están ligados al Token OTP sino al nombre de usuario. Por tanto, cualquier modificación o adición en este sentido no implica cambio del dispositivo.



3 DILIGENCIAMIENTO DEL FORMATO “NOVEDADES DE USUARIOS SEBRA”

El formato denominado “NOVEDADES DE USUARIOS SEBRA” ha sido diseñado para permitir a las Entidades Autorizadas solicitar las novedades mencionadas en el punto anterior en un solo documento. Como tal, tiene carácter de documento oficial para cualquier requerimiento, por tanto, para que sea válido, además de cumplir con los requisitos de seguridad y validación, la Entidad Autorizada DEBE hacer sus solicitudes exclusivamente a través de este medio.

Este formato podrá ser actualizado de acuerdo a las necesidades de cada sistema. A partir de su publicación, se anula cualquier versión anterior del documento. Así mismo, este documento NO DEBE SER MODIFICADO NI ALTERADO en ninguno de sus campos ya que esto implica su anulación inmediata.

A continuación se relaciona una breve descripción de cada campo (todos los campos son **obligatorios** a excepción de aquellos marcados como “Espacio Reservado” para el Centro de Soporte Informático). Para la oportuna atención de la solicitud, el formato debe ser completamente diligenciado y cumplir con todos los requisitos establecidos.

El formato está dividido en varias secciones a saber:

- Información básica de la Entidad Autorizada
- Usuarios
- Token OTP



- Observaciones
- Información del delegado PKI solicitante
- Recomendaciones
- Espacio reservado para el Centro de Soporte Informático

3.1 INFORMACIÓN BÁSICA DE LA ENTIDAD AUTORIZADA SOLICITANTE

- **Nombre:** Escribir el nombre completo de la Entidad Autorizada
- **NIT:** Escribir el NIT de la entidad, incluyendo el dígito de verificación.
- **Teléfono y fax:** Escribir un número de teléfono y un fax en el cual se pueda contactar al solicitante.

3.2 NOVEDADES DE USUARIO

Marque una SOLA “X” en el tipo de novedad que requiera por usuario según se describe a continuación:

- **Incluir Usuario:** Marcar este campo cuando requiera incluir a un nuevo usuario, teniendo en cuenta que para acceder al Sistema SEBRA todo usuario requiere de un Token OTP y que su inclusión implica, tal como se especifica en el formato, la asignación de este dispositivo y cuyo valor debe ser asumido por la Entidad Autorizada.
- **Retiro Definitivo de Usuario:** Marcar este campo cuando requiera retirar un usuario. Esta opción implica la eliminación total del usuario y servicios asociados relacionados en el formato; adicionalmente, el Token OTP que tenga asociado el usuario se libera.
- **Retirar Servicio:** Marcar este campo cuando requiera retirar uno o más servicios asociados a un usuario sin que implique su retiro definitivo del sistema; si el servicio que



se desea retirar es el único que el usuario tiene asociado, se debe optar por el retiro definitivo de usuario.

- **Adicionar Servicio:** Marcar este campo cuando requiera adicionar uno o más servicios para un usuario. Esta novedad mantiene en idénticas condiciones los demás servicios asociados previamente.

- **Nombres y Apellidos Completos:** Se debe escribir el nombre completo del usuario que trabajará en el sistema. **ESTA INFORMACIÓN ES DE VITAL IMPORTANCIA PUES DE ESTE DATO DEPENDE LA CONSTRUCCIÓN DEL NOMBRE DE USUARIO QUE SE ASIGNE PARA INGRESAR AL SISTEMA.**

- **Cédula de Ciudadanía:** Escribir el número de cédula del usuario que trabajará en el sistema. Este dato es importante para la creación e identificación del usuario en la base de datos de usuarios.

- **Ciudad:** Especificar el nombre de la ciudad donde está ubicado el usuario que trabajará en el sistema.

- **Servicios:** Se debe marcar con una “X” el(los) servicio(s) que se requiera(n) para el usuario relacionado en el formato. Tener en cuenta las opciones de perfiles que se presentan para cada uno de los servicios y seleccionar la que se ajuste a las necesidades y funciones que cumplirá.

3.3 NOVEDADES DE TOKEN OTP

Marque una SOLA “X” en el tipo de novedad que requiera para cada Token OTP según se describe a continuación:

- **Token OTP Serial No.:** En este campo se debe relacionar el serial del Token OTP que será objeto de la novedad. Este serial se encuentra en la parte posterior del dispositivo y corresponde a un número de ocho dígitos.



- **Blanqueo de PIN:** Marcar esta opción cuando requiera definir un nuevo PIN para el usuario.

- **Revisión Token OTP:** Marcar esta opción si ante eventuales inconvenientes de acceso o daño lógico, el usuario requiere su revisión. Es importante tener en cuenta, que el dispositivo deberá remitirse al Centro de Soporte Informático, mediante carta haciendo referencia a la solicitud electrónica previamente enviada por correo electrónico, para así realizar la revisión, emitir un diagnóstico sobre el daño o inconveniente y determinar si es objeto de reposición por garantía o no. **ES IMPORTANTE MENCIONAR QUE ESTOS DISPOSITIVOS ESTÁN FABRICADOS EN UN MATERIAL COMPACTO DE ALTA RESISTENCIA, CUALQUIER DAÑO FÍSICO SERÁ ATRIBUIBLE A MAL USO POR PARTE DEL USUARIO FINAL Y POR TAL MOTIVO SU REPOSICIÓN DERÁ RESPONSABILIDAD DE LA ENTIDAD AUTORIZADA. EN CASO DE DAÑO FÍSICO NO ES NECESARIO REMITIR EL DISPOSITIVO AL CENTRO DE SOPORTE.**

- **Reasignación:** Marcar esta opción cuando la Entidad Autorizada requiera reasignar el(los) dispositivo(s) según sus necesidades. Deberá relacionar el número serial del Token OTP a reasignar y los datos, tanto del usuario actual como del nuevo usuario. **IMPORTANTE:** Adicionalmente, deberá relacionar la inclusión y/o retiro definitivo de los usuarios objeto de la reasignación

- **Reposición Token OTP**
 - **Por pérdida:** Marcar esta opción si la Entidad Autorizada requiere reponer el(los) dispositivo(s). Adicionalmente, se debe remitir al Centro de Soporte Informático el original de la constancia juramentada del denuncia por pérdida.

- **Nombres y Apellidos Completos (Usuario para retirar):** Escribir el nombre completo del usuario que en el momento de la solicitud tiene asignado el Token OTP.



• **Nombres y Apellidos Completos (Usuario para incluir):** Escribir el nombre completo del usuario a incluir en el sistema SEBRA y que reemplazará al usuario relacionado en el campo anterior.

3.4 OBSERVACIONES

En este campo, la Entidad Autorizada podrá enunciar cualquier comentario que considere pertinente para la atención de la solicitud.

3.5 INFORMACIÓN OBLIGATORIA

En esta sección del formato se debe especificar quien realiza o autoriza la solicitud.

• **Nombre y Cargo del Delegado Solicitante:** Escribir el nombre completo y cargo del delegado PKI con responsabilidad administrativa que firma la solicitud.

• **Correo Electrónico:** Es **OBLIGATORIO** relacionar el buzón de correo electrónico del delegado remitente, preferiblemente de carácter corporativo, para envío de respuesta a la solicitud. El delegado deberá garantizar la seguridad y confiabilidad de dicho buzón.

3.6 RECOMENDACIONES

En esta sección del formato se relacionan algunos apartes importantes a tener en cuenta al momento de realizar la solicitud de novedades. Se sugiere leerla y tomar atenta nota de la información contenida en ella.

3.7 ESPACIO RESERVADO PARA EL CENTRO DE SOPORTE INFORMÁTICO

Esta sección del formato es de uso exclusivo para Centro de Soporte Informático y NO debe ser diligenciada ni modificada.



4 CONDICIONES PARA EL ENVÍO DE SOLICITUDES CON PKI

4.1 NOVEDADES DE USUARIO SISTEMA SEBRA

Cada solicitud enviada deberá cumplir con las siguientes condiciones de formato y seguridad:

4.1.1 *Firma Digital*

Cada archivo enviado deberá ser FIRMADO con el certificado digital PKI del delegado autorizado; NO DEBERÁ ENCRIPTARSE.

Únicamente será válida la firma de uno de los delegados plenamente autorizados; de no cumplirse con esta condición, la solicitud será rechazada y devuelta vía correo electrónico al remitente.

4.1.2 *Formato del archivo*

El formato original del documento es Excel. Posterior a la firma digital, el sistema PKI convertirá el archivo al formato seguro de entrust (.ent) y cambiará el icono original; éste último será el ÚNICO archivo que se recibirá vía correo electrónico; de no cumplirse con esta condición, la solicitud será rechazada y devuelta vía correo electrónico al remitente.

4.1.3 *Nombre del archivo*

El nombre de cada archivo debe conservar el siguiente estándar:

00000-AAAAMMDD-0X.xls.ent



Donde: 00000: corresponde al código de intermediario SEBRA de la entidad.

AAAAMMDD: corresponde a la fecha de solicitud.

0X: corresponde a un consecutivo de archivo que cada delegado deberá llevar y comenzará en 01.

4.1.4 Envío del archivo

El archivo deberá ser enviado únicamente al buzón de correo electrónico novedadsebra@banrep.gov.co; cualquier solicitud enviada a buzones diferentes no será atendida.

4.1.5 Información del archivo

La información contenida en cada archivo se revisará posterior al proceso de validación de seguridad PKI mencionado; por tanto, se aclara que aunque dichas condiciones sean validadas correctamente, no se garantizará la atención de la novedad si la información suministrada en el formato no es clara, completa y veraz.

4.2 AUTORIZACIÓN DE RETIRO DE TOKEN OTP

Cada solicitud enviada deberá cumplir con las siguientes condiciones de formato y Seguridad,

4.2.1 Firma Digital

Aplican las mismas condiciones del numeral 3.1.1.

4.2.2 Formato del archivo

Aplican las mismas condiciones del numeral 3.1.2.



4.2.3 *Nombre del archivo*

El nombre de cada archivo debe conservar el siguiente estándar:

AUT-00000-AAAAMMDD.xls.ent

Donde: AUT serán las siglas que indican el proceso; siempre iniciará con esta.

00000: corresponde al código de intermediario SEBRA de la entidad.

AAAAMMDD: corresponde a la fecha de solicitud.

4.2.4 *Envío del archivo*

Aplican las mismas condiciones del numeral 3.1.4.

4.2.5 *Entrega de Token OTP*

El funcionario autorizado deberá presentar su cédula de ciudadanía para validar la información previamente.



5 CONSIDERACIONES ADICIONALES DEL SERVICIO

5.1 RESPUESTA A LA SOLICITUD Y ENTREGA DE TOKEN OTP

El grupo de Administración de Usuarios SEBRA dará respuesta al Delegado PKI de la atención de su solicitud vía correo electrónico. El tiempo de atención de toda solicitud será de máximo tres (3) días hábiles contados a partir de la fecha de recibo.

5.1.1 *Validación de condiciones de solicitud y firma digital*

Este procedimiento es vital para validar la información del solicitante, debe cumplirse para poder atender los requerimientos.

Dicha solicitud será validada de acuerdo con las especificaciones mencionadas en el numeral 3 de este documento.

De presentarse algún inconveniente con la validación, la solicitud será devuelta mediante correo electrónico al remitente, informando la razón por la cual se rechaza y las indicaciones necesarias.

5.1.2 *Pruebas de Ingreso*

El usuario final deberá comunicarse, si lo requiere, con el Centro de Soporte Informático, al teléfono 3431000, para solicitar la respectiva asesoría según el caso.



5.2 ENTREGA DE TOKEN OTP

En cualquiera de los casos (Bogotá o sucursal), el Delegado PKI deberá diligenciar el formato denominado “AUTORIZACIÓN RETIRO DE TOKEN OTP” publicado en la página web³ del Banco, indicando los datos personales del funcionario autorizado para retirar el(s) Token(s) OTP; deberá firmarlo con su certificado PKI y enviarlo vía correo electrónico a la cuenta novedadsebra@banrep.gov.co. El funcionario autorizado deberá presentar su cédula de ciudadanía al momento de retirar el Token OTP en las oficinas del Banco de la República, en Bogotá o sucursal correspondiente.

La entrega de los Tokens OTP se realiza mediante Acta de Entrega firmada por las partes (Banco de la República y funcionario autorizado por la Entidad). Dicho documento representa la aceptación de recibo y cobro por concepto de adquisición y/o reposición de los Tokens OTP cuando éste aplique.

5.3 PÉRDIDA DE TOKEN

En caso de pérdida de un Token OTP, el delegado PKI deberá dar aviso inmediato mediante correo electrónico firmado con PKI al buzón novedadsebra@banrep.gov.co, para proceder a su bloqueo; de lo contrario la Entidad Autorizada asume todos los riesgos asociados. Si la Entidad Autorizada requiere la reposición por pérdida de un Token OTP deberá tramitarlo según el procedimiento descrito en el numeral 2.3.

Cuando los Tokens OTP cumplan su vida útil, de acuerdo a la fecha impresa en el respaldo del dispositivo, la Entidad Autorizada podrá solicitar nuevos dispositivos mediante carta firmada por el delegado PKI al buzón de correo novedadsebra@banrep.gov.co. En dicha comunicación deberá solicitarse la reposición por vencimiento de los Tokens OTP requeridos, relacionando número serial y usuario asignado. ES IMPORTANTE QUE EL DELEGADO PKI EXPRESE

³ http://www.banrep.gov.co/sistema-financiero/seb_sebra.htm#aspectos



EXPLÍCITAMENTE QUE TIENE CONOCIMIENTO Y ACEPTA EL COBRO QUE POR CONCEPTO DE LA ENTREGA DEL (LOS) NUEVO(S) TOKEN(S) OTP SE REALIZARÁ.

5.4 COBRO DE TOKEN OTP

El cobro de Tokens OTP, y los correspondientes impuestos, se efectúa a través de débito automático a la cuenta de depósito en moneda legal colombiana que la Entidad Autorizada tenga en el Banco de la República a más tardar el último día hábil del respectivo mes, de acuerdo a los Token OTP que hayan sido entregados con anterioridad a la fecha de corte (día 25 de cada mes). Por su carácter de entidades especiales, a las Entidades Autorizadas que se les expida cuenta de cobro, deberán pagar directamente en las ventanillas del Banco de la República.