

05/5/04



Banco de la República
Bogotá D. C., Colombia

Subgerencia de Informática
Unidad de Protección y Continuidad Informática

NOVEDADES USUARIOS SEBRA CON PKI
ADMINISTRACIÓN DE USUARIOS SEBRA

Abril de 2005

| | | |
|----------|--|-----------|
| 1 | INTRODUCCIÓN | 3 |
| 2 | SISTEMA DE SEGURIDAD PKI..... | 4 |
| 3 | REQUERIMIENTOS TÉCNICOS PARA EL SISTEMA DE SEGURIDAD PKI | 6 |
| 4 | NOMBRAMIENTO DEL DELEGADO CON RESPONSABILIDAD ADMINISTRATIVA | 8 |
| 5 | CONSIDERACIONES SOBRE EL MANEJO DE LAS NOVEDADES SEBRA CON PKI | 9 |
| 6 | DILIGENCIAMIENTO DEL FORMATO DE NOVEDADES USUARIOS Y ESTACIONES SISTEMA SEBRA | 10 |
| 7 | CÓNDICIONES PARA EL ENVÍO DE SOLICITUDES DE NOVEDADES SEBRA FIRMADAS CON PKI | 11 |
| 7.1 | NOVEDADES USUARIOS Y ESTACIONES SEBRA..... | 11 |
| 7.2 | AUTORIZACIÓN RETIRO DE TARJETAS INTELIGENTES..... | 12 |
| 8 | CONTINGENCIA SOLICITUDES DE NOVEDADES SEBRA CON PKI. | 14 |
| 8.1 | INCONVENIENTES CON PKI | 14 |
| 8.2 | PROBLEMAS DE CORREO CON BANCO REPÚBLICA | 15 |

1 INTRODUCCIÓN

El propósito de este documento es divulgar a las entidades SEBRA los cambios en el procedimiento que se debe seguir para el envío de las NOVEDADES USUARIOS SISTEMA SEBRA, con el fin de brindar un servicio ágil y eficiente, manteniendo la seguridad de las solicitudes a través del uso del Sistema de Seguridad PKI ofrecido por el Banco de la República.

En el presente documento se describen el nuevo procedimiento, roles y requisitos que deben tenerse en cuenta para la atención de las solicitudes realizadas por los clientes a través del formato NOVEDADES USUARIOS Y ESTACIONES SISTEMA SEBRA.

2 SISTEMA DE SEGURIDAD PKI

El Sistema PKI contribuye significativamente al logro y cumplimiento, en términos de seguridad informática, de las normas establecidas por el marco legal colombiano. Colombia y en particular el Banco, cuenta con un referente legal vigente que le permite subir su nivel de seguridad a través de herramientas avanzadas en seguridad como el PKI. Hoy en día un mensaje digital tiene el mismo efecto probatorio que el papel ante un juez y dependerá del modelo de seguridad que se haya aplicado, el tener los suficientes argumentos probatorios en caso de un incidente informático.

El modelo de seguridad del Banco busca principalmente el cumplimiento de los 7 fundamentos de seguridad informática, en todos sus servicios críticos, a saber:

- **Confidencialidad:** Cuando la información es sólo accesible por aquellos a los cuales se ha autorizado su acceso.
- **Integridad:** Cuando la información es exacta y completa. Cuando se garantiza que la información no se modifica desde su momento de creación.
- **Disponibilidad:** Cuando la información es accesible a los usuarios autorizados en el momento de requerirla.

05/5/04

- Autenticación: Cuando se puede garantizar la identidad de quien solicita acceso a la información.
- Autorización o Control de Acceso: Cuando la información es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo.
- No repudiación: Cuando la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en éste.
- Observancia: Cuando la información relacionada con las acciones y actividades de los usuarios (personas o procesos) se encuentra debidamente registrada y monitoreada. Además cuando se vela y propende por el adecuado funcionamiento del modelo de seguridad informática.

Es importante comentar, que la entidad de certificación, componente fundamental de la PKI, almacena sus claves (llaves) en dispositivos de alta seguridad (hardware), el cual requiere de varias intervenciones físicas para su acceso. Con esto y el hecho de tener un modelo de PKI supervisado por la Auditoría Informática y Control Interno, el Banco garantiza que el núcleo de seguridad informática, está debidamente protegido, pues además, los servidores donde está montado el PKI tienen un debido esquema de contingencia y están resguardados físicamente por un centro de cómputo que cumple con las especificaciones internacionales, tanto ambientales como de control de acceso, para la protección adecuada de dichas máquinas.

Podrán acceder al Sistema de Seguridad PKI todas las entidades afiliadas al Sistema SEBRA y otras entidades que sean expresamente autorizadas por el Banco de la República.

3 REQUERIMIENTOS TÉCNICOS PARA EL SISTEMA DE SEGURIDAD PKI

- Requerimientos Básicos de Hardware:
 - PC Pentium III de 600 MHz o superior
 - 128 MB Ram
 - Disco Duro de 10 GB
 - Puerto USB

- Requerimientos Básicos de Software:
 - Windows 2000 con Service Pack 4 o superior.
 - Windows XP
 - Entrust Intelligence 6.1 y Rainbow Technologies (software requerido para manejo de PKI que lo provee el Banco de la República)

- Token Criptográfico:

Después de la evaluación Técnica y Económica el proveedor seleccionado para el suministro de los tokens criptográficos es Rainbow con su distribuidor mayorista en Colombia, Afina de Colombia.

Los datos del Contacto son:

Afina Colombia

Calle 93 # 14-20 Oficina 413

Tel. +57 (1) 642-2545 Ext. 19

05/5/04

Fax. +57 (1) 642-2545 Ext. 11

Bogotá – Colombia

www.afinasis.com.co - www.afina.es

4 NOMBRAMIENTO DEL DELEGADO CON RESPONSABILIDAD ADMINISTRATIVA

Para el manejo de este proceso, la entidad deberá autorizar expresamente al funcionario que se encargará y responsabilizará de las solicitudes realizadas, quien recibirá el nombre de DELEGADO CON RESPONSABILIDAD ADMINISTRATIVA. Dicha autorización la debe realizar directamente el Representante Legal de cada entidad y los requerimientos para hacerlo son:

- Diligenciar el formato Delegación de Firmas y Certificados Digitales (Publicado en la página web <http://www.banrep.gov.co/ca-banrep>), el cual debe firmar el Representante Legal.
- Dicho formato debe ser diligenciado y remitido en original con firma autenticada y reconocimiento de texto ante notario.
- Deberá adjuntarse a este formato, un original del certificado de existencia y representación legal donde conste claramente dicha condición del firmante y con fecha de expedición menor a 30 días.
- La documentación completa deberá dirigirse a la Unidad de Protección y Continuidad de Informática (UPCI) en la Cra.7 No.14-78 piso 9, donde se validará la documentación y se iniciará el proceso de nombramiento.

5 CONSIDERACIONES SOBRE EL MANEJO DE LAS NOVEDADES SEBRA CON PKI

El manejo de las NOVEDADES USUARIOS Y ESTACIONES SISTEMA SEBRA continuará realizándose mediante el formato diseñado para el caso, cambiando a partir de este momento varios aspectos, a saber:

- Diligenciamiento del formato: El formato será diligenciado de forma electrónica, a través de nuestra página web (<http://www.banrep.gov.co/sebra/formatos4.htm>). Se guardará la información en un archivo de formato Excel que posteriormente deberá ser remitido para su atención.
- Envío y recepción del formato: El formato se remitirá para su atención, como un archivo adjunto firmado digitalmente con PKI, en un correo electrónico dirigido a la cuenta de correo novedadsebra@banrep.gov.co. Se eliminará entonces, la recepción vía fax y/o medio físico por parte del cliente; exceptuando el caso de la revisiones de tarjeta donde se deberá remitir la misma, acompañada de una carta haciendo referencia a la solicitud electrónica previamente enviada.
- Validación de Seguridad: La validación de seguridad realizada mediante el código de autorización ya no se empleará; en su lugar, la validez y confiabilidad de la solicitud la determinará la firma digital PKI. Esta firma solo podrá corresponder al funcionario encargado de esta responsabilidad, quien previamente deberá ser autorizado por la entidad y el Banco de la República.

6 DILIGENCIAMIENTO DEL FORMATO DE NOVEDADES USUARIOS Y ESTACIONES SISTEMA SEBRA

El diligenciamiento del formato de NOVEDADES USUARIOS Y ESTACIONES SISTEMA SEBRA, continuará rigiéndose por el documento denominado ADMINISTRACIÓN SERVICIOS SEBRA ENTIDADES EXTERNAS, publicado en <http://www.banrep.gov.co/sebra/aspectosadministrativos4.htm>, el cual reúne todas las indicaciones y recomendaciones para formalizar las solicitudes ante el Banco de la República. Igualmente, define el tiempo de atención de cada solicitud de acuerdo con el tipo de novedad realizada.

Este documento es la guía de los delegados y administradores para llevar el proceso exitosamente; por tanto, es de vital importancia su consulta y seguimiento.

7 CONDICIONES PARA EL ENVÍO DE SOLICITUDES DE NOVEDADES SEBRA FIRMADAS CON PKI

7.1 NOVEDADES USUARIOS Y ESTACIONES SEBRA

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

- 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, situación que se validará en cada solicitud, de incumplirse con esta condición, la solicitud será rechazada y devuelta vía correo al remitente.

- Formato del archivo

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

- 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.

- Envío del archivo

Solamente se tendrán en cuenta y se dará curso a las solicitudes recibidas en la cuenta de correo novedadsebra@banrep.gov.co; NINGUNA de las demás cuentas disponibles para comunicarse con el Centro de Soporte Informático será válida.

Igualmente, las respuestas a las solicitudes se remitirán de la cuenta de correo mencionada anteriormente.

- Información del archivo

La información contenida en cada archivo se validará 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.

7.2 AUTORIZACIÓN RETIRO DE TARJETAS INTELIGENTES

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

- 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, situación que se validará en cada solicitud, de incumplirse con esta condición, la solicitud será rechazada y devuelta vía correo al remitente.

- Formato del archivo

El formato original del documento es Excel, posterior a la firma digital, PKI convertirá el archivo al formato seguro de entrust (.ent) y cambiará el ícono original; éste último será el ÚNICO archivo que se recibirá vía mail. Si no

05/5/04

se cumple con esta condición, la solicitud será rechazada y devuelta vía correo al remitente.

- 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

- Envío del archivo

Solamente se tendrán en cuenta y se dará curso a las solicitudes recibidas en la cuenta de correo novedadsebra@banrep.gov.co; NINGUNA de las demás cuentas disponibles para comunicarse con el Centro de Soporte Informático será válida.

- Entrega de la tarjeta

El funcionario autorizado deberá presentar copia impresa de la autorización y su documento de identidad para validar la información previamente.

8 CONTINGENCIA SOLICITUDES DE NOVEDADES SEBRA CON PKI

8.1 INCONVENIENTES CON PKI

Los códigos de autorización actuales se mantendrán exclusivamente como mecanismo de contingencia ante eventualidades que imposibiliten el uso del sistema PKI, a saber:

- Problemas con la clave PKI.
- Fallas técnicas del token.

Sin embargo, se debe tener en cuenta que cada entidad deberá nombrar dos delegados; donde el primero será el titular y el segundo será el suplente. El procedimiento en condiciones normales será:

1. Firma digital PKI del Delegado Titular

En caso que el delegado titular no pueda ejercer su función:

2. Firma digital PKI del Delegado Suplente

Si el delegado suplente tampoco puede actuar por alguna de las eventualidades mencionadas, se procederá a realizar el proceso de recuperación del profile de los delegados, en el menor tiempo posible teniendo en cuenta el procedimiento para este caso.

Si el requerimiento lo amerita, se evaluará y aprobará el envío del formato Novedades Sistema Sebra, vía fax y con código de autorización. Una vez se haya solucionado el

05/5/04

inconveniente la entidad se comprometerá a formalizar el envío de los archivos a través de PKI, con el fin de mantener un control de las novedades.

Esta autorización dependerá del tipo de novedad que se requiera procesar, es decir, **que no será válida** la contingencia para casos como:

- Inclusión de Usuario
- Reasignaciones de Tarjeta
- Revisión de Tarjeta

Se autorizará para casos eventuales y de urgencia como:

- Pin Manual
- Blanqueo de Pin
- Adición de Servicio / IP

En todo caso, será el grupo de Administración Usuarios SEBRA, quien ante el reporte del problema, se encargará de evaluar la situación y determinará si autoriza o no, el uso de la contingencia con código de autorización para el manejo de las novedades SEBRA.

El Banco de la República, a través de su área de Seguridad Informática, se encuentra trabajando en una contingencia del esquema PKI, diferente a los códigos de autorización, estrategia que se dará a conocer cuando esté debidamente probada y funcionalmente estable.

8.2 PROBLEMAS DE CORREO CON BANCO REPÚBLICA

Se tendrá disponible para el envío de las solicitudes una cuenta de correo internet alterna, donde se podrán enviar los archivos mientras se supera el inconveniente. Esta cuenta se denominará novedadsebra@yahoo.com.

Sólo será válido el envío de solicitudes a esta cuenta previa confirmación y autorización del grupo de Administración Usuarios SEBRA.