



*Banco de la República*  
*Bogotá D. C., Colombia*

**Subgerencia de Informática**  
**Unidad de Soporte y Continuidad Informática**

**NOVEDADES DE USUARIO CON PKI**  
**UPCI-CDS-GI-4**

Febrero de 2010  
Versión 2.0



## TABLA DE CONTENIDO

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>INTRODUCCIÓN .....</b>   | <b>3</b>  |
| <b>2</b> | <b>SISTEMA DE SEGURIDAD PKI .....</b>   | <b>4</b>  |
| <b>3</b> | <b>REQUERIMIENTOS TÉCNICOS PARA EL SISTEMA DE<br/>SEGURIDAD PKI .....</b>         | <b>6</b>  |
| 3.1      | REQUERIMIENTOS BÁSICOS DE HARDWARE .....  | 6         |
| 3.2      | REQUERIMIENTOS BÁSICOS DE SOFTWARE .....  | 6         |
| 3.3      | TOKEN CRIPTOGRÁFICO PARA EL SISTEMA PKI .....                                     | 7         |
| <b>4</b> | <b>NOMBRAMIENTO DEL DELEGADO PKI CON RESPONSABILIDAD<br/>ADMINISTRATIVA .....</b> | <b>8</b>  |
| <b>5</b> | <b>NOVEDADES DE USUARIO PKI – CA BANREP .....</b>                                 | <b>9</b>  |
| <b>6</b> | <b>CONTINGENCIA ENVIO SOLICITUDES CON PKI.....</b>                                | <b>11</b> |
| 6.1      | INCONVENIENTES CON PKI .....  | 11        |



# 1 INTRODUCCIÓN

El propósito de este documento es dar a conocer a las Entidades Autorizadas las generalidades del Sistema de Seguridad PKI ofrecido por El Banco de la República

El Sistema de Seguridad 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 fortalecer 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.

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



## 2 SISTEMA DE SEGURIDAD PKI

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 los usuarios 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.
- **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 resaltar, que la entidad de certificación, componente fundamental de 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 los entes de control y vigilancia, El Banco de la República garantiza que el núcleo de seguridad informática, está debidamente protegido, pues además, los servidores donde reside 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.



## **3 REQUERIMIENTOS TÉCNICOS PARA EL SISTEMA DE SEGURIDAD PKI**

### **3.1 REQUERIMIENTOS BÁSICOS DE HARDWARE**

- Hardware mínimo: 2 GB de RAM, procesador de mínimo 2.6Ghz y el espacio en disco que requiera el funcionamiento del sistema operativo más las aplicaciones específicas a instalar.
- Sistema Operativo: Windows XP con SP3. Es necesario que el sistema operativo trabaje con procesamiento a 32 bits.
- Resolución de Monitor: se recomienda trabajar la pantalla a una resolución de 1024 x 768.
- Puertos USB (mínimo dos)

### **3.2 REQUERIMIENTOS BÁSICOS DE SOFTWARE**

- Navegador Web Internet Explorer V 7.05, que soporte SSL v.3 y cifrado a 128 bits.
- Plug-in de Java (JRE) instalado versión 1.5
- Antivirus actualizado
- Acrobat Reader 5.0 o superior
- Entrust Intelligence 6.1 y Drivers token (software requerido para manejo de PKI que lo provee El Banco de la República)



### 3.3 TOKEN CRIPTOGRÁFICO PARA EL SISTEMA PKI

El Token criptográfico se refiere al dispositivo de almacenamiento del Certificado Digital y que se debe conectar al puerto USB de un computador para poder hacer uso del certificado.

Como resultado de la evaluación técnica y económica, la referencia del Token criptográfico para el Sistema PKI es “iKey 2032” y/o “iKey 4000”.

Este dispositivo es distribuido a través de Afina de Colombia, mayorista en Colombia.

#### **Información de contacto:**

Afina de Colombia.  
Calle 93 # 14-20 Of. 413  
Bogotá, Colombia  
(P):+57 (1) 642-2545 Ext. 22  
(F):+57 (1) 618-1261  
(M):+57 (311) 811-4333

#### **Canales de Distribución de Tokens Criptográficos:**

1. Canal: Digiware.  
Tel: 623-2474.
2. Canal: Southern Technologies.  
Tel: 336-8620 ó 336-8609.
3. Canal: Internet Solutions.  
Tel: 312-0910.
4. Netco Ltda.  
Alejandro Naranjo  
Tel. 2843900  
Cra. 7 #27-52 of.201

Una vez adquiridos, la Entidad Autorizada deberá informar al Centro de Soporte Informático, a través del buzón de correo electrónico [ca-novedades@banrep.gov.co](mailto:ca-novedades@banrep.gov.co), la adquisición de los Tokens criptográficos.



## **4 NOMBRAMIENTO DEL DELEGADO PKI CON RESPONSABILIDAD ADMINISTRATIVA**

El representante legal de la Entidad Autorizada, por medio del formato “Delegación para el manejo de Firmas Digitales y Certificados”, publicado en la página web<sup>1</sup> de El Banco, autorizará expresamente a máximo dos (2) funcionarios que se responsabilizarán de realizar solicitudes a través de correo electrónico con PKI, estos delegados recibirán el nombre de DELEGADOS CON RESPONSABILIDAD ADMINISTRATIVA.

Dicho formato debe ser diligenciado y remitido<sup>2</sup> en original con firma autenticada y reconocimiento de texto ante notario, del representante legal de la Entidad Autorizada, adjuntando el certificado de existencia y representación legal donde conste claramente dicha condición, con fecha de expedición no mayor a 30 días, expedido por la Superintendencia Financiera de Colombia, y el certificado de Cámara de Comercio para aquellas entidades que no son vigiladas por la Superintendencia Financiera de Colombia.

---

<sup>1</sup> [http://www.banrep.gov.co/sistema-financiero/seb\\_sistema\\_PKI.htm](http://www.banrep.gov.co/sistema-financiero/seb_sistema_PKI.htm)

<sup>2</sup> Unidad de Soporte y Continuidad Informática Cra.7 No.14-78 piso 9



## **5 NOVEDADES DE USUARIO PKI – CA BANREP**

El formato denominado “NOVEDADES DE USUARIO PKI - CA BANREP<sup>3</sup>” ha sido diseñado para permitir a las Entidades Autorizadas solicitar las novedades de usuarios que requieren el envío/recepción de archivos firmados y encriptados a través del Sistema de seguridad PKI. 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<sup>4</sup>.

Este formato podrá ser actualizado de acuerdo a las necesidades. 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

---

<sup>3</sup> Disponible en <http://www.banrep.gov.co/documentos/sistema-financiero/exel/BR-3-598-0.xlt>

<sup>4</sup> Disponible en <http://www.banrep.gov.co/documentos/sistema-financiero/exel/BR-3-598-0.xlt>



anulación inmediata. El archivo deberá ser enviado únicamente al buzón de correo electrónico [ca-novedades@banrep.gov.co](mailto:ca-novedades@banrep.gov.co); cualquier solicitud enviada a buzones diferentes no será atendida.



## 6 CONTINGENCIA ENVIO SOLICITUDES CON PKI

### 6.1 INCONVENIENTES CON PKI

Los códigos de autorización<sup>5</sup> actuales se mantendrán exclusivamente como mecanismo de contingencia ante eventualidades que imposibiliten el uso del sistema PKI, a saber:

- Problemas con la clave PKI

En caso de presentarse inconvenientes con la clave PKI se realizará el procedimiento de recuperación del “profile”<sup>6</sup> del(los) delegado(s), en el menor tiempo posible. El Delegado PKI debe enviar un correo electrónico desde su buzón de correo corporativo al buzón de correo [ca-novedades@banrep.gov.co](mailto:ca-novedades@banrep.gov.co) solicitando la recuperación de(los) “profile(s)”.

- Fallas técnicas del Token criptográfico

En caso de fallas técnicas con el Token criptográfico, la Entidad Autorizada debe tramitar ante su proveedor la garantía y/o reemplazo del mismo.

---

<sup>5</sup> Códigos generados a través del Sistema Generador Automático de Claves (GAC)

<sup>6</sup> Perfil asociado a cada usuario PKI



Si el requerimiento lo amerita, se evaluará y aprobará el envío del formato “Novedades de Usuarios SEBRA” al fax 3430777, con código de autorización. Una vez se haya solucionado el 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 Tokens OTP<sup>7</sup>
- Revisión de Tokens OTP

Se autorizará para casos eventuales y de urgencia como:

- Pin Manual para Tokens OTP
- Blanqueo de Pin de Token OTP

---

<sup>7</sup> OTP: One Time Password. Dispositivo de seguridad, personal e intransferible, que le permitirá autenticarse al ingreso del sistema.