Banco de la República
Bogotá D. C., Colombia

Subgerencia de Informática
Departamento de Seguridad Informática

MANUAL DE USUARIO PARA EL SERVICIO
- *SISTEMA DE GESTIÓN PKI DE USUARIOS ROAMING* -

USI-GI-56 Manual de Usuario SGPKIUR

06 de Noviembre de 2007

Versión 1.0

CONTENIDO

1 INTRODUCCIÓN

1.1 OBJETO

El propósito de este documento es brindarle al usuario final un manual de uso de la herramienta ***Sistema de Gestión PKI de Usuarios Roaming*** para el manejo de sus certificados PKI de tipo *roaming*.

1.2 ALCANCE

Este documento solo aplica como un manual al usuario final brindándole una guía completa de cómo usar este servicio de ***Sistema de Gestión PKI de Usuarios Roaming*** (**SGPKIUR**).

1.3 AUDIENCIA

Este documento ira dirigido a todos los usuarios PKI del Banco de la Republica que dadas sus condiciones de ubicación no es posible o práctico que tengan certificados *desktop* o por *token*. Estos usuarios, externos al banco, se les crean un certificado *roaming*.

1.4 ORGANIZACIÓN DEL DOCUMENTO

La sección 2 explica los conceptos necesarios para el entendimiento de certificado PKI roaming. Posteriormente en la sección 3, se describe el funcionamiento de la aplicación.

2 INTRODUCCIÓN A USUARIOS PKI ROAMING

2.1 DESCRIPCIÓN GENERAL

Por medio de la infraestructura PKI del banco sus usuarios pueden intercambiar mensajes asegurando la confiabilidad, integridad/autenticidad y no repudiación de los mensajes. Para que esto sea posible los usuarios del sistema PKI deben tener asignadas unas credenciales. En las credenciales se almacena la información del usuario, sus llaves públicas y privadas.

La llave pública del usuario, que es dada a conocer a los demás usuarios, es contenida en un certificado digital. El certificado digital permite asegurar que la llave pública corresponde a la persona, entidad o servicio a la que indica que pertenece.

Los usuarios de tipo *roaming* almacenan sus credenciales en un directorio que puede ser accedido de forma remota. Estas credenciales se obtienen por medio del uso de un login y su respetiva contraseña (de ahora en adelante: password). De esta forma los usuarios que quieran interactuar servicios del Banco de la República habilitados para PKI pueden hacerlo sin la necesidad de tokens o almacenar archivos en sus equipos.

2.2 RESTRICCIONES

Para una correcta visualización, se recomienda el uso de Internet Explorer 6 SP2 o Internet Explorer 7. Es posible que con otros navegadores la visualización sea diferente.

2.3 BREVE DESCRIPCIÓN DE LA SOLUCIÓN

La aplicación WEB permite que usuarios PKI Roaming puedan crear sus credenciales y recuperarlas desde cualquier navegador. Sin embargo el usuario debe asegurarse que el equipo desde el cual se accede a la aplicación es seguro. Por ejemplo, no se recomienda el acceso desde cafés Internet debido a que los equipos pueden tener software malintencionado que capture datos sensibles como su password o el *referente number* y el *authentication code*.

La creación de credenciales (de ahora en adelante: crear certificado) se realiza cuando el usuario va a obtener sus credenciales por primera vez. La recuperación de credenciales (de ahora en adelante: recuperar certificado) se realiza cuando el usuario ya tiene credenciales pero que ha olvidad su contraseña. En ambos casos se debe tener el *referente number* y el *authentication code*

2.4 REFERENCE NUMBER Y AUTHENTICATION CODE

Para poder realizar la creación o recuperación del certificado, el usuario debe poseer un referente number y un authentication code. Estos son códigos de seguridad para controlar la creación y recuperación de certificados por parte del Banco de la República

Estos códigos son entregados por el Banco de la República a su destinatario y usted debe tener en cuenta las siguientes consideraciones:

- Son intransferibles
- El *referente Lumber* y el *authentication code* están correlacionados entre sí. El uno no funciona sin el otro y no funciona con otro código.
- Tiene una vida útil, si no son utilizados antes del tiempo de su vencimiento estos no podrán usarse.
- Pueden ser usados una sola vez debido a que perderán validez.

2.5 LOGIN Y PASSWORD

Un certificado roaming es identificado por el login. El login es generado automáticamente por la aplicación con base en un formato definido por el banco de la república y guarda relación con la información del usuario. Es de vital importancia que el usuario recuerde el login generado después de crear o recuperar un certificado.

El login tiene un formato definido por el Banco de la República y será similar a este formato: 42136578-pmendico-00-01000-01.

Durante el proceso de creación o recuperación el usuario debe ingresar su password que es de carácter personal e intransferible. Este password debe cumplir con unas características de seguridad mínimas recomendadas por la aplicación. Estas características deben ser:

- Contener al menos 10 caracteres.
- Contener al menos una letra minúscula.

- Contener al menos una letra mayúscula.
- Contener al menos un número
- Contener al menos un carácter especial no fonético.

3 *GESTIÓN PKI DE USUARIOS ROAMING*

3.1 DESCRIPCIÓN GENERAL

En esta sección se describe el uso de la aplicación de ***Sistema de Gestión PKI de Usuarios Roaming*** (**SGPKIUR**). Su funcionamiento y su aplicabilidad.

3.2 QUE ES

Sistema de Gestión PKI de Usuarios Roaming (**SGPKIUR**) es un servicio que permite a un usuario desde su navegador crear y recuperar certificados PKI.

3.3 CUANDO UTILIZAR LA APLICACIÓN

El usuario deberá acudir al servicio ***Sistema de Gestión PKI de Usuarios Roaming*** (**SGPKIUR**) por cualquiera de las siguientes razones:

1. El usuario va a crear su certificado *roaming* por primera vez.
2. El usuario ya tiene su certificado *roaming* pero ha bloqueado u olvidado su contraseña y desea recuperarlo.
3. El usuario desea cambiar la contraseña de su certificado *roaming*.

4 INTERFAZ

4.1 DESCRIPCIÓN GENERAL

A continuación se describe las pantallas, el funcionamiento y los resultados obtenidos durante el uso de la aplicación.

4.2 PAGINA INICIAL

La página de inicio muestra la siguiente información:

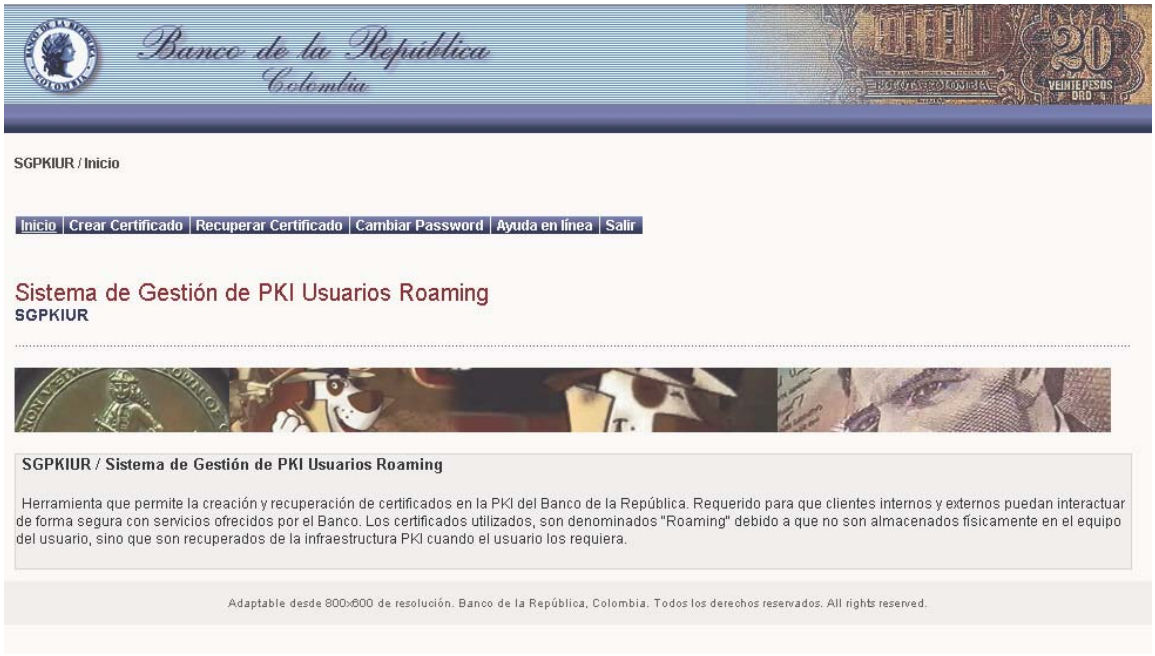


Imagen 1. Página principal

El menú de la aplicación en todas las páginas que compone la aplicación. Permite al usuario acceder a las distintas funcionalidades que están presentes en el ***Sistema de Gestión PKI de Usuarios Roaming.***

Cada opción se resume brevemente:

- Inicio: Lleva al usuario a la página principal (imagen 1.)

- Crear Certificado: Permite al usuario crear su certificado PKI por primera vez. Requiere el *authentication code* y el *reference number*. (ver sección 4.3)

- Recuperar Certificado: Permite al usuario recuperar su certificado debido a que este se encuentra bloqueado o el usuario ha olvidado su password. Requiere el *authentication code* y el *reference number* (ver sección 4.4).

- Cambiar Password: Permite al usuario cambiar la clave de acceso a su certificado. Requiere el login y password (ver sección 4.7).

- Ayuda en línea: Contiene información básica referente al servicio PKI roaming. Esta información es presentada de forma similar a un F.A.Q (ver sección 4.9).

- Salir: Permite al usuario salir de la aplicación de forma que cierra su ventana (ver sección 4.10).

4.3 PÁGINA CREAR CERTIFICADO

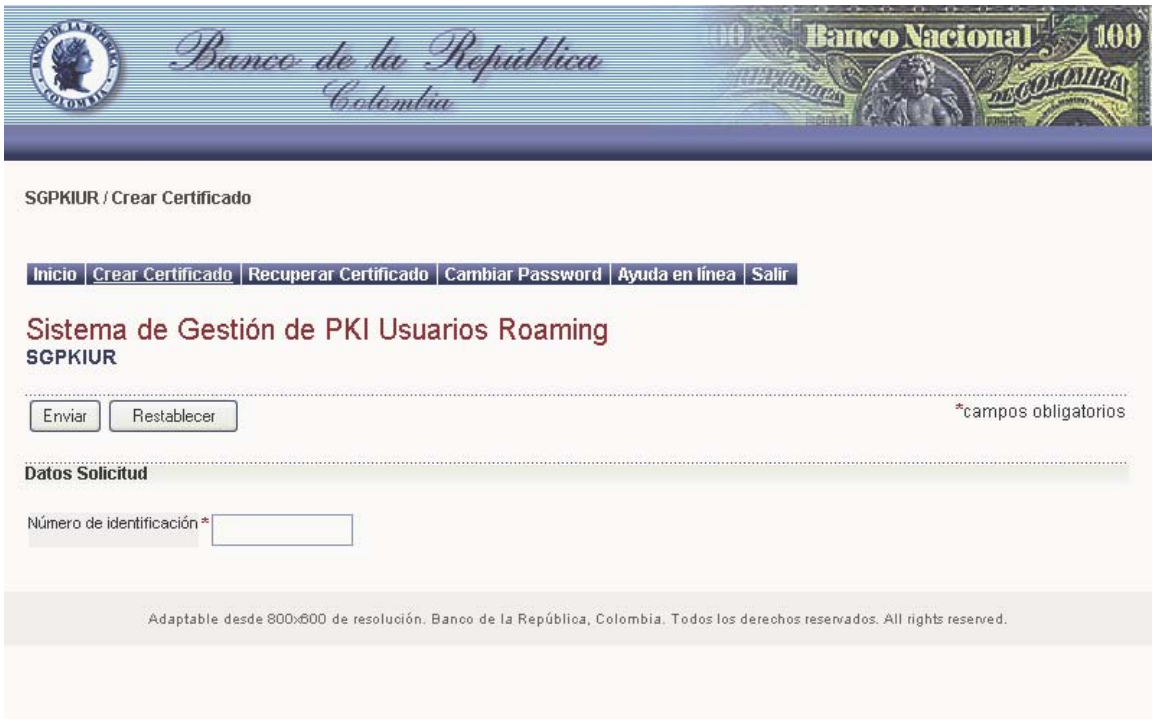


Imagen 2. Crear Certificado

Esta página está únicamente dirigida a aquellos usuarios que van a crear su certificado por primera vez. Se solicita el número de identificación del usuario (ejemplo: cédula de ciudadanía) con el cual se registro en el Banco.

Imagen 3. Solicitud de documento, crear certificado

Una vez ingresado el número de identificación se da clic en enviar. Si el usuario está registrado correctamente en el Banco será enviado a la página de datos de certificado. (Ver sección 4.5).

El campo "número de identificación" solo acepta desde cinco caracteres hasta doce caracteres numéricos. Omitir comas puntos y guiones.

El botón restablecer limpiará el campo de número de identificación. Pagina de Recuperar Certificado

4.4 PÁGINA RECUPERAR CERTIFICADO

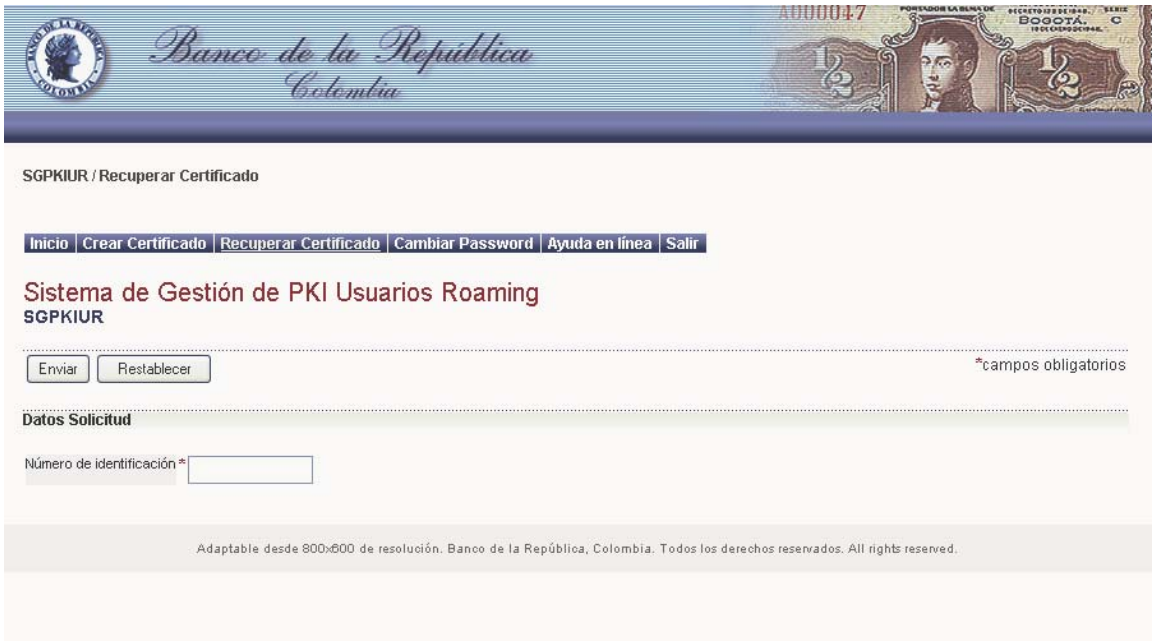


Imagen 4. Recuperar Certificado

A diferencia de la opción "crear certificado", la recuperación esta dirigida a aquellos usuarios que ya poseen un certificado *roaming* pero que han olvidado su contraseña o han bloqueado el certificado.

Se solicita el número de identificación del usuario (ejemplo: cédula de ciudadanía) con el cual se registro en el Banco.

Imagen 54. Solicitud de documento, recuperar certificado

Una vez ingresado el número de identificación se da clic en enviar. Si el usuario está registrado correctamente en el Banco será enviado a la página de datos de certificado (ver sección 4.5).

El campo "número de identificación" solo acepta desde cinco caracteres hasta doce caracteres numéricos. Omitir comas puntos y guiones.

El botón restablecer limpiará el campo de número de identificación.

4.5 PAGINA DE DATOS DE CERTIFICADO

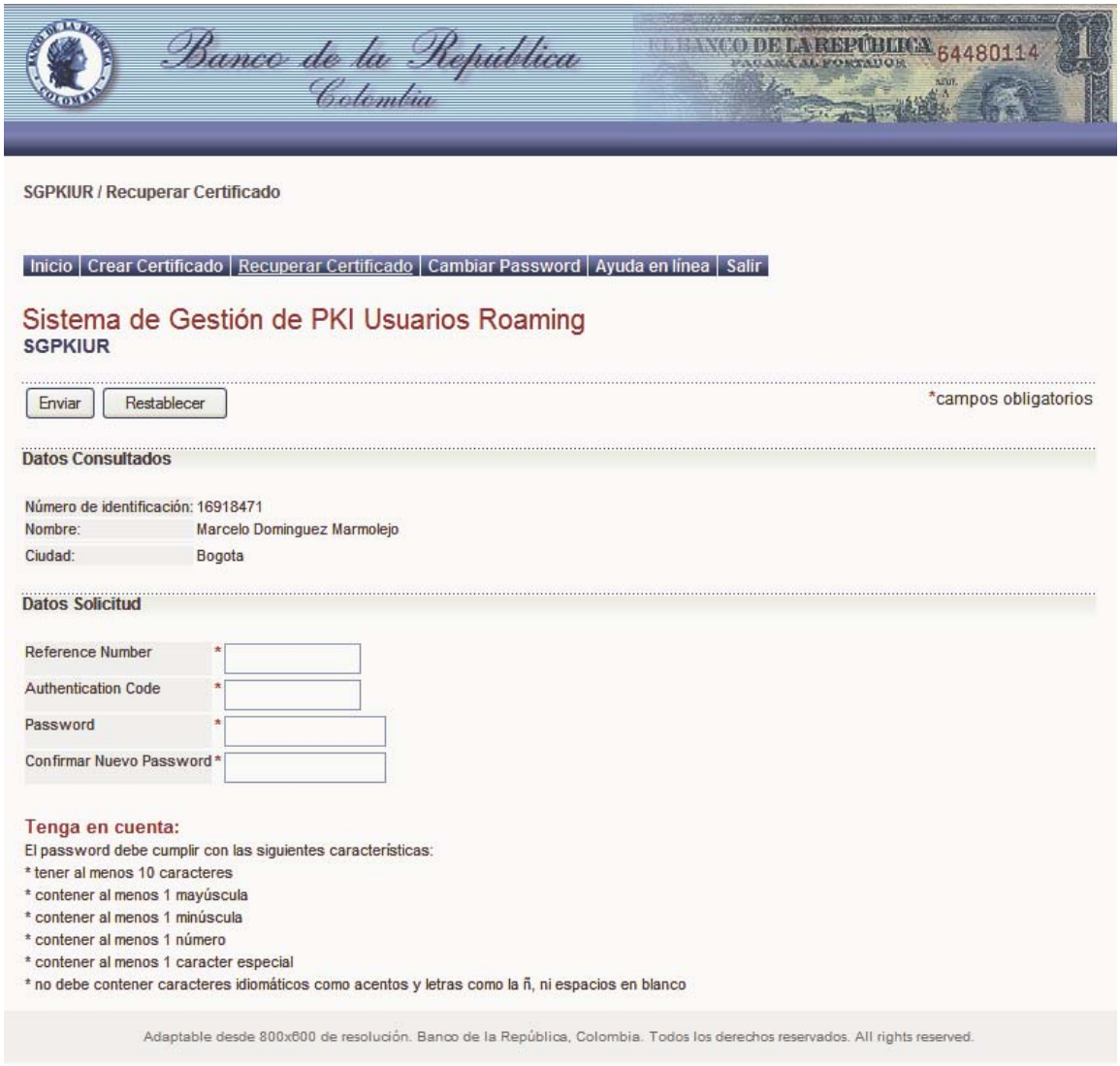


Imagen 6. Página de datos de certificado

Esta página es el resultado de ingresar un número de identificación que se encuentre registrado en el Banco de la República. Desplegará como campos no editables, el número de identificación, nombre y ciudad relacionados con el número de identificación.

El usuario debe ingresar:

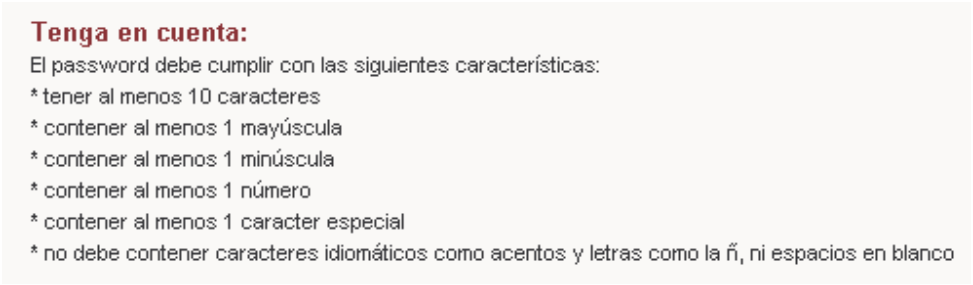
reference number: Solo acepta como entre 7 y 8 caracteres números.

authentication code: Solo acepta caracteres alfanuméricos. Deben ingresarse los doce caracteres sin guiones u otro carácter especial.

nuevo password: Crear su password, el cual utilizará para acceder a su certificado. Hasta un máximo de 40 caracteres.

Confirmar nuevo password: Confirma el password ingresado en el campo "nuevo password".

El password debe cumplir con las siguientes características indicadas en la página



Una vez ingresado los datos se da clic en enviar.

El botón restablecer limpiará el campo de número de identificación.

4.6 PAGINA DE RESULTADO

Al terminar el proceso correctamente se desplegará la figura 6.

Imagen 6. Página de resultado

Está página indica que el certificado fue correctamente creado/recuperado e indicará el login del usuario. Usted deber recordar este login y el password ingresado con el fin de de poder utilizar su certificado.

4.7 PAGINA DE CAMBIO DE PASSWORD

Si usted posee un certificado vigente y desea cambiar su password por uno nuevo. Al dar clic en "cambiar password", se desplegará la siguiente página.

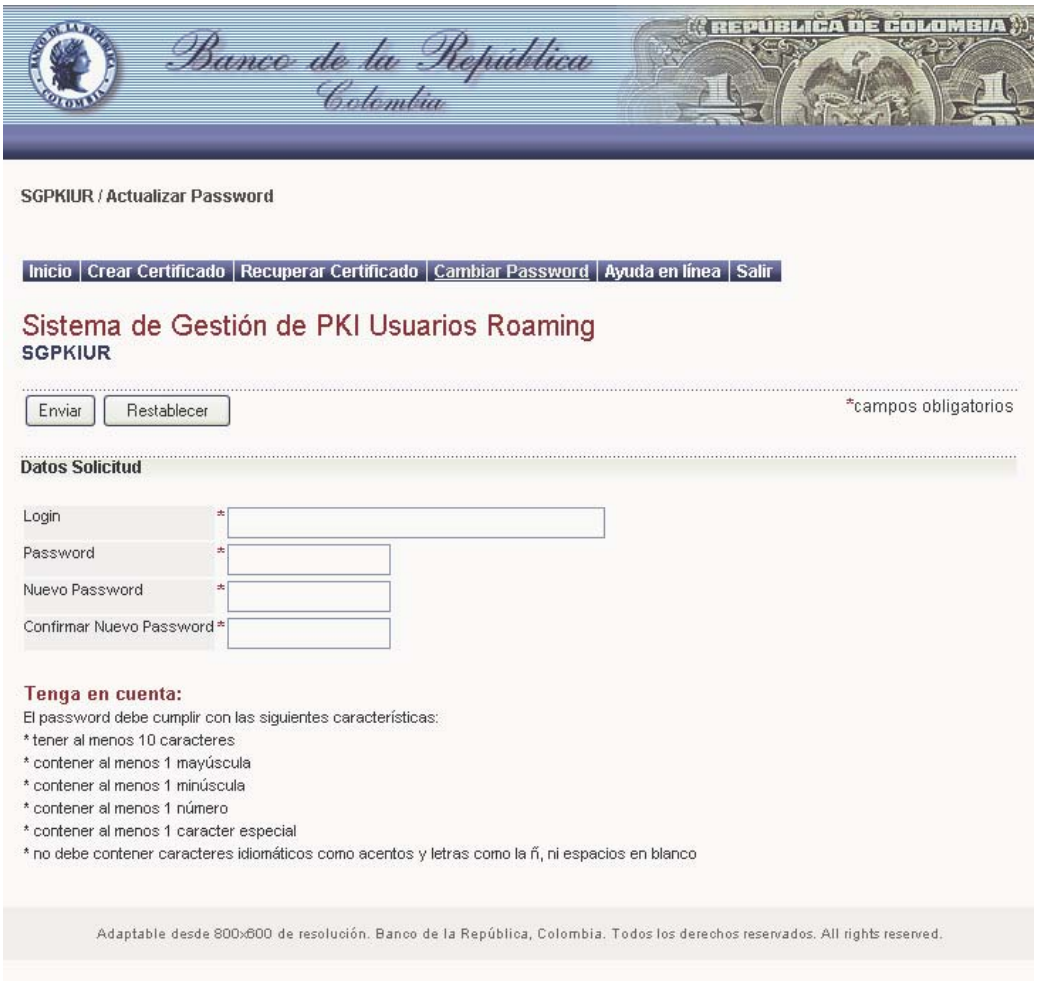


Imagen 7. Página de cambio de password

El usuario debe ingresar la información correspondiente a cada campo obligatorio:

*login: l*ogin con el cual se identifica el usuario, este es generado automáticamente cuando el usuario crea o recupera su certificado. Si usted ha olvidado su login debe comunicarse con el Banco de la República con el fin de iniciar el procedimiento para la recuperación de su certificado. Este campo acepta hasta 35 caracteres.

password: El password actual del usuario, este corresponde al último password ingresado en la recuperación, creación o cambio de password en la aplicación. El campo acepta hasta máximo 40 caracteres.

nuevo password: Ingresar el password del usuario, el cual utilizará para acceder a su certificado. Hasta un máximo de 40 caracteres. Este password debe tener las siguientes características.

Tenga en cuenta:

El password debe cumplir con las siguientes características:

* tener al menos 10 caracteres
* contener al menos 1 mayúscula
* contener al menos 1 minúscula
* contener al menos 1 número
* contener al menos 1 caracter especial
* no debe contener caracteres idiomáticos como acentos y letras como la ñ, ni espacios en blanco

confirmar nuevo password: Se repite el *password* ingresado en *nuevo password* con el fin de verificar que este se haya ingresado correctamente.

Una vez ingresado los datos se da clic en enviar.

El botón restablecer limpiará todos los campos: *login, password, nuevo password* y *confirmar nuevo password*.

Si el proceso finaliza correctamente se desplegará la página de resultado (ver sección 4.8).

4.8 PÁGINA DE RESULTADO CAMBIO DE PASSWORD

Al terminar el proceso de cambio de password correctamente se desplegará la figura 7

Imagen 8. Página de resultado cambio de password

El usuario debe recordar el password ingresado para poder hacer uso de su certificado.

4.9 AYUDA EN LÍNEA

Se accede a la información básica referente al servicio PKI roaming. Esta información es presentada de forma similar a un F.A.Q

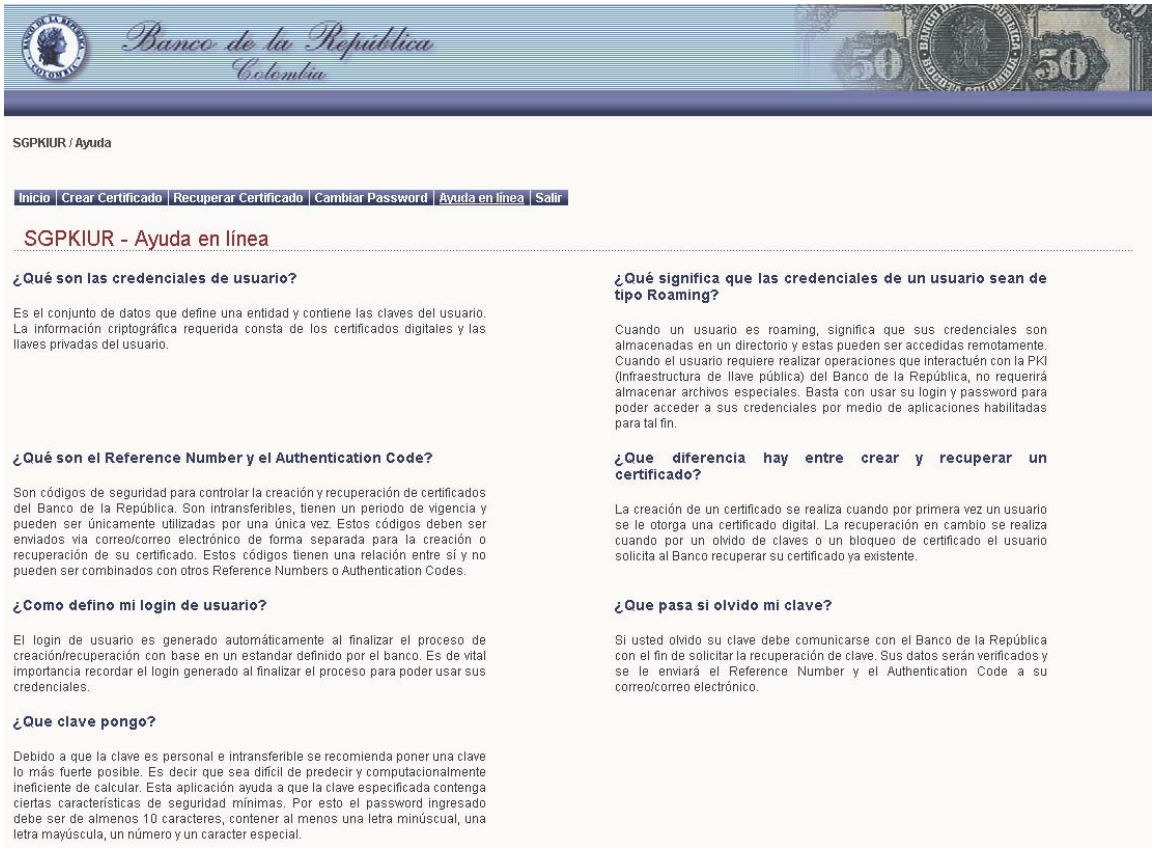


Imagen 9. Página de recultado cambio de password

4.10 SALIR

Con la opción “Salir” del menú, se cierra la sesión del usuario y ce cierra su ventana actual de navegación (Internet Explorer).

4.11 PÁGINAS DE ERROR

Ante una falla del sistema o validación de la información de usuario, se desplegará información relacionada con el error.

Imagen 10. Página de error

La página de error se compone de un mensaje y un código de error. Corresponde a validaciones o resultado de alguna operación incorrecta del sistema.

4.12 VALIDACIONES

En cada página existen validaciones asociadas a cada campo ingresado. Estas validaciones son hechas en el lado del servidor y son ejecutadas cuando el usuario da clic en el botón "Enviar".

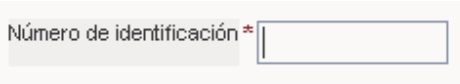
El resultado erróneo de la validación aparecerá en texto rojo frente al campo que se valida. Usted deberá corregir el error con el fin de proseguir en la recuperación, creación o cambio de password.

Las validaciones mostradas a continuación están dadas en orden, es decir, cuando dos o más validaciones dieran a lugar se mostrará la primera.

4.12.1 Validaciones creación/recuperación de certificado

Información adicional ver sección 4.3 y 4.4.

4.12.1.1 Sobre el campo número de cédula

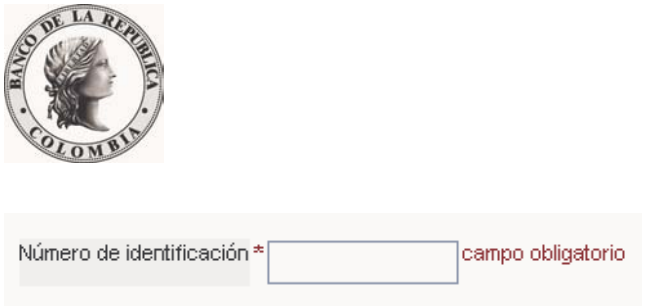


Si los datos ingresados tiene una longitud menor a 5 o mayor a 12 (Es posible que no vea el mensaje asociado a una longitud mayor a 12 debido a que la cantidad máxima de caracteres permitidos en el campos es 12). Usted verá alguno de los siguientes mensajes:

- `el valor es mayor a la longitud máxima permitida '12'.`
- `el valor es menor a la longitud mínima permitida '5'`

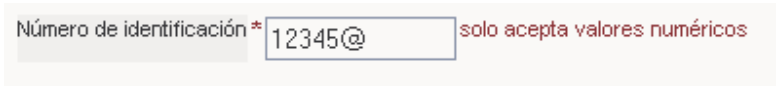
Si ingresa caracteres vacíos o no ingresa ningún texto, usted verá:

- `campo obligatorio`



Si ingresa un carácter no numérico, usted verá:

- `solo acepta valores numéricos`



4.12.2 Validaciones datos de certificado

Información adicional ver sección 4.5.

4.12.2.1 Sobre el campo reference number

Si los datos ingresados tiene una longitud menor a 7 o mayor a 8 (Es posible que no vea el mensaje asociado a una longitud mayor a 8 debido a que la cantidad máxima de caracteres permitidos en el campos es 8). Usted verá alguno de los siguientes mensajes:

- `el valor es mayor a la longitud máxima permitida '8'.`
- `el valor es menor a la longitud mínima permitida '7'`

Si ingresa caracteres vacíos o no ingresa ningún texto, usted verá:

- `campo obligatorio`

Si ingresa un carácter no numérico, usted verá:

- `solo acepta valores numéricos`

4.12.2.2 Sobre el campo authentication code

Si los datos ingresados tiene una longitud distinta a 12 (Es posible que no vea el mensaje asociado a una longitud mayor a 12 debido a que la cantidad máxima de caracteres permitidos en el campos es 12). Usted verá alguno de los siguientes mensajes:

- `el valor es mayor a la longitud máxima permitida '12'.`
- `el valor es menor a la longitud mínima permitida '12'`

Si ingresa caracteres vacíos o no ingresa ningún texto, usted verá:

- `campo obligatorio`

Si ingresa un carácter un caracter especial (distinto a letras y números), usted verá:

- `solo acepta valores alfanuméricos`

4.12.2.3 Sobre el campo password

Si los datos ingresados tiene una longitud menor a 10 o mayor a 40 (Es posible que no vea el mensaje asociado a una longitud mayor a 40 debido a que la cantidad máxima de caracteres permitidos en el campos es 40). Usted verá alguno de los siguientes mensajes:

- `el valor es mayor a la longitud máxima permitida '40'.`
- `el valor es menor a la longitud mínima permitida '10'`

Si no ingresa ningún texto, usted verá:

- `campo obligatorio`

Si el password ingresado no cumple con las características mínimas definidas, usted verá alguno de los siguientes mensajes dependiendo de la característica que no cumpla:

- `contiene una letra no permitida, verifique que no haya letras con acento, espacios o letras ñ`
- `debe contener al menos una letra minúscula`
- `debe contener al menos una letra mayúscula`
- `debe contener al menos un número`
- `debe contener al menos un caracter especial`

4.12.3 Validaciones datos cambiar password

Información adicional ver sección 4.7.

4.12.3.1 Sobre el campo login

Si los dato ingresado tiene una longitud mayor a 40 (Es posible que no vea el mensaje asociado a una longitud mayor a 40 debido a que la cantidad máxima de caracteres permitidos en el campo es 35). Usted verá el mensaje:

- `el valor es mayor a la longitud máxima permitida '40'.`

Si ingresa caracteres vacíos o no ingresa ningún texto, usted verá:

- `campo obligatorio`

4.12.3.2 Sobre el campo password

Si ingresa caracteres vacíos o no ingresa ningún texto, usted verá:

- `campo obligatorio`

4.12.3.3 Sobre el campo nuevo password y confirmar nuevo password

Si los datos ingresados tiene una longitud menor a 10 o mayor a 40 (Es posible que no vea el mensaje asociado a una longitud mayor a 40 debido a que la cantidad máxima de caracteres permitidos en el campos es 40). Usted verá alguno de los siguientes mensajes:

- `el valor es mayor a la longitud máxima permitida '40'.`
- `el valor es menor a la longitud mínima permitida '10'`

Si no ingresa ningún texto, usted verá:

- `campo obligatorio`

Si el password ingresado no cumple con las características mínimas definidas, usted verá alguno de los siguientes mensajes dependiendo de la característica que no cumpla:

- `contiene una letra no permitida, verifique que no haya letras con acento, espacios o letras ñ`
- `debe contener al menos una letra minúscula`
- `debe contener al menos una letra mayúscula`
- `debe contener al menos un número`
- `debe contener al menos un caracter especial`

5 GLOSARIO

Credencial: Información relacionada con el usuario, almacena su llave privada y certificado digital.

Usuario PKI Roaming: Usuario que almacena sus credenciales en un servidor y pueden ser accedidas de forma remota por medio de un *password*. Evita que el usuario almacene en su equipo de cómputo archivos que contengan las credenciales o el uso de dispositivos físicos adicionales.

Password: Contraseña o código de acceso, para que un usuario pueda acceder a sus credenciales.

Login: Identificación de la credencial del usuario. Este es generado de forma automática por la aplicación.

Crear certificado: Crear las credenciales de un usuario.

Recuperar certificado: Si el usuario ha bloqueado sus credenciales o ha olvidado el password, puede recuperarlo asignando una nueva contraseña.

Authentication Code / Reference number: Códigos de seguridad generados por El Banco de La República y entregados a un usuario que va a crear o recuperar un certificado. Estos códigos permiten controlar la creación de credenciales.

6 HISTORIA DE CAMBIOS DEL RESGISTRO

Tipo de Cambio	Fecha	Autor
Creación	Octubre 1 / 2007	Marcelo Domínguez
Actualización, se cambia definición de campo "password" por "nuevo password" en el punto 4.5 "página de datos de certificado". Se actualiza imagen 6. "página de datos de certificado"	Noviembre 6 / 2007	Marcelo Domínguez Marmolejo