Fecha: 08 SEP 2021

Destinatarios: Entidades usuarias SEBRA y demás entidades que empleen en su operación identidades electrónicas generadas por el Banco (en adelante Entidades Usuarias).

ASUNTO 7: FIRMA ELECTRÓNICA

La presente circular remplaza en su totalidad la Circular Externa Operativa y de Servicios DG-T-294 del 21 de abril de 2020 y 19 de marzo de 2019, correspondiente al Asunto 7: "DPC - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI CA BANREP", del manual corporativo de la Dirección General de Tecnología.

Como principales novedades se destaca lo siguiente:

- Se modifica el nombre del asunto de DPC - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI CA BANREP por el de “FIRMA ELECTRÓNICA”.
- Se reglamenta el uso de la Firma Electrónica para los servicios electrónicos ofrecidos por el Banco de la República.
- Se incorporan los conceptos y tipos de Identidad Electrónica e Instrumentos de Firma Electrónica.
- Se describen los procedimientos operativos para la gestión de las Identidades Electrónicas generadas por el Banco.
- Se detallan las obligaciones y responsabilidades de las partes involucradas.
- Se indican las condiciones de transición para homologar los certificados digitales vigentes generados por el Banco como identidades electrónicas.

Atentamente,

MARCELA OCAMPO DUQUE
Gerente Ejecutiva

LUIS FRANCISCO RIVAS DUEÑAS
Subgerente General de Servicios Corporativos

ASUNTO 07: FIRMA ELECTRÓNICA

1 OBJETO

Establecer los términos y condiciones para habilitar el uso de la firma electrónica en los servicios electrónicos ofrecidos por el Banco de la República (en adelante, el Banco), así como las modalidades y los procedimientos operativos relacionados, de conformidad con la normatividad vigente.

2 ASPECTOS JURÍDICOS

2.1 Fundamentos Jurídicos

La firma electrónica se emplea teniendo en cuenta el marco legal colombiano, en particular:

- La Ley 527 de 1999 que regula, entre otros aspectos, la firma digital y la firma electrónica.
- El artículo 244 del Código General del Proceso, adoptado mediante la Ley 1564 de 2012, el cual establece que se presumen auténticos los documentos en forma de mensajes de datos.
- El Decreto 2364 de 2012 (compilado en el Decreto Único Reglamentario 1074 de 2015) que reglamenta el artículo 7º de la Ley 527 de 1999 sobre la firma electrónica.

2.2 Política de Confidencialidad

El Banco de la República mantendrá la confidencialidad y reserva que legalmente corresponda en relación con la información recibida en desarrollo de las actividades y procedimientos descritos en la presente circular, tanto de las Entidades Usuarias, los Delegados con Responsabilidad Administrativa como de los Suscriptores, sin perjuicio de la información que de conformidad con las normas legales deba suministrar a las autoridades judiciales o administrativas competentes.

2.3 Protección de Datos Personales

En cumplimiento del régimen de protección de datos personales (Ley 1266 de 2008, Ley 1581 de 2012, Decreto 1074 de 2015 y demás normas que los modifiquen, complementen o sustituyan), el Banco de la República informa su política sobre el tratamiento de los datos personales proporcionados en el curso de los procedimientos descritos en la presente Circular Externa Operativa y de Servicios para las Entidades Usuarias, los Delegados con Responsabilidad Administrativa y Suscriptores.

Datos Generales - Responsable: Banco de la República, NIT No. 8600052167, Oficina Principal: Bogotá D.C. Contacto: A través del Sistema de Atención al Ciudadano (SAC): Puntos de atención presencial, Centro de atención telefónica (Línea gratuita nacional: 01 8000 911745), atención vía Web. Para mayor información, consulte la página Web del Banco de la República http://www.banrep.gov.co/atencion-ciudadano en la sección "Sistema de Atención al Ciudadano (SAC)".

Finalidad del tratamiento: Los datos personales suministrados por las Entidades Usuarias, los Delegados con Responsabilidad Administrativa y Suscriptores o que se deriven de los procesos acá

descritos son objeto de tratamiento (recolección, almacenamiento, uso, circulación o supresión) con la finalidad de cumplir con las actividades propias relacionadas con la Firma Electrónica descrita en la presente Circular, incluyendo la construcción de indicadores y estadísticas para el seguimiento y control de la prestación de dicho servicio, los controles de ley, la gestión, atención y trámite de las peticiones, quejas, reclamos, solicitudes de revisión, así como para dar cumplimiento a sus funciones constitucionales y legales.

El Banco de la República está comprometido con la seguridad y protección de los datos personales, y sus sistemas de gestión para manejo de información cuentan con las certificaciones vigentes ISO 9001 e ISO/lEC 27001, esta última referida a la seguridad de la información. De esta manera, buena parte de las políticas y estándares del sistema de gestión de la información de la Entidad están enfocadas a proteger la confidencialidad de la información: dispositivos de control de acceso y/o autenticación a la red, software para manejar niveles de autorización, monitorización de actividad en los sistemas y registro de estas actividades son algunos de los mecanismos que soportan estas políticas y estándares. La conservación de los documentos e información se efectúa en cumplimiento y dentro de los términos señalados en el artículo 55 de la Ley 31 de 1992.

Ejercicio de los derechos de los titulares de los datos personales: Los titulares de los datos personales podrán acceder, conocer, actualizar y rectificar dichos datos; ser informados sobre el uso dado a los mismos y la autorización con que se cuenta para ello; presentar consultas y reclamos sobre el manejo de tales datos; revocar la autorización o solicitar la supresión de sus datos, en los casos en que sea procedente, y los demás derechos que le confiere la Ley. Para ejercer tales derechos podrán contactarse a través de los mecanismos antes mencionados. Los procedimientos y términos para la atención de consultas, reclamos y demás peticiones referidas al ejercicio del derecho de habeas data seguirán lo dispuesto en la Ley 1266 de 2008 y los principios sobre protección de datos contemplados en la Ley 1581 de 2012.

Políticas o lineamientos generales de tratamiento de los datos personales: Puede consultarse en la página web del Banco de la República http://www.banrep.gov.co/proteccion-datos-personales en la sección “Protección de Datos Personales – Habeas Data”.
Fecha de entrada en vigencia: 16 de diciembre de 2016.

3 DESCRIPCIÓN Y CONDICIONES DE LA FIRMA ELECTRÓNICA

3.1 Identidad Electrónica

Corresponde a la identificación en formato electrónico asignada a una persona natural o jurídica (quien en adelante se denominará ***Suscriptor***) perteneciente a una Entidad Usuaria.

Un Suscriptor recibe una identidad electrónica que es utilizada para asegurar la autenticación, integridad y el no repudio en la información de la cual es originador. Esta identidad electrónica se denominará ***Identidad de firma***. Para los casos en que la información requiere grado de

confidencialidad, el Suscriptor recibe una segunda identidad electrónica que le permite operar con información cifrada criptográficamente. Esta identidad electrónica se denominará ***Identidad de cifrado***.

La Firma Electrónica se apalanca en una Infraestructura de Llaves Públicas (PKI) en la cual cada identidad electrónica consta de dos llaves (claves criptográficas), una denominada ***Llave Privada*** mediante la cual el suscriptor realiza la operación de firma o desciframiento de información, según sea el caso, y, otra llave, denominada ***Llave Pública***, mediante la cual el Banco de la República o un tercero puede realizar un proceso de verificación de firma o de cifrado de información, según sea el propósito.

Para tener disponible una identidad electrónica el Suscriptor requiere de dos códigos que serán generados en el proceso de solicitud respectivo. Para dar cumplimiento a la exclusividad de los datos de creación de la firma, el primer código (denominado ***Código de Autorización***) es suministrado al Suscriptor (mediante Acta de Aceptación de los términos de uso, forma ***BR-3-986-0***) una vez su solicitud de enrolamiento ha sido autenticada, validada y su identidad electrónica ha sido registrada por el Banco. El segundo código (denominado ***Número de Referencia***) es suministrado al Suscriptor una vez el Banco recibe copia digitalizada del Acta de Aceptación de los términos de uso, firmada y enviada desde el correo electrónico institucional del Delegado con Responsabilidad Administrativa de la respectiva entidad[1]. Con este segundo código, el Suscriptor realiza la creación y activación de su identidad electrónica. Este procedimiento se denomina ***Activación*** de la identidad electrónica y está descrito en la sección 3.6. Procedimientos Operacionales.

3.1.1 Identidad Electrónica para Persona Natural

Este tipo de identidad electrónica denominada "***Pertenencia a Empresa***" permite identificar y autenticar a una persona natural que en nombre de una Entidad Usuaria va a realizar intercambios de información con el Banco. La identidad electrónica se conforma a partir de los datos identificadores del Suscriptor (nombre completo, número de identificación y cuenta de correo institucional) y de los datos de identificación de la Entidad Usuaria que representa (número de identificación - NIT, dirección, domicilio y nombre de la entidad). Las Entidades Usuarias podrán solicitar y disponer de tantas identidades electrónicas de este tipo como requieran en su operación con el Banco.

3.1.2 Identidad Electrónica para Persona Jurídica

Este tipo de identidad electrónica denominada "***Persona Jurídica Entidad Empresa***" permite identificar y autenticar a una persona jurídica para habilitar procesos de integración de sistemas con el Banco. Se cuenta con los siguientes tipos de identidad electrónica:

a) Automatización de procesos criptográficos
b) Consumo de servicios de Mensajería
c) Integración de operaciones en un esquema B2B - "*Business to Business*"

[1] Persona designada y autorizada por la Entidad Usuaria para gestionar novedades relacionadas con sus suscriptores.

Para el primer caso, la identidad electrónica se conforma a partir de los datos identificadores de la Entidad Usuaria (número de identificación - NIT, dirección, domicilio, nombre de la entidad) y del acrónimo del servicio electrónico del cual la entidad es cliente. Para los servicios de mensajería y de integración B2B se emplea adicionalmente el prefijo **MBR** o **SB**, respectivamente.

Las Entidades Usuarias podrán solicitar y disponer de una identidad electrónica por cada tipo de operación (procesos criptográficos, mensajería o B2B) y por cada servicio electrónico u operación que realicen con el Banco.

3.2 Vigencia y Costo

Todas las identidades electrónicas generadas por el Banco tendrán una vigencia de dos (2) años. Tanto las activaciones como la gestión de novedades (renovaciones y revocaciones) no tendrán costo.

3.3 Instrumento de Firma Electrónica

Los pares de llaves correspondientes a una identidad electrónica (Llave Privada y Llave Pública) son generados y almacenados en el momento de activación en un dispositivo físico (*hardware*) o en un contendor digital (*software*) que se denominará ***Instrumento de Firma Electrónica - IFE***. Aunque el *IFE* contiene por defecto la identidad de firma de un Suscriptor, este podrá también almacenar la identidad de cifrado para los casos en que por requerimientos del servicio se haya definido el requisito de confidencialidad.

Todas las identidades electrónicas de tipo ***Pertenencia a Empresa*** de un Suscriptor estarán almacenadas en un único *IFE*. Dependiendo el tipo de *IFE* asociado a la identidad electrónica, este será custodiado por el Suscriptor o por el Banco de la República.

3.3.1. Identidad Electrónica en Dispositivo Físico

La tecnología criptográfica empleada para la construcción de estos dispositivos permite generar y almacenar las llaves que conforman la identidad electrónica dentro del ambiente protegido del dispositivo (denominado ***Token Criptográfico***). Estos dispositivos permiten doble factor de autenticación, operaciones compatibles con los algoritmos criptográficos empleados por la infraestructura PKI del Banco y portabilidad de las llaves, vía puertos USB.

Para operacionalizar este *IFE*, en la estación de trabajo del suscriptor se debe instalar el componente de software que gestiona el token criptográfico, así como el componente de software que interactúa con la plataforma PKI del Banco para la gestión de las llaves que componen la identidad electrónica. Los detalles técnicos asociados a este *IFE* están descritos en el documento *DSI-GI-128 Manual para la gestión de Instrumentos de Firma Electrónica emitidos el Banco de la República*, publicado en la página web del Banco, en el vínculo: http://www.banrep.gov.co/es/contenidos/pki

Toda vez que la generación de las llaves se realiza de manera local a la estación de trabajo del Suscriptor la conservación de la traza de auditoría de estos procesos es responsabilidad del mismo. De igual forma, es responsabilidad del Suscriptor la custodia y protección del *IFE*.

3.3.2. Identidad Electrónica en Contenedor Digital

Este tipo de *IFE* está generalmente asociado a una identidad electrónica de tipo Persona Jurídica Entidad Empresa. Las llaves que conforman la identidad electrónica son generadas y almacenadas en un contenedor o archivo digital en la estación de trabajo del Suscriptor. Este contenedor es protegido mediante una contraseña fuerte generada en el proceso de activación de la identidad.

Para operacionalizar este *IFE*, en la estación de trabajo del Suscriptor se debe instalar el componente de software que interactúa con la plataforma PKI del Banco para la gestión y uso de las llaves que componen la identidad electrónica. Después de realizar la activación de la identidad, este *IFE* permite la exportación de las llaves almacenadas a un nuevo archivo electrónico (formatos PKCS#12, JKS, entre otros) facilitando así la interoperabilidad en los sistemas informáticos de la Entidad Usuaria. Este procedimiento se denomina "**Transformación de Credenciales**" y se encuentra descrito en el documento *DSI-GI-128 Manual para la gestión de Instrumentos de Firma Electrónica emitidos el Banco de la República*, publicado en la página web del Banco, en el vínculo: http://www.banrep.gov.co/es/contenidos/pki

Toda vez que la generación de las llaves se realiza de manera local a la estación de trabajo del Suscriptor la conservación de la traza de auditoría de estos procesos es responsabilidad del Suscriptor. De la misma manera, es responsabilidad del Suscriptor la custodia y protección del *IFE*.

3.3.3. Identidad Electrónica Virtualizada

En este tipo de *IFE* las llaves que conforman la identidad electrónica son generadas y almacenadas en un repositorio seguro dentro de la infraestructura del Banco de la República. El acceso por parte del Suscriptor a su *IFE* es protegido mediante una contraseña fuerte generada en el proceso de activación de la identidad.

Para operacionalizar este *IFE*, en la estación de trabajo del Suscriptor se debe instalar el componente de software que interactúa con la plataforma PKI del Banco para la gestión y uso de las llaves que componen la identidad electrónica.

Los detalles técnicos asociados a este *IFE* están descritos en el documento *DSI-GI-128 Manual para la gestión de Instrumentos de Firma Electrónica emitidos el Banco de la República*, publicado en la página web del Banco, en el vínculo: http://www.banrep.gov.co/es/contenidos/pki

Toda vez que la generación y almacenamiento de las llaves se realiza dentro de la infraestructura tecnológica del Banco, la conservación de la traza de auditoría de estos procesos, así como la custodia y protección de los *IFEs* es de responsabilidad del Banco.

3.4 Modalidades de Firma Electrónica

3.4.1 Firma Electrónica

La firma electrónica de un mensaje de datos es un nuevo bloque de datos calculado a partir del mismo mensaje de datos y de la identidad de firma del Suscriptor a través de un componente de hardware o software propio o de terceros. La tecnología asociada a este proceso permite asegurar que este nuevo bloque de datos identifica inequívocamente al Suscriptor originador del mensaje y que el mensaje de datos no ha sido alterado, y asegura también el no repudio de la información originada.

Para los casos en que el IFE se encuentre bajo responsabilidad del Suscriptor, el cálculo de la firma electrónica y la traza de auditoría de estos procesos se realizan y conservan dentro del ecosistema tecnológico del Suscriptor.

3.4.2 Firma Electrónica Centralizada

En esta modalidad se emplea una identidad electrónica virtualizada, razón por la cual el cálculo de la firma electrónica y la traza de auditoría del proceso se realizan y conservan dentro de la infraestructura del Banco.

3.5 Aspectos Técnicos

El documento *DSI-GI-129 Aspectos técnicos del Servicio de Firma Electrónica del Banco de la República*, disponible en la página web del Banco, en el vínculo: http://www.banrep.gov.co/es/contenidos/pki, describe los aspectos técnicos relacionados con la firma electrónica tales como: seguridad de la información, controles de seguridad, registros de auditoria y gestión de incidentes y vulnerabilidades.

3.6 Procedimientos Operacionales

La gestión de solicitudes y novedades asociadas a la Firma Electrónica son llevadas a cabo por el Grupo de Administración de Usuarios del Departamento de Servicios de Tecnología Informática del Banco (La información de contacto está prevista en el numeral 9. INFORMACIÓN ADICIONAL de esta circular).

Los casos de excepción a estos procedimientos se encuentran descritos en la sección 3.7 Procedimientos Operativos de Excepción.

Los formatos para solicitud y gestión de las identidades electrónicas están disponibles en la página web del Banco, en el vínculo: https://www.banrep.gov.co/es/sebra

MQD

ASUNTO 07: FIRMA ELECTRÓNICA

3.6.1 Procedimiento para Enrolamiento de una Identidad Electrónica

3.6.1.1 Solicitud de Enrolamiento de Identidad Electrónica para Delegados con Responsabilidad Administrativa

a) El Representante Legal de la Entidad Usuaria diligencia en su totalidad el formato *Delegación para la Gestión de Identidades Electrónicas del Banco de la República* (Formato ***BR-3-986-1***). La firma del Representante Legal debe tener constancia de reconocimiento de firma y contenido ante notario público. Una vez realizado este trámite, el Representante Legal, desde su cuenta de correo corporativa, debe enviar al buzón de correo electrónico ca-novedades@banrep.gov.co este documento junto con un Certificado de existencia y representación legal de la entidad y/o Certificado de la Cámara de Comercio con fecha de expedición menor a treinta (30) días calendario.
b) El Grupo de Administración de Usuarios verifica la identidad del solicitante y el correcto diligenciamiento del formato.
c) Una vez verificada la solicitud, el Grupo de Administración de Usuarios procede a registrar la identidad electrónica del Delegado con Responsabilidad Administrativa y a generar los códigos (Número de Referencia y Código de Autorización) para la activación por parte del Delegado con Responsabilidad Administrativa.

3.6.1.2 Solicitud de Enrolamiento de Identidad Electrónica para Personas Naturales y Jurídicas

a) Para solicitar una identidad electrónica para Persona Natural, el Delegado con Responsabilidad Administrativa de la Entidad Usuaria registra en el Sistema SEBRA, opción "*Portal de Gestión de Identidades*" las Novedades de Suscriptor, especificando los datos requeridos para este tipo de identidad. Si la solicitud tiene como objeto una identidad para Persona Jurídica, el Delegado con Responsabilidad Administrativa procederá a diligenciar el formato ***BR-3-986-2*** - *Novedades del Suscriptor – Identidad Electrónica Banco de la República*, especificando los datos requeridos para este tipo de identidad.
b) El Grupo de Administración de Usuarios verifica la información recibida a través de la plataforma tecnológica y procede a registrar la identidad electrónica y a generar los códigos (Número de Referencia y Código de Autorización) para su activación por parte del Suscriptor.

3.6.2 Procedimiento para Activación de Identidad Electrónica

En términos generales este procedimiento es el mismo para los diferentes tipos de identidad (Persona Natural y Persona Jurídica). Se indica, cuando así se requiera, quién origina o quién recibe la información particular en cada actividad del flujo.

a) El Código de Autorización generado como resultado del proceso de solicitud será enviado por el Banco vía correo electrónico dentro del contenido del *Acta de Aceptación de los términos de uso – Firma Electrónica BANREP* ***(BR-3-986-0)*** directamente al buzón electrónico institucional del Suscriptor especificado en la solicitud. En caso de que se esté tramitando la identidad electrónica para el tipo Persona Jurídica o para el Delegado con Responsabilidad

Administrativa, se empleará el buzón electrónico institucional de este último, quien ejercerá el rol de Suscriptor para efectos de este procedimiento.

b) El Suscriptor debe imprimir y firmar el Acta antes citada y remitir copia digitalizada de la misma al Delegado con Responsabilidad Administrativa de su entidad.
c) El Delegado con Responsabilidad Administrativa procede a validar la identidad del solicitante verificando además que la información consignada en el Acta firmada por el Suscriptor esté conforme con la información suministrada en la solicitud realizada para esta identidad electrónica. En el caso de existir discrepancias en los datos del Suscriptor, el Delegado con Responsabilidad Administrativa deberá realizar una nueva solicitud y tramitar la eliminación del usuario ya creado en el Portal de Identidades.
d) Validada la identidad del Suscriptor, el Delegado con Responsabilidad Administrativa debe enviar a la dirección de correo electrónico *ca-novedades@banrep.gov.co* una copia digitalizada del Acta, firmada electrónicamente con su propia identidad. Si esta información no es recibida por el Banco a más tardar 24 horas antes de la expiración del Código de Autorización, el Delegado con Responsabilidad Administrativa deberá realizar una nueva solicitud.
e) Una vez el Grupo de Administración de Usuarios recibe el *Acta de Aceptación de los términos de uso*, verifica la firma del documento y procede a enviar el Número de Referencia al correo electrónico institucional del Suscriptor. En caso de estar tramitando la identidad electrónica para el Delegado con Responsabilidad Administrativa, se enviará el Número de Referencia para activación de su identidad electrónica una vez verificada la solicitud realizada por el representante legal.
f) Con el Código de Autorización y el Número de Referencia en poder del Suscriptor, éste podrá proceder con la activación de su identidad electrónica. Los requisitos y la descripción detallada del procedimiento de activación se presentan en el manual *DSI-GI-128 Manual para la gestión de Instrumentos de Firma Electrónica emitidos el Banco de la República*, publicado en la página web del Banco, en el vínculo: http://www.banrep.gov.co/es/contenidos/pki. En todos los casos, el proceso de activación se realizará en las instalaciones de cada entidad.
g) El Código de Autorización y el Número de Referencia podrán ser utilizados solamente una vez y dentro de los nueve (9) días calendario contados a partir de su generación. En caso de que el procedimiento de activación no se lleve a cabo en este período de tiempo, el Delegado con Responsabilidad Administrativa deberá realizar una nueva solicitud.

3.6.3 Procedimiento para Revocación de una Identidad Electrónica

La revocación es la acción explícita de anular la validez de una identidad electrónica antes de su fecha de expiración. Esta acción conduce a que esa identidad ya no podrá ser empleada por la persona natural o jurídica para procesos de firma electrónica.

Una identidad electrónica podrá ser revocada por cualquiera de las siguientes razones:

a) Porque se tenga conocimiento o existan indicios que permitan concluir que la Llave Privada asociada a la identidad electrónica o la contraseña asociada a su *IFE* haya sido divulgada o conocida por terceros así sean de la misma Entidad Usuaria.

b) Por la terminación del contrato SEBRA y/o finalización de la relación con el Banco de la República.
c) Por solicitud del Delegado con Responsabilidad Administrativa mediante comunicación en la cual se informe al Banco sobre:

1) La desvinculación o suspensión del Suscriptor de la Entidad Usuaria.
2) La imposibilidad del Suscriptor para cumplir con sus obligaciones.
3) Cambios presentados en la información contenida en la identidad electrónica del Suscriptor. Cualquier cambio de esta naturaleza deberá ser reportado de manera oportuna, registrando en el Sistema SEBRA, opción "*Portal de Gestión de Identidades*", las novedades de Suscriptor correspondientes.
4) Cualquier situación que implique riesgo de divulgación de la Llave Privada, en cuyo caso se deberá reportar tan pronto se tenga conocimiento de ello, a la dirección de correo electrónico ca-novedades@banrep.gov.co, adjuntando el formato de Novedades de Suscriptor firmado digitalmente por el Delegado con Responsabilidad Administrativa.

El procedimiento de revocación de una identidad electrónica es el siguiente:

a) El Delegado con Responsabilidad Administrativa registrará en el Sistema SEBRA, opción "*Portal de Gestión de Identidades*" las solicitudes de revocación de identidad electrónica.
b) El Grupo de Administración de Usuarios verifica y procesa las solicitudes recibidas. Para este caso, el proceso de revocación se realiza en un plazo no mayor a cuatro (4) horas hábiles una vez recibida y validada la solicitud.
c) Aplicada la revocación de la identidad electrónica, el Grupo de Administración de Usuarios, por medio de correo electrónico, enviará confirmación de la revocación al Delegado con Responsabilidad Administrativa.

3.6.4 Procedimiento para Recuperación de Información Cifrada

Este procedimiento tiene lugar cuando el Suscriptor no está disponible para descifrar los datos y la Entidad Usuaria a la cual pertenece o pertenecía requiere tener acceso a la información. El procedimiento para este caso es el siguiente:

a) El Delegado con Responsabilidad Administrativa realizará la solicitud por medio de carta firmada digitalmente por él a la cuenta ca-novedades@banrep.gov.co. En este documento deberá mencionar la fecha de retiro, la causa del retiro y el nombre completo con número de cédula del respectivo Suscriptor.
b) El Grupo de Administración de Usuarios valida la solicitud presentada y verifica su firma.
c) El Grupo de Administración de Usuarios recupera la identidad de cifrado del Suscriptor, generando así la información de activación respectiva (el Número de Referencia y el Código de Autorización).
d) El Número de Referencia y el Código de Autorización son enviados vía correo electrónico por el Banco directamente al Delegado con Responsabilidad Administrativa.
e) El Delegado con Responsabilidad Administrativa utilizará el Número de Referencia y el Código de Autorización recibido para recuperar la identidad de cifrado del Suscriptor requerido.

f) Una vez se haya recuperado la información, el Banco procederá a revocar las identidades creadas para habilitar este procedimiento.

Para que este procedimiento tenga éxito, el componente de software que interactúa con la plataforma PKI del Banco debe estar correctamente instalado en los computadores de la Entidad Usuaria. El Número de Referencia y el Código de Autorización pueden ser usados solamente una vez y deben ser usados dentro de los nueve (9) primeros días de su generación o antes de la fecha de expiración, la cual será indicada como parte del correo electrónico enviado al Delegado con Responsabilidad Administrativa.

3.6.5 Procedimiento para Conversión de Instrumento de Firma Electrónica

Este procedimiento tiene lugar cuando la Entidad Usuaria solicita que una identidad electrónica generada inicialmente en dispositivo físico se convierta a una identidad electrónica virtualizada. El procedimiento para este caso es el siguiente:

a) El Delegado con Responsabilidad Administrativa de la Entidad Usuaria registra en el Sistema SEBRA, opción "*Portal de Gestión de Identidades*", las Novedades de Suscriptor, en donde especifica la identidad electrónica para la cual se solicita la conversión.
b) El Grupo de Administración de Usuarios verifica la información recibida a través de la plataforma tecnológica y procede a recuperar la clave criptográfica del Suscriptor, generando así la información de activación respectiva (el Número de Referencia y el Código de Autorización).
c) El Código de Autorización generado como resultado del proceso de solicitud será enviado por el Banco vía correo electrónico junto con el *Acta de Aceptación de los términos de uso – Firma Electrónica BANREP (**BR-3-986-0**)* directamente al buzón electrónico institucional del Suscriptor especificado en la solicitud.
d) El Suscriptor debe imprimir y firmar esta Acta y remitir copia digitalizada de la misma al Delegado con Responsabilidad Administrativa de su entidad.
e) El Delegado con Responsabilidad Administrativa procede a validar la identidad del solicitante verificando además que la información consignada en el Acta firmada por el Suscriptor esté conforme con la información suministrada en la solicitud realizada para esta identidad electrónica. En el caso de existir discrepancias en los datos del Suscriptor, el Delegado con Responsabilidad Administrativa deberá realizar una nueva solicitud.
f) Validada la identidad del Suscriptor, el Delegado con Responsabilidad Administrativa debe enviar a la dirección de correo electrónico *ca-novedades@banrep.gov.co* una copia digitalizada del Acta, firmada electrónicamente con su propia identidad. Si esta información no es recibida por el Banco a más tardar 24 horas antes de la expiración del Código de Autorización, el Delegado con Responsabilidad Administrativa deberá realizar una nueva solicitud.
g) Una vez el Grupo de Administración de Usuarios recibe el *Acta de Aceptación de los términos de uso de la CA BANREP* firmada electrónicamente por el Delegado con Responsabilidad Administrativa, procede a verificar firma del documento y enviar el Número de Referencia al correo electrónico institucional del Suscriptor.
h) Con el Código de Autorización y el Número de Referencia en poder del Suscriptor, este podrá proceder con la recuperación de su identidad electrónica.

i) El Código de Autorización y el Número de Referencia podrán ser utilizados solamente una vez y dentro de los nueve (9) días calendario contados a partir de su generación. En caso de que el procedimiento de recuperación no se lleve a cabo en este período de tiempo, el Delegado con Responsabilidad Administrativa deberá realizar una nueva solicitud.

3.7 Procedimientos Operativos de Excepción

3.7.1 Firma Centralizada- Enrolamiento de una Identidad Electrónica por Homologación de un Certificado Digital

Para la modalidad de Firma Electrónica Centralizada, el Banco podrá, mediante un proceso automatizado, generar una nueva identidad electrónica a partir de los datos de identificación de una persona natural o jurídica obtenidos mediante el envío al Banco de un certificado digital (generado por una entidad de certificación abierta acreditada en el país) en donde el interesado aparezca como titular (sujeto) del certificado.

Esta identidad será validada en cada proceso de Firma Electrónica Centralizada, asegurando la vigencia y validez del certificado acreditado suministrado al Banco.

Los requisitos técnicos y las políticas del certificado generado por el Banco para este tipo de uso se encuentran definidos en el documento *DSI-GI-128 Manual para la gestión de Instrumentos de Firma Electrónica emitidos el Banco de la República*, publicado en la página web del Banco, en el vínculo: http://www.banrep.gov.co/es/contenidos/pki

3.8 Procedimientos Operativos de Contingencia

3.8.1 Solicitud de Enrolamiento de Identidad Electrónica para Delegados con Responsabilidad Administrativa

Cuando excepcionalmente no sea posible efectuar el reconocimiento de firma y contenido ante notario público del formato *Delegación para la Gestión de Identidades Electrónicas del Banco de la República* (Formato ***BR-3-986-1***), se deberá enviar al Banco copia digitalizada del mencionado formato, totalmente diligenciado, en las siguientes condiciones:

a) El formato deberá ser firmado mediante firma digital con un certificado digital emitido por una entidad de certificación digital abierta acreditada en el país.
b) En su defecto, se aceptará firma manuscrita digitalizada siempre y cuando el representante legal, como firmante del documento, al momento de su remisión manifieste que reconoce su firma y el contenido del mismo. Este procedimiento debe ser avalado y coordinado con el Centro de Soporte Informático del Banco.

3.8.2 Activación de Instrumento de Firma Electrónica en instalaciones del Banco de la República

El Suscriptor podrá activar su identidad en una estación del Centro de Soporte Informático del Banco, en un horario previamente acordado con el Grupo de Administración de Usuarios. Como parte de este procedimiento, se deberá firmar el *Acta de Aceptación de los términos de uso - Firma Electrónica BANREP* (***BR-3-986-0***).

3.8.3 Enrolamiento y activación de una Identidad Electrónica

Se debe manifestar la urgencia al Banco en caso de que la Entidad Usuaria no cuente con una identidad electrónica válida para operaciones, afectando el intercambio de información con los sistemas transaccionales del Banco, en casos como los siguientes:

1) El Suscriptor que regularmente realiza la operación no está disponible y los suscriptores contingentes gestionados por la Entidad Usuaria no cuentan con identidad electrónica válida.
2) No se ha hecho la recuperación de la identidad electrónica dentro de los plazos establecidos por el Banco y los códigos generados ya no están vigentes.
3) Se bloquea el dispositivo que almacena la identidad electrónica del Suscriptor titular (por fallas de autenticación, por ejemplo) y la Entidad Usuaria no cuenta con más identidades electrónicas válidas en ese momento.
4) La Llave Privada del Suscriptor ha sido comprometida y, ante ausencia de suscriptores contingentes, la nueva llave debe ser generada para mantener la operación.
5) Por daño físico del dispositivo criptográfico que almacena la identidad electrónica.

Para evitar situaciones como las que se describen, se recomienda que la Entidad Usuaria haga las gestiones respectivas para que cuente con más de una identidad electrónica válida y autorizada para realizar operaciones. Igualmente, se recuerda la importancia de que el Suscriptor tenga presente la vigencia de su identidad electrónica y adelante con la oportunidad debida las gestiones relacionadas con su renovación.

El procedimiento para atender esta contingencia operativa es el siguiente:

a) La Entidad Usuaria, contratista o proveedor del Banco deberá llamar a la línea del Centro de Soporte Informático del Banco (3431000 en Bogotá o 018000 423549 en el resto del país) para solicitar esta contingencia y deberá documentar las razones por las cuales no cuenta con una identidad electrónica válida para realizar operaciones. Aún en el caso en el que la entidad informe la necesidad de esta contingencia al área operativa del Banco con la que requiere establecer el intercambio de información deberá formalizar dicha solicitud contactando al área de Soporte Informático del Banco (ver sección 9. INFORMACIÓN ADICIONAL de esta circular).
b) El Centro de Soporte Informático del Banco reportará al Grupo de Administración de Usuarios la eventualidad reportada por la Entidad Usuaria. En caso de que exista alguna llamada o

correo enviado directamente a este Grupo para reportar la contingencia se solicitará a la entidad que realice el reporte de la novedad a través del Centro de Soporte Informático.

c) La Entidad Usuaria deberá, una vez ya se haya formalizado la contingencia, hacer uso de los canales establecidos para solicitar la creación/recuperación de la identidad electrónica.
d) El Grupo de Administración de Usuarios validará lo documentado en el caso o llamada abierta y coordinará la revisión de la información y la obtención de las respectivas aprobaciones con las demás áreas del Banco relacionadas (Jefatura de Soporte Informático y área de operativa de servicio) para atender la solicitud de manera inmediata. Si efectuada la revisión, el Banco considera que no es urgente su solución o que no hay razones válidas para atenderla a través de este procedimiento especial, se notificará a la Entidad Usuaria y la solicitud se tramitará dentro de los tiempos establecidos para una solicitud regular. De igual forma, si en el proceso se encuentra alguna irregularidad, la solicitud podrá ser rechazada.
e) Una vez la solicitud ha sido autorizada, se realizará la gestión para la emisión de la identidad electrónica y se comunicará al Centro de Soporte Informático para documentar y cerrar el caso.

4 OBLIGACIONES Y RESPONSABILIDADES

4.1 De la Entidad Usuaria:

a) Mantener actualizado el registro de Representación Legal y Delegados con Responsabilidad Administrativa.
b) Dar cumplimiento a esta circular, incluyendo las gestiones necesarias para que aquellos a quienes designe como Delegados con Responsabilidad Administrativa y como Suscriptores cumplan con las obligaciones que les corresponden.
c) Responder plenamente por el contenido de las comunicaciones enviadas por los Representantes Legales y Delegados con Responsabilidad Administrativa.
d) Asumir las consecuencias y/o perjuicios que puedan ocasionarle al Banco de la República y a terceros por el uso indebido o no autorizado de las identidades electrónicas generadas para su uso exclusivo con el Banco.
e) Mantener actualizado el software necesario para la generación de identidades electrónicas.
f) Definir esquemas operativos de contingencia que aseguren la continuidad del negocio.

4.2 Del Delegado con Responsabilidad Administrativa de la Entidad Usuaria:

a) Registrar en el Sistema SEBRA (Servicios Electrónicos del Banco de la República), opción "Portal de Gestión de Identidades" las novedades de Suscriptores a que haya lugar con el fin de mantener actualizado el registro de sus Suscriptores, garantizando que la información del Suscriptor sea completa y correcta.
b) Identificar y autenticar correctamente a los Suscriptores de la Entidad Usuaria que representa.

c) Suministrar al Banco la información correcta de identificación y autenticación del Suscriptor.
d) Revisar y gestionar la información de los Suscriptores entregada mensualmente por el Banco e informar acerca de las actualizaciones que considere necesarias.
e) Incluir en el Portal de Gestión de Identidades las respectivas novedades que considere necesarias para mantener los usuarios y claves criptográficas actualizadas (recuperación o revocación de la clave del Suscriptor).
f) Mantener vigentes y operativos los mecanismos requeridos para tramitar las novedades de sus Suscriptores.
g) Atender los procedimientos aquí descritos para los casos de contingencias.

4.3 Del Suscriptor:

a) Una vez sea generada su identidad electrónica, verificar que la información asociada a la misma sea correcta. En caso de encontrar alguna inconsistencia, informar al Grupo de Administración de Usuarios, a través del Buzón de correo electrónico ca-novedades@banrep.gov.co, para su corrección.
b) Utilizar correctamente su identidad electrónica para los fines previamente indicados por el Delegado con Responsabilidad Administrativa.
c) Utilizar correctamente el software para la generación de su *IFE*.
d) No revelar a ninguna persona la clave privada ni la información de activación de su identidad electrónica.
e) Conservar y custodiar tanto su identidad electrónica como su *IFE*, tomando las precauciones requeridas para evitar su pérdida, revelación, modificación, suplantación o uso no autorizado, incluso en los casos de conversión de su *IFE*. La identidad electrónica del Suscriptor debe ser considerada de uso personal e intransferible.
f) Solicitar la revocación de su identidad electrónica cuando se cumpla alguno de los supuestos previstos en esta circular.
g) Informar de inmediato al Grupo de Administración de Usuarios, a través del Buzón de correo electrónico ca-novedades@banrep.gov.co, cualquier situación que pueda afectar la validez de su identidad electrónica (Por ejemplo, cambio de alguno de los datos del Suscriptor).

4.4 Del Banco de la República:

a) Expedir las reglas, políticas y procedimientos sobre el uso de identidades electrónicas e *IFE*s y los servicios asociados y propender por su constante actualización.
b) Prestar los servicios relacionados con identidades electrónicas en los términos previstos en la presente circular con la debida imparcialidad, objetividad y competencia técnica.
c) Atender de manera oportuna las solicitudes presentadas por los Suscriptores y Delegados con Responsabilidad Administrativa.
d) Mantener la plataforma tecnológica que soporta los servicios vigentes, mitigando riesgos de obsolescencia.

e) Revisar de forma periódica el correcto cumplimiento de las políticas y procedimientos operativos descritos en la presente circular, en particular:

- Recibir y tramitar las solicitudes y documentos requeridos para la expedición de identidades electrónicas.
- Realizar la identificación y validación de los Delegados con Responsabilidad Administrativa de las Entidades Usuarias.
- Verificar que la información incorporada por referencia en la creación de la identidad electrónica sea exacta.
- Notificar al Suscriptor acerca de la generación de la información de activación de su identidad electrónica.
- Notificar al Delegado con Responsabilidad Administrativa y al Suscriptor de la revocación de sus identidades electrónicas cuando esta se produzca.
- Almacenar de forma segura, por el período de (1) un año, la documentación recibida por parte de las Entidades Usuarias.
- Dar respuesta a las consultas que las Entidades Usuarias realicen con respecto a la información relacionada con la Firma Electrónica.
- Eliminar, con una periodicidad semestral, los usuarios externos creados en la infraestructura PKI del Banco que se encuentren en estado adicionado o en recuperación de clave criptográfica y que no hayan hecho el proceso de activación de la clave después de tres meses.

4.5 Excepciones de Responsabilidad del Banco:

El Banco no será responsable por los siguientes eventos:

a) Los daños derivados del incumplimiento o el cumplimiento defectuoso de las obligaciones a cargo de las Entidades Usuarias, sus representantes legales, Delegados con Responsabilidad Administrativa o los Suscriptores de las mismas.
b) El uso incorrecto dado a las claves criptográficas, o los daños ocasionados como resultado de las operaciones o de las actividades cumplidas con éstos o con la información contenida en ellos.
c) Las inexactitudes o errores en las identidades electrónicas que hayan sido originados en la información suministrada por la Entidad Usuaria, el Delegado con Responsabilidad Administrativa o el Suscriptor de la misma.
d) Los daños derivados de operaciones realizadas por incumplir las limitaciones de uso señaladas en las políticas correspondientes a cada clave criptográfica.
e) Los errores o inconsistencias que puedan presentarse en el sistema de claves asimétricas, o cualquier otro riesgo no predecible de naturaleza similar, dada la complejidad de los sistemas informáticos y el propio riesgo tecnológico. Consecuentemente, de acuerdo con la costumbre internacional, la presencia de fallas para efectos legales se asimilará al caso fortuito o fuerza mayor.

5 ACUERDO SOBRE FIRMA ELECTRÓNICA

El acuerdo sobre el uso del mecanismo de firma electrónica se entenderá realizado cuando el Banco de la República reciba el *Acta de Aceptación de los términos de uso de Firma Electrónica* firmada electrónicamente por el Delegado con Responsabilidad Administrativa dentro del procedimiento para activación de una identidad electrónica. Por consiguiente, para efectos de la presunción contemplada en el artículo 2.2.2.47.7 del Decreto Único Reglamentario 1074 de 2015, se entiende que los mecanismos o técnicas de identificación personal y autenticación electrónica que se acuerdan utilizar, según lo previsto en la presente circular, cumplen los requisitos de firma electrónica.

6 CONFIABILIDAD DE LA FIRMA ELECTRÓNICA

La Firma Electrónica y Firma Electrónica Centralizada resultan confiables para cumplir con los requisitos de seguridad en la operación de los servicios electrónicos prestados por el Banco de la República en la medida en que los datos de creación de la Firma Electrónica corresponden exclusivamente al Suscriptor del Instrumento de Firma Electrónica (IFE) y en que es posible técnicamente detectar cualquier alteración no autorizada después del momento de la firma.

7 SEGURIDAD DE LA FIRMA ELECTRÓNICA

El Banco de la República determinará la seguridad en los procedimientos, métodos o dispositivos que utilice o llegue a utilizar para soportar los servicios de Firma Electrónica y Firma Electrónica Centralizada, usando entre otros, uno o varios factores tales como: concepto técnico emitido por perito u órgano independiente y especializado, una auditoría especializada, periódica e independiente.

8 TRANSITORIEDAD DE LA FIRMA DIGITAL

Para los Suscriptores que a la fecha de entrada en vigencia de esta circular posean un certificado digital vigente tipo Pertenencia a Empresa o de Persona Jurídica Entidad Empresa emitido por el Banco se dará por homologada la identificación del certificado como la identidad electrónica del Suscriptor; así mismo, el token criptográfico o el archivo digital con extensión *.epf* en poder del Suscriptor se entenderá como su *IFE.*

La implementación y el uso de Firma Electrónica Centralizada estará sujeta al desarrollo de la integración tecnológica respectiva entre el Banco y las Entidades Usuarias.

Para efectos de la transición entre el esquema de firma digital a firma electrónica, cuando se haga referencia en otras Circulares Externas Operativas y de Servicios del Banco de la República al término

"certificados digitales" u otra terminología propia de la firma digital, se entenderán referidos a las claves criptográficas e identidad electrónica y terminología propia del esquema de firma electrónica descrito en la presente circular.

9. INFORMACIÓN ADICIONAL

Para trámites operativos y consultas sobre la Firma Electrónica, los interesados pueden contactar al Centro de Soporte Informático del Banco de la Republica, Dirección General de Tecnología, Carrera 7 No. 14-78 Bogotá, Colombia, por los siguientes medios:

- Teléfono: 3431000, en horario de 6:00 am. a 9:00 p.m. de lunes a viernes, excepto días festivos
- Correo electrónico: ca-novedades@banrep.gov.co
- Fax: (571) 286 1686.

(ESPACIO DISPONIBLE)

MQD