MANUAL DE LA DIRECCIÓN GENERAL DE TECNOLOGÍA
CIRCULAR EXTERNA OPERATIVA Y DE SERVICIOS
DG-T - 294

Destinatarios: Usuarios de Servicio Electrónico PKI **Fecha:** 19 MAR 2019

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI CA BANREP

Apreciados señores:

La presente Circular Externa Operativa y de Servicios remplaza en su totalidad el **Asunto 7: "DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI CA BANREP"** contenido en la Circular Reglamentaria Externa DG-T-294 del 23 de marzo de 2018, correspondiente al Manual Corporativo de la Dirección General de Tecnología.

En esta circular se incorporan, entre otros, los siguientes aspectos relacionados con la gestión del servicio denominado PKI:

- Autoridad de Certificación Raíz de la CA BANREP
- Certificadora Subordinada de la CA BANREP
- Peticiones, quejas, reclamos, sugerencias y solicitudes de revisión
- Protección de datos personales
- Imparcialidad
- Identificación y autenticación.
- Se adicionan los servicios de estampado cronológico – TSA BANREP y de generación de firmas digitales.
- Se modifican los procedimientos de Solicitud de Certificados Digitales.
- Procedimientos de gestión de incidentes y vulnerabilidades

Adicionalmente, se modifica el nombre del Asunto pasando del "**DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI CA BANREP"** al de "**DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA CA BANREP".**

Atentamente;

MARCELA OCAMPO DUQUE
Gerente Ejecutiva

LUIS FRANCISCO RIVAS DUEÑAS
Subgerente General de Servicios Corporativos

Fecha: 19 MAR 2019

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

1. INTRODUCCIÓN

1.1 Objeto y alcance

Establecer la Declaración de Prácticas de Certificación (DPC) de la Entidad de Certificación Cerrada del Banco de la República (CA BANREP). Con el fin de incrementar los niveles de seguridad en los servicios electrónicos del Banco, de conformidad con la legislación vigente sobre mensajes de datos y firma digital, se definen las reglas para la generación y administración de claves y certificados de verificación de firma y de cifrado, el servicio de estampado cronológico, la generación de firmas digitales, así como los demás procesos y procedimientos que se deben cumplir para la operación de la CA BANREP.

1.2 Destinatarios

Los usuarios de los servicios electrónicos prestados por el Banco de la República (SEBRA) y los contratistas o proveedores de la Entidad que involucren el uso de medios electrónicos de la misma.

1.3 Condiciones Generales

El Banco de la República, identificado con NIT 860005216-7, es una entidad de derecho público, de rango constitucional, domiciliada en Bogotá y encargada de ejercer las funciones de banca central de Colombia. Está sometido a un régimen jurídico propio y especial, contenido en la Constitución Política (artículos 371 a 373), la Ley 31 de 1992 y sus Estatutos (Decreto 2520 de 1993).

La actuación del Banco de la República como Entidad de Certificación Cerrada (CA BANREP) se encuentra acreditada ante el Organismo Nacional de Acreditación de Colombia (ONAC) mediante registro de acreditación número 16-ECD-006 del 15 de agosto de 2017 (https://onac.org.co/certificados/16-ECD-006.pdf).

El certificado raíz de la CA BANREP, válido hasta el 07 de marzo de 2037 02:33:00 p.m., será utilizado exclusivamente para la emisión de certificados de autoridades de certificación subordinadas y para generar la lista de revocación de certificados de autoridades de certificación subordinada. Los certificados de CA subordinada a su vez emitirán los certificados de uso final.

1.4 Autoridad de Certificación Raíz de la CA BANREP

La Autoridad de Certificación Raíz (CA) es la autoridad de certificación Raíz de la Infraestructura de Clave Pública de la CA BANREP cuya función principal es emitir los certificados digitales a su plataforma de certificación digital. Los Certificados Digitales de Clave Pública de la CA BANREP son generados de acuerdo al estándar X.509 versión 3 (1996). Este estándar, que define la estructura

del Certificado de Clave Pública, es definido y mantenido por la Unión Internacional de Telecomunicaciones (UIT) y por la ISO (Organización de Estándares Internacionales).

El certificado raíz corresponde a un certificado que ninguna entidad de confianza superior firma digitalmente como raíz, es decir es un certificado auto firmado, estableciéndose a partir de allí la cadena de confianza. Esta característica también hace que en la estructura del certificado los valores de Nombre Distintivo (DN por sus siglas en idioma inglés) para Emisor y Sujeto sean los mismos. Para el caso del certificado raíz de la CA BANREP, el DN está compuesto por los siguientes valores:

- OU = CA Banrep Root
- OU = CA Banrep
- DC = banrep
- DC = gov
- DC = co

1.5 Certificadora Subordinada de la CA BANREP

Siguiendo el marco normativo y las buenas prácticas de la industria, dentro de la jerarquía de la CA BANREP se creó la entidad certificadora CA BANREP SUBORDINADA (cuyo certificado es firmado por la CA Raíz BANREP), siendo esta quien emite los certificados digitales a los usuarios finales (Suscriptores).

El DN del Emisor corresponde al DN del certificado raíz de la CA BANREP. El DN del sujeto de la certificadora subordinada está compuesto por los siguientes valores:

- OU = CA Banrep Root
- OU = CA Banrep
- DC = banrep
- DC = gov
- DC = co

Este certificado tiene validez hasta el 07 de enero de 2037 12:00:00 am.

1.6 Identificación

El nombre de la DPC es: Declaración de Prácticas de Certificación para la CA BANREP.

El identificador de objeto para esta DPC es 1.3.6.1.4.1.14236.1.2.1. De acuerdo a los códigos asignados al Banco de la República por la IANA (Internet Assigned Number Authority) (https://oidref.com/1.3.6.1.4.1.14236).

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

1.7 Responsables

1.7.1 Administración de la DPC

La dependencia del Banco de la República responsable de la administración de la DPC para la CA BANREP es el Departamento de Seguridad Informática de la Dirección General de Tecnología.

1.7.2 Contacto

Centro de Soporte Informático del Banco de la Republica.
Dirección General de Tecnología
Carrera 7 No. 14-78 Bogotá, Colombia
Teléfono: 3431000
E-mail: admon-ca-banrep@banrep.gov.co
Fax: (571) 286 1686

1.8 Información sobre la organización de la DPC

La DPC contenida en el presente documento ha sido elaborada con base en el documento RFC-3647, marco de trabajo para políticas de certificados y prácticas de certificación elaborado por la **International Engineering Task Force** (IETF) (http://www.ietf.org/rfc/rfc3647.txt?number=3647) y con base en el documento RFC-3628 marco para la definición de requerimientos para Autoridades de Estampado de Tiempo - TSAs (Time-Stamping Authorities) (https://tools.ietf.org/html/rfc3628).

1.9 Peticiones, quejas, reclamos, sugerencias y solicitudes de revisión

Para presentar cualquier petición, queja, reclamo, sugerencia o felicitación pueden utilizarse los canales establecidos en el Sistema de Atención al Ciudadano del Banco de la República en el siguiente vínculo: http://www.banrep.gov.co/es/atencion-al-ciudadano

Igualmente, en los eventos en que se requiera solicitar la revisión de alguna actuación/decisión de la CA BANREP, puede presentarse una solicitud de revisión a través del Sistema de Atención al Ciudadano. Para el efecto, se podrá ingresar por la opción Formulario Electrónico (https://totoro.banrep.gov.co/FormularioElectronico/), indicando en la sección de "*Datos Generales*" que el Tipo de Solicitud corresponde a una "*Petición*" y seleccionando como Categoría la opción "*Sistemas de pago y servicios bancarios*". En la sección denominada "*Detalles de la Solicitud*", en el primer campo de esta sección denominado "*Si usted ha realizado una solicitud anterior, enuncie el número correspondiente (C16-XXX).*", el usuario debe escribir "***SOLICITUD REVISIÓN ECD BANREP***". En la lista desplegable denominada "*Sucursal Banco*", se debe seleccionar "*Bogotá*" y en el campo de texto "*Mensaje*", deberá presentar en forma resumida (máximo 5,000 caracteres) en que consiste su solicitud de revisión.

2. CONDICIONES GENERALES

2.1 Obligaciones

2.1.1 Obligaciones generales de la CA BANREP:

2.1.1.1 Expedir las reglas, políticas y procedimientos sobre el uso de los Certificados Digitales, el uso del servicio de estampado cronológico, la generación de firmas digitales, y propender por su constante actualización.

2.1.1.2 Prestar el servicio de emisión de certificados y estampado cronológico conforme a los términos previstos en la presente DPC.

2.1.1.3 Atender las peticiones, quejas, reclamos y solicitudes de revisión presentadas por los suscriptores.

2.1.1.4 Mantener actualizadas las bases de datos de Certificados vigentes y revocados. La lista de Certificados revocados será publicada cada cinco (5) minutos.

2.1.1.5 Mantener la plataforma tecnológica vigente mitigando riesgos de obsolescencia.

2.1.1.6 Prestar los servicios con imparcialidad, objetividad y competencia técnica de las actividades y de las personas involucradas en el proceso de certificación digital, así como tomar las medidas necesarias para evitar cualquier influencia que pueda afectarla, realizando un proceso de revisión y seguimiento para la identificación y gestión de amenazas a la imparcialidad en aras del mejoramiento continuo de los servicios.

2.1.1.7 Informar a los proveedores la exigencia de cumplir los requisitos establecidos en el documento Criterios Específicos de Acreditación CEA (4.1-10) establecidos por ONAC, cuando sean aplicables.

2.1.1.8 Cumplir con los Criterios Específicos de Acreditación (CEA) 4-1.10 publicados en la página web del Organismo Nacional de Acreditación de Colombia - ONAC.

2.1.1.9 Informar a la ONAC la ocurrencia de cualquier evento establecido en la Declaración de Prácticas de Certificación que comprometa la prestación del servicio.

2.1.2 Obligaciones específicas como Entidad de Registro (ER):

La Entidad de Registro (ER) gestiona las solicitudes de novedades de certificados digitales. Son obligaciones de la ER las siguientes:

2.1.2.1 Recibir y tramitar las solicitudes y documentos requeridos para la expedición de Certificados, según esta DPC.

2.1.2.2 Realizar la identificación y validación de los Delegados con Responsabilidad Administrativa de las Entidades Usuarias.

2.1.2.3 Verificar que la información incorporada por referencia en el Certificado sea exacta.

2.1.2.4 Notificar al Suscriptor de la generación de la información de activación del Certificado.

2.1.2.5 Notificar al Delegado con Responsabilidad Administrativa y al Suscriptor de la revocación de su Certificado cuando esta se produzca por decisión de la CA BAN

REP en caso de incumplimiento de lo mencionado en el numeral 2.1.5 – Obligaciones del Suscriptor.

2.1.2.6 Atender las solicitudes de revocación de Certificados en el término de tres (3) días hábiles. Para los casos en los cuales la Entidad Usuaria requiera que la solicitud sea atendida en un tiempo menor y con carácter urgente, el Delegado con Responsabilidad Administrativa de la Entidad Usuaria deberá comunicarse telefónicamente al Centro de Soporte Informático al teléfono 3431000 en horario de 6:00 am - 9:00 pm en días hábiles, de lunes a viernes.

2.1.2.7 Eliminar el registro de los Suscriptores que han sido solicitados por parte de los Delegados con Responsabilidad Administrativa, cuando transcurrido más de un (1) mes del envío de la información de activación del Certificado, no se ha realizado la generación del mismo.

2.1.2.8 Almacenar de forma segura, por el período de (1) un año, la documentación recibida en los procesos de emisión de Certificados y de revocación de los mismos.

2.1.2.9 Dar respuesta a las consultas que las Entidades Usuarias realicen con respecto a la información relacionada con CA BANREP.

2.1.2.10 Cumplir con las demás obligaciones que se establecen en esta DPC.

2.1.3 Obligaciones de la Entidad Usuaria:

2.1.3.1 Mantener actualizado el registro de representación legal y Delegados con Responsabilidad Administrativa ante la ER.

2.1.3.2 Dar cumplimiento a esta DPC, incluyendo las gestiones necesarias para que aquellos a quienes designe como Delegado con Responsabilidad Administrativa y como Suscriptores cumplan con las obligaciones que les corresponden; y cumplir, así mismo, con la normatividad y regulaciones que rigen el uso de los Certificados Digitales.

2.1.3.3 Responder plenamente por el contenido de las comunicaciones enviadas por los representantes legales, Delegados con Responsabilidad Administrativa y Suscriptores, acompañadas de Firmas Digitales y Certificados, que al ser verificadas por el Banco de la República se considerarán auténticas.

2.1.3.4 Asumir las consecuencias y/o perjuicios que puedan ocasionarse al Banco de la República y a terceros, por el uso indebido o no autorizado de las Firmas Digitales, Certificados y del Software requerido para la operación de los mismos.

2.1.3.5 Cualquier otra que se derive de la ley o del contenido de esta DPC.

2.1.3.6 Mantener actualizado el software necesario para la generación de firmas digitales.

2.1.4 Obligaciones del Delegado con Responsabilidad Administrativa de la Entidad Usuaria:

2.1.4.1 Registrar en el Sistema SEBRA[1] (Servicios Electrónicos del Banco de la República), opción "Portal de Gestión de Identidades", las novedades de Suscriptores a que haya

[1] https://wsebra.banrep.gov.co

lugar con el fin de mantener actualizado el registro de suscriptores de la Entidad Usuaria, garantizando que la información del Suscriptor sea completa y correcta.

2.1.4.2 Identificar y autenticar correctamente a los Suscriptores de la Entidad Usuaria a la que pertenece, conforme a los procedimientos que se establecen en esta DPC, dentro de los cuales se especifica la documentación requerida.

2.1.4.3 Suministrar la información correcta de identificación y autenticación del Suscriptor a la ER.

2.1.4.4 Revisar la información de los Suscriptores entregada por la CA BANREP e informar las actualizaciones que considere necesarias.

2.1.4.5 Mantener vigente y operativos los mecanismos requeridos para realizar las novedades de Suscriptores de la Entidad Usuaria.

2.1.4.6 Cualquier otra que se derive de la ley o del contenido de esta DPC.

2.1.5 Obligaciones del Suscriptor de la Entidad Usuaria:

2.1.5.1 Una vez sea generado el Certificado por la CA BANREP, verificar que la información asociada al mismo sea correcta; en caso de encontrar alguna inconsistencia, informar a la ER para su corrección.

2.1.5.2 Utilizar correctamente el Certificado para los fines previamente indicados por el Delegado con Responsabilidad Administrativa.

2.1.5.3 Utilizar correctamente el software del servicio para la generación de firmas digitales, según lo establecido en esta DPC.

2.1.5.4 No revelar a ninguna persona la clave privada ni la información de activación del Certificado.

2.1.5.5 Conservar y custodiar el Certificado tomando las precauciones requeridas para evitar su pérdida, revelación, modificación, suplantación o uso no autorizado, incluso en los casos en donde la credencial requiera una trasformación de formato. Los Certificados son personales e intransferibles.

2.1.5.6 Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en la sección 4.6 de la presente DPC.

2.1.5.7 Informar de inmediato a la ER acerca de cualquier situación que pueda afectar la validez del Certificado (Por ejemplo, cambio de alguno de los datos del Suscriptor).

2.1.5.8 Cualquier otra que se derive de la ley o del contenido de esta DPC.

2.1.6 Obligaciones de los Usuarios (partes confiantes):

2.1.6.1 Verificar la validez de las firmas generadas mediante el uso de Certificados emitidos por la CA BANREP y cumplir con los demás procedimientos y requerimientos de seguridad previstos en esta DPC. El Usuario será responsable del uso y la confianza que le dé a los Certificados.

2.1.6.2 Informar al Contacto de la CA BANREP cualquier irregularidad, sospecha o indicio de mala utilización de los servicios prestados por la CA BANREP.

2.2 Responsabilidad

La CA BANREP, las Entidades Usuarias, los Delegados con Responsabilidad Administrativa, los Suscriptores y los Usuarios serán responsables del cumplimiento cabal y oportuno de las obligaciones señaladas en esta DPC, y en particular, de las asignadas en la Sección 2.1., según corresponda.

2.2.1 Excepciones de responsabilidad de la CA BANREP

La CA BANREP no será responsable por los siguientes eventos:

2.2.1.1 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, y de los Usuarios previstos en esta DPC.

2.2.1.2 El uso incorrecto dado a los Certificados y/o de las claves, o los daños ocasionados como resultado de las operaciones o de las actividades cumplidas con los Certificados o con la información contenida en ellos.

2.2.1.3 Las inexactitudes o errores en los Certificados que hayan sido originados en la información suministrada por la Entidad Usuaria, el Delegado con Responsabilidad Administrativa o el Suscriptor de la misma.

2.2.1.4 Los daños derivados de operaciones realizadas por incumplir las limitaciones de uso señaladas en las políticas correspondientes a cada tipo de Certificado.

2.2.1.5 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.

2.3 Aspectos jurídicos

2.3.1 Ley aplicable

La DPC se regirá e interpretará de acuerdo con la ley colombiana y las directrices e instrucciones emitidas por el Organismo Nacional de Acreditación de Colombia (ONAC) que sean aplicables.

2.3.2 Procedimiento de resolución de conflictos con Entidades Usuarias y Usuarios

Toda controversia o diferencia que pudiera surgir entre el Banco de la República y las Entidades Usuarias y/o los Suscriptores de las mismas y los Usuarios, en relación con la interpretación y/o aplicación de esta DPC, que no pueda ser resuelta de común acuerdo, dentro de los treinta (30) días comunes siguientes al momento en que dicha controversia o diferencia haya sido planteada,

se someterá a la decisión de un tribunal de arbitramento, de conformidad con las siguientes reglas:

2.3.2.1 El tribunal tendrá su sede en Bogotá, D.C. y se regirá por las normas del Centro de Arbitraje y Conciliación Mercantiles de la Cámara de Comercio de Bogotá.

2.3.2.2 El laudo será en derecho.

2.3.2.3 El tribunal estará conformado por un (1) árbitro que será designado de común acuerdo por las partes, de las listas de árbitros inscritos en la Cámara de Comercio de Bogotá.

2.3.2.4 Si las partes no se ponen de acuerdo para el nombramiento del árbitro en un plazo de treinta (30) días comunes, la designación será hecha por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, de una lista de diez (10) abogados que las partes elaboren de común acuerdo, tomados de la relación de árbitros inscritos en esa Entidad.

2.3.2.5 Si las partes, dentro de los treinta (30) días comunes al inicio del respectivo trámite, no pudieren elaborar la lista de nombres a que hace referencia el numeral anterior, el árbitro será designado por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá, de su lista de árbitros de primer nivel ("lista A").

2.3.2.6 En todos los casos, los árbitros designados deberán sujetarse a las tarifas de gastos y honorarios establecidas por el Centro de Arbitraje y Conciliación de la Cámara de Comercio de Bogotá.

2.4 Publicación y depósito de documentos de la CA BANREP

El contenido de esta DPC, así como de toda la información que se publique en relación con la CA BANREP podrán ser consultados en el sitio web del Banco de la República[2].

2.5 Confidencialidad y protección de los datos

2.5.1 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 su actividad de entidad de certificación de CA BANREP, 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] http://www.banrep.gov.co/es/contenidos/pki

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

2.5.2 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 DPC por 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 son objeto de tratamiento (recolección, almacenamiento, uso, circulación o supresión) para efectos de las actividades propias de la CA BANREP y con la finalidad de cumplir adecuadamente con su actividad como entidad certificadora, 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/IEC 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.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

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.

2.5.3 Derechos de propiedad intelectual

El Banco de la República es titular de los derechos de propiedad intelectual relacionados con el sistema de certificación que regula esta DPC, sin perjuicio de los derechos de autor que correspondan a los proveedores de software sobre todos o algunos de los componentes del sistema. En consecuencia, está prohibida la reproducción, distribución, comunicación pública o transformación de cualquiera de los elementos que la componen. No obstante, no se requerirá autorización del Banco para la reproducción del Certificado cuando esta sea necesaria para su utilización por parte del Suscriptor y de conformidad con los usos para los cuales fue expedido, según los términos de esta DPC.

2.5.4 Imparcialidad

La CA BANREP se compromete a asegurar la imparcialidad, objetividad y competencia técnica de las actividades y de las personas involucradas en el proceso de certificación digital, siendo este un objetivo imprescindible, permanente y fundamental para la organización. Por ello se establecerán todas las medidas necesarias para evitar cualquier posible influencia debida a otras actividades desarrolladas por el Banco, realizando un proceso de mejora continua, mediante la identificación y gestión de las amenazas a la imparcialidad.

La CA BANREP realizará una reunión anual en el primer semestre para revisar los cambios presentados en la gestión de riesgos de la imparcialidad y No discriminación. En caso de requerir una revisión extraordinaria, el Departamento de Seguridad Informática programará la citada reunión.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

La CA BANREP emite dos tipos de certificados para Suscriptores:

- **CERTIFICADOS DIGITALES DE PERTENENCIA A EMPRESA (PE):** Acredita la identidad de la persona natural titular del certificado, así como su vinculación a una determinada entidad jurídica. Este certificado no otorgará por sí mismo mayores facultades a su titular que las que posee por el desempeño de su actividad habitual. Se denominará Suscriptor dentro del contenido de esta DPC.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

- **CERTIFICADOS DIGITALES DE PERSONA JURIDICA ENTIDAD EMPRESA (PJEE):** Para la realización de trámites por parte de una aplicación que se ejecutan en una máquina en procesos automáticos de firma en nombre de una persona jurídica, para los cuales se requiera garantizar la autenticidad y la integridad de los datos enviados o almacenados digitalmente junto con el establecimiento de canales de comunicación seguros, que será representada por medio de una persona física (Delegado con Responsabilidad Administrativa), poseedor del certificado emitido bajo esta política y denominado Responsable.

3.1 Certificados digitales de pertenencia a empresa (PE)

3.1.1 Identificación y autenticación

Para identificar y autenticar los datos del Suscriptor para los certificados de pertenencia a empresa de las Entidades Usuarias se empleará el Nombre Distintivo (DN) el cual está formado de la siguiente manera:

- Componente de Dominio:
  dc=co
  dc=gov
  dc=banrep
- Unidad Organizacional:
  ou=CA Banrep
  ou=CA Banrep Subordinada
  ou=NIT de la entidad incluyendo digito de verificación (sólo los caracteres numéricos)

- Nombre común:
  cn=Nombre completo del Suscriptor.

Ejemplos:

DN: cn=Pedro Andrés Perez Ramírez, ou=8030130231, ou=CA Banrep Subordinada, ou=CA Banrep, dc=banrep, dc=gov, dc=co

3.1.2 Método de prueba de posesión de la Clave Privada

CA BANREP establecerá los mecanismos para generar la creación del Certificado de sus Suscriptores en un dispositivo Hardware que cumpla como mínimo con el estándar FIPS 140-2 Nivel 3.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

3.1.3 Requerimientos para que el nombre sea significativo

Para que el nombre sea significativo se deberá seguir lo establecido en el numeral 3.1.1.

3.1.4 Autenticación de la identidad de las Entidades Usuarias

La CA BANREP solamente aceptará requerimientos de Certificados de aquellas entidades que sean reportadas por las dependencias del Banco de la República por tener relación con las operaciones que llevan a cabo, y previa verificación por la ER.

3.1.5 Autenticación de la identidad individual

En todos los casos, la activación de Certificados para Delegados con Responsabilidad Administrativa y Suscriptores se realizará en forma remota en las instalaciones de cada entidad. Para casos de contingencia, el procedimiento podrá ser efectuado en las instalaciones del Banco de la República presentando como documento de identificación la cédula de ciudadanía ante la ER. Como parte de este procedimiento, se deberá firmar el "Acta de aceptación de los términos de uso de la CA BANREP" (BR-3-599-0)[3].

3.1.6 Autenticación para regeneración de claves

Los Suscriptores son autenticados usando su par de claves de Firma Digital. Cuando una clave de Firma Digital se encuentre vencida, la ER autenticará al Suscriptor que hace la solicitud, de la misma manera, como se menciona en las secciones 3.1.4 y 3.1.5.

3.1.7 Autenticación para regeneración de claves después de revocación

La ER llevará a cabo la autenticación después de una revocación según lo descrito en las secciones 3.1.4 y 3.1.5.

3.1.8 Autenticación para la solicitud de revocación

El Delegado con Responsabilidad Administrativa registrará en el Sistema SEBRA, opción "Portal de Gestión de Identidades", las solicitudes de revocación de Certificados.

3.2 Certificados Digitales de Persona Jurídica Entidad Empresa (PJEE)

3.2.1 Identificación y Autenticación

---

[3] Disponible en http://www.banrep.gov.co/sites/default/files/paginas/BR-3-599-0.pdf
El acta será parte de la carpeta que se conforme para la respectiva Entidad Usuaria en el archivo del Departamento de Servicios de Tecnología Informática.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

Para identificar y autenticar los datos de la solicitud para los Certificados Digitales de Persona Jurídica Entidad Empresa se empleará el Distinguished Name (DN) el cual está formado de la siguiente manera, teniendo en cuenta que existen dos tipos de certificados tipo PJEE, los cuales se determinan a continuación:

- **PJEE - Para comunicaciones B2B (Business to Business):** Certificados PJEE que son usados para autenticar los servidores de las Entidades Usuarias que acceden a recursos tecnológicos del Banco de la República de forma automática.

- **PJEE - Para Automatización de procesos Criptográficos:** Certificados que serán usados por servidores en la implementación de procesos automáticos de Firma Digital y/o cifrado por parte de en las Entidades Usuarias.

3.2.2 PJEE para comunicaciones B2B (Business to Business). El DN para los Certificados PJEE que son usados para autenticar los servidores de las Entidades Usuarias que acceden a recursos tecnológicos del Banco de la República de forma automática está formado de la siguiente manera:

- **Componente** de Dominio:
  dc=co
  dc=gov
  dc=banrep

- **Unidad** Organizacional:
  ou=CA Banrep
  ou=CA Banrep Subordinada
  ou=NIT de la entidad incluyendo digito de verificación (sólo los caracteres numéricos)

- **Nombre** común:
  cn=SB-NIT de la Entidad-Nemónico de la Aplicación con la que se va a interactuar.

Notas: En el caso de entidades que interactúan con varias aplicaciones, se debe generar un Certificado para intercambiar información con cada aplicación.

Ejemplos:
cn=SB-8030130231-CUD, ou=8030130231, ou=CA Banrep Subordinada, ou=CA Banrep, dc=Banrep, dc=gov, dc=co

cn=SB-8030130231-SOI, ou=8030130231, ou=CA Banrep Subordinada, ou=CA Banrep, dc=Banrep, dc=gov, dc=co

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

3.2.3 PJEE para Automatización de procesos Criptográficos. El DN para los certificados PJEE que serán usados en la implementación de procesos automáticos de Firma Digital y/o cifrado por parte de en las Entidades Usuarias están formados de la siguiente manera:

- **Componente** de Dominio:
  dc=co
  dc=gov
  dc=banrep

- **Unidad** Organizacional:
  ou=CA Banrep
  ou=CA Banrep Subordinada
  ou=NIT de la entidad incluyendo digito de verificación (sólo los caracteres numéricos)

- **Nombre** común:
  cn=NIT de la Entidad Nemónico de la Aplicación con la que se va a interactuar.

Notas: En el caso de entidades que interactúan con varias aplicaciones, se debe generar un Certificado PJEE para intercambiar información con cada aplicación.

Ejemplos:
cn=8030130231 SOI, ou=8030130231, ou=CA Banrep Subordinada, ou=CA Banrep, dc=Banrep, dc=gov, dc=co

3.2.4 Requerimientos para que el nombre sea significativo

Para que el nombre sea significativo se deberá seguir lo establecido en los numerales 3.2.2 o 3.2.3 dependiendo del tipo de certificado.

3.2.5 Método de prueba de posesión de la Clave Privada

CA BANREP establecerá los mecanismos para generar un archivo epf (Entrust Profile), el cual puede ser transformado en formatos PKCS#12 y JKS. Al respecto, deberá tenerse en cuenta el manual "**DSI-GI-97 Manual para la gestión de certificados emitidos por la Entidad de Certificación Digital Cerrada - CA BANREP**" localizado en http://www.banrep.gov.co/es/contenidos/pki.

Para este tipo de Certificados se considera Suscriptor al Delegado con Responsabilidad Administrativa, quien deberá cumplir con lo establecido en las secciones 2.1.4 y 2.1.5.

3.2.6 Autenticación de la identidad de las Entidades Usuarias

La CA BANREP solamente aceptará requerimientos de Certificados PJEE de aquellas entidades que sean informadas por las dependencias del Banco de la República por tener relación con las operaciones que llevan a cabo, y previa verificación por la ER.

3.2.7 Autenticación de la identidad individual

Para los certificados PJEE solicitados por los Delegados con Responsabilidad Administrativa, se deberán adjuntar los documentos indicados en el numeral 4.2.4. Solicitud de Certificados Persona Jurídica Entidad Empresa (PJEE).

3.2.8 Autenticación para regeneración de claves

Cuando una clave de Firma Digital se encuentre vencida, la ER debe autenticar al Suscriptor que hace la solicitud, de acuerdo a lo descrito en las secciones 3.2.6 y 3.2.7.

3.2.9 Autenticación para regeneración de claves después de revocación

La ER llevará a cabo la autenticación después de una revocación como se especifica en las secciones 3.2.6 y 3.2.7.

3.2.10 Autenticación para la solicitud de revocación

El Delegado con Responsabilidad Administrativa registrará en el Sistema SEBRA, opción "Portal de Gestión de Identidades", las solicitudes de revocación de Certificados.

3.3 Servicio de estampado cronológico – TSA BANREP

El estampado cronológico es un servicio complementario al servicio de emisión de Certificados Digitales Pertenencia a Empresa y Persona Jurídica Entidad Empresa, en donde la CA BANREP suministra de manera electrónica un mensaje de datos firmado digitalmente por la CA BANREP, lo que permite verificar la fecha y hora exacta del momento en el cual se realiza la solicitud a la CA BANREP, garantizando que no ha cambiado desde ese momento.

El TSA BANREP genera una estampa cronológica que incluye el HASH[4] del objeto digital, un número de serie único, y la fecha y hora actual obtenida del reloj del servidor que se encuentra sincronizado con la hora legal colombiana (ver sección 6.8 Sincronización de reloj). La estampa cronológica está firmada digitalmente por la TSA BANREP.

[4] Función computacional que toma como entrada un archivo de datos y genera como salida otro archivo de datos de longitud fija.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

El certificado de la TSA BANREP es emitido por la CA BANREP Subordinada.

3.3.1 Obligaciones generales de la TSA BANREP

La TSA BANREP tiene las siguientes obligaciones como autoridad de estampado cronológico:

3.3.1.1 Respetar y cumplir las disposiciones reglamentadas en esta DPC.
3.3.1.2 Emitir estampas cronológicas que cumplen las especificaciones de la RFC 3161.
3.3.1.3 Custodiar la llave privada que utiliza la TSA BANREP (Ver Sección 6.2.1 Estándares y módulos criptográfico).
3.3.1.4 Usar una fuente fiable de tiempo como referencia temporal en el proceso de emisión de estampas cronológicas (Ver sección 6.8 Sincronización de reloj).
3.3.1.5 Abstenerse de emitir estampas cronológicas en caso de que se vea comprometida la seguridad del servicio (compromiso de la llave de la TSA, compromiso de referencia temporal, etc.).

3.3.2 Excepciones de responsabilidad de la TSA BANREP

La TSA BANREP no será responsable por estampados cronológicos erróneos como consecuencia de la desincronización o no disponibilidad de los relojes externos, encargados de emitir la hora legal colombiana (Ver sección 6.8 Sincronización de reloj).

3.3.3 Información que contiene un estampado cronológico

La información contenida en un "estampado cronológico" proporciona dos datos:

3.3.3.1 Tiempo del día: Expresado en hora, minuto y segundo (hh : mm : ss) de acuerdo con el Sistema Internacional de Medidas (SI) adoptado en la República de Colombia para la medición del tiempo. Se entenderá para los efectos de interpretación de este dato que la hora puede tener un valor numérico que diariamente asciende desde cero (00) hasta veinticuatro (24), el minuto puede tener un valor numérico que cada hora asciende desde cero (00) hasta cincuenta y nueve (59), y que el segundo puede tener un valor numérico que cada minuto asciende desde cero (00) hasta cincuenta y nueve (59).
3.3.3.2 Fecha: Expresada en día, mes y año (dd : mm : aaaa) de acuerdo con el calendario Juliano que es el generalmente aceptado en la República de Colombia. Se entenderá para los efectos de interpretación de este dato que el día tendrá un valor numérico que puede ascender mensualmente de uno (01) a treinta y uno (31), de conformidad con el calendario generalmente aceptado en la República de Colombia; el mes puede tener un valor numérico que puede ascender anualmente desde uno (01) a doce (12); el año puede tener un valor que asciende partiendo del número dos mil seis (2.006) hasta el número tres mil (3.000).

El DN para el certificado de estampado cronológico está formado de la siguiente manera:

- **Componente** de Dominio:
  dc=co
  dc=gov
  dc=banrep

- **Unidad** Organizacional:
  ou=CA Banrep
  ou=CA Banrep Subordinada
  cn=Timestamp Server

3.4 Servicio de generación de firmas digitales

La generación de firmas digitales es un servicio complementario a los de emisión de certificados y estampado cronológico en los que la CA BANREP suministra el mecanismo técnico para generar firmas digitales a las entidades que tengan relación directa con los servicios que el Banco dispone.

El proceso de solicitud se debe realizar según lo descrito en el numeral 4.5 (Solicitud del Servicio de generación de firmas digitales).

Los estándares técnicos del servicio de generación de firmas digitales están establecidos en el numeral 6.9 Estándares técnicos del servicio de generación de firmas Digitales.

4 REQUERIMIENTOS OPERACIONALES

4.1 Formalización de los Delegados con Responsabilidad Administrativa ante la CA BANREP

Para formalizar y generar los certificados de los Delegados con Responsabilidad Administrativa deberán presentarse en físico los siguientes documentos:

4.1.1 Formato de "Delegación para el manejo de firmas digitales y certificados"[5], que deberá ser diligenciado en su totalidad para la generación del Certificado. La firma del Representante Legal de la Entidad Usuaria solicitante debe tener constancia de reconocimiento de firma y contenido ante notario público.

4.1.2 Certificado de existencia y representación legal de la Entidad Usuaria, con fecha de expedición menor a treinta (30) días calendario.

[5] Disponible en http://www.banrep.gov.co/sites/default/files/paginas/BR-3-600-0.docx

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

4.2 Solicitud de certificados Pertenencia a Empresa y Persona Jurídica Entidad Empresa

Es el proceso mediante el cual el Delegado con Responsabilidad Administrativa y/o el Suscriptor son inicialmente identificados en la CA BANREP.

4.2.1 Solicitud de certificados Pertenencia a Empresa para un Delegado con Responsabilidad Administrativa

El proceso de registro para las claves y Certificados del Delegado con Responsabilidad Administrativa será el siguiente:

4.2.1.1 El representante legal de la Entidad Usuaria diligenciará el formato "Delegación para el manejo de firmas digitales y Certificados".

4.2.1.2 Los documentos diligenciados deberán ser radicados en la Ventanilla de Correspondencia – Oficina Principal del Banco[6].

4.2.1.3 La ER autenticará la identidad del solicitante, de conformidad con lo establecido en el numeral 3.1.5.

4.2.1.4 Una vez autenticada la identidad del solicitante, la ER suministrará el Código de Autorización. Dicha entrega se formalizará mediante el "Acta de aceptación de los términos de uso de la CA BANREP" (BR-3-599-0).

4.2.2 Solicitud de Certificados Pertenencia a Empresa para Suscriptores (PE)

El proceso de registro para las claves y Certificados de Pertenencia a Empresa es el siguiente:

4.2.2.1 El Delegado con Responsabilidad Administrativa de la Entidad Usuaria registrará en el Sistema SEBRA, opción "Portal de Gestión de Identidades", las Novedades de Suscriptor, en donde especificará el tipo de certificado solicitado.

4.2.2.2 La ER verificará la información recibida a través de la plataforma tecnológica y procederá a efectuar el proceso solicitado.

4.2.3 Distribución de Certificados Pertenencia a Empresa para Suscriptores (PE)

Los Certificados son generados por la CA BANREP siguiendo el procedimiento descrito a continuación:

4.2.3.1 La ER registrará la información creando así el respectivo certificado en la CA BANREP. Este certificado queda en un estado "adicionado" mientras se finaliza el procedimiento. En este momento se generará la información de activación, la cual consta de un Código de Autorización y un Número de Referencia que son requeridos para la activación del Certificado.

---

[6] http://www.banrep.gov.co/sucursales/Bogotá

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

4.2.3.2 El Código de Autorización será enviado, mediante el "Acta de Aceptación de los términos de uso de la CA BANREP" (BR-3-599-0), vía correo electrónico, por la ER directamente al buzón electrónico corporativo del Suscriptor especificado en el formato de solicitud junto con la información relativa al trámite subsiguiente.

4.2.3.3 El Suscriptor imprimirá y firmará el "Acta de Aceptación de los términos de uso de la CA BANREP" (BR-3-599-0) y la entregará al Delegado con Responsabilidad Administrativa.

4.2.3.4 El Delegado con Responsabilidad Administrativa validará la identidad del Suscriptor solicitante comparando lo solicitado en el formato Novedades de Suscriptor Entidad de Certificación - CA BANREP (BR-3-598-0) con el acta firmada por el suscriptor mencionada en el numeral 4.2.3.3. En el evento de existir diferencia en la información del solicitante (nombres, apellidos, número de cédula, etc.), deberá repetirse la solicitud.

4.2.3.5 Validada la identidad, el Delegado con Responsabilidad Administrativa deberá hacer llegar una copia del acta digitalizada firmada digitalmente mencionada en el numeral 4.2.3.3 a la dirección de correo electrónico de la ER: ***ca-novedades@banrep.gov.co***. Si en las 24 horas anteriores a la fecha de expiración[7] del Código de Autorización, el Banco de la República no recibe el acta mencionada en el numeral 4.2.3.3 se deberá volver a realizar la solicitud.

4.2.3.6 Una vez la ER reciba el "Acta de Aceptación de los términos de uso de la CA BANREP" (BR-3-599-0) firmada digitalmente por el Delegado con Responsabilidad Administrativa, enviará el Número de Referencia al correo electrónico corporativo del Suscriptor.

4.2.3.7 Con el Código de Autorización y el Número de Referencia conocidos por el Suscriptor, este podrá proceder con la activación del certificado. Para que dicho procedimiento tenga éxito, el suscriptor debe poseer un Token Criptográfico según las especificaciones mencionadas en el manual "**DSI-GI-97 Manual para la gestión de certificados emitidos por la Entidad de Certificación Digital Cerrada - CA BANREP**" ubicado en http://www.banrep.gov.co/es/contenidos/pki. Será responsabilidad de la Entidad Usuaria y/o del Suscriptor la adquisición del Token criptográfico y de la licencia de software necesaria para su uso. Se debe garantizar que en el computador de la Entidad Usuaria esté correctamente instalado este software[8] y contar con una sesión habilitada en el portal de Servicios Electrónicos del Banco de la República- SEBRA. Si no se cuenta con esta conexión, la Entidad Usuaria deberá crear los Certificados en una estación del Centro de Soporte Informático del Banco, en un horario previamente acordado con la ER.

4.2.3.8 El Código de Autorización y el Número de Referencia podrán ser utilizados solamente una vez y dentro de los nueve (9) días contados a partir de su generación; en caso de no ser utilizados en este lapso, se debe realizar una nueva solicitud y repetir el procedimiento de distribución de Certificados.

[7] El acta indicará la fecha y hora de expiración del Código de Autorización.

[8] Software licenciado ESP (Entrust Security Provider) y SAC (Safenet Authentication Client).

4.2.4 Solicitud de Certificados Persona Jurídica Entidad Empresa (PJEE)

El proceso de registro para las claves y Certificados Persona Jurídica Entidad Empresa es el siguiente:

4.2.4.1 El Delegado con Responsabilidad Administrativa de la Entidad Usuaria registrará en el Sistema SEBRA, opción "Portal de Gestión de Identidades", las solicitudes de certificados de Suscriptor, en donde especificará el tipo de certificado solicitado, según lo descrito en la sección 3.2.1.

4.2.4.2 La ER verificará la información recibida a través de la plataforma tecnológica y procederá a crear el Certificado y a generar la información de activación del Certificado (Número de Referencia y Código de Autorización).

4.2.5 Distribución de Certificados Persona Jurídica Entidad Empresa (PJEE)

Los Certificados son generados por la CA BANREP siguiendo el procedimiento descrito a continuación:

4.2.5.1 La ER registrará la información creando el respectivo certificado en la CA BANREP. Este certificado queda en un estado "adicionado" mientras se finaliza el procedimiento. En ese momento se generará la información de activación, la cual consta de un Código de Autorización y un Número de Referencia que son requeridos para la activación del Certificado.

4.2.5.2 El Código de Autorización será enviado, mediante el "Acta de Aceptación de los términos de uso de la CA BANREP" (BR-3-599-0), vía correo electrónico, por la ER directamente al buzón electrónico corporativo del Delegado con Responsabilidad Administrativa junto con la información relativa al trámite subsiguiente.

4.2.5.3 El Delegado con Responsabilidad Administrativa imprimirá y firmará el "Acta de Aceptación de los términos de uso de la CA BANREP" (BR-3-599-0) y deberá hacer llegar una copia del acta digitalizada con firma digital a la dirección de correo electrónico de la ER: ***ca-novedades@banrep.gov.co***. Si en las 24 horas anteriores a la fecha de expiración[9] del Código de Autorización, el Banco de la República no recibe el acta mencionada en el numeral 4.2.3.3 se deberá volver a realizar la solicitud.

4.2.5.4 Una vez la ER reciba el "Acta de Aceptación de los términos de uso de la CA BANREP" (BR-3-599-0) firmada digitalmente por el Delegado con Responsabilidad Administrativa, remitirá el Número de Referencia al correo electrónico corporativo del Suscriptor.

4.2.5.5 Con el Código de Autorización y el Número de Referencia conocidos por el Suscriptor, este podrá proceder con la activación del certificado. Para que dicho procedimiento tenga éxito, en el computador de la Entidad Usuaria deberá estar correctamente instalado el software correspondiente[10] y tener una sesión habilitada

[9] El acta indicará la fecha y hora de expiración del Código de Autorización.

[10] Software licenciado ESP (Entrust Security Provider) y SAC (Safenet Authentication Client).

en el portal de Servicios Electrónicos del Banco de la República- SEBRA. Si no se cuenta con esta conexión, la Entidad Usuaria deberá crear los Certificados en una estación del Centro de Soporte Informático del Banco, en un horario previamente acordado con el Funcionario de la ER.

4.2.5.6 El Código de Autorización y el Número de Referencia podrán ser utilizados solamente una vez y dentro de los nueve (9) primeros días contados a partir de su generación; en caso de no ser utilizados en este lapso, se debe realizar una nueva solicitud y repetir el procedimiento de distribución de Certificados.

4.3 Solicitud del Servicio de estampado cronológico

El servicio de estampado cronológico será acordado entre el Banco de la República y las Entidades Usuarias para cada sistema informático de acuerdo con las normas aplicables y los requerimientos de seguridad establecidos para tal sistema.

4.4 Uso del servicio de estampado cronológico

Toda aplicación para la cual se determine el uso de estampado cronológico deberá contar con la interacción y uso de software aprobado por el Departamento de Seguridad Informática del Banco de la República que garantice el correcto consumo del servicio basados en el estándar RFC 3161.

La descarga del software y librerías para el consumo de servicios de estampado cronológico está disponible en https://caribe.banrep.gov.co/emisor. Este repositorio es de acceso exclusivo para usuarios que tengan un contrato SEBRA vigente con el Banco de la República.

4.5 Solicitud de generación de firmas digitales

El servicio de generación de firmas es de uso exclusivo para certificados emitidos por la CA BANREP; por lo tanto, quien realice el proceso de solicitud de certificados digitales según lo establecido en el numeral 4.2 podrá hacer uso del mismo.

La descarga del software y librerías para el consumo de servicios de estampado cronológico está disponible en https://caribe.banrep.gov.co/emisor. Este repositorio es de acceso exclusivo para usuarios que tengan un contrato SEBRA con el Banco de la República.

4.6 Aceptación de los Certificados

La inicialización por parte del Suscriptor constituye su aceptación de las claves y certificados emitidos por la CA BANREP y la aceptación de los términos y condiciones de su uso especificado en esta DPC.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

4.7 Revocación

4.7.1 Circunstancias para la revocación

Cualquier inquietud con respecto a la solicitud de revocación puede comunicarse vía telefónica al Centro de Soporte informático del Banco de la República al número 3431000 (6:00 am. - 9:00 p.m. de lunes a viernes, excepto días festivos), o a través de la dirección de correo electrónico ca-novedades@banrep.gov.co.

La CA BANREP puede revocar un certificado expedido por cualquiera de las siguientes razones:

4.7.1.1 Porque se tenga conocimiento o existan indicios que permitan concluir que la Clave Privada o contraseña haya sido divulgada o conocida por terceros así sean de la misma Entidad Usuaria.

4.7.1.2 Por la terminación del contrato y/o finalización de la relación con el Banco de la República.

4.7.1.3 Por solicitud del Delegado con Responsabilidad Administrativa mediante comunicación en la cual se informe:

a. La desvinculación o suspensión del Suscriptor de la Entidad Usuaria.
b. La imposibilidad del Suscriptor para cumplir con sus obligaciones.
c. Cambios presentados en la información contenida en el Certificado. Los cambios en la información de los Certificados deben ser reportados de manera oportuna diligenciando el formato de Novedades de Suscriptor Entidad de Certificación - CA BANREP (BR-3-598-0)[11]
d. Cualquier situación que implique riesgo de divulgación de la Clave 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.

4.7.2 Quiénes pueden solicitar la revocación

La CA BANREP acepta solicitudes de revocación provenientes de:

4.7.2.1 El Delegado con Responsabilidad Administrativa.
4.7.2.2 La ER.
4.7.2.3 La CA BANREP, a través de los Oficiales de Seguridad.

4.7.3 Procedimiento para revocación

[11] Disponible en http://www.banrep.gov.co/sites/default/files/paginas/BR-3-598-02.xls

4.7.3.1 El Delegado con Responsabilidad Administrativa registrará en el Sistema SEBRA, opción "Portal de Gestión de Identidades", las solicitudes de revocación de certificados.
4.7.3.2 La ER procesará las solicitudes.
4.7.3.3 La ER, por medio de un correo electrónico, enviará una confirmación de la revocación al Delegado con Responsabilidad Administrativa.

4.7.4 Acuerdo de servicio para la revocación de Certificados

La CA BANREP procesará toda solicitud de revocación por razones de riesgo de divulgación de las claves e incumplimiento de obligaciones, según considere la Entidad Usuaria. Todas las solicitudes serán procesadas dentro del horario establecido, una vez recibida la solicitud. Si la solicitud se considera urgente deberá informarse de ello mediante llamada al Centro de Soporte Tecnológico, teléfono 3431000.

4.7.5 Frecuencia de distribución de la lista de certificados revocados (CRL)

La CA BANREP actualizará la CRL cada siete días (7) o inmediatamente después de la revocación de un certificado. El proceso de publicación de la CRL podrá tomar hasta treinta (30) minutos.

4.7.6 Requerimiento de verificación de CRL

Para sistemas de información y/o aplicaciones que requieran el uso de claves y certificados de la CA BANREP se deberán verificar correctamente todos los certificados en la CRL antes de validar y/o usar la Clave Pública del Certificado.

4.8 Procedimiento de sistemas de seguridad y auditoría

4.8.1 Tipos de eventos registrados

Los siguientes tipos de eventos serán registrados automática o manualmente por parte de la CA BANREP y la TSA BANREP para propósitos de auditoría:

a. Administración de los Suscriptores y administradores de las ER.
b. Administración de los oficiales de seguridad.
c. Administración de claves y certificados.
d. Encendido y apagado de la CA.
e. Acceso de la CA al directorio.
f. Administración de la base de datos de la CA.
g. Intentos de entradas y salidas al sistema.
h. Intentos no autorizados de acceso a la red y sistemas de la PKI.
i. Administración de los registros de auditoría.
j. Cambios en la configuración del sistema.

k. Actualización de software y hardware.
l. Mantenimiento "programado" y "no programado" sobre el sistema y ubicación física.
m. Generación de estampas cronológicas.

4.8.2 Frecuencia del procesamiento de registros de auditoría

La CA BANREP, a través de los oficiales de seguridad, procesa las entradas de auditoría una vez cada tres (3) meses. El proceso de auditoría es el siguiente:

a. Acumulación de registros del sistema creados desde el último proceso.
b. Revisión de registros de auditoría al sistema.
c. Análisis y reportes de eventos significativos, alertas e irregularidades y resolución de las causas de los eventos.

4.8.3 Período de conservación de registros de auditoría

Los registros de auditoría son guardados por un (1) año.

4.8.4 Período de conservación de registros de estampado cronológico

Los eventos de generación de estampas cronológicas son almacenados en el colector de eventos del Banco por un período de dos (2) años.

4.8.5 Protección de los registros de auditoría

El acceso al sistema que contiene los registros de auditoría está restringido mediante una combinación de controles físicos y controles de seguridad del sistema. El sistema de cómputo, cintas de las copias de respaldo de los registros lógicos y físicos de auditoría son guardados en una zona de alta seguridad del Banco de la República.

4.8.6 Copia de respaldo de los registros de auditoría

Una copia de los registros físicos de auditoría será enviada a un lugar alterno con facilidad de almacenamiento, una (1) vez por mes. Los archivos de registro de auditoría son recogidos como parte del sistema de respaldo del servidor de la CA BANREP. Los medios físicos de almacenamiento de la copia de respaldo son conservados en el Centro de Cómputo principal una (1) vez por semana. Estos contienen copia semanal consolidada de los archivos de registro de auditoría.

4.8.7 Sistema de recolección de auditorías

El sistema de recolección de auditoría de la CA BANREP es una combinación de procesos manuales y automáticos realizados por el sistema operacional, la aplicación y el personal de la CA BANREP.

4.8.8 Análisis de vulnerabilidades

El Departamento de Seguridad Informática del Banco de la República conducirá los análisis de vulnerabilidades sobre la arquitectura de la CA BANREP de acuerdo con los procedimientos internos establecidos para esta actividad.

4.8.9 Procedimientos de gestión de incidentes y vulnerabilidades

La CA BANREP tiene establecido y probado el plan de continuidad tecnológica que define las acciones, recursos y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos y los servicios de certificación prestados por la AC Raíz o la AC Subordinada. El plan de continuidad tecnológica contempla los siguientes aspectos:

a. La redundancia de todos los componentes de la CA BANREP.
b. El chequeo completo y pruebas del plan de continuidad tecnológica bajo diferentes escenarios de riesgo.

En el caso de que se viera afectada la seguridad de la prestación de los servicios de verificación de firma de alguna de sus autoridades de certificación, la CA BANREP informará a todos los terceros conocidos sobre la indisponibilidad de los certificados y listas de revocación firmados. Tan pronto como sea posible se procederá al restablecimiento del servicio, de acuerdo con la magnitud y el impacto del incidente que active el plan de continuidad tecnológica.

El plan de continuidad tecnológica permite que la CA BANREP pueda continuar prestando sus servicios de emisión de certificados, servicio de firma digital y estampado cronológico, en presencia de desastres, después de identificar, evaluar, gestionar y minimizar cualquier tipo de riesgo.

Los procedimientos para la gestión de incidentes contemplan el registro y documentación de todas las incidencias, realizándose un seguimiento de estas. Se registra información relativa a: fecha, hora, tipo de incidencia, persona que comunica la misma, persona a quien se asigna la resolución de la incidencia, y documentación sobre la causa y sus efectos.

4.8.10 Daños en los recursos de computación, software o datos

La CA BANREP ha implementado un plan de contingencia tecnológica que se dirige a la recuperación de sus operaciones, frente a daños en los recursos computacionales, software y datos, el cual actualiza periódicamente de acuerdo a los resultados de las pruebas del mismo, con el fin de asegurar su vigencia en todo momento.

4.8.11 Seguridad en las instalaciones después de un desastre

El Banco de la República tiene establecido una contingencia y el plan de recuperación de desastres de la CA BANREP.

4.9 Conservación de registros

Los siguientes registros serán conservados por la CA BANREP:

a. Información de auditoría.
b. Solicitudes de los Suscriptores.
c. Certificados de CRL.
d. La Clave Privada de descifrado de los Suscriptores.
e. Reportes de discrepancia, compromiso de claves privadas y correspondencia asociada.
f. Los registros de auditoría, como mínimo (1) año.
g. Certificados y Claves Privadas, por veinte (20) años.
h. Una copia de todos los registros archivados, documentación recibida y las copias de respaldo, de acuerdo con los lineamientos establecidos por el Banco de la República
i. El acceso a los archivos de información de la CA BANREP se concede en concordancia con la política de confidencialidad especificada en la sección 2.5.

4.10 Disponibilidad de la CA BANREP

Los requisitos de notificación y los procedimientos de recuperación en caso de compromiso de la clave privada de la CA o desastre son los siguientes:

4.10.1 Continuidad tecnológica y operativa

La CA BANREP tiene implementado y probado un plan de contingencia tecnológica y operativa que permite la continuidad del servicio, los cuales involucran distintos escenarios de prueba para garantizar la eficiencia del plan.

4.10.2 Acuerdos de niveles de servicio

El horario para la recepción de solicitudes es de 7:00 a.m. a 9:00 p.m., lunes a viernes, excepto festivos. La atención y respuesta de toda solicitud referenciada en este documento se realizará dentro de los tres (3) días hábiles contados a partir de la hora y fecha de recibo de la misma, con base en el correspondiente orden de llegada. En caso de presentarse una urgencia manifiesta que comprometa la operación de alguno de los servicios del Banco de la República o de las entidades autorizadas, se atenderá con prioridad toda solicitud asociada a este evento, con el fin de minimizar riesgos sistémicos. En tal caso, el evento deberá ser registrado en el software de Mesa de Ayuda por parte del Centro de Soporte Tecnológico.

La CA BANREP, TSA BANREP y el servicio de generación de firmas digitales estarán disponibles mensualmente 99% del tiempo de lunes a viernes desde las 06:00 am hasta las 03:00 am del día siguiente excepto los días festivos.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

4.11 Cesación de actividades de la CA BANREP

En el caso de que la CA BANREP decida cesar sus actividades acreditadas ante la ONAC, informará de dicha cesación de servicios a la ONAC y a la Superintendencia de Industria y Comercio, con una antelación de 30 días, según lo establecido en el artículo 2.2.2.48.3.8. del Decreto 1074 de 2015. La CA BANREP informará a los Usuarios, Suscriptores y Entidades Usuarias acerca de la terminación de sus servicios, por lo menos con treinta (30) días de antelación, una vez autorizada para el efecto por la Organismo Nacional de Acreditación (ONAC).

La CA BANREP informará a todos los suscriptores mediante los esquemas de comunicación establecidos con las entidades usuarias, en el sitio web del Banco de la Republica, sobre lo siguiente:

a. La terminación de su actividad o actividades y la fecha precisa de cesación.
b. Las consecuencias jurídicas de la cesación respecto de los certificados expedidos.
c. La autorización emitida por la Superintendencia de Industria y Comercio para que la CA BANREP pueda cesar el servicio, y si es el caso, mantener la publicación de la CRL, hasta cuando expire el último de ellos.
d. La fecha exacta de revocación de los certificados de los suscriptores, CA subordinada y CA Raíz.

La terminación de la actividad o actividades se hará en la forma y siguiendo el cronograma presentado por el Banco de la Republica al ente de vigilancia y control y que este apruebe.

En cualquier caso, LA CA BANREP dispone de:

a. Un plan de continuidad del servicio.
b. Un plan que garantiza la continuidad en alta disponibilidad de la publicación en los repositorios (CRL) propios.
c. La adecuada destrucción de la llave privada de la entidad en caso de ser necesario mediante la inicialización de los HSM.

4.12 Cesación de Actividades de la TSA BANREP

En el caso de que la TSA BANREP decida cesar sus actividades acreditadas ante la ONAC, informará a de la cesación de los servicios a la ONAC y a la Superintendencia de Industria y Comercio, con una antelación de 30 días, según lo establecido en el artículo 2.2.2.48.3.8. del Decreto 1074 de 2015. La TSA BANREP informará a los Usuarios, y Entidades Usuarias acerca de la terminación de sus servicios, por lo menos con treinta (30) días de antelación, una vez autorizada para el efecto por la Organismo Nacional de Acreditación (ONAC).

La cesación de Actividades de la TSA BANREP estará también condicionada al cese de actividades de la CA BANREP.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

4.13 Otros requisitos operacionales

4.13.1 Recuperación de datos

La CA BANREP sigue la práctica descrita en este numeral para recuperar el certificado de cifrado de un Suscriptor con el fin de tener acceso a los datos encriptados con una de las Claves Públicas del mismo. Esta práctica se desarrolla 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 proceso tiene los siguientes puntos:

4.13.1.1 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.
4.13.1.2 La ER verificará la Firma Digital de la solicitud presentada.
4.13.1.3 La ER recuperará el Certificado del Suscriptor, generando así la información de activación respectiva (el Número de Referencia y el Código de Autorización).
4.13.1.4 El Número de Referencia y el Código de Autorización serán enviados vía correo electrónico firmado digitalmente por la ER directamente al Delegado con Responsabilidad Administrativa.
4.13.1.5 El Delegado con Responsabilidad Administrativa utilizará el Número de Referencia y el Código de Autorización recibido del Funcionario de la ER por correo electrónico para recuperar la identificación PKI del Suscriptor requerido.

Para que este procedimiento tenga éxito, el software necesario para el buen funcionamiento de los certificados digitales 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.

4.14Tipo de Certificado

Para los dos (2) tipos de certificados definidos en el presente documento que pueden ser emitidos por la CA BANREP para Entidades Usuarias se tiene establecido lo siguiente:

a. Para un certificado Pertenecía a Empresa (PE), un dispositivo Hardware PKCS#11 (Token Criptográfico) [12].

[12] Disponible en http://www.banrep.gov.co/es/contenidos/pki.

b. Para Certificados Persona Jurídica Entidad Empresa, un archivo EPF (Entrust Profile) que podrá ser transformado en formatos PKCS#12 o JKS.

4.15 Terminación de una Suscripción

Cuando la Entidad Usuaria desea terminar la vinculación de un Suscriptor en la CA BANREP deberá seguir el siguiente procedimiento:

4.15.1 El Delegado con Responsabilidad Administrativa registrará en el Sistema SEBRA, opción "Portal de Gestión de Identidades", las solicitudes de revocación de certificados de Suscriptores.

4.15.2 La ER almacenará los registros procesados en la plataforma tecnológica por el término de un (1) año, para efectos de auditoría.

4.15.3 La ER entrará al sistema de la CA BANREP y deshabilitará al Suscriptor, removerá los Certificados del Suscriptor del directorio, prevendrá ingresos posteriores del Suscriptor y revocará los Certificados con un código de razón de terminación.

4.15.4 Cuando el Suscriptor ya no requiera un Certificado de la CA BANREP deberá solicitar al Delegado con Responsabilidad Administrativa la revocación del Certificado Digital ante la CA BANREP.

5. CONTROLES DE SEGURIDAD FÍSICOS, DE PROCEDIMIENTOS Y DE PERSONAL

5.1 Controles físicos

Las operaciones de la CA BANREP y la ER son realizadas dentro de sus instalaciones, las cuales cuentan con niveles de protección.

Por otra parte, y con el fin de garantizar la continuidad de las operaciones, el Banco de la República mantiene un sitio para la recuperación ante desastres. Los centros de cómputo del Banco de la República cuentan con:

5.1.1 Acceso físico: El Banco de la República cuenta con control de acceso físico al edificio, a los pisos críticos y al centro de cómputo. El control de acceso en el primer caso es el carné de empleado, y en los demás casos es una cerradura electrónica con clave.

5.1.2 Energía y aire acondicionado: El Banco de la República cuenta con fuentes de energía primaria y secundaria, así como sistemas de ventilación, aire acondicionado, calefacción, prevención y detección de fuegos. Así mismo, ha tomado medidas preventivas razonables para minimizar el impacto que podría causar el agua en el Centro de Cómputo.

5.1.3 Almacenamiento de los medios: Todos los medios que contienen información del Banco de la República se encuentran almacenados en un sitio seguro y se conservan copias de los más críticos en un sitio remoto del Banco. Tales sitios, cuentan con procedimientos de control de acceso requeridos para minimizar el riesgo de daño.

5.1.4 Destrucción de medios y/o documentos: Todos los medios utilizados para el almacenamiento o aquellos documentos que contengan información, como claves, o cualquier otro material sensible de la CA BANREP deberán ser dispuestos según lo establece el Departamento de Gestión Documental del Banco.

5.2. Controles de procedimiento

5.2.1 Roles de confianza: Los roles de confianza son los empleados y contrapartes que realizan operaciones con el Banco de la República y que, por lo tanto, pueden hacer uso de los certificados para proteger sus operaciones. El Banco de la República mantiene políticas rigurosas de segregación funcional, y para realizar operaciones sensibles, cuenta con esquemas de doble intervención en donde se necesita más de un rol de confianza. La división de responsabilidades entre roles se detalla a continuación:

5.2.1.1 Usuario maestro CA BANREP

a. Configuración y mantenimiento del hardware y software de la CA BANREP.
b. Iniciación y terminación de los servicios de la CA BANREP.

5.2.1.2 Oficial CA BANREP

a. Configuración de las políticas de seguridad de la CA BANREP.
b. Administración de los administradores PKI y otros oficiales.

5.2.1.3 Funcionario de la ER

a. Administración de los procesos de suscripción.
b. Creación, renovación y revocación de Certificados.

5.2.1.4 Revisor cumplimento en CA BANREP

a. Facultad para revisar el cumplimiento de las políticas de certificados y de la DPC.
b. Facultad para revisar los logs de auditoría.

5.2.2 Roles de confianza para la ER: La CA BANREP debe asegurar que el personal asignado a la ER entiende su responsabilidad en la identificación y autenticación de potenciales Suscriptores y realiza las siguientes funciones:

a. Gestionar novedades de Suscriptores.
b. Validar la identidad y autorización del Delegado con Responsabilidad Administrativa.
c. Registrar la información del Suscriptor en la CA BANREP.
d. Proveer la información de activación para el intercambio de claves en línea y la creación de Certificados.

5.3 Controles de Personal

Todas las personas que realicen tareas relacionadas con la operación de la CA BANREP deben regirse por las políticas y lineamientos establecidos por el Sistema de Gestión de la Información.

6. CONTROLES TÉCNICOS DE SEGURIDAD DE LA INFORMACIÓN

Esta sección describe los controles técnicos de seguridad implementados por la CA BANREP y requeridos por los clientes.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

6.1.1.1 El par de claves de firma de la CA BANREP es generado durante la instalación inicial de la aplicación CA.
6.1.1.2 El par de claves de cifrado de los Suscriptores es generado por la aplicación CA.
6.1.1.3 El par de claves de firma es generado por la aplicación Cliente PKI.
6.1.1.4 Los algoritmos de generación de claves son los permitidos por la legislación colombiana vigente y normativa que regule las entidades de certificación.
6.1.1.5 La clave de verificación de la TSA BANREP es generada directamente por la CA BANREP y hace parte de la instalación y mantenimiento de los servidores de estampado cronológico.

6.1.2 Entrega de la Clave Privada a los Suscriptores

Las Claves Privadas de descifrado son generadas por la aplicación CA BANREP y entregadas a las aplicaciones PKI de los Suscriptores usando un protocolo compatible con PKIX parte 3.

6.1.3 Entrega de la Clave Pública al generador del Certificado

El par de claves de firma deben ser generadas por las aplicaciones Cliente PKI, lo que significa que la Clave Pública de verificación de firma debe ser transmitida de forma segura a la aplicación CA, para generar el certificado de verificación de firma. La entrega de las Claves Públicas a la aplicación CA será en línea, usando un protocolo compatible con PKIX parte 3 CMP, o por cualquier otra vía aprobada por la CA BANREP.

6.1.4 Entrega de la Clave Pública de la CA BANREP a los Suscriptores

La Clave Pública de verificación de firma de la CA BANREP será entregada en línea, en un certificado de la CA BANREP a los Suscriptores, usando un protocolo compatible con PKIX Parte 3, o por cualquier vía aprobada por la CA BANREP.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

6.1.5 Tamaño de las claves asimétricas

La CA BANREP genera claves asimétricas RSA (Rivest-Shamir-Adleman) con un tamaño de 4096 bits para el par de claves de firma de la CA y 2048 bits para los pares de claves de firma y cifrado de los Suscriptores.

6.1.6 Parámetros de generación de la clave pública

La CA BANREP no generará claves DSA (Digital Signature Algorithm). Las aplicaciones Cliente deberían generarlas según los parámetros establecidos en FIPS 186.

6.1.7 Generación de claves Hardware / Software

Las claves de la CA BANREP y la TSA BANREP son generadas usando un módulo criptográfico hardware que cumple con lo establecido en FIPS 140-2 Nivel 3.

Todas las claves de los Certificados Pertenencia a Empresa, correspondientes a los Funcionarios de la ER y de los Suscriptores son generadas usando hardware o software diseñado para cumplir con lo establecido en FIPS-140-2 Nivel 3.

6.1.8 Distribución llave pública TSA

La clave Pública de la TSA estará disponible a través de la infraestructura de llave pública provista por el Banco. Su acceso y uso se realizará a través de los mecanismos y software proporcionado y aprobado por el Banco de la República.

6.1.9 Propósito de uso de la clave

La clave de firma de la CA BANREP, únicamente puede firmar certificados y CRLs (Cetificate Revocation List).

La aplicación CA usada por la CA BANREP genera los certificados públicos de verificación de firma con el parámetro digital Signature establecido.

El Certificado de firma de la CA BANREP contiene los parámetros keyCertSign y CRLSign establecidos.

Los Certificados de cifrado contienen el parámetro keyEncipherment establecido.

En el caso de los Certificados de firma, las claves pueden ser utilizadas para la autenticación, no repudiación e integridad. En las diferentes entidades también pueden ser usadas para establecer una clave de sesión, excepto las claves de firma de la CA BANREP, que sólo pueden ser usadas para firmar certificados y CRLs.

El campo del Certificado KeyUsage debe ser usado según PKIX parte 1 "Certificate and CRL Profile". Uno de los siguientes valores de KeyUsage debe estar presente en los certificados:

La clave de firma de la TSA BANREP, únicamente puede firmar las solicitudes de estampa cronológico:

- **-digitalSignature**
- **-nonRepudiation**

Uno de los siguientes valores debe estar presente en el certificado de la CA:

- **-KeyCertSign**
- **-cRLSign**

En el caso de los Certificados de cifrado, las claves pueden ser usadas para el intercambio y establecimientos de claves de sesión y confidencialidad de datos.

El campo del Certificado KeyUsage debe ser usado según PKIX parte 1 "Certificate and CRL Profile". Uno de los siguientes valores de KeyUsage debe estar presente en los Certificados:

- **-KeyEncipherment**
- **-dataEncipherment**

6.2 Protección de la Clave Privada

6.2.1 Estándares y módulos criptográficos

Las operaciones de generación de la clave de Firma Digital de la CA BANREP, almacenamiento de la clave de Firma Digital de la CA y firma de Certificados deben ser realizadas en un módulo criptográfico en hardware, por lo menos certificado FIPS 140-2 nivel 3.

Las operaciones de generación de la clave de Firma Digital de la TSA BANREP, almacenamiento de la clave de estampado cronológico deben ser realizadas en un módulo criptográfico en hardware, por lo menos certificado FIPS 140-2 nivel 3.

Los módulos criptográficos usados por las Entidades Usuarias para sus suscriptores deben ser diseñados para reunir los requerimientos mínimos de FIPS 140-2 Nivel 3.

6.2.2 Control multi-persona de la Clave Privada (m de n)

La CA BANREP tiene implementado control de doble intervención para la generación de claves de la CA y para la generación de la clave de descifrado del servicio de recuperación de claves, una

persona asociada con los roles de Usuario Maestro u oficial de seguridad y un funcionario del área de control deben participar activamente.

6.2.3 Copia de seguridad de la Clave Privada

La aplicación CA BANREP mantiene en sus bases de datos un histórico de las claves de descifrado de los Suscriptores, con el propósito de recuperación de documentos.

La aplicación CA realiza una copia de respaldo dos (2) veces al día, y a estas se les realiza una copia de respaldo diariamente según las políticas de respaldo de backup de las máquinas de la CA BANREP.

A las claves privadas de firma de los Suscriptores no se les realiza copia de seguridad por parte de la CA BANREP.

6.2.4 Generación de la Clave Privada

La Clave Privada de firma de la CA BANREP es generada con un módulo criptográfico en hardware.

Las Claves Privadas de cifrado de los Suscriptores son generadas con un módulo software de la aplicación CA, y son transferidas a los módulos criptográficos de los Suscriptores usando un protocolo compatible con PKIX parte 3.

Respecto de las Claves Privadas de Firma Digital se tiene definido lo siguiente:

a. Para los certificados de Pertenencia a Empresa, un dispositivo Hardware PKCS#11 (Token Criptográfico) [13].
b. Para los certificados de Persona Jurídica Entidad Empresa, un archivo EPF (Entrust Profile) que podrá ser transformado en formatos PKCS#12 o JKS.

6.2.5 Método de activación de la clave privada

La clave de Firma Digital de la CA BANREP es activada como parte de la iniciación de la aplicación CA, la cual requiere la contraseña de un oficial de seguridad de la PKI y se trabaja con esquemas de doble intervención.

Los Suscriptores deben usar aplicaciones cliente PKI que acceden sus claves privadas como parte del proceso de log-in, en el cual un Suscriptor es autenticado usando una contraseña o cualquier otro mecanismo de autenticación fuerte, como pueden ser los tokens criptográficos.

[13] Disponible en http://www.banrep.gov.co/es/contenidos/pki.

6.2.6 Método de desactivación de la Clave Privada

La Clave Privada de firma de la CA BANREP no se puede acceder durante el tiempo en que la aplicación este apagada.

6.2.7 Generación de la Clave Privada TSA

La Clave Privada de firma de la TSA BANREP es generada con un módulo criptográfico en hardware.

La Clave se recupera cada dos años con la intervención de los administradores de la CA BANREP.

La CA BANREP mantendrá la aplicación de estampado cronológico con un certificado vigente.

6.2.8 Compromiso de la llave privada de la CA Subordinada

En el caso que la llave privada de la CA BANREP Subordinada sea comprometida, se procederá a realizar la revocación de los certificados de todos los suscriptores, junto con el certificado de la CA Subordinada.

Se generará un nuevo certificado de la CA Subordinada, usando el certificado de la CA Raíz y emitiendo de nuevo los certificados de los Suscriptores, siguiendo los protocolos de ceremonia y generación de llaves correspondientes.

6.2.9 Compromiso de la llave privada de la TSA

En el caso que la llave privada de la TSA sea comprometida, se procederá con la revocación del certificado digital.

Se validarán las condiciones que llevaron al compromiso de la llave y una vez se pueda asegurar la mitigación de las causas identificadas, se procederá con la generación de una nueva llave.

6.2.10 Actualización CRL – revocación certificado TSA

Toda vez que se haga una revocación del certificado y llave pública de la TSA, será generada una CRL según lo dispuesto dentro del funcionamiento de la CA BANREP.

6.2.11 Compromiso de la llave privada de la CA Raíz

En el caso que la llave privada de la CA BANREP Raíz sea comprometida, se procederá a realizar la revocación de los certificados de todos los suscriptores, junto con los certificados de la CA Subordinada y CA Raíz.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

Se generará un nuevo certificado de la CA Raíz, emitiendo de nuevo el certificado de la CA Subordinada, los certificados de los Suscriptores, siguiendo los protocolos de ceremonia y generación de llaves correspondientes.

6.2.12 Método de destrucción de la clave privada de la CA

La CA Raíz y la CA Subordinada eliminarán su clave privada cuando expire su plazo de vigencia o haya sido revocada. La destrucción se realizará utilizando el procedimiento técnico establecido por la CA BANREP para garantizar la eliminación definitiva de la clave dentro del HSM. Lo mismo ocurrirá con sus copias de seguridad.

6.2.13 Método de borrado de la clave privada

Cuando un Suscriptor no requiera hacer más uso del certificado PKI, deberá inicializar el token criptográfico con la herramienta del fabricante.

6.3 Otros aspectos de la administración del par de claves

6.3.1 Archivo de las claves públicas

La CA BANREP archivará las claves públicas de verificación de firma de la CA y los pares de claves de cifrado de los Suscriptores.

6.3.2 Períodos de uso de los Certificados y Claves Privadas

Los períodos de uso de las Claves Públicas y Privadas generadas por CA BANREP serán así:

6.3.2.1 Certificado de verificación de firma de la CA Raíz: Veinte (20) años.
6.3.2.2 Clave Privada de firma de la CA Raíz: Veinte (20) años.
6.3.2.3 Certificado de verificación de firma de la Subordinada: Veinte (20) años.
6.3.2.4 Clave Privada de firma de la CA Subordinada: Veinte (20) años.
6.3.2.5 Certificado de firma Pertenencia a Empresa: Dos (2) años.
6.3.2.6 Certificado de firma Persona Jurídica Entidad Empresa: Dos (2) años.
6.3.2.7 Clave Privada de firma Pertenencia a Empresa: Dos (2) años.
6.3.2.8 Clave Privada de firma Persona Jurídica Entidad Empresa: Dos (2) años.
6.3.2.9 Clave Pública de cifrado y Certificado de los Suscriptores: Dos (2) años.
6.3.2.10 Clave Pública de verificación de firma para comunicaciones B2B y procesos de automatización: Dos (2) años.
6.3.2.11 Clave Privada de firma para comunicaciones B2B y procesos de automatización: Dos (2) años.
6.3.2.12 Clave Pública de cifrado y certificado para comunicaciones B2B y procesos de automatización: Dos (2) años.
6.3.2.13 Clave Privada de descifrado de los Suscriptores: Dos (2) años.

6.3.2.14 Clave Privada de descifrado para comunicaciones B2B y Procesos automáticos: Dos (2) años.

6.4 Información de activación

6.4.1 Información de activación: Generación e instalación

El Número de Referencia y el Código de Autorización son generados en software por la aplicación de la CA BANREP y permanecen en la base de datos de la CA encriptados hasta que el Suscriptor cree o recupere su Certificado. La información de activación es enviada a los Suscriptores según el procedimiento descrito en la sección cuatro (4) de este documento.

Los Suscriptores usan contraseña para activar sus módulos criptográficos o crear los archivos con llaves privadas correspondientes (Aplica para certificados Persona Jurídica Entidad Empresa). Cada Suscriptor selecciona su propia contraseña basado en una política de contraseñas establecida por la CA BANREP y acorde con las políticas de seguridad del Banco de la República.

6.4.2 Información de activación: Protección

La información de activación es generada de manera segura por la aplicación CA y es grabada en la base de datos cifrada de la CA BANREP.

Las aplicaciones cliente PKI usan una contraseña proporcionada por el Suscriptor para cifrar el perfil del Suscriptor. Así se mantiene la confidencialidad de las Claves Privadas.

6.5 Controles de seguridad de los servidores

6.5.1 Requerimientos de seguridad para servidores específicos

La CA BANREP posee controles técnicos de seguridad, los cuales son reforzados por el sistema operativo de la máquina de la CA y la misma aplicación CA, incluyendo:

a. Controles de acceso a los servicios de la CA BANREP y roles de la PKI.
b. Segregación de los deberes para los roles de la PKI.
c. Identificación y autenticación de los roles de la PKI e identidades asociadas.
d. Sesiones seguras entre la aplicación CA y las aplicaciones cliente PKI.
e. La base de datos de la CA permanece cifrada.
f. Archivo del histórico de claves de la CA, Suscriptores e información de auditoría.
g. Auditoría sobre los eventos relacionados a la seguridad.
h. Mecanismos de recuperación de claves y de la aplicación CA.
i. Control físico de acceso mediante una compuerta con claves y tarjetas de acceso y además supervisión por parte del Departamento de Protección y Seguridad del Banco de la República.

6.6 Ciclo de vida de los controles técnicos

6.6.1 Controles de desarrollo del sistema

La aplicación CA y TSA, como todo el software de la PKI, fue desarrollada con los más altos niveles de calidad y seguridad; además, ha recibido varias certificaciones reconocidas a escala mundial como FIPS 140-2 Nivel 3, entre otras.

Las aplicaciones cliente PKI que se desarrollan en el Banco de la República cumplen con una metodología de desarrollo y aseguramiento de calidad de proyectos informáticos establecida en el Banco de la República.

6.6.2 Controles de la administración de la seguridad

Existen políticas, normas, estándares y mecanismos establecidos para administración de los problemas, cambios y configuración en el ámbito organizacional. En particular para los componentes hardware y software de la PKI se deben cumplir todos los estándares y procedimientos establecidos.

6.7. Controles de seguridad de red

La red de la CA BANREP actualmente está segmentada para proveer niveles adicionales de seguridad. El control de acceso a los servicios ofrecidos por la CA BANREP es controlado por un componente de seguridad tipo firewall.

6.8. Sincronización de reloj

Los mecanismos de la CA BANREP se tienen sincronizados con la hora legal colombiana que provee el Instituto Nacional de Meteorología de Colombia, de acuerdo a la documentación técnica entregada en el sitio oficial de la entidad.

6.9 Estándares técnicos del servicio de generación de firmas Digitales

Los estándares técnicos que usa el servicio de generación de firmas digitales incluyendo estampado cronológico es el siguiente:

El algoritmo de firma utilizado debe ser como mínimo SHA-256.

El mensaje fírmanos digitalmente, el cual es la salida del servicio de generación de firmas Digitales siguen los estándares:

- **PKCS#7**-CMS - RFC5126 CMS Advance.
- **Electronic** Signatures (CAdES)
- **W3C** XML Advanced Electronic Signatures (XAdES)
- **ETSI** TS(EN) 102 778 PDF Advanced Electronic Signature Profiles (PAdES)

7. PERFIL DE CERTIFICADOS Y CRL

Esta sección contiene las reglas y guías a seguir por la CA BANREP en cuanto a las extensiones de certificados X.509 y CRL a ser usados.

7.1 Perfil de Certificado

7.1.1 Numero de Versión

La CA BANREP genera certificados X.509 versión 3 según lo estipulado en PKIX Parte 1. Los siguientes campos básicos son soportados:

- **signature** : Firma de la CA para autenticar el Certificado.
- **issuer**: Nombre de la CA.
- **validity**: Fecha de activación y expiración del Certificado.
- **subject**: DN del Suscriptor.
- **subjectPublicKeyInformation**: Identificador del algoritmo y clave.
- **versión**: Versión del certificado X.509.
- **serialNumber**: Numero serial único para el Certificado.

Los siguientes campos de los certificados X.509 versión 3 no son soportados por la CA BANREP:

- **Issuer** unique identifier.
- **Subject** unique identifier.

7.1.2 Extensiones del Certificado

Las extensiones de los certificados versión 3 y el estado actual con respecto a la CA BANREP están especificadas así:

- **authorityKeyIdentifier**: Llenado por la aplicación CA.
- **subjectKeyIdentifier**: Llenado por la aplicación CA.
- **keyUsage**: Como se especifica en la sección 6.1.9.
- **privateKeyUsagePeriod**: Como se especifica en la sección 6.3.2.
- **policyMappings**: Usado únicamente para certificación cruzada.
- **subjectAlternativeName**: Nombre genérico = Dirección de correo electrónico SMIME.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

- **issuerAlternativeName**: Soportado pero no disponible por la CA BANREP.
- **basicConstraints**: Usado únicamente para certificación cruzada.
- **nameConstraints**: Usado únicamente para certificación cruzada.
- **policyConstraints**: Usado únicamente para certificación cruzada.

7.1.3 Identificadores de objeto de los algoritmos

Los algoritmos con sus OID soportados por la CA BANREP son:

Algoritmo Identificador de Objeto Autoridad de Generación

Algoritmo	Identificador de objeto	Autoridad de generación
Dsa-with-sha1	1 3 14 3 2 27	OIW Security SIG
sha1WithRSAEncryption	1 2 840 113549 1 1 5	RSA
sha256WithRSAEncryption	1 2 840 113549 1 1 11	RSA
sha512WithRSAEncryption	1.2.840.113549.1.1.13	RSA
Dsa-with-sha1	1 3 14 3 2 27	Security SIG
DES-EDE3-CBC	1 2 840 113549 3 7	RSA
Cast3CBC	1 2 840 113533 7 66 3	Entrust Technologies
Cast3MAC	1 2 840 113533 7 66 4	Entrust Technologies
Cast5CBC	1 2 840 113533 7 66 10	Entrust Technologies
Cast5MAC	1 2 840 113533 7 66 11	Entrust Technologies
3DESMAC	1 2 840 113533 7 66 14	Entrust Technologies

La CA y los Suscriptores de las entidades finales deben usar soportar para firma y verificación, los siguientes algoritmos:

- **RSA** 2048 de acuerdo con PKCS#1.
- **SHA**-2 según FIPS PUB 180-4.

7.1.4 Forma de nombres

Los certificados generados por la CA BANREP contienen el DN X.500 completo del generador y el asunto del certificado en los campos issuerName y subject.

Los DN son de la forma de un X.501 cadena de caracteres imprimible (RFC 2253)

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

7.1.5 Extensión (identificador de objeto) de política de Certificado

La CA BANREP soporta una política de certificados para firma digital y otra para confidencialidad. Cada certificado debe referenciar por lo menos un OID de política, y puede contener todos los que se desee siempre que no entre en conflicto con otras reglas.

7.2 Perfil CRL

7.2.1 Número de Versión

La CA BANREP genera CRLs y ARLs X.509 versión 2 de acuerdo a lo especificado en PKIX parte 1. Los siguientes son los campos soportados:

- **versión**: Configurado a Versión 2.
- **signature**: Identificador del algoritmo usado para firma de la CRL.
- **issuer**: EL DN de la CA BANREP.
- **thisUpdate**: Tiempo de la generación de la CRL.
- **nextUpdate**: Tiempo de la próxima generación de la CRL.
- **revokedCertificates**: número serial de los certificados revocados.

7.2.2 CRL y extensiones de la entrada CRL

Las CRL versión 2, ARL, y las extensiones de las entradas CRL y ARL de la CA BANREP están especificadas así:

- CRLNumber: Diligenciado por la aplicación CA.
- reasonCode: Diligenciado por la aplicación CA de la forma como lo diligenció el Delegado con Responsabilidad Administrativa. Puede contener los siguientes valores: (0) No especificada, (1) clave comprometida, (3) cambio en la afiliación, (4) reemplazado, (5) cesación de operaciones.
- holdInstructionCode: No soportada por la CA BANREP.
- invalidityDate: Diligenciado por la aplicación CA de la forma como lo diligencia el Funcionario de la ER.
- issuingDistributionPoint: Diligenciado por la aplicación CA.
- certificateIssuer: No soportada por la CA BANREP.
- deltaCRLIndicator: No soportada por la CA BANREP.

8. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

8.1 Modificación de la DPC

El Banco de la República podrá modificar esta Declaración de Prácticas de Certificación (DPC) cuando así lo requiera, por razones de tipo legal, técnico, administrativo o comercial.

8.2 Comunicación de las modificaciones a la DPC

Las modificaciones efectuadas a la DPC serán publicadas en la página Web del Banco (http://www.banrep.gov.co/contenidos/entidad-certificaci-n-cerrada-del-banco-rep-blica). Así mismo, en las instalaciones del Banco de la República se mantendrá un registro de las modificaciones realizadas para facilitar su consulta cronológica, de modo que se tendrá acceso, tanto a la versión actual como a las versiones anteriores.

9. GLOSARIO

A continuación, se relacionan los términos necesarios para La comprensión del presente documento, incluyendo términos técnicos y de tipo empresarial:

CA BANREP: Entidad de Certificación Cerrada del Banco de la República.

CEA: Criterios específicos de acreditación entidades de certificación digital establecidos por el ONAC.

Certificado: Registro electrónico en el que figura información del titular del certificado, su clave pública, vigencia y firma de la CA BANREP como Entidad de Certificación que lo emite.

Centro de Soporte Informático: Dependencia del Banco de la República encargada de dar soporte y apoyo en todo lo relacionado con Informática.

Clave Privada: Valor o valores numéricos que utilizados conjuntamente con un procedimiento matemático conocido sirve para generar la Firma Digital de un mensaje de datos.

Clave Pública: Valor o valores numéricos utilizados para verificar que una firma digital fue generada con la Clave Privada del Suscriptor.

Cliente PKI: Aplicación o Software cliente que usa y/o gestiona certificados digitales. Es capaz de realizar operaciones criptográficas como: firma digital, cifrado, verificación de firma, descifrado y estampado cronológico.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

Código de Autorización: Una de las partes de la información de activación, utilizada para la generación del Certificado, que será entregada por la ER de forma personal.

CRL: Lista de Certificados Revocados.

Delegado con Responsabilidad Administrativa: Funcionario autorizado por el representante legal de la Entidad Usuaria, el cual cumplirá con la función de administrador de los Suscriptores, a quien se le remitirá la documentación pertinente de la Entidad de Registro (ER). Es el autorizado para solicitar cualquier novedad de los Suscriptores de su entidad. Deben existir al menos dos delegados por Entidad Usuaria.

DGD: Departamento de Gestión Documental – Banco de la República.

DGT: Dirección General de Tecnología del Banco de la República.

DSI: Departamento de Seguridad Informática – Banco de la República.

DPC: Declaración de Prácticas de Certificación que es una manifestación pública de la Entidad de Certificación sobre las políticas y procedimientos específicos que aplica para la prestación de sus servicios.

Entidad de Certificación (EC) Cerrada: Entidad que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el Suscriptor, sin exigir remuneración por ello.

Entidad Usuaria: Entidad que realiza operaciones o cruza información con el Banco de la República y de la cual dependen uno o varios Suscriptores.

Entidad de Registro (ER): Persona natural o jurídica que administra (crea, modifica y revoca) los Suscriptores en la Entidad de Certificación. En el caso de la CA BANREP dicho rol es ejercido por el Grupo de Administración de Usuarios del Departamento de Servicios de Tecnología Informática.

EPF (Entrust Profile): Archivo de extensión .EPF en donde se almacena las Claves Privadas generadas por Entrust.

Estampado Cronológico: Mensaje de datos que vincula a otro mensaje de datos con un momento o período de tiempo concreto el cual permite establecer con una prueba que estos datos existían en ese momento o período de tiempo y que no sufrieron ninguna modificación a partir del momento en que se realizó el estampado.

FIPS: Federal Information Processing Standards Publications.

FIPS 140: Security Requirements for Cryptographic Modules.

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

FIPS 186: Estándar para DSS.

Firma Digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación (tomado de la Ley 527 de 1999, artículo 2°).

Funcionario ER: Empleado del Banco de la República encargado de tramitar las solicitudes de suscripción y requerimientos de las Entidades Usuarias relacionados con la Entidad de Certificación CA BANREP.

Grupo de Atención de Incidentes: Grupo interdisciplinario conformado por funcionarios de diferentes dependencias del Banco de la República.

JKS (Java Key Store): Almacén de claves disponible en el JDK

Número de Referencia: Una de las partes de la clave, utilizada para la generación del certificado, que será enviada a la cuenta de correo del Suscriptor por el Funcionario de la Entidad de Registro.

ONAC: Organismo Nacional de Acreditación de Colombia.

PKCS#7-CMS (Cryptographic Message Syntax): Estándar sobre la sintaxis del mensaje criptográfico, utilizado para firmar digitalmente, obtener el digest, autenticar, o cifrar arbitrariamente el contenido de un mensaje.

PKCS#11: Interfaz de dispositivo criptográfico ("**Cryp**tographic **Tok**en **I**nterface" o cryptoki)

PKCS#12: Define un formato de fichero usado comúnmente para almacenar Claves Privadas con su certificado de Clave Pública protegido mediante clave simétrica.

PKI: Infraestructura de gran alcance que se basa en conceptos de Claves Públicas y Privadas.

PKIX parte 3: Corresponde a un estándar liberado por el grupo de trabajo del IETF en temas de PKI y que define el protocolo para administrar las claves y los certificados, desde cómo se solicita un certificado hasta la infraestructura hasta el manejo del ciclo de vida de la PKI.

Profile: Estructura de datos en la cual se almacenan las claves de firma y cifrado de los usuarios, los respectivos certificados, el certificado de la Entidad de Certificación y otra información personal del dueño del certificado.

SEBRA: Portal de servicios electrónicos del Banco de la República (https://wsebra.banrep.gov.co). A través de esta página se ingresa al Portal de Gestión de Identidades, sistema en el que se realiza la gestión de novedades de suscriptores de la CA BANREP.

Fecha: 19 MAR 2019

ASUNTO 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN - CA BANREP

Servicios: Son los diferentes tipos de operación que realizan las Entidades Usuarias con algunas dependencias del Banco de la República. Todos los servicios deben ser relacionados por cada uno de los Suscriptores en un formato establecido por la CA BANREP.

SIC: Superintendencia de Industria y Comercio.

Suscriptor: Persona natural o jurídica, dependiente de la Entidad Usuaria, a quien la CA BANREP le ha expedido Certificados digitales.

TSA BANREP: Servicio de estampado cronológico de la CA BANREP.

Usuario: Persona que puede verificar un documento o mensaje de datos firmado.

(ESPACIO DISPONIBLE)