MANUAL DE INFORMÁTICA
CIRCULAR REGLAMENTARIA EXTERNA - DG-T-294

Destinatario: Usuarios del Sistemas de Seguridad Electrónico – PKI **Fecha:** 2 MAR. 2015

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

La presente Circular Reglamentaria Externa informa que se reemplaza en su totalidad la Circular Reglamentaria Externa SG-INF-294 del 27 de septiembre de 2007, correspondiente al Asunto 7: **"DPC DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI",** del Manual Corporativo de la Dirección General de Tecnología.

Se modifica el nombre del Asunto "DPC - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI" por "DPC - DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI CA BANREP".

El objetivo de esta circular es para actualizar procedimientos administrativos acerca del ciclo de vida de los certificados, roles y responsabilidades de los diferentes actores.

De esta forma se actualiza la reglamentación atendiendo las disposiciones legales vigentes.

Cualquier inquietud que tenga al respecto deberá comunicarse con nuestro Centro de Soporte Informático de la Dirección General de Tecnología del Banco de la República a los teléfonos (571) 343 1111 extensión 2000 o (571) 343 1000.

LUIS FRANCISCO RIVAS DUEÑAS
Subgerente General de Servicios Corporativos

FABIO MAURICIO PINZÓN GONZÁLEZ
Director General de Tecnología

CIRCULAR REGLAMENTARIA EXTERNA – DG-T-294

Fecha: 2 MAR. 2015

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

1. DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI CA BANREP

Introducción

1.1 Objeto

Este documento contiene la Declaración de Prácticas de Certificación (DPC) de la Entidad de Certificación Cerrada del Banco de la República (CA BANREP), establecida para incrementar los niveles de seguridad en los servicios electrónicos del Banco, de conformidad con la legislación vigente sobre mensajes de datos y firma digital.

1.2 Alcance

Definir el conjunto de reglas para la generación y administración de claves y certificados de verificación de firma y de cifrado, así como los demás procesos y procedimientos que se deben cumplir para la operación de la CA BANREP.

1.3 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.

1.4 Condiciones Generales

El Banco de la República es una entidad de derecho público, 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) fue autorizada por la Superintendencia de Industria y Comercio mediante la Resolución 6372 de febrero 28 de 2003. (http://www.onac.org.co/modulos/contenido/default.asp?idmodulo=455)

1.5 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) (http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers).

1.6 Responsables

1.6.1 Administración de la DPC

CIRCULAR REGLAMENTARIA EXTERNA – DG-T-294

Fecha: 2 MAR. 2015

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

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.

1.6.2 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

1.7 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 **Internacional Engineering Task Force** (IETF). (http://www.ietf.org/rfc/rfc3647.txt?number=3647).

2. CONDICIONES GENERALES

2.1 Obligaciones

2.1.1 Obligaciones generales de la CA BANREP:

2.1.1.1 Emitir normas, políticas y procedimientos que reglamenten el uso de los Certificados digitales, y propender por su constante actualización.
2.1.1.2 Mantener la plataforma tecnológica vigente mitigando riesgos de obsolescencia.
2.1.1.3 Mantener actualizadas las bases de datos de Certificados vigentes y revocados. La lista de Certificados revocados será publicada cada media hora.

2.1.2 Obligaciones específicas como Entidad de Registro (ER):

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 ésta 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 dos (2) 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 y por el periodo 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.

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

2.1.4.1 Realizar las novedades de Suscriptores a que haya lugar, con el fin de mantener actualizado el registro de los mismos 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 Enviar la documentación 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 No revelar a ninguna persona la clave privada ni la información de activación del Certificado.

2.1.5.4 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.

2.1.5.5 Solicitar la revocación del Certificado cuando se cumpla alguno de los supuestos previstos en la sección 4.5 de la presente DPC

2.1.5.6 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.

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

2.1.6 Obligaciones de los Usuarios:

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.

2.2 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 con 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 Dada la complejidad de los sistemas informáticos y el propio riesgo tecnológico, la CA BANREP no será responsable de los errores o inconsistencias que puedan presentarse en el sistema de claves asimétricas, o cualquier otro riesgo no predecible de naturaleza similar. 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 literal 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 consultadas en el sitio web del Banco de la República[1].

2.5 Confidencialidad y protección de los datos

2.5.1 Confidencialidad y reserva en la prestación de los servicios de certificación

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

2.5.2 Protección de datos personales

Los datos personales proporcionados al Banco de la República por las Entidades Usuarias, los Delegados con Responsabilidad Administrativa y Suscriptores de las mismas, serán objeto de tratamiento (recolección, almacenamiento, uso, circulación o supresión) para efectos de las actividades propias de la CA BANREP, incluyendo la construcción de indicadores y estadísticas para el seguimiento y control de la prestación de dicho servicio y, en todo caso, dentro de sus

[1] http://www.banrep.gov.co/es/contenidos/pki

funciones constitucionales y legales. Las políticas y lineamientos generales en materia de protección de datos personales se encuentran publicados en la página web del Banco de la República.[2]

2.6 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 ésta 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.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1 Registro inicial

Esta sección describe las prácticas seguidas por la ER y por el Delegado con Responsabilidad Administrativa para identificar y autenticar los datos de suscripción.

3.1.1 Tipos de nombres

El atributo "Subject" del certificado es diligenciado usando cadenas del tipo "nombre distinguido" DN, y no puede estar en blanco por ningún motivo. El DN para la CA BANREP está formado de la siguiente manera:

Componente de Dominio:
dc=co
dc=gov
dc=banrep
Unidad Organizacional:
ou=CA Banrep

Existen tres tipos de Certificados que pueden ser emitidos por la CA BANREP; para los Suscriptores, para comunicaciones B2B (Business to Business), y para realizar automatización de procesos criptográficos, los cuales se especifican a continuación:

3.1.1.1 Para los Suscriptores

El DN para los Suscriptores de las Entidades Usuarias está formado de la siguiente manera:

Componente de Dominio:
dc=co

[2] http://www.banrep.gov.co/proteccion-datos-personales

dc=gov
dc=banrep
Unidad Organizacional:
ou=CA Banrep
ou=NIT de la entidad incluyendo digito de verificación (solo los caracteres numéricos)
Nombre común:
cn=Nombre completo del Suscriptor.

Ejemplos:

DN: cn=Pedro Perez, ou=8030130231,ou=CA Banrep, dc=Banrep, dc=gov, dc=co

3.1.1.2 Para comunicaciones B2B (Business to Business)

El DN para los Certificados que son usados para autenticar los servidores de las Entidades Usuarias que acceden a recursos tecnológicos del Banco de la República de forma automática. Están formados de la siguiente manera:

Componente de Dominio:
dc=co
dc=gov
dc=banrep
Unidad Organizacional:
ou=CA Banrep
ou=NIT de la entidad incluyendo digito de verificación (solo 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, dc=Banrep, dc=gov, dc=co
cn=SB-8030130231-SOI, ou=8030130231,ou=CA Banrep, dc=Banrep, dc=gov, dc=co

3.1.1.3 Para Automatización de procesos Criptográficos

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

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

Unidad Organizacional:
ou=CA Banrep
ou=NIT de la entidad incluyendo digito de verificación (solo 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 para intercambiar información con cada aplicación.
Ejemplos:
cn=8030130231 SOI, ou=8030130231,ou=CA Banrep, dc=Banrep, dc=gov, dc=co

3.1.2 Requerimientos para que el nombre sea significativo

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

3.1.3 Método de prueba de posesión de la Clave Privada

La demostración de posesión de la Clave Privada de firma del Suscriptor sigue lo establecido en PKIX Parte 3. De acuerdo con los tipos de credenciales descritos en la sección 3.1.1. CA BANREP proporcionará los siguientes mecanismos de posesión de la Clave Privada:

3.1.3.1 Para los Suscriptores de las Entidades Usuarias

CA BANREP establecerá los mecanismos para generar la creación del Certificado de sus Suscriptores en un dispositivo Hardware PKCS#11.

3.1.3.2 Para comunicaciones B2B (Business to Business)

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 Documento de Transformación y Generación de Credenciales incorporado 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 2.1.3 y 2.1.4, de este documento.

3.1.3.3 Para Automatización de procesos Criptográficos de externos en la CA BANREP

CA BANREP proporcionará 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 Documento de Transformación y Generación de Credenciales incorporado en http://www.banrep.gov.co/es/contenidos/pki.

Para este tipo de Certificados se considera Suscriptor al Delegado con Responsabilidad Administrativa, quien debe cumplir con lo establecido en las secciones 2.1.3 y 2.1.4, de este documento.

3.1.4 Autenticación de la identidad de las Entidades Usuarias

La CA BANREP solamente aceptarán requerimientos de Certificados de aquellas entidades a las que las dependencias del Banco de la República informen por tener relación con las operaciones que llevan a cabo; los Delegados de la ER harán la verificación correspondiente.

3.1.5 Autenticación de la identidad individual

En todos los casos la activación de Certificados para Delegados con Responsabilidad Administrativa debe hacerse personalmente en las instalaciones del Banco de la República, presentando como documento de identificación la cédula de ciudadanía ante el Delegado de la ER. Como parte de este procedimiento, deberá firmar el "acta de aceptación de los términos de uso de la CA BANREP" (BR-3-599-0) [3].

Para los Suscriptores solicitados por los Delegados con Responsabilidad Administrativa, deberán adjuntar los documentos indicados en el numeral 4.2.2.

3.2 Autenticación para regeneración de claves

La CA BANREP realizará la operación de regeneración de claves de acuerdo con lo estipulado en PKIX parte 3 – Certificate Management Protocol. Los Suscriptores son autenticados usando su par de claves de firma digital. Cuando una clave de Firma Digital se encuentre vencida, el Delegado de la ER, debe autenticar al Suscriptor que hace la solicitud, de la misma manera, como se menciona en la sección 3.1.4 y 3.1.5

3.3 Autenticación para regeneración de claves después de revocación

El Delegado de la ER llevará a cabo la autenticación después de una revocación, como se especifica en secciones 3.1.4 y 3.1.5.

3.4 Autenticación para la solicitud de revocación

El Delegado con Responsabilidad Administrativa realizará las solicitudes de revocación mediante el envío de un correo electrónico a la cuenta **ca-novedades@banrep.gov.co**, adjuntando el formato de Novedades de Suscriptor Entidad de Certificación - CA BANREP, que deberá estar firmado digitalmente.

[3] Disponible en http://www.banrep.gov.co/sites/default/files/paginas/BR-3-599-0.doc El acta será parte de la carpeta que se conforme para la respectiva Entidad Usuaria en el archivo de la Unidad de Soporte y Continuidad Informática.

CIRCULAR REGLAMENTARIA EXTERNA – DG-T-294

Fecha: 2 MAR. 2015

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

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"[4], que deberá ser diligenciado en su totalidad ya que todos los datos allí solicitados son necesarios 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.

4.2 Solicitud de certificados

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 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" establecido para este fin.

4.2.1.2 Los documentos que diligenciará el solicitante deberán ser entregados en original al Delegado de la ER en el Centro de Soporte Informático, ubicado en la Oficina Principal del Banco de la República.

4.2.1.3 El Delegado de la ER deberá autenticar 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, el Delegado de la ER deberá suministrar 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) establecida para este fin.

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

4.2.2 Solicitud de Certificados para un Suscriptor

El proceso de registro para las claves y Certificados de los Suscriptores es el siguiente:

4.2.2.1 El Delegado con Responsabilidad Administrativa de la Entidad Usuaria diligenciará el formato Novedades de Suscriptor Entidad de Certificación - CA BANREP (BR-3-598-0)[5].

4.2.2.2 El formato de Novedades de Suscriptor Entidad de Certificación - CA BANREP totalmente diligenciado y firmado digitalmente por el Delegado con Responsabilidad Administrativa, se enviará junto con una copia escaneada del documento de identificación del Suscriptor, mediante correo electrónico a la cuenta ***ca-novedades@banrep.gov.co***.

4.2.2.3 El Delegado de la ER verificará que el firmante esté autorizado como Delegado con Responsabilidad Administrativa y procederá a crear el Suscriptor y a generar la información de activación del Certificado (Número de Referencia y Código de Autorización) respectiva.

4.3 Distribución de Certificados a los Suscriptores y Entidades Usuarias

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

4.3.1 El Delegado de la ER grabará la información, creando así el respectivo Suscriptor en la CA BANREP dejándolo en el estado "adicionado". En este momento se generará la información de activación del Suscriptor, la cual consta de un Código de Autorización y un Número de Referencia que son requeridos para la activación del Certificado.

4.3.2 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 el Delegado de la ER, directamente al buzón electrónico corporativo del Suscriptor especificado en el formato de solicitud, junto con la información relativa al trámite subsiguiente.

4.3.3 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.

4.3.4 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

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

mencionada en el numeral 4.3.3. En el evento de existir diferencia en la información del solicitante (nombres, apellidos, N° de cédula, etc.), deberá repetirse la solicitud.

4.3.5 Validada la identidad, el Delegado con Responsabilidad Administrativa deberá hacer llegar una copia del acta escaneada mencionada en el numeral 4.3.3 y con firma digital a la dirección de correo electrónico del delegado de la ER: ***ca-novedades@banrep.gov.co***. Si en las 24 horas anteriores a la fecha de expiración[6] [1] del Código de Autorización, el Banco de la República no recibe el acta mencionada en el numeral 4.3.3, se deberá volver a realizar la solicitud.

4.3.6 Una vez el Delegado de 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.

4.3.7 Con el Código de Autorización y el Número de Referencia conocidos por el Suscriptor, éste podrá proceder con la activación de la llave. Para que dicho procedimiento tenga éxito, en el computador de la Entidad Usuaria deberá estar correctamente instalado el software[7] y tener 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 el Delegado de la ER.

4.3.8 El Código de Autorización y el Número de Referencia podrán ser utilizados solamente una vez y dentro de los diez (10) 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.

4.4 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.

4.5 Revocación

4.5.1 Circunstancias para la revocación

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

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

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:

4.5.1.1 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.

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

4.5.1.3 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. Sobre 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)[8]
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.

4.5.2 Quiénes pueden solicitar la revocación

La CA BANREP acepta solicitudes de revocación de las siguientes personas:

4.5.2.1 El Delegado con Responsabilidad Administrativa. 4.5.2.2 El Delegado de la ER.
4.5.2.2 Los oficiales de seguridad de la CA BANREP.

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

4.5.3 Procedimiento para revocación:

4.5.3.1 El Delegado con Responsabilidad Administrativa deberá diligenciar el formato de Novedades de Suscriptor Entidad de Certificación - CA BANREP (BR-3-598-0)[9] y enviarlo firmado digitalmente por él, a la cuenta de correo **ca-novedades@banrep.gov.co**.

4.5.3.2 El Delegado de la ER deberá verificar la Firma Digital, corroborando que la solicitud es realizada por el Delegado con Responsabilidad Administrativa de la Entidad Usuaria. Adicionalmente, verificará que la información contenida en la solicitud sea correcta y esté completa.

4.5.3.3 El Delegado de la ER procesará las solicitudes.

4.5.3.4 El Delegado de la ER, por medio de un correo electrónico, enviará una confirmación de la revocación al Delegado con Responsabilidad Administrativa.

4.5.4 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.

4.5.5 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.

4.5.6 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.

4.6 Procedimiento de sistemas de seguridad y auditoría

4.6.1 Tipos de eventos registrados

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

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

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.

4.6.2 Frecuencia del procesamiento de registros de auditoría

Los oficiales de seguridad procesan 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.

4.6.3 Período de conservación de registros de auditoría

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

4.6.4 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, según lo establece el Banco de la República.

4.6.5 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 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 vez por semana. Estos contienen copia semanal consolidada de los archivos de registro de auditoría.

4.6.6 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 de la CA BANREP, la aplicación de la CA BANREP y el personal de la CA BANREP

4.6.7 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 a los procedimientos internos establecidos para esta actividad.

4.7 Conservación de registros

Los siguientes registros serán conservados por la CA BANREP:

4.7.1 Información de auditoría.
4.7.2 Solicitudes de los Suscriptores
4.7.3 Certificados de CRL
4.7.4 La Clave Privada de descifrado de los Suscriptores 4.7.5 Reportes de discrepancia, compromiso de claves privadas y correspondencia asociada.
4.7.5 La CA BANREP retendrá los registros de Auditoría como mínimo (1) año.
4.7.6 Certificados y Claves Privadas son retenidas veinte (20) años.
4.7.7 Una copia de todos los registros archivados, documentación recibida y las copias de respaldo son almacenadas de acuerdo con los lineamientos establecidos por el Banco de la República
4.7.8 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.

4.8 Cambio de clave

De acuerdo a los tipos de credenciales generadas por la CA-BANREP y descritos en el numeral 3.1.1, se establece que el tiempo de vida de las claves estará especificado de la siguiente forma:

4.8.1 Para los Suscriptores

Las claves emitidas para los Suscriptores tendrán una vigencia de dos (2) años.

4.8.2 Para comunicaciones B2B (Business to Business) en la CA- BANREP

Las claves emitidas para las comunicaciones B2B (Business to Business) tendrán una vigencia de dos (2) años.

4.8.3 Para Automatización de procesos Criptográficos en la CA- BANREP

Las claves emitidas para automatización de procesos Criptográficos tendrán una vigencia de dos (2) años.

4.9 Disponibilidad de la CA BANREP

4.9.1 Daños en los recursos de computación, software o datos

La CA BANREP ha implementado un plan de contingencia y recuperación de desastres, que se dirige a la recuperación de sus operaciones, frente a daños en los recursos computacionales, software y datos.

4.9.2 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.

4.10 Terminación de la CA BANREP

La CA BANREP notificará a los Usuarios, Suscriptores y Entidades Usuarias acerca de la terminación de sus servicios, por lo menos con noventa (90) días de antelación, una vez autorizada para el efecto por la Organismo Nacional de Acreditación (ONAC).

4.11 Otros requisitos operacionales

4.11.1 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:

4.11.1.1 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.

4.11.1.2 El Delegado de la ER verificará la Firma Digital de la solicitud presentada.

4.11.1.3 El Delegado de la ER recuperará el Certificado del Suscriptor, generando así la información de activación respectiva (el Número de Referencia y el Código de Autorización).

4.11.1.4 El Número de Referencia y el Código de Autorización serán enviados vía correo electrónico firmado digitalmente por el Delegado de la ER, directamente al Delegado con Responsabilidad Administrativa.

4.11.1.5 El Delegado con Responsabilidad Administrativa utilizará el Número de Referencia y el Código de Autorización recibido del Delegado 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 diez (10) 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.

4.11.2 Tipo de Certificado

Para los tres (3) tipos de certificados (establecidos en el numeral 3.1.1) que pueden ser emitidos por la CA BANREP para Entidades Usuarias, se tiene definido lo siguiente:

4.11.2.1 Para todos los Suscriptores, un dispositivo Hardware PKCS#11 (Token Criptográfico).

4.11.2.2 Para comunicaciones B2B (Business to Business), un archivo EPF (Entrust Profile) que podrá ser transformado en formatos PKCS#12 o JKS.

4.11.2.3 Para realizar automatización de procesos criptográficos, un archivo EPF (Entrust Profile) que podrá ser transformado en formatos PKCS#12 o JKS.

4.11.3 Terminación de una Suscripción

Esta práctica es seguida cuando la Entidad Usuaria desea terminar la vinculación de un Suscriptor en la CA BANREP:

4.11.3.1 El Delegado con Responsabilidad Administrativa, podrá iniciar este proceso diligenciando el formato de Novedades de Suscriptor Entidad de Certificación - CA BANREP (BR-3-598-0)[10] y enviarlo firmado digitalmente por él a la cuenta **ca-novedades@banrep.gov.co**.

4.11.3.2 El Delegado de la ER deberá verificar la Firma Digital, corroborando que la solicitud es realizada por el Delegado con Responsabilidad Administrativa. Adicionalmente, verificará que la información contenida en la solicitud sea correcta y esté completa.

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

4.11.3.3 El Delegado de la ER archivará una copia de la solicitud de terminación (Formato BR-3-598-0) en la carpeta que se conforme para la respectiva Entidad Usuaria en el archivo de la Unidad de Soporte y Continuidad Informática.

4.11.3.4 El Delegado de 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.

4.11.3.5 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 del Banco de la República 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, el Banco de la República, 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 nuestro Departamento de Gestión Documental.

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 Delegado 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 los Delegados de 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:

5.2.2.1 Gestionar novedades de Suscriptores.

5.2.2.2 Validar la identidad y autorización del Delegado con Responsabilidad Administrativa.

5.2.2.3 Registrar la información del Suscriptor en la CA BANREP.

5.2.2.4 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.

5.4 Grupo de atención de incidentes

Existe un Grupo de Atención de Incidentes conformado por: Oficial de Seguridad de la CA BANREP, Administrador de la ER, Control Interno, Auditor y demás personal requerido según el caso.

6. CONTROLES TÉCNICOS DE SEGURIDAD

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

El par de claves de firma de la CA BANREP es generado durante la instalación inicial de la aplicación CA.
El par de claves de cifrado de los Suscriptores es generado por la aplicación CA.
El par de claves de firma es generado por la aplicación Cliente PKI.
Los algoritmos de generación de claves son los permitidos por la legislación colombiana vigente y normativa que regule las entidades de certificación.

6.1.2 Entrega de la Clave Privada a los Suscriptores

Las Claves Privadas de descifrado son generadas por la aplicación CA 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 debe 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.

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 1024 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). La aplicación CA y las aplicaciones Cliente PKI deberían generarlas según los parámetros establecidos en FIPS 186.

6.1.7 Generación de claves Hardware / Software

Las claves de la CA BANREP son generadas usando un módulo criptográfico hardware que cumple con lo establecido en FIPS 140-1 nivel 3.
Todas las claves de los Delegados de la ER y de los Suscriptores son generadas usando hardware o software diseñado para cumplir con lo establecido en FIPS-140-1 o cualquier otro requerimiento de nivel equivalente de funcionalidad y seguridad.

6.1.8 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:

- -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. Todas las otras operaciones criptográficas de la CA pueden ser realizadas por módulos criptográficos, que por lo menos, sean certificados FIPS 140-1 nivel 2.

Los módulos criptográficos usados por las Entidades Usuarias para sus suscriptores deben ser diseñados para reunir los requerimientos mínimos de FIPS 140-1.

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 para cada uno de los tres (3) tipos de certificados (Expresado en el punto 3.1.1), se tiene definido lo siguiente:

6.2.4.1 Para los Suscriptores, un dispositivo Hardware PKCS#11 (Token Criptográfico).

6.2.4.2 Para comunicaciones B2B (Business to Business), un archivo EPF (Entrust Profile) que podrá ser transformado en formatos PKCS#12 o JKS.

6.2.4.3 Para realizar automatización de procesos criptográficos, 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 el password 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 token criptográficos.

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.
Los Suscriptores deben usar aplicaciones cliente PKI que finalizan el acceso a sus claves privadas como parte del proceso de log-out. Lo mismo se debería hacer después del período de inactividad establecido.

6.2.7 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 según lo especificado en la sección 4.7.

6.3.2 Períodos de uso de las Claves Públicas y Privadas

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

6.3.2.1 Clave Pública y Certificado de verificación de firma de la CA: veinte (20) años.

6.3.2.2 Clave Privada de firma de la CA: Veinte (20) años.

6.3.2.3 Clave Pública de verificación de firma de los Suscriptores: dos (2) años.

6.3.2.4 Clave Privada de firma de los Suscriptores: dos (2) años.

6.3.2.5 Clave Pública de cifrado y Certificado de los Suscriptores: dos (2) años.

6.3.2.6 Clave Pública de verificación de firma para comunicaciones B2B y procesos de automatización: dos (2) años.

6.3.2.7 Clave Privada de firma para comunicaciones B2B y procesos de automatización: Dos (2) años.

6.3.2.8 Clave Pública de cifrado y certificado para comunicaciones B2B y procesos de automatización: Dos (2) años.

6.3.2.9 Clave Privada de descifrado de los Suscriptores: dos (2) años.

6.3.2.10 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 4.3., de este documento.

Los Suscriptores usan contraseña para activar sus módulos criptográficos o crear los *profiles* correspondientes (Aplica para credenciales con fines de comunicaciones B2B o procesos de Automatización). 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:

6.5.1.1 Controles de acceso a los servicios de la CA BANREP y roles de la PKI.

6.5.1.2 Segregación de los deberes para los roles de la PKI.

6.5.1.3 Identificación y autenticación de los roles de la PKI e identidades asociadas.

6.5.1.4 Sesiones seguras entre la aplicación CA y las aplicaciones cliente PKI.

6.5.1.5 La base de datos de la CA permanece cifrada.

6.5.1.6 Archivo del histórico de claves de la CA, Suscriptores e información de auditoría.

6.5.1.7 Auditoría sobre los eventos relacionados a la seguridad.

6.5.1.8 Mecanismos de recuperación de claves y de la aplicación CA.

6.5.1.9 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.

6.5.1.10 Existe una parte aislada dentro del centro de cómputo, donde está ubicado el hardware que almacena la clave privada de la CA; los únicos con acceso autorizado a estas máquinas son los administradores del Departamento de Seguridad Informática.

6.6 Ciclo de vida de los controles técnicos

6.6.1 Controles de desarrollo del sistema

La aplicación CA, 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, 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 firewall.

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.
- 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.

Para mayor información ver secciones 4.2.1 y 4.2.2

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)

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 Numero 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 Delegado 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 total del presente documento, incluyendo términos técnicos y jerga de tipo empresarial:

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

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.

Código de Autorización: Una de las partes de la información de activación, utilizada para la generación del Certificado, que será entregada por el Delegado de 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 Certificación (ER). Es el autorizado para solicitar cualquier novedad de los Suscriptores de su entidad. Deben existir al menos dos delegados por Entidad Usuaria.

CIRCULAR REGLAMENTARIA EXTERNA – DG-T-294

Fecha: 2 MAR. 2015

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

Delegado ER: Funcionario 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.

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 de la Unidad de Soporte y Continuidad 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.

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°).

CIRCULAR REGLAMENTARIA EXTERNA – DG-T-294

Fecha: 2 MAR. 2015

ASUNTO: 7: DPC – DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA PKI 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 Delegado de la Entidad de Registro.

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 profile.

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.

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

(ESPACIO DISPONIBLE)