Banco de la República
Bogotá D. C., Colombia

Dirección General de Tecnología
Departamento de Seguridad Informática

ASPECTOS TÉCNICOS DEL SERVICIO DE FIRMA ELECTRÓNICA

DSI-GI-129

23 de septiembre de 2021
Versión #1.0

CONTENIDO

1 INTRODUCCIÓN

1.1 OBJETIVO

Presentar los aspectos técnicos relacionados con los servicios de Firma Electrónica del Banco de la República (BR)

1.2 ALCANCE

Describir el marco técnico y de seguridad informática del servicio de Firma Electrónica.

1.3 AUDIENCIA

Este documento está dirigido a todas las entidades financieras que en su operación con el Banco hacen uso de las identidades electrónicas generados por éste para asegurar criptográficamente el intercambio de información.

1.4 ORGANIZACIÓN DEL RESTO DEL DOCUMENTO

En la sección 2 se presentan y describen los controles técnicos que emplea el BR para asegurar tanto la plataforma tecnológica como la información generada por la gestión de los servicios de PKI.

En la sección 3 se encuentra la descripción de los registros de auditoria, tipos de eventos que se generan y conservan y el esquema de conservación de esta información.

En la sección 4 se detalla el esquema establecido por el BR para garantizar la disponibilidad de la infraestructura del servicio.

2 CONTROLES TÉCNICOS DE SEGURIDAD

Las claves de firma (verificación) de la AC-BR (Raíz y Subordinada) y de la Autoridad de Tiempo del BR (AT-BR) son generadas directamente por la AC-BR como parte del proceso de instalación de los componentes de la PKI.

Los algoritmos de generación de claves empleados son los permitidos por la legislación colombiana vigente y aquellos recomendados por la industria. La AC-BR genera claves asimétricas RSA (Rivest-Shamir-Adleman) con un tamaño de 4096 bits para el par de claves de firma de la misma AC-BR y de 2048 bits para los pares de claves de firma y cifrado de los Suscriptores. La AC-BR no generará claves DSA (Digital Signature Algorithm). Las aplicaciones Cliente deberían generarlas según los parámetros establecidos en FIPS 186.

Las claves de la AC-BR y de la AT-BR son generadas usando un módulo criptográfico de hardware que cumple con lo establecido en FIPS 140-2 Nivel 3. Por su parte, las claves criptográficas asociadas a las identidades electrónicas de los Suscriptores son generadas usando hardware o software diseñado para cumplir con lo establecido en FIPS 140-2 Nivel 3.

La clave de firma de la AC-BR se emplea únicamente para firmar certificados y CRLs (Cetificate Revocation List). La AC-BR genera las claves públicas de verificación de firma con los parámetros digital Signature, keyCertSign y CRLSign. Las claves de cifrado por su parte se generan con el parámetro keyEncipherment.

La clave Pública de la AT-BR 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.

La clave de firma de la AT-BR se emplea únicamente puede firmar las solicitudes de estampa cronológico: digitalSignature, nonRepudiation.

2.1 PROTECCIÓN DE LA CLAVE PRIVADA

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

Las operaciones de generación de la clave de Firma de la AC-BR, almacenamiento de la clave y firma de Certificados son realizadas en un módulo criptográfico en hardware certificado FIPS 140-2 nivel 3.

La AC-BR tiene implementado control de doble intervención para la generación de claves y para la generación de la clave de descifrado del servicio de recuperación de claves. Para el

caso, se requiere la participación de un funcionario roles de Usuario Maestro (Oficial de Seguridad) y un segundo funcionario autorizado previamente.

2.1.2 Copia de Seguridad de la Clave Privada

La AC-BR mantiene en sus bases de datos un histórico de las claves de descifrado de los Suscriptores con el propósito de recuperación de documentos. Para el efecto, se realiza una copia de respaldo dos (2) veces al día. A su vez, a estas copias se les realiza una segunda copia de respaldo diariamente según las políticas de respaldo de medios de las plataformas tecnológicas del BR.

A las claves privadas de firma de los Suscriptores no se realiza ninguna copia de seguridad por parte del BR.

2.1.3 Generación de la Clave Privada para Suscriptores

Las Claves Privadas de cifrado de los Suscriptores son generadas con un módulo software de la infraestructura PKI del BR 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 la identidad electrónica tipo Pertenencia a Empresa, un dispositivo Hardware PKCS#11 (Token Criptográfico).

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

Los Suscriptores deben usar aplicaciones cliente PKI que acceden a 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.

2.1.4 Compromiso de la Clave Privada de la AC-BR

En el caso que la clave privada de la AC-BR sea comprometida se procederá a realizar la revocación de todas las claves de todos los suscriptores junto con las claves mismas de la AC-BR.

En este escenario, se generará un nuevo par de claves para la AC-BR y emitiendo de nuevo las claves de los Suscriptores, siguiendo los protocolos de ceremonia y generación de llaves correspondientes.

2.1.5 Compromiso de la Clave Privada de la AT-BR

En el caso que la clave privada de la AT-BR sea comprometida se procederá con la revocación de esta clave. 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.

2.1.6 Generación de CRL por Revocación de Claves

Para todos los casos en que se realice una revocación de llaves será generada una nueva CRL.

2.1.7 Método de destrucción de la Clave Privada de la AC-BR

El BR eliminará la clave privada de la Ac-BR cuando expire su plazo de vigencia o cuando ésta haya sido revocada. La destrucción se realizará utilizando el procedimiento técnico establecido para garantizar la eliminación definitiva de la clave dentro del módulo HSM. Lo mismo ocurrirá con sus copias de seguridad.

2.1.8 Método de borrado de la Clave Privada del Suscriptor

Cuando un Suscriptor no requiera hacer más uso de las claves criptográficas generadas por el BR se deberá inicializar el token criptográfico con la herramienta del fabricante.

2.2 OTROS ASPECTOS DE LA ADMINISTRACIÓN DE CLAVES

2.2.1 Archivo de las Claves Públicas

La plataforma PKI del BR archivará las claves públicas de verificación de firma de la AC-BR y los pares de claves de cifrado de los Suscriptores.

2.2.2 Períodos de Uso de las Claves Públicas

Los períodos de uso de las Claves Públicas y Privadas generadas por la AC-BRP serán así:

- Clave de verificación de firma de la AC-BR (Raíz): Veinte (20) años.

- Clave Privada de firma de la AC-BR (Raíz): Veinte (20) años.

- Clave de verificación de firma de la AC-BR (Subordinada): Veinte (20) años.

- Clave Privada de firma de la AC-BR (Subordinada): Veinte (20) años.

- Clave de firma Pertenencia a Empresa: Dos (2) años.

- Clave de firma Persona Jurídica Entidad Empresa: Dos (2) años.

- Clave Privada de firma Pertenencia a Empresa: Dos (2) años.

- Clave Privada de firma Persona Jurídica Entidad Empresa: Dos (2) años.

- Clave Pública de cifrado y Certificado de los Suscriptores: Dos (2) años.

- Clave Pública de verificación de firma para comunicaciones B2B, procesos de automatización y Mensajería: Dos (2) años.

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

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

- Clave Privada de descifrado de los Suscriptores: Dos (2) años.

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

2.2.3 Claves de Activación de Identidad Electrónica

El Número de Referencia y el Código de Autorización son generados en software por la infraestructura PKI del BR y permanecen en su base de datos encriptados hasta que el Suscriptor cree o recupere sus Claves.

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 acorde con las políticas de seguridad del Banco de la República.

2.3 OTROS CONTROLES DE SEGURIDAD

2.3.1 Controles de Seguridad de los Servidores

La plataforma PKI del BR posee controles técnicos de seguridad los cuales son reforzados a través de los sistemas operativos de los componentes (servidores) que componen esta infraestructura y del mismo sistema PKI, incluyendo:

- Controles de acceso a los servicios de la PKI del BR.

- Roles configurados en la PKI.

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

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

- Sesiones seguras entre los componentes del sistema PKI y sus aplicaciones cliente.

- La base de datos de la infraestructura PKI permanece cifrada.

- Archivo del histórico de claves de la AC-BR, Suscriptores e información de auditoría.

- Auditoría sobre los eventos relacionados a la seguridad.

- Mecanismos de recuperación de claves.

- Control físico de acceso mediante una compuerta con claves y tarjetas de acceso y supervisión por parte del Departamento de Protección y Seguridad del BR.

2.3.2 Controles de la Administración de Seguridad

El BR tiene definidas políticas, normas, estándares y mecanismos para la administración de los incidentes, cambios y control de configuración de la plataforma tecnológica que soporta los servicios de PKI.

La red comunicaciones que soporta esta infraestructura está segmentada para proveer niveles adicionales de seguridad. El control de acceso a los servicios ofrecidos por la PKI es controlado por un componente de seguridad tipo firewall.

2.4 ANÁLISIS DE VULNERABILIDADES

El Departamento de Seguridad Informática del BR adelantará los análisis de vulnerabilidades sobre la infraestructura tecnológica que soporta la PKI de acuerdo con los procedimientos internos establecidos para esta actividad.

3 REGISTROS DE AUDITORÍA

Los registros de Auditoria de la PKI del BR resultan a partir de una combinación de procesos manuales y automáticos realizados por el sistema operacional, la aplicación y el personal administrativo de la plataforma.

3.1 TIPOS DE EVENTOS REGISTRADOS

Para propósitos de auditoría, los siguientes tipos de eventos serán registrados automática o manualmente por parte de la infraestructura PKI del BR:

- Administración de los Suscriptores y administradores de la infraestructura y componentes PKI.

- Gestión de la plataforma por parte de los Administradores (Oficiales de Seguridad).

- Administración de claves.

- Encendido y apagado de la AC-BR.

- Acceso de la AC-BR al directorio de usuarios PKI.

- Administración de la base de datos de la PKI.

- Intentos de entradas y salidas al sistema.

- Intentos no autorizados de acceso a la red y sistemas de la PKI.

- Administración de los registros de auditoría.

- Cambios en la configuración del sistema.

- Actualización de software y hardware.

- Mantenimiento "programado" y "no programado" sobre el sistema y ubicación física.

- Generación de estampas cronológicas.

3.2 FRECUENCIA DEL PROCESAMIENTO DE REGISTROS DE AUDITORIA

El BR, 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:

- Acumulación de registros del sistema creados desde el último proceso.

- Revisión de registros de auditoría al sistema.

- Análisis y reportes de eventos significativos, alertas e irregularidades y resolución de las causas de los eventos.

3.3 PROTECCIÓN Y PERÍODOS DE CONSERVACIÓN DE REGISTROS DE AUDITORIA

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.

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

Una copia de los registros físicos de auditoría es 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 de los servidores de la infraestructura PKI del BR. 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 DISPONIBILIDAD DE LA INFRAESTRUCTURA

El BR 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 infraestructura PKI. Este plan de continuidad tecnológica contempla los siguientes aspectos:

- La redundancia de todos los componentes de la infraestructura.

- 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 PKI el BR informará a todos los terceros conocidos sobre la indisponibilidad de la plataforma. 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.

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.

4.1 ACUERDOS DE NIVELES DE SERVICIO

La infraestructura que soporta el servicio de PKI del BR estará disponible 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.

4.1.1 Cesación del Servicio de PKI

El BR 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:

- La terminación de su actividad o actividades y la fecha precisa de cesación.

- Las consecuencias jurídicas de la cesación respecto de los certificados expedidos.

- La fecha exacta de revocación de las claves criptográficas de los suscriptores y de la AC-BR (Raíz y Subordinada).