Nuevo esquema de certificación digital en el Banco de la República

Last modified Saturday the 8th of June, 2013

Colombia es uno de los países pioneros en reglamentación respecto al trámite de mensajes digitales (comercio electrónico). El marco legal colombiano comprende:

- Ley 527 de Agosto de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación (parte de una PKI) y se dictan otras disposiciones,

- Decreto 1747 de Septiembre de 2000: Se reglamenta parcialmente la ley 527 en lo relacionado con las entidades de certificación, los certificados y las firmas digitales,

- Resolución 26930 de Octubre de 2000: Estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores,

Dado lo anterior y contando en el presente con elementos jurídicos suficientes y consolidados para soportar los intercambios electrónicos de manera segura, el Banco de la República ha adquirido y montado una infraestructura de llaves públicas (PKI).

Una PKI contribuye significativamente al logro y cumplimiento, en términos de seguridad informática, de las normas establecidas por el marco legal colombiano; dicho mejor, Colombia y en particular el Banco, cuenta con un referente legal vigente que le permite subir su nivel de seguridad a través de herramientas avanzadas en seguridad como el PKI. Hoy en día un mensaje digital tiene el mismo efecto probatorio que el papel ante un juez y dependerá del modelo de seguridad que se haya aplicado, el tener los suficientes argumentos probatorios en caso de un incidente informático.

El modelo de seguridad del Banco busca principalmente el cumplimiento de los 7 fundamentos de seguridad informática, en todos sus servicios críticos, a saber:

- Confidencialidad: Cuando la información es sólo accesible por aquellos a los cuales se ha autorizado su acceso.
- Integridad: Cuando la información es exacta y completa. Cuando se garantiza que la información no se modifica desde su momento de creación.
- Disponibilidad: Cuando la información es accesible a los usuarios autorizados en el momento de requerirla.
- Autenticación: Cuando se puede garantizar la identidad de quien solicita acceso a la información.
- Autorización o Control de Acceso: Cuando la información es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo.
- No repudiación: Cuando la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en éste.
- Observancia: Cuando la información relacionada con las acciones y actividades de los usuarios (personas o procesos) se encuentra debidamente registrada y monitoreada. Además cuando se vela y propende por el adecuado funcionamiento del modelo de seguridad informática.

En general, a partir de este año, todos los servicios sujetos a seguridad y contingencia, comenzarán a migrarse desde este año hacia plataformas de certificados digitales, a través de nuestra PKI.

Para finalizar es importante comentar, que la entidad de certificación, componente fundamental de la PKI, almacena sus claves (llaves) en dispositivos de alta seguridad (hardware), el cual requiere de varias intervenciones físicas para su acceso. Con esto y con el hecho de que nuestro modelo de PKI está supervisado por la Auditoria Informática y Control Interno, el Banco garantiza que el núcleo de seguridad informática, está debidamente protegido, pues además, los servidores donde está montado el PKI están resguardados físicamente por un centro de cómputo que cumple con las especificaciones internacionales, tanto ambientales como de control de acceso, para la protección adecuada de dichas máquinas.

Fuente: https://www.banrep.gov.co/es/contenidos/page/nuevo-esquema-certificaci-n-digital-banco-rep-blica