Banco de la República | Colombia
Somos el banco central de Colombia

Marco Legal – Firma Electrónica

Lunes, octubre 4 de 2021 - 12:00pm

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 1074 de Mayo de 2015.**
- **Decreto 2364 de Noviembre de 2012**. Se reglamenta el uso de la Firma Electrónica en el país.

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:

1. **Confidencialidad:** Cuando la información es sólo accesible por aquellos a los cuales se ha autorizado su acceso.
2. **Integridad:** Cuando la información es exacta y completa. Cuando se garantiza que la información no se modifica desde su momento de creación.
3. **Disponibilidad:** Cuando la información es accesible a los usuarios autorizados en el momento de requerirla.
4. **Autenticación:** Cuando se puede garantizar la identidad de quien solicita acceso a la información.
5. **Autorización o Control de Acceso:** Cuando la información es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo.
6. **No repudiación:** Cuando la información involucrada en un evento corresponde a quien participa en el mismo, quien no podrá desconocer su intervención en este.
7. **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.