ANEXO 3. Protección de la Clave Privada

Importancia de la protección de la clave privada e implicancias legales

Por: Abog. Mareille Astolfi Galván[1]

Cada suscriptor de Certificado Digital posee una pareja de claves (basados en un sistema criptográfico asimétrico):

- **Clave privada**: será custodiada por el suscriptor del certificado digital (quien es el propietario) y no se debe de dar a conocer a ningún otro.

- **Clave pública**: será conocida por todas las personas con quienes se relacione.

Este par de claves se obtienen mediante métodos matemáticos complicados de forma que por razones de tiempo de cómputo, es imposible conocer una clave a partir de la otra. Asimismo, esta pareja de claves es única y complementaria: lo que cifra una SÓLO lo puede descifrar la otra y viceversa.

La clave privada es almacenada de manera segura en un dispositivo criptográfico que cumpla con el Estándar FIPS 140-2 sección 4.7.2 o Common Criteria EAL4+, y está en posesión del suscriptor del certificado digital (tarjeta inteligente, token o disco duro de la computadora).

Es a través de la clave privada que el suscriptor de un certificado digital hará uso de su firma digital. Una firma digital tiene el mismo propósito que una manuscrita. Una firma manuscrita es sencilla de falsificar mientras que la digital es imposible en tanto un tercero no descubra o conozca el PIN de acceso o contraseña de la clave privada del suscriptor y tenga en su poder el dispositivo criptográfico donde se encuentra almacenada dicha clave.

La firma digital se basa en la propiedad sobre un mensaje o documento cifrado (resumen hash) utilizando la clave privada de un suscriptor de certificado digital y ésta sólo puede ser descifrado utilizando la clave pública asociada. De tal manera, se tiene la seguridad de que el mensaje o documento que ha podido descifrarse utilizando la clave pública sólo pudo cifrarse utilizando la clave privada.

Por tales razones, el suscriptor del certificado digital debe ser razonablemente diligente en la custodia de su clave privada, así como, con la en la custodia de su PIN de acceso o contraseña de su clave privada, con el fin de evitar usos no autorizados. Esta contraseña es creada por el suscriptor y debe ser conocida únicamente por él.

Ahora bien, en caso de extravío o pérdida de su tarjeta inteligente o token criptográfico se estaría garantizando que nadie que no conozca dicha contraseña o PIN de acceso podrá hacer uso de su firma digital.

---

[1] Especialista en Regulación de las TIC's. Sub Gerencia de Registro Digital – RENIEC.

El suscriptor del certificado digital deberá solicitar inmediatamente a la EREP la cancelación de su certificado, en cuanto se produzcan los siguientes hechos:

- Pérdida, robo o extravío de su dispositivo criptográfico que almacena su clave privada.

- Cuando sospeche el compromiso potencial de su clave privada, debido a la pérdida de su contraseña o sospecha de que un tercero conozca o pueda deducir dicha contraseña.

- Por exposición, puesta en peligro o uso indebido de la clave privada o de la contraseña o PIN de acceso a su clave privada.

- Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada o la contraseña o PIN de acceso a su clave privada.

El mal uso o uso no autorizado de una clave privada, debido a una falta de diligencia adecuada por parte del suscriptor del certificado digital (propietario de la clave privada) le generará implicancias legales, sólo en tanto un tercero suplante su identidad firmando digitalmente documentos o mensajes a nombre del suscriptor.