INTRODUCCIÓN

La revolución de las tecnologías de la información, conjuntamente con el desarrollo de las infraestructuras de comunicaciones, está haciendo cambiar significativamente las relaciones entre individuos y organizaciones, tanto en Europa, Estados Unidos, Asia, España como en todo el mundo. Estas nuevas formas de comunicación abren un gran abanico de posibilidades tanto para ciudadanos como para empresas y permiten comercializar productos y servicios de una forma ágil y económica.

En Ecuador, las distintas Administraciones están apostando decididamente por Internet como vía de comunicación, creando páginas webs con un contenido de interés público que están puestas a disposición de la ciudadanía. Estas iniciativas están teniendo una gran aceptación y una repercusión muy positiva en la opinión pública, que se traduce en una utilización cada vez más generalizada de la red.

Para responder debidamente a esta demanda, se hacía necesario aportar seguridad a las comunicaciones a través de Internet. Esta seguridad se expresa en términos de confidencialidad (sólo se muestran los datos o páginas al usuario autorizado a ello), integridad (nos aseguramos de que los mensajes intercambiados llegan a su destinatario sin modificaciones) no repudio (que el emisor o el receptor no se puede desdecir del propio mensaje).

Por cuanto antecede y como herramienta para alcanzar los objetivos anteriores (confidencialidad, integridad y no repudio), surgen los certificados electrónicos y la firma electrónica. Ambos son instrumentos capaces de garantizar la seguridad en las comunicaciones y la identidad de los usuarios, permitiendo la comprobación de la procedencia y asegurando la integridad de los mensajes intercambiados a través de la red.

Con ayuda de los certificados electrónicos se puede realizar la protección de la información mediante un cifrado o transformación criptográfica (ocultamiento o enmascaramiento de la información de forma que no sea legible sin realizar la operación inversa) de los mensajes, haciendo su contenido ilegible salvo para el destinatario. Con ayuda de los mismos certificados electrónicos y aplicando un algoritmo de firma electrónica, obtenemos de un texto, una secuencia de datos que permiten asegurar que el titular de ese certificado ha “firmado electrónicamente” el texto y que éste no ha sido modificado.

Las claves criptográficas (conjunto de datos o información manejada y gestionada por el usuario para realizar operaciones criptográficas) que posibilitan estas operaciones se generan en el momento de la solicitud del certificado y quedan unidas inequívocamente al titular de las mismas.

Todo lo anterior, se ve reforzado en Ecuador con una legislación de firma electrónica que permite ofrecer garantía y seguridad jurídica a las transacciones realizadas con los certificados electrónicos