Centro Sur Vol. 5 No. 3 – Julio Septiembre - Revista Centro Sur - eISSN: 2600-5743

http://centrosureditorial.com/index.php/revista

Aplicación e implicancias de la firma y certificados digitales en el marco de la ley 27269 - Perú

Application and Implications of the signature and digital certificates in the framework of Law 27269 - Peru

Gaby Jessica Nieto Fernández
Magister en Gestión Pública, Ministerio de Energía y Minas, Abogada, Universidad San Martín de Porres, gjnieto@gmail.com, https://orcid.org/0000-0003-0303-9915

Resumen

La presente investigación, busca identificar los beneficios de la aplicación e implicancias en el Perú de la Ley N° 27269 "Ley de Firmas y Certificados Digitales", modificada por Ley N° 27310 y de qué forma su aplicación ha contribuido en los avances de su optimización en el ámbito público y privado dentro del marco de instauración del gobierno electrónico en el Perú y a más de 19 años de su entrada en vigencia, el Reglamento de la Ley N° 27269, aprobado por Decreto Supremo N°052-2008-PCM, busca regular la utilización de las firmas digitales y el régimen de la infraestructura oficial de la firma electrónica, buscando diversos niveles de garantía y seguridad a fin de dar la misma eficacia jurídica y validez que se da a la firma manuscrita u otra análoga, sin embargo se han presentado inconvenientes para su aplicación, las mismas que analizaremos a fin de plantear posibles alternativas para un mejor control y mecanismo de seguridad.

https://doi.org/10.37955/cs.v5i3.165
Recibido Noviembre 12, 2020 / Aprobado abril, 03 2021 Páginas: 122-133
eISSN: 2600-5743

Abstract

This research seeks to identify the befits of the application and implications in Peru of Law No. 27269 "Law on Digital Signatures and Certificates", modified by Law No. 27310 and how its application has contributed to the progress of its optimization in the public and private sphere within the framework of the establishment of electronic government in Peru and more than 19 years after its entry into force, the Regulation of Law No. 27269, approved by Supreme Decree No. 052-2008-PCM, seeks to regulate the use of digital signatures and the regime of the official infrastructure of the electronic signature, looking for different levels of guarantee and security in order to give the same legal effectiveness and validity that is given to the handwritten or other similar signature, however there have been problems for its application, which we will analyze in order to propose possible alternatives for a better control and safety mechanism.

Palabras clave/ Keywords

Firma electrónica, Firmas digitales, Certificados Digitales, Gobierno Electrónico, niveles de seguridad

Electronic signature, Digital signatures, Digital Certificates, Electronic Government, Security levels

Introducción

En un mundo globalizado como el que vivimos actualmente, donde todas las operaciones comerciales se vienen realizando a través de mecanismos electrónicos, donde desde la comodidad del hogar o trabajo a través de un celular o computadora, puedes realizar compras, pagos y todo tipo de operaciones comerciales, situación que hace que los Países Latinoamericanos se preocupen por disminuir la brecha digital existente entre las empresas privadas y los gobiernos, por lo que entre dentro de sus políticas impulsan el avance de su agenda digital, a fin de poner la tecnología al servicio del ciudadano (Porrúa, 2019).

Las telecomunicaciones han crecido exponencialmente por la tecnología, dando mayor facilidad para realizar actividades diarias, tanto en las empresas como en casa (Torres y Oviedo, 2020; Govin, 2019, p. 4). Las TICs es parte esencial de la organización, genera y consigue efectos de productividad y sostenibilidad que mejoren la organización Duche, Gálvez, Marallano (2019). Actualmente, se está

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

en constante cambio gracias a la tecnología y a la globalización, por ello las TICs tienen un rol importante interviniendo en todos los sectores de la sociedad (Villao, 2016, p 43)

Sin embargo, según estudio publicado por el Banco Interamericano de Desarrollo en América Latina menos del 30% de los trámites pueden hacerse enteramente en línea y únicamente el 7% de los ciudadanos realizó en línea su último trámite, persistiendo la política del papel o el certificado. La marcha hacia un gobierno sigue en marcha, requiriendo el compromiso e inversión de los Países comprometidos con poner al alcance de los ciudadanos las bondades de la tecnología a fin de satisfacer sus necesidades (Porrúa, 2019).

El Perú, no ha sido ajeno a la implementación de políticas de gobierno digital, por la que entre otras promulgó la Ley N° 27269 "Ley de Firmas y Certificados Digitales", modificada por Ley N° 27310, norma que busca incorporar al reordenamiento jurídico peruano determinadas figuras jurídico informáticas para asegurar el resguardo de la información así como su transmisión por medio de elementos electrónicos mediante el uso de técnicas criptográficas. Cuando se trata de políticas públicas, implica "Estado en acción" por medio de las regulaciones del sistema político para la resolución de problemas públicos (Olivar, 2019). Para Salvador (2001), la firma digital se presenta como una necesidad por el sector privado y público, dando una solución para las políticas de seguridad en redes (p.52).

Asimismo, la citada norma busca señalar el marco regulatorio para la utilización de la firma electrónica, a la cual se le otorga la misma validez y eficacia jurídica del que goza la firma manuscrita o análoga, mediante las cuales las personas buscan manifestar indubitablemente una determinada voluntad.

Sin embargo todavía en el Perú no se ha implementado eficazmente la firma digital y Certificación digital, en las empresas públicas por falta de implementación de TICS, e infraestructura técnica digital, como software y hardware. En las entidades privadas la falta de implementación de mecanismos de control y seguridad no han viabilizado la implementación de la firma y certificación electrónica.

Estando a la Ley N° 27269, debemos tener presente que el medio electrónico es inseguro por naturaleza, para que se pueda lograr un adecuado nivel de seguridad dirigido a las personas que actúan en operaciones electrónicas, se requiere la utilización de una serie de herramientas técnicas, jurídicas y organizacionales que hagan viable el

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

proceso de intercambio de bienes y servicios en el mundo electrónico, espacio donde es fundamental identificar adecuadamente a las partes intervinientes en las diversas transacciones y operaciones que se presentan en dicho ámbito.

Sobre el particular siguiendo a Espinoza (2018) podemos señalar que:

> "En dicho contexto, Perú no puede ser ajeno a una realidad cuyos problemas legales se deben resolver desde el derecho informático, (…) con una visión informática, donde derecho y tecnología se unen para facilitar las operaciones electrónicas en entornos globalizados e interconectados. Es así que el sistema jurídico peruano se ha adaptado a las nuevas exigencias de los tiempos modernos. En concordancia con los avances del derecho informático, ha regulado en diversos cuerpos normativos tanto las firmas electrónicas como las firmas digitales". (p.242)

Al respecto debe tenerse en cuenta, siguiendo los parámetros establecidos por Espinoza (2018), que:

> "El Derecho Informático nos plantea una serie de instituciones que [facilitan] el desarrollo de mecanismos de prevención de todas aquellas situaciones no deseadas para los usuarios de las Nuevas Tecnologías de la Información, de tal forma que cuando se presentan determinadas circunstancias de afectación existen nuevas instituciones jurídicas que generan confianza a las personas [como a las entidades públicas y privadas] que realizan operaciones por medios electrónicos (…). (p. 293).

En ese sentido, Flores (2014), (Gamboa et al., 2019), define al Derecho Informático como una rama del derecho "(…) de carácter multidisciplinario, consistente en el conjunto de normas jurídicas que tienen como objeto regular relaciones y actos jurídicos surgidos en torno a la informática y el uso de los medios informáticos (…)." (p. xvi), al respecto debemos tener en cuenta que la definición planteada requiere ser complementada con aspectos relativos a la doctrina, jurisprudencia e investigación jurídica.

Es importante resaltar que el Derecho Informático es la nueva rama del Derecho que permite dar solución adecuada a los problemas generados por el uso de las Tecnologías de la Información y las Comunicaciones –TICs, por lo tanto, es la llamada a estudiar, analizar y procurar respuestas a la problemática cada vez más creciente en

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

relación con el nivel de uso de las Firmas Electrónicas en general y las Firmas Digitales en particular.

Debe tenerse en cuenta diversas herramientas técnicas, destacando aquellas que pueden ser configuradas tanto a nivel del hardware como del software. En cuanto al primer aspecto se requiere de un servidor que soporte los certificados digitales y el par de claves (clave pública y clave privada); además deberá configurarse dichos elementos al nivel que permitan la interacción web con las entidades de certificación y registro.

A nivel del hardware también es fundamental el uso de los Token USB criptográfico con sus respectivos conectores y puertos USB, que permitan el almacenamiento de los certificados electrónicos, el sistema de claves o llaves, todo ello dirigido para ser aplicado por los usuarios del sistema. Los dispositivos antes referidos deben tener una determinada capacidad de memoria, debiendo soportar los sistemas operativos que las partes requieran, debiendo tener algún nivel de recubrimiento que permita su aislamiento, garantizando posibles contingencias que pudieran suscitarse. Se requiere analizar siempre los aspectos jurídicos del hardware, en vista que en todo momento, para interactuar con las firmas y certificados digitales se debe interactuar en tanto en el mercado físico como en el mercado digital.

En cuanto al software es necesario en primer lugar que esté acreditado por INDECOPI, como entidad que regula y verifica los sistemas de Firmas y Certificados Digitales. El elemento inmaterial debe contar con su respectiva licencia de uso de software, que permita que los usuarios sean lícitos evitándose de esta forma posible sanciones por piratería de software, con las consecuencias legales de tales hechos.

En toda operación electrónica es de vital importancia determinar la identidad del titular de la firma digital. En dicho contexto es fundamental lo previsto por el Artículo 4° de la Ley 27269, al señalar que " El titular de la firma digital es la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos.

En el medio electrónico es fundamental determinar la identidad de la persona a la cual se le asignará el certificado digital, entendido este último, como aquel documento electrónico que presenta todos los elementos necesarios que permitan identificar plenamente al titular del sistema de firma digital.

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

Las entidades de verificación o registro juegan un rol muy importante, ya que son las llamadas a cumplir a cabalidad dichas funciones, de no realizar adecuadamente su labor de identificación se pueden generar graves problemas al sistema de firmas y certificados digitales, sobre todo a nivel de pérdida de confianza, lo que correspondería una externalidad negativa para el desarrollo de las operaciones electrónicas.

En tal sentido, el certificado digital es firmado por la entidad de certificación, y vincula al firmante con cada operación electrónica que proceda a firmar.

La responsabilidad por el firmado de operaciones electrónicas, es fundamental tener en cuente que el Artículo 5 de la Ley 27269, señala expresamente las obligaciones del titular de la firma digital, al respecto plantea que "El titular de la firma digital tiene la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione a través de la utilización de la firma digital, declaraciones o manifestaciones materiales exactas y completas".

Las firmas digitales y la certificación digital se desarrollan en un contexto muy sensible, por donde circulan datos personales, información de obligaciones y contratos, etc., entonces, por la propia inseguridad del medio electrónico es obligación fundamental del titular de la firma digital brindar declaraciones o manifestaciones de voluntad totalmente exactas, para evitar cualquier vulneración al sistema de firmado digital, y evitar de esta forma cualquier tipo de inseguridad a las operaciones electrónicas en general en la que confían las partes que intervienen en dicho contexto (Ovidio, 2006).

Es necesario resaltar que el titular del certificado digital se hará responsable del uso del par de claves, a saber, una clave pública y una clave privada, ambas generadas en el contexto de un sistema de criptografía asimétrica, es decir, de aquella ciencia del cifrado que permite dar altos niveles de seguridad a las operaciones electrónicas.

La Ley de Firmas y Certificados Digitales, desde el año 2000 señaló la conceptualización del certificado digital, en tal sentido, conforme lo previsto en el Artículo 6 de la Ley 27269, se define al certificado digital como "(…) el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad."

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

Se debe tener en cuenta que para la generación del certificado digital participa una entidad de certificación que haya acreditado fehacientemente la identidad del titular del certificado digital, dicho proceso lo puede hacer directamente la entidad de certificación cuando tiene funciones de entidad de registro, sino las tienen debe delegar dicha función a una entidad de registro, institución que en última instancia tiene la obligación de determinar claramente la identidad del titular del certificado digital, a quien se le atribuirá el par de claves, para efectos del firmado.

El titular del certificado digital se hará responsable del uso del par de claves, a saber, una clave pública y una clave privada, ambas generadas en el contexto de un sistema de criptografía asimétrica, es decir, de aquella ciencia del cifrado que permite dar altos niveles de seguridad a las operaciones electrónicas.

En el ámbito de lo previsto por la Ley 27269, es importante tener en cuenta que los certificados digitales son emitidos por las entidades de certificación y no por las de registro; el Artículo 7° de la acotada norma, la misma que nos informa sobre el contenido del certificado digital, en los términos siguientes:

Los certificados digitales emitidos por las entidades de certificación deben contener al menos:

1. Datos que identifiquen indubitablemente al suscriptor.
2. Datos que identifiquen a la Entidad de Certificación.
3. La clave pública.
4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos.
5. Número de serie del certificado.
6. Vigencia del certificado.
7. Firma digital de la Entidad de Certificación

También es fundamental tener en cuenta los datos que identifiquen a la entidad de certificación, en vista que depende de aquella entidad la emisión del certificado digital y la generación del sistema de firma digitales, tanto a nivel de hardware como de software.

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

El sistema jurídico peruano exige que en el certificado digital se incorpore la clave pública, debiendo entenderse que se refiere a los mecanismos de validación de la misma y las forma de acceder en el medio electrónico, para efectos de su reconocimiento, siempre en un contexto de autenticación técnica

En relación con el marco jurídico se requieren instrumentos legales con rango de Ley que otorgue valor a tales operaciones, asimismo, se requiere de un adecuado marco legal que otorgue el sustento jurídico que permita a los usuarios otorgue el sustento jurídico que permita a los usuarios de entornos virtuales tener el marco de referencia idóneo para su interacción permanente en el mundo electrónico.

En el Perú se ha dado la Ley N° 30096 “Ley de delitos Informáticos”, la misma que tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia (Dávila, 2020).

En este caso se protege un bien jurídico como: la confidencialidad, integridad y disponibilidad de la información. El empleo de las nuevas tecnologías genera progreso, sin embargo, cuando se usa para fines ilícitos, como acceder a información privada con la intención de causar daño, solo causa perjuicio económico.

En el Perú los delitos informáticos más comunes son: el fraude, hacking propagación maliciosa de un virus, suplantar la identidad, terrorismo, pornografía infantil, el envío de correo electrónicos para obtener datos pishing (obtener información privada como claves de cuentas bancarias y correos electrónicos), espionaje a fin de captar la información de una empresa, clonación de tarjetas, obtención de información personal y empresarial, fraudes bancarios, extorsión online, robo de datos de propiedad intelectual, ataques a los proveedores de internet, entre otros.

En la mayoría de los delitos informáticos, el delincuente cibernético, es la persona que tiene conocimientos informáticos y de sistemas lo que le permitiría acceder sin autorización a terminales públicas o privadas (acceso ilícito), quebrando o transgrediendo todos los sistemas de seguridad (Rodas y Loor, 2017).

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

En los delitos informáticos, el fin es impedir el acceso e imposibilitar el funcionamiento del sistema, este es el principal propósito y debe existir dolo (conocimiento y voluntad de ejecutar el delito). En los delitos informáticos se va a valorar el daño y en este caso se sanciona el uso indebido de las tecnologías de la información (Vela, 2020).

Materiales y Métodos

Esta investigación usó el método inductivo, por medio de un proceso analítico-sistemático; se utilizó la observación y revisión documentaria para la aplicabilidad e implicancias de la firma y certificados digitales en el marco de la Ley 27269, en el Perú.

Las revisiones bibliográficas se realizaron de manera exhaustiva utilizando el proceso inductivo, porque se toma de referencia las disposiciones del estado peruano con respecto a la modernización del estado mediante el uso de herramientas electrónicas en la gestión pública peruana, y se llegan a las conclusiones.

Resultados

Desde la dación de la Ley N° 27269 "Ley de Firmas y Certificados Digitales", modificada por Ley N° 27310, se ha visto que se vienen implementando políticas de seguridad y control de las mismas, la misma que se ve protegida por la Ley de Delitos Informáticos.

El Estado, viene implementando políticas a fin de dar avances significativos dentro de la aplicación del gobierno digital, con la Ley de Firma y Certificados Digitales, con lo que se incorporan al ordenamiento jurídico peruano figuras jurídicas informáticas para asegurar el resguardo de información así como su transmisión por medio de elementos electrónicos mediante uso de técnicas criptográficas.

El certificado digital debe contener todos aquellos datos del titular del sistema de firmado digital, pero la condición esencial es que no exista duda sobre la identidad del titular, siendo esa la razón por la cual la exigencia legal se vincula con una identificación indubitable del suscriptor.

En la presente investigación se observa que con la aplicación de la Ley 27269, se presentan avances significativos para los procesos que

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

requieren de firmas y certificados, impulsa el ordenamiento jurídico peruano y asegura la protección de la información; como también, su transmisión por medio de elementos electrónicos mediante uso de técnicas criptográficas. Así también, Arcetales y Gamboa (2019), afirman en su investigación que las nuevas tecnologías son relevantes para la mejora de la gestión pública, las TICs determinan un mayor valor público.

El empleo de las TICs en el gobierno logra una eficiencia y eficacia en los programas, mejorando el acceso y difusión de los mismos a la comunidad, empresas y organizaciones. Así también, Fernández (2001), en su investigación "La ley de firma digital Argentina", señala que es importante el uso de la firma digital para viabilizar procedimientos y también la aplicación de las sanciones que implican su regulación.

Conclusiones

Con el avance de la Tecnología, también se da el aumento de la criminalidad informática en el Perú y a nivel mundial, lo que trae consigo consecuencias económicas y numerosos fraudes cometidos por organizaciones delictivas que muchas veces no son denunciados o cuyos delitos son cometidos en el exterior sin que muchas veces exista una sanción, se pretende dar un avance en el gobierno electrónico, a través de la Implementación de la firma y Certificados Digitales, las mismas que permitirán que ciertos procedimientos sean más rápidos y eficaces.

Por tratarse de un contexto de seguridad informática, es fundamental que la entidad de certificación cuente con los mecanismos y criterios adecuados para una correcta acreditación de la metodología para verificar la firma digital del suscriptor. El Estado, debe invertir en Tecnología moderna a través de adquisición de software y hardware que permitan la implementación de los sistemas con mayor seguridad, lo que permitirá la confianza de la ciudanía en el uso de la firma digital.

Referencias

Dávila, W. (2020). Delitos informáticos Perú. Blog Resultado legal [12 de octubre del 2020]. http://resultadolegal.com/%EF%BB%BFdelitos-informaticos-peru/

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

Duche, A., Gálvez, P. y Marallano, P. (2019). La tecnología de la información y comunicación en la aplicación de estrategias para la gestión de la cadena de suministro en el ámbito empresarial: una revisión sistemática de la literatura. Centro Sur social science journal. 4(2). http://www.centrosureditorial.com/index.php/revista/article/view/86/241

Espinoza, J. (2018). Entre la firma electrónica y la firma digital: aproximaciones sobre su regulación en el Perú. *Revista del Instituto de Ciencias Jurídicas de Puebla*. 12 (41). https://www.revistaius.com/index.php/ius/article/view/315/601

Flores, L. (2014). *Derecho Informático*. Grupo Editorial Patria. 1er Ed. https://editorialpatria.com.mx/mobile/pdffiles/9786074380637.pdf

Gamboa, M., Barros, L., & Barros, C. (2019). Childhood Aggressiveness, Learning and Self-Regulation in Primary Students. *Luz. Revista Electrónica Trimestral de La Universidad de Holguín*, *53*(9), 1689–1699. https://luz.uho.edu.cu/index.php/luz/article/view/743/637

Govin, P. (2019). Tendencias de seguridad y vulnerabilidades en sistemas basados en la nube para procesos educativos. *Formación docente -revista iberoamericana de educación*. 2(3). http://www.revista-iberoamericana.org/index.php/es/article/view/25

Olivar, A. (2019) Políticas públicas, enfoque diferencial y epistemologías de coloniales: una vuelta de tuerca en la reivindicación de derechos de grupos minoritarios. *Centro Sur,* 3(1). http://www.centrosureditorial.com/index.php/revista/article/view/23/44.

Ovidio, J. (2006). Contratación Electrónica. *THĒMIS-Revista De Derecho*. (44), 253-269. http://revistas.pucp.edu.pe/index.php/themis/article/view/10075

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743

Porrúa, M. (2019). La Agenda Digital en América Latina: Un avance a distintas velocidades. Banco Interamericano de Desarrollo. [12 de octubre del 2020]. https://blogs.iadb.org/administracion-publica/es/la-agenda-de-gobierno-digital-en-america-latina/

Rodas, P. y Loor, E. (2017). Proceso de formación en tipificación en el código orgánico integral penal para los delitos cibernéticos. *Formación docente -revista iberoamericana de educación*. 1 (1). 42-79. http://www.revista-iberoamericana.org/index.php/es/article/view/4/pdf

Salvador, I. (2001). La firma digital: una tecnología para la intercomunicación en la Sociedad - RED. *Revista Española de Educación Científica*. 24(1). http://redc.revistas.csic.es/index.php/redc/article/view/33

Torres, Á. y Oviedo, B. (2020). Uso de las técnicas de la información y comunicación y su incidencia en el control de acceso. *Journal of business and entrepreneurial studies,* 4 (1). http://journalbusinesses.com/index.php/revista/article/view/66/181

Vela, N. (2020). Análisis de la falsificación de documentos y protección del bien jurídico en materia penal. *Journal of business and entrepreneurial studies*. 4(1). http://journalbusinesses.com/index.php/revista/article/view/26/59

Villao, D. (2016) Herramientas digitales en el aprendizaje de una segunda lengua. Sinergias educativas, vol. 1(2), Grupo Compás, Ecuador. http://www.redalyc.org/articulo.oa?id=573563368006.

Recibido Enero 12, 2021 / Aprobado mayo, 03 2021 Páginas: 122-133
eISSN: 2600-5743