Experiencia Profesional III

Profesor: Lic. Luis Mora Lizano

Obsolescencias del Notariado por el uso de la Firma Digital

Elaborado por: Manrique Pacheco Fischel

III Cuatrimestre 2022

Índice

Resumen

La implementación de las nuevas tecnologías en las diferentes disciplinas del notariado ha hecho posible que se busque complacer a los usuarios de productos notariales, con la posibilidad de tener acceso a dichos servicios las 24 horas y los 7 días de la semana. Con todo y lo que esta innovación ofrece, no deja de representar un alto riesgo de fraude, debido a la posibilidad de no poder autenticar en el mundo digital, ni la verdadera identidad de los participantes en el pacto, ni las verdaderas y auténticas intenciones y voluntades. Existen muchos intentos de garantizar estos elementos, sin embargo, sigue siendo un riesgo el que un servidor falle y no se pueda recuperar la información en él contenida. Este artículo trata estos elementos y ofrece importantes aportes, a tomar en cuenta, para poder identificar los avances que se han logrado y las lagunas y amenazas que todavía existen en cuanto a la legitimidad y autenticidad de los documentos digitales.

Palabras clave: Protocolo digital, firma digital, notariado digital, seguridad de documentos, autenticación digital, preservación de documentos y bibliotecas digitales, recuperación de información digital.

Abstract

The implementation of new technologies in the different disciplines of notaries have made it possible to seek to please users of notarial products with the possibility of having access to said services 24 hours a day, 7 days a week. Likewise, what this innovation offers is important, yet, it does not stop representing a high risk of fraud, due to the possibility of or being able to authenticate in the digital world, neither the true identity of the participants in the pact, nor the true and authentic intentions and wills. There are many attempts to guarantee these elements, however, it is still a risk that a server fails, and the information contained therein cannot be recovered. This article deals with these elements and offers important contributions to take into account in order to identify the progress that has been made and the gaps and threats that still exist in terms of the legitimacy and authenticity of digital documents.

Key words: Digital protocol, digital signature, digital notary, document security, digital authentication, document preservation and digital libraries, digital information retrieval.

Introducción

En medio de la era tecnológica, con la rápida evolución de las computadoras, los celulares, las tabletas y con la posibilidad de mantener una continua conexión a Internet, se hace necesario que todas las disciplinas profesionales busquen la protección de la información y la prevención de los delitos cibernéticos. A partir de esta necesidad de protección de usuarios, contraseñas, información y autorías nace el Derecho Informático. Con esta iniciativa se ha buscado paliar estas vulnerabilidades y se tipificaron actividades ilícitas realizadas por medio de dispositivos electrónicos.

Entre muchos, se ha destacado el jurista español Dr. Emilio Suñé Ilinas, quien ha planteado proyectos para convertir el ciberespacio en una nación cibernética sin límites:

> El Derecho de la informática, por seguir aportando razones singulares que avalan su autonomía, tiene mucho de Derecho Global, al tratarse de un Derecho muy internacionalizado, probablemente por el tipo de comunidades humanas que están en su base. La regulación jurídica de Internet, por ejemplo, plantea problemas globales, que requieren soluciones globales. Las grandes multinacionales del sector tele informático, que lo dominan casi todo por completo, no pueden -ni quieren- adaptarse a regulaciones estatales injustificadamente diversas y dispersas, cuando el mercado no es nacional, sino global (Suñé, 2000, p. 7).

Desde el Derecho pudiera pensarse que se logra contar con un adecuado nivel de protección, con la encriptación, teniendo en cuenta que la mayor de las veces la comprensión del tema tecnológico es poca. Sin embargo, la encriptación es un mecanismo para otorgar a la información atributos de confidencialidad, integridad, autenticidad y, dependiendo del mecanismo utilizado, podría objetarse el no repudio. Las bondades de los sistemas de información, por ejemplo, al procesar información económica de las empresas, permiten predecir los riesgos financieros de estas, con una precisión tal que podría incluso diagnosticarse, en términos de tiempo, la fecha en la que un ente empresarial puede estar en situación de insolvencia o iliquidez. En la protección de la información intervienen diferentes disciplinas, desde la informática, la gerencial, la logística, la matemática y hasta la jurídica, entre muchas otras.

En la medida en que se trata de terceras personas con acceso a las redes, sistemas informáticos, infraestructura e información estratégica de la compañía, se debe tener presente que estos terceros deben asumir una serie de obligaciones, cargas y deberes, al interactuar con la organización, así como los riesgos y las responsabilidades que conlleva el indebido tratamiento de la información para el titular de tales activos. Sin esta concepción holística del tema es frágil cualquier sistema de gestión de la seguridad de la información.

Hoy día, el Derecho es un invitado importante en la gestión de la información. En este sentido, es la herramienta ideal para aportar una serie de recomendaciones y controles jurídicos, en ocasiones matizados por la tecnología, para la gestión adecuada de aquellos activos tangibles e intangibles que involucren información relevante y valiosa para una organización, sea esta pública o privada.

Cambiar la perspectiva del problema de la seguridad de la información que pueden tener los responsables de esta en las organizaciones no es una tarea fácil; para ello es importante acudir a criterios objetivos que demuestren la importancia que tiene el Derecho en esta problemática, y acreditar cómo el tema, por ejemplo, de los incidentes informáticos puede tener una vocación judicial, siempre y cuando las evidencias de estos hayan sido adecuadamente recabadas.

Es en este contexto en el que Cano (2007), expone un punto importante, cuando afirma que:

> […] la gestión de la seguridad de la información debe ser revisada (¿complementada?) para no solamente cubrir las fallas de seguridad, sino para comprender la manera estructural y sistemática las tensiones entre los elementos que componen el sistema de gestión de la seguridad. En este sentido, consecuente con las tendencias internacionales y la realidad de un mundo global, la seguridad de la información se convierte en un elemento activo y estratégico para las empresas del siglo XXI (p. 3).

Con base en lo anterior, se puede inferir que la seguridad de la información es un factor crítico para que exista confiabilidad, disposición y certeza de que la inversión por realizar en algún proyecto esté respaldada, lo cual garantiza que los datos sensibles de los usuarios y de las empresas no serán *hackeados* por terceros.

En este artículo, se explorarán los antecedentes de la seguridad de la información, se definirán conceptos importantes como el notariado, las funciones del notario, la firma digital y sus ventajas y

desventajas, y se abordará el tema sobre las dificultades legales y prácticas para la implementación del Protocolo Digital en tiempo real. De igual manera, se desarrollará el tema de si en un documento firmado digitalmente, donde se da fe de sus firmantes, es necesaria la participación de un Notario que sea abogado, o sea, que al optar por la función de protocolo digital se estaría liberando la función notarial y permitiendo que profesionales de otras disciplinas se certifiquen en notariado, dejando de ser esta función exclusiva de los abogados.

Marco Teórico

Antecedentes

Cuando se plantea el tema de la seguridad de la información, se debe tomar en cuenta el aspecto de la dualidad de la inseguridad informática. Para ello se debe considerar qué controles y modelo de riesgos se deben implementar para garantizar que los posibles ataques cibernéticos no penetren en la organización.

Siendo así, la inseguridad informática es una disciplina dual donde los académicos y practicantes de la industria buscan las maneras detalladas para que ocurran eventos inesperados, establecer las condiciones extremas de funcionamiento de los dispositivos o de las estrategias, todo con el fin de hacer caminar en condiciones límite la operación de la organización y sus negocios. Se formulan preguntas clave como:

- ¿Cómo funciona el sistema?
- ¿Cómo reacciona ante una falla?
- ¿Cómo hacerlo fallar?

Por tanto, la inseguridad informática, como disciplina dual en el estudio de la seguridad informática, establece un paradigma complementario (es decir, dual a la seguridad informática) que comprende las propiedades emergentes de los sistemas (analizados) desde condiciones y realidades extremas, las cuales no son viables en una estrategia de protección causal (dualismo) sugerida por la seguridad informática actual. Se requiere que la funcionalidad del producto o sistema sea explorada de una manera metódica y que los resultados de las pruebas, sean positivos o negativos, puedan ser analizados en contexto y así ofrecer un concepto formal de este. En este contexto, las relaciones causales deben ser determinadas y concretadas, de tal manera que sea posible detallar y sustentar los posibles estados exhibidos por el sistema, al ser sometido a las pruebas de comportamiento sugeridas dentro del dominio de la definición del producto mismo.

Normativa de la Certificación Notarial

Según la normativa vigente en Costa Rica, para ser notario se debe haber cursado la carrera completa de Derecho y contar con un diploma que hace constar que se graduó en dicha especialidad.

Los notarios son funcionarios públicos del Estado, obligados a proporcionar seguridad jurídica a sus clientes. Por tal motivo, la certificación que los notarios emiten son documentos extendidos bajo su responsabilidad, mediante los cuales certifica o da fe del contenido de las escrituras matrices, inscripciones o documentos existentes en Registros y oficinas públicas, incluso, piezas de expedientes, libros, documentos y atestados, particulares o privados, sin necesidad de dejar razón o de levantar acta en el protocolo. Debe hacerse constar si es literal, en lo conducente o en relación.

La función notarial

El Instituto Guatemalteco de Derecho Notarial ha desarrollado una clara y concisa definición de la función notarial, y establece que se fundamenta en:

> "Una serie de principios éticos que aluden a criterios de imparcialidad, independencia, a la formación y capacitación permanente profesional, a las relaciones recíprocamente respetuosas con los colegas y con las organizaciones profesionales, a la lealtad con la competencia, a la indelegable intervención personal del notario en los actos que autoriza, al secreto profesional, al deber de asesoramiento y, por supuesto, a la diligencia y responsabilidad del notario." (par. 2). En sí, se puede definir que el "ejercicio del notariado es una función noble que se realiza con estricto apego a los postulados éticos y a las normas legales, ya que los notarios con su actuar contribuyen a la paz y al desarrollo económico y social de los países, y a fortalecer la seguridad jurídica en las sociedades (par. 1)

Partiendo de dicha definición, se considera que el Notario tiene una función pública, dentro de la cual debe:

> Recibir, interpretar y dar forma legal a la voluntad de las partes, redactando los instrumentos adecuados a ese fin, confiriéndoles autenticidad, conservando los originales de éstos y expidiendo copias que den fe de su contenido. Pero la función del notario no termina con la redacción del

instrumento público, pues el mismo tiene que cumplir con las obligaciones posteriores a la redacción del instrumento público (Salas, 1973, pp 60-61).

Ahora bien, entre las funciones notariales más comunes están:

a. Función receptiva: Muñoz (1992) considera que hay que tomar en consideración que muchas veces el compareciente no sabe realmente el documento notarial que pretende realizar, es por eso que se considera a esta función como la más importante, puesto que, si son mal interpretadas las palabras del compareciente o no es entendida con claridad su intención, el instrumento notarial que se realice pudiera terminar en un rotundo fracaso (p. 39).

b. Función directiva o asesora: Muñoz (2007), menciona que dicha función se realiza después de escuchar al cliente, y se da cuando el notario, como profesional en Derecho versado en la materia, aconseja al cliente sobre el documento o instrumento que debe redactarse (p. 40).

c. Función legitimadora: el notario asegura que los comparecientes son lo que dicen ser y por tanto debe verificar los documentos de identidad que corresponda (p. 41).

d. Función modeladora: Esta función, parafraseando a Muñoz (2007), consiste en la preparación mental que el notario realiza, al adecuar la voluntad de los comparecientes con lo que establece la normativa jurídica, en relación con el negocio jurídico a celebrar (p. 42).

e. Función preventiva: En esta función, de acuerdo con Muñoz (2007), el notario debe prevenir a los comparecientes cualquier problema que pueda resultar posterior a la realización del negocio jurídico, evitando posibles conflictos (p. 43).

f. Función autenticadora: Como menciona Muñoz (2007) “por tener fe pública, al estampar su firma y sello, el notario le está dando autenticidad al instrumento elaborado, lo autoriza, se convierte en el autor del documento” (p. 43), establece que el notario debe indicar la “advertencia a los otorgantes de los efectos legales del acto o contrato y de que deben presentar el testimonio a los registros respectivos” (p. 43).

g. Función receptiva: Para Muñoz (2007), esta función la realiza el notario al escuchar al cliente, quien en palabras sencillas le transmite al notario para qué lo requiere. Con esta función el notario se asegura de que las personas que requieren su servicio son las que dicen ser, verificando la identidad de las mismas por medio del documento personal de identificación, o por medio de dos testigos que el notario conozca. En el momento en que el notario firma y sella el instrumento público, el mismo es dotado de autenticidad, por tanto es cierto y produce seguridad jurídica y efectos. Esta función la realiza el notario al momento de firmar el instrumento público que elaboró dando forma a la voluntad de los comparecientes con la legislación jurídica vigente (p. 39)

Objetivo general

Esclarecer las dificultades legales y prácticas para la implementación del Protocolo Digital en tiempo real.

Objetivos específicos

1. Definir las ventajas y desventajas del uso de la firma digital.
2. Definir la necesidad real de un notario, ante el incremento del uso de la firma digital.

Desarrollo

El documento notarial

La labor documentadora es uno de los aspectos propios de la función notarial, principalmente por su efecto fedatario público, y cuyo fin es la gestación de un documento público notarial. Muchos autores piensan que el documento, como tal, creó al notario, pese a que hoy es el notario quien redacta el documento.

El documento notarial como representación

Según Pelosi (1997), el vocablo “documento” es todo aquello que permite enseñar cualquier cosa y es en sí mismo el medio para conocer cualquier cosa que se halle fuera del documento. Es en este concepto en donde reside el carácter de representatividad del documento, y es este aspecto, en particular, el que ha logrado trascender históricamente en el derecho notarial. Siendo así que el documento como tal da fe en el presente y, a la vez, sirve de memoria de ciertas cosas en el futuro.

El documento como forma y como prueba

Al analizar el “documento”, desde el punto de vista de su forma, se está refiriendo, en lo que amerita al derecho romanista en nuestro país, a la protección de la voluntad de los particulares como la fuente primaria para la creación de relaciones jurídicas en el orden del derecho privado. Por decirlo de otro modo, el “documento” es el plano físico en el cual se plasma la voluntad jurídica de los particulares, la cual se representa por medio de palabras, texto, gestos, entre otros.

Visto de este modo, es esta voluntad plasmada en texto y asentida entre particulares ante un notario, quien da fe de la existencia de esta relación, voluntad expresa o intención, la que hace que este “documento” se constituya a la vez como prueba; y es la conservación de este documento probatorio, lo que hace que estos acuerdos, negocios o voluntades externadas ante el notario, se conviertan en formas escritas que se conservan y perduran en el tiempo y que se revelan con un carácter de superioridad indudable.

El documento digital

La materialidad del documento se constituye en sí misma como “cosa”, y lo mismo le sucede a la grafía que en este se incorpora, siendo esta la característica principal del documento digital, que es la materialización de una serie de datos y códigos binarios registrados en un dispositivo de almacenamiento de datos o en el disco duro de una computadora.

En este tema hay que reconocer dos aspectos importantes, que se ven afectados con la digitalización del documento, a saber: que el documento digital pierde mucha relevancia en su principio de materialidad que como “cosa” es. El segundo aspecto está relacionado con el documento notarial y la tarea intelectual que representa la aplicación del protocolo digital, por lo que hay que identificar en qué método de almacenamiento se puede conservar el documento, para que no exista peligro de que se pierda esta prueba de la voluntad entre particulares.

Inmaterialidad del documento notarial digital

El documento digital se crea en una computadora y se localiza en alguna parte del disco duro de esa computadora, ordenador o servidor. El documento se localiza, se envía, se manipula y se recibe en una computadora; por tanto, está sujeto a actualización de software, caducidad, así como al soporte de los equipos de tecnología de la información, quienes por sus derechos como administradores de los equipos pueden encontrar maneras de alterar documentos y de conservar las firmas digitalizadas originales.

A este respecto, Madridejos (2007), ha logrado definir apropiadamente los riesgos que existen al digitalizar los documentos; al respecto afirma que:

> […] cuando vemos en la pantalla del ordenador un texto escrito con el sistema alfabético lo que se está produciendo es una especie de traducción simultánea, absolutamente volátil, de un texto creado y almacenado en el sistema binario. Los signos que vemos en la pantalla, reconocibles como signos de escritura, no existen en la realidad natural, sino tan sólo en el mundo de la llamada realidad virtual; carecen de entidad material[…].
>
> Continúa más adelante: […] Lo que vemos en la pantalla del ordenador no es lo que está almacenado en nuestro disco duro sino su exteriorización fugaz mediante un proceso instantáneo de descodificación al lenguaje alfabético del sistema binario (p. 37).

La firma digital

La Ley de Certificados, Firmas Digitales y Documentos Electrónicos, No. 8454, del 30 de agosto del 2005, confirió el fundamento jurídico para la emisión y el uso de Certificados de Firma Digital en Costa Rica, otorgándole a esta y a los documentos electrónicos la equivalencia jurídica y la misma fuerza probatoria que la de la firma manuscrita y los documentos físicos. Ambas autoridades certificadoras pertenecen a la Jerarquía Nacional de Certificadores Registrados y están debidamente inscritas y autorizadas, para su operación, por la Dirección de Certificadores de Firma Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), ente responsable de la administración y supervisión del sistema nacional de certificación digital.

Se le otorgó a la banca estatal y privada la misión de procesar las solicitudes de personas físicas y jurídicas, para cumplir con la normativa de Tributación Directa de gestionar de manera digital los reportes y las declaraciones de impuestos de las sociedades anónimas en el país.

Ventajas y desventajas de las firmas electrónicas

Es cierto que las firmas electrónicas son un fenómeno relativamente nuevo, pero ya presente en el tiempo idóneo para poder contrastar sus incuestionables ventajas, entre las cuales se destaca que al utilizarlas se ahorra tiempo y costes de los trámites que se realizan.

Además, las firmas digitales cuentan con tres elementos importantes que son: la autentificación que ofrecen equivale a la firma física del documento, la integridad de los documentos impide que éstos puedan ser editados o modificados y, por último, están libres de repudio de origen, ya que quien la envió no puede negar haber remitido el mensaje o realizado la transacción.

Otro aspecto importante es que los costos de su implementación pueden recuperarse cuanto más se utilice la firma. Los peritos calígrafos trabajan con las firmas electrónicas de forma habitual, por lo que se reduce el consumo de papel y la contaminación producida por los desplazamientos. La automatización de todo el proceso es una garantía de que no se van a producir fallos, que son relativamente habituales con los procesos manuales, y que se incrementan cuantas más personas intervengan. Quienes utilizan las firmas electrónicas dan muestra de que están actualizados, que se han incorporado al ritmo de los nuevos tiempos.

A su vez, se facilita la autentificación, un punto que valoramos especialmente desde nuestra profesión, pero que también afecta positivamente a todos. Es lógico, si se tiene en cuenta que uno de los ámbitos donde más se han implantado es en el de los negocios y en el empresarial, campos en los que se suelen propiciar conflictos que requieren de esta.

Además de lo anterior, la firma electrónica es ecológica, sin embargo, tienen algún aspecto controvertido o mejorable. Las firmas pueden ser *hackeadas* o utilizadas por un tercero, quien puede completar trámites ilegales por medio de la usurpación de identidad.

Un aspecto importante a tomar en cuenta es que se debe asegurar de que los certificados han sido otorgados por un organismo confiable y de que las claves están convenientemente guardadas, no disponibles para cualquiera.

¿En qué se pueden utilizar las firmas digitales?

El artículo 5 de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, N° 8454, indica que la firma digital es válida para lo siguiente:

a) La formación, formalización y ejecución de los contratos.

b) El señalamiento para notificaciones conforme a la Ley de notificaciones judiciales.

c) La tramitación, gestión y conservación de expedientes judiciales y administrativos; asimismo, la recepción, práctica y conservación de prueba, incluida la recibida por archivos y medios electrónicos. De igual manera, los órganos jurisdiccionales que requieran la actualización de certificaciones y, en general, de otras piezas, podrán proceder sobre simples impresiones de los documentos en línea efectuadas por el despacho o aceptar las impresiones de dichos documentos en línea, aportadas por la parte interesada y certificadas notarialmente.

d) La emisión de certificaciones, constancias y otros documentos.

e) La presentación, tramitación e inscripción de documentos en el Registro Nacional.

f) La gestión, conservación y utilización, en general, de protocolos notariales (Cap. II).

Por su parte, no se podrá aplicar la firma digital en los siguientes casos:

a) Los actos o negocios en los que, por mandato legal, la fijación física resulte consustancial.

b) Las disposiciones por causa de muerte.

c) Los actos y convenios relativos al Derecho de familia.

d) Los actos personalísimos en general (Cap. II).

De lo anterior se puede destacar que el rango de aplicación de la firma digital se deriva por la misma ley, por lo que la firma se aplicará en aquellas situaciones en las que la ley expresamente así lo permita.

Por otro lado, se hace necesario destacar que, para firmar un documento con la firma digital, se requiere de un certificado digital emitido por una Autoridad Certificadora Registrada, y el cual debe ser almacenado y custodiado en un dispositivo (Token o tarjetas inteligentes -smart cards-) que cumpla con el estándar FIPS 140 nivel 2. Este dispositivo es muy importante, ya que es el responsable de custodiar un secreto único (llave privada), que es utilizado para firmar digitalmente los documentos o archivos.

Conclusiones y Recomendaciones

Conclusiones

El notario debe fomentar la implantación de los sistemas de otorgamiento y la autorización de las escrituras matrices u originales en soporte electrónico, siempre presencialmente, ante sí mismo como notario, como alternativa al otorgamiento en soporte papel y, en un futuro, como sustitución de este.

Sin embargo, una firma electrónica de los otorgantes que se ingresa a un sistema a distancia y sin la presencia del notario en el proceso, pone en riesgo la certeza de que se apersonaron, teniendo al notario en inmediación, ya que este proceso no permite la adecuada identificación de la identidad de cada interesado, ni da fe de la información de consentimiento, ni se puede garantizar que quien haga uso de la firma digital sea su propietario y no un impostor. Estos factores, aislados o en conjunto, rompen la cadena de autenticidad.

En Costa Rica, se le otorgó al Banco Central, y no al Colegio de Abogados, encargarse de la implementación de la firma digital, lo que hace que mediante el uso de la firma digital se deba autenticar posesión de poder para utilizarla, pero sin mediación de testigos ni abogados que puedan otorgar la confidencialidad, confiabilidad y autenticidad de los deseos de cada parte en un trato.

Por eso se deben observar los elementos jurídicos que se realizan normalmente ante un notario, a fin de que, estando en presencia de él o ella, se pueda cumplir con el requisito de inescindibilidad entre la firma y el firmante (al igual que la firma hológrafa de nuestros días), como una adecuada herramienta para el otorgamiento de la escritura pública digital.

Por su complejidad y por los elementos de seguridad que se deben cumplir, la firma y el protocolo digital siguen siendo más seguros y auténticos, al realizar los trámites notariales de manera presencial ante un notario.

Pese a que las nuevas tecnologías presentan muchas opciones para poder ejercer el protocolo notarial a distancia, y por medio de páginas electrónicas en donde se puede subir la información, no se debe perder de vista que estas nuevas tecnologías pueden todavía permitir la perpetración de delitos electrónicos que afecten a personas físicas y jurídicas. Para ello se debe buscar la manera de encriptar los documentos y las grabaciones en línea, que permitan que tanto los abogados como las entidades que intervienen en el proceso de autenticación jurídica den fe de que quienes aparecen en las grabaciones sean quienes en verdad son.

Recomendaciones

En primer lugar, el protocolo digital obedece a la comodidad de poder tramitar este tipo de documentos y de peticiones de manera remota y, por tanto, es necesario que su autenticidad quede pendiente

de la corroboración contra el impreso original que debe permanecer en archivo y así mantener el original físico y la respectiva copia digitalizados.

También se hace necesario que se legalicen los protocolos y procedimientos estandarizados, para preservar dichos archivos a lo largo del tiempo.

Aunado a lo anterior, se debe definir qué distingue a un archivo digital original y auténtico de otro que no lo es y, en caso de no ser auténtico, quién o quiénes deben asumir la responsabilidad de autenticar un documento en formato digital.

La nueva legislación que admita los trámites por medio de páginas web y herramientas digitales debe también definir procedimientos de archivo y de desecho de documentos, los cuales eventualmente podrían consumir mucho espacio de archivos digitales y, en caso de que se decida usar la nube para archivar, cómo se garantiza que siempre se tenga acceso a esa herramienta.

Referencias

Asamblea Legislativa. (2005). Ley de Certificados, Firmas Digitales y Documentos Electrónicos N.º 8454. https://salasegunda.poder-judicial.go.cr/index.php/noticias-2005/186-ley-de-certificados-firmas-digitales-y-documentos-electronicos

Cano, J. (2007). *Inseguridad informática: ¡Un concepto dual en seguridad informática!* https://www.researchgate.net/profile/Jeimy-Cano-M/publication/228800533_Inseguridad_informatica_Un_concepto_dual_en_seguridad_informatica/links/0046352600e838d680000000/Inseguridad-informatica-Un-concepto-dual-en-seguridad-informatica.pdf

Infante Meléndez, G. A. (5 de octubre del 2020). *Naturaleza Jurídica del Notario Costarricense*. Portal de Revistas Académicas. https://www.academia.edu/44235340/Texto_del_art%C3%ADculo_35036_2_10_20180705_1_

Madridejos, A. (2007). La copia notarial electrónica. https://biblioteca.abogacia.es/Record/Xebook1-31010/t/la-copia-notarial-electronica-como-instrumento-de-legitimacion-en-el-trafico-alfonso-madridejos-fernandez

Falbo, S. (2017). Otorgamiento del documento notarial digital, y circulación electrónica del documento notarial. https://escribanos.org.ar/rnotarial/wp-content/uploads/2018/01/RNCba-95-2017-03-Doctrina.pdf

Muñoz, N. (2007). *Notario Público – Notario – Qué es un Notario – Funciones del Notario*. https://notaris.pe/notarias/notario-publico-notario-que-es-un-notario-funciones-del-notario-notario-de-lima-notario-peru/

Pelosi, C. A. (1997). El Documento Notarial. *Revista del Notariado*, *3º Reimpresión*, 120.

Suñe, E. (2000). *Tratado de Derecho Informático. Introducción y Protección de Datos Personales* (1ª ed., vol. I, p. 7). https://dialnet.unirioja.es/servlet/libro?codigo=778285

Tableau Software. (2016). Las 10 tendencias principales de la nube para 2017. United States: Tableau Software. https://www.tableau.com/sites/default/files/whitepapers/whitepaper_top_10_cloud_trends_2017_es-es.pdf

Muñoz, N. *Introducción al Estudio del Derecho Notarial.* 3º Ed. Guatemala C.A, 1992.

Vázquez Martínez, M. A. (n.d.). *Seguridad en la nube durante los próximos años*. https://revista.seguridad.unam.mx/numero29/seguridad-en-la-nube

Salas, Oscar A. *Derecho Notarial en Centroamérica y Panamá*. Editorial Costa Rica 1973. Pp. 60-61