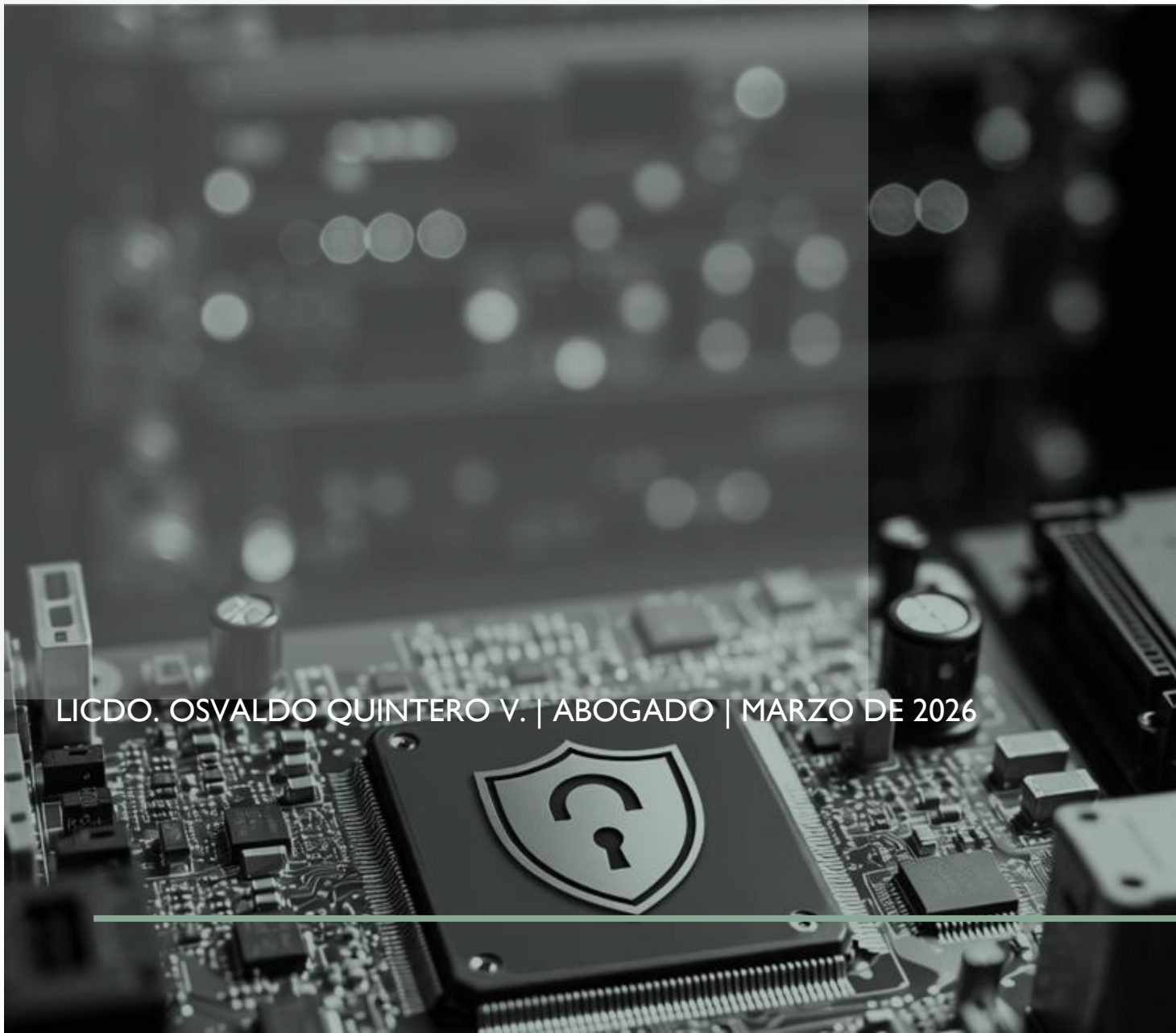
FIRMA ELECTRÓNICA

Guía rápida legal de aplicación para Panamá - Ensayo



LICDO. OSVALDO QUINTERO V. | ABOGADO | MARZO DE 2026

SOBRE EL AUTOR

El Licdo. Osvaldo Quintero V. es un abogado digital independiente graduado de la Universidad de Panamá en 1999, con MBA de la Universidad Latina de Ciencia y Tecnología en 2001, curso de tecnología PKI y autenticación electrónica en Taipei - Taiwán (China), cursos de ISO 27001 y con mas de una década de experiencia en el ámbito de la firma electrónica como ex asesor alegal y técnico en la Dirección Nacional de Firma Electrónica del Registro Público de Panamá y ex asesor en el área de Comercio Electrónico del Ministerio de Comercio e Industrias. También es programador con conocimientos de lenguajes como Python, Javascript y Solidity (Blockchain). Fue el creador y lider legal en la elaboración de la vigente Ley 82 de 2012 sobre firma electrónica y todas las reglamentaciones de la Ley 51 de 2008 en materia de firma electrónica hasta el 2025.

Tabla de contenido

INTRODUCCIÓN

El presente ensayo no pretende ser una guía completa ni definitiva sobre el tema de la firma electrónica sino mas bien un compendio de temas que causan confusión o suelen ser mal entendidos en el entorno nacional por los usuarios y sobre todo por los abogados que revisan las normas sobre firma electrónica en Panamá. Esperamos que aquí se resuelvan muchas dudas sobre el tema de la firma electrónica, queden plasmadas nuevas inquietudes y se despierte mas interés sobre este interesante tema. En futuras ediciones se desarrollaran mas elementos y otros temas que no se tocan en este ensayo, por ser bastante profundos, tales como el registro de prestadores de servicios de certificación y en que consiste una declaración de prácticas de certificación.

LEGISLACIÓN APLICABLE

- Ley 51 de 2008 (Ley principal. Regula la firma electrónica y los prestadores de servicios de certificación)
- Ley 82 de 2012 (Actualización Ley 51/2008 y ley que faculta al Registro Público ser ente rector de la FE y los PSC)
- Ley 83 de 2012 (Ley de trámites gubernamentales)
- Ley 144 de 2020 (Actualización de la Ley 83/2012)
- Decreto Ejecutivo 684 de 2013 (Reglamento de la Ley 51/2008)
- Decreto Ejecutivo 83 de 2023 (Actualización del DE 684/2013)
- Reglamentos Técnicos vigentes a la fecha emitidos por la Dirección Nacional de Firma Electrónica (DNFE):
  - ❖ Regl. Técnico 5 (Requisitos de la FE emitida por el Registro Público)
  - ❖ Regl. Técnico 7 (Requisitos del Sello de gobierno emitido por el Electrónico de Gobierno del Registro Público)
  - ❖ Regl. Técnico 8 (Requisitos técnicos para ser Prestador de Servicios de Certificación de carácter privado en Panamá).

Nota: La Ley 83 de 2012 también tiene reglamentos por Decreto Ejecutivo que no trataremos en este ensayo.

DEFINICIÓN DE FIRMA ELECTRÓNICA Y SU VALOR LEGAL

El artículo 2 nums. 20 y 21 Ley 51 de 2008 modificado por el artículo 7 de la Ley 82 de 2012 define firma electrónica y firma electrónica calificada como:

> ***"20. Firma electrónica.*** *Método Técnico para identificar a una persona y para indicar que esa persona aprueba la información que figura en un mensaje de datos o documento electrónico.*
>
> ***21. Firma electrónica calificada.*** *Firma electrónica cuya validez es respaldada por un certificado electrónico calificado que:*
>
> *a. Permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados.*
> *b. Está vinculada al firmante de manera única y a los datos a que se refiere.*
> *c. Ha sido creada utilizando dispositivos seguros de creación de firmas electrónicas, los cuales mantiene el firmante bajo su control exclusivo.*
> *d. Ha sido creada a través de la infraestructura de un prestador de servicios de certificación registrado ante la Dirección Nacional de Firma Electrónica."*

El **artículo 8** de la Ley 51 de 2008 (Modificado por Art. 14 - Ley 82 de 2012) define el valor legal de la Firma Electrónica de la siguiente manera:

> *"Valor legal de la Firma Electrónica: Cuando la ley exija la firma de una persona o establezca consecuencias por la ausencia de la firma de esa persona, dicho requerimiento de firma quedará satisfecho con un mensaje de datos sí:*
>
> ***1.*** *Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación.*
> ***2.*** *Que el método es confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado.*

Los anteriores requisitos se darán por satisfechos cuando ambos estén presentes, pero se presumirán de pleno derecho en el caso de que se esté en presencia de una firma electrónica calificada y por tanto en la emisión intervenga un prestador de servicios de certificación autorizado por la Dirección Nacional de Firma Electrónica.".

FIRMA ELECTRÓNICA SIMPLE Y CALIFICADA

Si estudiamos el artículo 8 de la Ley 51 de 2008 antes mencionado, observamos la distinción doctrinal entre la llamada "firma electrónica simple" y la "firma electrónica calificada". Ambas tienen valor legal con la distinción fundamental que la firma electrónica calificada tiene presunción de validez de pleno derecho. La firma electrónica simple, que es la no calificada, tiene valor legal cuando se da por satisfecho el numeral 1 y 2 del artículo 8 en cuestión; y la firma electrónica calificada, es aquella emitida por un prestador de servicios de certificación (en adelante PSC) registrado en la Dirección Nacional de Firma Electrónica y también la emitida por el propio Registro Público de Panamá como PSC del gobierno nacional según la Ley 82 de 2012. En resumen, la firma electrónica simple para que tenga valor legal en un litigio debe probarse (que cumple ambos numerales 1 y 2 del artículo 8) mientras que la firma electrónica calificada entraría en un proceso, en principio, de manera mucho más ventajosa con una presunción de validez por imperio de la ley que no requiere prueba, es decir que, en teoría, la firma electrónica calificada tiene validez legal automática.

QUE DOCUMENTOS PUEDEN FIRMASE CON FIRMA ELECTRÓNICA CALIFICADA

Respuesta corta: todos, antes de la Ley 82 de 2012, el artículo 4 de la Ley 51 de 2008 decía lo siguiente:

*"**Artículo 4.** Valor legal de los documentos electrónicos y de la firma electrónica. Cuando la ley requiera que la información conste en un documento escrito, se le reconocerá validez, efectos jurídicos y fuerza obligatoria a los actos y contratos que hayan sido otorgados o adoptados a través de medios electrónicos en documentos electrónicos de conformidad con esta Ley y sus reglamentos.*
Lo dispuesto en el presente artículo no será aplicable a los actos para los cuales la ley exige una solemnidad que no sea verificable mediante documento electrónico." (El subrayado es nuestro)

El último párrafo tácitamente excluía que los poderes, contratos que requerían escritura pública, testamentos y muchos documentos más se hicieron por documento electrónico, por ende, no permitían firma electrónica pero afortunadamente la Ley 82 de 2012 modifico este artículo de la siguiente manera:

***"Artículo 4 (Modificado por Art. 10 - Ley 82 de 2012).** Valor legal de los documentos electrónicos. Cuando la ley requiera que la información conste en un documento escrito, se le reconocerá validez, efectos jurídicos y fuerza obligatoria a los actos, poderes y contratos y a todo documento que haya sido otorgado o recibido a través de mensajes de datos, de conformidad con esta Ley y sus reglamentos, siempre que la información que este contiene sea accesible para su posterior consulta."* (El subrayado es nuestro)

La Ley 82 de 2012, elimina las restricciones establecidas en la norma anterior. Ahora la única condición que se establece es que el documento electrónico otorgado o recibido a través de "mensajes de datos" puedan consultarse, es decir, estén alojados en algún repositorio.

¿CÓMO PROBAR LA FIRMA ELECTRÓNICA SIMPLE PARA QUE TENGA VALOR LEGAL?

Repasemos nuevamente el **artículo 8** de la Ley 51 de 2008 (Modificado por Art. 14 - Ley 82 de 2012), cuyos numerales 1 y 2 establecen lo siguiente:

Art. 8 numeral 1:

> ***"1.*** *Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación."*

Hay múltiples maneras de lograr esto. A manera de ejemplo, esto se puede lograr a través de una combinación de: Logs (bitácoras); cláusulas contractuales donde las partes concuerdan el uso de un método firma electrónica simple específico; un mensaje de datos que enlaza lo indexado y registrado en las bitácoras; el mensaje de datos que contiene la aprobación dada por el firmante (ej. una firma electrónica usando algoritmos como el RSA-SHA 256, ECDSA, firma biométrica que se vincula criptográficamente al documento, el uso de formatos como XAdES, CAdES o PAdES); el mensaje de datos que permita identificar al firmante (ej. una dirección Blockchain), etc.

Art. 8 numeral 2:

> "**2**. *Que el método es confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado."*

A través del uso de un método de firma electrónica confiable, por ejemplo, el uso de los algoritmos arriba mencionados, el uso de certificados electrónicos x509, contar con certificaciones de seguridad tipo ISO 21188, ISO 27001, SOC-2, webtrust, ETSI-EN 319 411-1, ETSI EN 319 411-2, ETSI EN 401, eiDAS, etc.[1]

VALOR LEGAL ESPECIAL DE LA FIRMA ELECTRÓNICA CALIFICADA

Repasemos nuevamente el último párrafo del **artículo 8** de la Ley 51 de 2008 modificado por la Ley 82 de 2012 y que establece lo siguiente:

> *"Valor legal de la Firma Electrónica: Cuando la ley exija la firma de una persona o establezca consecuencias por la ausencia de la firma de esa persona, dicho requerimiento de firma quedará satisfecho con un mensaje de datos sí:*
>
> ***1.*** *Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación.*
>
> ***2.*** *Que el método es confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado.*

[1] No se recomienda el uso de algoritmos deprecados por la industria tales como el sha-128 y el md5.

Los anteriores requisitos se darán por satisfechos cuando ambos estén presentes, pero se presumirán de pleno derecho en el caso de que se esté en presencia de una firma electrónica calificada y por tanto en la emisión intervenga un prestador de servicios de certificación autorizado por la Dirección Nacional de Firma Electrónica." (el subrayado es nuestro).

Aquí vemos que la firma electrónica calificada produce el efecto jurídico de que se presume que ambos numerales 1 y 2 están presentes, por ende, la firma electrónica tiene valor legal automático como si fuera manuscrita, probando todo lo que establece su definición que vimos anteriormente cuando examinamos los nums. 20 y 21 del art. 2 de la Ley 51 de 2008 modificada por el art 7 de la Ley 82 de 2012 y la cual volvemos a repasar:

*"**20. Firma electrónica.** Método Técnico para identificar a una persona y para indicar que esa persona aprueba la información que figura en un mensaje de datos o documento electrónico.*

***21. Firma electrónica calificada.** Firma electrónica cuya validez es respaldada por un certificado electrónico calificado que:*

a. Permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados.
b. Está vinculada al firmante de manera única y a los datos a que se refiere.
c. Ha sido creada utilizando dispositivos seguros de creación de firmas electrónicas, los cuales mantiene el firmante bajo su control exclusivo.

Ha sido creada a través de la infraestructura de un prestador de servicios de certificación registrado ante la Dirección Nacional de Firma Electrónica."

O sea, la firma electrónica calificada es una firma electrónica (método técnico que indica que una persona aprueba una información en un mensaje de datos o documento electrónico); respaldada por un certificado electrónico calificado emitido por un PSC legalmente autorizado; que permite probar los literales a, b y c del numeral 21 arriba mencionado y que tiene PRESUNCIÓN DE PLENO DERECHO de que se cumplieron los numerales 1 y 2 del artículo 8 arriba mencionado.

Lo interesante es como nuestra legislación no restringe la firma electrónica calificada al nombre de la persona perfectamente la presunción de pleno de derecho puede abarcar toda la información adicional que contiene el certificado electrónico calificado, que por obligación legal ha sido previamente revisado y verificado minuciosamente por el PSC antes de la emisión del certificado electrónico para firmar (ver art. 26 de la Ley 51 de 2008 modificado por el art. 28 de la Ley 82 de 2012). Por ende la presunción de validez abarcaría la identidad de la persona, datos como su nombre "Juan Pérez", su número de cédula o pasaporte, su condición legal al firmar según el perfil del certificado electrónico (ej. Funcionario público de un Ministerio, representante legal o apoderado legal de la Sociedad Anónima "EQUIS, S.A"), su condición profesional (profesional de la abogacía, médico, traductor público autorizado, etc.) y más, eliminándose la necesidad de probar a través del papel con las famosas "Copias autenticadas" todas estas condiciones personales con una connotación legal, indistintamente sea en un juicio o en una plataforma electrónica. Claro está, para que esto funcione en un juicio la jurisprudencia tiene que acompañar y favorecer esta posibilidad.[2]

[2] Los documentos legales donde aparecen toda la información que contiene un certificado electrónico calificado se llaman "Declaración de prácticas de certificación" y "Políticas de certificación". Ambos documentos son obligatorios para todos los PSC de conformidad con la Ley 51 de 2008 y el Decreto Ejecutivo 684 de 2013. Cada PSC tiene que tenerlos disponibles en su página web para consulta de sus usuarios.

Es importante destacar que lamentablemente la jurisprudencia panameña y el nuevo código de procedimiento civil no reconoce aún el valor legal automático de la firma electrónica de tipo calificada haciendo que la misma en la práctica tenga un valor legal reducido de su propósito inicial, que es la presunción de validez, según la Ley 51 de 2008.

EL PROBLEMA DEL VALIDADOR DE FIRMA ELECTRÓNICA

En la práctica en Panamá, la firma electrónica calificada en Panamá carece del uso habitual de lo que la ley 51 de 2008 en su artículo 12 denomina *dispositivo de verificación de firma electrónica* (o sea un validador) que si bien es obligación legal de los PSC explicarle a sus usuarios como se valida una firma electrónica, los PSC existentes en Panamá tienen métodos propios muy rudimentarios de validación, quedando relegada la validación de una firma electrónica calificada a algo que se encuentra en una zona gris entre lo oficial y lo no oficial, difícil de exportar por el usuario para utilizarse en un proceso como prueba y dependiente de métodos manuales como peritajes y capturas de pantalla (de la validación hecha por Adobe Reader por ejm.) lo cual está totalmente alejado del propósito inicial de la firma electrónica calificada, que es la posibilidad de verificar el consentimiento de una persona sobre un mensaje de datos o documento electrónico, su autenticidad e integridad, todo en uno, de manera simple, electrónica y automática.

A la fecha, no existe un validador oficial de firma electrónica de parte del Registro Público que sea realmente abierto al público, de fácil acceso y que exporte el resultado de la validación para uso probatorio. Igualmente, los PSC privados actuales cuentan con validadores propios igualmente rudimentarios. En ambos casos, relegados al formato PaDES (para documentos PDFs únicamente) y con un resultado no exportable, olvidando el uso del formato CAdES que es realmente el formato más útil, pero que requiere de la existencia no solo de un validador sino también de un firmador especial y a la fecha ningún PSC local los ofrece.

Creemos que esta situación de poca importancia al validador ha causado en consecuencia que se reduzca la importancia de la firma electrónica calificada y que la jurisprudencia a la fecha tenga criterios muy propios, para poder validar judicialmente un documento electrónico ante los tribunales, métodos que no mencionan la presunción y las definiciones de la firma electrónica calificada; y que implican, la necesidad de probar la "autenticidad e integridad" de un documento electrónico mediante un peritaje que examine la "cadena de custodia" y la "autenticidad e integridad" de un documento electrónico apoyándose en los artículos 6,7,44,45 y 46 de la Ley 51 de 2008, llamando la atención que los artículo 44,45 y 46 se encuentran en el Título IV de "Almacenamiento Tecnológico de Documentos" y no en el Título III de "Firma electrónica"[3].

Mas recientemente, el nuevo Código de Procedimiento Civil, (Ley 402 de 2023), reafirma y condensa la jurisprudencia previa en un solo artículo al regular la "prueba electrónica" en su artículo 414 cuando establece:

> *"**Artículo 414.** Prueba electrónica. La prueba electrónica es la información que sirve para adquirir convencimiento de la certeza de una pretensión alegada por alguna de las partes, indistintamente del tipo de dispositivo o la tecnología utilizada para su creación o fijación, la cual puede encontrarse contenida en medios físicos o lógicos de almacenamiento de información.*
> *La prueba electrónica se fundamenta en los principios de objetividad, autenticidad y conservación, legalidad, idoneidad, integridad, documentación y neutralidad electrónica.*
> *La prueba electrónica será admisible y tendrá la misma fuerza probatoria que este Código atribuye al medio de que se trate.*

[3] Al final de este documento dejamos una lista de la jurisprudencia relevante que sustenta nuestro criterio.

Se considerará válida si existe la garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva. La integridad de la prueba será resultado de un procedimiento de verificación tecnológico aplicado, que permita determinar con certeza que no ha sido modificada desde el momento de su emisión. Al momento de introducir la prueba electrónica, esta deberá ser presentada y conservada en su formato original, obtenida de forma lícita e íntegra.
La valoración de la prueba electrónica quedará sujeta a los siguientes presupuestos:

1. *Al someterse el documento a almacenamiento tecnológico, este deberá quedar conservado en un medio de almacenamiento adecuado.*
2. *Los documentos o pruebas electrónicas deben quedar almacenados en forma nítida, íntegra y con absoluta fidelidad.*
3. *Sea posible determinar, con precisión, la fecha y la hora en que la prueba electrónica fue almacenada tecnológicamente.*
4. *La recuperación de la prueba electrónica se lleve a cabo mediante mecanismos de clonación de todos los sectores, obteniendo una copia íntegra a los almacenados en el dispositivo original.*
5. *Se hayan cumplido los procedimientos de la cadena de custodia.*

La omisión de cualquiera de los requisitos anteriores, así como la alteración o adulteración, que afecten la integridad de la prueba electrónica donde ha sido almacenada, harán perder la eficacia probatoria de este medio."

Esta norma, implícitamente contempla la prueba electrónica básicamente como un peritaje donde, en resumen, se comprueba la integridad y autenticidad de un mensaje de datos o documento electrónico, donde el perito experto va a analizar el documento electrónico, email, chats de whatsapp, etc. vía extracción manual de los mismos del dispositivo, luego con sus instrumentos especializados, hace un cálculo posterior del hash de lo extraído (con un algoritmo no especificado en la ley), hace una "copia espejo" de ese material, para luego presentarlo al tribunal en una cadena de custodia. Esta norma al no mencionar la firma electrónica de tipo calificada, en consecuencia, no pondera si el cálculo del hash de un documento se hizo al momento exacto de su firma, que es lo óptimo tal como se hace con la firma electrónica calificada, en vez del cálculo de un hash hecho por un perito, que es mucho después de la creación o firma del documento. La firma electrónica calificada está pensada para no requerir perito pues gracias al dispositivo de verificación de firma, se válida automáticamente la firma electrónica en el documento, el hash calculado en el momento de la creación de la firma, su autenticidad e integridad, todo en uno. Por otro lado, potencialmente dificultándose más las cosas para la firma electrónica calificada, el numeral 1 de este artículo 414 de la Ley 402 de 2023, menciona el "almacenamiento tecnológico" obviando el hecho de que este tema está regulado por el Título IV de la Ley 51 de 2008, siento el ente rector la Dirección General de Comercio Electrónico del Ministerio de Comercio e Industrias y sus reglamentos técnicos (algo no contemplado por ese artículo 414 o la jurisprudencia existente) y no podemos olvidar que la firma electrónica calificada es una tecnología que por ley tiene presunción de validez, de la integridad y autenticidad, del documento firmado y está regulada por los reglamentos técnicos de la Dirección Nacional de Firma Electrónica del Registro Público de Panamá.

Consideramos, que la utilidad del perito informático y sus métodos en el ámbito judicial, son más apropiados para el análisis de la validez legal de mensajes de datos y documentos electrónicos cuando no se usa firma electrónica o sólo firma electrónica simple; mas no cuando se utiliza la firma electrónica calificada. Adicionalmente, si reconocemos y nos parece correcto que la jurisprudencia y el nuevo código procesal civil desconocen el valor legal de las llamadas "Autenticaciones de firma electrónica" hechas por algunos notarios públicos y que, a nuestro criterio, no tienen ningún fundamento legal ni mucho menos técnico, de hecho la Ley 51 de 2008 modificada por la Ley 82 de 2012 es clara que

tanto los notarios como el Estado en el sector público solo deben admitir y reconocer la firma electrónica calificada como la contempla esa Ley.[4]

A nivel técnico, a grosso modo, lo que ocurre con una firma electrónica calificada es que se calcula el valor hash a un documento electrónico al momento exacto de la firma (usando un algoritmo SHA-256 por ejm.) y luego se encripta ese hash usando la llamada "Clave privada" que se encuentra en el certificado electrónico calificado emitido por un PSC[5]. Adicionalmente, el chip de un *smartcard* (o el *storage* remoto del PSC si es firma en la nube) contiene un certificado electrónico calificado con la llamada "Clave pública", de ahí el nombre de esta tecnología como "Tecnología de clave pública" (o PKI - *Public key infrastructure* por sus siglas en inglés) certificado este que a su vez está firmado por el PSC. Este certificado con la clave pública se copia e incrusta en los documentos firmados. Cuando usted envía un documento con firma electrónica a la contraparte, usted está realmente enviando ese documento con un hash encriptado usando la clave privada (A) y eso constituye realmente la firma electrónica más un certificado electrónico incrustado. Su contraparte al abrir el documento y verificarlo, usando por ejemplo el aplicativo Adobe Reader, se calcula nuevamente el hash (B) y se leen los datos en el certificado incrustado, entre ellos la clave pública y usando esa clave se desencripta el hash (A); si A y B concuerdan, se válida por internet con el correspondiente PSC la cadena de confianza que aparece en ese certificado; y si satisfactoriamente se valida esa cadena de confianza, le aparece al destinatario en pantalla que la firma es válida, quien la firmó, que el documento es auténtico e integro, que se usó una firma calificada con un certificado electrónico calificado emitido por un PSC legalmente autorizado en el país, todo en uno y en cuestión de segundos…sin peritos.

Entonces, la respuesta lógica a la pregunta de cómo se valida (o más bien como se "verifica" que es el término que aparece en la ley) una firma electrónica calificada es que se valida de manera ELECTRÓNICA. Ya sabemos que uno de estos "aplicativos" de verificación es el comúnmente utilizado Adobe Reader, no obstante la verificación de firma que hace este aplicativo no es la mejor para el ámbito legal nacional pues requiere una complicada configuración manual hecha previamente por el usuario para que funcione correctamente y esto puede dar a lugar a manipulaciones o equivocaciones de todo tipo y esto sin incluir que el Adobe Reader trae, instalados por defecto, muchos certificados electrónicos que no tienen valor legal en Panamá (por no ser calificados o sea reconocidos por la Dirección Nacional de Firma Electrónica), por tanto va a mostrar como válido toda clase de documentos electrónicos sin valor legal en Panamá trayéndole confusión al usuario y requiriendo una verificación adicional manual y visual del certificado electrónico usado para la firma electrónica (a ver si es calificado) lo que nos vuelve a traer al uso de peritos. Para evitar todo esto, lo correcto es utilizar un validador de firma electrónica previamente configurado por el PSC, que sólo contiene instalados certificados calificados en Panamá, y que éste sea su validador oficial. Esta es una explicación corta del problema de Adobe Reader que además sólo puede validar documentos en formato PAdES cuando existen otros formatos como el XAdES y sumamente versátiles como el CAdES[6] que son muy utilizados en otras latitudes, especialmente Europa.

QUE ES EL SELLADO DE TIEMPO

El sellado de tiempo es una firma electrónica adicional puesta en el documento electrónico y que contiene la fecha y la hora al momento de la creación de la firma. Esto evita el uso de la hora de la computadora que puede ser manipulado

[4] Ver art 9 de la Ley 51 de 2008 modificado por el art. 15 de la Ley 82 de 2012; art 13 de la Ley 51 de 2008 modificado por el art. 17 de la Ley 82 de 2012; y los arts 51 a 56 de la Ley 82 de 2012.

[5] La clave privada se encuentra en el chip criptográfico para el caso de firmas electrónicas emitidas con *smartcard* por un PSC o está alojada en un dispositivo de hardware HSM (Hardware Security Module) de propiedad del PSC para el caso de la llamada "Firma electrónica en la nube" o "Firma electrónica centralizada".

[6] PAdES (PDF Advanced Electronic Signature), XAdES (PDF Advanced Electronic Signature), CAdES (CMS Advanced Electronic Signature). El formata CAdES permite firmar todo tipo de documentos más allá de los PDF (Ej. jpg, docx, etc.).

por el usuario. Según la Ley 51 de 2008 este sellado de tiempo es pues una hora y fecha con valor legal en Panamá y es el equivalente digital de pasar un documento en papel por una máquina de fechar documentos, el mismo se encuentra definido legalmente en el numeral 46 del Art. 2 de la Ley 51 de 2008 que fue adicionado por el Art. 7 de la Ley 82 de 2012. Cuando usted firma un documento electrónico con firma electrónica calificada usando Adobe Reader por ejemplo, si este está correctamente configurado con el servidor de sellado de tiempo del PSC, se firma el documento con la firma calificada de sellado de tiempo, la cual incluye un certificado electrónico calificado del PSC sólo para este propósito. Firmar con sellado de tiempo es lo que se conoce como firmar con LTV o *Long Term Validation* ya que, al expirar el certificado electrónico (los certificados electrónicos expiran periódicamente según el PSC que se utilice), la firma electrónica suya usada en un documento aparecerá como inválida al tratar de verificarse, a menos que tenga LTV.

¿EL CÓDIGO QR ES UNA FIRMA ELECTRÓNICA?

Usualmente no. El código QR es solo una imagen que puede, de manera condensada contener algunos datos, usualmente enlaces a otras direcciones URL. Esa dirección si pudiese apuntar a un repositorio donde está el documento original con firma electrónica. Igualmente, en el código QR esos datos si pudieran contener una firma electrónica con algoritmo RSA-SHA 256, ECDSA o un hash del certificado. El problema radica en que el código QR no puede alojar mucha información, esto hace difícil que un QR contenga en sí una firma electrónica (el hash del documento encriptado con una clave privada) más el certificado con la clave pública necesaria para verificar, pero no imposible. Advertimos, que el QR mal implementado, por ser una imagen, es fácilmente manipulable (hasta con Photoshop) y que maliciosamente puede dirigir un navegador a un enlace no muy seguro. Esto es la parte técnica.

En estricto derecho, como la Ley 51 de 2008 define firma electrónica calificada como aquella respaldada por un certificado electrónico calificado, mientras ese QR no esté respaldado por un certificado electrónico calificado, pues no es una firma electrónica calificada. Como firma electrónica simple si lo pudiera ser, pero se tendría que cumplir con mucho ingenio los numerales 1 y 2 del artículo 8 de la Ley 51 de 2008. Entonces para que sea fácil "transformar" legalmente un QR en una firma electrónica con valor legal se necesita de normas distintas a la Ley 51 de 2008 que lo permitan. Aquí, sin ánimo de criticar el uso del QR que tiene gran utilidad, a veces nos encontramos con resoluciones de gobierno que han adoptado el QR como una especie confusa de firma electrónica, escritas con mucha ligereza jurídica y carentes de buen análisis técnico.

¿SE PUEDE "CERTIFICAR" UNA FIRMA ELECTRÓNICA CALIFICADA?

Nuestro ámbito jurídico muy propenso a la "certificación". En nuestro medio, tanto abogados como fiscales y jueces son propensos a pedirle "certificaciones" a la autoridad rectora de un tema para saber si es cierta o no alguna cosa. Por ejemplo, al Registro Público de Panamá sus usuarios constantemente le piden certificaciones de fincas o de sociedades inscritas. De manera coincidente el tema de la firma electrónica utiliza el término "Certificado" pero con una connotación muy distinta. En el ámbito de la firma electrónica el término "Certificado" se refiere a un *digital certificate* (por sus siglas en inglés) que es un archivo creado por una autoridad de certificación (el PSC) que se incrusta en un chip o via software en una computadora y que permite firmar o validar una firma electrónica. Que pasa entonces si algún interesado, a falta de que exista un validador oficial o usar un perito, quiere pedirle a la Dirección Nacional de Firma Electrónica del Registro Público de Panamá (Ente rector) que le "certifique" que la firma electrónica de "Juan Pérez" en un documento es válida. El artículo 45 del Decreto Ejecutivo 684 de 2013 dice lo siguiente:

> ***"Artículo 45.*** *Puesto que la firma electrónica calificada se presume auténtica por imperio de la Ley y para que se de este efecto jurídico sólo basta con validarla electrónicamente, todo ciudadano, autoridad administrativa o judicial que solicite al Registro Público o a cualquier prestador autorizado de servicios de certificación público o privado una certificación de firma electrónica calificada sólo se le extenderá al interesado una constancia de que el firmante es o no usuario de la firma electrónica calificada, si tiene o no un certificado electrónico vigente, el perfil de uso de dicho certificado electrónico y que esta constancia no constituye un requisito fundamental de evidencia probatoria."*

Entonces esa Dirección sólo le emitirá al interesado una "constancia" de que la DNFE como PSC le emitió una firma electrónica a "Juan Pérez" de "persona natural", o de "representante legal de la persona jurídica EQUIS, S.A." o que "Juan Pérez" tiene firma electrónica "de profesional de la abogacía" que está aún vigente. Sin especificar si la firma en el documento es válida o no (Recordemos que este sería el trabajo del validador que en teoría debería tener todo PSC). O sea, el PSC no expide una certificación de información como los abogados están acostumbrados a pedir. Pero hay una situación interesante que podría ocurrir y que trataremos en el siguiente punto de este ensayo.

¿SON VÁLIDAS LAS FIRMA ELECTRÓNICAS EMITIDAS EN EL EXTRANJERO?

La Ley 51 de 2008 tiene las siguientes reglas para los certificados electrónicos emitidos por PSC del extranjero:

> *"**Artículo 17 - Ley 51 de 2008 modificado por Art. 20 - Ley 82 de 2012).*** Reconocimiento de certificados extranjeros. Los certificados emitidos por prestadores de servicios de certificación de firmas electrónicas extranjeros podrán ser reconocidos en los mismos términos y condiciones establecidos por esta Ley para los certificados calificados en cualquiera de los siguientes casos:*
>
> 1. *Cuando tales certificados sean reconocidos en virtud de acuerdos con otros países, ya sean bilaterales o multilaterales, o efectuados en el marco de organizaciones internacionales de las que Panamá sea parte.*
> 2. *Cuando tales certificados sean emitidos por prestadores de servicios de certificación debidamente avalados en su país de origen por instituciones homólogas a la Dirección Nacional de Firma Electrónica de el Registro Público, que requieren para su reconocimiento estándares que garanticen la seguridad en la creación del certificado y la regularidad de los detalles del certificado, así como su validez y vigencia.*
> 3. *Cuando se acredite que tales certificados fueron emitidos por un prestador de servicios de certificación que cumple con los estándares mínimos requeridos para un prestador de servicios de certificación de firmas electrónicas registrado ante la Dirección Nacional de Firma Electrónica de el Registro Público."*

Este tema se encuentra reglamentado muy someramente en el Decreto Ejecutivo 684 de 2013 en su artículo 3 así:

> ***"Artículo 3.*** *De forma complementaria a lo establecido en la Ley, la Dirección tendrá las siguientes funciones:*
>
> *1…*
>
> *5. Aprobar y dar reconocimiento a los certificados electrónicos extranjeros en los términos establecidos en el artículo 17 de la Ley 51 de 2008…"* (el subrayado es nuestro).

Si a esto le añadimos lo establecido en el artículo 2 de la Ley 82 de 2012 que dice:

> *"**Artículo 2.** El Registro Público de Panamá dentro de sus funciones podrá **certificar**, prestar y ofrecer la firma electrónica, la firma electrónica calificada, el servicio de sellado de tiempo, el de archivo y conservación de mensajes de datos y otros servicios complementarios, así como cobrar tasas por ofrecer estos servicios, cuyos montos y procedimiento de cobro serán determinados en el reglamento..."* (El subrayado es nuestro)

Si sumamos las tres normas concluimos que, en teoría, la Dirección Nacional de Firma Electrónica puede reconocer como válido en Panamá certificados electrónicos emitidos por un PSC del extranjero, lo que daría validez legal a las firmas electrónicas que utilicen estos certificados y el Registro Público de Panamá si podría CERTIFICAR (ahora si en la terminología común del abogado) esa validez según el artículo 2 de la Ley 82 de 2012, saltándose la constancia que menciona el artículo 45 del Decreto Ejecutivo 684 de 2013 pues esa constancia solo aplicaría a firmas electrónicas emitidas por el propio PSC y en este caso estamos solicitando ***certificar*** un reconocimiento de certificado electrónico del extranjero en base al artículo 17 de la Ley 51.

¿CÚALES SON LOS PSC AUTORIZADOS PARA OPERAR EN PANAMÁ?

1. El propio Registro Público de Panamá. (Por virtud de los artículos 1 y 2 de la Ley 82 de 2012).
2. Los autorizados para operar como PSC por la Dirección Nacional de Firma Electrónica del Registro Público de Panamá cuya resolución de registro se publicó en Gaceta Oficial y se encuentran en la lista que se encuentra publicada en la página web de la Dirección Nacional de Firma Electrónica.

EL CASO DE LA LEY 144 DE 2020

Mencionamos esta ley que aún no ha sido implementada en la práctica pues la misma crea un régimen legal paralelo a la firma electrónica calificada para los trámites gubernamentales denominado "identidad digital" y que por ende permitiría wallets de identidad digital. Así pues, los numerales 6, 7 del artículo 83 de 2012 modificada por el artículo 2 de la Ley 144 de 2020 dicen los siguiente:

> *"**Artículo 2.** El artículo 3 de la Ley 83 de 2012 queda así:*
>
> ***Artículo 3. Definiciones**. Para los efectos de esta Ley, los siguientes términos entenderán así:*
>
> *1. …*
>
> *…*
>
> *6. Firma electrónica. Equivalente electrónico a la firma manuscrita, es un método técnico para identificar a una persona de manera inequívoca y para indicar que esa persona aprueba la información que figura en un mensaje de datos, documento electrónico o cualquier medio electrónico, asegurando la integridad del documento firmado y su no repudio.*
>
> *7. Identidad digital. Plataforma tecnológica para la comprobación de la identidad por vía electrónica o digital, que permite que los usuarios pueden ser validados y verificados de manera inequívoca, y facilite al usuario iniciar y realizar trámites de forma directa, expedita y segura con el Estado en las diversas plataformas gubernamentales,*

permitiendo la validación y verificación de estos al inicio de la gestión del trámite, durante o al momento de la finalización de este.

La identidad digital podrá contener diversas formas de validación de identidad, según la tecnología disponible, y puede reemplazar el requerimiento de firma electrónica.

8…

…" (El subrayado es nuestro).

El artículo 4 de la Ley 83 de 2012 modificada por el artículo 3 de la Ley 144 de 2020 dice lo siguiente:

*"**Artículo 3**. El artículo 4 de la Ley 83 de 2012 queda así:*

***Artículo 4.** Facultades. Para garantizar la prestación de servicios por medios e instrumentos electrónicos, las entidades públicas harán uso de las siguientes facultades y resguardarán los derechos que aquí se enmarcan:*

***1.** …*

…

10. Los documentos presentados por los usuarios por medios electrónicos que contengan la firma electrónica, de conformidad con la Ley 51 de 2008, producirán en términos de esta Ley los mismos efectos que los documentos firmados de manera autógrafa; sin embargo, tendrán el mismo efecto legal en caso de que se establezcan nuevos marcos regulatorios con respecto a firmas electrónicas o digitales, así como el uso de la identidad digital.

11. …" (El subrayado es nuestro)

JURISPRUDENCIA RELEVANTE

Nota: Por protección de datos personales en esta lista se evita poner nombres de las partes. Por número de negocio fácilmente se encuentra esta jurisprudencia en el buscador del Órgano Judicial.

1. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: PROCESOS COMUNES
NÚMERO DE NEGOCIO: 583542025
FECHA DE NEGOCIO: 14-04-2025
JERARQUÍA: TRIBUNAL SUPERIOR
DEPENDENCIA JUDICIAL: TRIBUNAL SUPERIOR DE TRABAJO
NÚMERO DE RESOLUCIÓN: ---
FECHA DE RESOLUCIÓN: 19-06-2025

2. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: CONTENCIOSO ADMINISTRATIVO
NÚMERO DE NEGOCIO: 228002025
FECHA DE NEGOCIO: 11-02-2025
JERARQUÍA: CORTE SUPREMA DE JUSTICIA
MATERIA: SALA TERCERA CONTENCIOSO ADMINISTRATIVO Y LABORAL
DEPENDENCIA JUDICIAL: CORTE SUPREMA DE JUSTICIA
NÚMERO DE RESOLUCIÓN: --
FECHA DE RESOLUCIÓN: 13-05-2025

3. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: PROCESOS COMUNES
NÚMERO DE NEGOCIO: 473442025
FECHA DE NEGOCIO: 27-03-2025

JERARQUÍA: TRIBUNAL SUPERIOR
DEPENDENCIA JUDICIAL: TRIBUNAL SUPERIOR DE TRABAJO
NÚMERO DE RESOLUCIÓN: ---
FECHA DE RESOLUCIÓN: 05-05-2025

4. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: ACCIONES CONTENCIOSO ADMINISTRATIVAS DE PLENA JURISDICCIÓN
NÚMERO DE NEGOCIO: 3302019
FECHA DE NEGOCIO: 15-05-2019
JERARQUÍA: CORTE SUPREMA DE JUSTICIA
MATERIA: SALA TERCERA CONTENCIOSO ADMINISTRATIVO Y LABORAL
DEPENDENCIA JUDICIAL: CORTE SUPREMA DE JUSTICIA
NÚMERO DE RESOLUCIÓN: --
FECHA DE RESOLUCIÓN: 15-09-2022

5. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: PROCESOS COMUNES
NÚMERO DE NEGOCIO: 583542025
FECHA DE NEGOCIO: 14-04-2025
JERARQUÍA: TRIBUNAL SUPERIOR
DEPENDENCIA JUDICIAL: TRIBUNAL SUPERIOR DE TRABAJO
NÚMERO DE RESOLUCIÓN: ---
FECHA DE RESOLUCIÓN: 19-06-2025
RAMA DEL DERECHO: LABORAL

6. INSTANCIA: RECURSO EXTRAORDINARIO
TIPO DE NEGOCIO: RECURSO DE CASACION
NÚMERO DE NEGOCIO: 656852020
FECHA DE NEGOCIO: 29-09-2020
JERARQUÍA: CORTE SUPREMA DE JUSTICIA
MATERIA: SALA PRIMERA DE LO CIVIL
DEPENDENCIA JUDICIAL: CORTE SUPREMA DE JUSTICIA
NÚMERO DE RESOLUCIÓN: --
FECHA DE RESOLUCIÓN: 03-12-2021
RAMA DEL DERECHO: CIVIL

7. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: PROCESOS CIVILES Y AGRARIOS
NÚMERO DE NEGOCIO: 781242024
FECHA DE NEGOCIO: 26-07-2024
JERARQUÍA: TRIBUNAL SUPERIOR
MATERIA: CIVIL
DEPENDENCIA JUDICIAL: TRIBUNAL SUPERIOR
NÚMERO DE RESOLUCIÓN:
FECHA DE RESOLUCIÓN: 18-12-2024

8. INSTANCIA: RECURSO EXTRAORDINARIO
TIPO DE NEGOCIO: RECURSO DE CASACIÓN
NÚMERO DE NEGOCIO: 1311182024
FECHA DE NEGOCIO: 16-02-2024
JERARQUÍA: CORTE SUPREMA DE JUSTICIA
MATERIA: SALA SEGUNDA DE LO PENAL
DEPENDENCIA JUDICIAL: CORTE SUPREMA DE JUSTICIA
NÚMERO DE RESOLUCIÓN: --
FECHA DE RESOLUCIÓN: 23-09-2024

9. INSTANCIA: SEGUNDA
PROVINCIA: PANAMÁ

TIPO DE NEGOCIO: PROCESOS COMUNES
NÚMERO DE NEGOCIO: 379972024
FECHA DE NEGOCIO: 11-04-2024
JERARQUÍA: TRIBUNAL SUPERIOR
DEPENDENCIA JUDICIAL: TRIBUNAL SUPERIOR DE TRABAJO
NÚMERO DE RESOLUCIÓN: ---
FECHA DE RESOLUCIÓN: 25-06-2024

10. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: PROCESOS COMUNES
NÚMERO DE NEGOCIO: 18132024
FECHA DE NEGOCIO: 05-01-2024
JERARQUÍA: TRIBUNAL SUPERIOR
MATERIA: TRABAJO
DEPENDENCIA JUDICIAL: TRIBUNAL SUPERIOR DE TRABAJO
NÚMERO DE RESOLUCIÓN:
FECHA DE RESOLUCIÓN: 30-04-2024

11. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: PROCESO DE PROTECCION AL CONSUMIDOR
NÚMERO DE NEGOCIO: 23412024
FECHA DE NEGOCIO: 05-01-2024
JERARQUÍA: TRIBUNAL SUPERIOR
DEPENDENCIA JUDICIAL: TERCER TRIBUNAL SUPERIOR - LIBRE COMPETENCIA Y ASUNTOS DEL CONSUMIDOR
FECHA DE RESOLUCIÓN: 07-02-2024

12. INSTANCIA: SEGUNDA
TIPO DE NEGOCIO: PROCESO DE PROTECCION AL CONSUMIDOR
NÚMERO DE NEGOCIO: 1220772023
FECHA DE NEGOCIO: 16-11-2023
JERARQUÍA: TRIBUNAL SUPERIOR
MATERIA: LIBRE COMPETENCIA
DEPENDENCIA JUDICIAL: TERCER TRIBUNAL SUPERIOR - LIBRE COMPETENCIA Y ASUNTOS DEL CONSUMIDOR
FECHA DE RESOLUCIÓN: 05-01-2024

Si tienen preguntas o desean mas información sobre este tema pueden contactarme a:
Licdo. Osvaldo Quintero V. - correo electrónico: tradslegal@outlook.com o a través de nuestros canales de whatsapp (6951-1835) e instagram (@tradslegal_panama).