

Nota sobre la obtención y uso de la firma electrónica en los informes de auditoría y otros documentos

La reciente declaración del estado de alarma por parte del gobierno para la gestión de la actual situación de crisis sanitaria ocasionada por el COVID-19, ha provocado un cambio en nuestra manera de trabajar impulsando el teletrabajo y la digitalización de los procesos. Por este motivo consideramos necesario emitir esta nota de carácter divulgativo acerca del uso de la firma digital en distintos ámbitos y especialmente de la firma digital reconocida por ser esta la que tiene la misma validez que la manuscrita.

No obstante lo anterior, los procedimientos y las soluciones tecnológicas a las que se hace mención en el presente documento no son los únicos que actualmente existen y, por ello, es responsabilidad del firmante y de quien vaya a confiar en dicha firma el evaluar en función de cada caso y a medida que el tiempo transcurra, cuales son y serán los procedimientos y soluciones que mejor consigan el grado de seguridad exigido atendiendo a sus circunstancias particulares y a la organización interna del despacho o firma correspondiente.

El presente documento, que tiene carácter meramente informativo y en modo alguno puede considerarse vinculante, expresa el criterio del ICJCE sobre la materia tratada, sin perjuicio del superior criterio del ICAC, de cualesquiera otras Administraciones Públicas competentes y de los Juzgados y Tribunales. Este escrito ha sido preparado únicamente para asistir a nuestros miembros en relación con esta materia y no debe suplir o sustituir el conocimiento de la normativa aplicable y, en particular, la reguladora de contabilidad y/o auditoría de cuentas, así como la reflexión personal del censor y su juicio profesional. El ICJCE declina toda responsabilidad y obligación en que se pueda incurrir, directa o indirectamente, como consecuencia del uso y aplicación de este documento.

En esta nota abordaremos los siguientes temas:

- I. Aspectos Jurídicos
- II. Firma electrónica cualificada o reconocida
 - a. ¿Cómo obtengo la firma electrónica reconocida?
 - b. ¿Cómo utilizo la firma electrónica reconocida?
 - c. ¿Qué necesito para usar el DNle y DNI 3.0?
- III. Firma electrónica cualificada o reconocida en los informes de auditoría
- IV. Firma electrónica en la formulación de las cuentas anuales y en otros documentos
- V. ¿Cómo valido la firma electrónica que contiene un documento digital?
- VI. ¿Cómo elaboro el juego del informe de auditoría y las cuentas anuales?
- VII. Sello del ICJCE
- VIII. Enlaces de interés

I. Aspectos jurídicos

El marco jurídico regulador de la firma electrónica parte fundamentalmente de dos normas, una de ámbito nacional y otra de ámbito europeo: la Ley 59/2003, de 19 de diciembre, de firma electrónica, cuya última modificación data de 2019 (en adelante LFE), y el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento e-IDAS).

Sin ánimo de hacer aquí un análisis detenido del régimen jurídico de la firma electrónica, sí conviene identificar algunos conceptos clave, como el de firma electrónica y documento electrónico, las distintas clases de unas y otros, así como los principales efectos jurídicos que les atribuyen las normas indicadas.

A) Firma electrónica

1. Concepto y clases: Los artículos 3 de la LFE y 3 del Reglamento e-IDAS definen la firma electrónica y contemplan tres clases de firma electrónica:

a) La **firma electrónica** (a veces identificada como firma electrónica **simple**) es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

b) La **firma electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control.

c) La **firma electrónica cualificada (o reconocida)** es la firma electrónica avanzada basada en un certificado cualificado (o reconocido) y generada mediante un dispositivo cualificado o seguro de creación de firma.

2. Firma en nombre propio o en representación. El firmante es la persona que utiliza un dispositivo de creación de firma y puede actuar bien en nombre propio o bien en nombre de una persona física o jurídica a la que representa.

Para firmar **en nombre de una persona jurídica** se puede solicitar un certificado electrónico de la persona jurídica (art. 7 de la LFE).

Según la LFE, los datos de creación de esa firma en nombre de una persona jurídica solo podrán ser utilizados en el ámbito del giro o tráfico ordinario de la persona jurídica y en sus relaciones con las Administraciones públicas. Además, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia (lo que figurará en el certificado electrónico). Los actos o contratos en que se utilice la firma de la persona jurídica dentro de tales límites se entenderán hechos por la persona jurídica. Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica sólo quedará vinculada frente a terceros si los asume como propios o se hubiesen celebrado en su interés; en caso contrario se podrá desencadenar la responsabilidad del responsable de su custodia y de quien la utilizó (art. 7 de la LFE).

La LFE también regula los datos que han de contener los certificados electrónicos reconocidos (tales como la identificación del firmante, periodo de validez, límites de uso del certificado, límites del valor de las transacciones para las que puede utilizarse el certificado, etc.). Si el certificado reconocido admite una relación de representación, según el artículo 11.4 de la LFE debería incluir una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales. Si bien, esto en la práctica puede no suceder. De tal forma que es posible obtener un certificado de persona física representante de jurídica, de la Fábrica Nacional de Moneda y Timbre (FNMT) por ejemplo, que no contendrá esa información. También porque, en general, las aplicaciones informáticas destinatarias de hacer uso de esa información no están preparadas para ello.

También regula la LFE el **documento nacional de identidad electrónico (DNIe)**, que acredita electrónicamente la identidad personal de su titular, y permite la firma electrónica cualificada de documentos. Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del DNI-e para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

3. Efectos jurídicos. En relación con los efectos jurídicos de la firma electrónica, cabe destacar lo siguiente:

- a) No se pueden denegar efectos jurídicos (ni se puede inadmitir como prueba en procedimientos judiciales) a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada (art. 25.1 del Reglamento e-IDAS y art. 3.9 de la LFE).
- b) Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita (art. 25.2 del Reglamento e-IDAS y art. 3.4 de la LFE). Además, si se basa en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros.
- c) Ello no impide que se pueda impugnar la autenticidad de una firma electrónica; en tal caso se realizarán las comprobaciones correspondientes, de acuerdo con lo dispuesto en el art. 3.8 de la LEF y en la Ley de Enjuiciamiento Civil, en materia de prueba.

También está prevista la utilización de la firma electrónica en el seno de las Administraciones públicas, en las relaciones entre éstas, y en las relaciones de las Administraciones públicas con los particulares. Su regulación general está incorporada a la Ley 39/2015 (en particular, para la identificación y firma de los interesados) y a la Ley 40/2015 (arts. 38 ss., sobre funcionamiento electrónico del sector público).

B) Documento electrónico

Un documento electrónico es una información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico. Al igual que sucede con los documentos en papel, el documento electrónico puede tener distinta naturaleza:

1. Documentos **públicos**: firmados electrónicamente por funcionarios dotados de fe pública judicial, notarial o administrativa, en el ámbito de sus competencias y con los requisitos exigidos por la ley.
2. Documentos **administrativos**: firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones, conforme a su legislación específica.
3. Documentos **privados**: los que no tienen carácter público ni administrativo (es decir, los firmados electrónicamente por sujetos privados, o bien por funcionarios o empleados públicos al margen de sus funciones o sin los requisitos establecidos legalmente).

En cuanto a sus **efectos jurídicos**, tales documentos tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza (públicos, administrativos o privados), de conformidad con la legislación aplicable a cada uno de ellos (art. 3.7 de la LEF), de forma que no se pueden

denegar efectos jurídicos (ni inadmitir como medio de prueba) a un documento electrónico por el mero hecho de estar en formato electrónico (art. 45 del Reglamento e-IDAS).

En todo caso, lo dispuesto en la LFE no modifica la regulación de las funciones que corresponden a los funcionarios que tengan legalmente la **facultad de dar fe** en documentos, en lo que se refiere al ámbito de sus competencias siempre que actúen con los requisitos exigidos en la ley. Pero, en el ámbito de la documentación electrónica, *“corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa”* (disposición adicional primera de la LEF).

II. Firma electrónica reconocida

El Instituto Nacional de Ciberseguridad de España (INCIBE, sociedad dependiente del Mº de Asuntos Económicos y Transformación Digital) nos explica en el siguiente [enlace](#) qué es una firma electrónica cualificada o reconocida, cómo obtenerla y cómo usarla. A continuación, resumimos los principales pasos:

Para poder realizar firma electrónica cualificada, previamente, será necesario contar con un certificado digital como por ejemplo FNMT o el del DNI electrónico (DNIE), que autentica, — mediante una pareja de claves en un fichero software o en tarjeta inteligente— la identidad (como persona física o jurídica) del firmante. Estos certificados son emitidos por una entidad emisora de certificados de confianza pública que dan fe de que el portador del certificado es quien dice ser. Existen varias autoridades de certificación o prestadores de servicios electrónicos de confianza (véase *enlace* en el siguiente apartado) como son: la citada FNMT, la Agencia de Tecnología y Certificación Electrónica de la Generalitat Valenciana, la Agència Catalana de Certificació, la Dirección General de la Policía (para el DNI), etc. No obstante, los certificados emitidos por estos prestadores de servicios electrónicos de confianza no determinan, por sí solos, que la firma electrónica generada sea reconocida, ya que para ello requieren la utilización de un dispositivo cualificado o seguro de creación de firma.

Las entidades certificadoras expiden distintos tipos de certificados, dependiendo de si el solicitante es un ciudadano, **un representante de una empresa** (persona jurídica, de entidad sin personalidad jurídica y, para administradores únicos y solidarios) o un empleado público.

a) ¿Cómo obtengo la firma electrónica reconocida?

Lo primero que necesitas es un certificado electrónico reconocido, existen dos tipos:

- **DNI Electrónico (DNIE y DNI3.0)**
- **Otros tipos de certificados:** El listado completo de los prestadores de servicios electrónicos de confianza cualificados reconocido por el Mº de Asuntos Económicos y Transformación Digital lo puedes consultar en el siguiente [enlace](#).

1. **Realizar una solicitud online.** Al final de este proceso se obtiene un código que será necesario para poder acreditar tu identidad. A este respecto, es muy importante que solicitud y descarga sucedan en el mismo ordenador/navegador y si es posible que tengan lugar los mínimos cambios posibles en ese tiempo para evitar que se invalide la misma.
2. **Presentarse en una Oficina de Registro para acreditar tu identidad.** Para el DNI tendrás que personarte en las oficinas de la D.G. de la Policía. **Si solicitas un certificado de representante**

de una empresa, además debes acreditar la existencia de la entidad, que tienes el poder de representación y su vigencia (Ver el siguiente [enlace](#) para la obtención de certificados electrónicos para empresas). La Agencia Tributaria actúa como Oficina de Registro de los certificados emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT, prestador de servicios electrónicos de confianza reconocido por el Mº de Asuntos Económicos y Transformación Digital). También hay Oficinas de Registro en la Tesorería General de la Seguridad Social, la Comisión Nacional del Mercado de Valores (CNMV) o en la Comunidad Foral de Navarra. Puedes buscar la Oficina de Registro para acreditar tu identidad en el siguiente [enlace](#).

3. **Descargar el Certificado.** Para ello, habrá sido necesario realizar el registro presencial y estar en posesión del código obtenido en el primer paso que permitirá descargar el certificado vía Internet en un dispositivo cualificado o seguro de creación de firma.

b) ¿Cómo utilizo la firma electrónica reconocida?

El INCIBE nos indica en el siguiente [enlace](#) que una vez que dispones de un certificado electrónico la firma se puede realizar de dos formas:

- online, a través de un servicio cualificado o seguro de verificación y generación de firmas electrónicas como es **VALIDe** (En relación con los portales online de firma, debe valorarse el riesgo que implica “subir” nuestro archivo a ese portal. Es importante validar los términos de uso, política de confidencialidad, etc. Este riesgo no suele manifestarse en las versiones de escritorio pues el archivo nunca sale de nuestro PC durante el proceso de firma);
- a través de **aplicaciones de firma electrónica** o de **ofimática** siempre que, tras ser descargadas y ejecutadas en un ordenador, permitan realizar de forma segura firmas de documentación sin la necesidad de estar conectado a internet.

Es importante que se valore la necesidad de usar herramientas de firma digital que soporten LTV (long term validation) ya que, este tipo de herramientas, garantizan la posibilidad de validar la firma electrónica a partir del momento en que caduca el certificado que se usa para la firma digital.

Ahora bien, no es la única forma de disponer de garantías, así en el caso de auditoría si en el momento de obtención de las cuentas anuales e informe de gestión firmados digitalmente se genera una copia imprimible, a través de la misma se podrá evidenciar la validez de la firma en el momento de la obtención del documento. Así se ha de conservar en los papeles de auditoría un doble juego, (versión digital e imprimible), de forma que permite, sin que sea necesario exigir el LTV, evidenciar la validez del documento firmado.

c) ¿Qué necesitas para usar el DNle y DNI 3.0?

En el siguiente [enlace](#) de la Dirección General de la Policía se detallan los elementos hardware y software que son necesarios para la utilización tanto del DNle como del DNI 3.0.

Para la utilización de esta tipología de DNI, es necesario contar con determinados elementos de hardware y software que nos van a permitir el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

Mientras que el DNle sólo permite el acceso mediante contacto, el DNI 3.0 dispone de un chip Dual interface, que permite también la conexión inalámbrica a través de la antena NFC.

III. Firma electrónica reconocida en los informes de auditoría

En la normativa de auditoría no se hace ninguna mención al tipo de firma (manuscrita o electrónica) que se debe incluir en el informe de auditoría de cuentas anuales, ni tampoco impide que se utilice ninguna de ellas, y únicamente contempla aspectos relacionados con quién debe firmar ese informe y la fecha en que se firma el mismo.

El ICAC ya contestó en su consulta 3 de auditoría del BOICAC 120 la posibilidad de firmar los informes de auditoría de cuentas mediante firma electrónica, pero considerando que, en el caso de utilizar firma electrónica, ésta deberá cumplir las condiciones y características exigidas por la Ley 59/2003, de 19 de diciembre, para la firma electrónica reconocida (para ello deberá estar basada en un Certificado Reconocido por Ministerio de Asuntos Económicos y Transformación Digital), al ser esta la que tiene la misma validez que la firma manuscrita; señala también que el hecho de que el informe de auditoría se firme electrónicamente no afecta al régimen regulado sobre esta materia en la normativa reguladora de la actividad de auditoría.

Y ello, tanto en los supuestos de auditores de cuentas personas físicas, en los que serán dichos auditores quienes deberán firmar personalmente el informe de auditoría, como en los de sociedades de auditoría, en los que el informe de auditoría deberá firmarse por el auditor o auditores principales responsables designados a tal efecto por la sociedad en cuyo nombre actúan.

Por tanto, la firma electrónica reconocida de un auditor persona física debe ser utilizada para la firma electrónica de informes de auditoría por los **auditores individuales**. En el caso de sociedades de auditoría, **se recomienda habilitar** a favor del auditor o auditores principales responsables designados **el correspondiente certificado electrónico de persona física representante de persona jurídica para actuar en nombre de una sociedad de auditoría** a efectos del informe de auditoría **y que se utilice**, cuando dichos auditores firmen en nombre de la sociedad. La habilitación de estos certificados con poderes específicos para la firma de informes de auditoría o con poderes más amplios deberá ser evaluado por cada despacho en función de las necesidades y circunstancias de cada caso debiendo implementarse los controles internos que se consideren necesarios.

No obstante y debido a las fuertes restricciones de movilidad y dificultades de obtención de firmas electrónicas reconocidas provocadas por el COVID-19, las sociedades de auditoría pueden permitir, sujeto a sus políticas internas, el uso de la firma electrónica reconocida de persona física por los **auditores principales responsables designados** a tal efecto por una sociedad de auditoría cuando actúen en nombre de la sociedad **siendo necesario**, al igual que se requiere con el certificado electrónico de personas jurídicas, que tengan **en vigor el poder de representación** de la sociedad de auditoría a efectos de los encargos de auditoría que firmen en nombre de la sociedad (poder que, en su caso, deberá estar debidamente inscrito en el Registro Mercantil), y que, conste en el informe de auditoría la razón social y el número de ROAC de la sociedad en cuyo nombre actúan.

La firma electrónica de cualquier documento deja constancia de la fecha, e incluso de la hora, minuto y segundo en la que se firma electrónicamente el archivo electrónico, que se corresponde con la que figura en el ordenador desde el que se realiza la firma. Así para la firma electrónica de los informes de auditoría tenemos que atender a la normativa de auditoría.

La Ley 22/2015 de Auditoría de Cuentas (LAC), en su artículo 5. Informe de auditoría de cuentas anuales, en su apartado 1.g) dice:

“5.1.g) Fecha y firma de quien o quienes lo hubieran realizado. La fecha del informe de auditoría será aquella en que el auditor de cuentas y la sociedad de auditoría han completado los procedimientos de auditoría necesarios para formarse una opinión sobre las cuentas anuales”.

IV. Firma electrónica en la formulación de las cuentas anuales y en otros documentos

La actual situación de crisis sanitaria y las medidas adoptadas por los gobiernos para combatirla (especialmente, en España, la declaración de estado de alarma mediante el Real Decreto 463/2020, de 14 de marzo) están provocando dificultades especiales en las entidades a la hora de formular las cuentas anuales por los medios tradicionales (reuniones presenciales de los Administradores y firma manuscrita de las cuentas anuales). En este sentido, hay que considerar que los administradores pueden no tener habilitada la firma electrónica que les permita la firma de las cuentas anuales en formato digital en cuyo caso podría considerarse como evidencia de la adecuada formulación de las cuentas una certificación del secretario del consejo de administración en la que se deje constancia del acuerdo tomado por el consejo de administración respecto de la formulación de las cuentas anuales, así como de la conformidad con las cuentas de todos los administradores o, en caso contrario, de los reparos expresados (para estos casos, ver [Circular ES04/2020 Nota técnica sobre la posible falta de firma de los administradores de las cuentas anuales y el informe de gestión sobrevenida por el COVID-19](#)).

Por tanto, en los casos en los que los administradores tengan habilitada la firma electrónica reconocida, todo lo indicado en relación con la obtención y uso de dicha la firma electrónica debe ser también tenido en cuenta en estos casos.

En aquellas ocasiones en las que se esté actuando en representación del administrador persona jurídica **se recomienda habilitar** a favor del representante **el correspondiente certificado electrónico de persona física representante de persona jurídica para actuar en nombre de esta y que se utilice** en lugar de utilizar la firma electrónica reconocida de persona física como pueda ser el DNle.

En el caso de que las cuentas anuales hayan sido formuladas con firmas electrónicas avanzadas nos tenemos que cuestionar la validez de dichas firmas. No obstante, como hemos expuesto en el apartado I “Aspectos jurídicos”, la firma avanzada, permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control. Adicionalmente, de acuerdo con el art. 25.1 del Reglamento e-IDAS, no se pueden denegar efectos jurídicos (ni se puede inadmitir como prueba en procedimientos judiciales) a una firma electrónica por el mero hecho de ser electrónica o porque no cumpla los requisitos de la firma electrónica cualificada. En este contexto, podremos aceptar estas cuentas como formuladas, siempre que se realicen procedimientos de auditoría complementarios que permitan minimizar los riesgos derivados del uso de una firma con menor nivel de garantías.

Existen prestadores de servicios electrónicos de confianza que proporcionan la firma electrónica avanzada y que es utilizada más habitualmente por las entidades para la firma de otros documentos distintos a las cuentas anuales y que no requieren el grado de seguridad que otorga la firma electrónica reconocida. Las cuentas anuales es un documento que por tener efectos frente a terceros y ser público (al requerir su depósito en el registro mercantil) se aconseja, en

todo caso, ser firmado mediante la firma que otorga el mayor grado de seguridad, la firma electrónica reconocida o alternativamente se realicen procedimientos de auditoría complementarios tendentes a cubrir los riesgos de la utilización de una firma avanzada, básicamente orientados a validar la identidad de la persona que efectivamente realizó la firma electrónica (comprobación de certificaciones emitidas por plataformas de gestión de firmas, cartas de confirmación de firma firmadas manualmente, verificación del origen del fichero electrónico, etc.).

V. ¿Cómo valido la firma electrónica que contiene un documento digital?

Firma electrónica reconocida:

La validación de una firma electrónica es el proceso por el que se comprueba la **identidad del firmante**, la **integridad del documento firmado** y la **validez temporal del certificado utilizado**. Las dos primeras verificaciones se pueden realizar desde una aplicación sin conexión a internet simplemente utilizando el certificado incluido en la misma firma. Pero, ¿cómo sabemos si ese certificado es válido?, ¿estaba revocado en el momento de la firma? o ¿si la Autoridad que lo emitió es de confianza?. El proceso de validación de la firma no puede separarse del proceso de validación del certificado usado para la firma. Y por eso, la validación de la firma, implica también la validación del certificado.

Por tanto, las tres validaciones dependen de la capacidad de validar el certificado, para lo cual es necesaria una conexión a internet que permita acceder a una plataforma de validación de certificados como puede ser **VALIDe**.

En este sentido, el proceso de validación podría constar de dos fases:

- a) Validación a través de las propiedades del propio documento digital firmado electrónicamente, verificando identidad del firmante, integridad del documento, que el mismo no ha sufrido alteraciones desde el momento en que se firmó, tipo de certificado utilizado, emisor del certificado (esto último con el fin de chequear posteriormente si el emisor es un prestador de servicios electrónico de confianza); y, si se considera necesario
- b) Validación a través de una plataforma de validación de firma como VALIDe que además de realizar una validación electrónica permite la generación del correspondiente justificante de validación o versión imprimible del documento y que, en el caso de que el firmante no haya utilizado una firma con LTV puede servir de evidencia de la comprobación realizada sobre la validez una vez el certificado haya expirado en el futuro.

De cara al uso de una plataforma de validación como VALIDe, debemos prestar atención a nuestro deber de confidencialidad y hay que advertir que este tipo de webs de validación de firmas exigen subir el archivo a la plataforma antes de descargar el justificante de validación de la firma, por lo que se debería obtener previamente la correspondiente autorización la entidad. Alternativamente, se podría solicitar a la entidad que sea ella quien realice el proceso de validación a través de la plataforma VALIDe y nos remita, junto con el fichero digital, el fichero imprimible obtenido como justificante de la validación, de forma que se puedan realizar y documentar las dos fases del proceso de validación indicadas anteriormente.

En el siguiente **enlace** se detallan algunas cuestiones de interés en relación con la validación de firmas.

Firma electrónica avanzada:

Como hemos comentado anteriormente, en el caso de firmas electrónicas avanzadas, habrá que evaluar la necesidad de realizar procedimientos de auditoría complementarios en función de las circunstancias (tipo de documentación a validar y herramientas informáticas y servicios electrónicos de confianza utilizados) y con el objeto de minimizar los riesgos derivados del uso de una firma con menor nivel de garantías.

VI. ¿Cómo elaboro el juego del informe de auditoría y las cuentas anuales?

El artículo 5.4 de la LAC indica:

“El informe de auditoría de cuentas anuales deberá ir acompañado de la totalidad de documentos que componen las cuentas objeto de auditoría y, en su caso, del informe de gestión. La publicación de estos documentos, junto con el informe de auditoría, se regirá por lo dispuesto en el marco normativo de información financiera que resulte aplicable.”

A la hora de firmar electrónicamente un informe de auditoría tenemos que tener cuidado de no incumplir la legislación vigente. Por ello, se recomienda incorporar la firma electrónica reconocida únicamente y exclusivamente en el informe de auditoría (en la misma página que aparecería la firma manuscrita) y luego proceder a montar el juego de documentos que componen el informe de auditoría junto con las cuentas anuales, en lugar de juntar ambos documentos en uno solo y proceder a su firma ya que el documento entero quedaría firmado electrónicamente por el auditor, es decir la firma del auditor también quedaría reflejada en las cuentas anuales formuladas y firmadas por los administradores.

A la hora de montar este juego de informe de auditoría y cuentas anuales se pueden dar distintas combinaciones:

		Cuentas anuales	
		Con firma manuscrita	Con firma electrónica
Informe de auditoría	Con firma manuscrita	<i>Situación 1</i>	<i>Situación 2</i>
	Con firma electrónica	<i>Situación 3</i>	<i>Situación 4</i>

a) Situación 1:

Ante esta situación, una vez tengamos las cuentas anuales originales válidamente formuladas y nuestro informe de auditoría original, ambos con firma manuscrita, si el cliente necesita tener una copia de ambos para poder presentarlo a entidades financieras u otros organismos, excepcionalmente y dada la situación de alarma se le podría enviar un documento en PDF del juego de informe de auditoría junto con las cuentas anuales y guardarnos el original, para enviar en paralelo o a la mayor brevedad posible al menos un juego original.

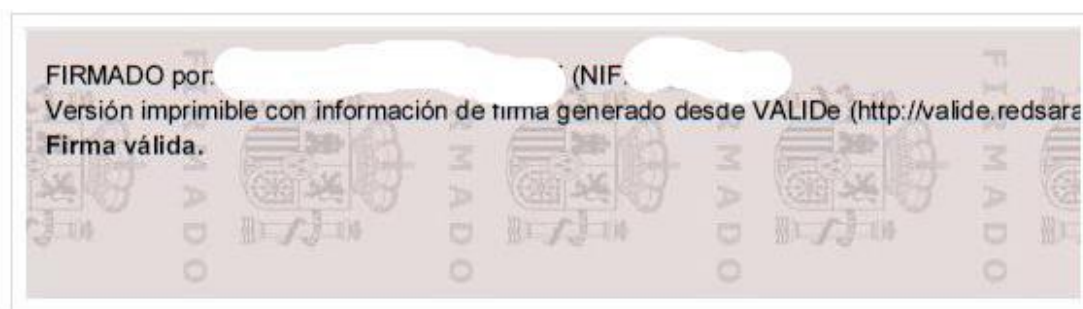
b) Situación 2:

En esta situación, al tener ambos documentos firmados de manera distinta debemos proceder a generar una copia imprimible de las cuentas anuales (debiendo tenerse en cuenta lo indicado en el apartado V anterior en relación con el riesgo de confidencialidad y la alternativa de que

sea el cliente quién nos proporcione el fichero imprimible procedente de VALIDe) a través de una plataforma de validación de certificados como puede ser VALIDe (cabría asimismo la posibilidad de obtención de una copia imprimible a través de alguna otra plataforma que no necesariamente sea una plataforma de validación), en cuyo caso, el proceso a seguir sería el siguiente:

1. Se accede al servicio de **Validar Firma** donde se subirá el archivo firmado digitalmente y se da a la opción validar.
2. Una vez realizada la validación de la firma digital la plataforma indica si la firma es válida.
3. Se activa un aviso de “descargar justificante” que se descarga y deberá guardarse en el equipo con extensión pdf.

La versión imprimible del archivo firmado digitalmente tiene otra firma digital de los Servicios de Firma Electrónica e Identidad Digital que incorpora una banda en la que consta lo siguiente:



Si se sigue el mencionado procedimiento, esta será la versión imprimible del documento.

Posteriormente, procederemos a montar un juego en formato físico de ambos documentos (copia imprimible de las cuentas anuales firmadas electrónicamente más el informe de auditoría firmado de forma manuscrita). En todo caso, el auditor deberá mantener las cuentas anuales firmadas electrónicamente. Al igual que en la Situación 1, excepcionalmente y dada la situación de alarma se podría enviar un documento en PDF del juego de informe de auditoría junto con las cuentas anuales y guardarnos el original, para enviar en paralelo o a la mayor brevedad posible al menos un juego original.

c) Situación 3:

En este caso al ser el informe de auditoría el documento firmado electrónicamente se elaborará un juego electrónico compuesto por el informe de auditoría firmado electrónicamente más copia electrónica de las cuentas anuales, en los términos descritos en la situación 4 y que será entregado a la entidad. Nosotros deberemos mantener en, todo caso, un original de las cuentas anuales firmadas manuscritas.

d) Situación 4:

En esta situación, primero de deben firmar electrónicamente los dos documentos por separado y posteriormente reunirlos en una unidad PDF integrada a través de un programa informático que lo permita como puede ser, por ejemplo, Adobe Acrobat Prosiguiendo los siguientes pasos:

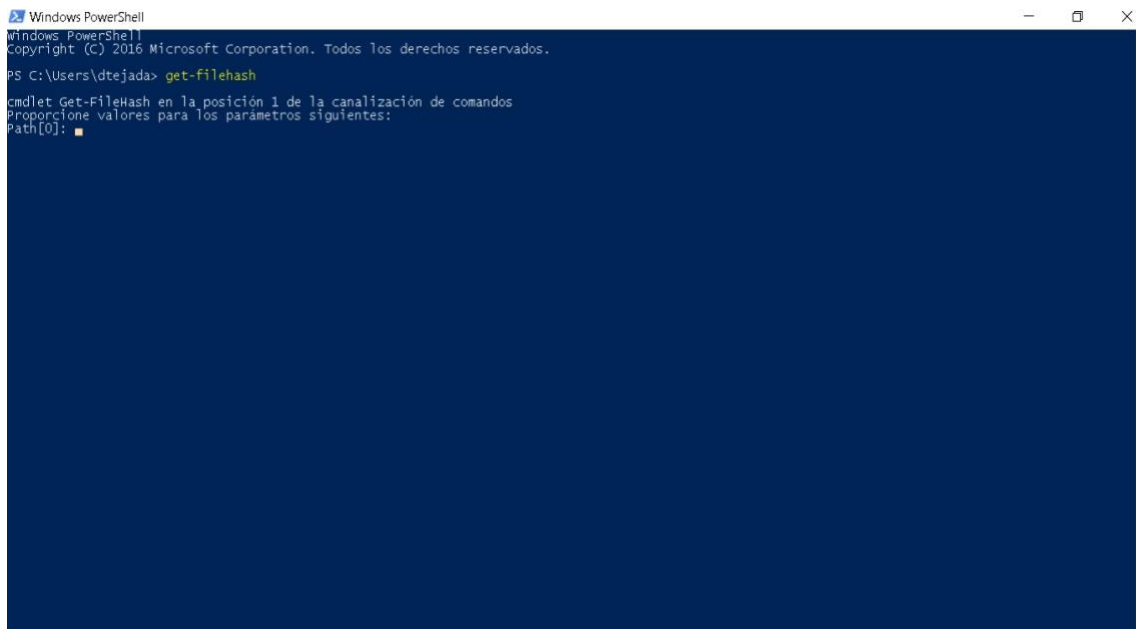
1. Abrir el menú Herramientas de Adobe pro y selecciona Archivo/Crear cartera PDF.

2. Añadir archivos: haz clic en “Agregar archivos” y selecciona los archivos que deseas incluir en tu PDF.
3. Guardar la cartera pdf creada a través de la opción de guardar siendo esta cartera la que debemos enviar a la entidad.

Posteriormente a la generación de la cartera o portfolio, y con anterioridad a su envío al cliente por correo electrónico, es conveniente asegurar la integridad de este archivo electrónico (Portfolio PDF). Una forma de hacerlo es calculando el código hash de dicho archivo, guardándolo como parte del protocolo interno del portfolio y su posterior envío al cliente. En la medida en que el Portfolio PDF no sufra modificaciones, cálculos posteriores del código hash de ese mismo archivo arrojarán el mismo resultado y tendremos por tanto la certeza de que el archivo electrónico no ha sufrido ningún tipo de alteración, pues si hubiera sucedido, por pequeña que fuera, el código hash resultante tras la modificación sería distinto. En este sentido, es importante que en el correo electrónico que se envíe al cliente adjuntando el Portfolio se informe del código hash correspondiente a dicho archivo, que permite asegurar la integridad del mismo.

Para calcular el código hash de un archivo se pueden utilizar múltiples soluciones. Los sistemas operativos Linux, Mac o windows lo tienen posibilitado desde su propio sistema operativo a través de diferentes líneas de comando, por ejemplo, en el caso de windows, se puede calcular a través del command let (cmdlet) de Microsoft PowerShell Get-FileHash, tal y como se indica a continuación:

- Ejecutar Windows Powershell, en el buscador de programas, escribir powershell y abrirlo.
- Escribir get-filehash y pulsar enter, momento en el que aparecerá la siguiente secuencia de datos.

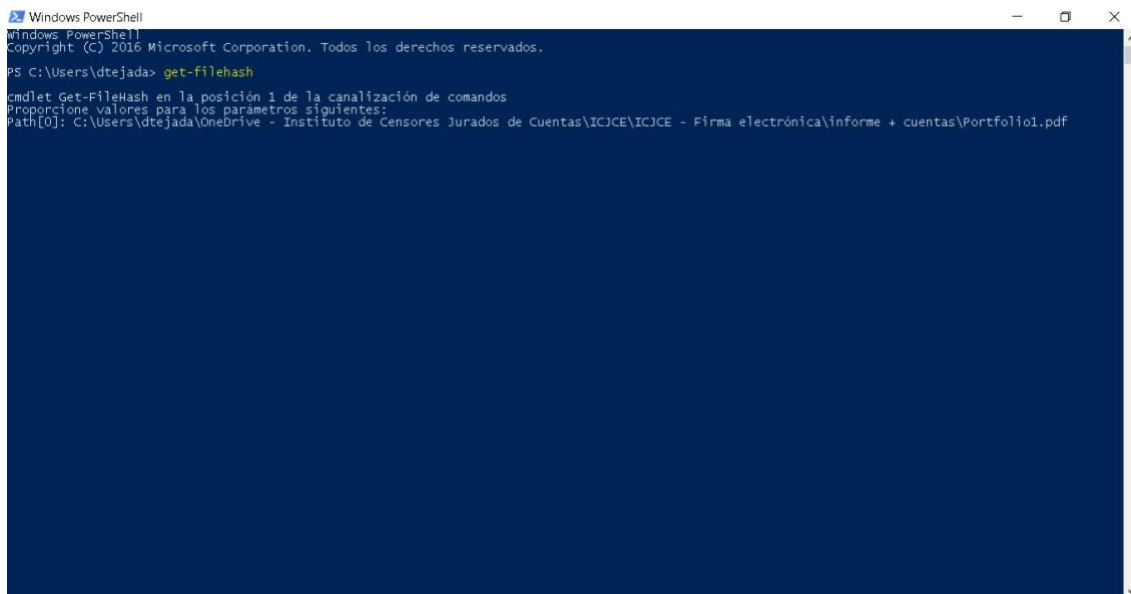


```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\dtejada> get-filehash

cmdlet Get-FileHash en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
Path[0]:
```

- Escribir \ruta\nombre exacto del archivo en el espacio habilitado para ello, es decir después de Path [0], tal y como se muestra en el ejemplo:

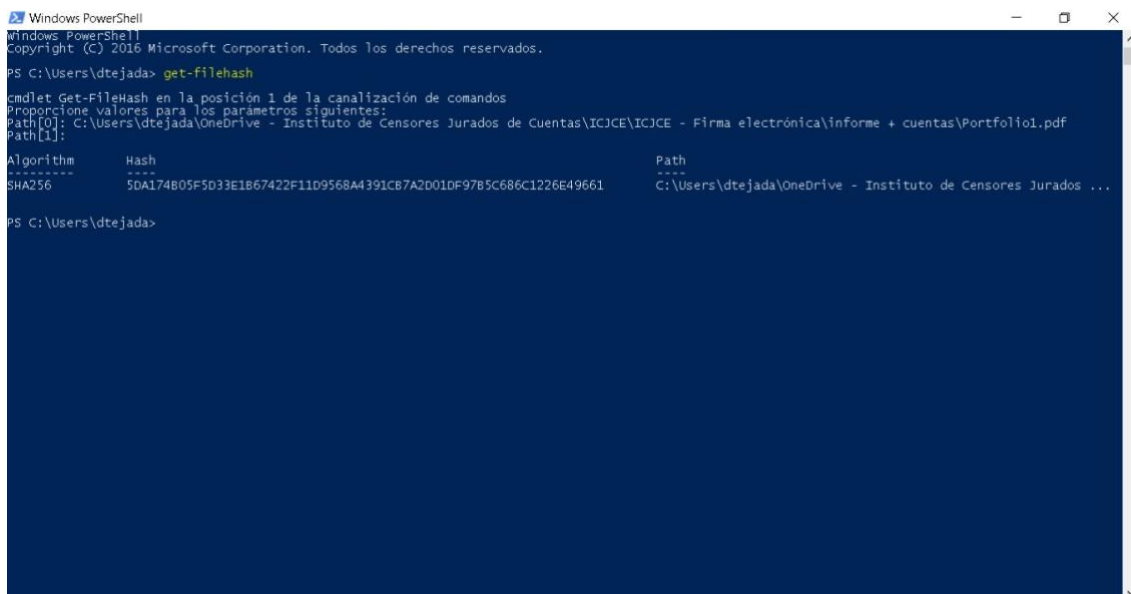


```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\dtejada> get-filehash

cmdlet Get-FileHash en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
Path[0]: C:\Users\dtejada\OneDrive - Instituto de Censores Jurados de Cuentas\ICJCE\ICJCE - Firma electrónica\informe + cuentas\Portfolio1.pdf
```

- Una vez escrita la ruta y el nombre del archivo pulsar enter, en ese momento dará la opción de introducir un segundo archivo, si no se cumplimentan más datos y se vuelve a pulsar enter el programa calculará el hash del archivo:



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\dtejada> get-filehash

cmdlet Get-FileHash en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
Path[0]: C:\Users\dtejada\OneDrive - Instituto de Censores Jurados de Cuentas\ICJCE\ICJCE - Firma electrónica\informe + cuentas\Portfolio1.pdf
Path[1]:

Algorithm      Hash                                     Path
-----
SHA256         5DA174B05F5D33E1B67422F11D9568A4391CB7A2D01DF97B5C686C1226E49661  C:\Users\dtejada\OneDrive - Instituto de Censores Jurados ...

PS C:\Users\dtejada>
```

VII. El sello del ICJCE

Como consecuencia de la crisis del COVID-19 y ante la imposibilidad de disponer físicamente del sello éstos se seguirán solicitando a las distintas agrupaciones donde se comunicará al solicitante el número o números de los sellos solicitados y en el informe de auditoría hay que hacer la siguiente mención en el mismo lugar en el que habitualmente se inserta el sello físico:

"Este informe se corresponde con el sello distintivo nº xx/xx/xxxxx emitido por el Instituto de Censores Jurados de Cuentas de España."

Esta información se detalla en la [Circular G04/2020](#).

Este mismo procedimiento se seguirá en el caso de emisión de informes de auditoría con firma digital.

VIII. Enlaces de interés:

<https://firmaelectronica.gob.es/Home/Ciudadanos/SubHomeCosasDeberiasSaber.html>

<https://www.sede.fnmt.gob.es/certificados>

<https://valide.redsara.es/valide/>

<https://www.incibe.es/protege-tu-empresa/blog/sabes-utilizar-firma-electronica>

https://sede.sepe.gob.es/contenidosSede/generico.do?pagina=firma/ayuda_firma_autoridades.html

<https://sede.minetur.gob.es/es-es/firmaelectronica/Paginas/firma.aspx>