AUDITORES

INSTITUTO DE CENSORES JURADOS DE CUENTAS DE ESPAÑA

RESUELVE TUS DUDAS SOBRE EL ARCHIVO ELECTRÓNICO, LA COMPILACIÓN E IDENTIFICACIÓN DEL ARCHIVO COMPILADO Y SU POSIBLE MODIFICACIÓN POSTERIOR

Colección Ideas de Gestión

Marzo de 2022

Este documento ha sido preparado por la Comisión Depymes del Instituto de Censores Jurados de Cuentas de España.

ISBN: 978-84-17367-30-5

INDICE

1. INTRODUCCIÓN

El artículo 29.2 de la Ley 22/2015, de 20 de julio de Auditoría de Cuentas (LAC) recoge dos requerimientos de especial interés para los profesionales del sector, en particular, la elaboración de un archivo de auditoría por cada trabajo de auditoría de cuentas y el cierre del archivo de auditoría en un plazo de 60 días, lo que se conoce como plazo de compilación.

A este respecto, el Real Decreto 2/2021, de 12 de enero, por el que se aprueba el Reglamento de desarrollo de la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas (RLAC), ha incorporado requerimientos tales como: creación de un archivo electrónico de auditoría; imposibilidad de modificar el mismo después de la fecha del informe de auditoría; identificación única del archivo de auditoría compilado y evidencia de la fecha de compilación; generación de un archivo complementario en el caso de que sea necesario modificar un archivo de auditoría compilado; así como la custodia, accesibilidad y recuperabilidad de la documentación de auditoría.

No obstante, muchas de estas cuestiones que parecen novedosas, ya estaban contempladas en la NIA ES 230 sobre Documentación de auditoría, que establece en los apartados 14 a 16 qué es la compilación, qué se puede hacer tras compilar un archivo y cómo actuar en el caso de modificar un archivo compilado. Asimismo, la Norma Internacional de Gestión de la Calidad 1 (NIGC 1 ES) Gestión de la calidad en las firmas de auditoría que realizan auditorías de estados financieros, también trata la compilación y el archivo de la documentación del encargo.

Conforme a la normativa aplicable brevemente reseñada, se pone de manifiesto la necesidad de tener adecuadamente diseñadas e implementadas políticas y procedimientos para: la creación de un archivo electrónico; la compilación e identificación del archivo compilado y su posible modificación posterior; así como para la custodia y accesibilidad del archivo de auditoría.

Si bien los programas de auditoría suelen incorporar estas funcionalidades y por ello son una solución que aporta solidez organizativa al proceso de documentación y archivo, este documento de ayuda pretende dar a conocer otras soluciones que existen en el mercado, de forma que el auditor pueda abordar los requerimientos normativos antes mencionados de una forma sencilla si no dispone de un programa de auditoría o si este no tiene implementadas determinadas funcionalidades.

2. REFERENCIA NORMATIVA

La normativa que plantea los requerimientos que han generado las cuestiones a tratar en este documento son:

Ley 22/2015, de 20 de julio de Auditoría de Cuentas (LAC): Artículo 29, apartado 2.

Real Decreto 2/2021, de 12 de enero, por el que se aprueba el Reglamento de desarrollo de la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas (RLAC): Artículo 67, apartado 2 letra g); artículo 69 apartados 2 y 3; y artículo 72, apartado 2.

NIA-ES 230 sobre Documentación de auditoría: Apartados 14 a 16 y apartados A21 a A24 de la Guía de aplicación.

NIGC 1 ES Norma internacional de gestión de la calidad en las firmas de auditoría que realizan auditorías de estados financieros: Apartado 31 f) y apartados A83 a A85 de la Guía de aplicación.

3. PASOS A SEGUIR

1. REVISAR LA DOCUMENTACIÓN DEL ARCHIVO DE AUDITORÍA

La NIA ES 230 sobre Documentación de auditoría, el resto de NIA ES en el apartado correspondiente a documentación, la LAC y el RLAC establecen requerimientos de documentación del archivo de auditoría cuyo cumplimiento corresponde al equipo del encargo y, en su caso, al auditor principal responsable. Asimismo, los equipos de los encargos deberán cumplir con las políticas y procedimientos internos de la firma en materia de documentación y archivo.

Con carácter previo a la compilación del archivo, parece que lo adecuado es comprobar que la documentación de auditoría está completa. No existe un criterio unificado pues cada firma puede establecer su propio protocolo de comprobación, unas mediante la cumplimentación de un *checklist* y otras mediante la cumplimentación de documentos que proponen los programas de auditoría para el mismo fin.

En todo caso, es recomendable que estos documentos estén permanentemente actualizados para cumplir siempre con los requerimientos normativos, por esto, a veces las soluciones más sencillas como una hoja de Excel, permiten añadir, quitar o modificar los elementos de comprobación de la documentación del archivo de forma ágil.

Ilustración 1: Checklist en Excel de puntos a revisar antes de realizar la compilación.

2. CREACIÓN DE UN ARCHIVO ELECTRÓNICO

Los artículos 29.2 de la LAC y 67.2 f) del RLAC establecen la obligación de elaborar un archivo por cada trabajo de auditoría y que ese archivo sea electrónico, respectivamente.

Cuando los auditores no disponen de un programa de auditoría que, en la mayoría de los casos, opera también como un gestor de ficheros, como paso previo a la generación del archivo compilado, se requiere que la documentación de auditoría esté compuesta en su totalidad de ficheros electrónicos (PDFs, Excel, Word, etc) y a su vez, organizada conforme a una estructura lógica que permita la comprensión del trabajo realizado por un auditor que no haya tenido relación previa con la auditoría.

Un ejemplo de estructura del trabajo en carpetas es el que se presenta en la imagen siguiente:

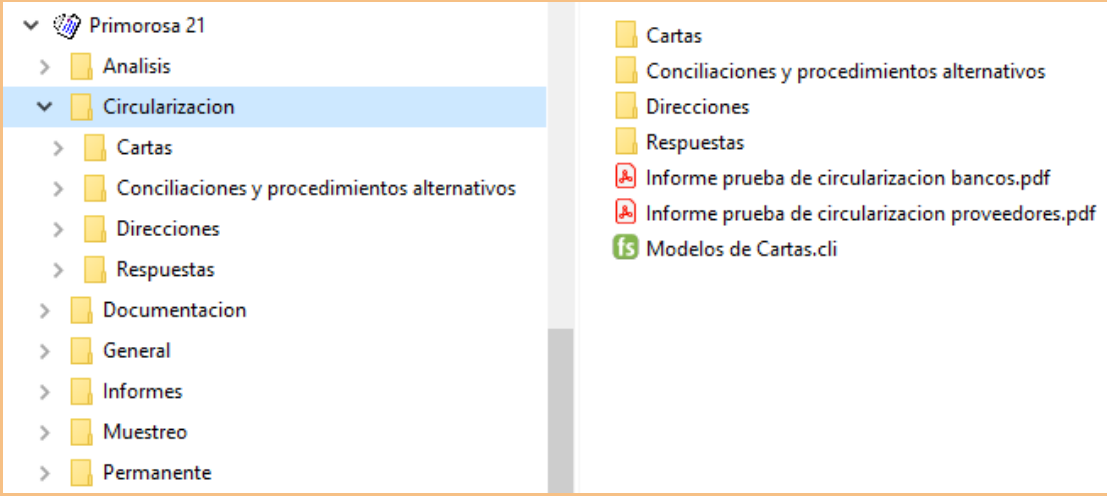


Ilustración 2: La documentación del encargo estructurada en carpetas.

3. COMPILACIÓN E IDENTIFICACIÓN DEL ARCHIVO COMPILADO

El artículo 69.1 del RLAC establece que *"toda la documentación referida en este apartado deberá compilarse en formato archivo electrónico, con las debidas medidas de seguridad que garanticen su autenticidad"* y *"no podrá considerarse que constituya evidencia del trabajo de auditoría realizado la documentación o información no incluida en el citado archivo"*. Asimismo, el artículo 72.2 del RLAC establece que los sistemas informáticos de los auditores deben disponer de controles que garanticen, entre otros, *"una identificación única del archivo generado compilado y de la fecha de la compilación"*.

Un modo sencillo de cumplir con estos requerimientos es, una vez cumplidos los pasos 1 y 2 anteriores, generar un único fichero comprimido que contenga toda la documentación del archivo de auditoría.

Tanto el sistema operativo Windows como MacOS disponen de utilidades nativas del propio sistema operativo que permiten comprimir y descomprimir ficheros en formato ZIP. Si además debemos cumplir con la identificación del archivo compilado y la restricción de acceso, tendremos que hacer uso de las funcionalidades más avanzadas, tales como el cifrado de un fichero con una contraseña y para ello, necesitaremos programas de terceros.

Existen varios programas de compresión que se pueden utilizar, entre los más utilizados tenemos 7Zip, Winzip y Winrar. Los dos últimos son versiones de pago pero que se pueden usar gratuitamente si no nos importa cerrar algunos mensajes publicitarios de vez en cuando. Estos programas llevan mucho tiempo funcionando, lo que parece ser una muestra de su fiabilidad. Uno de los que resultan más cómodos de usar es 7Zip que, además de ser gratuito, es compatible con la mayor parte de sistemas de compresión utilizados en Windows y Linux. En el caso de los usuarios de Mac, el programa más extendido es el Winzip.

En el siguiente ejemplo vamos a ver cómo crear un único archivo de auditoría que quede identificado, usando la herramienta 7Zip. Mostraremos además como podemos añadirle un grado adicional de seguridad mediante la asignación de una contraseña que impedirá que nadie que no la conozca pueda acceder a los contenidos del fichero.

En primer lugar, abrimos el explorador de carpetas de Windows (tecla Windows+E), seleccionamos la carpeta principal de la documentación del encargo y pulsamos en el botón derecho del ratón. En el menú de 7Zip elegiremos la opción "Añadir al archivo".

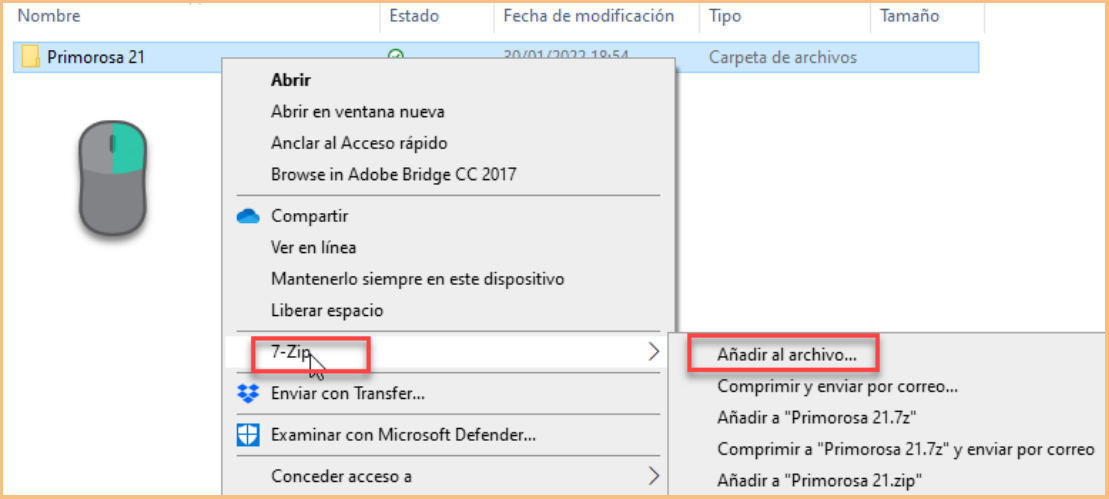


Ilustración 3: Comprimir la carpeta del encargo con 7Zip.

A continuación, seleccionaremos el tipo de compresión (zip es la más extendida) y estableceremos una contraseña para el fichero creado. Una contraseña adecuada y que garantice que no pueda ser forzada con facilidad es aquella que contiene entre 6 y 8 caracteres, incluyendo entre ellas en mayúsculas, minúsculas, números y algún símbolo.

ATENCIÓN: Es imprescindible no extraviar esta contraseña ya que nos será imposible acceder al fichero si no la recordamos. No es estrictamente necesario establecer una contraseña si podemos garantizar mediante otros medios que el acceso al archivo está restringido y que nadie no autorizado puede acceder a él, por ejemplo, mediante la gestión de permisos de carpetas de red o permisos de usuarios en un servicio de almacenamiento en la nube.

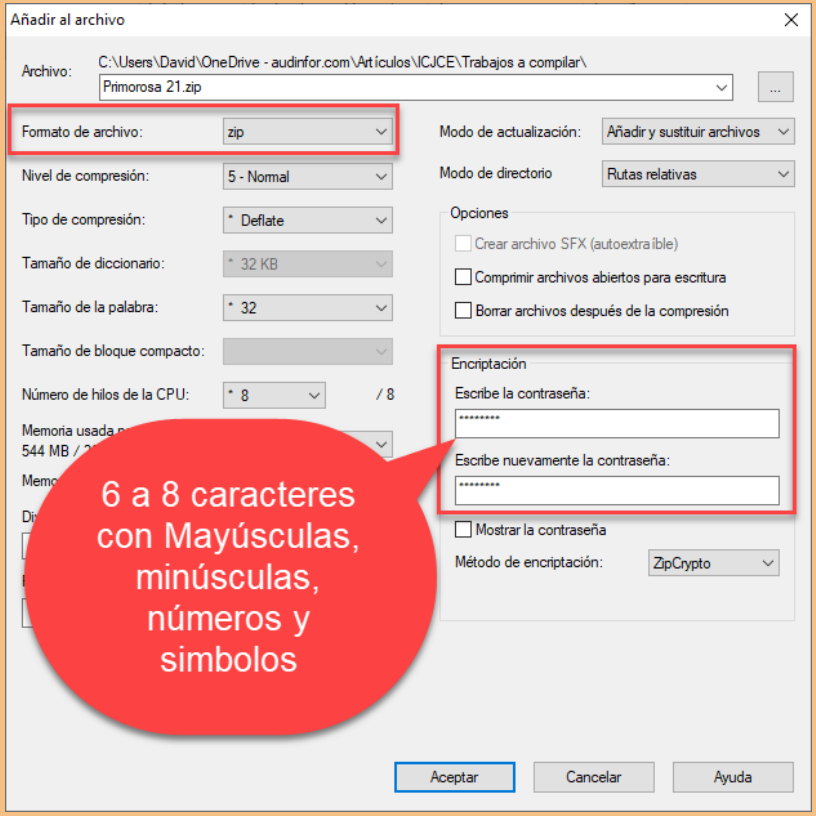
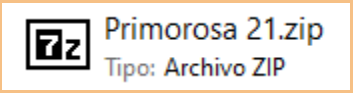


Ilustración 4: Detalle de las opciones para comprimir e incluir una contraseña.

Al finalizar el proceso de archivo obtendremos un fichero que contiene toda la documentación y que, además, estará comprimido para un almacenamiento más eficiente.



Antes de continuar, deberemos de comprobar que el fichero se puede abrir y que la información se ha procesado correctamente. Para abrir el fichero haremos doble click en el archivo, que tendrá la extensión .zip, y comprobaremos que los ficheros están ahí. Podemos navegar por las diferentes carpetas e intentar abrir un fichero Excel o un fichero Word para ver si se abre correctamente y si la contraseña es la adecuada.

Con esto habríamos concluido la compilación del archivo, pero **¿cómo identificarlo de forma única y dejar evidencia de la fecha de compilación?**

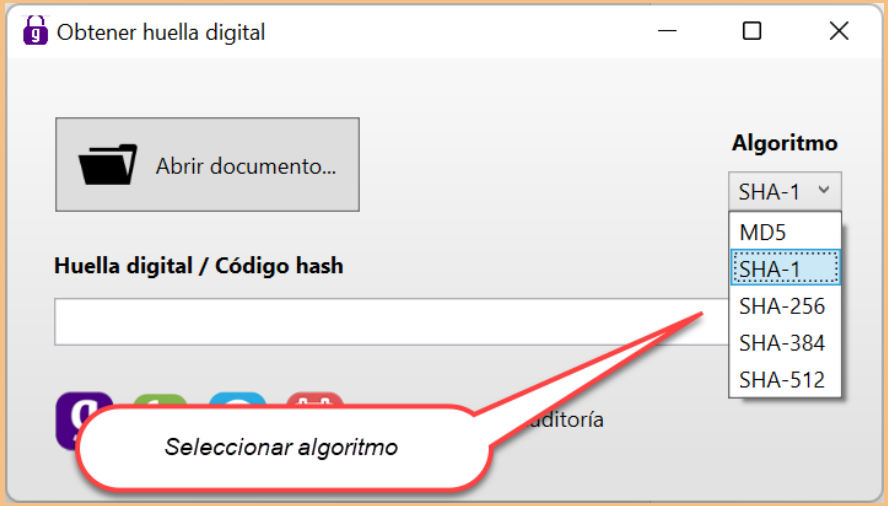
Un método muy sencillo es mediante la obtención de un código alfanumérico *hash*, que consiste en una identificación única de los atributos de un archivo. Este código se puede obtener mediante el uso de uno de los muchos algoritmos standard de generación de código *hash* disponibles.

El código *hash* puede obtenerse accediendo a un sencillo programa gratuito que, analiza las propiedades del archivo (contenido, tamaño, caracteres que contiene, fecha de creación, etc.) y permite obtener una especie de "foto" del archivo compilado en forma de un código que contiene caracteres y números. Si el fichero se modifica, por mínimo que sea el cambio, al volver a generar el código *hash*, este será diferente al inicial.

¿Qué pasos seguir para obtener un código hash que actúe como identificador único del archivo generado compilado?

En primer lugar, **descargar una utilidad para obtener el código *hash***. Nosotros hemos desarrollado una pequeña utilidad (Windows) para este propósito y que está disponible de forma gratuita en este enlace. No obstante, también se puede usar HashMyFiles o QuickHash, este último se puede utilizar con sistemas operativos MacOS. Aunque existen también proveedores de servicios alojados en la nube, pero si desconocemos las medidas de seguridad empleadas como proveedor de servicios, debemos evitar subir este tipo de archivos para la obtención del código hash.

A continuación, **seleccionar el fichero a compilar y el algoritmo**: Desde el menú *Abrir documento*, elegiremos el archivo previamente compilado, luego marcaremos el algoritmo que queremos utilizar. La elección del algoritmo varía en función de la seguridad para evitar la alteración del fichero. Por ello, si queremos un grado de seguridad tal que, para cualquier cambio en el archivo compilado *"quede constancia de las acciones realizadas"*, tal y como exige el artículo 72.2 del RLAC, deberemos seleccionar un algoritmo de seguridad que deje constancia del cambio en el código *hash*. En este sentido, los algoritmos SHA (*Secure Hash Algorithm*, desarrollados por la *National Institute for Standards and Technology*) se caracterizan por ser de los más seguros, siendo el SHA-256 el que actualmente se utiliza en las transacciones con criptomonedas como bitcoin.



Finalmente, **almacenar el algoritmo obtenido en nuestros archivos**. Lo que nos permitirá obtener la identificación única mediante un código alfanumérico parecido a este:

"7c32d2a2521f76a6fdef5ac4c244a54d76394145"

Este código es el que demostrará que nuestro archivo de auditoría compilado no ha sufrido alteraciones. Podemos comprobar que, si cambiamos el fichero de ubicación, el código no se altera, pero si accedemos a él y borramos un archivo, por ejemplo, al ejecutar la aplicación de generación de código hash, el código será diferente.

4. RESTRICCIÓN DE ACCESO A UN ARCHIVO COMPILADO

El artículo 72.2 del RLAC establece que los sistemas informáticos de los auditores deben disponer de controles que garanticen, entre otros, *"la accesibilidad y autorización restringida para su acceso (…)"* y que *"no sea posible la modificación de los archivos de cada trabajo de auditoría una vez transcurrido el plazo máximo de compilación, para que quede constancia de las acciones realizadas sobre dichos archivos y se reduzca el riesgo de deterioro o pérdida"*.

Una de las formas de conseguir el control de acceso puede ser la *encriptación* del archivo mediante el uso de una contraseña que solamente el personal autorizado pueda conocer. El personal autorizado deberá determinarse por la firma.

Asimismo, a través de la utilización de un código *hash*, previamente comentado, si se altera el contenido de un documento, por muy pequeño que sea el cambio, al volver a generar el código *hash*, que recordemos que contiene información sobre las propiedades del archivo, y en particular, sobre la fecha de creación, se generará un código *hash* diferente del generado inicialmente, es decir, en el momento de la compilación.

En definitiva, mediante las restricciones de acceso se garantiza que quede evidencia de cualquier posible cambio, así como de la confidencialidad de la documentación de auditoría.

5. ACCESO A UN ARCHIVO COMPILADO Y GENERACIÓN DE UN ARCHIVO COMPLEMENTARIO

El artículo 69.3 del RLAC establece que *"una vez compilado el archivo, en el caso de hechos (…) que requieran la aplicación de procedimientos de auditoría o en aquellas situaciones en las que con motivo de un plan de subsanación sea necesario incluir documentación adicional, el auditor deberá disponer de políticas y procedimientos que permitan generar a partir del archivo compilado, un archivo complementario en el que deberá quedar documentado quien autoriza el cambio en el archivo complementario respecto al compilado, los motivos y fecha del cambio y la documentación modificada con el objeto de que cualquier tercero pueda realizar un adecuado seguimiento de las modificaciones"*.

En este sentido, el apartado 16 de la NIA ES 230 establece que *"cuando el auditor considere necesario modificar la documentación de auditoría existente o añadir nueva documentación de auditoría después de que se haya terminado la compilación del archivo final de auditoría (…) el auditor documentará: (a) los motivos específicos para hacerlas; y (b) la fecha y las personas que las realizaron y revisaron*.

¿Cómo acceder a un archivo compilado?

Si necesitamos acceder a la documentación contenida en el fichero compilado, el modo correcto de hacerlo no es accediendo al archivo compilado identificado de forma única y navegando por él para revisar un documento, sino que el procedimiento adecuado sería *extraer* todo el contenido a una carpeta nueva, y así poder analizar y revisar la documentación sin riesgo de alterar los contenidos del fichero original. Si accedemos directamente al fichero compilado, es posible que accidentalmente, cambiemos el contenido de alguno de los archivos o demos a guardar incluso sin hacer cambios, lo que podría causar que el fichero al compilarlo (comprimirlo) sea diferente y al pasarlo por un generador de códigos *hash*, se genere uno diferente al original.

¿Cómo generar un archivo complementario?

En el caso de que, como indica el artículo 69.3 del RLAC, *con motivo de un plan de subsanación sea necesario incluir documentación adicional*, el método más adecuado para hacerlo sería el siguiente:

1) Extraer la información del archivo compilado a una carpeta nueva.
2) Realizar las modificaciones, supresiones y adiciones oportunas en esa carpeta.
3) Redactar e incorporar un documento en el que se describan y justifiquen los cambios realizados en la documentación de auditoría.
4) Volver a realizar los pasos descritos en el apartado *3) Compilación e identificación del archivo compilado* de este documento.

En relación con la necesidad de documentar el motivo por el que es necesario acceder a un archivo compilado, la propia contraseña para el acceso restringido viene a cubrir el requerimiento de autorización mientras que la documentación del cambio debería quedar recogida en el archivo complementario, tal y como se ha indicado previamente.

6. ADOPTAR LAS MEDIDAS NECESARIAS PARA GARANTIZAR CUSTODIA Y CONSERVACIÓN DEL ARCHIVO COMPILADO

Visto todo lo anterior, parece razonable, por tanto, diseñar e implementar una política interna para el archivo, restricción y autorización de acceso, custodia y conservación de los archivos de trabajo compilados. Asimismo, entre estas políticas podría contemplarse la creación de una base de datos que incluya información tal como la fecha de emisión del informe de auditoría, fecha de compilación, ubicación, nombre del fichero, persona responsable de autorizar el acceso, y el código *hash* del fichero. El artículo 72.2 del RLAC establece que *"los auditores de cuentas deberán disponer de sistemas informáticos que cuenten con controles, que aseguren la custodia, integridad y recuperación de la información"*. En particular, se establecen como medidas de seguridad: *"deberán realizarse de forma rutinaria copias de seguridad en formato informático en el momento de su creación, cuando se produzcan modificaciones y, en caso de no haberlas, al menos, una vez al año"*. Esto puede llevarse a cabo a través de diferentes procedimientos de respaldo de la información. Entre los más habituales están los siguientes:

a) **Copia de seguridad de la información en unidades externas o de red**. La mayor parte de las firmas y despachos disponen de sistemas de respaldo de la información. Estos sistemas deben de contener procedimientos de respaldo de la información con una periodicidad mínima y que almacenen las copias de seguridad en ubicaciones distintas del centro de trabajo, de modo que cubran eventualidades tales como incendio o deterioro por inundaciones. Tanto en el caso de que se usen discos duros externos, llaves USB o se haga una copia en un servidor de la red, debe de existir una copia de éstos en un lugar fuera de la oficina.

b) **Copia de seguridad en un servicio de almacenamiento en la nube**. Cada vez es más habitual el uso de servicios de almacenamiento en la nube, tales como como Onedrive (Microsoft 365), Drive (Gsuite) o Dropbox. Estos servicios sincronizan la información almacenada en los discos duros locales del usuario en servidores ubicados en la nube, de modo que se pueden recuperar en cualquier momento y descargarlos en cualquier ordenador. Estos servicios incluyen también la recuperación de diferentes versiones de los archivos a lo largo del tiempo, lo que puede ser muy interesante en caso de ataques de tipo *ransomware*.

4. CONCLUSIÓN

La generación de un archivo electrónico, su compilación, identificación única, acceso, custodia y conservación deben contemplarse como parte de las políticas y procedimientos del auditor de modo que se aporte fiabilidad y seguridad a la documentación que sirve de base para la emisión del informe de auditoría.

Este documento pretende ser una reflexión sobre este proceso, que no tiene que ser necesariamente complejo y que puede dimensionarse en función de las características de cada firma o despacho. Por tanto, si bien este proceso puede parecer un desafío creo que el gran desafío es que nuestro equipo, así como nuestros procedimientos y sistemas operen correctamente de modo que se realice un trabajo de auditoría de calidad y se sirva al interés público.

Autor: David Uyarra Delgado, socio de Ensys Consultores Informáticos y responsable del proyecto Gesia y ForTiming

AUDITORES

INSTITUTO DE CENSORES JURADOS
DE CUENTAS DE ESPAÑA

Paseo de la Habana, 1 – 28036, Madrid
Teléfono: 914460354
E-mail: auditoria@icjce.es
www.icjce.es