I. DISPOSICIONES GENERALES

MINISTERIO DE JUSTICIA

12906 *Resolución de 20 de noviembre de 2014, de la Dirección General de los Registros y del Notariado, por la que se modifica el anexo II de la Orden JUS/206/2009, de 28 de enero, por la que se aprueban nuevos modelos para la presentación en el Registro Mercantil de las cuentas anuales de los sujetos obligados a su publicación.*

La Orden JUS/206/2009, de 28 de enero, por la que se aprueban nuevos modelos para la presentación en el Registro Mercantil de las cuentas anuales de los sujetos obligados a su publicación establece en su anexo II.1.2 que «la huella digital correspondiente al depósito se generará aplicándole al fichero.ZIP el algoritmo estándar MD5 (rfc 1321)…»

En relación a dicho algoritmo MD5 (rfc 1321), el Centro Criptológico Nacional (CNN), en su Guía/Norma de Seguridad de las TIC (CNN-STIC-807) Criptología de empleo en el Esquema Nacional de Seguridad, indica lo siguiente:

«2.MD5

559. La función resumen conocida como MD5 sigue siendo utilizada hoy día a pesar de que se han hallado debilidades ([Wang and Yu, 2005]) y su uso no está permitido para aplicaciones de seguridad.

No obstante se ha incluido en esta guía dado que algunos certificados digitales emitidos por determinadas autoridades de certificación siguen empleándola. En cualquier caso, debe quedar claro que el uso de esta función no está permitido en el ENS.»

Por lo tanto, al ser MD5 un estándar con debilidades y que su uso no está permitido en el Esquema Nacional de Seguridad, se hace necesario su sustitución por un estándar seguro y aceptado por el ENS.

En su virtud, al amparo de lo dispuesto en la disposición adicional de la Orden JUS/206/2009, de 28 de enero, resuelvo:

Único. *Modificación en el anexo II.I.2: Depósito de cuentas.*

Se sustituye la actual redacción:

> «…la huella digital correspondiente al depósito se generará aplicándole al fichero.ZIP el algoritmo estándar MD5 (rfc 1321) el cual producirá una huella digital de 128 bits, a la que se añadirán por la izquierda dos bits a cero para conseguir una huella de 130 bits, que se agrupará en paquetes de 5 bits, cada uno de los cuales se considerará como la expresión, en sistema binario de numeración, de un entero en sistema decimal de numeración entre 0 y 31 y que se traducirá por el carácter ASCII que ocupe ese número de orden en la lista siguiente: {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F,G,H,J,K,M,N,P,R,S,T,U,V,X,Y,Z} de forma que la huella digital tendrá siempre 26 dígitos alfanuméricos en mayúsculas. Nótese que se han evitado los caracteres I, L, Ñ, O, W, que pueden resultar parecidos a otros de la lista (I –1, L–1, O–0, etc.).
>
> La visualización e impresión de esta huella digital se realizará en formato ASCII y también en el formato estándar de código de barras EAN 128A.»

Por la siguiente:

> «…la huella digital correspondiente al depósito se generará aplicándole al fichero.ZIP el algoritmo estándar SHA256 (RFC 6234) el cual producirá un hash de

cve: BOE-A-2014-12906

256 bits (32 bytes), dicho conjunto de bits a su vez se codificará para su conversión en texto según el estándar BinHex (RFC 1741). La visualización e impresión de esta huella digital se podrá realizar en el formato estándar de código de barras EAN 128A.»

Madrid, 20 de noviembre de 2014.–El Director General de los Registros y del Notariado, Francisco Javier Gómez Gálligo.

cve: BOE-A-2014-12906