A. Comentarios al Modelo de Acuerdo entre Autoridades Competentes

Introducción

1. El Modelo AAC establece un nexo entre el ECR y las bases legales para el intercambio (tales como la Convención sobre Asistencia Administrativa Mutua en Materia Fiscal u otros convenios fiscales bilaterales). El Modelo AAC consta de un preámbulo y siete secciones, y contempla las modalidades de intercambio para garantizar un flujo adecuado de información. El preámbulo contiene considerandos relativos a los reportes domésticos y las reglas de debida diligencia sobre las que se sustenta el intercambio de información de conformidad con el Modelo AAC. Asimismo, contiene considerandos relativos a la confidencialidad, las garantías en materia de protección de datos y la existencia de la infraestructura necesaria para un intercambio eficaz.

2. El Modelo AAC contiene una sección relativa a definiciones (Sección 1), abarca el tipo de información que será intercambiada (Sección 2), los plazos y modalidades para el intercambio (Sección 3), colaboración en materia de cumplimiento y aplicación (Sección 4) y obligaciones de confidencialidad y protección de datos (Sección 5). Las Secciones 4, 6 y 7 abordan las consultas entre Autoridades Competentes, las modificaciones al Acuerdo y la vigencia del mismo, incluyendo su suspensión y denuncia.

3. El Modelo AAC se ha redactado como un acuerdo bilateral recíproco basado en el principio de que el intercambio automático es recíproco y se llevará a cabo bilateralmente. Con el fin de minimizar los costes asociados a la firma de múltiples acuerdos bilaterales entre Autoridades Competentes, el intercambio de información podría también implementarse a través de un acuerdo multilateral entre Autoridades Competentes. Una versión multilateral del Modelo AAC está incluida como Anexo 1. Aun cuando el acuerdo sería multilateral, el intercambio de información en sí mismo se llevaría a cabo de forma bilateral. Por otra parte, es posible que, en ciertos casos, algunas

jurisdicciones deseen concluir un acuerdo bilateral no recíproco (por ejemplo, si una jurisdicción no tiene un impuesto sobre la renta). A estos efectos, se incluye una versión no recíproca del Modelo AAC como Anexo 2. El G20 y otros han admitido la posibilidad de que los países en desarrollo se enfrenten a problemas concretos de capacidad respecto del intercambio automático de información, lo que representa un aspecto clave que ha de ser abordado. Por esta razón, en julio de 2013, el G20 hizo un llamamiento en el Foro Global sobre Transparencia e Intercambio de Información para Fines Fiscales para colaborar con el Grupo de Trabajo sobre Fiscalidad y Desarrollo de la OCDE y el Banco Mundial, entre otros, para ayudar a los países en desarrollo a identificar sus necesidades de asistencia y capacitación técnica.

4. Las jurisdicciones podrán también suscribir un acuerdo intergubernamental multilateral o bien múltiples acuerdos intergubernamentales que, por derecho propio o en virtud de la legislación regional, constituirían convenios internacionales que abarcan tanto las obligaciones de reporte y los procedimientos de debida diligencia, acompañados de un ACC de alcance más limitado.

Comentarios al preámbulo

1. El preámbulo («considerandos»), proporciona un contexto y un marco pertinentes al incluir una frase de referencia al fundamento jurídico subyacente que permite el intercambio automático de información.

2. El primer considerando sirve de introducción y podrá adaptarse a las circunstancias particulares de las jurisdicciones que suscriban el Acuerdo.

3. El segundo considerando se remite a la obligación de reportar la información relativa a ciertas cuentas que la legislación de las respectivas jurisdicciones de las Autoridades Competentes impone, o ha de imponer, a las instituciones financieras con arreglo al alcance del intercambio previsto en la Sección 2 del presente Acuerdo.

4. El lenguaje alternativo de este considerando permite a las jurisdicciones, si así lo desean, concluir un acuerdo entre Autoridades Competentes antes incluso de que una de las jurisdicciones, o ambas, dispongan de normas pertinentes en materia de debida diligencia y reporte de información. Véanse también el apartado 3 de la Sección 3 (apartado 3 de los Comentarios a la Sección 3) y la Sección 7 (apartado 1 de los Comentarios a la Sección 7).

5. El tercer considerando determina el fundamento jurídico que autoriza el intercambio automático de información sobre cuentas financieras y permite a las Autoridades Competentes acordar el alcance y modalidades de tales intercambios automáticos. El alcance acordado debe ser compatible con el alcance del intercambio contemplado en el artículo 2 del presente Acuerdo. Otros instrumentos jurídicos (diferentes a los convenios de doble imposición o a la Convención sobre Asistencia Administrativa Mutua en Materia Fiscal) que permiten el intercambio automático de información con fines fiscales incluyen ciertos acuerdos de intercambio de información tributaria o acuerdos regionales de cooperación entre administraciones tributarias. Desde una perspectiva regional, el intercambio automático de información también puede articularse sobre la base del Derecho de la Unión Europea o instrumentos normativos de la Comunidad Andina que aborden los contenidos del Modelo AAC y del ECR.

6. El cuarto considerando establece que las Autoridades Competentes han desarrollado y cuentan con: *(i)* las garantías adecuadas para preservar la

confidencialidad de la información recibida, y *(ii)* una infraestructura que permite un intercambio eficaz. Los Comentarios a la Sección 5 del Modelo AAC proporcionan más información.

Comentarios a la Sección 1 sobre Definiciones

Apartado 1 – Definiciones

1. El apartado 1 contiene las definiciones de los términos y expresiones propios del presente Acuerdo. Las definiciones de los restantes términos y expresiones utilizados en el Acuerdo figuran en la Sección VIII del ECR.

2. Los subapartados 1(a) y (b) incluyen una descripción de las jurisdicciones que suscriben el Acuerdo. Las Autoridades Competentes pueden acordar libremente las definiciones de las expresiones «[Jurisdicción A]» y «[Jurisdicción B]»; no obstante, dichas definiciones deben ser coherentes y compatibles con las definiciones que figuran en el instrumento jurídico subyacente. Asimismo, las Autoridades Competentes pueden optar por introducir una descripción geográfica (incluyendo una referencia a plataformas continentales); sin embargo, bastará una definición política. He aquí un ejemplo de definición política: «La expresión «México» significa los Estados Unidos Mexicanos».

3. La definición de la expresión «Autoridad Competente» descrita en el subapartado 1(c) incluye una descripción de las Autoridades Competentes para los efectos del presente Acuerdo. Esta definición permite que cada jurisdicción designe a una o más autoridades como la(s) competente(s). No obstante, dicha definición debe ser coherente y compatible con la que figura en el instrumento jurídico subyacente.

4. Las expresiones que figuran en los subapartados 1(d) a (k) alinean el alcance del intercambio de información entre las jurisdicciones que suscriban el Acuerdo al ámbito de aplicación del ECR. Dichas expresiones se refieren a:

- las instituciones financieras obligadas a reportar: «Institución Financiera [gentilicio Jurisdicción A]», «Institución Financiera [gentilicio Jurisdicción B]», e «Institución Financiera Sujeta a Reportar», compatibles con las expresiones «Institución Financiera Sujeta a Reportar» e «Institución Financiera de una Jurisdicción Participante» descritas en los subapartados A(1) y (2) de la Sección VIII del ECR (véanse los apartados 2 a 6 de los Comentarios a la Sección VIII);

- las cuentas financieras reportadas: «Cuenta Reportable», «Cuenta Reportable [gentilicio Jurisdicción A]» y «Cuenta Reportable [gentilicio Jurisdicción B]», que son consistentes con la expresión «Cuenta Reportable» descrita en el subapartado D(1) de la Sección VIII del ECR (véase el apartado 105 de los Comentarios a la Sección VIII), y
- los titulares de las cuentas objeto del reporte: «Persona [gentilicio Jurisdicción A]» y «Persona [gentilicio Jurisdicción B]», consistentes con las expresiones «Persona Reportable» y «Persona de una Jurisdicción Reportable» descritas en los subapartados D(2) y (3) de la Sección VIII del ECR (véanse los apartados 106 a 116 de los Comentarios a la Sección VIII).

5. El subapartado 1(l) contiene la definición del acrónimo «NIF», correspondiente éste a una expresión que también se define en el subapartado E(5) de la Sección VIII del ECR. Mientras que esta última define el NIF como el Número de Identificación Fiscal o el equivalente funcional en ausencia de un Número de Identificación Fiscal (véanse los apartados 146 a 149 de los Comentarios a la Sección VIII), el objeto de la primera es identificar los NIFs de las jurisdicciones que suscriban el Acuerdo. Las expresiones «NIF [gentilicio Jurisdicción A]» y «NIF [gentilicio Jurisdicción B]» definidas en los subapartados 1(m) y (n) también sirven a este propósito.

6. El Modelo AAC no define la expresión «Estándar Común de Reporte» (ECR), aunque la versión multilateral del Modelo de Acuerdo entre Autoridades Competentes sí incluye una definición de esa expresión. Es probable que el ECR, incluyendo las modalidades de TI, se actualice periódicamente a medida que cada vez más jurisdicciones implementen y se familiaricen con el ECR. En el contexto de un acuerdo multilateral, las Autoridades Competentes podrán suscribir el acuerdo en fechas diferentes y, debido a las diferentes fechas de firma, puede ocurrir que el ECR haya sido actualizado entretanto. Para abordar esta situación, la versión multilateral define el ECR como «el estándar para el intercambio automático de información sobre cuentas financieras desarrollado conjuntamente por la OCDE y los países del G20, presentado con motivo de la reunión del G20 en 2014 y publicado en el sitio web de la OCDE». Asimismo, para garantizar la interpretación conforme a la que se prevé que todas las jurisdicciones aplicarán la versión más reciente del Estándar, el tercer considerando establece que se «contempla la modificación periódica de la legislación interna de las Jurisdicciones con el fin de reflejar las actualizaciones al ECR y, una vez adoptadas dichas modificaciones por una determinada Jurisdicción, se entenderá que la definición de «Estándar Común de Reporte» se refiere a la versión actualizada respecto de esa Jurisdicción». En un acuerdo bilateral, no se plantea el mismo problema toda vez que las Autoridades Competentes

generalmente firman en la misma fecha. Sin embargo, aun cuando se trate de un acuerdo bilateral, es posible que dichas Autoridades deseen referirse explícitamente a las actualizaciones al ECR de la misma forma que se establece en la versión multilateral (definir la expresión «Estándar Común de Reporte» y añadir un considerando que establezca la expectativa de que las jurisdicciones modifiquen las disposiciones de su normativa interna para reflejar las actualizaciones al ECR).

Apartado 2 – Regla general de interpretación

7. El apartado 2 establece la regla general de interpretación. La primera frase del apartado 2 indica claramente que aquellos términos y expresiones con mayúscula inicial utilizados, que no estén definidos en el propio Modelo AAC se interpretarán de forma consistente con el significado que se les dé en el ECR. Ello transmite la idea, también expresada en el preámbulo, de que las jurisdicciones han introducido procedimientos de notificación y debida diligencia (incluyendo las definiciones correspondientes) consistentes con el ECR.

8. La segunda frase del apartado 2 dispone que, a menos que del contexto se infiera una interpretación diferente o que las Autoridades Competentes acuerden un significado común, los términos y expresiones no definidos en el presente Acuerdo o en el ECR tendrán el significado que en ese momento le atribuya la legislación de la jurisdicción que aplica el Acuerdo. A este respecto, prevalecerá el significado atribuido por la legislación fiscal aplicable de esa jurisdicción sobre el que resultaría de otras ramas del Derecho de dicha jurisdicción. Por otra parte, atendiendo al contexto, las Autoridades Competentes deberán tomar como referencia los Comentarios al ECR y sus definiciones de los distintos términos y expresiones.

Comentarios a la Sección 2 sobre Intercambio de Información Respecto de las Cuentas Reportables

1. Esta Sección estipula que la información a intercambiar es aquella que establezca, específicamente, las disposiciones en materia de reporte y debida diligencia del ECR. Véanse la Sección I (Obligaciones generales de reporte) del ECR y los Comentarios correspondientes.

2. El primer apartado hace referencia al fundamento legal para el intercambio y dispone que la información habrá de intercambiarse anualmente. También es posible que la información sea intercambiada con una frecuencia mayor a un año; por ejemplo, cuando una Autoridad Competente reciba datos corregidos de una Institución Financiera Sujeta a Reportar, dicha información se remitirá, por lo general, a la otra Autoridad Competente lo antes posible. La información que ha de intercambiarse es la información obtenida en virtud del ECR y la que se especifica, concretamente, en el apartado 2.

3. El apartado 1 aclara que el intercambio de información está sujeto a lo dispuesto en el ECR en materia de reporte y debida diligencia. En consecuencia, mientras dichas disposiciones no exijan el reporte, por ejemplo, de un NIF respecto de una Cuenta Reportable en particular, tampoco existirá la obligación de intercambiar esa información. Véanse las excepciones previstas en los apartados C a F de la Sección I del ECR y los apartados 25 a 35 de los Comentarios a la Sección I.

4. El subapartado 2(d) de la Sección 2 dispone que una jurisdicción está obligada a intercambiar el saldo o valor de una cuenta al final del año civil correspondiente o de otro período de reporte apropiado. No obstante, el apartado 11 de los Comentarios a la Sección I del ECR determina que, como alternativa, las jurisdicciones podrán exigir a las instituciones financieras que les reporten el saldo o el valor promedio de la cuenta durante el año civil considerado u otro período de reporte apropiado. La posibilidad de que una jurisdicción requiera el reporte del saldo o valor promedio de una cuenta en lugar del saldo al cierre del ejercicio deberá establecerse en el Acuerdo, incluyendo las normas aplicables para determinar el saldo o valor promedio de una cuenta, con el fin de establecer claramente la información reportable.

Comentarios a la Sección 3 sobre Plazos y Modalidades de Intercambio de Información

Apartados 1 y 2 – Importe, naturaleza y moneda de denominación de los pagos

1. El apartado 1 dispone que, para los efectos del intercambio de información previsto en la Sección 2, el importe y la naturaleza de los pagos efectuados en relación con una Cuenta Reportable pueden determinarse de conformidad con los principios de la legislación fiscal de la jurisdicción que envía la información. El apartado 2 establece que se identificará en la información intercambiada la moneda en la que se denomine cada uno de los importes a los que se refiere.

Apartados 3 y 4 – Plazos para el intercambio de información

2. El apartado 3 estipula que el intercambio de información deberá tener lugar en el plazo de nueve meses contados a partir de la finalización del año civil al que se refiere la información. El primer año respecto del cual se intercambiará información se dejará en blanco para que las jurisdicciones lo introduzcan. El periodo de nueve meses mencionado en el apartado 3 representa un estándar mínimo y las jurisdicciones tienen la libertad de fijar periodos más breves. Por ejemplo, los Estados Miembros de la Unión Europea están sujetos a un plazo de 6 meses en virtud de la «Directiva del Ahorro».

3. El apartado 3 dispone igualmente que, sin perjuicio del año que las Autoridades Competentes elijan como el año respecto del cual se llevará a cabo el primer intercambio, la obligación de intercambiar información respecto de un año civil se aplica, únicamente, si ambas jurisdicciones tienen en vigor legislación que requiera reportar información respecto de dicho año civil que sea consistente con el alcance del intercambio descrito en la Sección 2 y en el ECR. Esta frase no surtirá efecto alguno si, en el momento en que se firme el Acuerdo, ambas jurisdicciones disponen de legislación interna compatible con el ECR. Si una o ninguna de las jurisdicciones tiene

en vigor dicha legislación al momento de la firma, la frase surtirá efectos para garantizar que, tras la entrada en vigor del Acuerdo y pese a que el período de vigencia del ECR sea mayor en una de las jurisdicciones, la única información que será obligatorio intercambiar será la relativa a los años durante los cuales ambas jurisdicciones tengan en vigor las obligaciones de reporte. No obstante, una Jurisdicción podrá optar, de conformidad con su legislación interna, por intercambiar información respecto de años anteriores, en cuyo caso dicho intercambio resultará igualmente compatible con el ECR y el Modelo AAC.

4. El siguiente ejemplo ilustra el funcionamiento del apartado 3 en caso de que una jurisdicción no disponga de legislación que regule la obligación de intercambiar información respecto del año civil acordado en los términos de la primera frase del apartado 3: las Jurisdicciones A y B suscriben el Modelo AAC el 30 de abril de 2015 y acuerdan que intercambiarán información respecto del año 2016 y subsecuentes. La Jurisdicción A notifica, el 7 de junio de 2015, que dispone de normas que regulan la obligación de intercambiar información respecto del año 2016. Por su parte, la Jurisdicción B notifica, el 1 de noviembre de 2015, que dispone de normas que regulan la obligación de intercambiar información respecto del año 2017. En este caso, con base en la última frase del apartado 3, la Jurisdicción A no estará obligada a intercambiar información respecto del año 2016. Ambas jurisdicciones, A y B, estarán obligadas a intercambiar información respecto de 2017. Sin embargo, la Jurisdicción A puede optar, al amparo de su legislación interna, por enviar información a la Jurisdicción B respecto de 2016, aun cuando la Jurisdicción A no reciba información relativa al año 2016.

5. El apartado 4 contiene una excepción respecto del año en que el importe bruto de los productos ha de reportarse. Probablemente sea más difícil para las Instituciones Financieras Sujetas a Reportar el implementar procedimientos para obtener el importe bruto total de los productos de la venta o reembolso de propiedad. Así, al aplicar el ECR, las jurisdicciones pueden optar por reportar gradualmente la información relativa a dichos importes brutos. Si no se contempla una disposición transitoria, el apartado 4 será innecesario. Si una de las jurisdicciones contempla tal disposición transitoria, será necesario incluir el apartado 4, donde se establece que, no obstante lo dispuesto en el apartado 3, la información que ha de intercambiarse respecto del año especificado en el apartado 3 será aquella mencionada en el apartado 2 de la Sección 2, a excepción de los ingresos brutos descritos en el subapartado 2(e)(2) de la Sección 2. En dicho caso, las jurisdicciones deberán especificar el año respecto del cual los ingresos brutos deberán reportarse.

6. El Acuerdo no impide la aplicación de las disposiciones previstas en los artículos 2 y 3 respecto de la información obtenida con anterioridad a

la fecha de entrada en vigor del Acuerdo, siempre que se proporcione dicha información después de que el Acuerdo entre en vigor y las disposiciones de las Secciones 2 y 3 surtan efectos. No obstante, puede que las Autoridades Competentes consideren útil aclarar en qué medida las disposiciones señaladas en las Secciones 2 y 3 resultan aplicables a dicha información.

Apartados 5 y 6 – Modalidades de Tecnología de la Información

Esquema ECR y guía del usuario

7. El apartado 5 dispone que las Autoridades Competentes intercambiarán de forma automática la información descrita en la Sección 2 y la presentarán conforme a un esquema en lenguaje de marcas extensible (XML) del ECR. La guía de usuario del ECR, incluida en el Anexo 3, proporciona directrices respecto del esquema y su uso.

Transmisión de datos y estándares de cifrado

8. El apartado 6 establece que las Autoridades Competentes acordarán uno o varios métodos de transmisión de datos, incluidos los estándares de cifrado.

Estándares mínimos adecuados

9. Todo método de transmisión debe cumplir con estándares mínimos adecuados para garantizar la confidencialidad e integridad de los datos durante la transmisión. El término confidencialidad significa que los datos o información no estarán disponibles o serán revelados a personas no autorizadas. El término integridad significa que los datos o información no han sido modificados o alterados de forma no autorizada. Con el tiempo, dichos estándares serán susceptibles de modificarse en relación con las capacidades tecnológicas. Esto incluye la utilización de canales de comunicación y protocolos seguros que aseguren la confidencialidad e integridad de los datos mediante el cifrado, medidas físicas de conversión de datos o la combinación de ambos.

10. El Modelo AAC no establece una única solución para la transmisión o el cifrado de datos, ya que ello podría limitar la capacidad de las Autoridades Competentes para acordar sistemas y prácticas que ya estén en uso o que resulten idóneas en determinadas circunstancias. Dado que la responsabilidad de los datos recae sobre la jurisdicción que envía la información hasta en tanto la jurisdicción destinataria los reciba, es posible, dependiendo de las requerimientos nacionales, que se acuerden distintos procesos para ambas partes del intercambio bilateral (esto es, emisor y receptor). Por ejemplo, la

jurisdicción A puede utilizar un protocolo de transferencia de datos a través de navegador y la jurisdicción B un servidor direccionado a través de una red segura para el intercambio de datos. Sin embargo, dado que las jurisdicciones efectuarían un intercambio automático de información en los términos del ECR con otras tantas jurisdicciones, cabe plantearse la conveniencia de diseñar una arquitectura internacional sostenible para la transmisión de datos que mitigue, en la medida de lo posible, la necesidad de adoptar y mantener múltiples métodos de transmisión y/o cifrado de datos.

Cifrado de datos

11. El cifrado de datos está diseñado para garantizar tanto la confidencialidad como la integridad de los datos. Garantiza que los datos se transforman para hacerlos ininteligibles para quienes no dispongan de la clave de descifrado. Todos los archivos de datos objeto de intercambio deberán cifrarse, conforme a un estándar mínimo de seguridad y la vía de transmisión deberá cifrarse o convertirse mediante un método físico seguro con procedimientos de control y auditoría a fin de monitorear el acceso a, y la copia de, archivos. Uno de los métodos de cifrado de uso generalizado para el intercambio de información emplea tanto una clave pública como una clave privada. El algoritmo criptográfico de clave pública lleva utilizándose varias décadas y permite a las partes interesadas intercambiar datos cifrados sin necesidad de revelar con antelación una clave secreta compartida. La parte remitente cifra el archivo de datos mediante una clave pública, y sólo la parte receptora posee la clave privada segura que permite descifrar los datos. Existen estándares de longitud de clave de cifrado de uso internacional ampliamente reconocidos por proporcionar el nivel de seguridad idóneo para proteger los datos financieros de carácter personal, tanto en el presente como en el futuro previsible, tales como el denominado estándar de cifrado avanzado de longitud de clave de 256 bits (AES, por sus siglas en inglés).

Métodos de transmisión electrónica

12. Si bien solía ser habitual enviar archivos de datos cifrados en disquetes flexibles, tarjetas de memoria y discos compactos cuya entrega e intercambio tenía lugar físicamente o por correo certificado entre Autoridades Competentes, la transferencia de datos a través de herramientas portátiles requiere de un control adicional e implica un mayor riesgo (aun cuando se refuerce su integridad y confidencialidad mediante el cifrado de los datos). En la actualidad, es extremadamente sencillo, desde un punto de vista tecnológico, transferir datos utilizando un navegador web a través del cual, a un coste reducido, se proporcionan capacidades de cifrado, no revocación y no repudio de los datos, de ahí que la utilización de herramientas portátiles haya

dejado de considerarse la mejor práctica. Se recomienda utilizar un método de transmisión que permita un protocolo integrado de extremo a extremo para la transmisión de archivos electrónicos como la mejor práctica actual, ya se base en una arquitectura servidor-servidor o en un sistema de acceso a través de navegador[1]. Como alternativa, puede utilizarse un servicio de correo electrónico seguro que cumpla unas especificaciones y estándares mínimos, aunque pueda generar costes de instalación más altos o una mayor dificultad de uso para administrar los accesos de usuario y la seguridad de los datos, incluyendo limitaciones al tamaño de los archivos y otros problemas con el cortafuegos, de ahí la importancia de una evaluación inicial y reevaluación automática del riesgo en seguridad de la información.

Implementación de seguridad operativa

13. La confidencialidad y seguridad de los datos transmitidos también dependen de la implementación de procedimientos de administración, organización y operación apropiados, así como de medidas y herramientas técnicas como el soporte físico (hardware) y soporte lógico (software). Si bien el cumplimiento de determinados estándares no es obligatorio, lo más idóneo sería administrar la seguridad de forma consistente con los estándares y mejores prácticas tales como la serie de normas ISO 27000 para la Seguridad de la Información, según esta se modifique en el transcurso del tiempo. Más concretamente, debe concederse el acceso a los datos únicamente a las partes autorizadas durante el proceso de transmisión, debiendo existir un control férreo del acceso a las claves de cifrado, especialmente a la clave secreta. Asimismo, debería conservarse un registro de todos los accesos autorizados a los datos o a las claves, como un registro de accesos del sistema. Para mayor información sobre los estándares en materia de protección de datos y confidencialidad, véanse los Comentarios a la Sección 5.

1. La tecnología SERVICIOS WEB que utiliza el protocolo de seguridad en servicios web (WSS) representa otro estándar asequible cada vez más utilizado en entornos seguros, y engloba una serie de servicios que utilizan el protocolo de transferencia de hipertexto (HTTP) a través de métodos estándar tales como GET y POST. Algunos ejemplos de protocolos de transmisión internacionalmente aceptados por cumplir los requerimientos de utilizar protocolos y canales para la transmisión segura de datos que garanticen la confidencialidad e integridad de los mismos incluyen la capa de transporte seguro (TLS) versión 1.1 para intercambios seguros de datos a través de acceso a navegador, y el protocolo de transferencia segura de archivos (SFTP) para la transferencia masiva de datos programada, aunque éstos no son los únicos protocolos que pueden ofrecer soluciones apropiadas.

Comentarios a la Sección 4 sobre Colaboración en Materia de Cumplimiento y Aplicación

1. Esta Sección trata sobre la colaboración entre Autoridades Competentes en materia de cumplimiento y aplicación del Acuerdo y dispone que, cuando una Autoridad Competente tenga razones para creer que un error ha podido originar una transmisión de datos incorrecta o incompleta, o considere que existe un incumplimiento por parte de la Institución Financiera Sujeta a Reportar, esa Autoridad Competente lo notificará a la otra Autoridad Competente. La Autoridad Competente notificada al respecto adoptará las medidas oportunas al amparo de su legislación interna para atender los errores o el incumplimiento a los que se refiera la notificación. Véanse los Comentarios a la Sección IX del ECR en relación con las normas y procedimientos administrativos que las jurisdicciones deben aplicar para garantizar el cumplimiento efectivo del ECR.

2. La notificación a la que se refiere esta Sección deberá realizarse por escrito identificando claramente el error o el incumplimiento observados, así como las razones por las que se cree que han tenido lugar. La Autoridad Competente notificada deberá proporcionar una respuesta o actualización pertinentes a la mayor brevedad, en un plazo máximo de 90 días naturales contados a partir de la recepción de la notificación remitida por la otra Autoridad Competente. Si no se resuelve el problema, cada 90 días la Autoridad Competente deberá proporcionar una actualización a la otra Autoridad Competente. Por el contrario, si tras revisar y examinar la notificación de buena fe, la Autoridad Competente notificada considera que no existe, o no se ha producido, el error o incumplimiento descritos en la citada notificación, deberá, a la mayor brevedad posible, comunicárselo a la otra Autoridad Competente por escrito y argumentar debidamente sus razones.

3. La Sección 4 no contempla el contacto directo entre la Autoridad Competente de una jurisdicción y una Institución Financiera Sujeta a Reportar de la otra jurisdicción. Como alternativa, ambas Autoridades Competentes pueden optar por autorizar el contacto directo entre una Autoridad Competente de una jurisdicción y la mencionada Institución de la otra jurisdicción en caso de verificarse errores administrativos u otros

errores leves. La decisión de incluir esta opción dependerá de la legislación interna de las respectivas jurisdicciones, pudiendo influir también el volumen de solicitudes que una Autoridad Competente prevé recibir. Si ambas Autoridades Competentes están de acuerdo con dicho enfoque, deberá utilizarse la siguiente redacción en sustitución de la redacción actual del artículo 4:

1. Una Autoridad Competente podrá enviar una solicitud de información directamente a una Institución Financiera Sujeta a Reportar de la otra jurisdicción cuando tenga razones para creer que se han producido errores administrativos, u otros errores menores, que hayan podido originar un reporte de información inexacto o incompleto. Una Autoridad Competente notificará a la otra Autoridad Competente cuando la primera envíe una solicitud de información a una Institución Financiera Sujeta a Reportar de la otra jurisdicción.

2. Una Autoridad Competente notificará a la otra Autoridad Competente cuando la primera tenga razones para creer que existe incumplimiento por parte de una Institución Financiera Sujeta a Reportar de las obligaciones de reporte y de los procedimientos de debida diligencia aplicables con arreglo al ECR. La Autoridad Competente notificada al respecto adoptará las medidas oportunas al amparo de su legislación interna para abordar y subsanar el incumplimiento al que se refiera la notificación.

4. La legislación interna de la jurisdicción en que esté ubicada la Institución Financiera Sujeta a Reportar, incluyendo la legislación aplicable a la protección de datos de carácter personal será aplicable a dicho contacto directo.

Comentarios a la Sección 5 sobre Confidencialidad y Protección de Datos

1. La confidencialidad de los datos relativos a los contribuyentes ha sido siempre un pilar fundamental de los sistemas y regímenes fiscales. Tanto los contribuyentes como las administraciones tributarias tienen legalmente derecho a contar con que se preserve el carácter confidencial de los datos intercambiados. Para confiar en sus respectivos sistemas fiscales y cumplir con las obligaciones que les son legalmente exigibles, los contribuyentes necesitan saber que la información financiera, generalmente confidencial, no se divulga indebidamente, ya sea intencional o accidentalmente. Los ciudadanos y gobiernos confiarán en el intercambio internacional sólo si la información intercambiada se utiliza y divulga de conformidad con el instrumento con base en el cual se lleve a cabo dicho intercambio. Es una cuestión tanto de marco jurídico como de disponer de sistemas y procedimientos adecuados para garantizar la observancia del marco jurídico en la práctica y la no divulgación de la información sin autorización. La capacidad de proteger la confidencialidad de la información tributaria es también fruto de una «cultura responsable» en el seno de la administración tributaria, extensible al amplio espectro de sistemas, procedimientos y procesos a fin de garantizar el respeto del marco jurídico en la práctica y la protección de la seguridad e integridad de los datos que se manejan. A medida que aumenta el grado de sofisticación de una administración tributaria, han de adecuarse también las prácticas y procesos de confidencialidad que garantizan el carácter privado de la información intercambiada[2]. Varias jurisdicciones cuentan con normas específicas en materia de protección de datos de carácter personal que se aplican, igualmente, a la información relativa a los contribuyentes.

2. Las Secciones 5 y 7, junto a las afirmaciones del cuarto considerando del preámbulo, reconocen de manera explícita la transcendencia de la confidencialidad y la protección de datos en relación con el intercambio automático de información sobre cuentas financieras. Los Comentarios siguientes analizan brevemente los apartados 1 y 2, seguidos de un análisis

2. La guía con el título «Garantizando la confidencialidad», OCDE, París, 2012, se encuentra disponible en www.oecd.org/ctp/exchange-of-tax-information/informe-garantizando-la-confidencialidad.pdf.

exhaustivo de la confidencialidad y la protección de datos en relación con el ECR.

Apartado 1 – Confidencialidad y Protección de Datos Personales

3. Toda la información intercambiada estará sujeta a las normas sobre confidencialidad y demás garantías previstas en el instrumento jurídico subyacente. Esto incluye los propósitos para los cuales la información podrá ser utilizada y los límites aplicables a los sujetos a quienes podrá revelárseles dicha información.

4. Muchas jurisdicciones cuentan con normas específicas en materia de protección de datos personales igualmente aplicables a la información relativa a los contribuyentes. Entre los países que aplican normas especiales en materia de protección de datos al intercambio de información, se encuentran los Estados Miembros de la UE (ya se trate de un intercambio con otro Estado Miembro de la UE o con un tercer país o jurisdicción). Estas normas comprenden, entre otros, los derechos de acceso, rectificación, cancelación u oposición del sujeto al que se refiere la información, así como la existencia de un mecanismo de supervisión para proteger los derechos del interesado. El apartado 1 de la Sección 5 contempla que la Autoridad Competente que proporciona la información podrá especificar en el Acuerdo entre Autoridades Competentes, en la medida en que resulte necesario para garantizar el nivel exigido de protección de los datos de carácter personal, las garantías particulares exigibles al amparo de su legislación interna. Por su parte, la Autoridad Competente receptora deberá garantizar la puesta en práctica y observancia de cualquier garantía especificada, al tiempo que tratará la información recibida no sólo con arreglo a lo dispuesto en su propia normativa, sino también aplicando las medidas de seguridad adicionales que resulten exigibles para garantizar la protección de los datos en virtud de la legislación interna de la Autoridad Competente que suministra la información. Dichas garantías o medidas de seguridad adicionales, tal como especifica la Autoridad Competente que proporciona los datos, podrán referirse, por ejemplo, al acceso individual a los datos. La especificación de esas garantías puede no ser necesaria cuando la Autoridad Competente que suministra la información considere que la Autoridad Competente receptora o destinataria de la información cumple la garantía de ofrecer el nivel exigido de protección de los datos suministrados. En cualquier caso, estas garantías deberán limitarse a lo estrictamente necesario para garantizar la protección de los datos nominativos sin impedir indebidamente o retrasar el intercambio efectivo de información.

5. Los instrumentos de intercambio de información contemplan, generalmente, que no habrá de suministrarse la información a otra jurisdicción si su divulgación resulta contraria al *orden público* de la jurisdicción que

proporciona la información[3]. Aunque no resulta común que esto se traslade al contexto del intercambio de información entre Autoridades Competentes, puede que ciertas jurisdicciones exijan a sus correspondientes Autoridades Competentes que especifiquen la imposibilidad de utilizar o divulgar la información suministrada en procedimientos que podrían traducirse en la imposición y ejecución de la pena de muerte, tortura u otras graves violaciones de los derechos humanos (cuando, por ejemplo, las pesquisas fiscales están motivadas por persecuciones políticas, raciales o religiosas), ya que ello contravendría el orden público de la jurisdicción remitente. En ese caso, podrá incluirse una disposición a tal fin en el Acuerdo de Autoridad Competente.

Apartado 2 – Vulneración de la Confidencialidad

6. El asegurar la confidencialidad de la información recibida al amparo del instrumento jurídico aplicable es crucial. El apartado 2 de la Sección 5 dispone que, en caso de vulneración de la confidencialidad o de inobservancia de las garantías oportunas (incluyendo las garantías adicionales (de haberlas) especificadas por la Autoridad Competente que suministra la información), la Autoridad Competente deberá notificar inmediatamente a la otra Autoridad Competente dicha violación o inobservancia, incluyendo las sanciones y acciones correctivas que correspondan. El contenido de cualquier notificación deberá respetar las normas de confidencialidad y la legislación nacional de la jurisdicción en la que se haya producido dicha violación o inobservancia. Asimismo, la Sección 7 establece explícitamente que el incumplimiento de las disposiciones en materia de confidencialidad y protección de datos (incluidas las garantías adicionales (de haberlas) especificadas por la Autoridad Competente que proporciona la información) se considerará un incumplimiento significativo y será motivo suficiente para la suspensión inmediata del Acuerdo de Autoridad Competente.

Confidencialidad y Protección de Datos de conformidad con el ECR

7. Son tres los componentes esenciales para asegurar la aplicación de las garantías apropiadas para la protección de la información intercambiada de forma automática: *(i)* el marco jurídico, *(ii)* el sistema de gestión de la seguridad de la información: prácticas y procedimientos, y *(iii)* el mecanismo de supervisión del cumplimiento y las sanciones aplicables a una posible vulneración de la confidencialidad. Cada uno de estos aspectos se analiza más adelante. El Anexo 4 es un cuestionario[4] que traduce el debate en una

3. Véanse el ejemplo que figura en el subapartado 3(c) del Artículo 26 del Modelo de Convenio de la OCDE y el subapartado 2(d) del Artículo 21 de Asistencia Administrativa Mutua en Materia Fiscal.

4. El ejemplo de cuestionario del Anexo 4 es el utilizado por Estados Unidos para

serie de preguntas y que puede representar una herramienta de utilidad para que las jurisdicciones evalúen si se cumplen las garantías exigidas en materia de confidencialidad y protección de datos. Las jurisdicciones pueden optar por diseñar su propio cuestionario para dar traslado a los principios de la confidencialidad y la protección de datos previstos en el ECR. Puede ser que otras jurisdicciones no empleen el cuestionario por contar con una relación de intercambio automático de información con otra jurisdicción en curso y hayan expresado previamente su conformidad con las medidas de seguridad pertinentes aplicadas por la jurisdicción participante a fin de proteger la información intercambiada de forma automática.

1. Marco jurídico

8. El marco jurídico debe garantizar la confidencialidad de la información tributaria intercambiada y limitar su uso a los fines pertinentes en los términos del instrumento de intercambio de información. Los dos componentes básicos de dicho marco jurídico son los términos del instrumento aplicable y la legislación interna de la jurisdicción en cuestión.

9. Todos los convenios bilaterales y multilaterales para evitar la doble imposición, así como otros instrumentos jurídicos que regulan el intercambio de información fiscal, deben contemplar disposiciones que obliguen al mantenimiento de la confidencialidad de los datos intercambiados y limiten su uso a ciertos fines. El Modelo de Convenio de la OCDE es una muestra de ello. El apartado 2 del Artículo 26 del Modelo de Convenio establece que la información relativa a un contribuyente recibida por una Autoridad Competente recibirá el tratamiento de información confidencial, del mismo modo que la información sobre un determinado contribuyente obtenida con arreglo a la legislación interna de la jurisdicción. La divulgación de dicha información se limita a «personas o autoridades (incluyendo órganos jurisdiccionales y órganos de la administración)» encargados de la evaluación, recaudación, administración o ejecución de los impuestos comprendidos, o de actuaciones de enjuiciamiento, apelaciones o supervisión. Asimismo, se permite el uso de dicha información para otros fines siempre que lo autoricen ambas Autoridades Competentes y así lo dispongan las legislaciones nacionales de ambos Estados. De forma análoga, el Artículo 22 de la Convención sobre Asistencia Administrativa Mutua en Materia Fiscal establece el carácter confidencial de la información intercambiada y su protección, del mismo modo en que la información obtenida al amparo de la legislación interna de la parte interesada, e impone limitaciones relativas al uso y divulgación de dicha información.

---

los efectos de FATCA, en su versión del 20 de marzo de 2014, una vez suprimidas las especificaciones de Estados Unidos.

10. La legislación interna debe contemplar disposiciones suficientes para proteger la confidencialidad de la información de los contribuyentes y prever circunstancias específicas y limitadas bajo las cuales esa información podrá divulgarse y utilizarse. Asimismo, la legislación doméstica deberá imponer multas o sanciones significativas ante la divulgación o el uso indebido de la información de un contribuyente. Asimismo, la legislación interna deberá establecer que los instrumentos internacionales de intercambio de información de la jurisdicción son jurídicamente vinculantes, hasta el punto de que las obligaciones de confidencialidad contempladas en dichos instrumentos son igualmente vinculantes. Adicionalmente, las disposiciones internas en materia de garantías y seguridad de la información del contribuyente deberán resultar también aplicables a la información recibida de otro gobierno en los términos de un instrumento de intercambio.

2. Sistemas de gestión de la seguridad de la información: Prácticas y Procedimientos

11. Para que las protecciones jurídicas otorgadas por el instrumento de intercambio de información y la legislación interna sean efectivas, deben desarrollarse prácticas y procedimientos que garanticen que la información intercambiada de un contribuyente puede utilizarse, única y exclusivamente, con fines fiscales (u otros fines legalmente previstos), que impidan también la cesión de esos datos a personas o autoridades gubernamentales que no estén relacionados con la evaluación, recaudación, administración o ejecución de los impuestos comprendidos, o de actuaciones de enjuiciamiento, apelaciones o supervisión.

12. Un sistema de gestión de la seguridad de la información consiste en un conjunto de políticas, prácticas y procedimientos relativos a la gestión de la seguridad de la información, incluyendo los riesgos de TI asociados. No se trata de una simple cuestión técnica, sino que abarca también aspectos de gestión, culturales y organizativos. Como se explica con más detalle a continuación, las prácticas y procedimientos implementados por las administraciones tributarias deben abarcar todos los aspectos relevantes para la protección de la confidencialidad, incluyendo un proceso de selección del personal encargado de manejar la información, límites sobre quién(es) tiene(n) acceso a la información y sistemas de detección y rastreo de posibles casos de divulgación no autorizada. Las prácticas y procedimientos de gestión de la seguridad de la información empleados por la administración tributaria de cada jurisdicción deben adecuarse a los estándares o mejores prácticas internacionalmente aceptados que garanticen la protección de los datos confidenciales de un contribuyente[5]. Más concretamente, ello incluye los siguientes controles de referencia:

5. Los estándares internacionalmente aceptados para la seguridad de la información

2.1. Personal (comprobación de antecedentes, contratos de trabajo, formación)

13. Las administraciones tributarias deben asegurarse de que las personas que ocupen cargos de responsabilidad y tengan acceso a la información sean personas honestas y responsables, y cuyos privilegios de acceso se gestionan y supervisan pertinentemente. Los empleados, consultores y demás personal con acceso a información confidencial deben seleccionarse escrupulosamente por motivos de seguridad. Los consultores con acceso a la información de los contribuyentes deben estar sujetos contractualmente a las mismas obligaciones que el resto del personal para preservar la confidencialidad de esos datos.

14. Las administraciones tributarias deben asegurarse también de que el personal con acceso a la información conozca ampliamente las obligaciones de confidencialidad inherentes a sus cargos, los riesgos para la seguridad asociados a sus actividades, las normas, las políticas y los procedimientos en materia de seguridad/confidencialidad aplicables. Mientras el personal siga teniendo acceso a la información, deberán continuar también los cursos de formación anuales o con mayor frecuencia.

15. Asimismo, deberán existir procedimientos para suspender rápidamente el acceso a la información confidencial por parte del personal rescindido, trasladado, o jubilado, al dejar de necesitar dicho acceso. No obstante, las obligaciones en materia de confidencialidad continuarán aun cuando haya cesado el acceso a los datos.

2.2. Acceso a Instalaciones y Almacenamiento Físico de Documentos

16. Las administraciones tributarias deberán contar con medidas de seguridad para restringir el acceso a sus instalaciones. Estas medidas a menudo incluyen la presencia de guardias de seguridad, políticas en contra de visitantes no acompañados, pases de seguridad o sistemas automáticos de control de acceso del personal y límites de acceso del personal a las áreas en que se encuentra la información sensible.

---

se conocen como «serie de normas ISO/IEC 27000», publicados conjuntamente por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI). Esta serie de normas establece las mejores prácticas en materia de gestión de la seguridad de la información, riesgos y procedimientos de control en el contexto de un sistema completo de gestión de la seguridad de la información. Una administración tributaria deberá poder acreditar fácilmente que se ajusta a lo dispuesto en la serie de normas ISO/IEC 27000 o que dispone de un marco equivalente para la seguridad de la información, al tiempo que la información relativa a un determinado contribuyente, obtenida en virtud de un instrumento jurídico, está protegida con arreglo a dicho marco.

17. Las administraciones tributarias deberán también almacenar los documentos confidenciales de forma segura. Puede protegerse la información guardándola en depósitos o cámaras cerradas, tales como archivadores (cerrados mediante una combinación de seguridad o bajo llave), cajas fuertes y cámaras de seguridad, debiendo limitarse igualmente el acceso a dichas combinaciones o llaves. La seguridad de las instalaciones de almacenamiento físico variará en función de la clasificación de su contenido, debiendo otorgar la clasificación apropiada a la información tributaria transferida masivamente con motivo de un intercambio automático. Asimismo, las administraciones tributarias deberán garantizar la seguridad de los datos aun cuando éstos se trasladen a lugares de trabajo alternativos.

2.3. Planificación

18. Las administraciones tributarias deberán contar un plan de acción para desarrollar, documentar, actualizar e implementar la seguridad de los sistemas de información.

2.4. Gestión de la Configuración

19. Las administraciones tributarias deberán controlar y administrar la configuración de los sistemas de información. Para ello, deberán desarrollar, documentar, ejecutar y actualizar los controles de seguridad pertinentes.

2.5. Control del Acceso

20. Las administraciones tributarias deberán restringir el acceso al sistema a usuarios y dispositivos autorizados (incluyendo otros sistemas de información). Los usuarios autorizados sólo tendrán acceso a las operaciones y funciones que estén autorizados a desarrollar.

2.6. Identificación y Autenticación

21. Los sistemas de información deberán disponer de los medios necesarios para almacenar y autenticar la identidad de los usuarios y dispositivos que requieran acceso a los mismos. Dichos sistemas deberán ser, igualmente, capaces de identificar a cualquier usuario no autorizado e impedirle que tenga acceso a información confidencial.

2.7. Control y Responsabilidades

22. Los usuarios no autorizados podrán rendir cuenta de sus acciones solo si se pueden rastrear las mismas. En consecuencia, es esencial que las administraciones tributarias habiliten y conserven un registro de control de

los sistemas de información con el fin de supervisar, analizar, investigar e informar acerca de toda actividad irregular, no autorizada o inapropiada del sistema de información.

2.8. Mantenimiento

23. Las administraciones tributarias deberán llevar a cabo funciones de mantenimiento periódicas y oportunas de sus sistemas, así como también deben realizar controles efectivos de las herramientas, técnicas y mecanismos de mantenimiento del sistema y del personal que hace uso de los mismos.

2.9. Protección del sistema y de las Comunicaciones

24. Las administraciones tributarias deberán supervisar, controlar y proteger las comunicaciones, tanto a nivel externo como interno, de los sistemas de información. Estos controles deben incluir procedimientos destinados a eliminar archivos residuales, proporcionar confidencialidad en las transferencias de datos y validar algoritmos y módulos criptográficos.

2.10. Integridad del Sistema y de la Información

25. Las administraciones tributarias deberán identificar, notificar y corregir (o adoptar medidas correctivas para subsanar) oportunamente, cualquier incidencia en materia de tecnología y seguridad de la comunicación de la información, proporcionando protección contra códigos maliciosos y supervisando las alertas de seguridad y avisos del sistema.

2.11. Evaluaciones de Seguridad

26. Las administraciones tributarias deberán desarrollar y actualizar regularmente un protocolo de revisión de los procesos utilizados para probar, validar y autorizar los controles de seguridad para proteger los datos, corregir posibles deficiencias y minimizar riesgos. La frecuencia de dichas actualizaciones deberá llevarse a cabo en intervalos adecuados en alineación con los estándares y normas internacionalmente aceptados, o las mejores prácticas. Del mismo modo, deberán contar con un programa para revisar la forma en que se autorizan las operaciones y conexiones al sistema de información, así como los procedimientos para supervisar los controles de seguridad del sistema.

2.12. Planificación de Medidas de Contingencia

27. Las administraciones tributarias deberán establecer e implementar planes de actuación en caso de emergencia, operaciones auxiliares y un plan de recuperación de los sistemas de información en caso de catástrofe.

2.13. Evaluación de Riesgos

28. Toda administración tributaria debe evaluar el riesgo potencial de accesos no autorizados a la información de los contribuyentes, así como el riesgo y la magnitud de los daños con motivo del uso, divulgación, alteración, modificación o destrucción no autorizados de dicha información, o de los sistemas de información del contribuyente. Las administraciones tributarias deben actualizar periódicamente sus evaluaciones de riesgos, o siempre que se produzcan cambios significativos en el sistema de información, en las instalaciones en las que está ubicado dicho sistema o en otras condiciones que pueden afectar al estado de seguridad o adecuación del sistema.

2.14. Adquisición de Sistemas y Servicios

29. Las administraciones tributarias deben asegurarse de que los proveedores externos de sistemas de información encargados de procesar, almacenar y transmitir la información intercambiada conforme al instrumento jurídico que autorice dicho intercambio, empleen controles de seguridad compatibles con los requerimientos de seguridad informática necesarios.

2.15. Protección de Medios Documentales

30. Las administraciones tributarias deben proteger la información, ya se encuentre impresa o almacenada en medios digitales, restringir el acceso a la información a usuarios autorizados y desinfectar o destruir dichos medios digitales antes de su puesta a disposición o reutilización.

2.16. Identificación de Datos

31. Los datos intercambiados al amparo del instrumento jurídico por el que se rige dicho intercambio deben estar protegidos en todo momento contra cualquier divulgación involuntaria. Si la información forma parte de un archivo que incluye otros datos y es materialmente imposible aislar los unos de los otros, habrá que implementar procedimientos que garanticen que el archivo entero está salvaguardado y claramente etiquetado para indicar la inclusión de los datos intercambiados al amparo del mencionado instrumento jurídico. La información también deberá estar claramente etiquetada.

32. Es necesario implementar procedimientos que garanticen, antes de entregar dicho archivo a una persona o entidad no autorizadas a acceder a los datos intercambiados al amparo de un instrumento jurídico, que dichos datos han sido eliminados en su totalidad. En caso de que la información se encuentre almacenada en una base de datos, habrá que implementar procedimientos que garanticen que, antes de dar acceso a dicha base de datos

a una persona o entidad no autorizadas a acceder a los datos intercambiados al amparo de un instrumento jurídico, que todos los datos han sido eliminados de dicha base de datos (o particionados/protegidos de forma tal que impida que alguna persona o entidad no autorizadas puedan acceder a los mismos).

2.17. Políticas de Transferencia de Datos

33. Las administraciones tributarias deberán contar con políticas que requieran la destrucción de los datos en cuanto dejen de ser necesarios y que garanticen la eliminación segura de la información confidencial. Las trituradoras de papel, incineradoras, o incluso las destructoras de contenedores herméticos resultan apropiadas para destruir documentos en papel, mientras que los documentos electrónicos deberían borrarse cuando ya no sean necesarios. La información confidencial debe ser eliminada antes de destruir los ordenadores y dispositivos de almacenamiento en que se almacenen.

3. Supervisión del Cumplimiento de Normas y Sanciones en Caso de Vulneración de la Confidencialidad

34. Además de preservar la confidencialidad de la información intercambiada conforme a un determinado instrumento jurídico, las administraciones tributarias deberán ser capaces de garantizar que esa información será utilizada estrictamente para los fines estipulados en el acuerdo de intercambio de información. Por lo tanto, el mero hecho de adecuarse a un marco de seguridad de la información aceptable no basta, por sí solo, para proteger los datos fiscales objeto de intercambio. Por otra parte, la normativa interna debe imponer multas o sanciones por la divulgación o el uso indebidos de la información referida a un contribuyente concreto. Para garantizar su aplicación, dichas normas deben verse reforzadas por recursos y procedimientos administrativos adecuados.

3.1. Penas y Sanciones

35. La legislación interna deberá imponer multas o sanciones por la divulgación o el uso indebido de la información de un contribuyente, al tiempo que las administraciones tributarias deberán, por su parte, imponer *de facto* esas multas y sanciones al personal que infrinja las políticas y procedimientos en materia de seguridad con el fin de disuadir a otros de verse involucrados en infracciones similares. Para garantizar su aplicación, dicha legislación interna deberá reforzarse mediante recursos y procedimientos administrativos adecuados. Las administraciones tributarias deberán implementar un procedimiento sancionador formal aplicable al personal y proveedores externos de servicios que incumplan las políticas y procedimientos de seguridad de la información establecidos. Esas políticas deberán abarcar tanto sanciones civiles como penales aplicables en caso de inspección o divulgación no autorizadas.

3.2. Regulación del Acceso y Divulgación de la Información sin Autorización

36. Además de contar con políticas que regulen el acceso a la información confidencial, las administraciones tributarias también deben disponer de procedimientos para supervisar el cumplimiento de esas políticas y detectar todo acceso y divulgación de la información no autorizados. Si esto ocurre, debe realizarse una investigación seguida de la elaboración de un informe de gestión. Este informe deberá incluir:

- recomendaciones para minimizar las repercusiones del incidente;
- un análisis de cómo evitar incidentes similares en el futuro;
- recomendaciones sobre la imposición de determinadas multas o sanciones a la(s) persona(s) responsable(s) de la infracción, señalando que las fuerzas o cuerpos de seguridad deberán intervenir cuando existan sospechas de revelación intencionada de datos, y
- razones en las que se fundamenta la sólida convicción conforme a la que, una vez implementadas, las novedades normativas y las sanciones recomendadas desincentivarán la comisión de infracciones similares en el futuro.

37. Adicionalmente, las administraciones tributarias deberán contar con un procedimiento de revisión y aprobación de recomendaciones sobre cambios normativos y procedimentales con el fin de evitar futuras violaciones. Los servicios de inspección o los órganos de dirección de las administraciones tributarias deberán asegurarse de que se implementen las recomendaciones aprobadas.

Comentarios a la Sección 6
Sobre Consultas y Modificaciones

1. Esta Sección versa sobre las consultas entre Autoridades Competentes y sobre las modificaciones al Acuerdo entre Autoridades Competentes (AAC).

Apartado 1 – Consultas

2. Este apartado dispone que, en caso de surgir dificultades en la aplicación o la interpretación del presente Acuerdo, cualesquiera de las Autoridades Competentes podrán formular consultas para el desarrollo de medidas que garanticen el cumplimiento de este Acuerdo. También podrán formularse las consultas pertinentes para analizar la calidad de la información recibida.

3. Las Autoridades Competentes podrán comunicarse entre sí por carta, fax, teléfono, reuniones directas o por cualquier otro medio pertinente, con el fin de alcanzar un acuerdo sobre medidas que garanticen el cumplimiento de este Acuerdo.

Apartado 2 – Modificaciones

4. Este apartado aclara que el Acuerdo podrá modificarse mediante consentimiento escrito de las Autoridades Competentes. Salvo que las Autoridades Competentes dispongan lo contrario, dicha modificación será efectiva el primer día del mes siguiente al periodo de un mes contado a partir de la última entre:

- la fecha de firma de dicho acuerdo escrito, o
- la fecha en que las notificaciones sean intercambiadas para los efectos de ese acuerdo escrito.

5. Tal como se pone de manifiesto en la Introducción a los Comentarios al Modelo Acuerdo de Autoridad Competente, las jurisdicciones podrán suscribir un acuerdo intergubernamental multilateral, o bien múltiples acuerdos intergubernamentales que, por derecho propio, constituirían convenios internacionales que abarcan tanto las obligaciones de reporte como los procedimientos de debida diligencia, acompañados de un ACC de alcance más limitado. En estos casos, se aplicarán normas distintas respecto de dichas modificaciones.

Comentarios a la Sección 7 sobre Vigencia del Acuerdo

Apartado 1 – Entrada en vigor

1. El apartado 1 prevé dos alternativas relativas a la fecha de entrada en vigor. La primera, cuando las jurisdicciones suscriban este Acuerdo tras haber implementado ambas la legislación necesaria para implementar el ECR, dichas jurisdicciones fijarán una fecha de entrada en vigor del Acuerdo. La segunda, si las Autoridades Competentes firman el Acuerdo antes de que una o ambas jurisdicciones hayan implementado la legislación necesaria, podrán optar por esta segunda alternativa, en cuyo caso el Acuerdo entrará en vigor en la fecha de la última notificación efectuada para indicar que la jurisdicción en cuestión ha adoptado la legislación necesaria para dar cumplimiento al Acuerdo.

Apartado 2 – Suspensión

2. El apartado 2 contiene los pormenores sobre la posibilidad que tiene una Autoridad Competente de suspender el Acuerdo cuando determine que existe, o ha existido, un incumplimiento significativo por parte de la otra Autoridad Competente. En la medida de lo posible, las Autoridades Competentes deberán intentar resolver posibles problemas de incumplimiento, incluso aquéllos de incumplimiento significativo, antes de notificar su intención de suspender los efectos del Acuerdo.

3. Para suspender el Acuerdo, una Autoridad Competente deberá notificar por escrito a la otra Autoridad Competente su intención de suspender los efectos del Acuerdo. La notificación deberá contener una descripción detallada del incumplimiento significativo que se haya verificado, o se esté verificando, y, siempre que sea posible, una descripción de los pasos que deberán seguirse para resolver el problema. Dicha suspensión causará efecto inmediato.

4. La Autoridad Competente notificada deberá, tan pronto como sea posible, emprender las iniciativas necesarias para abordar el incumplimiento significativo. Una vez que el incumplimiento se haya resuelto, la Autoridad

Competente notificada deberá ponerlo en conocimiento de la otra Autoridad Competente. Tras la resolución satisfactoria del problema, la Autoridad Competente que envió la notificación de suspensión deberá confirmar por escrito a la Autoridad Competente notificada que el Acuerdo vuelve a tener efecto, por lo que el intercambio de información se restablecerá a la mayor brevedad posible.

5. El apartado 2 dispone que el incumplimiento significativo incluye, pero no está limitado a:

- la inobservancia de las disposiciones en materia de confidencialidad y protección de datos del presente Acuerdo (incluyendo las garantías adicionales especificadas en el Acuerdo de Autoridad Competente) como, por ejemplo, que la información se utiliza para fines no previstos en el instrumento jurídico subyacente por el que se rige el intercambio, o que la legislación interna sea modificada de modo tal que se comprometa la confidencialidad de la información;
- la omisión por la Autoridad Competente de la obligación de proporcionar información en plazo o adecuada, tal como prevé este Acuerdo;
- la determinación del estatus de Cuentas Excluidas o de Instituciones Financieras No Sujetas a Reportar, de manera tal que resulte inconsistente con los objetivos del ECR y frustre los mismos, o
- la inexistencia de normas y procedimientos administrativos para garantizar la aplicación efectiva de los procedimientos de reporte y debida diligencia contemplados en el ECR.

6. Mientras la suspensión esté en vigor, toda la información que haya sido recibida en los términos del Acuerdo mantendrá el carácter confidencial y deberá ajustarse a lo previsto en la Sección 5 del Acuerdo, incluyendo cualquier otra garantía adicional en materia de protección de datos especificada por la Autoridad Competente que proporciona la información y por el instrumento jurídico subyacente.

Apartado 3 – Denuncia

7. El apartado 3 contiene la cláusula de denuncia. Cualquiera de las Autoridades Competentes podrá denunciar el presente Acuerdo mediante la notificación de denuncia por escrito a la otra Autoridad Competente. La denuncia así notificada será efectiva el primer día del mes siguiente a la expiración del plazo de 12 meses, contados a partir de la fecha de la notificación de denuncia. Así, por ejemplo, una Autoridad Competente podrá optar por denunciar el presente Acuerdo en caso de que se haya suspendido el mismo y la otra Autoridad Competente no haya resuelto problemas de incumplimiento significativo en un plazo razonable.

8. La denuncia del instrumento jurídico subyacente en virtud del cual se haya suscrito el Acuerdo de Autoridad Competente dará lugar a la denuncia automática de éste. Por consiguiente, en tales circunstancias, no será necesario denunciar el Acuerdo de Autoridad Competente por separado.

9. El apartado 3 estipula que, en caso de denuncia, toda la información que haya sido recibida en los términos del Acuerdo mantendrá el carácter confidencial y deberá ajustarse a lo previsto en la Sección 5 del Acuerdo, incluyendo cualquier otra garantía adicional en materia de protección de datos especificada por la Autoridad Competente que proporciona la información y por el instrumento jurídico subyacente.