Asociación Española de Compliance

# Grupos de trabajo de ASCOM

# Prevención del blanqueo de capitales

## Las buenas prácticas de PBC

Septiembre 2020

www.asociacioncompliance.com

# Las buenas prácticas de PBC

## I. IDENTIFICACIÓN FORMAL E IDENTIFICACIÓN DEL TITULAR REAL

### 1. Identificación formal del cliente

Consiste en la identificación y comprobación con carácter previo al establecimiento de la relación de negocios o a la ejecución de cualesquiera operaciones, mediante documentos fehacientes, de la identidad del cliente.

Los documentos de identificación deberán encontrarse en vigor en el momento de establecer relaciones de negocio o ejecutar operaciones ocasionales. En el supuesto de personas jurídicas, la vigencia de los datos consignados en la documentación aportada deberá acreditarse mediante una declaración responsable del cliente.

#### 1.1. En el caso de personas físicas, los documentos válidos para cumplir este requisito podrían ser:

- En el caso de personas físicas de nacionalidad española: El Documento Nacional de Identidad (DNI) o el Pasaporte.
- En el caso de personas físicas de nacionalidad extranjera: la Tarjeta de Identidad de Extranjero, el Pasaporte, la Tarjeta de Residencia o, en el caso de ciudadanos de la Unión Europea o del Espacio Económico Europeo, el documento oficial de identidad personal expedido por las autoridades de origen.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

### 1.2 . En el caso de personas jurídicas consiste en la obtención de los documentos públicos que acrediten su existencia y contengan su denominación social, domicilio, forma jurídica, estatutos, la identidad de sus administradores, y número de identificación fiscal. Los documentos válidos para cumplir este requisito podrían ser:

En el caso de compañías residentes en España:

- Escritura actualizada de constitución registrada en el Registro Mercantil y tarjeta del CIF.
- Certificación emitida por el Registrador Mercantil, que incluya la información necesaria.

En el caso de compañías extranjeras sin establecimiento permanente en España:

- Los documentos públicos que acrediten la información requerida, junto con una traducción jurada en caso de que sea necesario.

Para la obtención de los documentos públicos que acrediten los poderes de los representantes de la sociedad autorizados en la relación de negocio con el sujeto obligado, los documentos válidos para cumplir este requisito podrían ser:

1. En cuanto a los documentos de identidad de los apoderados, los documentos válidos para cumplir este requisito serían los mismos que los mencionados en el apartado 1.1.
2. En cuanto a los poderes:

   En el caso de compañías residentes en España:

   - Certificación emitida por el Registrador Mercantil probatoria de dichos poderes.
   - Las escrituras de poder en vigor y registradas en el Registro Mercantil, que acrediten las facultades otorgadas a los apoderados.

   En el caso de compañías extranjeras sin establecimiento permanente en España:

   - Los documentos públicos que acrediten los poderes otorgados, junto con una traducción jurada en caso de que sea necesario.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

## 2. Titular Real:

La persona o personas físicas por cuya cuenta se pretenda establecer una relación de negocios o intervenir en cualesquiera operaciones.

La persona o personas físicas que:

a) en último término posean o controlen, directa o indirectamente, un porcentaje superior al 25 por ciento del capital o de los derechos de voto de una persona jurídica, o que

b) a través de acuerdos o disposiciones estatutarias o por otros medios ejerzan el control, directo o indirecto, de la gestión de una persona jurídica.

Cuando no exista una persona física que posea o controle, directa o indirectamente, un porcentaje superior al 25 por ciento del capital o de los derechos de voto de la persona jurídica, o que por otros medios ejerza el control, directo o indirecto, de la persona jurídica, se considerará que ejerce dicho control el administrador o administradores.

En el caso de los fideicomisos, como el trust anglosajón, tendrán la consideración de titulares reales todas las personas siguientes:

1º el fideicomitente, aquél que entrega los bienes al sujeto denominado fiduciario para que realice el fin a que se destine el fideicomiso,

2º el fiduciario o fiduciarios, persona física o moral encargada de un fideicomiso y de la propiedad de los bienes que lo integran, a solicitud de un fideicomitente y en beneficio de un tercero,

3º el protector, si lo hubiera, cuyo fin es salvaguardar los activos del fideicomiso,

4º los beneficiarios o, cuando aún estén por designar, la categoría de personas en beneficio de la cual se ha creado o actúa la estructura jurídica; y

5º cualquier otra persona física que ejerza en último término el control del fideicomiso a través de la propiedad directa o indirecta o a través de otros medios.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

En el supuesto de instrumentos jurídicos análogos al trust, como las fiducias o el treuhand de la legislación alemana, los sujetos obligados identificarán y adoptarán medidas adecuadas a fin de comprobar la identidad de las personas que ocupen posiciones equivalentes o similares a las relacionadas en los números 1.º a 5.º del apartado anterior.

La identificación y comprobación de la identidad del titular real podrá realizarse, con carácter general, mediante una declaración responsable del cliente o de la persona que tenga atribuida la representación de la persona jurídica.

Para la obtención de la información y documentación para determinar la estructura de propiedad y control del cliente, podrían ser válidos cualquiera de los siguientes documentos:

- Estructura corporativa
- Documento firmado por un representante indicando la estructura accionarial
- Otros documentos fidedignos como por ejemplo un informe obtenido de proveedores profesionales de información

# 3. Medidas de diligencia:

## 3.1. Medidas de diligencia debida normales y reforzadas para clientes de riesgo tanto Medio como Alto:

Comprobar la información sobre los titulares reales manifestados por el cliente. A esta finalidad, podrían ser válidos los siguientes tipos de documentos:

- Informes adquiridos de registros mercantiles que incluyan información sobre los titulares reales
- Acta notarial de titularidad real
- Últimas cuentas anuales que incluyan información sobre los titulares reales o estructura accionarial
- Informe obtenido de proveedores profesionales de información siempre que incluya información completa sobre los titulares reales

## 3.2. Medidas simplificadas de diligencia debida para clientes de riesgo Bajo:

No verificar la identidad del cliente y del titular o titulares reales, excepto que se considere oportuno en base a las circunstancias específicas de la relación de negocios (por ejemplo: volúmenes operativos elevados, factores de riesgo identificados, etc.).



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# 4. Principales novedades de la Quinta Directiva (DIRECTIVA (UE) 2018/843 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 30 de mayo de 2018) con relación a la identificación del cliente y obtención del titular real:

## 4.1. Obligación de identificar al consumidor para las tarjetas anónimas de prepago de uso múltiple, en caso de operaciones remotas de pago cuyo importe sea superior a 50 EUR:

*(14) Las tarjetas de prepago de uso múltiple tienen utilizaciones legítimas y son un instrumento que contribuye a la inclusión social y financiera. No obstante, las tarjetas de prepago anónimas son fáciles de utilizar para financiar la logística y los atentados terroristas. Resulta por lo tanto esencial privar a los terroristas de ese medio de financiación de sus operaciones, reduciendo más aún los límites y los importes máximos por debajo de los cuales se autoriza a las entidades obligadas a no aplicar algunas de las medidas de diligencia debida con respecto al cliente contempladas en la Directiva (UE) 2015/849. Por tanto, sin dejar de lado las necesidades de los consumidores en cuanto a la utilización de instrumentos de prepago de uso múltiple y sin impedir su empleo para fomentar la inclusión social y financiera, es esencial rebajar los umbrales actualmente aplicables a las tarjetas anónimas de prepago de uso múltiple e identificar al consumidor en caso de operaciones remotas de pago cuyo importe sea superior a 50 EUR.*

## 4.2. Los Estados miembros deben facilitar el acceso a la información relativa a la titularidad real a través de registros centrales:

*(33) Los Estados miembros deben por lo tanto facilitar el acceso a la información relativa a la titularidad real de las sociedades y otras entidades jurídicas de una manera*



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

*suficientemente coherente y coordinada, a través de registros centrales en los que se exponga información relativa a esa titularidad real y de unas normas claras de acceso público, de forma que los terceros puedan determinar, en toda la Unión, quiénes son los titulares reales de las sociedades y otras entidades jurídicas. Es esencial establecer asimismo un marco jurídico coherente que garantice un mejor acceso a la información relativa a la titularidad real de los fideicomisos (del tipo «trust») e instrumentos jurídicos análogos, una vez registrados en la Unión. Las normas aplicables a los fideicomisos (del tipo «trust») e instrumentos jurídicos análogos en lo que respecta al acceso a la información relativa a su titularidad real deben ser comparables a las normas correspondientes que se aplican a las sociedades y otras entidades jurídicas.*

### 4.3. Interconexión de los registros centrales de los Estados miembros que contengan información relativa a los beneficiarios reales:

*(37) La interconexión de los registros centrales de los Estados miembros que contengan información relativa a los beneficiarios reales a través de la plataforma central europea creada en virtud de la Directiva (UE) 2017/1132 del Parlamento Europeo y del Consejo (1) requiere la coordinación de sistemas nacionales con características técnicas diversas. Ello implica la adopción de medidas y especificaciones técnicas que habrán de tener en cuenta las diferencias entre los registros. A fin de garantizar condiciones uniformes de ejecución de la presente Directiva, deben conferirse a la Comisión competencias de ejecución para abordar estos problemas técnicos y operativos. Dichas competencias deben ejercerse de conformidad con el procedimiento de examen previsto en el artículo 5 del Reglamento (UE) n.o 182/2011 del Parlamento Europeo y del Consejo (2). En cualquier caso, la participación de los Estados miembros en el funcionamiento del sistema en su conjunto debe asegurarse por medio de un diálogo periódico entre la Comisión y los representantes de los Estados miembros sobre las cuestiones referentes al funcionamiento del sistema y su futuro desarrollo.*

### 4.4. El registro de información relativa a la titularidad real de los fideicomisos (del tipo «trust») e instrumentos jurídicos análogos:

*(26) Debe aclararse el factor específico que determina qué Estado miembro es responsable de la vigilancia y el registro de información relativa a la titularidad real de los fideicomisos (del tipo «trust») e instrumentos jurídicos análogos. Debido a las diferencias entre los ordenamientos jurídicos de los Estados miembros, algunos fideicomisos (del tipo «trust») e instrumentos jurídicos análogos no son objeto de vigilancia ni están registrados en ningún lugar de la Unión. La información sobre la titularidad real de los fideicomisos (del tipo «trust») y de los instrumentos jurídicos análogos se debe registrar en el lugar de establecimiento o residencia de*



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

*los fiduciarios de tales fideicomisos y de las personas que ostenten una posición equivalente en instrumentos jurídicos análogos. La vigilancia efectiva y el registro de la información sobre la titularidad real de dichos fideicomisos (del tipo «trust») y los instrumentos jurídicos análogos requieren, además, la cooperación entre los Estados miembros. La interconexión de los registros de los Estados miembros de titulares reales de tales fideicomisos e instrumentos jurídicos análogos haría accesible esta información, y además aseguraría que se evite el registro múltiple de los mismos fideicomisos e instrumentos jurídicos análogos dentro de la Unión.*



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

| IDENTIFICACIÓN: Consiste en la identificación y comprobación con carácter previo, mediante documentos fehacientes, de la identidad del cliente | | |
|---|---|---|
| **Tipos** | **Nacionalidad** | **Posible documentación valida** |
| Personas Físicas | Nacionalidad Española | DNI o Pasaporte |
| | Nacionalidad Extranjera | Tarjeta de Residencia |
| | | Pasaporte |
| | | Tarjeta de Identidad de Extranjero |
| Personas Jurídicas | Residentes en España | Escritura actualizada de constitución registrada en el Registro Mercantil |
| | | Tarjeta del CIF |
| | | Certificación emitida por el Registrador Mercantil |
| | Extranjeras sin establecimiento permanente en España | Los documentos públicos que acrediten la información requerida, junto con una traducción jurada en caso de que sea necesario. |
| **OBTENCIÓN TITULAR REAL: persona física o personas físicas que en último término posean o controlen, directa o indirectamente, un porcentaje superior al 25 por ciento del capital o de los derechos de voto de una persona jurídica, o que a través de acuerdos o disposiciones estatutarias o por otros medios ejerzan el control, directo o indirecto, de la gestión de una persona jurídica. Cuando no exista una persona física se considerará que ejerce dicho control el administrador o administradores.** | | |
| Para la obtención de la información y documentación para determinar la estructura de propiedad y control del cliente, podrían ser válidos cualquiera de los siguientes documentos:<br>• Estructura corporativa<br>• Documento firmado por un representante indicando la estructura accionarial<br>• Otros documentos fidedignos como por ejemplo un informe obtenido de proveedores profesionales de información | | |
| **Nota:En el supuesto de instrumentos jurídicos como el trust, como las fiducias o el treuhand de la legislación alemana, los sujetos obligados identificarán y adoptarán medidas adecuadas a fin de comprobar la identidad de las personas que ocupen posiciones equivalentes o similares.** | | |

| MEDIDAS DE DILIGENCIA DEBIDA EN FUNCIÓN AL RIESGO | | |
|---|---|---|
| **TIPO DE DILIGENCIA** | **QUÉ HACER** | **CÓMO** |
| Medidas de diligencia debida normales y reforzadas para clientes de **riesgo tanto Medio como Alto:** | Verificar la información sobre los titulares reales declarados por el cliente. | Informes de registros mercantiles o similares |
| | | Acta notarial de titularidad real |
| | | Últimas cuentas anuales (si incluyen los titulares reales o estructura accionarial) |
| | | Informe de proveedores de información siempre que contenga los titulares reales |
| Medidas simplificadas de diligencia debida para clientes de **riesgo Bajo:** | No verificar la identidad del cliente y del titular o titulares reales, salvo que se considere apropiado en base a las circunstancias específicas de la relación de negocios (ej. factores de riesgo identificados, volúmenes operativos | |

| NOVEDADES V DIRECTIVA DE BLANQUEO relativas a identificación de cliente y obtención de titular real |
|---|
| Obligación de identificar al consumidor para las tarjetas anónimas de prepago de uso múltiple, en caso de operaciones remotas de pago cuyo importe sea super |
| Los Estados miembros deben facilitar el acceso a la información relativa a la titularidad real a través de registros centrales |
| Interconexión de los registros centrales de los Estados miembros que contengan información relativa a los beneficiarios reales |
| El registro de información relativa a la titularidad real de los fideicomisos (del tipo «trust») e instrumentos jurídicos análogos |



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# II. PROPÓSITO E ÍNDOLE DE LA RELACIÓN DE NEGOCIOS Y ORIGEN DE FONDOS

El artículo 5 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, así como el artículo 10 del Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, tratan, definen y desarrollan el concepto de propósito e índole de los negocios.

Así pues, se establece que los sujetos obligados están obligados a recabar de sus clientes información a fin de conocer la naturaleza de su actividad profesional o empresarial, que será registrada por el sujeto obligado con carácter previo al inicio de la relación de negocios y adoptarán medidas dirigidas a comprobar razonablemente la veracidad de dicha información.

Según el Artículo 5 de la Ley 10/2010, las medidas que debe tomar el sujeto obligados para el conocimiento del cliente son las siguientes:

- Obtención de información sobre el propósito e índole prevista de la relación de negocios.
- Obtención de información a fin de conocer la naturaleza de su actividad profesional y empresarial.
- Comprobación razonable de la veracidad de la información aportada por el cliente.
- Establecimiento y aplicación de procedimientos de verificación de la actividad declarada por el cliente.
- Obtención del cliente de los documentos que guarden relación con la actividad declarada.
- Obtención de información ajena al propio cliente sobre la actividad declarada

Los sujetos obligados deberán comprobar las actividades declaradas por los clientes en los supuestos indicados



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

más abajo, ya sea mediante documentación aportada por el cliente, mediante la obtención de información de fuentes fiables independientes o mediante la realización de visitas presenciales a las oficinas, almacenes o locales declarados por el cliente como lugares donde ejerce su actividad mercantil, dejando constancia por escrito del resultado de dicha visita:

a. Cuando el cliente o la relación de negocios presenten riesgos superiores al promedio, por disposición normativa o porque así se desprenda del análisis de riesgo del sujeto obligado.

b. Cuando del seguimiento de la relación de negocios resulte que las operaciones activas o pasivas del cliente no se corresponden con su actividad declarada o con sus antecedentes operativos.

c. Cuando concurran circunstancias que determinen el examen especial de conformidad con el artículo 17 de la Ley 10/2010 o la comunicación por indicio de conformidad con el artículo 18 de la Ley 10/2010.

Además de todo esto, existe de la obligación de hacer un seguimiento de la relación de negocios a fin de garantizar que coincidan con el conocimiento que tenga el sujeto obligado del cliente y de su perfil empresarial y de riesgo, ya que este estudio del propósito e índole de los negocios, no tiene razón de ser sin un seguimiento de los mismos.

Igualmente los sujetos obligados deberán incrementar tal seguimiento cuando aprecien riesgos superiores al promedio (por disposición normativa o porque así se desprenda del análisis de riesgo del sujeto obligado), actualizando el seguimiento periódicamente.

Como se ha indicado, además de determinar el propósito e índole de los negocios, las entidades aplicarán medidas de seguimiento continuo a la relación de negocios, incluido el escrutinio de las operaciones efectuadas a lo largo de dicha relación a fin de garantizar que coincidan con la actividad profesional o empresarial del cliente y con sus antecedentes operativos, así como que se aseguren de que los documentos, datos e informaciones obtenidos como consecuencia de la aplicación de las medidas de debida diligencia se mantengan actualizados y se encuentren vigentes.

El escrutinio tendrá carácter integral, debiendo incorporar todos los productos del cliente con el sujeto obligado y, en su caso, con otras sociedades del grupo.

El incumplimiento de la aplicación de estas medidas de diligencia debida, implica la comisión de una infracción, así como la interposición de su correspondiente sanción.

Están consideradas como infracción grave, entre otras, y contempladas en la LPBC y FT:



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

- El incumplimiento de la obligación de obtener información sobre el propósito e índole de la relación de negocios (art. 52 c) Ley 10/2010).
- El incumplimiento de la obligación de aplicar medidas de seguimiento continuo a la relación de negocios, en su caso (art. 52 d) Ley 10/2010).

Establecida la graduación de la infracción, las sanciones (art. 57 Ley 10/2010) pueden ser diversas, desde sanciones, amonestaciones, y la posibilidad además, de sancionar a administradores.

Cabe destacar que, los sujetos obligados, no establecerán relaciones de negocio, ni ejecutarán operaciones cuando no puedan aplicar las medidas de diligencia debida que prevé la ley, poniendo fin a la relación de negocios cuando no puedan aplicar dichas medidas; la negativa de las entidades a establecer relaciones de negocio o a ejecutar operaciones o la terminación de la relación por no poder aplicar las medidas de diligencia debida no conllevará, salvo que medie enriquecimiento injusto, ningún tipo de responsabilidad para la entidad.

Ente los documentos que se podrían solicitar al cliente se pueden señalar los siguientes:

### Clientes personas físicas asalariados o pensionistas

- Nómina, pensión o subsidio reciente.
- Certificado de haberes, pensión o subsidio reciente.
- Certificado de vida laboral.
- Contrato laboral vigente.
- Última declaración del I.R.P.F.
- Informe de visita a las instalaciones de la empresa del cliente.
- Cualquier otro documento que acredite razonablemente la actividad del cliente.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

## Clientes personas físicas profesionales liberales o autónomos

- Acreditación del pago de los seguros sociales.
- Carné del colegio o asociación profesional.
- Recibo reciente del colegio o asociación profesional correspondiente.
- Recibo de la seguridad social de autónomos.
- Alta de la licencia fiscal.
- Última declaración del I.R.P.F.
- Última declaración del I.V.A. o retención del I.R.P.F.
- Autorización administrativa, en su caso (por ejemplo, tarjeta de transporte).
- Informe de visita a las oficinas del cliente, si las hubiera.
- Cualquier otro documento que acredite razonablemente la actividad del cliente.

Respecto a la actividad profesional de los clientes, se aplicarán, con carácter general, las siguientes reglas:

- Clientes de riesgo bajo: se inferirá el propósito y naturaleza de la misma por el tipo de operaciones o relación de negocios establecida.
- Clientes de riesgo medio: bastará con una declaración del cliente.
- Clientes de riesgo alto: se exige la comprobación de la actividad declarada por el cliente.

## Otros clientes personas físicas (menores, amas de casa, estudiantes, rentistas, religiosos, etc.)

- Última declaración del I.R.P.F., en su caso.
- Beca, en su caso.
- Matrícula académica.
- Carné de estudiante.
- Contratos de alquiler de inmuebles, si procede.
- Contratos de venta de inmuebles, si procede.
- Contratos de ventas societarias, si procede.
- Posiciones de valores (acredita el cobro de dividendos de relevancia), si procede.
- Cualquier otro documento que acredite razonablemente la capacidad de generación de fondos del cliente.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

## Clientes personas jurídicas

- Alta de la licencia fiscal.
- Último Impuesto de Sociedades, en caso de ser una sociedad mercantil.
- Última declaración del I.V.A., en caso de ser una sociedad mercantil.
- Memoria anual de actividades.
- Cuentas anuales.
- Auditoría externa anual.
- Presupuestos del ejercicio.
- Consultas a bases de datos de sociedades mercantiles sobre la sociedad cliente.
- Informe de visita a las oficinas del cliente.
- Cualquier otra documentación comercial, financiera o legal que acredite razonablemente la actividad.

Tras desarrollas y evaluar lo que implica la medida del estudio del propósito e índole de los negocios, pasamos a indicar algunos ejemplos de indicadores de riesgo clasificados por sujetos obligados (algunos), en relación con esta medida, y que han sido extraídos del amplio catálogo de operaciones de riesgo, que la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias pone a nuestra disposición.

## Indicadores de riesgo en función del sujeto obligado de que se trate:

- **Entidades aseguradoras y corredores de seguros (ramo de vida):**

  a. Negativa o resistencia a facilitar la información y documentación necesaria para conocer sus actividades y restantes circunstancias relacionadas con la contratación de una póliza.

  b. Uso de datos de identidad falsos, o voluntariamente, erróneos, relativos a la actividad que acredita su capacidad económica, en el proceso de contratación de una póliza



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

c. En los procesos de contratación de productos a través de canales no presenciales (internet, atención telefónica, correo, etc.) debe valorarse el riesgo de alteración, total o parcial, de los documentos de identidad y otros relacionados con la actividad o capacidad económica de los contratantes.

d. Intervinientes sobre los que exista constancia de su relación con actividades criminales o grupos terroristas, o que hayan sido condenados por delitos, o que estén relacionados con personas que se encuentren en alguno de los casos anteriores.

e. Los intervinientes en las pólizas deberán acreditar su relación y la razón por la que cada uno asume una posición concreta.

f. Tomadores individuales que mantengan varias pólizas en iguales o diferentes productos cuya suma total de las primas represente un importe excesivo en relación a sus ingresos declarados y su perfil de negocio.

- **Entidades de crédito:**

a) Ingresos en efectivo de billetes de alta cuantía en comparación con el tipo de negocio de la cuenta.

b) Cualquier cuenta que no muestra coherencia con las actividades normales bancarias o de negocios, pero que se utilizan por personas o sociedades para recibir o abonar fondos que no tienen una relación clara con el titular de esa cuenta y/o su negocio.

c) Abonos en cuenta de numerosas operaciones con tarjetas con disposición inmediata. Estos abonos se suelen realizar en cuentas de sociedades de reciente constitución, lo que dificulta el conocimiento de la naturaleza de su actividad profesional o empresarial así como la relación de negocios.

d) Representantes que dificulten o pretendan ocultar la identidad del último beneficiario o persona que corresponda, contrariamente al procedimiento normal para el tipo de negocios de que se trate.

- **Entidades de pago, cambio de moneda o actividades de giro o transferencia:**

a) Existencia de dudas sobre la veracidad de los datos aportados por el cliente sobre su actividad, el origen o el destino de los fondos.

b) Operaciones que por su cuantía o periodicidad no se corresponden con el status económico del cliente o los ingresos generados por su actividad.

c) Empresa o empresario que actuando como cliente:

i. participa en operaciones que se suelen realizar con billetes de alta denominación cuando las características de su actividad no justifica dicho uso



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

ii. ordena o recibe transferencias a/de personas en otros países sin que haya un motivo comercial aparente o para la que da una explicación incoherente con la naturaleza de su negocio o actividad

iii. es renuente a dar información completa sobre el tipo de negocio, propósito de la operación o cualquier otra información requerida por el establecimiento.

d) Clientes que señalan como origen de los fondos expresiones generales como ahorro, trabajo, venta, etc., sin ninguna referencia sobre la operación o actividad generadora de los fondos.

e) Operaciones sin una razón comercial aparente o que no se corresponde con los negocios del cliente o sus antecedentes operativos.

- **Notarios, registradores, abogados, auditores y otros profesionales.**

a) Clientes que se presentan como una entidad de negocios pero que no tienen información pública sobre su actividad (página web, publicidad, o difusión en internet)



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# III. PERSONAS CON RESPONSABILIDAD PÚBLICA Y TRATAMIENTO DE DATOS DE PERSONAS CON RESPONSABILIDAD PÚBLICA

## Personas con responsabilidad pública = medidas de diligencia debida reforzada

| ÁMBITO | FUNCIÓN PÚBLICA |
|---|---|
| **Gobierno estatal** | Jefes de Estado/Gobierno (Presidente) |
| | Vicepresidente del Gobierno |
| | Miembros del Gobierno entre los que se encuentran los Ministros. |
| | Secretarios de Estado, Subsecretarios, Secretarios Generales y Secretarios Generales Técnicos |
| | Diputados nacionales |
| | Senadores |
| | Directores Generales de la Administración General del Estado |
| **Gobierno Autonómico** | Presidentes |
| | Vicepresidente |
| | Diputados Autonómicos |
| | Consejeros |
| | Miembros de los Consejos de Gobierno (ej. Directores generales) |
| | Delegados de Gobierno en las Comunidades Autónomas, Ceuta y Melilla |
| **Gobierno Local (población > 50.000 habitantes)** | Alcaldes |
| | Concejales |
| **Relacionados con tribunales** | Magistrados del Tribunal Supremo |
| | Magistrados del Tribunal Constitucional |
| | Magistrados de instancias judiciales que no admitan recurso. |
| | Altos miembros del Ministerio Fiscal |
| | Altos miembros del Tribunal de Cuentas |
| **Personal Militar** | Alto personal militar de las Fuerzas Armadas |
| **Personal Diplomático** | Embajadores |
| | Encargados de negocios |
| | Jefes de misión diplomática permanente |



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

| ÁMBITO | FUNCIÓN PÚBLICA |
|---|---|
| **Entidades públicas** | Miembros del Consejo de Bancos Centrales |
| | Presidentes, vicepresidentes, Directores Generales, Directores Ejecutivos y Subdirectores Generales (cuando su nombramiento se efectúa por decisión del Consejo de Ministros o por sus propios órganos de gobierno) |
| | Delegados de Gobierno en Entidades de Derecho Público |
| | Director General de Entidades Gestoras y Servicios Comunes de la Seguridad Social |
| | Presidentes y Directores de las Agencias Estatales |
| | Presidentes y Directores de las Autoridades Portuarias |
| | Presidente y Secretario General del Consejo Económico y Social |
| | Presidente, Vicepresidente y resto de miembros del Consejo de la CNMC (Comisión Nacional de Mercados y de la Competencia) |
| | Presidente del Consejo de Transparencia y Buen Gobierno |
| | Presidente de la Autoridad Independiente de Responsabilidad Fiscal |
| | Presidente, Vicepresidente y Vocales del Consejo de la CNMV (Comisión Nacional del Mercado de Valores) |
| | Presidente, Consejeros y Secretario General del Consejo de Seguridad Nuclear |
| | Presidente, Directores, Directores Ejecutivo y Secretarios Generales o equivalentes y miembros de los órganos rectores de cualquier otro organismo regulador o de supervisión. |
| **Organizaciones internacionales** | Directores, incluidos directores adjuntos |
| | Miembros del consejo de administración o función equivalente |
| | Jefes de representación permanente ante organizaciones internacionales |
| **Partidos políticos (solo con representación parlamentaria)** | Miembros de la alta dirección |
| **Organizaciones sindicales y empresariales** | Miembros de la alta dirección |

**No tendrá la consideración de alto cargo quien sea nombrado por el Consejo de Ministros para el ejercicio temporal de alguna función o representación pública y no tenga en ese momento la condición de alto cargo.*



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

### Familiares y allegados a PEP = medidas de diligencia debida reforzada

| CONSIDERACIÓN | TIPO DE RELACIÓN |
|---|---|
| FAMILIAR | Cónyuge o persona ligada de forma estable por análoga relación de afectividad |
| | Padres |
| | Hijos |
| | Cónyuge o personas ligadas a los hijos de forma estable por análoga relación de afectividad |
| ALLEGADO | Toda persona que ostente la titularidad o control de un instrumento o persona jurídicos conjuntamente con una persona con responsabilidad pública. Se incluye aquéllos que se hayan constituido en beneficio de la misma. |
| | Toda persona que mantenga relaciones empresariales estrechas con una persona con responsabilidad pública |

## NOVEDADES 4ª DIRECTIVA

- No hay distinción de riesgo entre PEPs nacionales y extranjeros
- Incluye el supuesto de beneficiarios de pólizas de seguros de vida que sean PEP. En estos casos, se han de aplicar medidas de diligencia debida antes de proceder al pago, rescate, etc.: informar al inmediato nivel directivo, llevar a cabo comprobaciones adicionales sobre el tomador de la póliza y realizar un examen especial para determinar si es susceptible de comunicar por indicio de blanqueo.
- Transcurrido el plazo de 2 años desde el cese del desempeño de sus funciones, el sujeto obligado aplicará medidas de diligencia debida adecuadas, en función del riesgo que pudiera seguir presentado el cliente, y hasta tanto se determine por el sujeto obligado que ya no representa un riesgo específico derivado de su antigua condición de persona con responsabilidad pública

## PROXIMOS PASOS 5ª DIRECTIVA

Se establece la obligación de que los Estados miembros publiquen listados de los cargos que implican la consideración como tal, que serán unificados por la Comisión en un listado único comunitario.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# IV. EL SEGUIMIENTO CONTINUO DE LA RELACIÓN DE NEGOCIOS

## 1. Introducción

Tanto para la prevención del blanqueo de capitales y la financiación del terrorismo, como para la buena gestión de riesgo, y una vez se haya realizado la diligencia debida para la admisión de un cliente, existen ciertas medidas de control interno que deben tenerse en cuenta para el seguimiento continuo de la relación de negocios a lo largo de la relación con el cliente.

El objetivo es que la organización conozca completamente a sus clientes para evitar cualquier riesgo que el trato con esos clientes pueda suponer para la organización. Además de ser una obligación reglamentaria, la gestión continuada es un componente fundamental para un control comercial adecuado y una buena práctica de gestión de riesgos, facilitando la transparencia financiera.

Las medidas de control para el seguimiento continuado incluyen:

- La actualización de documentos, datos e información del cliente.
- "Screening" del cliente y de todas sus estructuras de control contra:
    - *Listas de sanciones*
    - *Listas internas*, también conocidas como "listas privadas" o "listas grises". Son las listas de personas y entidades que pueden representar un riesgo de delito financiero para la entidad, y que han sido identificadas a través de los procedimientos internos de la entidad o de la inteligencia.
    - *Noticias negativas*
- Monitorización de transacciones/ operaciones efectuadas, incluido el origen de fondos



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# 2. Marco normativo en España

Conjuntamente a las obligaciones de diligencia debida (estipulado en el capítulo II), el principio básico del marco normativo es que se debe realizar un seguimiento continuo de la relación de negocios.

## 2.1. Artículo 6: Seguimiento continuo de la relación de negocios Ley 10/2010, de 28 de abril

Las organizaciones deben aplicar medidas de **seguimiento continuo a la relación de negocios**, incluida la investigación de **las operaciones efectuadas** a lo largo de la relación con sus clientes para asegurar y demostrar que cuentan con un perfil empresarial y de riesgo adecuado, incluyendo el **origen de los fondos.**

Se debe garantizar que los documentos, datos e información de que se disponga de los mismos estén actualizados.

**Ver**: https://www.boe.es/buscar/act.php?id=BOE-A-2010-6737
https://www.sepblac.es/wp-content/uploads/2018/09/ley_10_2010.pdf

## 2.2. Artículo 11: Seguimiento continuo de la relación de negocios del Reglamento de la Ley 10/2010

**Artículo 11 (1):** Las organizaciones deberán realizar investigaciones de las operaciones efectuadas a lo largo de la relación de negocio con sus clientes **para garantizar que coinciden con la actividad profesional o empresarial reportada y con sus antecedentes operativos**.

Las organizaciones deberán **incrementarán el seguimiento cuando evidencien riesgos** superiores al promedio por disposición normativa o como resultado de su análisis de riesgo.

Las investigaciones deberán ser completas, incluyendo **todos los productos** del cliente con la organización, y las otras sociedades pertenecientes al grupo.

**Ver:** https://www.boe.es/buscar/doc.php?id=BOE-A-2007-15157
https://www.sepblac.es/wp-content/uploads/2018/02/real_decreto_304_2014.pdf

**Artículo 11 (2):** Las organizaciones deberán realizar **periódicamente procesos de revisión** con el objetivo de asegurar que los documentos, **datos e informaciones** obtenidos en el proceso de diligencia debida se mantengan **actualizados y se encuentren vigentes**.

El manual mencionado en el **artículo 33** determinará, en **función del riesgo**, la periodicidad de los procesos de revisión documental para los clientes de riesgo superior al promedio y deberá ser como mínimo anualmente.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

## 2.3. Artículo 33: Manual de prevención del Reglamento de la Ley 10/2010

**Artículo 33 (1):** Los procedimientos de control interno que establezcan las organizaciones serán documentados en un manual de prevención del blanqueo de capitales y de la financiación del terrorismo y deberá incluir como mínimo, los siguientes factores:

a. **Una política de admisión de clientes**, con descripción exacta de los clientes que puedan suponer un **riesgo superior al promedio** por disposición normativa o porque así lo indique el análisis de riesgo, las medidas a adoptar para mitigarlo incluyendo:
   - La negación a establecer relaciones de negocio
   - A ejecutar operaciones o
   - A la terminación de la relación de negocios.

b. Un procedimiento estructurado de diligencia debida que incluya la **actualización periódica de la documentación e información requerida**. **La actualización será** regulada **cuando se verifique un cambio importante en la actividad del cliente que pueda influir en su perfil de riesgo.**

c. Un procedimiento estructurado de **aplicación de las medidas de diligencia debida** a los **clientes existentes en función del riesgo** que tendrá en cuenta las medidas aplicadas previamente y la adecuación de los datos obtenidos.

d. Una relación de hechos u operaciones que puedan estar **relacionados con el blanqueo de capitales o la financiación del terrorismo**, estableciendo su revisión periódica y difusión entre los directivos, empleados y agentes de la organización.

e. Una descripción detallada de los flujos internos de información, con instrucciones precisas a los directivos, empleados y agentes de la organización sobre **cómo proceder** en relación con los hechos u operaciones que puedan estar relacionados con el blanqueo de capitales o la financiación del terrorismo.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

f. Un procedimiento para la **detección de hechos u operaciones sujetas a revisión especial**, con descripción de las herramientas o aplicaciones informáticas y de las alertas establecidas.

g. Un procedimiento **estructurado de la revisión especial** que definirá las fases del proceso de análisis y las fuentes de información a utilizar, formalizando por escrito el resultado del examen y las decisiones adoptadas.

h. Una descripción detallada del **funcionamiento de los órganos de control interno**, que incluya su composición, competencias y periodicidad de sus reuniones.

i. Las medidas para asegurar el **conocimiento de los procedimientos de control interno** por parte de los directivos, empleados y agentes de la organización, incluyendo la difusión periódica y la realización de capacitaciones según su plan anual.

j. Las medidas a adoptar para **verificar el cumplimiento de los procedimientos de control interno** por parte de los directivos, empleados y agentes de la organización.

k. Los requisitos y criterios de contratación de agentes, que deberán obedecer a lo señalado en el artículo 37.2.

l. Las medidas a adoptar para asegurarse de que los intermediarios de la organización aplican procedimientos adecuados de prevención del blanqueo de capitales y de la financiación del terrorismo.

m. Un **procedimiento de verificación periódica de las medidas de control interno, asegurando que es adecuado y eficaz**. Los equipos de auditoría interna serán los responsables de dicha actividad.

n. La **actualización periódica** de las medidas de control interno, según los desarrollos observados en el sector, el análisis del perfil de negocio y la operativa de la organización.

o. Un **procedimiento de conservación de documentos** que garantice su adecuada gestión y disponibilidad.

**Artículo 33 (2):** Las organizaciones deberán **verificar y actualizar periódicamente el manual** en términos de los factores m) y n) del apartado anterior. El Servicio Ejecutivo de la Comisión podrá supervisar o inspeccionar la efectiva aplicación de las medidas de control interno previstas en el manual, conforme a lo mencionado en el artículo 47 de la Ley 10/2010, de 28 de abril.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# 3. Guías de SEPBLAC

## 3.1. SEPBLAC: Recomendaciones sobre las medidas de control interno para la prevención del blanqueo de capitales y de la financiación del terrorismo. 4.04.2013

Para facilitar a las organizaciones el cumplimiento de las obligaciones establecidas en el artículo 26 (*Políticas y procedimientos*) y en el marco de lo establecido en el artículo 45.4.g (*Órganos de apoyo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, Efectuar recomendaciones a los sujetos obligados orientadas a la mejora de las medidas de control interno*) de la Ley 10/2010, el Sepblac ha compilado las siguientes recomendaciones sobre **las medidas de control interno** de PBC/FT. Esta guía **no es propiamente reglamentación, sin embargo, deberían ser adoptadas para contar con un control interno adecuado**.

**Ver**: https://www.sepblac.es/wp-content/uploads/2018/03/recomendaciones_sobre_medidas_de_control_interno_pbcft.pdf

**"El primer requisito para que las organizaciones puedan realizar una buena tarea de prevención es ser conscientes de su propio riesgo".**

### 3.1.1. Principios generales

- **Principio 2.1 "Enfoque riesgo":** Las organizaciones deberán desarrollar sus procedimientos **en función del riesgo** de BC/FT propio a su actividad y forma de operar.
- **Principio 2.3 "Foco de la prevención":** Los procedimientos de prevención no deberán enfocarse exclusivamente en la capacidad para detectar, analizar y comunicar la operativa con indicios, sino que también deberán **anticipar** posibles clientes u operaciones de riesgo.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

- **Principio 2.7 "Pilares de la prevención":** Los procedimientos de prevención deben basarse en la determinación del **titular real**, el conocimiento del **origen de los fondos**, y **la coherencia de la operativa** realizada.

Los pilares para consolidar procedimientos en materia de PBC/FT de las organizaciones, teniendo en cuenta la aplicación del enfoque riesgo anteriormente mencionado (conocer perfil empresarial y de riesgo), son aquéllos que permitan determinar el titular real de la operativa realizada, conocer el origen de los fondos empleados por los clientes y la coherencia de la operativa realizada por el cliente. Solicitar y obtener la **documentación e información apropiada a cada caso concreto en función del riesgo** será **antes de iniciar la relación de negocios**

### 3.1.2. Recomendaciones sobre las medidas de control interno para la prevención del blanqueo de capitales y de la financiación del terrorismo

#### 3.1.2.1. Medidas de diligencia debida y su aplicación

- Las medidas aplicadas para realizar un seguimiento continuo de la relación de negocios que garantice que las operaciones efectuadas por el cliente encajan con el conocimiento que tenga la organización del propio cliente y de su perfil empresarial y de riesgo, **deben ser sensibles a los cambios de comportamiento de los clientes**.
- Las medidas establecidas para garantizar que los documentos, datos e información disponibles estén actualizados y deben **fijar plazos razonables de actualización** para cada categoría de clientes en función del nivel de riesgo presentado.
- Particularmente en el caso de **nuevos clientes durante los primeros meses desde el inicio** de su operativa, así como las operaciones que impliquen la utilización de productos o la prestación de servicios nuevos que no hayan sido ofrecidos anteriormente por la organización, deberán realizar un seguimiento específico y reforzado de sus actividades, a fin de garantizar que la operativa efectuada por los mismos encaja con el conocimiento que la organización tiene de sus propios clientes, de su perfil empresarial y de riesgo.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

### 3.1.2.2. Detección y análisis de las operaciones susceptibles de estar relacionadas con el blanqueo de capitales o la financiación del terrorismo

a. **Sistema o sistemas de alertas** utilizados para detectar cualquier **operación** que, por su naturaleza, pudiera estar relacionada con el BC/FT:
   - Resultar compleja, inusual o sin un propósito económico o lícito aparente
   - Presentar indicios de simulación o fraude

b. Para el procedimiento específico de detectar **operaciones** relacionadas con la financiación del terrorismo, se debe establecer la **consulta de listas internacionales publicadas, previo al establecimiento de la relación de negocios, así como la verificación periódica** de **toda la base de clientes** de la entidad con dichas listas para tener en cuenta posibles actualizaciones.

c. **Aplicación o aplicaciones informáticas** utilizadas para la detección de **operaciones** susceptibles de estar relacionadas con el BC/FT, referentes a:
   - Personas, órgano o departamento encargado de la gestión y utilización de dichas aplicaciones.
   - Tipos de alertas establecidas y características de estas, umbrales de riesgo definidos, circuitos de tratamiento de las distintas alertas dejando constancia de los trabajos realizados al respecto.
   - Alertas basadas en la detección de operaciones efectuadas que no coincidan con el conocimiento que tenga el sujeto obligado del cliente y de su perfil empresarial y de riesgo.
   - Acceso a otras aplicaciones informáticas de la entidad que contengan información relevante desde la perspectiva de la prevención.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

- Procedimiento implementado para la incorporación de nuevas variables de riesgo al sistema de alertas según la experiencia práctica de la entidad.

d. La organización debe disponer de **procedimientos ágiles para el tratamiento y detección** de aquellas operativas sobre las que sea necesario aplicar las medidas de diligencia debida de forma urgente dada la inmediatez con la que se producen o ejecutan

## 3.2. SEPBLAC: Buenas Prácticas - Aplicación de listas de personas y entidades sujetas a sanciones y contramedidas financieras internacionales enero 2015

La normativa española de prevención del blanqueo de capitales y de la financiación del terrorismo recuerda que adicional a las acordadas por las autoridades nacionales, **las medidas restrictivas y sanciones** de la Unión Europea son de **aplicación obligatoria**, siendo **su incumplimiento constitutivo de infracción grave o muy grave.**

Uno de los aspectos prácticos más destacados es el cumplimiento de las obligaciones al verificar que los clientes, o las personas con las que se realizan operaciones, no están incluidos en las listas de sanciones publicadas (en adelante, denominadas a veces simplemente “listas”).

**Ver:** https://www.sepblac.es/wp-content/uploads/2018/03/aplicacion_de_listas_de_personas_y_entidades_sujetas_a_sanciones_y_contramedidas_financieras_internacionales.pdf

### 3.2.1. Buenas prácticas en la determinación de bases de datos y transacciones

#### BUENA PRÁCTICA 1: Elaborar un consolidado de todas las bases de datos y diferentes tipos de operaciones o transacciones que puede realizar la entidad.

En el análisis de riesgo que debenrealizar los sujetos obligados es buena práctica que se incluya **una relación completa de las bases de datos** y **diferentes tipos de operaciones o transacciones** de la entidad.

Es importante recordar que el análisis de riesgo debe documentarse y ser **revisado periódicamente** o cuando se presente **un cambio significativo** que pueda influir en el perfil de riesgo del sujeto obligado.

Es importante incluir a **todas las áreas de negocio en el análisis de riesgo,** entre los más relevantes:

- El área comercial, internacional, tesorería, gestión de carteras y gestión patrimonial (banca personal), depositaría, venta de inmuebles, y otras;
- Los diferentes canales de distribución que se utilicen tales como los agentes bancarios, la banca telefónica, por internet, y otros; y todos los intervinientes en las operaciones.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

El **análisis de riesgo será la base de partida** para diseñar las medidas que darán cumplimiento a las obligaciones relativas a sanciones y contramedidas financieras internacionales, atendiendo al nivel de riesgo que se presente en cada tipo de operación o base de datos.

### BUENA PRÁCTICA 2: Verificar contra listas todas las bases de datos y tipos de operaciones

El punto de partida más acertado en **la definición de bases de datos y de tipos de operaciones a verificar** contra listas es **afirmar que siempre procede realizar verificaciones**, en vez de analizar caso a caso cuando procede realizar, o no, la verificación.

### BUENA PRÁCTICA 3: Decidir no verificar contra listas sólo cuando exista total certeza de "riesgo cero" por haberse realizado verificaciones anteriores

Es buena práctica que la decisión de no verificar contra listas alguna base de datos u operación se tome sólo cuando exista certeza de que **todos los intervinientes ya han sido verificados** con anterioridad por estar incluidos en bases de datos que **periódicamente son objeto de comprobación** contra listas actualizadas.

Es importante **documentar por escrito las razones que justifiquen que no se apliquen listas** a determinadas bases de datos o tipos de operaciones.

### BUENA PRÁCTICA 4: Analizar y documentar el efecto en los procedimientos a implantar de la intervención de un tercero con obligación de cumplir con el régimen de sanciones y contramedidas financieras

La intervención en las operaciones de un tercero sujeto a las obligaciones en esta materia es **un factor atenuador del riesgo**, pero no hasta el grado de eliminarlo por completo.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Es buena práctica analizar y documentar debidamente **el efecto que la intervención de un tercero** sujeto a las obligaciones tiene en los procedimientos implantados por el sujeto obligado. Por ejemplo, el caso de una transferencia recibida de una entidad bancaria nacional o de la Unión Europea.

**Ese efecto no puede consistir en no aplicar ninguna medida de verificación** ya que, atendiendo a la norma, cuando se detecte que se ha operado con una persona incluida en listas, el que se hubiera decidido previamente no aplicar medida alguna de verificación, confiando en que los terceros no cometan errores, no eximiría a la entidad de la exigencia de responsabilidades por las autoridades.

### BUENA PRÁCTICA 5: Aplicar las listas a todas las personas que intervengan

La aplicación de listas no se ha de limitar, por ejemplo, a los titulares, sino que también se debe extender a todos los intervinientes: apoderados, autorizados, titulares reales, avalistas, etc.

### BUENA PRÁCTICA 6: En el caso de operaciones, verificar quienes no son clientes

En el caso de transferencias recibidas, es preciso verificar al ordenante, en la medida en que el beneficiario, que es cliente de la entidad, ya debe haber sido objeto de verificación.

La decisión correcta sería la contraria en el caso de transferencias ordenadas.

### BUENA PRÁCTICA 7: En el caso de operaciones, verificar no sólo los campos relativos a los intervinientes, sino también los que recojan el "concepto" o contengan "observaciones"

La verificación de que los campos "concepto" u otros que recojan observaciones por lo general no incluyen nombres de personas incluidas en listas, sin embargo, la entidad podría ser sancionada si en esos campos existen datos de personas o entidades que intervengan en la operación

## 3.2.2. Buenas prácticas en la obtención de las listas a verificar

### BUENA PRÁCTICA 8: Conocer bien el contenido y la estructura de las listas

Las organizaciones deben **conocer con cierta profundidad el contenido y la estructura** de las listas publicadas.

Debe tenerse en cuenta que las **listas aprobadas por Reglamentos comunitarios son obligatorias desde el momento de su publicación**, por lo que las entidades deben encontrarse en condiciones de aplicar desde ese momento las sanciones y contramedidas financieras previstas en los mismos.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

En el caso de los **listados aprobados por Naciones Unidas**, aunque no directamente obligatorios para los sujetos privados, son incorporados posteriormente por Reglamentos comunitarios, por lo que resulta buena práctica que las entidades tengan un conocimiento de estos, de tal manera que puedan anticipar su aplicación.

**BUENA PRÁCTICA 9: Justificar la conveniencia de contratar un determinado proveedor externo de listas**

Si bien las listas obligatorias son públicamente accesibles - las Naciones Unidas y la Unión Europea facilitan en sus páginas en internet la relación actualizada de personas físicas y jurídicas incluidas en listas - muchas entidades prefieren acudir a proveedores externos que les facilitan estas listas.

Al elegir un proveedor, se deberían tener en cuenta las **garantías de servicio** que ofrece y su **rapidez en la incorporación** de las adiciones o modificaciones que se realicen en las listas oficiales.

### 3.2.3. Buenas prácticas en el proceso de aplicación

**BUENA PRÁCTICA 10: Valorar la conveniencia de desarrollar un sistema propio para realizar la verificación contra listas o, por el contrario, contratar una solución informática externa**

El contraste de forma segura y eficiente de las bases de datos y de las operaciones de una entidad frente a listas es **una tarea que exige contar con aplicaciones informáticas complejas**.

Es buena práctica analizar la conveniencia de desarrollar un sistema propio para realizar la verificación contra listas o, por el contrario, contratar una solución informática externa.

Es importante que las entidades que decidan contratar **proveedores externos** escojan al más conveniente sólo después de **un análisis minucioso** de sus



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

necesidades, y que tengan en cuenta que con la contratación de esos servicios **no pueden dar por resuelto el aspecto tecnológico del contraste de listas**. Esto es, en los dos casos – desarrollo propio o solución externa.

### BUENA PRÁCTICA 11: Fijar y revisar periódicamente, los umbrales de aproximación a los nombres contenidos en listas cuya superación se considera que debe generar una alerta

**No es buena práctica** que una entidad decida que, para que se genere una alerta, deba existir **una coincidencia total entre la persona** que se verifica y una incluida en listas.

**Los algoritmos de búsqueda** que se empleen deben ser capaces de poder obviar errores en la introducción mecanográfica de nombres, transliteraciones alternativas o la utilización de abreviaturas diferentes a las que figuran en listas.

Es buena práctica **analizar con detalle el grado de aproximación o de similitud** a los nombres contenidos en las listas que se exige para que genere una alerta. Evidentemente, ello implica que las entidades han tener un **conocimiento adecuado del algoritmo de búsqueda** empleado por las aplicaciones que utilizan.

### BUENA PRÁCTICA 12: Adoptar una decisión razonada sobre el momento de realización de las verificaciones

Para cada proceso de base de datos y tipo de operación, es buena práctica que se **recojan por escrito los motivos que aconsejan realizar la verificación en tiempo real** (proceso **online**) o en un **momento posterior** (procesos en **batch**). En el caso de los procesos en batch, también es aconsejable que conste su periodicidad por escrito.

### BUENA PRÁCTICA 13: Realizar verificaciones periódicas de las bases de datos para asegurar que las listas nuevas, o las modificaciones de listas anteriores, se aplican debidamente

Sin perjuicio de los procesos online relativos a bases de datos, la aplicación de procesos en batch a toda la base de datos permite asegurar que las listas nuevas, o las modificaciones de listas anteriores, se aplican debidamente.

Es recomendable que los procesos batch, se ejecuten **de forma rutinaria**, y **no solo cuando se tenga conocimiento de que se han modificado las listas.**



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

**BUENA PRÁCTICA 14: Comprobar periódicamente el correcto funcionamiento del sistema de detección, mediante la simulación de altas de clientes o de operaciones que incluyan nombres de personas iguales o similares a los incluidos en listas**

Es buena práctica **comprobar periódicamente el correcto funcionamiento** del sistema de detección.

**Realizar simulaciones** de altas de clientes o de operaciones que incluyan nombres de personas iguales o similares a los incluidos en listas son la mejor manera de poder asegurar el funcionamiento correcto del sistema.

Desde la detección de posibles coincidencias hasta la gestión de los casos de inclusión de un cliente en listas - y realizar, en su caso, las correcciones o adaptaciones necesarias.

**BUENA PRÁCTICA 15: Mantener un registro de las verificaciones realizadas.**

En relación especialmente con los procesos en batch, es conveniente llevar un registro en el que se anoten todas sus ejecuciones.

**BUENA PRÁCTICA 16: Asegurar la intervención de los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo en el diseño o modificación de los procesos informáticos.**

Es buena práctica que los órganos de prevención participen activamente en las actuaciones de la entidad en el terreno informático que afecten a las bases de datos o a las operaciones sujetas a verificación contra listas.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

### 3.2.4. Buenas prácticas en la gestión de alertas

**BUENA PRÁCTICA 17: Describir detalladamente las acciones a realizar cuando se produce una alerta sobre una posible coincidencia de nombres.**

Se comprueba que el sistema de gestión de alertas funciona mejor cuando existen **procedimientos escritos** que guíen **como actuar** cuando se genere una alerta sobre una posible coincidencia entre la persona que se verifica y una incluida en listas son detallados y exhaustivos.

**BUENA PRÁCTICA: 18 Impedir de forma automática que las operaciones se ejecuten hasta que se alcance la conclusión de que la alerta no responde a un caso real de coincidencia de nombres.**

En vez de presuponer que la entidad puede gestionar las alertas con rapidez y, en caso de coincidencia real de nombres, cancelar o retrotraer una operación ya ejecutada, la actuación más prudente es bloquear la operación e impedir su ejecución hasta que se resuelva la alerta.

**BUENA PRÁCTICA 19: Atribuir la capacidad de conocimiento y decisión final sobre las alertas a los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo**

Sin perjuicio de la intervención en la gestión de las alertas de personas o departamentos de la entidad distintos de los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo, la buena práctica es que **el órgano de prevención**:

- Tenga conocimiento de todas las alertas generadas; e
- Intervenga necesariamente en su resolución de forma que, sin al menos su visto bueno, no pueda considerarse resuelta una alerta.

La intervención de los órganos de prevención en los términos antes señalados **presupone que el número de alertas que se generan es razonable, para lo que es importante que el algoritmo de búsqueda esté bien definido**.

**BUENA PRÁCTICA 20: Facilitar a los órganos de prevención del blanqueo de capitales y de la financiación del terrorismo acceso directo a toda la información necesaria.**

Para que puedan realizar su tarea de forma eficaz, los órganos de prevención deberían tener **acceso directo** a toda la información, externa o interna a la entidad, que necesiten.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

**BUENA PRÁCTICA 21:** En el caso de **entidades financieras** es buena práctica que, dentro de las unidades de prevención, uno o más empleados estén **dedicados en exclusiva a sanciones y contramedidas financieras**. Ello permitiría asegurar que se cuenta con **personas debidamente especializadas**.

Debe tenerse en cuenta que las listas son **solo una parte de la actividad** exigida por las normas en relación con sanciones y contramedidas financieras, **existiendo otras limitaciones o prohibiciones**, como las relativas a la exportación o importación de determinados productos o la prestación de ciertos tipos de servicios, que requieren del desarrollo de los adecuados controles por parte de la entidad.

### BUENA PRÁCTICA 22: Mantener un archivo integral de todas las alertas

La buena práctica aconseja mantener un archivo único con todas las alertas que se han analizado en el tiempo. Se debe registrar toda la información relevante: datos de la operación, persona potencialmente incluida en listas, fecha de generación de la alerta, fecha de resolución, motivos, documentación soporte, etc.

### BUENA PRÁCTICA 23: Definir criterios para impedir reiteradas alertas idénticas

Los procedimientos del sistema de alertas pueden **prever que no se generen nuevas alertas sobre personas concretas respecto de las que ya se ha comprobado con certeza que no son las personas incluidas** en listas. Ello puede reducir de forma apreciable la carga de trabajo asociada a la gestión de alertas.

### BUENA PRÁCTICA 24: Aplicar medidas de diligencia debida reforzada a las personas sobre las que no se puede afirmar con certeza que no están incluidas en listas

En algunos casos puede ser difícil asegurar que



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

la persona analizada no está incluida en listas. La buena práctica aconseja establecer **medidas de diligencia debida reforzada** a esas personas (en particular, el seguimiento reforzado). Ejemplo: los casos de homonimia.

### 3.2.5. Buenas prácticas en el tratamiento de los casos de coincidencia real con listas

**BUENA PRÁCTICA 25: Describir detalladamente las acciones a realizar cuando se concluye que un cliente o un interviniente en una operación está incluido en listas.**

Es buena práctica que **los procedimientos precisen de antemano**, con el mayor detalle posible, todos los pasos y decisiones que se deben adoptar para dar cumplimiento efectivo a la obligación de bloqueo de los fondos y comunicación a las autoridades cuando se concluye que un cliente, o un interviniente en una operación, están incluidos en listas.

Al respecto, dada la naturaleza de la materia, debería analizarse la oportunidad de que los **servicios jurídicos de la entidad participen** en la elaboración y actualización de los procedimientos.

**BUENA PRÁCTICA 26: Examinar las operaciones anteriores realizadas por un cliente que ha sido incluido en listas**

Sin perjuicio de que se adopten las medidas necesarias para dar cumplimiento a las obligaciones legales, cuando se comprueba que un cliente ha sido incluido en listas la buena práctica es **realizar un examen especial de su actividad anterior**. También deberían ser **examinadas las operaciones de otras personas relacionadas con el cliente.**

**BUENA PRÁCTICA 27: En el caso de que una persona incluida en listas aparezca como contraparte en una operación con un cliente de la entidad, examinar todas las operaciones del cliente, aunque no aparezcan en principio relacionadas con la persona en listas**

Como en la buena práctica anterior, también procede realizar examen especial en estos casos.

**BUENA PRÁCTICA 28: Considerar la aplicación de listas un proceso permanente**

La aplicación de listas no debería considerarse un proceso cerrado en el que las decisiones se toman una vez y luego sólo es necesario ponerlas en práctica. Por el contrario, es recomendable que cada cierto tiempo se **revise de forma global todo el proceso** de verificación de listas.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# 4. Noticias negativas

Si bien no es un requisito reglamentario en España ni una directriz específica, la búsqueda de noticias negativas sobre una persona o empresa es una parte importante del proceso de diligencia debida, tanto en la fase de admisión como parte del seguimiento continuado.

Sin embargo, en otras jurisdicciones, como en el Reino Unido y Estados Unidos, se exige la utilización de medios de comunicación adversos.

## 4.1. Reino Unido- FCA

La repetición de la selección de medios adversos se enumera como uno de los ejemplos de medidas que los bancos pueden adoptar al examinar las relaciones comerciales, y como ejemplo del tipo de información que los intermediarios pueden obtener como parte del proceso de diligencia debida, como ejemplo de seguimiento continuado y la prevención de soborno y la corrupción.

**Ver:** https://www.handbook.fca.org.uk/handbook/document/FC2_FCA_20160307.pdf

## 4.2. Estados Unido- FinCEN

Los requisitos de diligencia debida respecto al cliente para las instituciones financieras deben desarrollar procedimientos basados en el riesgo para determinar si y/o cuando sería apropiado realizar una investigación adicional de estos nombres a través de programas de búsqueda negativa en los medios de comunicación.

Ver: https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf

## 4.3. Europa- Directivas de Prevención de Blanqueo de Capitales y Financiación del Terrorismo

**La cuarta directiva** busca que las empresas realicen una diligencia debida reforzada para los clientes de alto riesgo, proceso que incluye “realizar búsquedas de código abierto o de medios adversos”. El 10 de



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

enero de 2020, la cuarta directiva se reforzó con **la quinta directiva**, prestando mayor atención a la diligencia debida digital y fomentando el uso de la detección automatizada de medios adversos.

Ver: https://esas-joint-committee.europa.eu/Publications/Guidelines/Guidelines%20on%20Risk%20Factors_EN_04-01-2018.pdf

**La Autoridad Bancaria Europea (ABE)**

**Artículos 17 y 18 4) de la Directiva (UE) 2015/849 (4AMLD):** Informa de la diligencia debida simplificada y reforzada del cliente y los factores que las instituciones crediticias y financieras deben tener en cuenta al evaluar el riesgo de blanqueo de dinero y financiación del terrorismo asociado a las relaciones comerciales individuales y las transacciones ocasionales.

Si existen informes adversos en los medios de comunicación u otras fuentes de información relevantes sobre el cliente pueden ser pertinentes al considerar el riesgo asociado a la reputación de un cliente o de los beneficiarios finales. Las medidas de diligencia reforzadas pueden incluir el aumento de la cantidad de información obtenida como búsquedas adversas en los medios de comunicación.

## 4.4. GAFI

GAFI recomienda “búsquedas de medios adversos verificables” como parte de las evaluaciones de riesgo del cliente.

GUIDANCE FOR A RISK-BASED APPROACH THE BANKING SECTOR

Ver: http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

GUIDANCE FOR A RISK-BASED APPROACH LEGAL PROFESSIONALS

Ver: http://www.fatf-gafi.org/media/fatf/Risk-Based-Approach-Legal-Professionals.pdf

## 4.5. Los componentes claves

En resumen, los componentes clave para la detección de medios adversos incluyen:

- Identificar quién debe ser examinado, y con qué frecuencia
- La selección y detección, manualmente o a través de herramientas / proveedores automatizados
- Revisar para evaluar los resultados y confirmar las coincidencias
- Decidir las acciones en torno a las coincidencias identificadas y actualizar los sistemas DILIGENCIA DEBIDA



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# 5. La externalización del seguimiento continuo

Los avances, el aumento de los costes en la tecnología, las regulaciones (y multas) existentes y futuras de la industria financiera y las relaciones costes-ingreso en las organizaciones hacen que **la plataforma de servicios de seguimiento continuo** (diligencia debida/ KYC (´*Know your Customer*´) sea la solución más adecuada, viable y efectiva de la industria para todos estos cambios constantes.

Además, los múltiples beneficios que ofrece **un único fichero de diligencia debida del cliente** (aunque el riesgo puede variar por la actividad que tenga dicho cliente con cada entidad), en contraposición a que cada organización lleve a cabo un proceso de seguimiento continuo y diligencia debida propio, que a menudo son comunes entre las empresas.

Es necesario **automatizar y hacer procesos eficientes** para asegurar un **mejor control y cumplimiento**. La externalización de los componentes de la cadena de valor para **reducir los costes y el riesgo operacionales** ayudará a gestionar las obligaciones reglamentarias de manera asequible.

Todos estos factores exigentes suponen la creciente necesidad en el mercado de una solución que proporcione **nuevos entornos de colaboración** que permitan compartir los costes y la normalización de los procesos.

En los últimos años, han existido muchos casos de multas relacionadas con deficiencias en el programa PBC/FT/. El primer paso para tener un programa PBC/FT adecuado es el diseño de un proceso completo de diligencia debida que ayude a **identificar y proporcionar un nivel del riesgo** de los clientes finales. Si este proceso no se implementa correctamente, conducirá a deficiencias en otros procesos para detectar el lavado de dinero y el financiamiento del terrorismo.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Para que el proceso de diligencia debida sea eficaz, es necesario permitir la **normalización, armonización y racionalización** de las políticas de cumplimiento, los procedimientos operativos y la presentación de informes de gestión.

La lucha contra el blanqueo de dinero y la financiación del terrorismo es un desafío mundial, multiinstitucional e intergubernamental, con **seguimiento continuo y la diligencia debida en el corazón del sistema de defensa**.

Por consiguiente, la legislación contra el blanqueo de dinero y la financiación del terrorismo es de **naturaleza global y se encuentra en gran medida estandarizada** (Directivas de la UE contra el blanqueo de dinero Recomendaciones del Grupo de Acción Financiera Internacional "GAFI").

Cada organización sujeta a la legislación tiene la misma exposición a todos los requisitos reglamentarios.

Aunque la legislación no especifica la interpretación y aplicación precisas de los requisitos de la diligencia debida, existen directrices proporcionadas por las diversas Unidades de Inteligencia Financiera (SEPBLAC, FinCEN (Financial Crimes Enforcement Network) en EE. UU., etc.), que tienen por objeto fomentar una mayor normalización y armonización en todo el sector.

## 5.1. La externalización de procesos de diligencia debida

Cada institución sujeta a la legislación PBC/FT tiene la misma carga regulatoria de diligencia debida. En lugar de que cada institución tenga que gestionar su propio proceso de diligencia debida cada vez que surgen cambios en la normativa, existen **plataformas que se encargan de centralizar este servicio**.

## 5.2. Los obstáculos y la solución

**OBSTÁCULOS**

- Expansión y cambio constantes de la **carga y el escrutinio regulatorio**
- Cambios rápidos en el **panorama de riesgos** (clientes, producto, canal, país)
- Carácter **manual intensivo** del proceso de KYC
- El KYC **no es una competencia central**
- **Eficiencias** reducidas
- Plazos de incorporación prolongados
- Aumento de los **costes**
- Ejercicios de reparación que **consumen recursos**
- Aumento de la presión sobre la relación entre **costes e ingresos**

**KYC BPO COMO SOLUCIÓN**

Plataforma que ofrece servicios para la externalización de los diferentes componentes del proceso de KYC. Esta plataforma ofrece:

- **Estandarización**
- **Racionalización**
- **Automatización**
- Personal **especializado** y con experiencia
- Mejor manejo del **riesgo** de BC y FT
- Aumento de la **eficiencia**
- Reducción de los **costes** operativos
- Mejora de los **controles** y presentación de **informes**


*BPO= Business Process Oustourcing*



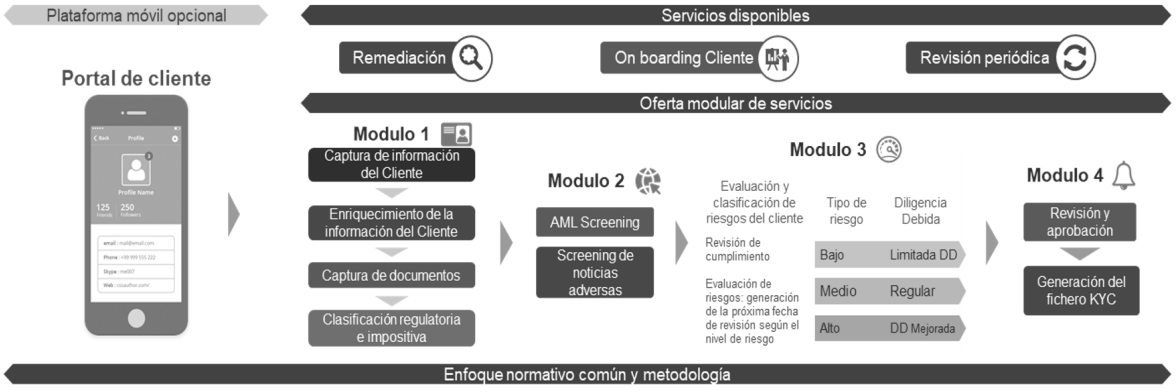
© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

La externalización de los componentes del proceso de diligencia debida reduce los costes operativos y mejora la gestión de riesgos, ayudando a cumplir con las obligaciones regulatorias de una manera rentable y eficiente.

Los distintos participantes (*cliente= cliente final, miembro= organizaciones que participan en el servicio, regulador= Unidad de Inteligencia Financiera*) tienen necesidades particulares que la plataforma puede satisfacer con éxito:

| CLIENTE | MIEMBROS | REGULADOR/ SUPERVISOR |
|---|---|---|
| • Reduce la cantidad de tiempo que se requiere para completar el mismo papeleo de KYC para diferentes instituciones<br>• Reduce los plazos de incorporación, ya que los datos y la documentación están disponibles | • El cumplimiento de KYC es un negocio que no genera ingresos y no es competitivo<br>• Incrementa la cercanía con el cliente, reduce los tiempos de incorporación y mejora el servicio al cliente<br>• Disminución de los costes operativos para solucionar problemas y desarrollar un mejor entorno para cumplir con los requisitos de KYC<br>• Aprovecha los beneficios de las mejores prácticas de la industria en un entorno normativo en constante cambio<br>• Mejor preparación para el escrutinio regulatorio y reducir los riesgos de incumplimiento | • Implementación de procedimientos eficaces de diligencia debida para los clientes/consultores<br>• Mejores prácticas y enfoque estándar para el cumplimiento de los KYC<br>• Enfoque de la diligencia debida basado en el riesgo del cliente<br>• Mejora del nivel de información de la industria<br>• Aumenta la eficiencia de las investigaciones y los exámenes<br>• Aprovecha los beneficios de la cohesión de la industria en los programas de cumplimiento ALD |

## 5.3. Un ejemplo de oferta y servicios básicos de la externalización del servicio de diligencia debida




Estos servicios **se pueden proporcionar diferenciando niveles de exigencia**

| Por el nivel de riesgo del cliente | Por el tipo de cliente | Por el tipo de cliente |
|---|---|---|
| • Bajo, Medio, Alto<br>• Diligencia Debida Mejorada<br>• Diligencia Debida Limitada<br>• Diligencia Debida Básica | • Bancos, fondos de cobertura, administradores de activos, administradores de inversiones<br>• Compañías de seguros<br>• Instituciones no financieras<br>• Otros | • Bancos, fondos de cobertura, administradores de activos, administradores de inversiones<br>• Compañías de seguros<br>• Instituciones no financieras<br>• Otros |



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

### 5.3.1. Los beneficios de un servicio externalizado

La externalización de la plataforma KYC proporciona beneficios tanto para los miembros/ entidades como para los clientes finales.

| | MIEMBROS | CLIENTES |
|---|---|---|
| BENEFICIOS | • Reducción de los costes de recopilación, evaluación y actualización de la información de los clientes<br>• Mejoría del proceso de KYC mediante economías de escala<br>• Reducción de errores manuales en los datos gracias a la mejora de la automatización y calidad de los datos<br>• Reducción de los costes asociados con el mantenimiento de un equipo interno completo para gestionar el proceso de KYC<br>• Mejora la experiencia de los clientes a medida que los bancos aprovechan los datos disponibles<br>• Cumple con los requisitos y matices regulatorios de KYC de manera más efectiva para las operaciones globales<br>• Integración eficiente de nuevas tecnologías<br>• Automatización de procesos<br>• Gestión de los cambios del mercado<br>• Capacidad para mantener el sistema y los procesos actualizados con la regulación | • Elimina la necesidad de proporcionar documentación de KYC a todos los bancos<br>• Evita la confirmación periódica de validez de la información<br>• Proporciona mayor privacidad de los datos ya que reduce la cantidad de copias de documentos confidenciales flotando en el ecosistema<br>• Apertura de nuevas cuentas más ágil y fácil<br>• Mejora en la experiencia del cliente<br>• Aumento del control de los datos y documentos del cliente mediante el intercambio de permisos |

### 5.3.2. Un servicio mutualizado de diligencia debida

Las organizaciones y sus clientes enfrentan diariamente distintos puntos de dolor al llevar a cabo el proceso diligencia debida, entre los más destacados:

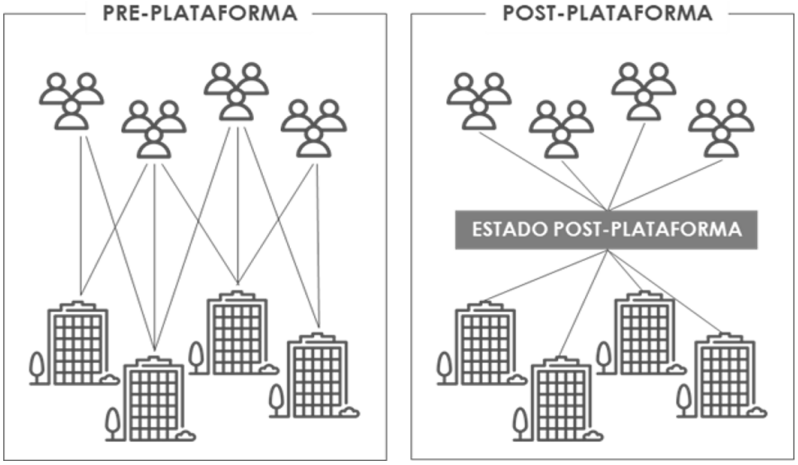
- La falta de un proceso estándar de diligencia debida
- Contactos duplicados con clientes
- Redundancia en el papeleo
- Largos plazos de admisión de clientes
- Aumento de los costes operacionales
- Alto escrutinio regulador
- Ejercicios de remediación requeridos
- Riesgo de plataforma y proveedor
- Mantenimiento de dicha plataforma

El mercado espera un servicio de diligencia debida que **mutualice tanto los costes como los servicios y haga más eficientes los esfuerzos de la práctica de diligencia debida**. En lugar de que cada institución participante tenga que administrar su propia colección de documentos de clientes, almacenar los documentos, evaluar los riesgos, seleccionar los riesgos, ejecutar la diligencia debida continuada y otros procesos relacionados; busca que exista **una herramienta que dé solución transversal.**



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

Una utilidad diligencia debida facilitará este objetivo de normalización y armonización, reducirá las incoherencias entre las instituciones, disminuirá la capacidad de los delincuentes para explotar la información y solventará la visión descoordinada entre las instituciones.




## 5.3.3. Los beneficios de mutualizar los procesos de diligencia debida

| Cumplimiento, mitigación de riesgos y reducción de las sanciones y los requisitos de capital conexos | Mejora de la supervisión y la presentación de informes |
|---|---|
| Identificación de buenas fuentes de datos<br>Beneficios de la red de intercambio de co-nocimientos y prácticas óptimas entre instituciones<br>• - Estandarización del modelo de funciona-miento de los objetivos en todas las instituciones | • Disponer de un registro/sistema de registro del proceso y los resultados<br>• Identificación rápida de las áreas problemáticas y de las acciones<br>• Mejora de la presentación de informes y la coordinación entre los diferentes organismos de aplicación, por ejemplo, SEPBLAC con otras UIF, SEPBLAC y otros organismos reguladores locales, por ejemplo, el Banco de España/ CNMV, los diferentes tribunales españoles, FATCA (Ley de Cumplimiento Tributario de Cuentas Extranjeras), etc. |
| **Mejora de la credibilidad en la industria** | |
| Que puede ser extrapolado a un beneficio más amplio para la industria | |
| **Mejora de la cooperación en la industria** | • Transformar el enfoque fragmentado de la comunicación con los clientes y el regulador<br>• Cumplir con la mayor expectativa los gobiernos, las UIF y las instituciones privadas internacional de cooperación entre los gobiernos, las UIF y las instituciones privadas |
| Que están en línea con las expectativas in-ternacionales: GAFT, etc. | |



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

A continuación, se detallan los beneficios que tendrán los miembros participantes de la utilizada de diligencia debida:

- Reducción del alcance de los clientes
- Mutualizar los costes: Menores costes en reunir, evaluar y actualizar la información de los clientes
- Automatización de los procesos
- Reducción de los costes asociados con el mantenimiento de un equipo interno completo para gestionar el proceso diligencia debida
- Mejora en la reputación de la institución
- Beneficios compartidos: los beneficios de los clientes son también beneficios para el miembro de la empresa de servicios públicos
- Enfoque tecnológico y aprendizaje automático
- Alineación de las innovaciones de la plataforma y los requisitos de los costes
- Mejora en la experiencia del cliente
- Cumplimiento de los requisitos, buenas prácticas y matices reglamentarios de la diligencia debida de forma eficaz para las operaciones mundiales
- Gestión de cambios del mercado
- Capacidad de mantener el sistema y los procesos actualizados con normatividad vigente

### 5.3.4. Algunos servicios de diligencia debida mutualizados

| |  **Paises Nórdicos** |  **Irlanda** |  **Sudáfrica** |  **EEUU** |
|---|---|---|---|---|
| Resumen | La empresa diligencia debida fue creada por los principales bancos nórdicos como una empresa conjunta | Proyecto para analizar los beneficios de implementar una utilidad diligencia debida en los bancos irlandeses. Impulsado por Deloitte y el BPFI | Utilidad nacional diligencia debida para grandes empresas, fondos de cobertura y gestores de activos | Plataforma estandarizada para recoger y gestionar los datos del cliente y estandarizarlos |
| Participantes | DNB<br>Danske<br>Nordea<br>Svenska Handelsbanken<br>Skandinaviska Enskilda | AIB<br>BoI<br>KBC<br>PTSB<br>UISTER Bank | Barclays Africa<br>Rand Merchant Bank<br>Standard Bank of South Africa<br>Standard Chartered Bank | Barclays<br>BNY Mellon<br>Credit Suisse<br>Goldman Sachs<br>JPMorgan Chase<br>State Street |



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# 6. Recursos internacionales

A continuación, figura una lista de algunas directrices adicionales de fuentes internacionales que pueden considerarse.

Las Recomendaciones de GAFI

**Ver:** https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Spanish.pdf

FATF GUIDANCE Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion With a Supplement on Customer Due Diligence

**Ver:** http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

FAFT International best practices targeted financial sanctions related to terrorism and terrorist financing (recommendation 6)

**Ver:** http://www.fatf-gafi.org/media/fatf/documents/recommendations/BUENA PRÁCTICAP-Fin-Sanctions-TF-R6.pdf

FATF Guidance politically exposed persons (recommendations 12 and 22)

**Ver:** http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

Wolfsberg Guidance on Sanctions Screening 2019

**Ver:** https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# V. RELACIONES DE NEGOCIO Y OPERACIONES NO PRESENCIALES

Las relaciones no presenciales cada vez son más frecuentes por el avance del mundo digital, en especial, si bien se pueden asociar a otras formas de operativa en las que, por las circunstancias especiales, no se puede tener un contacto con el cliente, por ejemplo, en la compra venta de bienes en los que intervienen abogados o terceros, en los que hay que cumplir unos requisitos de identificación establecidos en la normativa vigente.

No obstante, precisamente, por este crecimiento digital se está llevando a cabo estudios y avances en las vías de identificación no presencial para hacer más eficientes los procesos y garantizar la seguridad y evitar fraudes.

La Normativa aplicable a los sujetos obligados en España establece como primera medida normal de diligencia debida la identificación formal de los clientes con los que se establecen relaciones de negocio y que como sabemos no admite excepción alguna.

No obstante, debemos considerar que no siempre es posible que los clientes que se encuentren físicamente presentes, por lo que existe una serie de medidas reforzadas de diligencia debida que, por un lado, permiten establecer dichas relaciones, pero incrementa el riesgo de incurrir en responsabilidades en caso de no llevarlas a cabo correctamente. En la actualidad existen varios colectivos de los denominados “sujetos obligados” que en este momento pueden llevar a cabo la implementación de los medios y herramientas que permitan dar cumplimiento al establecimiento de las relaciones de negocio de manera no presencial con la seguridad y especificaciones que la norma señala.

El establecimiento de las relaciones de negocio y operaciones no presenciales, se regulan tanto en la LPBCFT como en el RD 304/2014 que la desarrolla, en ambos casos en su sección 3ª del Capítulo II, relativo a las “Medidas reforzadas de Diligencia Debida”.

De conformidad con lo que establece la Normativa, en su Artículo 12 y 21, respectivamente, se permite a los sujetos obligados la posibilidad de establecer relaciones de negocio o a ejecutar operaciones a través de medios telefónicos, electrónicos o telemáticos con clientes que no se encuentren presentes físicamente, cuando la identidad del cliente quede acreditada mediante el empleo de procedimientos seguros de identificación de clientes en operaciones no presenciales.

Para poder llevar a cabo dicha operativa, deberán concurrir alguna de las siguientes circunstancias que explicaremos a continuación:



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

**a. FIRMA ELECTRÓNICA**

La identidad del cliente quede acreditada de conformidad con lo dispuesto en la normativa aplicable sobre firma electrónica, denominada Ley 59/2003, de 19 de diciembre, de firma electrónica.

**b. IDENTIDAD DEL CLIENTE**

La identidad del cliente quede acreditada mediante copia del documento de identidad, de los establecidos en el artículo 6, que corresponda, siempre que dicha copia esté expedida por un fedatario público.

**c. PRIMER INGRESO**

El primer ingreso proceda de una cuenta a nombre del mismo cliente abierta en una entidad domiciliada en España, en la Unión Europea o en países terceros equivalentes.

**d. PROCEDIMIENTOS AUTORIZADOS POR SEPBLAC:**

De conformidad con la habilitación otorgada normativamente al SEPBLAC, cabe la posibilidad de llevar a cabo la identificación del cliente y que su identidad quede acreditada mediante el empleo de otros procedimientos seguros de identificación de clientes en operaciones no presenciales, siempre que tales procedimientos hayan sido previamente autorizados por el SEPBLAC.

En este sentido, el Sepblac ante la necesidad que tenían, en especial las entidades financieras y otros sujetos dedicados al consumo, dinero electrónico, etcétera publicó en su página web, entre otras, las medidas de identificación basadas en los siguientes procedimientos de identificación no presencial:

1. **Autorización de procedimiento de identificación no presencial**

   https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_procedimiento_identificacion_no_presencial.pdf



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

El artículo 21.1.d) del Reglamento de la Ley 10/2010, dispone que los sujetos obligados podrán establecer relaciones de negocio o ejecutar operaciones a través de medios telefónicos, electrónicos o telemáticos con clientes que no se encuentren físicamente presentes cuando la identidad del cliente quede acreditada mediante el empleo de procedimientos seguros de identificación de clientes en operaciones no presenciales, siempre que tales procedimientos hayan sido previamente autorizados por el SEPBLAC.

En ese sentido, se ha autorizado el procedimiento de identificación no presencial denominado "Procedimiento de solicitud de confirmación de datos sobre titularidad de cuentas entre entidades" del Sistema Nacional de Compensación Electrónica que permite a la entidades apoyarse entre ellas para confirmar datos, verificar información y confirmar datos sobre la titularidad de cuentas entre entidades.

2. **Autorización de procedimientos de identificación no presencial mediante videoconferencia**

https://www.sepblac.es/wp-content/uploads/2018/02/autorizacion_identificacion_mediante_videoconferencia.pdf

En este sentido, se autoriza el empleo por los sujetos obligados de procedimientos de

identificación no presencial mediante videoconferencia y se favorece el uso de las nuevas tecnologías siempre que las mismas proporcionen niveles adecuados de seguridad, en el entendido de que la innovación tecnológica en el sector financiero tiene el potencial de reducir costes, aumentar la competencia y proporcionar un mejor servicio a los clientes.

A este respecto, los sujetos que implementen esta clase de procedimientos deberán asegurarse que los documentos identificativos son los mencionados en el artículo 6 de la Ley, que realicen previamente un análisis de riesgo especifico detallado en el artículo 32.2. del Reglamento, establecerá procedimientos y testará la eficacia del mismo antes de la implementación, se asegurará de que esta clase de procediientos se lleven a cabo por personas con formación especifica, y deberá ser grabado y almacenado el proceso de identificación conforme al artículo 25 de la Ley.

3. **Autorización de procedimientos de vídeo-identificación**

https://www.sepblac.es/wp-content/uploads/2018/02/Autorizacion_video_identificacion.pdf



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

El fomento de la innovación tecnológica en el sector financiero aconseja ahora autorizar asimismo procedimientos de video-identificación en los que no medie una interactuación en línea entre el cliente potencial y un agente u operador del sujeto obligado (procesos no asistidos). La omisión de dicha interactuación y su sustitución por un control posterior de la grabación suponen, no obstante, riesgos superiores que han de ser adecuadamente mitigados, lo que justifica que la presente autorización imponga cautelas adicionales.

Adicionalmente a las especificaciones señaladas patra los procesos de videoconferencia, se establecen requerimientos de buenas prácticas en el uso de esta clase de proceso tales como: (i) que el proceso se realiza por el cliente desde un único dispositivo, (ii) que las imágenes y el sonido son inmediatamente transmitidos al sujeto obligado en formato digital, sin alteración y en directo ("streaming") y (iii) que el sujeto obligado procede a la grabación inmediata del proceso de modo que permita su posterior reproducción en secuencia.

Adicionalmente, hace tan sólo unos días (6/3/2020), **GAFI ha emitido una guía** que analiza el uso de sistemas de **identificación digital** en el proceso de diligencia debida requerido por la normativa de prevención del blanqueo de capitales y la financiación del terrorismo (PBCyFT) en aras de fomentar la utilización de estas funcionalidades para la identificación no presencial en los sectores digitales. Esta guía se dirige principalmente a entidades financieras y proveedores que actúan en este mercado y es muy oportuno dados los escasos criterios supervisores publicados y la falta de armonización normativa.

La guía analiza los requisitos para el uso de sistemas de identificación digital al aplicar las medidas de diligencia debida que exige la normativa de PBCyFT. La comprensión del funcionamiento de los sistemas de identificación digital es esencial para aplicar correctamente un enfoque basado en riesgo.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

La guía es un documento extenso y prolijo que aborda el uso de las tecnologías de identificación digital en:

a. **Identificación formal** y verificación de la identidad del **cliente (persona física y persona jurídica)** al establecer relaciones de negocio.

b. Apoyo de las tecnologías de identificación digital en el **seguimiento continuo de la relación de negocio**.

En ese sentido, el GAFI hace hincapié en que la identificación y verificación no presencial del cliente, por sistemas de identificación digital que cumplan con los niveles de garantía adecuados, no tiene por qué implicar un aumento del riesgo respecto a la identificación presencial.

La guía introduce asimismo elementos novedosos como los de portabilidad e interoperabilidad de los mecanismos de identificación digital.

Otros aspectos de interés que se desarrollan en la guía:

### 1. Potenciales riesgos y beneficios de la identificación digital

La sección IV de la guía relaciona detalladamente los beneficios potenciales de los sistemas de identificación digital y sus posibles riesgos, que deben ser identificados, comprendidos y controlados.

Como potenciales beneficios destacan los siguientes:

a. Reducción de los errores humanos en las medidas de control interno.

b. Mejora de la experiencia de usuario del cliente.

c. Ahorro de costes.

d. Facilitación del seguimiento continuado de la relación de negocio.

Como riesgos destacan:

a. Suplantación de identidad y otros problemas de seguridad (ciberataques, protección de datos y violaciones de la seguridad).

b. Aparición de posibles obstáculos al acceder a la información detallada de identidad para la debida diligencia y el seguimiento continuo de la relación de negocio.

c. Problemas de conectividad.

d. Diferencias entre los marcos legislativos sobre identificación digital de los países.

### 2. Fiabilidad de los sistemas de identificación digital

La sección V orienta a las autoridades nacionales y las entidades sobre cómo aplicar un enfoque basado en riesgo al usar sistemas de identificación digital en el proceso



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

de diligencia debida. De nuevo el enfoque basado en riesgo es el que sigue marcando las pautas, lógicamente, en el proceso de utilización de la identificación digital.

El enfoque que adopta el GAFI se basa en dos elementos clave:

- La **comprensión amplia de la seguridad de la tecnología del sistema de identificación digital (incluyendo su arquitectura y gobierno)** que debe tener la entidad para determinar su fiabilidad e independencia.
- El **análisis de riesgo de si el sistema de identificación digital proporciona un nivel adecuado de fiabilidad e independencia,** una vez conocidos los niveles de garantía de la herramienta, que debe realizar la entidad.

En este sentido, tanto la Norma como las directrices de SEPBLAC y la Guía de GAFI, señalan una serie de medidas adicionales que deberían atender los sujetos obligados que opten por realizar esta clase de identificación, la no presencial.

Dichas medidas se resumen en:

### 1. Obtención de documentación original

En todos los casos, cuando se haya realizado la identificación telemática en el plazo de un mes desde el establecimiento de la relación de negocio, los sujetos obligados deberán obtener de los clientes identificados de manera no presencial, una copia de los documentos necesarios para practicar la diligencia debida.

### 2. Necesaria identificación presencial en caso de discrepancias

Cuando se aprecien discrepancias entre los datos facilitados por el cliente y otra información accesible o en poder del sujeto obligado, será preceptivo proceder a la identificación presencial.

### 3. Adopción de medidas adicionales en caso de apreciación de nuevos riesgos

Los sujetos obligados adoptarán medidas adicionales de diligencia debida cuando en el curso de la relación de



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

negocio aprecien riesgos superiores al riesgo promedio.

Esto es, adoptar un **enfoque basado en el riesgo** para confiar en los sistemas de identificación digital, que incluya:

- comprender los niveles de garantía del sistema de identificación digital, en particular para la verificación y autenticación de la identidad, y
- asegurar que los niveles de garantía sean apropiados para los riesgos de blanqueo de capitales y financiación del terrorismo referidos al cliente, al producto, a la jurisdicción, al alcance geográfico, etc.

**4. Entender los componentes básicos de los sistemas de identificación digital,**

En particular el de las pruebas de identidad y el de autenticación, y cómo estos se relacionan con los elementos básicos del proceso de diligencia debida.

**5. Procesos antifraude y de ciberseguridad**

Utilizar **procesos antifraude y de ciberseguridad,** cuando sea pertinente**,** para apoyar la comprobación y autenticación de la identidad digital (identificación y verificación del cliente, y seguimiento continuado de la relación de negocio).

**6. Disponer en las entidades de acceso constante a la información y las pruebas de identidad subyacentes o a la información digital necesaria para la identificación y verificación de las personas, y de un proceso que permita a las autoridades obtenerla.**

**7. Establecimiento de Políticas y Procedimientos ad hoc para afrontar riesgos específicos.**

Los sujetos obligados establecerán políticas y procedimientos para afrontar los riesgos específicos asociados con las relaciones de negocio y operaciones no presenciales.

Revisar las **políticas internas** cuando la identificación no presencial de **clientes se clasifique siempre como de alto riesgo**, puesto que la identificación de clientes basada en sistemas de identificación digital independientes y fiables, junto con la existencia de medidas de mitigación de riesgos, puede suponer un riesgo estándar e incluso bajo.

**8. Criterios adicionales para identificación a sujetos afectados por la Regulación del Juego.**

Los criterios para la acreditación de la identidad del cliente en relación con los sujetos obligados sometidos a la Ley 13/2011, de 27 de mayo, de regulación del juego, y en su normativa de desarrollo, se determinarán en el proceso de concesión de licencias generales por la Dirección General de Ordenación del Juego, previo informe favorable del Servicio Ejecutivo de la Comisión.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

# VI. PRODUCTOS U OPERACIONES PROPICIAS AL ANONIMATO Y NUEVOS DESARROLLOS TECNOLÓGICOS

Partimos del **art. 16 de la Ley 10/2010 de 28 de abril de prevención del blanqueo de capitales y de la financiación del terrorismo** donde se establece "*los sujetos obligados prestarán especial atención a todo riesgo de blanqueo de capitales o de financiación del terrorismo que pueda derivarse de productos u operaciones propicias al anonimato, o de nuevos desarrollos tecnológicos, y tomarán medidas adecuadas a fin de impedir su uso para fines de blanqueo de capitales o de financiación del terrorismo. En tales casos, los sujetos obligados efectuarán un análisis específico de los posibles riesgos en relación con el blanqueo de capitales o de la financiación del terrorismo, que deberá documentarse y estar a disposición de las autoridades competentes*".

A raíz de la entrada en vigor, el 9 de julio de 2018, de la **Directiva (UE) 2018/843** del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, llamada también "Quinta Directiva", se ha visto modificada la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modificaban las Directivas 2009/138/CE y 2013/36/UE. Los Estados miembros han tenido que transponer esta Directiva antes del 10 de enero de 2020.

La "Quinta Directiva" incorpora a la lista de sujetos obligados a los **proveedores de servicios de cambio de moneda virtual** en moneda fiduciaria, así como a los **proveedores de servicios de custodia de monederos electrónicos** ya que considera que estos no estaban obligados por la Unión a detectar actividades sospechosas y por lo tanto, los grupos terroristas podían ser capaces de transferir dinero hacia el sistema financiero de la Unión o dentro de las redes



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

de monedas virtuales ocultando transferencias o gozando de cierto anonimato en esas plataformas. (art. 2 apdo. 1 letras g) y h)) Los Estados miembros garantizarán que los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias y los proveedores de servicios de custodia de monederos electrónicos estén registrados (art. 47 apdo. 1)

Otro cambio que ha supuesto la entrada en vigor de la "Quinta Directiva" es la limitación del **uso de tarjetas prepago** de uso múltiple emitidas en la Unión y **reduce el umbral** para poder realizar operaciones de reembolso o retirada de efectivo del valor monetario del dinero electrónico a 50 EUR (antes 100 EUR) sin tener que aplicar las medidas de diligencia debida oportunas y sin dejar de lado las necesidades de los consumidores. Cuando el "instrumento de pago no es recargable, o tiene un límite máximo mensual para transacciones de pago de 150 EUR (antes 250 EUR) que solo puede utilizarse en ese Estado miembro concreto y cuando el importe máximo almacenado electrónicamente no es superior a 150 EUR (antes 250 EUR que podía aumentarse hasta 500 EUR) (art. 12 apdo. 1 letras a) y b) y apdo. 2)

Además, las **tarjetas prepago de fuera de la Unión** emitidas por terceros países solamente se puedan utilizar en la Unión si cumplen requisitos equivalentes a los establecidos en Derecho de la Unión. Los Estados miembros podrán decidir no aceptar en su territorio los pagos efectuados con tarjetas de prepago anónimas. (art. 12 apdo. 3)

Las **Unidades de Inteligencia Financiera** (UIF, en el caso de España el SEPBLAC) deben poder obtener informaciones que les permitan asociar las direcciones de las monedas virtuales a la identidad del propietario de la moneda virtual para poder **combatir** los riesgos asociados con el **anonimato**. Los últimos avances técnicos en la digitalización de las transacciones y los pagos permiten una identificación remota o electrónica segura. Los delincuentes mueven el producto de las actividades ilícitas a través de numerosos intermediarios financieros con el fin de evitar que sea detectado.

Los sujetos obligados deberán examinar el contexto y la finalidad de todas las transacciones que sean transacciones complejas, o sean de un importe inusitadamente elevado, o bien que se lleven a cabo en una pauta no habitual o que no tengan una finalidad económica o lícita aparente. Deberán reforzar el grado y la naturaleza de la supervisión de la relación de negocios, a fin de determinar si tales transacciones o actividades parecen sospechosas. (art. 18 apdo. 2)

Dos conceptos que hay que tener en cuenta son el de **moneda virtual** que es la representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública y que puede transferirse, almacenarse y negociarse



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

por medios electrónicos y el de **proveedor de servicios de custodia de monederos electrónicos** que es el aquel que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes para la tenencia, almacenamiento y transferencia de monedas virtuales.

El **Grupo de Acción Financiera Internacional** (GAFI) ha ido adoptando soluciones a lo largo de los años para minimizar la amenaza planteada por las nuevas tecnologías.

Presentó un Informe para advertir del **riesgo de realizar operaciones sin identificarse con los nuevos métodos de pago** (*Report on new payment methods*, 2006). También apuntó a que debería prestarse más atención a los **servicios de pago por Internet** (*Money laundering and terrorism financing: Vulnerabilities of comercial websites and internet payment systems* y *Money laundering using new payment methods*, 2010) y a las **tarjetas prepago** puesto que permiten extraer dinero de un cajero automático sin necesidad de identificarse ni de disponer de una cuenta bancaria. Ha dado directrices sobre tarjetas prepago, pagos móviles y servicios de pago en Internet, así como, sobre monedas virtuales ya que suponen un riesgo potencial de blanqueo y financiación del terrorismo.

En la **Recomendación 1 del GAFI** sobre evaluación de riesgos y aplicación de un enfoque basado en riesgo requiere que los países identifiquen y evalúen los riesgos y creen las condiciones para mitigarlos, por lo tanto, si hay un riesgo asociado a las monedas virtuales y el uso de nuevas tecnologías, deriva una obligación de los países de intervenir legalmente.

La **Recomendación 14 del GAFI** sobre servicios de transferencia de dinero o valores establece que los países deben tomar medidas para asegurar que las personas naturales o jurídicas que prestan servicios de transferencia de dinero o valores tengan licencia o estén registradas, y estén sujetas a sistemas eficaces para



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

el monitoreo y para asegurar el cumplimiento con las medidas establecidas en las Recomendaciones del GAFI.

La **Recomendación 15 del GAFI** sobre nuevas tecnologías dispone que los países y las instituciones financieras deben identificar y evaluar los riesgos de lavado de activos o financiamiento del terrorismo que pudieran surgir por el desarrollo de nuevos productos y nuevas prácticas comerciales y por el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como existentes.

Con respecto a la **Recomendación 16 del GAFI** sobre transferencias electrónicas, los países deben asegurar que las instituciones financieras incluyan información sobre el ordenante y el beneficiario de una transferencia electrónica.

Sobre las nuevas tecnologías en prevención del blanqueo de capitales tenemos el **análisis predictivo** que está diseñado para que las organizaciones puedan investigar las actividades financieras sospechosas más eficazmente. Se generan informes y alertas aumentando la eficacia de las investigaciones. Los usuarios que tienen acceso a esta herramienta pueden modificar o crear multitud de escenarios posibles para controlar más riesgos y conductas y encontrar con más facilidad los delitos fiscales. Permiten anticipar el comportamiento de personas o sistemas y así poder tomas mejores decisiones.

La **inteligencia artificial** y el ***Machine Learning*** permiten identificar patrones de comportamiento reduciendo posibles positivos que se producen sobre todo cuando se chequean denominaciones de personas y activos de distintos países e idiomas.

La **biometría** mediante el reconocimiento facial que permita a las entidades aplicar las medidas de diligencia debida y *Know Your Costumer* adecuadas y cumplir con la regulación. El cliente recibe un SMS o e-mail para validar su identidad, tendrá que realizar una captura del DNI y completar la validación biométrica o prueba de vida a través de sus rasgos faciales, también el proceso de firma digital avanzada.

La **tecnología *blockchain*** que también sirve para prevenir actividades ilícitas. Es un registro en la red capaz de registrar todas las transacciones que se introduzcan en la misma. Se almacenan datos a los que se accede a través de las diferentes direcciones pudiendo consultar cualquier movimiento que se haya producido sin necesidad de papel o desplazamientos a los registros tal y como los conocemos en la actualidad.

En el Anteproyecto de Ley de junio de 2020 por el que se modifica la Ley 10/2010 de 28 de abril cabe destacar la Disposición adicional segunda donde se regula el Registro de proveedores de servicios de cambio de moneda virtual por moneda de curso legal y monedero de custodia, dependiente del Banco de España. En este Registro deberán estar inscritas las personas que provean servicios de cambio



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

de monedas virtuales por moneda fiduciaria y servicios de custodia de monederos electrónicos a residentes en España. El acceso al registro estará condicionado al cumplimiento de los requisitos de honorabilidad comercial y profesional que se determinen reglamentariamente ya que si no fuera el caso, determinará la pérdida de la inscripción en este Registro. El Banco de España supervisará el cumplimiento de la obligación de registro y de las condiciones de honorabilidad exigidas para el acceso y mantenimiento de la inscripción.



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.

## Participantes en el grupo de trabajo que han elaborado este documento:

Coordinador/a del grupo de trabajo:

- Wessels, Gail

Participantes (por orden alfabético):

- De Vicente Rodriguez, Teresa
- Goiria Martinez, Natalia
- Madrid Gil, Claudia
- Millan, Adolfo
- Passau, Rosa
- Peredo Pérez, Alvaro
- Rial, Denise
- Rodríguez Fernández, Gema
- Santos Arjona, Rebeca
- Wessels, Gail



© ASCOM. Prohibida la distribución o reproducción total o parcial de este documento sin el consentimiento de ASCOM.


Asociación
Española
de Compliance