IAESIR Finance
www.iaesirfinance.com

IAESIR
FINANCE

IAESIR

IAESIR Finance Regulatory Compliance Manual

Operations Manual and Code of Ethics

Compliance Office

@iaesirfinance @iaesirfinance support@iaesirfinance.com

IAESIR FINANCE

MANUAL DE POLÍTICAS INTERNAS PARA LA PREVENCIÓN DEL BLANQUEO DE CAPITALES Y DE LA FINANCIACIÓN DEL TERRORISMO

INTRODUCCIÓN

COMPLIANCE OFFICE

Desde la Dirección General y todos los miembros que formamos el equipo de IAESIR somos conscientes de la trascendencia que la prevención del blanqueo de capitales y la financiación del terrorismo suscita.

La Sociedad ha aprobado este Manual de Prevención de Blanqueo de Capitales y Financiación del Terrorismo (PBCFT), que además de estar supervisado en su cumplimiento por nuestro departamento interno de Compliance, cuenta con la auditoría externa de nuestro parthner en Compliance RAP Informes Legales S.L, así como con la validación expresa por parte de nuestro Exchange oficial BINANCE.

Con el fin de seguir cumpliendo con las obligaciones previstas en la normativa sobre PBCFT, y siendo la transparencia en todos nuestros procedimientos nuestra principal máxima a seguir, ponemos a su disposición este manual para que le sirva de ayuda y referencia a la hora de conocer nuestra forma de operar y los procedimientos a seguir para garantizar la máxima seguridad a nuestros clientes.

TÍTULO I. PROCEDIMIENTOS INTERNOS DE DILIGENCIA DEBIDA, ADMISIÓN DE CLIENTES Y ANÁLISIS DE OPERACIONES

Artículo 1.- Medidas de diligencia debida

1.1. ACEPTACIÓN DE CLIENTES

Como desarrollo de lo dispuesto en el Manual, los procedimientos de aceptación de clientes, así como los procedimientos de identificación y conocimiento de los mismos, ayudan a proteger a la Sociedad de ser utilizada como vehículo para llevar a cabo actividades delictivas o para estafar a la propia entidad.

Los procedimientos tienen pues como finalidad la prevención de los riesgos (reputacional, operativo, legal...) que pueden implicar a la Sociedad, a participar incluso involuntariamente, en actividades ilegales o poco éticas.

La aceptación de clientes por parte de la Sociedad se fundamenta en el establecimiento de relaciones comerciales basadas en la comunicación transparente y que sea el propio cliente el que afirme o niegue su propia información y en el conocimiento de las empresas participadas y de sus actividades económicas.

Hay que resaltar que la Sociedad no recomienda ningún tipo de inversión o promueve o estimula que lleven a cabo ningún tipo de operación así como tampoco favorece o recomienda que se tome decisiones de inversión sobre la base de las recomendaciones de inversión realizadas por la Sociedad.

La Sociedad clasificará a los clientes de conformidad con la clasificación detallada más abajo, limitando sus operaciones al riesgo preconcebido en función del tramo donde opere, teniendo en cuenta que las operaciones que lleve a cabo el cliente son totalmente autónomas y diseñadas por el propio cliente, limitándose la responsabilidad de la Sociedad a acreditar el origen de los fondos cada vez que solicita su entrada como cliente así como que su capacidad económica es suficiente para poder asumir el riesgo en la operativa que plantea. Estos límites están basados en la orientación al riesgo interna de la Sociedad que es aprobada por el órgano de administración, periódicamente, así como implementada y desarrollada internamente.

Identificación y conocimiento de los clientes

En el establecimiento de relaciones comerciales, la Sociedad exige la identificación mediante prueba biométrica y pruebas de vida de sus clientes.

Es importante resaltar que no se iniciarán relaciones comerciales cuando el cliente se niegue a identificarse o la identificación no resulte veraz o suficiente.

La comprobación de la identidad de los potenciales clientes se realizará mediante documentos fehacientes vigentes, con fotografía y firma, verificando que la firma utilizada en los contratos y comprobantes coincide con la del documento de identificación.

La identificación clara y concreta del cliente es un elemento esencial dentro del proceso de establecimiento de relaciones, así como la obtención de toda la información necesaria acerca de la identidad de cada nuevo cliente.

El proceso de identificación se articula de la siguiente forma:

- ·Documentación de identificación y conocimiento del cliente: En el procedimiento de aceptación de cliente de la Sociedad, se solicitará la información y documentación necesaria de acuerdo con la normativa interna vigente:
- ·Identificación de la persona física o jurídica: Tarjeta de Residencia, Tarjeta de Identidad de Extranjero o Pasaporte en vigor / CIF de la sociedad y escritura de constitución. En caso de personas jurídicas no residentes deberá asegurarse si es necesario la apostilla de la Haya.
- ·Escritura de poderes en virtud del cual operan los representantes y autorizados.
- ·Documento de identidad de las personas que actúan como autorizados/representantes.
- ·Escritura de poderes de los representantes y autorizados.
- ·Debe determinarse la estructura de propiedad o control, aportando documento descriptivo de la estructura accionarial, debidamente firmado por el administrador.
- ·Declaración responsable del cliente de último beneficiario para identificar al titular real (persona física) o acta de titularidad real del notario y, para sociedades con riesgo superior al promedio, comprobación de dicha identificación mediante la obtención de documentación o fuentes externas fiables.
- ·Documentación que acredite la actividad económica o profesional indicada por la sociedad.
- ·En casos de sujetos obligados a la Ley de prevención de blanqueo de capitales y de la financiación del terrorismo, acreditación de su condición y/o auditoria de experto externo.
- ·Informaciones públicas para evaluar posibles riesgos reputacionales.

Toda la documentación de identificación y conocimiento del cliente recogida, se digitaliza y se archiva en la carpeta de expediente del cliente.

Identificación del Titular Real:

Con carácter previo al establecimiento de relaciones de negocio o a la ejecución de cualquier operación, se debe identificar y adoptar medidas necesarias para comprobar la identidad del Titular Real.

A los efectos de la Ley, se entiende por Titular Real:

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

2. La persona o personas físicas que en último término posean o controlen, directa o indirectamente, un porcentaje superior al 25% del capital o de los derechos de voto de una persona jurídico, o que a través de acuerdos o disposiciones estatutarias o por otros medios ejerzan el control, directo o indirecto, de una persona jurídica.
Serán indicadores de control por otros medios, entre otros, los previstos en el artículo 22 (1) a (5) de la Directiva 2013/34/UE del Parlamento Europeo y el Consejo, de 26 de junio de 2013 sobre los estados financieros anuales, los estados financieros consolidados y otros informes afines de ciertos tipos de empresas.

Se exceptúan las sociedades que coticen en un mercado regulado y que estén sujetas a requisitos de información acordes con el Derecho de la Unión o normas internacionales equivalentes que garanticen la adecuada transparencia de la información sobre la propiedad.

Si no existe ninguna persona física que disponga de un porcentaje superior al 25%, se considerará que ejerce dicho control el administrador o administradores. En el caso de que el administrador sea una persona jurídica, se entenderá que el control es ejercido por la persona física nombrada por el administrador persona jurídica.

3. La persona o personas físicas que sean titulares o ejerzan el control del 25% o más de los bienes de instrumento o persona jurídicos que administre o distribuya fondos, o, cuando los beneficiarios estén aún por designar, la categoría de personas en beneficio de la cual se ha creado o actúa principalmente la persona o instrumento jurídicos.

Se debe recabar información de los clientes para determinar si éstos actúan por cuenta propia o de terceros. Cuando existan indicios o certeza de que los clientes no actúan por cuenta propia, se debe recabar la información precisa a fin de conocer la identidad de las personas por cuenta de las que actúan y caso de tratarse de personas clasificados de riesgo superior al promedio, obtener y digitalizar la documentación identifacativa de los titulares reales, la documentación que acredite la actividad económica o profesional de éstos y la documentación que acredite la coherencia del origen lícito de los fondos que aportan, tal como se indica en el capítulo anterior.

Se deben adoptar medidas adecuadas al efecto de determinar la estructura de propiedad y de control de las personas jurídicas.

La Ley obliga a no establecer o mantener relaciones de negocio con personas jurídicas, cuya estructura de propiedad y de control no haya podido determinarse. Si se trata de sociedades cuyas acciones estén representadas mediante títulos al portador, se aplicará la prohibición anterior salvo que se pueda determinar por otros medios la estructura de propiedad y de control. Esta prohibición no será aplicable a la conversión de los títulos al portador en títulos nominativos o en anotaciones en cuenta.

Se deberá informar de la estructura accionarial o de control de todas las personas jurídicas ya dadas de alta con anterioridad, ya que no se podrán vincular como titulares o equivalentes a ningún nuevo contrato o producto en el caso que no exista dicha información. La pantalla de detalle del vínculo permitirá también acceder al formulario de estructura accionarial o de control para cumplimentar la información y poder finalizar la vinculación.

Además de lo descrito en las letras precedentes, en el caso de que la persona jurídica esté clasificada por el sistema como de riesgo alto en materia de PBCFT, se deberá hacer constar en el documento de "estructura accionarial o de control", en el caso de que exista, toda la cadena de personas jurídicas interpuestas hasta llegar a identificar a las personas físicas titulares reales, obtenido documentación que acredite la propiedad de todas ellas.

No obstante, será preceptiva la obtención de documentación adicional o de información de fuentes fiables independientes cuando el cliente, el titular real, la relación de negocios o la operación presenten riesgos superiores al promedio, así como:

a. Cuando existan indicios de que la identidad del titular real, declarada por el cliente no es exacta o veraz.

b. Cuando concurran indicios de blanqueo de capitales o de financiación del terrorismo que impliquen examen especial o comunicación por indicio.

Se lleva a cabo una prueba de identidad digital a través de un sistema de verificación digital en el que además de insertar fotografías, se pedirá el escaneo de toda la documentación acreditativa.

Tanto las fotografías, como la documentación escaneada pasarán a formar parte del archivo digital de IAESIR, el cual cumple con todas las medidas legales para el cumplimiento de la Ley de Protección de Datos.

1.2. PERSONAS PROHIBIDAS

No se establecerán o mantendrán relaciones comerciales con personas que dificulten, a través de la ocultación o por cualquier otro medio, datos sobre su identificación, personalidad, residencia o actividad. Tampoco se establecerán relaciones comerciales

con personas de las que se tenga constancia que estén relacionadas con cualquier actividad delictiva, ni con personas físicas o jurídicas que operen sin las autorizaciones administrativas pertinentes en los casos en que sean necesarias.

Para ello se coteja la aparición del posible cliente en los listados internacionales que tenemos internamente configurados durante la admisión de este.

Por tanto, cuando en los contactos previos con el potencial cliente, no parezcan claros los motivos por los cuales pretende abrir la cuenta, o cuando los mismos provoquen dudas o sospechas razonables sobre la licitud y coherencia de las actividades que desarrollan u operativa que pretenden canalizar, se comunicará a la persona que no podemos atender su solicitud de inicio de relaciones comerciales.

Así pues, no se establecerán relaciones de negocio, con siguientes categorías de clientes, o proveedores:

- Personas o entidades vinculadas a grupos u organizaciones terroristas o las que lleven a cabo actividades terroristas o contribuyan a los fines perseguidos por dichos grupos u organizaciones, así como tampoco aquellas personas o entidades incluidas en alguna de las listas públicas de personas sancionadas por vinculación con el terrorismo o grupos afines.
- Personas o sociedades que conste que estén relacionadas con cualquier tipo de actividad delictiva.
- Personas o sociedades que tengan negocios cuya naturaleza haga imposible la verificación de la legitimidad de sus actividades o la procedencia de sus fondos.
- Personas o sociedades que rehúsen facilitar información o la documentación requerida.

- Cualquier persona física, entidad u organización que legalmente deba disponer de alguna autorización administrativa para operar, y que carezca de ella (sociedades de inversión, entidades de pago, remesadoras de fondos, casinos, bingos, ONG, casas de cambio, etc.).
- Actividades relacionadas con la prestación de servicios sexuales (prostíbulos, clubs de alterne, etc.).
- Asociaciones o similares relacionadas con el consumo de sustancias estupefacientes o similares (clubs de fumadores de marihuana, etc.).
- Personas objeto que fueron objeto de examen especial y se determinó su cancelación, y que en la nueva petición de alta existen indicios de BCFT o la información o documentación aportada es insuficiente para aplicar las medidas de diligencia debida reforzada.

1.3. SEGMENTACIÓN POR RIESGO DE LOS CLIENTES

En este sentido la Sociedad ha categorizado a los clientes en tres clases:

a) Clientes minoristas no cualificados: Esta es la categoría en la que se encuentran la mayoría de los inversores particulares. Su límite de operaciones es inferior dado que son aquellos con menos conocimientos y experiencia en la compra u operativa de este tipo de activos Como cliente minorista, recibirá el mayor grado de protección.

b) Clientes minoristas avanzados: Serán aquellos que afirmen serlo o por su forma de actuar se detecte que tienen esa condición. Su límite de operativa es superior y se le requiere más documentación. En consecuencia, reciben menos protección ya que tienen más capacidad para comprender la naturaleza y los riesgos de los mercados, productos y servicios de inversión.

c) Clientes profesionales: aquellos que operan por cuenta de terceros.

1.4. APLICACIÓN DE LAS MEDIDAS DE DILIGENCIA DEBIDA EN LA ACEPTACIÓN DE NUEVOS CLIENTES

La Sociedad solicitará la cumplimentación del cuestionario "Know your client" en el que el cliente se compromete a decir la verdad.

Se le proporcionará un documento en función del tipo de cliente que indique con preguntas idóneas al tipo de cliente por el que se vaya a clasificar.

Además de lo anterior la Sociedad llevará a cabo las siguientes operaciones:

- Rastreo de todas las personas intervinientes en la operación. Antes de iniciar la relación de negocio, se deberá contrastar manualmente las personas intervinientes.
- Análisis de la información/documentación facilitada: La Sociedad solicitará la documentación necesaria para conocer la estructura de propiedad, los titulares reales, el accionariado resultante tras la operación de inversión o desinversión así como él órgano de administración de la compañía.
- El análisis de la información facilitada tendrá en cuenta:
  - Coherencia de la información y documentación facilitada.
  - Realización de los controles necesarios y razonables para comprobar la veracidad de la información facilitada (mediante mecanismos adicionales como registros oficiales, páginas Web, servicios de información económica u otros que en cada momento resulten más adecuados para contrastar la información).
  - Verificación sobre operativa/vinculación de la sociedad con países de alto riesgo en materia de blanqueo de capitales y/o financiación del terrorismo.

Como los Clientes se dirigen a la Sociedad a través de medios telemáticos, no encontrándose físicamente presentes, para poder entablar relaciones de negocio deberá concurrir alguna de las siguientes circunstancias:

a) La identidad del Cliente quede acreditada de conformidad con lo dispuesto en la normativa aplicable sobre firma electrónica, mediante firma electrónica cualificada.

b) La identidad del Cliente quede acreditada mediante copia Tarjeta de Residencia, Tarjeta de Identidad de Extranjero o Pasaporte en vigor.

c) El primer ingreso proceda de una cuenta a nombre del mismo Cliente abierta en una entidad domiciliada en la Unión Europea o en países terceros equivalentes.

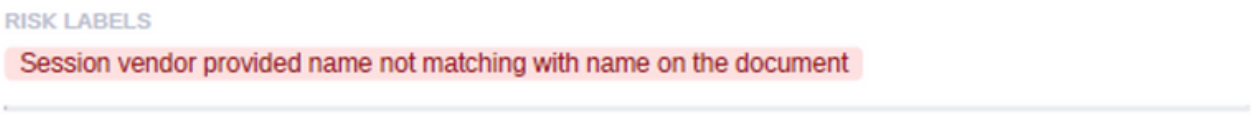
d) La identidad del cliente quede acreditada mediante el empleo de otros procedimientos seguros de identificación de clientes en operaciones no presenciales, siempre que tales procedimientos hayan sido previamente autorizados por el Organismo de Prevención.

En todo caso, en el plazo de un mes desde el establecimiento de la relación de negocio, se deberá obtener de estos clientes una copia de los documentos necesarios para practicar la diligencia debida.

Cuando se aprecien discrepancias entre los datos facilitados por el cliente y otra información accesible, será preceptivo contactar con el Cliente.

Tal y como se ha señalado con anterioridad, en las relaciones de negocio que mantiene la Sociedad, que son no presenciales, se aplicarán las medidas reforzadas de diligencia debida señaladas anteriormente.

La aplicación utilizada ejecutará el siguiente control de análisis de la documentación proporcionada de forma automática, avisando en caso de que esta no coincida con los datos aportados, tal y como se muestra a continuación



En caso de duda o sospecha se produce un escalado de forma inmediata que analiza la documentación proporcionada.

Cualquier persona que por su profesión o actividad pertenezcan a la Administración General del Estado, Administraciones de las Regiones, Entidades que integren la administración local así como cualquier otra entidad del sector público o bien sea una Autoridad, es decir, cualquier persona que tenga cargo o jurisdicción propia como miembro de alguna corporación, tribunal u órgano colegiado, y en todo caso si

pertenece al Congreso de los Diputados, a las Asambleas legislativas o sea un cargo electo de un partido político (en adelante "PRP") será tratado como un cliente minorista avanzado a los efectos de aportación de la documentación.

1.5. SEGUIMIENTO CONTINUO DE LA RELACIÓN DE NEGOCIOS

La Sociedad aplicará medidas de seguimiento continuo a la relación de negocios, a lo largo de dicha relación a fin de garantizar que:

a) Las informaciones aportadas por el Cliente coincidan con el conocimiento que se tenga del mismo y de su perfil empresarial y de riesgo, incluido el origen de los fondos.

b) Los documentos, datos e información de que se disponga estén actualizados. La actualización será preceptiva cuando se verifique un cambio relevante en la actividad del cliente que pudiera influir en su perfil de riesgo.

1.6. REVISIÓN DE LA DOCUMENTACIÓN E INFORMACIÓN

La Sociedad revisará todos los documentos, datos e informaciones obtenidos como consecuencia de la aplicación de las medidas de debida diligencia descritas en este Manual, para garantizar que se mantengan actualizados y se encuentren vigentes y se realizará una comunicación al responsable de blanqueo designado si se detectara algún comportamiento sospechoso.

No obstante, lo anterior, tendrá lugar la actualización inmediata de toda la documentación e información referida a un Cliente cuando se tenga conocimiento de un cambio relevante en la actividad del Cliente que pudiera influir en su perfil de riesgo.

Artículo 2.- Conservación de documentos

La Sociedad conservará durante diez años los originales o copias con fuerza probatoria de los documentos o registros correspondientes que acrediten adecuadamente la realización de las operaciones y las relaciones de negocio con sus Clientes.

La Sociedad conservará durante un plazo de cinco años, copia de los documentos fehacientes de identificación, las declaraciones del cliente, la documentación e información aportada por el cliente u obtenida de fuentes fiables independientes, la documentación contractual, y los resultados de cualquier análisis efectuado.

Los documentos fehacientes de identificación de los intervinientes en una relación de negocios o una operación se almacenarán en soportes ópticos, magnéticos o electrónicos que garanticen su integridad, la correcta lectura de los datos, la imposibilidad de manipulación y su adecuada conservación y localización.

Asimismo, la Sociedad conservará información sobre aquellas operaciones meramente intentadas que no fueron ejecutadas atendiendo a su riesgo asociado con objeto de ponerlas en comunicación del Organismo de Prevención en caso de ser necesario.

Una vez transcurrido el periodo de diez o cinco años, de conformidad a lo anterior, se procederá a la eliminación de la documentación.

Artículo 3.- Medidas simplificadas de diligencia debida

La Sociedad, en función del riesgo y dependiendo del tipo de Cliente, aplicarán las medidas simplificadas de diligencia debida respecto de los siguientes Clientes:

a) Entidades de derecho público de los Estados miembros de la Unión Europea o de países terceros equivalentes.

b) Las sociedades u otras personas jurídicas controladas o participadas mayoritariamente por entidades de derecho público de los Estados miembros de la Unión Europea o de países terceros equivalentes.

c) Entidades financieras, exceptuadas las entidades de pago, domiciliadas en la Unión Europea o en países terceros equivalentes que sean objeto de supervisión para garantizar el cumplimiento de las obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo.

d) Las sucursales o filiales de entidades financieras, exceptuando las entidades de pago, domiciliadas en la Unión Europea o en países terceros equivalentes, cuando estén sometidas por la matriz a procedimientos de prevención del blanqueo de capitales y de la financiación del terrorismo.

e) Sociedades con cotización en bolsa cuyos valores se admitan a negociación en un mercado regulado de la Unión Europea o de países terceros equivalentes, así como sus sucursales y filiales participadas mayoritariamente.

En los supuestos precedentes, la Sociedad podrá aplicar, en función del riesgo, una o varias de las siguientes medidas:

a) Comprobar la identidad del Cliente o del titular real únicamente cuando se supere un umbral cuantitativo superior a 100.000 euros, con posterioridad al establecimiento de la relación de negocios.

b) Reducir la periodicidad de revisión documental, de tal forma que pase a ser de dos (2) años.

c) No recabar información sobre la actividad profesional o empresarial del Cliente, infiriendo el propósito y naturaleza por el tipo de operaciones o relación de negocios establecida.

Queda prohibida la aplicación de medidas simplificadas de diligencia debida en el caso de países terceros no calificados como equivalentes o respecto de los que la Comisión Europea adopte una decisión sancionadora.

La Sociedad reunirá, en todo caso, la información suficiente para determinar si el Cliente puede acogerse a una de las excepciones previstas en este artículo.

En ningún caso la Sociedad podrá aplicar medidas simplificadas de diligencia debida, o cesará de aplicarlas, si concurren o surgen indicios o certeza de blanqueo de capitales o de financiación del terrorismo o riesgos superiores al promedio.

Artículo 4.- Medidas reforzadas de diligencia debida.

La Sociedad presentará además de las medidas normales de diligencia debida, medidas reforzadas en relación con los países que presenten deficiencias estratégicas en sus sistemas de lucha contra el blanqueo de capitales y la financiación del terrorismo y figuren en la decisión de la Comisión Europea adoptada de conformidad con lo dispuesto en el artículo 9 de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015.

Asimismo, se aplicarán además de las medidas normales de diligencia debida, otras medidas reforzadas en las ocasiones en que la especial naturaleza del negocio presente un riesgo más elevado de blanqueo de capitales o financiación del terrorismo, que serán aplicadas en todo caso en las siguientes actividades:

a) Operaciones en circunstancias inusuales (aquellas cuya cuantía, características y periodicidad no guardan relación con la actividad y tipo del cliente, salen de los parámetros de normalidad o no tienen un fundamento legal evidente).

b) Operaciones con clientes no residentes en la Unión Europea.

c) Operaciones con sociedades de mera tenencia de activos.

d) Operaciones con sociedades cuya estructura accionarial y de control no sea transparente o resulte inusual o excesivamente compleja.

e) Operaciones con clientes que empleen habitualmente medios de pago al portador.

f) Operaciones con clientes de países, territorios o jurisdicciones de riesgo recogidos en el presente Manual, o que supongan transferencia de fondos de o hacia tales países, territorios o jurisdicciones.

Estas medidas consistirán en todo caso en:

- Aplicar procedimientos adecuados en función del riesgo a fin de determinar los riesgos asociados a la operación.
- Actualizar, al menos anualmente, los datos obtenidos en el proceso de aceptación del cliente.
- Obtener documentación o información adicional sobre el Cliente y sobre el titular real (p. ej. Declaraciones fiscales, nóminas, contratos, escrituras públicas, certificados de Registros Públicos, informes de auditores, dictámenes de expertos independientes, ...)

Así mismo, se podrán imponer limitaciones a las operaciones por su naturaleza, su cuantía o los medios de pago empleados como las que se exponen en el Artículo siguiente, que podrán terminar, en función de la concurrencia en la operativa de indicios o certeza de relación con el blanqueo de capitales o la financiación del terrorismo, con su no ejecución y con una comunicación al Organismo de Prevención.

Artículo 5. Examen especial de operaciones sospechosas

La Sociedad examinarán, dentro de sus respectivas esferas de actuación, cualquier operación que por su naturaleza pueda estar aparentemente vinculada al blanqueo de capitales o a la financiación del terrorismo, esto es, toda operación compleja, inusual, o que no tenga un propósito económico o lícito aparente, o que presente indicios de simulación o fraude y, en especial, las operaciones que a continuación se describen. Estas operaciones pueden requerir actuaciones en materia de aceptación o rechazo de Clientes de clasificación de los mismos por criterios de riesgo de blanqueo, de realización de comunicaciones o de análisis especial de operaciones.

A continuación, se detalla un catálogo de características que, de concurrir en una operación, pueden llevar a su consideración como sospechosa:

- **Por el tamaño y frecuencia de las operaciones**

a) Estructurar operaciones en pequeñas cantidades, o en cantidades por debajo de los umbrales de mantenimiento de registros o informes, similar a estructurar operaciones en efectivo.

b) Realizar múltiples operaciones de alto valor:

- En una sucesión breve, como en un período de 24 horas;
- En un patrón escalonado y regular, sin más operaciones registradas durante un largo periodo posterior, lo cual es particularmente común en casos relacionados con ransomware; o
- A una cuenta recién creada o previamente inactiva.

c) Transferir criptomonedas inmediatamente a múltiples prestadores de servicios de intercambio de moneda virtual o de billetera de moneda virtual ("Prestador"), especialmente a proveedores registrados o que operan en otra jurisdicción donde:

- no hay relación con el lugar donde vive o realiza negocios el cliente; o
- regulación PBCFT inexistente o débil.

d) Depositar una criptomoneda en una wallet de un exchage y luego, a menudo, inmediatamente:

  - retirar la criptomoneda sin actividad de cambios a otras criptomonedas, lo cual es un paso innecesario e incurre en tarifas de operación;
  - convertir las criptomonedas en múltiples tipos de criptomonedas, incurriendo nuevamente en tarifas de operación adicionales, pero sin una explicación comercial lógica (por ejemplo, diversificación de la cartera); o
  - retirar las criptomonedas de un Prestador inmediatamente a una cartera privada.

e) Aceptar recursos sospechosos de ser robados o fraudulentos:

·Depositar recursos de direcciones de wallets que han sido identificadas como tenedoras de fondos robados, o direcciones de wallets vinculadas a los tenedores de fondos robados.

- Operaciones relativas a nuevos usuarios

a) Realizar un gran depósito inicial para abrir una nueva relación con un Prestador, mientras que el monto financiado es inconsistente con el perfil del cliente.

b) Realizar un gran depósito inicial para abrir una nueva relación con un Prestador y financiar el depósito completo el primer día que se abre, y que el cliente comience a negociar el monto total o una gran parte del monto ese mismo día o un día después, o si el cliente retira el importe total al día siguiente. Como la mayoría de las criptomonedas tienen un límite transaccional para los depósitos, el lavado de grandes cantidades también se puede realizar a través del comercio extrabursátil.

c) Un nuevo usuario intenta negociar el saldo completo de las criptomonedas, o retira las criptomonedas e intenta enviar el saldo completo fuera de la plataforma.

- Operaciones relativas a todos los usuarios

a) Operaciones que involucran el uso de múltiples criptomonedas, o múltiples cuentas, sin una explicación comercial lógica.

b) Hacer transferencias frecuentes en un período de tiempo determinado (por ejemplo, un día, una semana, un mes, etc.) a la misma cuenta de criptomonedas:

- por más de una persona;
- desde la misma dirección IP por una o más personas; o
- en relación con grandes cantidades.

c) Operaciones entrantes de muchas carteras no relacionadas en cantidades relativamente pequeñas (acumulación de recursos) con transferencia posterior a otra cartera o cambio completo por moneda fiduciaria. Dichas operaciones de varias cuentas acumuladas relacionadas pueden utilizar inicialmente criptomonedas en lugar de moneda fiduciaria.

d) Realizar un cambio de moneda virtual-fiduciaria con una pérdida potencial (por ejemplo, cuando el valor de criptomoneda fluctúa, o independientemente de las comisiones anormalmente altas en comparación con los estándares de la industria, y especialmente cuando las operaciones no tienen una explicación comercial lógica).

e) Convertir una gran cantidad de moneda fiduciaria en criptomonedas, o una gran cantidad de un tipo de criptomonedas en otros tipos de criptomonedas, sin una explicación comercial lógica.

Cuando, de conformidad con lo anterior, una operación esté siendo objeto de análisis especial, deberán documentarse las fases de análisis, las gestiones realizadas y las fuentes de información consultadas, conforme al siguiente protocolo:

Cada operación o hecho sospechoso detectado recibirá un número de expediente para facilitar su ordenación y las comunicaciones en referencia a ella.

Se analizará la información y documentación obtenida del cliente, fuentes de información públicas externas (registros oficiales (mercantil, de la propiedad...), búsquedas en internet, visitas presenciales a las oficinas, almacenes o locales declarados por el cliente como lugares donde ejerce su actividad mercantil, y se revisará el histórico de operaciones realizadas por el cliente con anterioridad en el registro de operaciones de la Sociedad con el objeto de comprobar la correspondencia entre importes, fechas, beneficiarios, documentos aportados, frecuencia, concepto...

En caso de resultar la información incompleta o insuficiente para extraer una conclusión acerca del carácter sospechoso de la operación, el Responsable se dirigirá directamente al cliente con el objeto de conseguir la información o documentación adicional que en cada caso sea precisa.

Se estudiará la correspondencia entre la actividad del cliente y las operaciones realizadas. En el supuesto de detectarse una falta de correspondencia clara se deberá solicitar la acreditación de los fondos.

Se utilizarán las distintas bases de datos a las que la Sociedad pueda tener acceso para averiguar si hay alguna coincidencia entre los nombres y apellidos de las personas en dichas listas y los nombres y apellidos de las personas involucradas en la operación sospechosa.

En caso de que se necesite información adicional se deberá contactar con la persona que comunicó la operación.

Concluido el análisis técnico, el Compliance Officer determinará si procede o no la comunicación al Organismo de Prevención, en función de la concurrencia en la operativa de indicios o certeza de relación con el blanqueo de capitales o la financiación del terrorismo. Toda decisión del responsable de blanqueo deberá basarse en criterios homogéneos y deberá estar debidamente motivada.

Compliance Officer será el responsable de elaborar, revisar anualmente y difundir vía correo electrónico entre sus directivos, empleados y colaboradores externos una

relación de operaciones que por su naturaleza puedan ser susceptibles de estar relacionadas con el blanqueo de capitales y la financiación del terrorismo.

Artículo 7.- Deber de confidencialidad

Las entidades obligadas no revelarán al Cliente ni a terceros las actuaciones que estén realizando en relación con sus obligaciones en materia de PBCFT.

Los procedimientos de comunicación interna de las entidades obligadas al Compliance Officer así como los procedimientos de comunicación externa de éste último al Organismo de Prevención responderán a los principios de rapidez, seguridad, eficacia y coordinación.

En especial, las entidades obligadas deberán guardar la más estricta confidencialidad con respecto a las operaciones que estén siendo objeto de análisis o hayan sido comunicadas al Organismo de Prevención.

Artículo 8.- Alertas e información interna. Comunicación de potenciales incumplimientos

a) Comunicación de operativa sospechosa

La Sociedad tiene establecidos procedimientos de comunicación a fin de que se puedan comunicar inmediatamente al Compliance Officer los hechos que pudieran tener relevancia en la PBCFT.

Las comunicaciones habrán de contener como mínimo los datos que permitan individualizar al sujeto o sujetos afectados, hechos u operaciones, cuantías, lugar y fechas a que se circunscriben, tal y como se indica en el formulario habilitado a estos efectos. De dichas comunicaciones deberá quedar constancia tanto para el comunicante como para él órgano de comunicación.

Las comunicaciones internas al Compliance Officer se realizarán por correo electrónico. Cada empleado lo hará llegar al Compliance Officer a la dirección que este tenga disponible o entregándo lo personalmente en sobre cerrado.

Efectuada la comunicación al Compliance Officer, el directivo o empleado quedará exento de responsabilidad.

El Compliance Officer adoptará las medidas adecuadas para mantener la confidencialidad sobre la identidad de la persona/s que hayan realizado la comunicación.

Recibida una comunicación, el Compliance Officer procederá a su inmediato análisis o comprobación para determinar la relación de los hechos u operaciones comunicados con el blanqueo de capitales. Si se apreciara indicio o certeza de blanqueo de capitales se procederá conforme a lo indicado en este Manual. Toda operación identificada como objeto de necesario análisis especial, figurará en un registro numérico secuencial en el que constarán, además de tal número identificativo, los siguientes campos:

a) Fecha de apertura del expediente de análisis.

b) Descripción sucinta de la causa de la inclusión de la transacción en el análisis.

c) Descripción de la operativa analizada.

d) Decisión sobre el expediente y las razones en que se basa.

e) Fecha de cierre.

f) Decisión sobre su comunicación o no al Organismo de Prevención y su fecha, así como la fecha en que, en su caso, se realizó la comunicación.

g) Otros datos.

Las transacciones en las que concurran las circunstancias objeto de consideración en el presente procedimiento, serán objeto de expediente físico. En él se incluirá una copia de los documentos asociados al análisis realizado.

Las técnicas de análisis a utilizar, de acuerdo con la decisión del Compliance Officer, y, en todo caso, de acuerdo con las características específicas de la investigación en curso, serán las siguientes:

a) Búsqueda en Internet.

b) Búsqueda en Registros Oficiales (dependiendo de su existencia, y de acuerdo con la jurisdicción de los intervinientes).

c) Solicitud de opinión al gestor del Cliente.

d) Consultas a terceros.

e) Análisis económico-financiero de los datos de las transacciones (reconstrucción de movimientos, análisis de suficiencia de flujos de caja, cuantificación del origen de fondos, etc.).

f) Otras que de acuerdo con las características pudieran contribuir a su esclarecimiento (entrevistas, solicitudes adicionales de información a los intervinientes, etc.).

Todo análisis debe concluir con una de las siguientes decisiones:

a) Comunicación al Organismo de Prevención de la transacción por considerarla sospechosa, de acuerdo con las reglas oportunas para la toma de decisiones y los procedimientos en vigor para tal resolución.

b) Archivo de las actuaciones por considerar normal la transacción.

c) Mantenimiento en seguimiento de los intervinientes hasta la consecución de un grado de esclarecimiento tal que permita la clasificación en uno de los dos anteriores estados.

Cualquiera que sea el criterio adoptado se informará a la Persona Obligada del curso dado a su comunicación.

Todo empleado tiene la posibilidad de comunicar directamente al Organismo de Prevención operaciones con indicios o certeza de estar relacionadas con el blanqueo de capitales, en los casos en que el Compliance Officer no informe al comunicante del curso dado a su comunicación en el plazo de veinte días hábiles desde la comunicación al Compliance Officer.

b) Comunicación de potenciales incumplimientos

La Sociedad tiene a disposición de todos sus empleados, directivos o agentes un canal interno de denuncias para que estos puedan comunicar, incluso anónimamente, información relevante sobre posibles incumplimientos o carencias, en materia de PBCFT, que tengan lugar en el seno de la Sociedad, tanto en lo relativo a incumplimientos expresos de la normativa de aplicación, como en el desarrollo de las políticas y procedimientos internos.

El canal será gestionado por el Representante, que ejercerá las funciones de administrador del mismo, dando tramitación a las denuncias recibidas para que se adopten las resoluciones que correspondan.

El tratamiento de las denuncias se realizará de conformidad con la normativa de protección de datos de carácter personal.

El canal de denuncias se constituye como un canal interno, independiente y con las garantías suficientes de confidencialidad y protección al denunciante frente a posibles represalias, discriminaciones y cualquier otro tipo de trato injusto.

El procedimiento no requiere la identificación del denunciante, si bien de producirse, el administrador del canal garantizará la confidencialidad, siempre que se obre de buena fe, a lo largo del proceso y, en particular, que el denunciado y, en su caso, sus superiores no puedan acceder a los datos identificativos del denunciante, salvo que ello fuera estrictamente necesario para la resolución del expediente.

El plazo de que dispondrá el Compliance Officer para resolver el procedimiento abierto será de 15 días naturales, a contar desde el día siguiente a que el administrador hubiera recibido la denuncia. En ese plazo de tiempo, el denunciante podrá informarse sobre el estado de su denuncia mediante el envío de un correo electrónico al administrador utilizando el número de referencia que figurará en el acuse de recibo inicial, que deberá resolverla en el plazo de 48 horas. El denunciante debe guardar confidencialidad sobre la información de que tenga conocimiento en el marco del procedimiento.

c) Sistema de Alertas

La Sociedad determinará un sistema de alertas mediante la aplicación de herramientas informáticas de conformidad con lo dispuesto en el artículo 16.

Artículo 9.- Comunicaciones externas al Organismo de Prevención

9.1- Comunicación de operaciones sospechosas

Una vez realizado el examen especial establecido en el artículo 5, y habiéndose determinado la concurrencia en la operativa de indicios o certeza de relación con el blanqueo de capitales o la financiación del terrorismo, se efectuará sin dilación la comunicación por indicio, usando , en su caso, el formulario que el Organismo de Prevención pueda tener habilitado a estos efectos.

Sin perjuicio de lo anterior, la Sociedad adoptará inmediatamente medidas adicionales de gestión y mitigación del riesgo, que deberán tomar en consideración el riesgo de revelación.

The communication of suspicious transactions will contain, in accordance with PBCFT regulations, the following information:

a) The relationship and identification of the natural or legal persons participating in the operation and the concept of their participation in it.

b) The known activity of the natural or legal persons participating in the operations and the correspondence between the activity and the operations carried out.

c) The list of the operations and dates to which they refer, indicating their nature, currency in which they are carried out, amount, place or places of execution, purpose and payment or collection instruments used.

d) The procedures carried out within the framework of the special examination regulated in this Manual.

e) Exposition of the circumstances of all kinds from which the indication or certainty of connection to "money laundering" can be inferred or that reveal the lack of economic, professional or business justification for carrying out the activities.

f) Information about the decision adopted or that will foreseeably be adopted regarding the continuation or interruption of the business relationship with the client or clients participating in the operation, as well as the justification for this decision.

Article 10.- Controls for the detection of the possible relationship of Clients with the financing of terrorism or PRP

a) EU List

The Company will consult the European Union list of sanctions and terrorist organizations and groups prior to the admission of a Client, in addition to the periodic cross-checking of said lists with existing Client databases when updates occur. This filter will be carried out by the Company Representative. This list (and modifications to it) can be found at the following internet addresses:

https://data.europa.eu/euodp/es/data/dataset/consolidated-list-of-persons-groups- and-entities-subject-to-eu-financial-sanctions/resource/3a1d5dd6-244e-4118- 82d3-db3be0554112

https://eeas.europa.eu/headquarters/headquartershomepage_en/8442/Consolidated%20list%20of%20sanctions

https://www.consilium.europa.eu/en/policies/fight-against-terrorism/terrorist- list/

El citado contraste se realizará con la siguiente periodicidad:

1. Posibles nuevos Clientes: antes de ser admitidos mediante el cotejo en las aplicaciones accesibles internamente.
2. Clientes ya admitidos: cada vez que se produzca una actualización de la lista o, en su caso, con carácter semestral por parte de la Sociedad.

El Representante dejará constancia por escrito del contraste. En caso de positivos con la lista de la Unión Europea no se admitirá a la persona como Cliente.

b) Control de PRP

La Sociedad verificará si sus Clientes responden a la definición de persona con responsabilidad pública mediante la declaración del Cliente, así como la consulta a registros de terceros. En caso de que el Cliente responda a la definición de persona de responsabilidad pública, aplicará las medidas pertinentes, de conformidad con los procedimientos descritos en este Manual.

TÍTULO II. DE LOS PROCEDIMIENTOS DE EVALUACIÓN

Artículo 11.- Análisis de riesgo

Los procedimientos de control interno de la Sociedad se fundamentarán en un previo análisis de riesgo realizado por la misma. En concreto, la Sociedad realizará un Informe de Autoevaluación de Riesgo de carácter eminentemente práctico adaptado a su actividad, en el que se identifica y evalúa su exposición al riesgo de blanqueo de capitales y financiación del terrorismo.

En concreto, en el mencionado informe de autoevaluación tendrá en cuenta los siguientes aspectos:

a) Datos básicos de la Sociedad.

b) Los canales utilizados para el ingreso, movimiento y transmisión de los fondos, con referencia al riesgo que suponen.

c) Tipologías de clientes, especificando los que puedan presentar un mayor riesgo en materia de prevención.

d) Actuaciones de los clientes que puedan suponer un mayor riesgo de blanqueo de capitales y financiación del terrorismo.

e) El propósito de la operación.

f) El nivel de activos del cliente, el volumen de las operaciones y la regularidad o duración de la relación de negocios.

g) Zonas geográficas de actividad de la Sociedad, especificando aquellas de mayor riesgo con o en las que opera el sujeto obligado.

El análisis de riesgo será revisado por el Compliance Officer con carácter anual y, en todo caso, cuando se verifique un cambio significativo en la actividad, volumen de negocios o estructura de la Sociedad que pudiera influir en su perfil de riesgo.

Artículo 12.- Informe de Experto Externo

Los procedimientos y órganos de control interno y de comunicación serán objeto de examen anual por un experto externo.

El informe del experto independiente deberá emitirse dentro de los dos meses siguientes a la fecha de referencia. En todo caso, en los dos años sucesivos a la emisión del informe éste podrá ser sustituido por un informe de seguimiento emitido por el experto externo, y referido exclusivamente a la adecuación de las medidas adoptadas por la Sociedad para solventar las deficiencias identificadas en su caso.

Los resultados del examen serán consignados en un informe escrito de carácter reservado que describirá detalladamente las medidas de control interno existentes, valorará su eficacia operativa y propondrá, en su caso, eventuales rectificaciones o mejoras. Este informe, que incluirá una descripción detallada de la trayectoria profesional del experto que lo redacta, estará a disposición del Organismo de Prevención durante los cinco años siguientes a la fecha de su emisión.

Las sugerencias de rectificación o mejora, así como las conclusiones más significativas del informe deberán ser puestas en conocimiento del órgano de administración en el plazo máximo de tres meses contados desde la fecha de emisión del mismo, con constancia en acta de la toma en consideración.

En caso de que existan deficiencias, el órgano de administración adoptará, sin dilación, medidas necesarias para solventar las deficiencias identificadas en los informes de experto externo. Y si las deficiencias no fuesen susceptibles de resolución inmediata, el órgano de administración adoptará, expresamente, un plan de remedio, que establecerá un calendario preciso para la implantación de las medidas correctoras que no podrá exceder, con carácter general, de un año natural.

No se podrá encomendar la práctica del examen externo a aquellas personas físicas que hayan prestado o presten cualquier otra clase de servicios retribuidos a la Sociedad durante los tres años anteriores o posteriores a la emisión del informe.

Todos los clientes pueden comprobar la vigencia de las supervisiones del Compliance Externo a través de los siguientes enlaces:

https://rapinformes.es/prevencion-blanqueo-capitales-financiacion-terrorismo/

https://rapinformes.es/compliance-penal/

Del mismo modo, existe un canal de comunicación directa con nuestro manager en Binance, Edgar Arellano Reyes, (edgar.r@binance.com), a quien se le puede consultar cualquier duda relacionada con la gestión de IAESIR.

Artículo 13.- Estándares éticos en la contratación de empleados, directivos y agentes

La Sociedad garantiza altos estándares éticos en la contratación de directivos, empleados o agentes. A estos efectos, se aplicarán a estos colectivos los criterios de idoneidad fijados por la normativa sectorial que les resulte de aplicación en cada momento. En defecto de normativa específica, para la determinación de la concurrencia de altos estándares éticos en directivos, empleados o agentes del sujeto obligado, se tomará en consideración su trayectoria profesional, valorándose la observancia y respeto a las leyes mercantiles u otras que regulen la actividad económica y la vida de los negocios, así como a las buenas prácticas del sector de actividad de que se trate.

En todo caso, no se considerará que concurren altos estándares éticos cuando el empleado, directivo o agente:

- ·Cuente con antecedentes penales no cancelados ni susceptibles de cancelación por delitos dolosos contra el patrimonio, y contra el orden socioeconómico, contra la Hacienda Pública y Seguridad Social, delitos contra la Administración Pública y falsedades;
- ·Haya sido sancionado mediante resolución administrativa firme con la suspensión o separación del cargo por infracción de la normativa de PBCFT. Esta circunstancia se apreciará durante el tiempo que se prolongue la sanción.

TÍTULO III. DE LA FORMACIÓN INTERNA EN MATERIA DE PREVENCIÓN DE CAPITALES

Artículo 14.- Formación

La entidad obligada adoptará las medidas oportunas para que su personal tenga un conocimiento adecuado de las exigencias derivadas de la normativa sobre prevención del blanqueo de capitales y la financiación del terrorismo.

En concreto los empleados recibirán un curso de formación al menos una vez al año, y a la finalización del mismo realizarán una prueba de conocimientos. Se comprobará la asistencia del personal.

La entidad obligada aprobará el plan anual, propuesto por el Compliance Officer, que deberá fundamentarse en los riesgos identificados y preverá las acciones formativas específicas para los directivos, empleados y agentes, incluyendo asimismo las acciones formativas a este respecto.

Anualmente deberá documentarse el grado de cumplimiento del plan de formación.

Asimismo, el presente Manual se encontrará siempre disponible para todos los empleados, y en caso de que el mismo sea modificado o actualizado, se informará por correo electrónico de dicho cambio o actualización.

TÍTULO IV. DE LA EXENCIÓN DE RESPONSABILIDAD

Artículo 15.- Exención de Responsabilidad

La comunicación de buena fe de las informaciones derivadas del presente Manual por parte de los empleados al Compliance Officer o, en su caso, directamente al Organismo de Prevención, no constituirá para éstos violación de las restricciones sobre revelación de información impuestas por vía contractual o por cualquier disposición legal o reglamentaria y no implicará ningún tipo de responsabilidad.

TÍTULO V. HERRAMIENTAS INFORMÁTICAS

Artículo 16.- Herramientas Informáticas

Dado el volumen de la cartera de Clientes, para la identificación de operaciones, la Sociedad se apoyará en las aplicaciones como son Excel y Access, utilizando sus bases de datos, explotándolas con herramientas informáticas (Office).

Adicionalmente, la Sociedad verificará, los nombres y números de documentos de identificación de los Clientes, así como el importe de las transacciones con objeto de evitar posibles fraccionamientos de operaciones que debieran ser comunicadas en la comunicación mensual obligatoria.

En caso de que el volumen de la cartera de Clientes haga necesario la utilización de medios electrónicos para la extracción de operaciones, la Sociedad se proveerá de dichos medios.

Asimismo, se configurarán las herramientas informáticas de manera que se generen alertas centralizadas cada vez que se hayan recibido fondos de Clientes:

a) Por cuantía superior a 10.000 euros.
b) Residentes en países, territorios o jurisdicciones recogidas en el Anexo I del Manual.
c) Que reúnan la condición de PRP.

El destinatario de estas alertas será el Compliance Officer, que deberán llevar a cabo un examen especial de dichas operaciones.

Para ello, las herramientas informáticas contarán con los siguientes recursos y medidas:

- Ficha de cliente: Cada cliente posee una ficha personalizada dentro del sistema informático en la que se puedan consultar.

- Todos los datos personales del cliente.
- Los documentos relacionados con el cliente.
- Detalle de las operaciones realizadas con la Sociedad.
- Campos obligatorios: Herramienta destinada a impedir que se proceda al alta del cliente o de la operación cuando todos los datos del cliente o de la operación no constan completos.

- Paraísos fiscales y territorios no cooperantes: El sistema informático detecta la presencia (ya sea por razones de nacionalidad, residencia, destino u origen de los fondos) de jurisdicciones de riesgo. En estos supuestos se activará una alerta que advertirá de la necesidad de que se adopten las medidas previstas.

- Personas sujetas a prohibición de operar: El sistema informático detecta la coincidencia de los datos del remitente y beneficiario con los contenidos en las listas OFAC, de la Unión Europea y de la ONU de personas o entidades sujetas a prohibición de operar y, en tal caso, bloquea de forma automática la ejecución de la operación.

- Actividad: En el supuesto de que, al introducir en la Ficha de Cliente la actividad profesional o empresarial, se indicase alguna de las consideradas como actividades de riesgo, de conformidad con la

Política de Admisión de Clientes o el Catálogo de Operaciones de Riesgo, se activará una alerta que advertirá de la necesidad de recabar la documentación adicional al poseer el cliente un perfil de riesgo.

Así mismo, las herramientas informáticas tendrán las siguientes prestaciones:

- Configura una lista negra de usuarios conflictivos.
- Avisa de los movimientos o transferencias emitidas u ordenadas desde países o territorios considerados de riesgo en tiempo real.
- Detecta provisiones de fondos efectuadas por terceros distintos al titular de la cuenta. Solicitudes de reembolso a cuentas de terceros distintos al titular de la cuenta.
- Detecta estructuraciones, transacciones de elevadas cuantías, cuentas inactivas, transacciones interconectadas realizadas por diferentes intervinientes, a monedas mejoradas con anonimato, operaciones relacionadas con mercados opacos, servicios de mezcladores, etc).
- Detecta nombres de dominio de Internet a través de proxies o que utilizan registradores de nombres de dominio (DNS) que suprimen o redactan a los propietarios de los nombres de dominio.
- Detecta dirección IP asociada con una red oscura u otro software similar que permite la comunicación anónima, incluyendo correos electrónicos cifrados y VPN.

TÍTULO VI. COLABORACIÓN CON EL SEPBLAC U OTRAS AUTORIDADES

Artículo 17.- Colaboración con el Organismo de Prevención u otras Autoridades

Los requerimientos que puedan formular el Organismo de Prevención u otras Autoridades a la Sociedad serán atendidos por el Compliance Officer, quien elaborará con toda claridad las respuestas a los mismos en el plazo establecido por las citadas Autoridades.

Transcurrido el plazo para la remisión de la documentación o información requerida sin que ésta haya sido aportada o cuando se aporte de forma incompleta por omisión de datos que impidan examinar la situación en debida forma, se entenderá incumplida la obligación establecida en el presente artículo.

En este sentido, la Sociedad establecerá, en el marco de las medidas de control interno, sistemas que les permitan responder de forma completa y diligente a las solicitudes de información que les Organismo de Prevención u otras autoridades legalmente competentes sobre si mantienen o han mantenido a lo largo de los diez años anteriores relaciones de negocios con determinadas personas físicas o jurídicas y sobre la naturaleza de dichas relaciones.

TÍTULO VII. REVISIÓN DE LOS PROCEDIMIENTOS Y MEDIDAS DE CONTROL INTERNO

Artículo 18.- Revisión de Procedimientos

El Compliance Officer será el encargado de revisar, con una frecuencia anual, la eficacia de los procedimientos y de medidas de control interno destinadas a la prevención de blanqueo de capitales y de la financiación del terrorismo, con vistas a comprobar el adecuado cumplimiento de los mismos, recomendando, en su caso, la elaboración de procedimientos no existentes, así como la mejora o implantación de nuevos controles para la detección de operaciones susceptibles de blanqueo de capitales.

En su caso, la eficacia de los procedimientos podrá evaluarse mediante análisis de muestras obtenidas de las operaciones realizadas. Quedará constancia por escrito de los resultados de la revisión, de la información comunicada al órgano de administración sobre dichos resultados y de las mejoras propuestas.

Todos los manuales, así como la información, archivos o soportes relacionados en los mismos, serán de acceso permitido a los clientes que lo soliciten mediante los canales de comunicación establecidos para ello.