RIESGOS DE FRAUDE Y CRIMINALIDAD

ASOCIADOS AL MUNDO DE LAS APUESTAS.

MEDIDA 4.1.3 – Actualizar los análisis existentes sobre riesgos de fraude y criminalidad asociados al mundo de las apuestas.
Objetivo
Actualizar los riesgos de fraude y criminalidad asociados a las apuestas, a partir del análisis de riesgos de fraude en los juegos de ámbito estatal elaborado de conformidad con las directrices del Consejo de Políticas de juego de 12 de septiembre de 2017.
Justificación
La enorme evolución del mercado de apuestas también ha llevado aparejada una transformación de los riesgos asociados a este segmento de los juegos de azar, como se han encargado de señalar, desde muy diversas perspectivas, distintos estudios[1]. El Consejo de Políticas del Juego aprobó, el 12 de septiembre de 2017, dentro del Programa de actuaciones de los Grupos de Trabajo para 2017 y 2018, la realización de un análisis del fraude en la actividad de juego. Para abordar esta tarea, el 12 de enero de 2018 se constituyó un Grupo de trabajo conformado por representantes de la Dirección General de Policía Nacional, la Dirección General de Ordenación del Juego y de varias comunidades autónomas. El análisis realizado, fundado en la norma ISO 31000 es completo y abarca todas las modalidades de fraude existentes en los mercados de juego de ámbito estatal y autonómico. Resulta de interés especificar dicho análisis exclusivamente para el mercado de las apuestas, con vistas a conocer de un modo más concreto su naturaleza y su entorno.
Ejecución
La Dirección General de Ordenación del Juego, a través de los datos del Sistema de Control Interno y de los que recabe de manera directa de los operadores de juego de ámbito estatal, elaborará un informe sobre los mercados de apuestas de ámbito estatal que presentará al Pleno de la Comisión para su toma en conocimiento en el último trimestre de 2020.

[1] Entre otros, the French Institute for International and Strategic Affairs (2017). Preventing criminal risks linked to the sports betting market: final report; Asser Institute (2015). The odds of Match Fixing.

CORREO ELECTRÓNICO:
dgoj.dgeneral@hacienda.gob.es

C/ ATOCHA, 3
28071 MADRID
TEL: +34 91 571 40 80
FAX: +34 91 571 17 36

1 Índice

2 Contexto

Las administraciones públicas deben velar por garantizar la protección de los usuarios del juego, de los menores y de las personas con problemas con el juego y la prevención de las conductas adictivas, así como otorgar seguridad jurídica a operadores y jugadores, prevenir y colaborar en la persecución de las actividades ilícitas y garantizar el respeto de la regulación.

En nuestros días el sector del juego se ha convertido en una compleja industria en la que convergen aspectos tan amplios como el ocio, las transacciones económicas o la aleatoriedad en un entorno tecnológico en continua evolución y en el que surgen nuevos riesgos que es necesario conocer para poder adoptar las medidas adecuadas.

Existe un amplio espectro de riesgos que pueden materializarse en el desarrollo de actividades de juego y en una primera aproximación se podría diferenciar en riegos de carácter tecnológico, riesgos procedimentales o bien riesgos propios de naturaleza del juego. Los riegos de carácter tecnológico pueden a su vez dividirse en función de su impacto, atendiendo a si la materialización de estos riesgos supone un problema para la integridad de la información, la confidencialidad, la autenticación o la disponibilidad de la información o los servicios. En lo que respecta a los procedimientos de los operadores, tenemos los riegos asociados al proceso de acreditación de identidad, los riesgos de carácter económico, como el blanqueo de capitales, y los riesgos en el uso fraudulento de medios de pago. Por último, en relación con los juegos, el análisis podría hacerse según el tipo de juego (juegos de cartas, bingos, máquinas de azar, recreativas de juego con premio o apuestas) o bien según el canal de venta, presencial, online o escenarios mixtos.

El análisis de los principales riesgos subyacentes a la actividad del juego facilita la identificación de aquellos **escenarios** que puedan suponer una merma en la protección de los derechos de los jugadores, de los operadores, de la sociedad en su conjunto y en definitiva de los objetivos de regulación, de cara a adoptar posibles medidas administrativas y regulatorias.

Para ello siguiendo el marco de referencia de ISO 31000, la DGOJ realizó un análisis y evaluación de riesgos basado en el posible **impacto** que una materialización de éstos podría tener en los objetivos de la regulación y en la **probabilidad** de ocurrencia del riesgo para cada uno de los escenarios definidos.

El análisis debe partir de los objetivos de la regulación de la actividad de juego, para posteriormente identificar los riesgos subyacentes a esta actividad y las causas que los provocan.

3 Objetivos

Los objetivos de la Ley 13/2011, de 27 de mayo, de regulación del juego (Ley 13/2011) son garantizar la protección de los usuarios del juego, de los menores y de las personas con problemas con el juego y la prevención de las conductas adictivas, otorgar seguridad jurídica a operadores y jugadores, así como prevenir y colaborar en la persecución de las actividades ilícitas.

Dentro de cada uno de los objetivos, es posible concretar determinadas áreas de acción prioritarias.

- **Prevenir las conductas adictivas.**
    - Establecer mecanismos para promover un juego seguro y responsable.
- **Proteger los derechos de los menores.**
    - Establecer las medidas que impidan el acceso al juego por parte de menores.
- **Protección del orden público y lucha contra el fraude.**
    - Prevenir, detectar y perseguir actividades delictivas como el blanqueo de capitales por empresas de juego o bien a través de empresas de juego.
    - Prevenir, detectar y perseguir el amaño en el deporte que en muchas ocasiones es posible por medio de la extorsión y vinculado a organizaciones criminales.
    - Prevenir, detectar y perseguir actividades fraudulentas como la suplantación de identidad, el fraude en tarjetas de crédito, el uso en el juego de dinero robado.
- **Salvaguarda de los derechos de los participantes en los juegos.**
    - Promover un juego justo y honesto, estableciendo mecanismos para evitar actividades fraudulentas en el juego como la colusión.
    - Proporcionar seguridad jurídica para el jugador, así como la protección de sus fondos depositados y de sus datos personales.
    - Perseguir el juego ilegal.
- **Entorno de seguridad jurídica para los operadores.**
    - Concretar adicionalmente las condiciones de cumplimiento y diligencia de los operadores.

La lucha contra el fraude constituye uno de los fundamentos de la Ley 13/2011 y en consecuencia del establecimiento de un marco regulado para la actividad de juego de ámbito estatal ofrecida mediante la correspondiente licencia. En este sentido, el establecimiento de sistemas y mecanismos para la prevención del fraude y del blanqueo de capitales es una obligación expresamente contenida en el título habilitante para ofrecer actividades de juego de ámbito estatal, en concreto en las distintas licencias generales de las que son titulares los operadores[2].

Una correcta gestión de riesgos de fraude en el juego parte de una adecuada identificación inicial de los riesgos a los que el operador está expuesto. La evaluación de los riesgos de fraude debe tener por resultado el establecimiento de medidas sistemáticas de prevención que los eviten y de detección que permitan descubrir los casos de fraude que se produzcan, así como la determinación de las acciones correctivas para ayudar a asegurar que un potencial fraude se aborde de forma adecuada y oportuna. Por último, toda la tarea de gestión del fraude debe medirse y documentarse a través de los informes de evaluación.

[2] El apartado cuarto de los Términos y condiciones de la licencia general establece que "*El titular de la licencia general dispondrá los sistemas y mecanismos para evitar y prevenir el fraude y el blanqueo de capitales en los términos establecidos en el Manual de prevención del fraude, en el Plan Operativo y en el Proyecto de los sistemas técnicos de juego aportados junto a su solicitud de licencia, así como en el manual de procedimiento de prevención presentado junto a la solicitud de licencia y modificado de acuerdo con las observaciones puestas de manifiesto por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales; y siempre sin perjuicio del cumplimiento de las instrucciones que a estos efectos pudieran ser dictadas por la Dirección General de Ordenación del Juego, el referido Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias y demás organismos competentes.*"

La experiencia adquirida con el desarrollo de las actividades de juego en un entorno regulado y controlado desde 2012 ha permitido conocer y tomar conciencia de la existencia de diversos tipos de fraude que pueden producirse en las plataformas de juego. Por este motivo, con el propósito de establecer las bases de lo que la DGOJ entiende por gestión diligente de dicho fraude, y sin perjuicio de las especificidades aplicables dentro de cada organización, este centro directivo publicó en diciembre de 2018 una "*Nota técnica sobre la gestión del fraude en operadores de juego*" en la que se analizaban los principales tipos de fraude identificados susceptibles de producirse en un operador de juego, las medidas estructurales de prevención y detección ya establecidas en la regulación, incluidas las previstas en las instrucciones de la DGOJ, los escenarios de riesgo cualificado que deben tenerse en cuenta para la protección de los derechos de los jugadores con especial atención a los colectivos vulnerables, así como las posibles acciones a realizar para la gestión de las alertas según los casos.

Este documento es una actualización del mencionado documento tras el análisis y evaluación que de los riesgos en él comprendidos se ha realizado siguiendo el marco de referencia de ISO 31000 y a la luz de la experiencia en el estudio de la información de usuarios y de transacciones de juego aportada por los operadores, la gestión de los expedientes de comprobación y las actuaciones de colaboración con las fuerzas de seguridad del estado.

4 Identificación de riesgos de fraude

Una vez concretados los objetivos de la regulación de la actividad de juego, es necesario identificar los riesgos subyacentes a esta actividad y las causas que los provocan. A continuación, se presenta la relación de riesgos identificados en el análisis, clasificados en tres grupos según se pongan de manifiesto en el usuario, en las transacciones o en el tipo de producto.

4.1 Riesgos de usuario

4.1.1 Ocultación de la identidad real de los jugadores (fraude de identidad)

Consideramos fraude en los datos de identidad aquellas prácticas consistentes en:

a) Intentos de registro con los datos de identidad propios, pero alterando alguno de los datos, normalmente la edad.

Este tipo de engaño en los datos de identidad puede tener como fin eludir los controles de acceso de menores establecidos por la DGOJ y los operadores. Cualquier alteración de los datos de identidad - DNI/NIE, nombre, apellidos o edad - es automáticamente detectada por el servicio de verificación de identidad del jugador ofrecido por la DGOJ y comunicada al operador para que se bloquee el proceso de alta.

b) Intentos de registro con los datos de identidad propios, pero usando varios documentos de identidad con los mismos datos - DNI, NIE, pasaporte, número de la seguridad social – con el fin de crear varias cuentas de juego en el mismo operador.

   Incluso, en el caso de residentes, uso de documentos diferentes al DNI/NIE para evitar el control del RGIAJ.

c) Alta de registro de usuario con datos de terceros o cesión de uso de un registro de usuario verificado.

El engaño en los datos de identidad puede tener como fin eludir los controles de acceso o de juego establecidos por los operadores y responder a diferentes motivaciones. A modo de ejemplo se incluyen algunas de estas motivaciones:

- ✓ Personas que intentan acceder al juego teniéndolo **prohibido** en virtud de lo establecido en el artículo 6.2) de la Ley 13/2011, tales como menores, personas con problemas en el juego que se han inscrito en el RGIAJ o que se han autoexcluido en el operador, personas vinculadas al operador o personas vinculadas al deporte.
- ✓ Personas que, como consecuencia del **amaño** de un evento deportivo, tienen conocimiento, directo o indirecto, de su futuro resultado y utilizan las apuestas para obtener una ganancia.
- ✓ Jugadores que actúan de forma coordinada en juegos de círculo, para obtener una ventaja adicional sobre el resto de los jugadores o para introducir **fondos de origen ilícito** y traspasarlos a una cuenta de juego verificada.
- ✓ Jugadores que buscan la **elusión fiscal** en el Impuesto sobre la Renta de las ganancias obtenidas en el juego.
- ✓ Personas previamente bloqueadas por el operador en aplicación de sus políticas de prevención del fraude.
- ✓ Jugadores que intentan distribuir el volumen total de las apuestas realizadas entre varias identidades, para evitar la atención del operador sobre un único apostante.
- ✓ Jugadores que consideran tener especial habilidad en las apuestas y “comparten” ese conocimiento con terceros que, además les ceden la gestión de la cuenta de juego, a cambio de una contraprestación.
- ✓ Jugadores que desean realizar apuestas por encima del nivel aceptado por el operador y usan varias cuentas para eludir los controles.
- ✓ Jugadores que buscan aprovechar varias veces las ventajas de los bonos de bienvenida ofrecidos por los operadores a los nuevos clientes.

En estos casos, el uso de datos de terceros puede ser consentido o no consentido.

Hablamos de suplantación de identidad consentida cuando es conocida y no denunciada. Puede producirse en el entorno familiar o de amigos o, bien con terceros que ceden los datos de identidad a cambio de una contraprestación que puede ser recibida una única vez - venta de los datos de identidad, incluido algún medio de pago, o venta de la cuenta de juego - o de forma periódica siguiendo un modelo de “alquiler de cuenta de juego”. En este último modelo, el arrendador de la cuenta corrobora la autenticidad de ésta ante los diferentes controles

del operador (llamadas de comprobación, prueba de vida, etc.) o del banco en una cesión de uso también de los medios de pago asociados al registro.

Hablamos de suplantación de identidad no consentida cuando no es conocida por el titular de los datos de identidad. En estos casos los medios de pago usados pueden ser anónimos o no haciendo uso de tarjetas de terceros. Dentro de este grupo se incluye el uso de identidades de personas fallecidas[3].

4.1.2 Ocultación de la localización (fraude de geolocalización)

Denominamos fraude de geolocalización, en el contexto de la actividad de juego online al uso de redes privadas virtuales (VPNs) o de proxy para ocultar la dirección IP del dispositivo con intención de ocultar la localización del jugador. La finalidad de estas prácticas puede ser variada:

- Personas que ocultan su localización en España para saltarse los controles de identidad establecidos por el operador en la plataforma ".es" por alguno de los motivos ya descritos en el punto anterior.
- Personas que intentan eludir los controles de trazabilidad de las transacciones por motivos fiscales.
- El jugador reside en jurisdicciones de alto riesgo o de no confianza del GAFI/UE por lo que intenta ocultarlo.

Estas prácticas pueden afectar a los operadores de juego que, directamente o a través de sus matrices o filiales, operan en otras jurisdicciones.

4.2 Riesgo de transacciones

4.2.1 Fraude en los medios de pago

Denominamos fraude en los medios de pago al uso por un jugador de un medio de pago, principalmente tarjetas, a nombre de otra persona. Este tipo de fraude puede ser consentido o no consentido.

Hablamos de fraude en medios de pago consentido cuando es conocido por el titular del medio de pago. En ocasiones, el uso de una tarjeta de otra persona se acompaña de un posterior repudio de las transacciones realizadas. Puede ir asociado al uso de la identidad del titular de la tarjeta.

[3] Desde noviembre de 2018 la DGOJ proporciona a los operadores de juego información sobre los registros de usuario cuyos datos de identidad se corresponden con los de personas fallecidas según consta en la sección de personas difuntas del Registro Civil. Esta información permite al operador impedir el alta de nuevos registros con datos de identidad correspondientes a una persona fallecida y, en relación con su base de datos histórica de usuarios, le permite adoptar las medidas que resulten oportunas de conformidad con lo dispuesto en el artículo 33.2 y/o 35.3 del Real Decreto 1614/2011, de 14 de noviembre, por el que se desarrolla la Ley 13/2011, de 27 de mayo, de regulación del juego, en lo relativo a licencias, autorizaciones y registros del juego, sin perjuicio de las restantes disposiciones que en materia de derecho civil resulten de aplicación.

Hablamos de fraude en medios de pago no consentido cuando no es conocido por el titular de los datos de identidad. Normalmente es denunciado ante la policía en el momento en que el titular tiene conocimiento del uso indebido de la tarjeta.

4.2.2 Fraude en el origen de fondos

Denominamos fraude en el origen de fondos al uso por un jugador de dinero robado, de dinero que el usuario no está autorizado a disponer o utilizar a tal efecto, o de dinero cuyo origen no puede justificar.

El uso en las plataformas de juego de fondos con un origen ilícito puede estar relacionado con un problema en el juego que lleva al jugador a no poder financiar con sus recursos propios su nivel de gasto en juego, o bien, con un intento por parte del jugador de utilizar la plataforma de juego para desviar dichos fondos hacia cuentas de juego verificadas, pudiendo tratarse de una práctica relacionada con el blanqueo de capitales.

El blanqueo de capitales en el sector del juego generalmente se ha presentado desde tres perspectivas diferentes:

1. Transferencia de fondos a través de la plataforma de juego, realizando depósitos y retiradas en las cuentas de juego con el fin de obtener un justificante de cobro de premios con apariencia legítima.
2. Traspaso de fondos entre diferentes jugadores, realizando depósitos procedentes de actividades delictivas para luego perderlos en juegos de círculo[4] ante quienes, en apariencia, los han obtenido de forma legítima, pudiendo proceder así a su retirada.
3. Utilización de fondos procedentes de actividades delictivas para utilizar en el juego como actividad lúdica.

4.3 Riesgo de producto

Los juegos se pueden clasificar en cuatro categorías diferentes.

a) Juegos en los que es posible realizar jugadas de bajo riesgo en juegos de probabilidades fijas con cobertura (ruleta, punto y banca, apuestas). Una jugada de bajo riesgo es aquella con bajas, incluso mínimas, ganancias, pero con poca probabilidad de pérdida.
    a. En la ruleta hacer una apuesta en rojo y negro -o par e impar- al mismo tiempo, operación también conocida como “cubrir la mesa”.
    b. En punto y banca hacer una apuesta en el banquero y el jugador al mismo tiempo.
    c. En apuestas la técnica conocida como arbitraje. Se trata de apuestas a cuota 1,01, incluso con opción de recompra, en uno o en varios operadores.
b) Juegos en los que no es posible colocar apuestas de bajo riesgo, como slots, loterías o bingo. Se trata de juegos de probabilidades fijas sin posible cobertura. En los juegos de azar puro no es posible realizar

[4] Se conoce como juegos de círculo a aquellos como el póquer o el punto y banca en los que un grupo reducido de jugadores constituyen un fondo o bote para el premio y se enfrentan entre sí para ganar dicho premio.

apuestas de bajo riesgo porque no se puede "cubrir" el resultado con otra apuesta. Por ejemplo, en las máquinas de azar, cada tirada permite una sola apuesta y el resultado de esta apuesta no puede ser cubierto por otra apuesta.

c) Juegos de círculo, como el póquer o el punto y banca, en los que es posible la colusión entre jugadores. para obtener un beneficio en perjuicio de un tercero, trasladar ganancias en el juego a otras cuentas por motivos de elusión tributaria o trasladar fondos ilícitos hacia cuentas verificadas que permitan la retirada.
d) Las apuestas, en sus modalidades de contrapartida y cruzadas, constituyen una categoría específica por su posible vinculación con eventos o competiciones deportivas adulteradas o con el uso de información privilegiada. Denominamos fraude en apuestas vinculado a amaños de eventos deportivos a la utilización de las apuestas para obtener un beneficio teniendo conocimiento de que un determinado hecho o evento deportivo ha sido previamente amañado.

   La amenaza de las apuestas fraudulentas por estar vinculadas a un amaño en un evento deportivo es una cuestión compleja de analizar y que tiene carácter trasnacional, pudiendo afectar a cualquier deporte y competición deportiva, y realizándose las apuestas fraudulentas en operadores de apuestas pertenecientes a cualquier jurisdicción.

   La complejidad del entorno que rodea las apuestas deportivas requiere un esfuerzo continuo y conjunto de todas las partes interesadas para identificar las vulnerabilidades, realizar acciones preventivas y disuasorias y establecer mecanismos de detección y persecución, con el objetivo de evitar que se comprometa la integridad en el deporte y que, en caso de producirse, permita la identificación de los involucrados.

5 La gestión del riesgo de fraude

La gestión de los riesgos de fraude en la actividad de juego requiere que el operador implante un sistema de gestión de cumplimiento normativo y principios de buen gobierno.

El operador de juego debe implantar un sistema de gestión de riesgos de fraude en el juego basado en la definición, gestión y mantenimiento de una matriz de riesgos de fraude que responda y se adapte a su modelo de negocio y sus particularidades. Esto implica una descripción de la operativa con la evaluación del riesgo inherente a ella, las medidas de control y el riesgo residual que resulta después de aplicar las medidas, que debe ser mínimo.

El operador debe implantar procedimientos de control interno que incluyan la monitorización activa de sus jugadores, que le permita tener un primer análisis de datos de éstos y que constituya el punto de partida para posteriores análisis de riesgos. Este proceso, también conocido como Know Your Costumer (KYC), debe estar integrado y retroalimentarse de los procesos de diligencia debida establecidos por el operador en materia de normativa

antifraude, blanqueo de capitales y financiación del terrorismo, la prevención de amaños en eventos deportivos, así como los procesos que incluyan interacciones con los jugadores como son la gestión de reclamaciones e incidencias.

Junto a ello deben existir programas de formación en materia de fraude en el juego para el conjunto del personal interno, prestando especial atención al personal que compone el centro de atención al usuario o el servicio de atención al cliente, los gestores personales de cuentas de cliente y en general cualquier servicio que tenga relación directa con los clientes.

Asimismo, se deben definir los protocolos de examen especial de determinadas operaciones y de comunicación con organismos oficiales competentes según la materia:

- En el caso de sospechas o indicios de fraude por blanqueo de capitales, los operadores tienen la obligación de comunicarlos al Servicio ejecutivo de prevención del blanqueo de capitales -SEPBLAC - (http://www.sepblac.es/).
- En el caso de otro tipo de fraudes que podrían derivar en delitos, los operadores tienen la obligación de comunicarlo a la Dirección General de Policía/ Dirección General de Guardia Civil.

Todo ello sin perjuicio de las obligaciones de comunicación con la DGOJ.

6 Algunos escenarios e indicadores y medidas

Se incluyen a continuación, clasificados según las áreas de riesgo analizadas, algunos escenarios de riesgo detectados en la operativa de juego. Se recogen algunos tipos de operaciones e indicadores que muestran un riesgo potencial de vinculación a actividades de fraude a partir de la experiencia acumulada por la DGOJ. Aunque en ningún caso se trata de una enumeración de todos los casos posibles, deben ser tenidos en cuenta por los operadores a la hora de elaborar su propia relación de operaciones de riesgo dentro del proceso interno de análisis y gestión de riesgos.

6.1 Riesgo de usuario

Escenarios de riesgo en la fase de verificación de identidad: grupos vulnerables

1. Intento de alta de registro usando los datos de identidad o de conexión - nombre y apellidos, domicilio, número de teléfono, correo electrónico, dirección IP, identificación de dispositivo u otros - coincidentes con

los de un intento fallido de registro de un menor, con los de una persona inscrita en el RGIAJ o autoexcluida en el operador.

2. Intento de alta de registro usando los datos de identidad de personas fallecidas.

Escenarios de riesgo en la fase de verificación de identidad: cuentas duplicadas

3. Existe una cuenta activa asociada a los mismos datos de identidad - DNI/NIE, nombre, apellidos y edad -.
4. Existen varios registros de usuario con coincidencia en datos de identidad - nombre, apellidos y edad - pero diferente documento correspondientes a personas que se dan de alta varias veces en un mismo operador usando su DNI, NIE y/o pasaporte.
5. Se aprecian relaciones con otras cuentas, tales como mismo teléfono, misma IP, mismo correo electrónico, mismo domicilio.
6. Dirección postal compartida por varias personas y esa dirección corresponde también con la de una empresa.

Escenarios de riesgo en el seguimiento

7. El documento de identidad aportado por el jugador ha caducado.
8. Se producen cambios en los datos de identidad aportados: dirección, medio de pago, origen geográfico de las transacciones.
9. El cliente no aporta los datos y justificantes solicitados.

Escenarios de riesgo en la localización del jugador

10. Varias conexiones simultáneas o consecutivas desde IP diferentes con múltiples localizaciones, especialmente si están geográficamente distanciadas.
11. Uso de la misma IP y/o dispositivo por varios usuarios.
12. El usuario utiliza herramientas tecnológicas para camuflar u ocultar su origen geográfico o su localización; por ejemplo, accede desde direccionamiento IP asignado a servicios en la nube - hosting de equipos, redes privadas virtuales, servicios proxy o similares -.

Escenarios de riesgo en el tipo de jugador

13. El nivel de gasto se sitúa muy por encima de la capacidad económica acreditada por el jugador.
14. La profesión o área de responsabilidad del usuario le permite acceso al dinero de otras personas o entidades.
15. El usuario es una persona con responsabilidad pública.
16. El usuario reside en/tiene nacionalidad de jurisdicciones de alto riesgo o de no confianza del GAFI/UE o no ha sido posible identificar su residencia/nacionalidad.

17. No coincide el país de residencia, el del medio de pago y la localización del cliente: por ejemplo, la IP indica que el cliente se conecta desde Afganistán.
18. El usuario gestiona la cuenta de una o varias personas, con o sin conocimiento de éstas[5].
19. En las comunicaciones con el operador se aprecian circunstancias anómalas.

6.2 Riesgo de medios de pago

1. Utilización de medios de pago anónimos, tales como tarjetas prepago o medios de pago eWallet[6] que no permitan la trazabilidad de las transacciones.
2. Utilización de métodos de pago de los que el usuario no es el titular.
3. Utilización de tarjetas de crédito corporativas.
4. Combinación de múltiples medios de pago.
5. El país del medio de pago no coincide con el del usuario que realiza la transacción.
6. El origen o destino de los fondos es una zona geográfica de alto riesgo o lugares no confiables, en base a las listas de países publicadas por organismos como el GAFI[7] o la propia Unión Europea.
7. Realización de transacciones de retirada de efectivo en locales presenciales de juego con el consiguiente traslado a éstos del riesgo, que dependerá entonces de los controles de identidad y origen de fondos que el local realice.

6.3 Riesgo de transacciones

Existen operaciones que, por su volumen, su frecuencia o por los antecedentes conocidos en la forma de operar del cliente resultan anómalas y, por tanto, requieren un examen especial. Algunos ejemplos de estas posibles conductas son los siguientes:

1. Patrones de depósito/juego/retiradas anómalos por su frecuencia o por su volumen. En todos los casos el objetivo perseguido puede incluir la solicitud de obtención de un certificado u otro medio de prueba de ingresos con apariencia legal.
    a. Muchos depósitos de la misma cantidad en un breve espacio de tiempo y usando múltiples medios de pago.

[5] Se han detectado casos de uso de identidades obtenidas mediante la lectura de la documentación en buzones dentro de los portales, encuestas en calle o ingeniería social.

[6] El uso de monederos electrónicos (eWallet) permiten al usuario trasladar fondos fácilmente entre cuentas bancarias, tarjetas de débito o de crédito. Son métodos, en general, difíciles de trazar y pueden ofrecer cierto nivel de anonimato.

[7] GAFI: Grupo de Acción Financiera Internacional. Publica una lista de países no cooperantes y jurisdicciones de alto riesgo: https://www.uiaf.gov.co/asuntos_internacionales/lista_paises_no_cooperantes_29282

b. Simulación de actividad de juego: el usuario deposita dinero en la plataforma de juegos y lo retira sin jugar o jugando solo con una cantidad mínima. Esta simulación de juego puede ser realizada por un jugador o por varios actuando de forma coordinada.
c. El jugador solo realiza apuestas de bajo riesgo y en volumen que no justifica los movimientos de depósito y retirada.
d. El jugador utiliza el importe depositado en una única apuesta o jugada de bajo riesgo, para luego retirar el importe del premio y comenzar de nuevo.

2. Cambios drásticos en la realización de apuestas, que sugieren que la cuenta ha pasado a ser usada por otra identidad.
3. Cuentas inactivas que de repente se activan con conductas anómalas: cambio de datos de correo o de teléfono, cambio de contraseña de acceso, cambio en el medio de pago.
4. Número elevado de transacciones de depósito o de retirada en un espacio corto de tiempo, individualmente por debajo del umbral de 2.000€, pero por encima en conjunto.
5. Transacciones por importes elevados, en base a umbrales predefinidos en las reglas de determinación de riesgos, tanto por importe como por número de operaciones.

6.4 Riesgo de producto

Fraude vinculado al póquer

Puesto que el póquer es un juego de cartas en el que un grupo reducido de jugadores se enfrentan entre sí para ganar un fondo del juego o bote previamente constituido entre ellos, es posible que se produzca colusión entre los jugadores. Hasta ahora se han detectado tres tipos de casos de colusión:

- Colusión entre varios participantes para obtener premios perjudicando a un tercero.
- Colusión para trasladar las ganancias obtenidas a otra cuenta por motivos de elusión tributaria.
- Colusión para trasladar fondos ilícitos hacia cuentas verificadas que permitan la retirada. Se han observado casos en los que múltiples jugadores realizan depósitos con tarjetas robadas por debajo del umbral de los 150 euros de depósito que exige la verificación documental, perdiendo todo lo depositado en favor de una única cuenta que sí ha sido verificada, pero con documentos falseados.

En un entorno de liquidez internacional se dificulta la detección de estas prácticas al repartirse los roles entre jugadores de diferentes jurisdicciones.

Fraude vinculado a amaños de eventos deportivos

Relacionadas con las apuestas también existen algunas operaciones que resultan anómalas por lo que es necesario monitorizar las apuestas para poder detectar estas anomalías y posteriormente analizarlas. Una anomalía no constituye por sí misma una evidencia de fraude en un determinado evento, aunque sí puede ser una alerta sobre

apuestas irregulares o sospechosas. El análisis de las alertas relativas a amaños de eventos deportivos debe incorporar una graduación de éstas, basada en la confluencia de indicios.

Las acciones de detección también han de contemplar lo descrito en los apartados de fraude de identidad y medios de pago, ya que es práctica habitual para la realización de apuestas vinculadas a amaños la utilización de múltiples identidades falsas, saltándose así los controles del operador y disimulando los beneficios.

Las alertas detectadas por el sistema de monitorización de las apuestas una vez analizadas deberán ser comunicadas a la DGOJ, que gestiona el sistema nacional de alertas. En el marco de la política de gestión de riesgos de fraude relativo a amaños, el operador ha de definir los supuestos en los que generará una alerta que será objeto de análisis y de reporte a través de la plataforma SIGMA Share[8].

Algunos ejemplos de estas posibles conductas son los siguientes:

Análisis del registro de usuario

1. Altas de registros de usuario coincidentes con las personas que tienen prohibido el acceso al juego en virtud de lo establecido en el artículo 6.2) de la Ley 13/2011, y en particular personas vinculadas al operador o personas vinculadas al deporte que el operador conozca.

Análisis de la forma de juego

Detección de determinados comportamientos relacionados con las apuestas y las cuentas del jugador:

2. Cuentas de juego usadas específicamente para un evento después de haber permanecido inactivas durante un período de tiempo significativo desde su apertura.
3. Apuestas que muestran que el jugador no lleva una pauta normal de gestión monetaria, por ejemplo, se juega todo el contenido del monedero o apuesta a cualquier cuota.
4. Usuarios que usan todo el saldo disponible o hasta los niveles máximos de participación permitidos en una serie de mercados, o realizan varias apuestas máximas en el mismo resultado para un evento.
5. Usuarios que muestran un perfil ganador con un determinado jugador o equipo.
6. Las estrategias de juego seguidas por usuarios anteriores que ya han sido bloqueados replicadas en nuevos usuarios.

Análisis de las apuestas realizadas

Sobre las apuestas ya realizadas por los jugadores:

[8] La plataforma SIGMA Share es la herramienta de compartición de información relativa a alertas en apuestas y en eventos y competiciones deportivas relativas a posibles amaños.

7. Cambios drásticos en el patrón de apuestas, tales como cantidades muy superiores al patrón habitual, tanto en número como en importe.
8. Evidencia de "*Smurfing"*: clientes respecto a los que existen indicios de que están gestionando varias cuentas al mismo tiempo para colocar su apuesta con importes inferiores para no llamar la atención o maximizar el retorno.
9. Actividad elevada de apuestas coordinadas, con diferencia de segundos entre ellas antes de que el operador baje la cuota o retire el evento.
10. En apuestas combinadas, aquellas que tengan asociado más de un hecho en un evento alertado.
11. Apuestas muy concretas, individualizadas y sin conexión con patrones anteriores de juego, por ejemplo, en tenis, apuestas a un juego o a un set concreto.
12. Apuestas inusuales de cuota alta, camufladas dentro de una apuesta múltiple que incluye otras muy seguras.

7 Medidas de control que contemplan los procesos de cumplimiento

A continuación, se describen un conjunto de medidas de control que contribuyen a minimizar la probabilidad de aparición de los escenarios de riesgo descritos o, en su caso, el impacto que dichos riesgos pudiera producir. La lista que se incluye no es una enumeración exhaustiva de las medidas necesarias o posibles, aunque deben ser tenidas en cuenta por los operadores a la hora de elaborar sus propios protocolos de gestión de riesgos.

Medidas en el proceso de registro de un nuevo usuario

1. La toma de datos y la verificación de datos de identidad, de edad, de inscripción en el RGIAJ y de no inscripción en el registro de fallecidos.
2. La comprobación documental de la identidad. Existe un límite de depósito de 150 euros para usuarios no verificados documentalmente y la prohibición de hacer retiradas.
3. Comprobación del teléfono y de la cuenta de correo, para asegurar que el cliente tiene acceso a ambas cosas, mediante el uso de doble factor de verificación con cada uno de ellos.
4. La dirección postal debería ser válida, incluso podría estar en blanco, pero nunca inventada.
5. Comprobaciones adicionales para el caso de teléfonos y correos electrónicos asignados a más de un usuario.
6. Rechazo de las direcciones de correo temporales, que impiden la comunicación habitual con el usuario a través de ellas.

Medidas en la admisión de nuevos clientes: el operador debe establecer los protocolos de comprobación y las reglas de admisión de clientes

7. Clientes que no se pueden admitir: menores y prohibidos; los clientes ya registrados.
8. Clientes en la lista de PEP[9] o con nacionalidad, residencia o localización en países de alto riesgo.
9. Clientes que no han completado todos los datos de información personal.

Medidas en el proceso de comprobación y aceptación de un nuevo medio de pago

10. Analizar el riesgo del medio de pago usado, por ejemplo, si el medio de pago está autorizado para operar en España, o si el medio de pago admite el uso de criptomonedas.
11. Permitir únicamente aquellos medios de pago que realicen la autenticación reforzada de clientes según la normativa de servicios de pago digitales PSD2.
12. Verificar que el jugador es titular del medio de pago, salvo medio de pago anónimo.
13. Limitar del número de medios de pago utilizados por un usuario.

Medidas en el seguimiento continuo de las actividades del cliente

Según el nivel de riesgo del cliente o de las transacciones se adoptarán las medidas complementarias adecuadas orientadas, según los casos, a confirmar la identidad del cliente, la residencia o la localización, la identidad de los medios de pago, el origen de los fondos o a obtener conocimiento de la capacidad económica o de la riqueza del jugador.

La información obtenida se deberá adecuar al riesgo de forma que la empresa se asegure de que la identidad del jugador es correcta, que los fondos usados en el juego son legítimos y no proceden de actividades delictivas y que las operaciones realizadas por el jugador no esconden otra finalidad diferente al juego.

El alcance de la comprobación puede ser:

14. Reforzar la comprobación de identidad documental, incluida la prueba de vida -si no se ha realizado antes, o si la actividad del jugador ha sufrido algún cambio significativo- o el contacto directo con el cliente.
15. Comprobación del domicilio.
16. Comprobación de nacionalidad/residencia en los casos que se utilice el pasaporte como medio de identificación.
17. En caso de clientes con nacionalidad española, obligatoriedad del uso del DNI.
18. Uso de autenticación de dos factores en el alta, la modificación y en el *login*, de forma que las operaciones no se podrán completar hasta que el usuario introduzca un código PIN enviado por el operador al móvil o acepte un mensaje enviado al correo electrónico.

[9] PEP: Personas expuestas políticamente, personas con responsabilidad pública

19. Aviso de cualquier cambio en los datos de identidad.
20. Aviso de conexión desde un dispositivo nuevo.
21. Hay que confirmar que el nivel de gasto del jugador es acorde a su capacidad económica, para lo que es importante establecer los protocolos que determinen los supuestos en los que se realizará esta comprobación. Estos protocolos pueden ir desde el establecimiento de un umbral máximo de depósito en un periodo determinado que se aplicará a todos los jugadores, hasta la definición de reglas de cálculo de riesgo individualizadas y basadas en el volumen de depósitos o el nivel de gasto acumulado. Los medios de prueba para realizar esta comprobación normalmente incluyen el contacto con el jugador para obtener prueba documental suficiente. El análisis de riesgo debe incluir (1) la determinación de las fuentes de fondos aceptables - por ejemplo, herencias, donaciones o regalos recibidos pueden plantear riesgos de fraude no asumibles; (2) la determinación de los elementos de prueba de orígenes de fondos que son aceptables - por ejemplo, meros depósitos en cuenta o justificantes de transferencia de premios de otros operadores de juego pueden plantear riesgos de fraude no asumibles.