Nota técnica sobre la gestión de fraude en operadores de juego.

ÍNDICE

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

1. Introducción

La lucha contra el fraude constituye uno de los fundamentos de la Ley 13/2011, de 27 de mayo, de regulación del juego (Ley 13/2011 o LRJ) 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 detentadas por los operadores.

La Dirección General de Ordenación del Juego (DGOJ) considera necesario que los operadores incorporen en su estrategia y procedimiento operativo una adecuada política de análisis de fraude y de gestión de los riesgos que se detecten. Así, desde 2017 se ha incorporado a los términos y condiciones de las nuevas solicitudes de licencia la necesidad de que el operador elabore un manual de fraude con el detalle de los procedimientos y medidas implementados para la identificación de los escenarios de fraude y su tratamiento[1]. Igualmente está previsto consagrar esta necesidad a nivel legislativo en el futuro próximo.

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 derivar en el establecimiento de medidas sistemáticas de prevención que los eviten y de detección que permitan descubrir los casos de fraude que se materialicen, así como la determinación de las acciones correctivas para ayudar a

[1] 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.*"

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.

En este documento se analizan los principales tipos de fraude identificados por la DGOJ susceptibles de producirse en un operador de juego, las medidas estructurales de prevención y detección establecidas en la regulación o que constituyen instrucciones de esta Dirección General, 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.

El propósito del documento es resultar de ayuda al operador de juego apuntando el contenido mínimo que, sin perjuicio de las especificidades aplicables a cada organización, cabe considerar desde el punto de vista de la gestión integral del fraude por parte de los operadores licenciados, ofreciendo predictibilidad sobre lo que esta Dirección General entiende por gestión diligente de dicho fraude.

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. Del análisis de la información de la que disponemos - los datos de registro de usuarios y de transacciones de juego aportada por los operadores, la información en los expedientes de denuncia y en las actuaciones de colaboración con las fuerzas de seguridad del estado - se pone de manifiesto que el principal riesgo de fraude en las plataformas de juego es la suplantación de identidad, consentida o no consentida. Estas prácticas tienen como fin eludir los controles de acceso establecidos por los operadores, por lo que, sin perjuicio de ser el cauce para otro tipo de fraudes, podrían estar siendo usadas por personas que tienen prohibido el acceso al juego tales como menores, personas con problemas de juego que se han inscrito en el RGIAJ[2] o que se han autoexcluido en el operador, personas vinculadas al operador o personas vinculadas al deporte. El uso de datos de identidad de terceros para abrir una cuenta de juego o la cesión de uso de la cuenta de juego también puede ser el instrumento utilizado por “amañadores” de eventos deportivos para obtener beneficios de las apuestas. Otros riesgos con menor

[2] Registro General de Interdicción de Acceso al Juego.

incidencia, pero también con un alto impacto en las personas y en la actividad de juego son el uso de tarjetas u otros medios de pago ajenos, la utilización para el juego de dinero ajeno o cuya procedencia no es posible justificar o la utilización de información privilegiada para obtener ventajas frente a otros jugadores.

En este documento se analizan estos diferentes tipos de fraude estableciendo un sistema de control en dos niveles para la identificación de los riesgos existentes y la reacción del operador ante los mismos.

El nivel 1 lo forman un conjunto de medidas que deben ser adoptadas e implantadas por todos los operadores de juego y que tienen un carácter transversal sobre el conjunto de jugadores. En algunos casos, las instrucciones están desarrolladas con un alto nivel de detalle a través de la normativa de juego. En otros casos, se definen los escenarios de riesgo cualificado, es decir, aquellos patrones observados en la actividad de juego, concretos e identificables y que potencialmente tiene una mayor probabilidad de responder a un caso de fraude. El operador debe analizar estos escenarios de riesgo cualificado para concretar sus propias medidas y procedimientos partiendo de este documento y de su propio conocimiento y experiencia.

El nivel 2 se compone de las directrices que deben regir el sistema de gestión de fraude de los operadores en cuanto a la aparición de posibles riesgos sobrevenidos. En este nivel se establece una amplia relación de escenarios de riesgo y las medidas a adoptar para esclarecer los hechos y en última instancia actuar contra el fraude en caso de confirmación.

Dada la importancia que tiene para todos los actores del mercado del juego, independientemente de su naturaleza pública o privada, el objetivo del presente documento es establecer un marco de referencia que sirva a los operadores para la implantación de su propio sistema de gestión del riesgo de fraude, siempre y en todo caso con pleno respeto a la normativa que resultase de aplicación. Entendemos que este marco de referencia debe concebirse como un marco vivo que ha de adaptarse en todo momento a las especificidades y singularidades del fraude en el mercado de juego online, que es una actividad que está sujeta a una constante evolución e innovación.

2. Tipos de fraude en el juego online

A. El fraude en los datos de identidad

1. CONTEXTO

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 de la DGOJ y comunicada al operador para que se bloquee el proceso de alta.

B. 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 respondiendo a diferentes motivaciones. A modo de ejemplo se incluyen algunas de estas motivaciones:

   - Personas que tienen prohibido el acceso al juego 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 tienen conocimiento, directo o indirecto, de un futuro resultado amañado de un evento deportivo y utilizan las apuestas para obtener una ganancia.
   - Personas previamente bloqueadas por el operador en aplicación de sus políticas de prevención del fraude.

- 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.
- Jugadores que buscan la elusión de la tributación en el Impuesto sobre la Renta de las ganancias obtenidas en el juego.

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; generalmente se produce en el entorno familiar o de amigos o con terceros que ceden los datos de identidad a cambio de una contraprestación que puede ser recibida una única vez 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 la misma ante los diferentes controles del operador 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.

La correcta gestión de los riesgos de fraude se desglosa en dos niveles. Para cada uno de los niveles se describen los escenarios de riesgo cualificado identificados por la Dirección General y se establecen las medidas que deben ser implantadas por los operadores de juego.

2. CONTROLES Y ACCIONES DE NIVEL 1 RELATIVAS A SUPLANTACIONES DE IDENTIDAD

Forman parte del nivel 1 para la prevención de la suplantación de identidad las siguientes medidas[3]:

2.1. Verificación de la identidad de jugadores

El proceso de verificación de identidad de jugadores consiste en recabar la información del registro de usuario y verificar la veracidad de los datos aportados. Incluye las siguientes medidas de control:

a) Cumplimiento por parte del jugador del formulario de registro completando el conjunto de datos establecidos en la normativa de juego.
b) Comprobar la veracidad de los datos aportados de DNI/NIE, nombre, apellidos y edad. Esta verificación puede realizarse a través del servicio web de verificación de identidad proporcionado por la DGOJ.
c) Comprobar la no inscripción en el registro de interdictos a través del servicio web de verificación de RGIAJ proporcionado por la DGOJ.
d) Revisar los posibles errores en los datos introducidos tales como calles o códigos postales inexistentes, no coincidencia entre el código postal y la ciudad de residencia o entre el código postal y el código de residencia fiscal.
e) Comprobar que un jugador no se ha registrado en el operador con posterioridad a su fecha de fallecimiento.

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

a) 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 datos de identidad o de conexión – coincidentes con los de un intento fallido de registro de un menor[4].

[3] Artículos 26 y 27 del Real Decreto 1613/2011, de 14 de noviembre, por el que se desarrolla la Ley 13/2011, de 27 de mayo, regulación del juego, en lo relativo a los requisitos técnicos de las actividades de juego y su normativa de desarrollo.

4 El 14 de noviembre de 2018 la DGOJ ha puesto en marcha una nueva funcionalidad ampliada del servicio de verificación de identidad del jugador que permite al operador conocer los intentos de alta de registro en los que se utilice un DNI asociado a un menor de edad que ha modificado alguno de los datos de identidad o de edad durante el proceso de registro. Hasta ahora, cuando el sistema detectaba un error en los datos de identidad daba

b) 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 datos de identidad o de conexión – coincidentes con los de una persona inscrita en el RGIAJ o autoexcluida en el operador.

c) Intento de alta de registro usando los datos de identidad de personas fallecidas[5]. Tras el bloqueo de la cuenta por el operador, se producen intentos de registro usando alguno de los datos de identidad o de conexión - nombre y apellidos, domicilio, número de teléfono, correo electrónico, dirección IP, identificación de dispositivo u otros datos de identidad o de conexión - coincidentes con los de la persona fallecida o los del intento de registro.

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

d) Existe una cuenta activa asociada a los mismos datos de identidad –DNI/NIE, nombre, apellidos y edad-.

un mensaje de "datos con errores" pero no proporcionaba información de detalle del error. Con esta funcionalidad ampliada los operadores podrán conocer cuándo un error en el proceso de verificación es debido a intentos de alta con un DNI de un menor. Con esta información podrán incluir controles adicionales para detectar la posible reutilización de los mismos datos de identidad o de conexión de ese intento de registro – nombre y apellidos, domicilio, número de teléfono, correo electrónico, dirección IP, identificación de dispositivo - con el fin de impedir futuros intentos de acceso utilizando otras identidades.

5 El 14 de noviembre de 2018 la DGOJ ha puesto en marcha una nueva funcionalidad ampliada del servicio de verificación de identidad del jugador para incorporar la 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. Con esta información el operador podrá 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 podrá 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.

e) 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.

f) Se han creado de forma secuencial varios registros de usuario desde el mismo dispositivo y dirección IP en un corto espacio de tiempo usando diferentes datos de identidad aunque normalmente compartiendo el mismo teléfono y/o la misma dirección de correo electrónico.

2.1.3. Acciones a realizar en los escenarios descritos

Pasar a la fase de verificación documental.

2.2. Verificación documental del jugador

La verificación documental del jugador permite comprobar la veracidad de los datos de identidad aportados en el registro de usuario por el jugador mediante un procedimiento de solicitud de documentos fehacientes.

La comprobación documental de los datos de identidad tiene como finalidad garantizar que la identidad manifestada por el participante se corresponde con la identidad real. El proceso de comprobación implica obtener copia de un documento válido y, en la medida de lo posible, comprobar que no ha sido alterado y que realmente pertenece a quien lo presenta.

Según se establece en la Resolución de 12 de julio de 2012, por la que se aprueba la disposición que desarrolla los artículos 26 y 27 del Real Decreto 1613/2011, de 14 de noviembre, en relación con la identificación de los participantes en los juegos y el control de las prohibiciones subjetivas a la participación, modificada a través de la Resolución de 31 de octubre de 2018, de la Dirección General de Ordenación del Juego, por la que se modifican determinadas resoluciones sobre las actividades de juego previstas en la ley 13/2011, de 27 de mayo, de regulación del juego, los jugadores no verificados documentalmente solo podrán depositar hasta un límite conjunto de 150 euros, y participar en los juegos, pero no podrán retirar los premios.

2.2.1. Acciones a realizar en la fase de verificación documental

Comprobar que el documento aportado pertenece a la persona identificada en el registro.

Puede realizarse por diferentes procedimientos que van desde el envío por el jugador de una fotografía sosteniendo su documento original a una altura que permita además la comparación de su cara con la fotografía adjunta a dicho documento, hasta la aplicación de un procedimiento completo de verificación de identidad digital (digital onboarding).

Se entiende por Digital Onboarding el proceso de identificación no presencial que permite a los usuarios darse de alta como nuevos clientes de una manera totalmente digital. Recientemente están apareciendo en el mercado diversas herramientas de digital onboarding que incluyen funcionalidades avanzadas como las siguientes[6]:

1. Procesos automáticos de registro de usuarios.
2. Identificación automática de documentos.
3. Comprobación de la veracidad de la autenticidad de los documentos.
4. Extracción de datos biométricos y alfanuméricos contenidos en un documento de identidad.
5. Contraste de la foto contenida en un documento de identidad con la imagen de la persona.
6. Prueba de vida.
7. Videoconferencia.
8. Validación del teléfono móvil.

En el contexto de esta obligación de carácter general, se establecen los siguientes escenarios de riesgo.

2.2.2. Escenarios de riesgo en la fase de verificación documental

g) Existen dudas en la veracidad de los documentos de identificación aportados tales como falsificación o manipulación de los documentos.

6 En el marco de la comprobación de la autenticidad de documentos, existen estándares en la industria como la norma ICAO 9303 o la norma ISO/IEC 7501-1. En el contexto del reconocimiento facial, existen algoritmos de referencia evaluados por NIST (National Institute of Standard and Technology).

h) Existen dudas sobre la correspondencia entre el titular del documento y la persona real que realiza el registro.

2.2.3. Otras acciones posibles en los escenarios descritos según los casos

- Repetir el proceso de verificación documental de la identidad.
- Solicitar al jugador nuevos documentos: nuevo documento de identidad, copia de alguna factura de servicios (luz, agua u otros), etc.
- Realizar un contacto telefónico: llamada telefónica o videoconferencia.
- Validar el teléfono móvil del jugador mediante el envío de un SMS.
- Validar el correo electrónico del jugador mediante el envío de un mensaje con un enlace de verificación.
- Validar el domicilio del jugador mediante el envío de una carta.

3. CONTROLES Y ACCIONES DE NIVEL 2 RELATIVAS A SUPLANTACIONES DE IDENTIDAD

3.1. Seguimiento activo de la relación con el jugador

Una vez superado de forma satisfactoria el nivel 1, entra en juego el nivel 2. Una adecuada gestión de los riesgos de suplantación de identidad requiere la adopción de medidas adicionales de control durante el desarrollo de la relación contractual con el jugador con el fin de detectar aquellos casos de fraude en los datos de identidad que no han podido ser detectados en el proceso de alta. Este nivel consiste fundamentalmente en el seguimiento activo del jugador y debe contemplar una relación dinámica y en constante revisión de posibles escenarios de riesgos cualificados.

3.1.1. Escenarios de riesgo durante la actividad de juego

i) Se realizan actividades de juego - depósito, participación o retirada de fondos - usando una cuenta de juego de una persona fallecida después de la fecha de fallecimiento.

j) Se producen intentos de desbloqueo de usuarios bloqueados por inscripción en el RGIAJ o por autoexclusión en los servicios de atención al usuario en los que interviene directamente el personal del operador.

k) Hay varias reclamaciones de similar contenido interpuestas por un conjunto jugadores que comparten datos de identidad, de domicilio, de teléfono, de dirección de correo electrónico, de dispositivo o de dirección IP.

l) Hay actividad de juego de usuarios de avanzada edad con un comportamiento de juego anómalo por el tipo de juego, por el horario de juego o por la intensidad de la actividad.

3.1.2. Acciones a realizar en los escenarios descritos

El supuesto i) supone un claro indicio de utilización de datos de identidad por un tercero.

En los casos j), k) y l) procede confirmar la identidad del jugador aplicando las acciones contempladas para la correcta verificación de la identidad del jugador descritas anteriormente. La elección de las medidas concretas a aplicar dependerá del caso concreto y de la información disponible.

4. RESOLUCIÓN UNILATERAL DEL CONTRATO Y COMUNICACIÓN A LA DGOJ

En caso de probarse que el jugador ha incurrido en fraude de identidad o que haya permitido la utilización de sus datos por terceros, el operador podrá aplicar el artículo 33.2 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 las licencias, autorizaciones y registros del juego (en adelante RDL).

B. El fraude en los medios de pago

1. CONTEXTO

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.

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.

Se establece un sistema de control en dos niveles.

2. CONTROLES Y ACCIONES DE NIVEL 1 RELATIVAS A MEDIOS DE PAGO

2.1. Trazabilidad de las transacciones

En el marco de la política de gestión de riesgos de fraude de medios de pago, el operador debe garantizar que todas las transacciones tengan trazabilidad completa. El análisis y gestión del fraude el operador se prestará atención especial a los medios de pago cuya titularidad no pueda ser inmediatamente identificada o verificada. La verificación del medio de pago es el proceso mediante el cual se obtienen los datos del titular del medio de pago[7].

En general, se considera diligente tener en cuenta los siguientes criterios:

- Las retiradas de fondos de la cuenta de juego se realizarán a través del mismo medio de pago utilizado para el depósito[8], siempre que permita la trazabilidad. En caso contrario, la retirada deberá utilizar un medio de pago trazable y verificado.

[7] Para garantizar la trazabilidad de las transacciones y facilitar cualquier investigación posterior por fraude en medios de pago el operador debe conservar los datos del titular del medio de pago verificado y los cuatro últimos dígitos de la cuenta o tarjeta; o bien habilitar los mecanismos para su obtención en caso de requerimiento de información por parte de las autoridades españolas competentes.

[8] Artículo 38 apartado 1 del RDL.

- En particular, si el medio de pago usado en el depósito es anónimo, las retiradas se realizarán mediante un medio de pago que sea trazable y esté verificado (p. ej. mediante transferencia bancaria o mediante tarjeta cuando haya sido verificada).
- Se intentará minimizar el número de diferentes medios de pago usados por el jugador.

2.1.1. Escenarios de riesgo

a) Intento de retirada de fondos de la cuenta de juego a un medio de pago anónimo.

b) Intento de retirada de fondos de la cuenta de juego a un medio de pago diferente al de depósito mientras el medio de pago sea nominal pero no esté verificado.

2.1.2. Acciones a realizar en los escenarios descritos

No se permitirán las retiradas de fondos usando medios de pago anónimos.

No se permitirán las retiradas de fondos usando un medio de pago diferente al usado para el depósito hasta que no se verifique que pertenece al titular de la cuenta de juego.

3. CONTROLES Y ACCIONES DE NIVEL 2 RELATIVAS A MEDIOS DE PAGO

3.1. Seguimiento activo de la relación con el jugador

Una adecuada gestión de los riesgos de fraude en medios de pago requiere la adopción de medidas adicionales de control durante el desarrollo de la relación contractual con el jugador con el fin de detectar aquellos casos de fraude que no han podido ser detectados en la aplicación de las medidas de nivel 1.

3.1.1. Escenarios de riesgo en los medios de pago

c) Solicitud de retirada de fondos sin haber realizado actividad de juego.

3.1.2. Acciones a realizar en los escenarios de riesgo descritos

La solicitud de retirada de fondos de la cuenta de juego sin haber realizado actividad de juego o con una actividad mínima en relación a los depósitos requiere un análisis de las circunstancias concretas del caso para descartar un posible fraude.

4. RESOLUCIÓN UNILATERAL DEL CONTRATO Y COMUNICACIÓN A LA DGOJ

En caso de probarse que el jugador ha incurrido en fraude en los medios de pago, el operador podrá aplicar el artículo 33.2 del RDL.

C. El fraude en el origen de fondos

1. CONTEXTO

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.

2. CONTROLES Y ACCIONES DE NIVEL 1 RELATIVAS A ORIGEN DE FONDOS

2.1. Comprobación de la capacidad económica del jugador

La comprobación de la capacidad económica del jugador en relación con su nivel de gasto tiene como fin comprobar que los fondos usados por el jugador le pertenecen[9].

En el marco de la política de gestión de riesgos de fraude en el origen de fondos, el operador ha de definir los supuestos en los que en todo caso se ha de realizar la comprobación de la capacidad económica del jugador.

2.1.1. Escenarios de riesgo en la fase de comprobación de la capacidad económica

a) Un volumen de depósitos acumulado en el año igual o superior a 36.000 euros.

b) Los usuarios calificados como clientes “VIP”. Los jugadores calificados como usuarios “VIP” requieren un seguimiento de las circunstancias que motivan esa categorización y la comprobación de que el jugador no está disponiendo de fondos que no son suyos.

[9] La comprobación de la capacidad económica del jugador también es un elemento a tener en cuenta en la política de juego responsable del operador por lo que también tiene como objetivo prevenir el juego con préstamos de terceros.

2.1.2. Acciones a realizar en los escenarios descritos

La comprobación de la capacidad económica del jugador puede ser realizada mediante cualquier medio de prueba generalmente admitido, por ejemplo solicitando al jugador documentos justificativos de solvencia (nómina, vida laboral, declaración por el Impuesto de Renta de las Personas Físicas, etc.).

D. El fraude de geolocalización

1. CONTEXTO

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

- Personas que intentan saltarse los controles de identidad establecidos por el operador en la plataforma ".es" por alguno de los motivos ya descritos en el punto 2.A de este documento.
- Personas que intentan eludir los controles de trazabilidad de las transacciones por motivos fiscales.

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

2. CONTROLES Y ACCIONES DE NIVEL 1 RELATIVAS A GEOLOCALIZACIÓN

2.1. <u>Control de la oferta de juego</u>

El operador, que directamente o a través de sus matrices o filiales opera en otras jurisdicciones, deberá implantar medidas que le permitan, en la medida de lo posible, detectar y evitar las conexiones de usuarios localizados en España que intenten acceder a las plataformas de juego diferentes a la autorizada por una licencia española usando tecnologías de red cuyo fin sea ocultar su dirección IP.

2.1.1. Escenarios de riesgo en la fase de comprobación de la localización del jugador

El principal problema para la correcta geolocalización proviene de los servicios de proxy, VPNs y roaming por lo que la geolocalización no siempre garantiza al 100% la ubicación del usuario.

2.1.2. Acciones a realizar en los escenarios descritos

En primer lugar, el operador puede mantener listas de IPs de proxies o de VPNs conocidas públicamente. De esta forma, una conexión de un jugador desde una de estas IPs puede suponer un indicio de que la localización real del jugador no es la de la IP de conexión requiriéndose comprobaciones adicionales con otras fuentes para contrastar la localización del jugador.

Para aumentar el número de casos con geolocalización correcta de los jugadores los operadores de juego pueden implementar servicios adicionales de geolocalización de IPs o de contraste de la IP del jugador con bases de datos de geolocalización. Existen soluciones comerciales que facilitan la geolocalización. La elección de la herramienta dependerá de los datos que se deseen saber de la IP, el tipo de servicio requerido (comprobación por petición HTTP, base de datos de geolocalización, etc.) y de la precisión de la misma.

Además, en el caso de las aplicaciones para dispositivos móviles, se puede complementar la geolocalización IP con la geolocalización física (GPS, Wifi, redes móviles en rango, …).

En todo caso, el uso de herramientas de geolocalización debe complementarse con medidas adicionales de control basadas en los datos de identidad, los datos de residencia y de medios de pago usados, así como en la aplicación de procedimientos para la detección de fraude. En ocasiones, las mismas empresas que ofrecen herramientas de geolocalización, incluyen servicios antifraude.

E. El fraude en apuestas vinculado a amaños de eventos deportivos

1. CONTEXTO

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, realizándose las apuestas fraudulentas en operadores de apuestas de cualquier jurisdicción.

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 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, pueda identificarse a los involucrados.

2. CONTROLES Y ACCIONES DE NIVEL 1 RELATIVAS A AMAÑOS

2.1. Acciones preventivas

2.1.1. Formación

La principal línea de prevención es la formación. Corresponde a cada parte interesada, desde su esfera de competencia, colaborar en la trasmisión del mensaje de los riesgos de amañar un evento deportivo o de apostar teniendo conocimiento del mismo, así como informar claramente de las consecuencias de amaño y de la apuesta conociendo el amaño.

Esta acción puede llevarse a cabo de múltiples maneras: talleres, mensajes, trípticos, campañas publicitarias, manuales, anuncios, notas informativas, etc. Cada interesado valorará cuál es la estrategia que mejor se adapta a sus objetivos.

2.1.2. Obligaciones de información

La lucha contra el fraude en apuestas vinculado a amaños de eventos se apoya en la compartición de información con un doble objetivo, por un lado, poner en conocimiento de los interesados la existencia de situaciones anómalas que pudieran ser indicio de un posible amaño, y por otro lado construir la inteligencia necesaria para la lucha contra este tipo de fraude cada vez más sofisticado.

La compartición de información sobre un posible amaño debe producirse al menos en los siguientes niveles:

- Con los Cuerpos y Fuerzas de Seguridad del Estado sobre posibles delitos.
- Con la DGOJ sobre las alertas relativas a posibles eventos amañados.

La generación de "inteligencia" entre todos los interesados se alimenta del intercambio de conocimiento, técnicas y procedimientos de investigación, buenas prácticas, etc.

2.2 Acciones de detección

Las acciones de detección se basan en la monitorización de las apuestas para la detección de anomalías y su posterior análisis e investigación. Estas anomalías, aunque no constituyen por sí mismas una evidencia de fraude en un determinado evento, sí que constituyen una alerta sobre apuestas irregulares[10] o sospechosas[11].

El análisis de las alertas relativas a amaños de eventos deportivos debe incorporar una graduación de las mismas basada en la confluencia de indicios. En definitiva, hasta que no haya evidencias o confluencia de muchos indicios una alerta es estrictamente una anomalía en el comportamiento del mercado de apuestas que no puede explicarse.

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 analizada deberán ser comunicadas a la DGOJ, que gestiona el sistema nacional de alertas.

3. CONTROLES Y ACCIONES DE NIVEL 2 RELATIVAS A AMAÑOS

3.1. Seguimiento activo del desarrollo de los eventos y de las apuestas realizadas

[10] Apuesta deportiva irregular: cualquier apuesta deportiva que no se ajuste a las apuestas habituales o previsibles del mercado de que se trate o que guarde relación con una competición deportiva que se desarrolle conforme a pautas no habituales. Fuente: Convenio de Macolin.

[11] Apuesta deportiva sospechosa: cualquier apuesta deportiva que, atendiendo a pruebas fiables y no contradictorias, parezca estar vinculada a una manipulación de la competición respecto de la cual se realiza dicha apuesta. Fuente: Convenio de Macolin.

En el marco de la política de gestión de riesgos de fraude relativo a amaños, el operador ha de definir los supuestos en los generará una alerta que será objeto de análisis y de reporte a SIGMA[12].

3.1.1. Escenarios de riesgo en el análisis de las altas de usuario

a) Altas de registros de usuarios 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.

b) Altas de registros de usuarios con el mismo patrón en el login, en la dirección de correo e incluso en los depósitos iniciales. Varios registros de usuario con coincidencia en datos como el teléfono, el correo electrónico, el dispositivo o la dirección IP.

c) Varios registros de usuario creados en un corto espacio de tiempo con datos de domicilio en una zona geográfica muy concentrada - incluso en la misma manzana de edificios-.

d) Varios intentos fallidos de verificación con iguales datos de identidad, pero variando DNI, fechas de nacimiento o variantes del nombre (i.e.: José Antonio, José Antoni, Josep Antoni).

e) Utilización de cuentas de correo creadas en servidores cifrados extremo a extremo. La utilización de cuentas de correo cuya principal característica es el cifrado extremo a extremo, impiden al proveedor de la cuenta acceder al contenido de dichos correos lo que dificulta la trazabilidad de las operaciones en caso de investigación por la policía.

f) Utilización de cuentas de correo “efímeras” que desaparecen en pocos días cuyo fin principal es evitar el exceso de correos de publicidad o spam, pero que también pueden ser usadas para ocultar la identidad real.

[12] SIGMA: servicio de información global del mercado de apuestas de la DGOJ que gestiona las alertas por apuestas sospechosas o irregulares.

g) Cuentas de usuario que se abren en fechas previas a un evento para apostar específicamente al mismo.

h) Cuentas nuevas abiertas en la misma área o región, especialmente si la región en cuestión puede asociarse con uno o más de los participantes en un evento.

i) Existen indicios de que la cuenta está bajo control de un tercero. Por ejemplo, la cuenta está a nombre de una mujer, pero la dirección de correo es masculina.

3.1.2. Escenarios de riesgo en el análisis de la forma de juego

j) Cuentas de juego usadas específicamente para un evento después de haber permanecido inactiva durante un período de tiempo significativo desde su apertura.

k) 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.

l) 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.

m) Usuarios que muestran un perfil ganador con un determinado jugador o equipo.

n) Las estrategias de juego seguidas por usuarios anteriores que ya han sido bloqueados que se replican en nuevos usuarios.

3.1.3. Escenarios de riesgo en el análisis de las apuestas realizadas

o) Cambios drásticos en el patrón de apuestas, tales como apuestas significativamente por encima del patrón habitual, tanto en número como en importe.

p) 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.

q) Actividad elevada de apuestas coordinadas, con diferencia de segundos entre ellas antes de que el operador baje la cuota o retire el evento.

r) En apuestas combinadas, aquellas que tengan asociados más de un hecho en un evento alertado.

s) 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.

t) Apuestas inusuales camufladas dentro de una apuesta múltiple que incluye apuestas bajas y muy seguras.

3.1.4. Acciones a realizar en los escenarios descritos

Una alerta debe generar las siguientes acciones:

- Comunicar a la DGOJ la alerta a través del servicio de SIGMA.
- Informar a la D. G. de Policía si hay indicios de delito.

3. La gestión de riesgos de fraude

El sistema concreto de gestión de riesgos debe estar adaptado a la realidad de cada operador – tipos de juego ofertados, canales de comercialización usados, tipo de clientes, tipos de medios de pago admitidos o tecnología usada. No obstante existen unos principios generales que tienen carácter transversal y su aplicación resulta necesaria para cualquier tipo de operador. Para una correcta implantación de un sistema de detección y gestión de riesgos, se recomienda la consulta e implantación de los siguientes estándares:

- Norma UNE-ISO 19600: Sistemas de Gestión de Compliance. Directrices.
- Norma ISO 31000: Gestión de riesgos.

Las anteriores normas definen y explican en mayor profundidad la implantación en la organización de un modelo de gestión de cumplimiento basado en riesgos, y en ellas se establecen principios generales como los siguientes:

1. El operador de juego debe implantar un **Sistema de gestión de cumplimiento normativo** y principios de buen gobierno (ISO 19600).
2. En el organigrama del operador de juego debe existir un responsable de cumplimiento normativo ("**Compliance Officer**" o cargo similar), encargado del control interno y normativo de la compañía. Este cargo debe disponer de independencia orgánica y reportar directamente a la alta dirección.
3. Deben existir programas de **formación en materia de fraude en el juego** al conjunto del personal interno. En este sentido, se debe prestar especial atención al personal que compone el CAU (Centro de atención al usuario) o el SAC (Servicio de atención al cliente), los gestores personales de cuentas de cliente y en general cualquier servicio que tenga relación directa con los clientes.
4. El operador de juego debe implantar un **sistema de gestión de riesgos de fraude en el juego** (ISO 31000). Este sistema de gestión se basa en la definición, gestión y mantenimiento de una matriz de riesgos de fraude en el juego, definida en función del modelo de negocio y la idiosincrasia de cada operador.
5. El operador debe implantar procedimientos de **monitorización activa de sus jugadores** que le permita tener un primer análisis de datos de sus jugadores 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 anti-fraude, 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.

6. En el seno del operador debe existir un **canal de comunicaciones con organismos oficiales** donde se contemplen al menos los siguientes:
   - En el caso de sospechas o indicios de fraude por blanqueo de capitales, los operadores tendrán la obligación de comunicarlos al **SEPBLAC** (http://www.sepblac.es/).
   - En el caso de otro tipo de fraudes que podrían derivar en delitos, los operadores tendrán la obligación de comunicarlo a la **D. G. de Policía**.
   - Las obligaciones de información con la **DGOJ**, tales como la información en el Sistema de Control Interno de los estados del registro de usuario, el informe trimestral de cuentas bloqueadas y la comunicación inmediata de alertas en apuestas dentro de la plataforma de SIGMA.

4. ANEXO – Bibliografía

Estándares de certificación:

- Norma UNE-ISO 19600 Sistemas de Gestión de Compliance. Directrices.
- Norma ISO 31000- Gestión de riesgos.

Documentación sobre el diseño de un Sistemas de Gestión de Compliance:

- Las 40 recomendaciones del GAFI constituyen el marco básico de lucha contra el blanqueo de capitales.
  http://www.sepblac.es/espanol/informes_y_publicaciones/40%20recomendaciones_feb2012.pdf

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

- Documento sobre la aproximación a la prevención del blanqueo de capitales y la financiación del terrorismo desde un enfoque basado en el riesgo.

  http://www.sepblac.es/espanol/informes_y_publicaciones/documento%20_recomendaciones_sobre_medidas%20_control_interno_PBCFT.pdf

  http://www.sepblac.es/espanol/informes_y_publicaciones/38960576.pdf