ESTABLECIMIENTO DE UN SERVICIO DE ALERTA DE INTENTOS DE ACTIVACIÓN DE REGISTROS DE USUARIO EN OPERADORES DE JUEGO ONLINE ("PHISHINGALERT")

1 Identificación dentro del Programa de trabajo de Juego Responsable

Prioridad: Protección del participante

Estrategia: Aumento de la efectividad de los mecanismos de información y prevención

Acción 2.4.1: Establecimiento de un servicio de alerta de intentos de activación de registros de usuario en operadores de juego online (PhishingAlert)
JUSTIFICACIÓN: En el proceso inicial de registro de una persona como usuario de un operador de juego en línea, existe la posibilidad de que otra persona intente ese registro mediante alguna técnica de suplantación de identidad en medios electrónicos. En este ámbito, la DGOJ proporciona a los operadores un servicio (el Sistema de Verificación de Jugadores, SVJ), al objeto de facilitar la verificación de los datos de identidad de la persona que solicita un registro de usuario mediante DNI o NIE. Adicionalmente, existen otras previsiones normativas que vienen a limitar la posibilidad de participación en los juegos de azar o la retirada de los depósitos de la cuenta de juego mientras que no se produzca una verificación documental del jugador. Sin embargo, y a pesar de que los controles anteriormente mencionados, así como la existencia de otras obligaciones de los operadores para detectar la suplantación de identidad, es necesario proporcionar otros servicios de valor añadido que vengan a proporcionar una mayor información sobre el uso de los datos de identidad en los operadores de juego, proporcionando una mayor seguridad a la sociedad en su conjunto sobre el acceso no consentido a las plataformas de juego online. Por ello, se plantea la puesta en marcha de un nuevo servicio, esta vez de utilidad directa para el ciudadano, en la medida que podrá informarle de los intentos de registro en un operador de juego utilizando los datos de identidad de aquellos que se hayan suscrito al mismo, complementando el resto de trabajos que está realizando la DGOJ para reforzar las garantías del proceso de verificación de identidad previos a la activación de un registro de usuario.
OBJETIVO: Puesta en marcha de un "servicio de alerta" de la DGOJ para: 1. Reforzar las garantías de los sistemas de identificación de los participantes y del acceso seguro a las actividades de juego de ámbito estatal (juego seguro). 2. La protección del ciudadano mediante un servicio informativo que le ayude a detectar intentos de suplantación de identidad en la activación de registros de usuario.

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

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

PRINCIPALES COMETIDOS DEL CAJR: Desde la DGOJ se mostraría a los miembros de la Sección Protección al Participante las principales características del desarrollo del servicio propuesto, consistente en líneas generales, en la posibilidad de detección de intentos de activación de registros de aquellos ciudadanos que hubiesen solicitado la activación de esta funcionalidad. Una vez se dispongan de las consideraciones sobre el diseño del servicio, la DGOJ procederá a su puesta en marcha.
SECCIÓN IMPLICADA: Protección al Participante

2 Antecedentes

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. En este sentido, el desarrollo de sistemas y mecanismos para la prevención del fraude y del blanqueo de capitales es una obligación expresamente contenida en la normativa de juego.

Desde el inicio de la actividad del juego online – junio de 2012-, la DGOJ facilita a los operadores de juego con habilitación estatal la verificación de la identidad de los participantes, así como conocer si están o no incluidos en el Registro General de Interdicciones de Acceso al Juego (RGIAJ) a través de la utilización de un servicio[1] de interconexión automatizado.

En lo que se refiere a la verificación de identidad, el citado servicio facilita a los operadores la verificación mediante el acceso electrónico en tiempo real, de los datos de identidad (nombre, apellidos, fecha de nacimiento y número del documento identificativo) de los solicitantes que empleen para su identificación el documento nacional de identidad (DNI) o el número de identificación de extranjeros (NIE), así como a la condición de mayoría de edad del participante.

Con respecto al RGIAJ, a través del mismo servicio se habilita la posibilidad de comprobar que los participantes no figuran inscritos en el mismo, proceso que se realiza en el momento de la apertura de una cuenta de juego por parte de los participantes. Así mismo, también se utiliza por los operadores de

[1] *Se ofrece en cumplimiento de los 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 de 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.*

juego, esta vez con frecuencia horaria, para verificar que ninguno de los participantes con registro de usuario activo figuran inscritos en el RGIAJ.

3 Evolución de la verificación de identidad

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 dispone este regulador - 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 de edad, personas con problemas de 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.

En este contexto, la DGOJ ha puesto en marcha recientemente una serie de medidas regulatorias y técnicas con el fin de reforzar los procedimientos llevados a cabo por los operadores de juego en materia de gestión del fraude en general y de los procesos de verificación de identidad sobre los datos aportados por los participantes en particular. Las principales medidas son las siguientes:

- Con fecha 8 de noviembre de 2018 se publica 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. Mediante esta Resolución se modifican, entre otras, 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 y viene a exigir la necesidad de verificar documentalmente a los participantes para acceder a la práctica del juego, restringiendo en caso contrario su actividad en las plataformas de juego (no podrán retirar premios ni realizar depósitos que de forma acumulada superen los 150€).
- Con fecha 14 de noviembre de 2018 la DGOJ ha puesto en marcha una nueva funcionalidad 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. Con esta funcionalidad los operadores podrán conocer cuándo un error en el proceso de verificación es debido a intentos de alta con un DNI de un menor e 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.

Así mismo, se procede a incorporar en el mencionado servicio de verificación de identidad del jugador 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.

- Con fecha 21 de diciembre de 2018 se publica la Nota técnica sobre la gestión de fraude en operadores de juego. 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.

4 El nuevo servicio de alertas por suplantación de identidad “PhishingAlert”

Continuando con las medidas de lucha contra el fraude y suplantación de identidad, la DGOJ tiene previsto ofrecer a los ciudadanos un servicio en virtud del cual se detectan los intentos de activación de un registro de usuario en un operador de juego con licencia estatal proporcionando datos de identidad coincidentes con aquellos que se hayan inscrito en este servicio, y a los que se informaría de tal circunstancia.

Con este servicio se pretende, además, dar respuesta a algunas de las demandas sociales respecto del incremento de la protección de los menores de edad, dificultando la posibilidad de que los mismos puedan acceder a servicios de juego online mediante la utilización de la identidad de alguno de sus allegados mayores de edad. De esa forma, para aquellas personas que puedan tener cierta prevención respecto del uso de su identidad por menores de edad cercanos, esta medida viene a complementar la efectividad del resto de medidas mencionadas en el punto III de este documento, coadyuvando a configurar un entorno donde se puede asegurar en gran medida la correspondencia entre la identidad manifestada por el participante y la identidad real del mismo, evitando así la necesidad de establecer otras medidas de mayor impacto como la necesidad de inscribirse en el RGIAJ para evitar el uso de la identidad propia por terceros, lo que supondría, además de la realización del trámite en cuestión, adulterar el propósito del citado Registro, por cuanto se viene a autolimitar la participación en los juegos de azar por un motivo distinto del que inspira la creación del RGIAJ. Todo ello sin perjuicio de los avances que se puedan realizar para fomentar el uso de herramientas que acrediten la identidad de los participantes, como el uso de certificados digitales[2].

4.1 Alcance del servicio.

El servicio de alerta será aplicable respecto de los juegos de azar en línea incluidos dentro del ámbito de aplicación de la Ley 13/2011 para cuya participación se requiera la identificación del participante, y siempre que el operador de juego se haya adherido al servicio y proceda a verificar los datos aportados por el solicitante a través Sistema de Verificación de Identidad de la DGOJ, de acuerdo al procedimiento establecido en el apartado Séptimo de la Resolución de 12 de julio de 2012, de la DGOJ, por la que se aprueba la disposición que desarrolla los artículos 26 y 27 del Real Decreto 1613/2011.

El sistema de alerta sólo se activará en caso de “respuesta positiva” de la consulta efectuada por el operador en el Servicio de Verificación del Jugador (SVJ): coincidencia de los datos proporcionados en la fase de intento de registro con los almacenados en la Base de Datos del DNI de la Dirección General de la Policía, de acuerdo a lo que dispone el apartado Séptimo.3 de la citada Resolución de 12 de julio de 2012, de la DGOJ.

[2] *Ver http://www.ordenacionjuego.es/es/noticia-kit-dni-moviles*

4.2 Finalidad.

- La protección de ciudadanos, participantes o no en plataformas de juego online con licencia estatal, interesados en que mediante un mecanismo informativo se les traslade la utilización de sus datos de identidad en actividades de juego en línea de ámbito estatal.
- Juego Seguro: reforzar las garantías de los participantes de estar utilizando un operador de juego con licencia estatal.

4.3 Colaboración de los operadores con licencia

La implementación de este servicio en lo que respecta a los operadores de juego con licencia estatal no supone ninguna adaptación técnica en los mecanismos de intercambio de información con la DGOJ. No obstante el operador deberá disponer de una línea de atención a aquellas personas que habiéndose inscrito en el servicio reciban la alerta correspondiente y necesiten aclarar las circunstancias concretas que la determinaron. Por ello, y ante la incertidumbre sobre la aceptación y uso por parte de la ciudadanía de este servicio, no se ha considerado conveniente el incorporar este servicio dentro la normativa obligatoria a cumplir por parte de los operadores de juego con licencia estatal, diseñando una primera fase basada en las adhesiones voluntarias al servicio por parte de los operadores. Desde la DGOJ, una vez haya transcurrido el tiempo necesario que permita valorar la utilidad del servicio, incluyendo las consideraciones que puedan realizar los operadores suscritos al mismo, evaluará la posibilidad de incorporarlo al resto de obligaciones a cumplir por los operadores de juego con licencia estatal.

Por otro lado, los operadores de juego con licencia estatal que soliciten la incorporación a este servicio deberán comprometerse a:

- Facilitar y mantener actualizado a través de la sede electrónica de la Dirección General el alta en el servicio, así como las URL's, teléfonos o direcciones de correo de atención a los clientes que sean alertados por el sistema de una posible suplantación de identidad. Esta información sólo será proporcionada a aquellos interesados suscritos al servicio en los correspondientes avisos de utilización de credenciales, no previéndose la puesta a disposición pública.
- En una primera fase, proporcionar a la DGOJ un informe de valoración del servicio centrado en la interacción con aquellos particulares suscritos al mismo. Dependiendo de la evolución del servicio, se valorará conjuntamente entre la DGOJ y los operadores suscritos, la periodicidad más conveniente para emitir el informe o incluso la posibilidad de su suspensión.

- Comunicar a la DGOJ, mediante la utilización de la operación “bajaJugador” del SVJ, el cese de la relación contractual con su cliente (en términos de estado del participante, cuando éste no esté “activo”).
- Si el jugador vuelve a la situación de activo en el operador, éste deberá volver a verificar la identidad y la situación en el RGIAJ mediante el SVJ, para que el jugador reciba una nueva comunicación por reactivación del servicio en ese operador.
- A atender adecuadamente las peticiones de información que realicen los jugadores respecto al uso de sus datos de identidad y que se deriven del procedimiento descrito a continuación.

4.4 Interacción con el servicio por parte de los ciudadanos

El usuario podrá realizar las operaciones de inscripción, modificación, baja o solicitud de informe de situación a través de los medios electrónicos y presenciales actualmente disponibles en la DGOJ:

- Modelo disponible en la sede electrónica de la DGOJ, cumplimentado, firmado y presentado en cualquiera de las oficinas de registro habilitadas para la presentación de escritos a las Administración General del Estado o en una oficina de Correos.
- Mediante la presentación de la solicitud en el registro electrónico de la DGOJ, firmada con DNI electrónico, certificado electrónico reconocido o a través del sistema Cl@ve.

En una fase posterior está previsto desarrollar una aplicación móvil que permita a los usuarios gestionar tanto el alta como el resto de funciones del servicio mediante el uso de dispositivos móviles.

Las comunicaciones generadas por el servicio se realizarán a través de la sede electrónica y en Carpeta ciudadana, y en su caso por vía postal, dependiendo de la selección realizada por el ciudadano en el momento de su registro. De forma adicional, se realizará un preaviso al correo electrónico proporcionado por el interesado en la solicitud.

4.4.1 Inscripción

Podrá solicitar el alta en el servicio cualquier persona mayor de edad, residente en España con DNI o NIE, tanto si está actualmente registrado en algún operador, como si no está registrado.

El interesado deberá aportar fotocopia del DNI/NIE (salvo en solicitud electrónica) conjuntamente con el resto de datos exigidos para verificar en SVJ (nombre, apellidos, fecha de nacimiento y número del documento de identificación del usuario).

La inscripción en el servicio se realizará de forma inmediata si se solicita por medios electrónicos. En el caso solicitud vía papel, se tramitará en un plazo máximo de 3 días hábiles desde su recepción en las oficinas de la DGOJ.

En el momento de inscripción en el servicio, se comunicará al ciudadano el alta en el servicio y se le remitirá un informe de situación para los operadores adheridos que hayan verificado su identidad correctamente hasta ese momento.

Phishingalert_informe_inscripcion.pdf

La inscripción en el servicio tendrá carácter indefinido, pudiendo el interesado solicitar su baja en cualquier momento.

4.4.2 Modificación del servicio

Los usuarios del servicio podrán modificar en cualquier momento por los medios anteriormente indicados el medio preferente para la realización de las notificaciones y los datos asociados a la misma.

4.4.3 Solicitud de informe de estado en el servicio

Los usuarios podrán solicitar el informe de su situación respecto al servicio.

En el informe se indicará si el usuario está inscrito o no en el servicio. En caso afirmativo, se le informará de su historial de inscripciones y cancelaciones, así como el conjunto de operadores que verificó su identidad de forma correcta en cada periodo de alta, indicando la fecha de consulta del operador al SVJ.

Asociado a cada operador se facilitarán los datos de contacto de la unidad de atención al cliente en materia de suplantación de identidad que hayan facilitado.

Certificado Persona Phishing

4.4.4 Baja en el servicio

En las solicitudes de cancelación, una vez comprobado que el solicitante está correctamente suscrito al servicio, se cancelará en el registro de "PhishingAlert". Además, se comunicará de forma automática al interesado el informe de situación en ese momento.

4.5 Funcionamiento de las alertas

En el momento en el que el operador de juego realiza la verificación de identidad de un solicitante a través del SVJ de la DGOJ, se cotejan sus datos con los de las personas inscritas en el Servicio de alerta: nombre, apellidos, fecha de nacimiento y número de identificación utilizado (DNI o NIE).

En caso de coincidencia de datos (solicitante de registro de usuario y persona inscrita en servicio alerta), la DGOJ comunica esa circunstancia al interesado inscrito en el servicio a través del medio elegido (sede electrónica, medios postales y en el futuro app móvil).

En la comunicación que recibe el interesado del servicio, se indicará que se dirija al operador para la resolución de las controversias que puedan derivarse del proceso de registro detectado.

Notificación por alta en operador

En ese caso, el operador deberá proceder a gestionar la solicitud del interesado, realizando las medidas que correspondan dependiendo de la comprobación material que se pueda realizar sobre la existencia de una posible suplantación de identidad.

4.6 Calendario de implantación

Tareas a ejecutar	Entrada en producción
Se mantiene la version del SVJ 2.4[3]	24/06/2019
Adaptación "Informe Datos Operador" ofrecido a operadores de juego con licencia estatal a través de la sede electrónica para incluir la información del servicio comunicada por el operador	24/06/2019

[3] *Funcionalmente el SVJ no cambia en relación al uso que tienen que hacer los operadores de juego con licencia estatal. Si bien internamente se realizarán los cambios necesarios para lanzar las alertas a los jugadores, se trata de una versión menor que no afecta al end-point del servicio.*

Adaptación del "Tramite Tasadas" de la sede electrónica para la gestión de la adhesión del operador al servicio	24/06/2019
Disposición pública de los trámites orientados a los interesados	15/07/2019
Adaptación servicios de la sede electrónica para soporte en movilidad	01/04/2020
Desarrollo de la app móvil[4]	01/04/2020

4.7 Posible evolución de servicio

Tal y como se ha descrito, el servicio de "PhishingAlert" se posiciona como un servicio de alerta ante posibles intentos de registro en operadores de juego utilizando las credenciales del interesado suscrito. En la línea de reforzar las medidas existentes para evitar la suplantación de identidad no deseada, así como superar las limitaciones en relación con el uso del RGIAJ en estos supuestos y que han sido detalladas en el apartado IV, el nuevo servicio de alertas por suplantación de identidad "PhishingAlert", completa las medidas regulatorias existentes como la necesidad de realizar una verificación documental de los participantes en el juego (ver apartado III Evolución de la Verificación de la identidad). De esa forma, para toda aquella persona suscrita en el servicio de "PhishingAlert", el proceso de registro en cualquier operador de juego online con licencia estatal debería requerir la realización del proceso de verificación documental, sin necesidad de diferirlo a situaciones de retirada premios o de realizar depósitos que de forma acumulada superen los 150€.

4.8 Análisis de las aportaciones recibidas desde la Sección Protección al Participante del CAJR

Con el propósito de la mejora de la definición y alcance del servicio, se procedió a circular el presente documento entre los miembros de la Sección de Protección al Participante del Consejo Asesor de Juego Responsable. Durante el plazo de recepción de observaciones, abierto entre el 14 y el 31 de mayo de 2019, se recibieron propuestas de cinco de los miembros de la sección. Adicionalmente, se recibieron manifestaciones de otros miembros de la sección en las que se indicaba la que la medida planteada suponía un avance en el incremento de la protección de la ciudadanía en su conjunto en relación al juego online.

[4] *El desarrollo de la aplicación móvil se realiza en colaboración con la Fábrica Nacional de Moneda y Timbre (FNMT)*

A continuación, se realiza un resumen de las propuestas de mejora recibidas y su valoración por parte de la DGOJ:

- **<u>Propuesta 1</u>: Posible no utilidad del servicio una vez esté plenamente operativo la verificación documental de participantes.**

  <u>Valoración:</u> Como se detalla en el apartado 3 de este documento, Evolución de la verificación de identidad, 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 viene a exigir la necesidad de verificar documentalmente a los participantes para acceder a la práctica del juego, restringiendo en caso contrario su actividad en las plataformas de juego (no podrán retirar premios ni realizar depósitos que de forma acumulada superen los 150€).

  El servicio de PhishingAlert está diseñado para actuar en el momento de registro en las plataformas de juego y, por tanto, de forma previa a cualquier actividad de juego que determine la necesidad de la realización de la verificación documental. Por ello se entiende que son dos medidas de carácter complementario.

- **<u>Propuesta 2:</u> Modificación del nombre, sustituyendo el actual "PhishingAlert" por "Alerta por Suplantación de Identidad" debido a "posibles confusiones de términos".**

  <u>Valoración:</u> El término "phishing" [5] es un concepto internacionalmente aceptado y ampliamente consolidado, asociado a aquellas prácticas donde un ciberdelincuente realiza procesos de suplantación de identidad. Por ello se considera adecuado mantener la utilización del término, sin perjuicio de incorporar de forma aclaratoria la dicción propuesta en el material que se elabore para su difusión.

[5] *https://es.wikipedia.org/wiki/Phishing: conocido como suplantación de identidad, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.*

- **<u>Propuesta 3:</u> Obligatoriedad de incorporación al servicio por parte de los operadores con licencia para comercializar juego online estatal.**

  <u>Valoración:</u> Se solicita que la medida sea de obligado cumplimiento para los operadores con licencia para comercializar juego online estatal y no de adhesión voluntaria tal y como se plantea en la definición del servicio.

  Previa a la valoración de la obligatoriedad de incorporación de la medida se considera necesario realizar una valoración de la evolución y funcionamiento del servicio, cuestión que por el momento no es posible dado que se trata de un nuevo servicio y se desconocen extremos tales como el grado de aceptación de la media, el número de consultas que se derivarían a los operadores o la casuística de las mismas. Por ello, en el acuerdo de adhesión de los operadores se incluirá como parte del alcance del servicio, el envío a la DGOJ antes de finalizar el primer trimestre de cada año, una memoria de análisis del impacto del servicio y su valoración. A la vista de los datos recibidos, así como del impacto del mismo en la población general en términos de número de inscritos, la DGOJ procederá a valorar su incorporación como servicio de obligado cumplimiento.

  No obstante, la DGOJ tiene previsto incorporar la adhesión al servicio PhishingAlert dentro del conjunto de requisitos a ser considerados para la obtención de un futuro distintivo en relación a la atención al participante y creado a tal efecto por la DGOJ. Dada la relevancia en términos reputacionales que puede tener para los operadores la obtención de dicho distintivo, así como la propia importancia que se deriva del servicio PhishingAlert, se espera que la adhesión al mismo tenga carácter mayoritario.

- **<u>Propuesta 4</u>: Centralizar en la DGOJ las posibles consultas de los ciudadanos.**

  <u>Valoración</u>: La necesidad de que sean los propios operadores los que puedan resolver las posibles consultas de los inscritos en el servicio se debe a que los mismos tienen a su disposición la información necesaria para resolver las situaciones que se planteen y proceder a comprobar de manera fehaciente si ha existido un caso de suplantación de identidad. Es necesario recordar que la DGOJ solo dispone de los datos de identificación y del dispositivo utilizado, mientras que los operadores disponen de otros adicionales que serán utilizables en el proceso de consulta derivado del servicio de PhishingAlert.

Adicionalmente, al objeto de verificar la concordancia entre el intento de registro y la identidad del interesado que comunica que no se debe a una acción suya, la DGOJ debería disponer de las herramientas (procesos de prueba de vida) y personal necesario para realizar esa tarea, así como la disponibilidad de un servicio de atención modo 24x7. Todo ello supondría un gran impacto en la organización de difícil justificación para un servicio del que se desconoce su grado de uso futuro. Por otro lado, es preciso recordar los operadores ya disponen de los mismos por cuanto la actual normativa en lo que a la verificación de identidad se refiere les obliga a ello.

Por otro último, aún en el caso de que la DGOJ detectase la existencia de la suplantación, en último término sería el operador el que debería realizar las acciones que se deriven de la misma, y en especial, el cierre de la cuenta de juego y finalización de la relación que le une con el participante. Dado que se trata de relaciones contractuales de carácter privado, esos procesos deben ser realizados conforme a lo contemplado en la normativa de juego y de defensa de los consumidores y usuarios.

- **Propuesta 5: Obligatoriedad de inscripción para determinados colectivos, como aquellos de edad avanzada, en el servicio PhishingAlert**

  Valoración: La inscripción obligatoria o automática en el servicio de PhishingAlert para determinados colectivos, debería operarse a través de una modificación normativa con rango de Ley, que además habilitase el intercambio de datos con determinados registros para con estos efectos.

  En todo caso, y más allá de que la modificación legal retrasaría la puesta en producción del servicio, se descarta esta opción por su potencial impacto sobre los derechos fundamentales de las personas afectadas.

- **Propuesta 6: Verificación documental fehaciente de la persona que solicita su inscripción en el registro**

  Valoración: Aunque se trate de un servicio administrativo, su funcionamiento práctico es asimilable a la de un procedimiento administrativo. De esa forma, la inscripción, modificación y baja requerirá la presentación de los documentos acreditativos de la identidad de solicitante y el cotejo de los mismos por parte de la DGOJ, tal y como se realiza en los trámites relacionados con el Registro General de interdicciones de Acceso al Juego (RGIAJ). Todo ello

sin perjuicio de que podrá realizarse de forma electrónica a través del uso de certificados digitales o medios análogos que aseguran la identificación y voluntad del solicitante.

- **Propuesta 7: Actualización de los datos de contacto**

  Valoración: Se solicita la inclusión de mecanismos de comunicación automatizados periódicos a los inscritos en el servicio como recordatorio para que, en el caso de que sea necesario, procedan a actualizar sus datos, de forma que en se asegure que en el caso de tener que realizar una comunicación por "PhishingAlert" se asegure que es recibida por el interesado inscrito en el servicio.

  Sin perjuicio de futuros análisis de coste en razón del número de inscritos en el servicio, se considera oportuna la inclusión de esta nueva funcionalidad. De esa forma, una vez pasado un año desde la inscripción, cada interesado recibirá una comunicación a través de los medios de contacto indicados en su solicitud informando del estado de su inscripción y de la necesidad de actualizar los medios de contacto en el caso de que hayan variado para asegurar la correcta recepción de las comunicaciones generadas por el servicio.