GUÍA PARA EL DISEÑO E IMPLEMENTACIÓN DE CANALES SEGUROS DE TRANSMISIÓN DE INFORMACIÓN SOBRE MANIPULACIÓN DE LAS COMPETICIONES DEPORTIVAS

1. Introducción

La Comisión Nacional para combatir la manipulación de las competiciones deportivas y el fraude en las apuestas (en adelante, CONFAD), creada por Orden PCI/759/2019, de 9 de julio, tiene por objetivo constituir un cauce formalizado de diálogo y cooperación entre autoridades públicas estatales, entidades deportivas y operadores de juego al objeto de prevenir y erradicar la corrupción y la manipulación de las competiciones y las apuestas mediante una actuación coordinada entre sus miembros.

Para ello, la CONFAD se configura como un espacio común de colaboración entre todos sus miembros, además de un elemento orgánico esencial en la lucha contra este tipo de prácticas fraudulentas. Este enfoque pluridimensional constituye, sin duda, un aspecto clave a la hora de determinar el modo en que la Comisión Nacional puede alcanzar sus objetivos.

El pasado 28 de julio de 2020, la CONFAD aprobó su plan nacional para el periodo 2020-2021, con cuatro grandes áreas de trabajo y el objetivo de abarcar un amplio espectro de actuaciones. Dentro del área de control y seguimiento, la medida número 4.3.4, "*Diseñar, o en su caso mejorar, canales seguros de transmisión de información sobre manipulación de las competiciones deportivas*", tiene por objetivo diseñar y definir los puntos de referencia a los que cualquier persona pueda dirigirse para transmitir información que pudiera ser relevante en relación con la manipulación de competiciones deportivas.

Esta medida responde a la creciente preocupación social en torno a un fenómeno que supone una de las mayores amenazas que se ciernen sobre el deporte, pues atenta contra sus valores esenciales y aleja de su entorno a aficionados y seguidores, además de afectar al normal desarrollo de las actividades relacionadas con el juego, menoscabando los intereses de sus participantes y de los operadores de este sector.

En este sentido, comprometerse con la integridad en el deporte y el juego regulado requiere de la existencia de marcos estructurados para informar, identificar y resolver los problemas e irregularidades que puedan producirse. Los mecanismos efectivos de recepción de información son esenciales para la lucha contra la corrupción en ambos sectores y, de hecho, pueden considerarse como una de las herramientas más importantes para la detección temprana del fraude; puesto que posibilitan la apertura de líneas de investigación esenciales y otorgan a los deportistas y al resto de los actores implicados la oportunidad de ser protagonistas en la salvaguarda de la integridad en el deporte.

Ahora bien, la consecución de este fin requiere la generación de un entorno adecuado de confianza y seguridad para quienes deseen colaborar en la persecución de estas prácticas antideportivas, entorno en el que se garantice la adecuada recepción de la información por parte de las autoridades competentes. La creación de canales seguros y confidenciales de transmisión de la información, facilitará que la información pueda ser conocida en las instancias oportunas y contribuirá a reforzar el mensaje claro y unívoco de que la corrupción en el deporte no será tolerada.

2. Objeto y finalidad de la guía

El objeto de esta guía es la descripción del procedimiento para el tratamiento de las comunicaciones relativas a hechos que puedan suponer una infracción de las normas nacionales o internacionales del deporte o de las apuestas deportivas, o que menoscaben la integridad y ética en el deporte.

En particular, esta guía busca proporcionar las pautas orientativas que faciliten a aquellas organizaciones interesadas, el establecimiento de un canal seguro de transmisión y evaluación de la información, la posible investigación consiguiente, el redireccionamiento de los resultados obtenidos a la instancia adecuada, y el cierre de las actuaciones, todo ello en el marco del respeto a la debida confidencialidad.

No tiene por fin esta guía proporcionar una pauta para la determinación e implantación de las acciones reguladoras o sancionadoras que pudieran derivarse de las comunicaciones recibidas, una vez comprobados los hechos.

El establecimiento de un canal de transmisión y recepción de información resulta recomendable no sólo para las organizaciones deportivas, sino también para los operadores de juego que comercialicen modalidades de juego vinculadas a este tipo de actividades y para la propia autoridad reguladora del juego.

Asumiendo la dificultad que el establecimiento de estos mecanismos puede suponer para cualquier organización, este documento pretende servir de guía para su efectiva puesta en práctica, mediante un enfoque sencillo y lo suficientemente abierto como para abarcar la heterogeneidad organizativa de sus potenciales destinatarios.

En este sentido, debe subrayarse que la ya larga experiencia de ciertas organizaciones con sistemas de este tipo ha evidenciado su extraordinaria utilidad.

Se trata, en definitiva, de proporcionar un recurso que, a modo de guía de mínimos, pueda ser fácilmente utilizada por cualquier tipo de organización independientemente de sus características, bien para el establecimiento de un canal de información, bien para la adopción de buenas prácticas en aquellas que ya lo pudieran haber establecido, y que permita su adaptación a las singularidades de cada cual, tanto por razón de su actividad, del sector en el que operen, de la naturaleza de sus miembros, de su tamaño, o de cualquier otra especificidad.

Por último, ha de señalarse que todas las menciones contenidas en este documento deben entenderse realizadas con pleno respeto y sin menoscabo de la normativa vigente en la actualidad, y, en particular, de la referida al deporte, el juego regulado y la protección de datos de carácter personal.

3. Principios generales en la implantación de canales seguros de transmisión de la información

Cualquier organización involucrada en la lucha contra el fraude deportivo o en las apuestas, a la hora de tomar la decisión de implantar un canal seguro de transmisión de información[1], debiera orientar esta decisión con base en los siguientes principios:

1. Compromiso de las organizaciones.

   Este mecanismo no puede ser implantado con éxito sin el obligado compromiso de la organización, lo cual requiere la implicación de los máximos órganos decisorios, así como la aportación de los recursos humanos, materiales y económicos suficientes, y la participación de personal cualificado.

   Además del apoyo de la cúpula de la organización, el canal de transmisión debe estructurarse de tal forma que cuente con procedimientos conocidos, que incluyan una clara asignación de responsabilidades, y vías de comunicación con otras instancias y con el informante.

2. La confidencialidad de la información y la protección del informante.

   Las organizaciones velarán porque no se revele la identidad del informante, sin su consentimiento expreso, a ninguna persona que no sea un miembro autorizado de la autoridad destinataria competente para el seguimiento y recepción de las informaciones, tanto dentro de la organización como fuera de la misma; también velarán porque no se revele la identidad de aquellos terceros que aparezcan en la información suministrada.

[1] Sin perjuicio de lo establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el establecimiento por una organización de carácter privado de un canal de transmisión de información, y la gestión de sus datos, tiene su fundamento jurídico en lo establecido en el artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGD), en cuyos dos primeros párrafos establece lo siguiente:

"Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.

El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos".

Lo anterior también se aplicará a cualquier otra información de la que se pueda deducir directa o indirectamente la identidad del informante o de cualquier tercero mencionado. En este sentido, se establecerán protocolos para la protección de la persona informante, considerando como tal cualquier persona física o jurídica que comunique hechos que puedan lugar a la existencia de responsabilidades administrativas, penales o disciplinarias.

En este sentido, puede considerarse información confidencial cualquier dato que permita conocer la identidad de las personas físicas o jurídicas que pongan en conocimiento de la organización cualquier incumplimiento de la normativa en la materia objeto de esta guía, incluyéndose datos como nombre y apellidos, DNI o documento análogo, dirección postal o electrónica, IP, u otros que permitan una identificación de la persona física o jurídica. En particular, tendrá esa consideración, el propio hecho de la existencia de una comunicación, así como la naturaleza y detalles de los hechos comunicados.

En cualquier caso, aquellas circunstancias que permitieran la flexibilización o incluso el decaimiento de las medidas relativas a la confidencialidad del informante, por ejemplo, y sin ánimo de exhaustividad, las derivadas de haber comunicado o hecho público éste la información, deberán estar predeterminadas por la organización y ser advertidas expresamente al potencial informante.

En el caso de ruptura de la confidencialidad, y con independencia de la persona a la que sea imputable la misma, la organización velará para que estas personas no sufran, ni durante ni después de la investigación, ningún tipo de aislamiento, persecución o empeoramiento de sus condiciones laborales o profesionales, ni ningún tipo de medida que implique cualquier forma de perjuicio o discriminación. Si la organización es conocedora de que estos hechos se están produciendo, ejercerá las acciones que estén a su alcance para el cese de los mismos y el restablecimiento del informante en su situación inicial.

3. Confianza, integridad y seguridad del sistema.

La eventualidad de que un sujeto conocedor de un hecho susceptible de constituir corrupción en el ámbito deportivo o de fraude en el de las apuestas tome la decisión de ponerlo en conocimiento de la organización depende en gran medida del grado de confianza que deposite en los canales de información a su disposición. De ahí que la organización haya de realizar un esfuerzo en trasladar la plena confiabilidad y seguridad del sistema, especialmente desde la perspectiva de la garantía de la confidencialidad, tanto por la adecuación de los protocolos y sistemas informáticos frente a brechas de seguridad como por la estructuración del mismo. Para ello, la organización debe potenciar la transparencia en cuanto a los mecanismos mediante los que asegura esta confidencialidad, así como la percepción de su actividad por los potenciales informantes como íntegra y ética, sobre todo por parte de sus máximos órganos decisores.

4. Imparcialidad.

   Los criterios que adopte la organización en el momento de procesar, investigar, y comunicar a las autoridades competentes, en su caso, los hechos informados, deben ser objetivos, preestablecidos y transparentes, asegurando que no existen interferencias ni influencias indebidas. En particular, la persona o departamento responsable del tratamiento de la información deberá contar con las herramientas necesarias para asegurar esa ausencia de interferencias e influencias, lo que implica la necesaria independencia en la organización, y la suficiente formación.

5. Difusión.

   Tanto los empleados de la organización, como posibles destinatarios del canal y otros terceros, deberán ser informados acerca de la existencia de estos sistemas de información, así como de la forma de acceso a los mismos.

4. Las características básicas de los canales seguros de transmisión de la información y la información suministrada al potencial informante

Atendiendo a las capacidades, recursos económicos, humanos y técnicos disponibles, toda organización debe hacer una valoración de cuál o cuáles sean los canales más idóneos para el suministro de información relacionada con posibles manipulaciones de competiciones deportivas.

Así, existe una variada tipología de canales disponibles: oficinas de atención presencial, llamadas telefónicas atendidas, llamadas telefónicas grabadas, correo electrónico, plataforma online, o aplicación de móvil.

En cualquier caso, todos los canales, cuando sean más de uno, deben asegurar que la información llega al mismo destino y es procesada uniformemente, garantizando, de manera adecuada a la naturaleza del canal, su seguridad y confidencialidad.

4.1. Las características básicas de los canales seguros de transmisión de la información.

Sin perjuicio de la opción escogida, existen una serie de aspectos y características de los distintos canales que toda organización debiera tomar en consideración en la implementación de un mecanismo de esta naturaleza:

- Disponibilidad 24X7: la permanente disponibilidad del canal es una característica muy relevante ya que remueve los obstáculos estructurales que dificultan o impiden a la persona que ha decidido revelar hechos susceptibles de reproche de cualquier naturaleza, dar ese paso en cualquier momento. De esta forma, es recomendable la existencia de, por lo menos, un canal que permita su acceso 24 horas al día, siete días a la semana.
- Interacción personal: la decisión de revelar hechos susceptibles de reproche y las consecuencias derivadas de su puesta en conocimiento puede suponer para algunas personas, en función de la relación que guarden con el conocimiento de los mismos, una situación crítica o difícil que se traslade a su propio ámbito personal. Desde esta perspectiva, es recomendable que, en algún momento del proceso, tanto el público destinatario potencial como aquellos que se hayan constituido en informantes, tengan conocimiento de que tienen la posibilidad de interactuar de forma directa con las personas responsables del tratamiento de su información.
- Secreto de la comunicación: las comunicaciones deberán quedar encriptadas, y en el caso de las llamadas de teléfono, se asegurará que no aparece el número del informante.

- Suministro de información adecuada y suficiente para todos aquellos que quieran revelar información: en el diseño del canal de información debe prestarse una especial atención al contenido informativo que se destine al público objetivo de cada organización, de forma que, en función de cuál sea éste y atendiendo a sus intereses, la información proporcionada resulte útil para todos aquellos que se encuentran en la disyuntiva poner en conocimiento hechos relevantes.

4.2. El suministro de información al público objetivo.

La recepción de una información fiable y que permita un tratamiento eficiente y eficaz por la organización destinataria está en relación directa con la calidad y cantidad de información que se ponga a disposición del público objetivo de la organización, que comprenderá su universo de potenciales informantes, con carácter previo a su interacción con el canal.

En este sentido, una adecuada y suficiente puesta a disposición de esta información debiera abordar, como mínimo, las siguientes cuestiones[2]:

- Cómo presentar la comunicación, y qué información concreta es relevante para la organización destinataria.
- Cómo se va a gestionar la comunicación, incluyendo todos los aspectos relevantes en cuanto a la seguridad en su tratamiento.
- Cuáles son las diferencias en la gestión de la información proporcionada de manera anónima y nominativa.

Además, en el caso particular de las comunicaciones nominativas, los potenciales informantes debieran estar en disposición de conocer:

- La forma en que se les va a responder, así como el plazo, y la información que van a recibir en relación con los diversos hitos del procedimiento. Particularmente, se le indicará la manera en que podrá volver a comunicarse con la organización en el futuro.
- Lo que la organización va a ofrecer, o poner a disposición, del potencial informante. Puede tratarse de cuestiones relacionadas con la política de privacidad y la confidencialidad de sus datos, con el tipo y periodicidad de la información que va a recibir, con la tutela que puede esperar obtener (por ejemplo, si se le va a ofrecer algún tipo de asesoramiento legal), o, finalmente, con la extensión, material y temporal, de la protección que pueda recibir.
- Las medidas que se van a llevar a cabo para asegurar la confidencialidad de su comunicación, así como la protección de su integridad.
- Las circunstancias relacionadas con el tratamiento de sus datos personales y la posibilidad de ejercer los derechos que le asisten de acuerdo con el Reglamento General de Protección de Datos (en adelante, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGD).

[2] Véanse dos buenos ejemplos en las páginas web https://ioc.integrityline.org/ y https://integrity.worldrugby.org/index.php.

En aquellos casos en los que la información proporcionada provenga de fuentes anónimas, deberá advertirse al potencial informante de los siguientes aspectos:

- Que se asegure de que la información que proporciona no permita la trazabilidad hacia su persona, incluyendo la recomendación de adopción de medidas para la ocultación de su dirección IP.
- Que utilice una conexión internet segura, con el símbolo de bloqueo en el navegador.

Especialmente en los canales informáticos (web y app), y en la medida de lo posible en el resto, es importante que se proporcione un formulario, estandarizado y estructurado, que oriente al informante sobre el contenido y forma de presentación de la información, y, en particular, que aborde los siguientes aspectos[3]:

1. En cuanto al tipo de información, habrá de comenzar catalogando qué es lo que se quiere comunicar. Para ello, es recomendable que el formulario comience con un listado cerrado de hechos susceptibles de infracción, para que el informante elija necesariamente uno de ellos, y con ello realice una primera orientación de la categorización de la información que proporciona.
2. Se le ofrecerá al informante, a continuación, unos apartados para que rellene sus datos personales (nombre y apellidos) y de contacto (correo electrónico y teléfono), además de un campo donde el informante puede pedir recibir comunicaciones, informando de la vía para hacerlo. En este punto se consignará un apartado ofreciendo la posibilidad de que la aportación de información sea anónima, que deshabilitaría la necesidad de incluir los datos anteriores.
3. En relación con los sujetos intervinientes, se puede preguntar sobre la organización o club al que pertenece el informante, su ciudad y país de residencia, por un lado, así como informaciones acerca de la persona o entidad sobre la que pretende informar y su ciudad y país de residencia (y algún dato de contacto, si lo tuviera). Podrá consignarse una petición de información sobre si tiene noticia de que alguien más conociera de esas informaciones, aun sin estar involucrado.
4. Es importante habilitar un buen conjunto de campos para la introducción de la información descriptiva de los hechos (qué pasó, cuándo y dónde). Adicionalmente, son relevantes los datos relativos al deporte y competición afectada (incluyendo el evento concreto), así como acerca del mercado del juego y las apuestas realizadas.
5. Si los hechos siguen desarrollándose actualmente, o considera razonablemente que pueden volver a ocurrir en el corto o medio plazo.
6. Si posee alguna prueba de lo informado y, en caso afirmativo, una descripción de la misma.
7. Se le ofrecerá la posibilidad de cargar documentos.
8. Debe valorarse la posibilidad de ofrecer un campo abierto, que permita al informante reflejar cualquier otra cuestión que a su juicio sea relevante.

[3] Cfr. https://ioc.integrityline.org/

Antes de habilitar su envío, el informante deberá asegurar la veracidad de las informaciones y aceptar su responsabilidad en el caso de comunicación falsa o de mala fe. Además, se le informará de la política de privacidad. El establecimiento de un canal de estas características requiere para su efectividad del mayor grado de conocimiento por los potenciales destinatarios, por lo que cada organización que decida su puesta en práctica, debe prever la adopción de las medidas más idóneas para la difusión de su existencia y la promoción de su uso entre sus asociados. Para ello, contactará, en la medida de lo posible, con éstos, realizará campañas de sensibilización y programas formativos.

5. El proceso de tratamiento de la información recibida

Toda organización, en el diseño del proceso de tratamiento de la información recibida, debería tener en cuenta, con las necesarias adaptaciones en función de sus singularidades y en ejercicio de su autonomía organizativa, las siguientes fases:

a) Recepción de la comunicación y remisión al responsable asignado;

b) Evaluación;

c) Investigación;

d) Direccionamiento;

e) Cierre del caso;

f) Aprendizaje del proceso - Retroalimentación

PASOS A REALIZAR	DESCRIPCIÓN
RECEPCIÓN Y REMISIÓN	Se recibe en alguno de los canales y se remite al responsable
REGISTRO	Se registra en la aplicación informática
EVALUACIÓN*	Se hace una evaluación inicial, diferente si es nominativa o anónima
INVESTIGACIÓN	En el caso de que sea necesaria
REDIRECCIONAMIENTO*	Se remite a la autoridad competente
CIERRE DEL CASO*	Cuando ya esté resuelto en la organización o redireccionado al competente, con consentimiento de éste
APRENDER DEL PROCESO	Retroalimentación, posibilidad de tomar acciones correctoras y preventivas
GESTIÓN DOCUMENTAL	Tomar medidas de protección de datos, supresión de los mismos
* Tras estos pasos se informará de los mismos al informante, si se conocen sus datos	

Se describen a continuación los principales hitos de cada una de ellas.

a) Recepción de la comunicación y remisión al responsable asignado.

- Acuse de recibo: en primer lugar, se acusará recibo de la información recibida[4], siempre y cuando se trate de una comunicación nominativa y, por tanto, conste la identidad del remitente. Se asignará un número de registro y se le informará del plazo dentro del cual se le comunicarán los pasos que se van a llevar a cabo, los cuales pueden también ser explicados en esta misma comunicación.
- También deberá informarse acerca de dónde y cómo puede comunicarse otra vez sobre la misma cuestión, y de qué forma. En este caso concreto, una buena práctica es establecer un registro particular de comunicación, asignándole un usuario y contraseña para que pueda acceder nuevamente a la misma para modificarla, añadir información o cualquier otra cuestión que quisiera trasladar a la organización.
- Los mismos canales de protección se podrán utilizar, por los que ya hayan actuado como informantes, para comunicar represalias u otras actuaciones lesivas derivadas del envío de la información.
- En la medida que los medios disponibles lo permitan, puede valorarse la posibilidad de ofrecer asesoría legal en relación con consultas concretas que pueda plantear el informante sobre hechos relacionados con la información remitida.
- Debe decidirse, en este momento, la persona responsable de la comunicación con el informante, y las medidas de confidencialidad que se van a adoptar, así como acerca de la forma en que se va a clasificar la información.
- En particular, respecto a la designación del responsable: la responsabilidad quedará claramente delimitada, asignándose a una sola persona o departamento, para mayor protección de la confidencialidad. Esta persona o departamento se ocupará de todas las fases, registrando cada novedad en la aplicación informática, asegurando la confidencialidad e integridad de la información, y manteniendo los contactos que sean necesarios con el informante y con el resto de personas que queden involucradas en el procedimiento.
- Se garantizará la independencia orgánica y funcional del responsable del procedimiento, y se le dotará de las herramientas necesarias, dentro de las posibilidades que determine el tamaño y estructura de cada organización.

[4] Un posible modelo de acuse de recibo lo ofrece el documento "Reporting Mechanisms in Sport – A practical guide for development and implementation", United Nations Office on Drugs and Crime (UNODC) and International Olympic Committee:

"Le escribo para comunicarle la recepción de su información sobre…

Gracias por comunicar con nosotros y por la información recibida. Intentaremos responderle en el plazo de 10 días. Es posible que tengamos que hablar con usted en algún momento del proceso. Mientras tanto, si tiene alguna otra información que añadir o una cuestión de cualquier tipo, por favor no dude en contactarme de nuevo.

Desde este mismo momento tiene usted garantizada la confidencialidad de sus datos. Esta organización tratará la información con la máxima diligencia y velará, en toda ocasión, porque se mantenga la protección en la integridad de su persona".

b) Evaluación.

- Análisis preliminar de la información:

  Recibida la información, y con carácter previo a la a su evaluación material, procede realizar una serie de actuaciones previas, relacionadas con la urgencia del asunto, la posible necesidad de información adicional, la existencia de comunicaciones previas relacionadas (y que, por tanto, puedan requerir de una valoración conjunta), las condiciones subjetivas del informante en caso de conocer sus datos, y la posible necesidad de adoptar precauciones suplementarias ante el riesgo de ruptura de la confidencialidad o de potenciales represalias, derivados de las características del caso.

  Este análisis preliminar incluirá una primera determinación de las posibles responsabilidades – penales, administrativas, disciplinarias o cualquier otra - a que pudieran dar lugar los hechos comunicados, o, en caso de no apreciarse la concurrencia de ninguna, debe derivar en el cierre del caso.

  Se fijarán también, desde este primer momento, las medidas técnicas y organizativas concretas necesarias en relación con la política de privacidad.

  Finalmente, deberá asegurarse, desde este momento, y en todo el proceso, la presunción de inocencia de las personas objeto de la comunicación.

- Proceso de verificación:

  En el caso de comunicaciones anónimas, el inicio de actuaciones por parte de la organización solo se producirá cuando se haya comprobado la existencia de indicios razonables de veracidad de los hechos o las conductas que hayan sido objeto de las mismas.

  En el supuesto de las comunicaciones nominativas, si hubiera dudas sobre la verosimilitud de las mismas, o si se considerara que de los hechos comunicados no se puede derivar responsabilidad alguna, se pondrá de manifiesto al informante para que alegue lo que estime conveniente, tras lo cual se decidirá si se continúan las actuaciones o se cierra el caso. Ambas posibilidades serán comunicadas al informante.

  Todo proceso de verificación de la información debe realizarse mediante un análisis sólido y sistemático, que contendrá parámetros de evaluación en diversas áreas, como la fiabilidad de la fuente, la validez de los datos, o la sensibilidad potencial de los mismos[5].

- Adopción de medidas urgentes:

  En caso de que la naturaleza de la comunicación requiera una actuación urgente, el responsable propondrá a las entidades competentes la adopción de las medidas necesarias.

[5] Véase, como ejemplo, el sistema 5x5x5, utilizado por la Unidad de Inteligencia de Apuestas Deportivas del Reino Unido: http://ukcrimeanalysis.blogspot.com/2010/11/5x5x5-system.html.

c) Investigación.

En esta fase deberán valorarse los riesgos que las actuaciones de investigación pudieran tener en la protección de la confidencialidad del informante, al ser este un momento especialmente delicado.

Con carácter previo a toda investigación, y en el supuesto de que el informante sea conocido, es fundamental averiguar si éste ha hablado con alguien más de los hechos comunicados.

Las comunicaciones anónimas deben ser estar sujetas a determinadas condiciones, referidas, específicamente, a la mayor velocidad e intensidad con que deben investigarse, así como a la necesidad de un examen exhaustivo, con especial precaución, con la finalidad de evitar el riesgo de mal uso.

Lo importante en este momento es mantener la confianza del informante y el espíritu de colaboración proactiva. En particular mediante el mantenimiento de una comunicación bidireccional con el mismo, informando de las actuaciones realizadas, cuando sea posible, y permitiendo a aquél la posibilidad de seguir enriqueciendo su comunicación mediante el uso de su registro particular de comunicaciones.

d) Redireccionamiento.

En función del resultado de las actuaciones de investigación, se adoptarán, en su caso, las decisiones de redireccionamiento de la información a las autoridades competentes, en atención a la naturaleza de los hechos investigados.

Serán destinatarias de dichos datos las autoridades competentes para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan, así como el personal con funciones de gestión y control de recursos humanos solo cuando proceda la adopción de medidas disciplinarias contra un trabajador.

Para la remisión de la información se articulará un expediente que contendrá el contenido de la comunicación, los resultados de las investigaciones llevadas a cabo, las comunicaciones sucesivas mantenidas con el informador, así como cualquier otro dato que se estime importante.

En todo caso, deberán minimizarse los datos que se van a compartir, que deberán ser los estrictamente necesarios.

Por otro lado, si se considerara que no hay lugar a más actuaciones que practicar, se cerrará el caso con indicación motivada al informante.

e) Cierre del caso.

Independientemente del resultado de la investigación y las acciones adoptadas, se remitirá comunicación motivada al informante.

Se deberán aplicar, en este momento, todas las medidas de protección de datos personales a las que se ha aludido más atrás, incluida la supresión de los datos, salvo que sean necesarios por estar en curso una investigación, y mientras dure ésta.

f) Retroalimentación. El aprendizaje del proceso.

La experiencia e información acumulada en el proceso de gestión de comunicaciones es un activo importante que puede servir en el tratamiento de futura información. Para ello, resulta posible mantener en el sistema de forma anonimizada la información de casos cerrados, lo que permitirá conformar un fondo documental estructurado en la organización, con el fin de ayudar en futuros casos, especialmente en materia de prevención, mejora del sistema y conocimiento de las actividades ilícitas.

También puede utilizarse esta información para conocer dónde deben dirigirse los esfuerzos preventivos o dónde prestar más atención (por ejemplo, en competiciones determinadas, deportes concretos, etc.).

Cada cierto tiempo, además, es conveniente realizar una evaluación del sistema, para mejorar materias como el canal de acceso, la evaluación inicial, la clasificación, los medios de investigación o las comunicaciones con los informantes.

6. Sobre la información gestionada por el canal y la protección de los datos de carácter personal

Toda la información y documentación que se reciba, además de la que se genere en el proceso de tratamiento, incluidas las notificaciones al exterior, así como los datos relativos a las actuaciones de la organización, se cargará y referenciará por el responsable designado en una aplicación informática, aplicándose en su caso las medidas que correspondan en función de la confidencialidad.

Tendrán acceso a la información contenida en la aplicación, tanto el responsable designado, como otras personas que, en función de sus competencias, se determinen expresamente. Todo acceso a la información que obre en el sistema deberá producirse con un sistema de verificación de la identidad que requiera nombre de usuario y contraseña, y que permita su registro y su trazabilidad[6].

La organización estará obligada a garantizar la confidencialidad de los datos personales de los informantes, y seguirá las indicaciones previstas por la normativa de protección de datos de carácter personal, en particular las contenidas en el Reglamento General de Protección de Datos[7] y la LOPDGD.

La transmisión de información puede implicar tratamientos de datos personales que encuentra su fundamento en el art. 6.1.e) del RGPD, esto es, en que el tratamiento es necesario para el cumplimiento de una misión realizada en interés público, con base jurídica en el artículo 24, relativo a los sistemas de información de denuncias internas de la LOPDGD.

En particular, el párrafo 3 del artículo 24 de la LOPDGD establece lo siguiente:

> "*Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.*
>
> *En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.*

[6] En todo caso se recuerda expresamente que, de conformidad con lo dispuesto en el artículo 24 de la Ley Orgánica 3/2018, el acceso a la información en la que obren datos de carácter personal "*quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.*"

[7] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme al apartado 2 de este artículo, la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas".

La responsabilidad de dicho tratamiento, a los efectos del RGPD, recae en la organización que implanta el canal o los canales de información, siendo interesados las personas físicas comunicantes y terceros afectados, y los datos personales a tratar identificativos y de contacto.

De conformidad con lo que dispone el artículo 24.2 de la LOPD, el acceso a los datos quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad que ha implantado este canal, desarrollen las funciones de control interno y de cumplimiento, o a los encargados de tratamiento que eventualmente se designen a tal efecto. Además, pueden ser destinatarios de dichos datos, con base a los presupuestos establecidos en este documento, las autoridades competentes, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan, y el personal con funciones de gestión y control de recursos humanos solo cuando proceda la adopción de medidas disciplinarias contra un trabajador.

Esta información descriptiva del tratamiento deberá constar en el Registro de Actividades de Tratamiento de la organización, así como en la información facilitada a los informantes nominativos en el momento de presentar la comunicación, en ambos casos de conformidad con los artículos 13 y 30 del RGPD, respectivamente.