Política de Principios de actuación y Protocolo de Gestión del Canal Ético de ZENITH BR MEDIA S.A. (Sistema Interno de Información)

AUTOR: Equipo externo de compliance	REVISADO POR: Comité de Cumplimiento	APROBADO POR: Órgano de Gobierno
Fecha: 04/2026	Fecha: 05/2026	Fecha: 21/05/2026

Control de versiones

Versión. Revisión	Fecha aprobación	Modificaciones
1.0	24/04/2025	Edición del documento
2.0	21/05/2026	Se incluye una aclaración respecto a las represalias, añadiéndose que se refiere a conductas perjudiciales.

1. Preámbulo

El presente documento recoge los Principios de Actuación y el Protocolo de Gestión del Canal Ético – Sistema Interno de Información (en adelante, "el Protocolo") de **ZENITH BR MEDIA, S.A.** (en adelante, *ZENITH BR* o *la Organización*) constituye la guía de actuación de la Organización ante el conocimiento de la presunta comisión de un delito o irregularidad administrativa grave o muy grave, así como ante cualquier posible infracción del derecho de la Unión Europea (p.e: fraude de subvenciones, infracción del derecho de la competencia, evasión fiscal, etc).

A través del presente Protocolo, queda expresamente establecido cómo gestionar la información o denuncias recibidas, qué decisiones se deberían adoptar y qué proceso de investigación se debería llevar a cabo, tanto desde una vertiente pre-procesal como también desde la eventualidad de un procedimiento penal dirigido contra la Organización.

El presente Protocolo pretende dar cumplimiento al Código Penal vigente, así como a los estándares nacionales e internacionales en materia de Compliance (UNE 19601 y UNE ISO 37301, por ejemplo), la Directiva (Unión Europea) 2019/1937 de 23 de octubre de 2019 relativa a la protección a los denunciantes y la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

El Protocolo actúa como parte de la cultura de cumplimiento implantada en nuestra Organización.

En ZENITH BR no barajamos otra opción ante informaciones relacionadas con la presunta comisión de un delito, que la denuncia, la colaboración con las autoridades y la reparación e indemnización del daño causado, sin dejar de tener en cuenta los derechos y garantías constitucionales que asisten a la Organización y a todos sus Consejeros, Administradores, Altos Directivos y Empleados/as.

Por último, este Protocolo se fundamenta en el deber de información y colaboración inherente a todos los Consejeros, Administradores, Altos Directivos y Empleados/as de la Organización ante cualquier presunta incidencia, incumplimiento o irregularidad.

El Protocolo se estructura en tres partes:

1. Disposiciones generales.

2. Protocolo de actuación pre-procesal.

3. Protocolo de actuación procesal, en caso de que ya exista un procedimiento penal que se dirija contra la Organización.

2. Disposiciones generales

Principios de actuación que rigen nuestra Política del Canal Ético

1. Principio de Independencia y Autonomía del Responsable del Sistema

2. Principio de Eficiencia a nivel de herramienta y de gestión

3. Principio de Tolerancia cero ante incumplimientos

4. Principio de Confidencialidad y Anonimato

5. Principio de Objetividad, Neutralidad y Honradez

6. Principio de Prohibición de Represalias, conductas perjudiciales o de medidas negativas contra la persona que denuncia o informa

¿Quién queda protegido bajo el alcance del presente protocolo en el uso del canal?

Los trabajadores (presentes y antiguos, así como trabajadores en prácticas o en formación) de ZENITH BR, así como aquellos terceros con los que mantiene relación (proveedores, contratistas, subcontratistas, administradores, clientes, personas en proceso de selección, personas que presten asistencia a los informantes, representantes legales de los trabajadores y sus entornos, empresas propiedad del informante o en las que tenga una participación influyente, accionistas y miembros de los órganos de administración, etc.).

¿Qué tipo de cuestiones pueden comunicarse a través del canal?

Informaciones / comunicaciones sobre cuestiones que puedan suponer un riesgo de comisión de un ilícito penal (delitos), infracciones administrativas graves o muy graves (por ejemplo, en cuestiones relativas a la Hacienda Pública o la Seguridad Social) e infracciones del derecho de la Unión Europea (por ejemplo, en cuestiones relativas al derecho de la competencia, impuestos o a los intereses financieros).

De conformidad con la Ley 2/2023, de 20 de febrero, el Sistema Interno de Información tiene por objeto exclusivamente la comunicación de este tipo de infracciones, quedando por tanto fuera de su alcance aquellas cuestiones que no encajen en dicho ámbito. Lo anterior se entiende sin perjuicio de que cualquier información recibida será analizada preliminarmente por el Responsable del Sistema a efectos de determinar su correcta clasificación y canalización.

Asimismo, podrán canalizarse consultas relacionadas con estas materias.

Las cuestiones relativas a posibles situaciones de acoso, sean del tipo que sean y dado su carácter delictivo y las posibles implicaciones en la responsabilidad penal de la empresa, serán gestionadas conforme al Procedimiento de Prevención del Acoso existente en la compañía. De igual forma, el equipo responsable de aplicar el Procedimiento de Prevención del Acoso deberá estar en permanente comunicación con el Responsable del Sistema al que deberá informar por escrito de todas las cuestiones relacionadas con el expediente, desde la incoación del mismo hasta el cierre del expediente.

Los meros conflictos laborales o quejas de empleados serán redirigidos al área de Recursos Humanos, o a quien desempeñe dicha función a nivel interno, para su resolución, informando que el canal de denuncias no es la vía correcta, no siendo por tanto el Responsable del Sistema la función responsable de estas cuestiones.

Las posibles quejas de clientes serán redirigidas al área de Atención al Cliente, o a quien desempeñe dicha función a nivel interno, para su resolución informando que el canal de denuncias no es la vía correcta, no siendo por tanto el Responsable del Sistema la función responsable de estas cuestiones.

Garantías del denunciante / informante

Destacan:

- seguridad de la información, anonimato y la confidencialidad de las comunicaciones.

- seguimiento de lo comunicado y derecho a estar informado

- correcta gestión de los posibles conflictos de interés por la organización

- opción de indicar un domicilio "seguro" a los efectos de las posibles notificaciones que sean necesarias intercambiar.

Asimismo, el informante que comunique una posible irregularidad, la cual sea comunicada a las autoridades competentes tras la investigación pertinente, será sujeto de las **medidas de protección** siguientes:

- Información y asesoramiento completos e independientes, fácilmente accesibles y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias / conductas perjudiciales, y derechos de la persona afectada.

- Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.

- Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante, A.A.I. tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

- Etc

Por último, la principal garantía que ampara al informante es la prohibición absoluta de toma de represalias / conductas perjudiciales de cualquier tipo contra el denunciante de buena fe. Tendrán la consideración de represalia:

- Suspensión, despido o extinción de contrato

- Daños reputacionales

- Intimidación

- Acoso

- Referencias negativas

- Discriminación o trato desfavorable o injusto

- Degradación o denegación de ascensos

- Modificación sustancial de las condiciones de trabajo

- Denegación de formación o de una licencia o permiso

- Medidas disciplinarias de cualquier tipo

- Etc.

Todo lo anterior aplica, salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.

ZENITH BR velará por evitar cualquier tipo de represalia / conducta perjudicial sobre quienes hubieran planteado de buena fe sus comunicaciones. Se considera que el informante actúa de buena fe cuando tenga motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o ésta se base en indicios de los que razonablemente pudiera desprenderse la existencia de un incumplimiento de la normativa interna o externa, o cualquier otra materia bajo el ámbito de aplicación de este Protocolo.

En caso de sufrir represalias / conductas perjudiciales, se deberá informar inmediatamente al Responsable del Sistema interno de información. El Responsable del Sistema realizará una investigación y seguimiento periódico de la situación del informante y, en su caso, de aquellas personas incluidas en el régimen de protección. Si el Responsable del Sistema constatase que durante la vigencia del régimen de protección se han adoptado represalias, estigmatización o vejación además de las medidas disciplinarias y/o sanciones administrativas que pudieran resultar de aplicación a los autores, se adoptarán las medidas necesarias y disponibles para restituir al represaliado a la situación previa al perjuicio sufrido.

Garantías del denunciado / parte afectada

Las personas que hayan sido denunciadas a través del Canal nunca podrán ser penalizados por una simple notificación, siendo, en todo caso, necesario que se compruebe previamente la veracidad de la comunicación y se conceda a las personas implicadas la oportunidad de ofrecer una explicación a la situación denunciada.

Se garantizará siempre y en todo caso la presunción de inocencia y el derecho al honor y a la intimidad de la persona afectada.

Las personas denunciadas serán informadas tan pronto como sea posible de los hechos que se le atribuyen. Excepcionalmente, si existe riesgo importante de que la notificación al denunciado ponga en peligro la eficacia de la investigación o recopilación de pruebas, no se procederá a la notificación hasta que cese dicho riesgo. Todo ello alineado con lo indicado relativo a protección de datos que se detalla con posterioridad. En ningún caso se le comunicará a la persona afectada la identidad del informante.

Del mismo modo, la información relativa a la persona afectada (denunciada) se tratará con estricta confidencialidad. A fin de garantizar el derecho de defensa de la persona afectada, ésta podrá ser oída cuando la Organización lo determine, y se le advertirá de la posibilidad de comparecer asistida de abogado y que aporte aquellos medios de prueba que considere adecuados y pertinentes.

¿Quién es el Responsable del Sistema Interno de Información?

El Responsable del Sistema es el Comité de Cumplimiento (en adelante, también nos referiremos a él como el "*Comité*"), órgano permanente que ha de desarrollar sus funciones de forma independiente, imparcial y autónoma y con competencias ejecutivas para decidir las acciones a adoptar ante el conocimiento de indicios de cualquier presunto hecho delictivo que pueda tener consecuencias penales o cualquier otro tipo de consecuencias para la Organización. Asimismo, el Comité tiene competencias para informar al Consejo de Administración sobre los presuntos hechos delictivos siempre que lo considere necesario y, en todo caso, cuando pudieran afectar

seriamente a la reputación de la Organización o a nuestros intereses corporativos. De igual manera, si se pudiera llegar a ver afectada la reputación de la Organización o de alguno de los miembros del Consejo de Administración, será puesto en conocimiento del Área Jurídica (en caso de que exista), a la Dirección General y/o de las personas encargadas de los medios de comunicación y las redes sociales para garantizar un adecuado tratamiento de la situación.

El Comité podrá conocer tanto de aquellos casos en los que exista notificación por parte del Ministerio Fiscal sobre la existencia de una investigación o de un procedimiento penal ya en curso contra la Organización, como en aquellos casos en los que la detección se haya producido por mecanismos internos como, por ejemplo, a través del Canal Ético de la Organización.

Las principales competencias del Responsable del Sistema en relación al canal son:

- Gestionar la herramienta de Canal Ético a través de los servicios de una empresa externa, cuya principal función es la recepción de la comunicación y minimizar los posibles conflictos de interés.

- Llevar a cabo la investigación de los hechos, asistiéndose en caso de que la neutralidad, imparcialidad y objetividad de la cuestión lo requiera, de expertos externos.

- Realizar un informe sobre el resultado de la investigación realizada, poniendo de manifiesto si se dan por acreditados los hechos denunciados y proponer las medidas adecuadas para la resolución del hecho, así como, en su caso, las medidas disciplinarias a tomar, pudiendo siempre delegar esta facultad en el externo experto objetivo.

- Levantar acta de todas las acciones realizadas en relación con el expediente, dejando constancia de ello y trazabilidad en el aplicativo del Canal.

- Resolver las dudas y consultas que se susciten en relación con el Canal Ético

- Elaborar y difundir notas interpretativas sobre el presente procedimiento, así como formar al respecto a los empleados (tareas de formación, sensibilización y concienciación).

- Cambios al presente documento para adecuarlo a la realidad normativa en cada momento o a la evolución del negocio, sometiéndolo en su caso al órgano de administración.

- Mantener el registro de denuncias internas (libro – registro de las comunicaciones recibidas, sean consultas o denuncias, así como de las investigaciones pertinentes realizadas). El plazo máximo de conservación de esta información será de 10 años.

Protección de datos

El tratamiento y la cesión de los datos obtenidos como resultado de las denuncias recibidas y de las actuaciones realizadas en el transcurso de su gestión, especialmente los de carácter personal, están sometidos al respeto de los principios de la protección de datos, a la normativa vigente en materia de protección de datos y en particular al artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que establece el régimen jurídico aplicable a los “sistemas de información de denuncias internas”. La base legitimadora del tratamiento es el cumplimiento

de una obligación legal (artículo 8 de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019).

Así mismo, en cumplimiento del artículo 31 de la LOPDGDD, el Canal de denuncias estará incluido como un tratamiento en el Registro de Actividades de Tratamiento.

- Tratamiento de los datos del Canal Ético

El acceso al canal está limitado dentro del ámbito de sus competencias y funciones exclusivamente a:

- El Responsable del Sistema y a quien lo gestione directamente.

- El responsable de recursos humanos o quien desempeñe dichas funciones a nivel interno, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador.

- El responsable de los servicios jurídicos de la entidad o quien desempeñe dichas funciones a nivel interno, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

En ningún caso serán objeto de recolocación o tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley de protección del informante.

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

Si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

El plazo máximo de conservación de los datos en cualquier caso es de 10 años.

- Derechos de la parte afectada / denunciado:

Los interesados podrán ejercer los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

- Derechos del informante:

Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas.

La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En particular, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión

No se obtendrán datos que permitan la identificación del informante y se cuenta con las medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

Terminología

Por último, se aporta la siguiente tabla con el fin de clarificar los conceptos utilizados a lo largo del presente documento, los cuales podrán ser utilizados indistintamente:

DENUNCIA	Información, comunicación…
DENUNCIADO/A	Parte afectada o persona afectada
DENUNCIANTE	Informante
CANAL DE DENUNCIAS	Canal ético, sistema de información interna, etc
RESPONSABLE DEL SISTEMA	Comité de Cumplimiento, cuya composición y funciones han sido aprobados por el Consejo de Administración de la Organización

RÉGIMEN SANCIONADOR	Régimen donde se regulan las conductas no aceptadas por la organización y susceptibles de sanción en relación a su Sistema de Gestión de Compliance Penal, o régimen sancionador previsto en el Convenio/s Colectivo/s que resulte de aplicación a la Organización, o en su defecto, el previsto en la Ley del Estatuto de los Trabajadores

3. Protocolo de actuación pre-procesal

3.1. Recepción de denuncias o comunicaciones de presuntas irregularidades o hechos delictivos

Todos los miembros de la Organización en caso de ser conocedores de alguna irregularidad o en caso de sufrirlas personalmente se comprometen a informar al Responsable del Sistema al respecto a través de los canales establecidos para tal fin. Asimismo, en caso de que un trabajador/a que no sea el Responsable del Sistema reciba una comunicación / información susceptible de ser parte del alcance de este documento, deberá trasladarlo de inmediato al Responsable del Sistema y deberá guardar absoluta confidencialidad. En caso de que esta persona quebrante la confidencialidad de la información que le ha sido comunicada podrá ser sancionado por falta muy grave conforme al Convenio Colectivo / Estatuto del Trabajador que resulte de aplicación.

Por su parte, la Organización garantiza un tratamiento de la situación de forma estrictamente confidencial garantizando, sin prejuzgar:

- el amparo de la víctima y el cese inmediato de estas actuaciones, poniéndolo en conocimiento de las autoridades en caso de que fuera necesario;

- la protección del denunciante / informante, castigando toda posible represalia o conducta perjudicial contra él.

- la presunción de inocencia de la persona afectada, la protección de su derecho al honor y derecho a ser oído en el transcurso del expediente cuando la Organización determine en base al correcto devenir de la investigación.

Toda conducta contraria a lo aquí expuesto se sancionará conforme a lo establecido en el Régimen Sancionador.

Las denuncias / incidencias se podrán comunicar a través de nuestro canal ético, siendo el receptor directo de las mismas una empresa externa que se encargará de mantener altos índices de confidencialidad sobre lo comunicado, así como activar los protocolos necesarios para evitar los posibles conflictos de interés entre los hechos denunciados y los miembros del Responsable del Sistema a los que se les hará llegar la información. Es decir, en caso de que algún miembro del Responsable del Sistema esté afectado por los hechos informados, sea directa o indirectamente, la empresa externa se encargará de apartarle del expediente (recusación) y comunicar lo sucedido al resto de miembros del Responsable del Sistema, bajo los más altos estándares de confidencialidad. Asimismo, los propios miembros del Responsable del Sistema también deberán abstenerse en caso de que detecten cualquier posible conflicto de interés.

Los canales o sistemas de información internos implementados por la Organización son:

- Plataforma web proveída por una empresa especializada: https://zenithbr.canaletico.es

  El Canal Ético funciona mediante una plataforma web externa que permite el anonimato del informante y que cumple con todos los más altos estándares de seguridad de la información, confidencialidad y protección de datos.

  Una vez enviada la comunicación, ésta quedará registrada automáticamente en la plataforma del Canal, generando un número de expediente para poder realizar el seguimiento, incluso anónimamente y adjuntar toda la documentación relacionada con dicha comunicación, en caso de que exista.

- También se permite realizar comunicaciones de forma verbal mediante entrevista presencial o virtual con el Responsable del Sistema. Dicha entrevista deberá ser transcrita en acta o grabada, previa autorización del informante, manteniendo siempre los mismos niveles de confidencialidad que en cualquier otro supuesto, y permitiendo al informante ejercer sus derechos de supresión, oposición, portabilidad, limitación, acceso y rectificación.

  En caso de que el informante quiera trasladar una información al Responsable del Sistema, deberá ser agendada la reunión en el plazo máximo de 7 días.

Una vez recibida la comunicación y si a la vista de la información disponible y los intereses en juego se considera pertinente, se procederá a incoar y aperturar el expediente. En cualquier caso, y con independencia de que finalmente sea necesario investigar o no se dará acuse de recibo al denunciante / informante en el plazo máximo de 7 días.

Todas las incidencias o denuncias recibidas, independientemente del medio por el que lleguen, serán registradas y custodiadas por el Responsable del Sistema, cumplimentando los siguientes datos:

1. Fecha de notificación de la incidencia.
2. Tipo de Incidencia.
3. Descripción detallada de la incidencia.
4. Fecha y hora en que se produjo la incidencia.
5. Persona o personas que realizan la notificación.
6. Persona a quien se comunica la incidencia.
7. Referencia.
8. Investigación (sí o no)
9. Conclusiones
10. Fecha de cierre

El registro de incidencias se mantendrá permanentemente actualizado y a disposición de los Auditores y/o los órganos de la Administración de Justicia. Igualmente, se llevará un registro de todas las dudas / consultas recibidas.

Asimismo, todos los miembros de los grupos de interés de la Organización tienen a su disposición (en la plataforma del canal ético) los canales externos autonómicos, nacionales y europeos, incluyendo la Autoridad Independiente de Protección del Informante (A.A.I.), de conformidad con la Ley 2/2023. No obstante, el canal interno de información se establece como la vía preferente para la comunicación de posibles infracciones, garantizando una gestión eficaz y confidencial.

3.2. Incoación del procedimiento y apertura del expediente

Partiendo de la premisa de que en todo caso se debe acusar recibo en 7 días, pueden darse las situaciones siguientes:

En el caso de que la información trasladada no sea parte del alcance de este procedimiento, y por tanto no debiera haberse utilizado para tal fin el canal ético, se responderá en este sentido por escrito al informante a través del aplicativo y se dará por cerrado el expediente.

En el caso de aquellos asuntos sobre los que esté pendiente resolución judicial o se esté cursando el correspondiente expediente administrativo, se podrá suspender la tramitación de la denuncia, sin perjuicio de que se investiguen los problemas generales planteados en la misma y se emitan las recomendaciones genéricas pertinentes.

En el caso de que lo comunicado sí sea parte del alcance de este procedimiento y no esté pendiente de resolución judicial o expediente administrativo, la empresa externa que reciba las comunicaciones elaborará un informe inicial con una valoración de la información disponible sobre la irregularidad o presunto hecho delictivo en cuestión o, en su caso, sobre los posibles problemas para obtener información. Este informe tendrá carácter reservado y confidencial y se regirá por lo dispuesto en la normativa vigente de protección de datos. Asimismo, se podrán adoptar las medidas necesarias para asegurarse de forma preliminar de la veracidad de los hechos y para solicitar al denunciante las alegaciones o aportación de pruebas que éste considere oportunas al objeto de facilitar la actuación de la investigación y el esclarecimiento de los hechos.

3.3. La investigación corporativa

La conducción de la investigación interna de la denuncia a fin de verificar o desestimar las sospechas de las irregularidades cometidas, será realizada por el Responsable del Sistema Interno o por quien éste considere conveniente que intervenga en dicha investigación para el buen desarrollo de la misma y para garantizar la imparcialidad y objetividad de la investigación. No obstante, en el hipotético supuesto, en el que la persona que cometiera la presunta irregularidad formara parte del equipo encargado de la investigación se le recusará de forma inmediata, y se pondrá en conocimiento, si se estimara necesario, del Consejo de Administración.

La investigación se llevará a cabo de acuerdo con sus protocolos internos de actuación y reportaran sus actuaciones, siempre que se considere necesario, al Consejo de Administración, contando con el asesoramiento constante del asesor jurídico externo o del equipo que preste dichos servicios.

En aquellos supuestos en que los presuntos hechos delictivos entraran en colisión con los intereses corporativos de la Organización o pudieran llegar a dañar de forma directa su reputación o la de alguno de sus Consejeros o Administradores, se pondrá en conocimiento del Consejo de Administración, del Área Jurídica (o de quien desempeñe dichas funciones) y, si se considera necesario, también del área encargada de los medios de comunicación.

Por otro lado, en función de las circunstancias concretas del caso, como por ejemplo la conveniencia de una mayor objetividad e imparcialidad de la investigación, el Responsable del Sistema podrá decidir que la misma sea externalizada a expertos en la materia. En estos casos, el Responsable del Sistema determinará el plazo en el que deberá realizarse la investigación, que sólo podrá ser prorrogado mediante autorización del propio órgano y los objetivos de la misma. Asimismo, el Responsable del Sistema será informado en todo momento de la marcha, la consecución de objetivos y los progresos de la investigación y tendrá en cuenta especialmente la supervisión de aspectos como la disponibilidad de los recursos necesarios para el mismo, así como el acceso a toda la documentación e información necesaria para la investigación a través del acceso a las dependencias de la Organización y del uso de todos los medios jurídicamente válidos, incluyendo, entre otros: entrevistas, el examen de la documentación de cualquier tipo y en cualquier soporte, la recuperación y el análisis de la información contenida en soportes informáticos mediante el uso de herramientas informáticas que preserven la integridad de la evidencia y la posibilidad de aportarla como medio de prueba a un procedimiento penal, etcétera. Los Empleados/as pueden solicitar en las entrevistas la presencia de un representante legal de los trabajadores.

Una vez finalizada la investigación ya sea interna o externa, se confeccionará un informe con las conclusiones de la misma y con propuestas de actuación concretas. El informe debe contener, en todo caso, una relación circunstanciada de hechos, las actuaciones realizadas con el fin de esclarecer los mismos y la valoración de las pruebas practicadas y de los indicios obtenidos.

El plazo máximo para comunicarle al informante el estado de situación del expediente es de tres meses a contar desde la fecha del acuse de recibo, ampliable a otros tres meses en caso de que el devenir de la investigación lo requiera.

3.4. Actuaciones tras la conclusión de la investigación corporativa interna

El informe con el que concluya la investigación será la base sobre la que el Responsable del Sistema decidirá las siguientes actuaciones, siendo éste, junto al Consejo de Administración, en caso de que se considere necesario, el único órgano competente para adoptar las decisiones con base en los resultados obtenidos mediante la investigación.

3.5. Archivo del expediente

A partir de la presentación del informe, el Responsable del Sistema tendrá que valorar en un plazo máximo de 10 días, que podrá ser prorrogado excepcionalmente previa justificación por la complejidad o las características especiales del caso, si de la investigación no se derivan datos que exijan más actuaciones por parte de la Organización, al no existir indicios suficientes de la presunta comisión de un hecho delictivo, o en todo caso resultan hechos que por su escasa relevancia no deban motivar ulteriores actuaciones. En ese caso el expediente se archivará.

3.6. Comunicación de denuncias falsas o de mala fe

El Canal Ético debe emplearse de manera responsable y adecuada.

La comunicación de hechos falsos, con una actitud maliciosa y moralmente deshonesta, supone una infracción de la buena fe que debe presidir las relaciones de trabajo dentro de ZENITH BR, pudiendo derivar en medidas disciplinarias de conformidad con el Régimen Disciplinario existente en la Organización, en el Estatuto del Trabajador o en el Convenio Colectivo aplicable.

Si, tras el oportuno análisis, se pudiera concluir que los hechos comunicados son manifiestamente falsos y que la comunicación ha sido presentada con actitud maliciosa y mala

fe: (i) se archivará la comunicación, documentando los motivos que han llevado a archivar el expediente, finalizando la labor de investigación; (ii) se trasladará dicha circunstancia a la Dirección de RRHH o quien desempeñe dicha función para que se propongan medidas disciplinarias de conformidad con el Régimen Disciplinario correspondiente.

La decisión de inadmitir a trámite se comunicará al informante a la mayor brevedad posible y se ha de motivar.

3.7. Actuaciones en caso de detección de indicios de un presunto hecho delictivo

En caso de que se constate la existencia de indicios de comisión de un presunto hecho delictivo, el Responsable del Sistema Interno, como único órgano competente para diseñar y elaborar de forma centralizada todas las actuaciones de la Organización como reacción a la detección del presunto hecho, instará a los responsables a la toma de las decisiones que consideren convenientes y oportunas, informando puntualmente de las mismas al Consejo de Administración.

El Responsable del Sistema Interno es el órgano competente para la custodia de las pruebas o evidencias obtenidas en tanto en cuanto no se pongan a disposición de las autoridades. Dicha custodia podrá ser delegada en el área que se considere más apropiada, en función de las circunstancias concretas de cada caso.

En caso de indicios de delitos, se deberá remitir la cuestión al Ministerio Fiscal español, o en caso de que afecte a los intereses de la Unión Europea, a la Fiscalía de la Unión Europea.

3.8. Actuaciones en relación al Sistema de Gestión de Compliance Penal

Tras la finalización de la situación de crisis el Responsable del Sistema Interno informará al Consejo de Administración de las posibles deficiencias detectadas o lagunas del Sistema de Gestión de Compliance Penal, en caso de que existan, y se instará a la adopción de las decisiones que se consideren adecuadas.

3.9. Medidas cautelares

A iniciativa propia, o a instancia del responsable de la investigación corporativa interna regulada en el punto 3.3., el Responsable del Sistema Interno podrá acordar directamente o instar a las áreas competentes la adopción de las medidas cautelares necesarias, para evitar cualquier consecuencia negativa para la Organización o para proteger a los Consejeros, Administradores, Altos Directivos y Empleados/as.

3.10. Registro de expedientes

El Responsable del Sistema Interno será el encargado de la custodia de los expedientes una vez finalizados de tal modo que se garantice su integridad y su control cronológico.

Cada expediente contendrá todos los documentos relacionados con las decisiones tomadas, especialmente los relativos a las políticas y procedimientos de reacción seguidos por la Organización ante la presunta comisión de un hecho delictivo y las comunicaciones intercambiadas con las áreas que han participado en el procedimiento o a las que se ha instado a la adopción de medidas cautelares.

4. Protocolo de actuación procesal

4.1 Ámbito de aplicación

El protocolo de actuación procesal se activa en el momento en el que se dirija un procedimiento penal o una investigación del Ministerio Fiscal directamente contra la Organización, o bien cuando de la actuación pre-procesal se derive una actuación procesal penal.

Se creará de forma previa un Comité de Crisis siendo parte del mismo el Responsable del Sistema y personas expertas en comunicación, entre otros miembros. Asimismo, se denominará de forma previa el interlocutor. El fin de dicho Comité es defender los intereses de ZENITH BR frente a terceros, más allá del ámbito puramente penal.

El Comité de Crisis, a instancias de los informes y consideraciones legales del Área Jurídica o quien preste dichos servicios, será el órgano encargado de gestionar las líneas básicas de la estrategia procesal, así como de todas las estrategias corporativas de reacción al procedimiento penal.

Es de aplicación a este Protocolo de actuación procesal lo dispuesto en el apartado 3.3 (La investigación corporativa interna) y 3.9 (Medidas cautelares).

4.2 Designación del representante procesal

El Área Jurídica propondrá quien puede ser nombrado representante procesal cuando existan especiales motivos de oportunidad, incompatibilidad o afectación de los hechos y/o potenciales responsabilidades a los servicios centrales de la Organización.

El Responsable del Sistema Interno informará al Consejo de Administración sobre el abogado defensor y procurador que resulten idóneos para la defensa y representación de la Organización, el cual podrá formar parte de las reuniones que se convoquen sobre el pleito en cuestión como invitado consultivo. Para los representantes legales se utilizarán los estándares de representación actualmente vigentes en la Organización.

ZENITH BR se reserva su derecho a modificar sus representantes legales en función del devenir del procedimiento.

Nunca podrá ser designado representante procesal de ZENITH BR una persona que pueda tener conflictos de intereses procesales con la Organización. En este sentido se velará particularmente porque personas relacionadas con los hechos susceptibles de revestir categoría de ilícito penal no sean designados representantes procesales.

Para finalizar, ZENITH BR se compromete a colaborar activamente con la Administración de Justicia en tanto cuanto sea necesario, aportando información y pruebas para esclarecer los hechos, llegándose a confesar culpable de una infracción en caso de que así sea, y reparando en todo caso el daño causado a la mayor brevedad (artículo 31 bis apartado 4 del Código Penal).