

PLAN DE PREVENCIÓN PENAL

Marzo 2018
(edición 1)



- **Nombre o Razón social:** FRONTING CORREDURÍA DE SEGUROS Y REASEGUROS, S.L.
- **Domicilio:** Avda. Eduardo dato nº 44, planta 1, local 6, 41005
- **Inscripción en el Registro DGS:**
- **NIF:** B90335886
- **Descripción de la actividad:** Correduría de Seguros

ÍNDICE

1.- INTRODUCCIÓN.

2.- OBJETO, ÁMBITO DE APLICACIÓN Y METODOLOGÍA.

2.I. Objeto del Plan.

2.II. Ámbito de Aplicación.

2.III. Metodología.

3.-ANÁLISIS DE RIESGOS PENALES.

3.I. Evaluación de riesgos penales.

3.II. Mapa de Procesos.

4.- SUPERVISIÓN Y DIFUSIÓN DEL MODELO.

4.I. Supervisión y control del modelo.

4.II. Difusión del modelo y actualización.

5.- CANAL ÉTICO/CANAL DE DENUNCIAS.

5.I. Objeto.

5.II. Comunicación de infracciones.

5.III. Tramitación de denuncias.

5.IV. Protección de datos.

ANEXO I.- Órgano de control y órgano de decisión.

1.- INTRODUCCIÓN

La evolución legislativa genera en las empresas la necesidad de adaptarse a los cambios y adoptar prácticas y políticas novedosas para ellas. Desde que en 1885 se promulgó nuestro, todavía vigente, Código de Comercio, el concepto de empresario ha variado gradualmente de un contexto más cercano a la “tienda” o “almacén”, hasta convertirse en un Derecho de Mercado, como escenario en que se realizan los intercambios jurídicos y económicos, y en el que al Estado le corresponde una nueva y determinada función regulatoria.

De esta forma han ido apareciendo, desde hace décadas, una serie de tópicos que han venido asentado el concepto de ética de los negocios como forma más eficiente de gestionar las empresas, con mayor concepto de humanización y un mayor respeto a la ley y a los derechos individuales y sociales. Esta evolución nos ubica hoy en día dentro del fenómeno de la autorregulación de las sociedades mercantiles, donde no resulta suficiente la imposición voluntaria de estándares de conducta y protocolos, sino que los poderes públicos condicionan y fomentan esas estructuras de autorregulación dentro de la empresa.

En esta línea aparece la Ley Orgánica 1/2015, de reforma de la Ley 10/1995 –nuestro vigente Código Penal-, que nos presenta los modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos. Este modelo de organización, o programa de cumplimiento penal o normativo, supone trasladar a la empresa la función de prevención penal, permitiendo que estas se autorregulen y se doten ellas mismas de mecanismos de la forma que mejor se ajusten a su estructura y funcionamiento.

Ante esta necesidad planteada por imperativo legal, **FRONTING CORREDURÍA DE SEGUROS Y REASEGUROS, S.L.** (en adelante **FRONTING**), ha desarrollado este Plan de Prevención Penal o Normativo, que además se enmarca dentro de la política de estricto cumplimiento de la normativa vigente, y en línea con los documentos de Política de Empresa y Responsabilidad Empresarial, así como de Gestión Integrada.

El presente Plan de Prevención supone la herramienta apropiada para la prevención de delitos dentro del seno de la empresa, y concretamente para el supuesto de la comisión de los referidos en el artículo 31 bis.1 del Código Penal:

- a) De los delitos cometidos en nombre o por cuenta de la empresa, y en su beneficio directo o indirecto, de las personas autorizadas para tomar decisiones en nombre de la persona jurídica, o que tengan facultades de organización y control.
- b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y beneficio directo o indirecto de la empresa, estando sometidos a la autoridad de las personas del punto anterior.

Con este fin se realiza, y se adopta el compromiso de garantizar su difusión favoreciendo su aplicación en toda la empresa, sus socios, asociados y franquiciados, así como el de los mecanismos que este plan pueda implementar, o los órganos previstos para su correcta aplicación y funcionamiento.

Específicamente, en el compliance en mediadores de seguros, la reforma del código penal impacta con gran fuerza en todo el ámbito asegurador de nuestro entorno. Así, a las medidas de control interno que ya se exigían a las entidades aseguradoras y mediadores en, por ejemplo, el ámbito del blanqueo de capitales en el ramo de vida, se suman otras para intentar evitar que en el seno de las mismas se cometan determinados delitos que preocupan al legislador.

2. OBJETO, AMBITO DE APLICACIÓN Y METODOLOGÍA.

2.I. OBJETO

El objeto del presente Plan de Prevención Penal es servir de manera eficaz a la prevención de delitos en la empresa, de formas que todos los miembros de la misma encuentren en él la herramienta adecuada para ello. De esta forma, este plan funciona como mecanismo capaz de ayudar a los empleados y colaboradores y miembros de toda la red de **FRONTING** en la prevención de delitos, pues les proporcionará un mecanismo capaz de identificar conductas y procedimientos punibles penalmente, tanto propios como de terceros, y que ocurran en el seno de la empresa o sus actividades.

Así mismo, es objeto de este plan de prevención es la correcta formación de la voluntad de la empresa respecto a las acciones a emprender ante una situación de riesgo penal, de forma que se garantice la defensa de sus intereses teniendo en consideración la normativa legal y su situación procesal.

En último lugar, también es su objeto implementar un canal óptimo y capaz de resolver y tramitar todas las situaciones en las que los miembros de la red de **FRONTING** puedan apreciar cualquier violación real o percibida por ellos de la normativa vigente. Todos los socios, asociados, franquiciados y colaboradores de **FRONTING** ya sea directa o indirectamente deben sentirse responsables de la estricta aplicación de este Plan, dada la importancia de la Política empresarial de cumplimiento y compromiso con la normativa vigente.

2.II. ÁMBITO DE APLICACIÓN

La aplicación afecta a la totalidad de la red como se ha dicho. La observancia y aplicación del mismo será imperativa tanto para los empleados como para los directivos de las distintas personas jurídicas. Por tanto, se verán afectados aquellos empleados, empresas y sus colaboradores, que realicen actividades comerciales para **FRONTING** dentro de su red y ello en la medida en que intervengan en los procesos productivos con riesgos penales de los comprendidos en la matriz de riesgos penales.

También los servicios externos de **FRONTING** deben conocer y aplicar el plan en sus relaciones con la empresa, de forma que las operaciones que realicen en relación con la empresa se atengan a un estricto cumplimiento de lo contenido en él.

2.III. METODOLOGÍA

Para la realización de este modelo de organización y prevención se ha seguido un método que ha permitido la personalización de los riesgos penales que pueden darse en el seno de **FRONTING**. Esta tarea se ha realizado a través del acercamiento al funcionamiento normal y habitual de la Correduría analizando las conductas habituales, los procedimientos establecidos para la realización de su actividad diaria como mediador de seguros. De esta forma se ha podido definir y concretar, entre otros, los procesos existentes en el modelo productivo de **FRONTING**.

Definidos los procesos existentes se ha procedido a identificar los riesgos penales existentes en la persona jurídica y en el resto de la red, a clasificarlos en función de su impacto y su probabilidad, obteniendo un mapa de riesgos adaptado a la empresa. Esta identificación se ha realizado desde un doble prisma, teniendo en cuenta por un lado los riesgos inherentes a toda empresa por el hecho de serlo, y los riesgos propios del sector de Mediación y del modelo productivo y organizativo de **FRONTING**.

De igual forma, se ha procedido a establecer un canal ético o de denuncias, que servirá como vía de comunicación para permitir que se ponga en conocimiento de la persona jurídica las posibles vulneraciones penales (pero también normativas en general) que se puedan producir y le afecten en forma alguna, a fin de que por esta se puedan iniciar las comprobaciones o averiguaciones oportunas, además de tomar las medidas adecuadas. Pero siendo el canal de denuncias un ente inanimado por sí mismo, al igual que lo es el modelo de prevención, se ha dotado también de un órgano de control y supervisión, que a la vez servirá como organismo de instrucción, clasificación, archivo y trámite de las denuncias o comunicaciones recibidas.

En último lugar, se prevén también mecanismos de supervisión y actualización del modelo, ya que este nace con vocación de acompañar a la sociedad en todo su recorrido, por lo que debe estar siempre

condicionado a un momento y condiciones puntuales, debiendo ser capaz de adaptarse a los cambios y necesidades.

En suma, por lo descrito se da cumplimiento a lo previsto en el párrafo primero del apartado 2º del artículo 31.bis del Código Penal vigente, de forma que viene a desarrollar y establecer el modelo de organización y gestión, incluyendo las medidas de vigilancia y control idóneas para prevenir delitos y reducir de forma significativa la comisión de los mismos.

3. ANÁLISIS DE RIESGOS PENALES

3.1. EVALUACIÓN DE RIESGOS

El Corredor de Seguros como persona jurídica deberá velar porque las personas que tiene bajo su autoridad no incurran en supuestos de riesgo penal, pues de cometerse, sería la propia Correduría la que resultaría imputada. Y ello es así porque el art. 31.bis.1 C.P. no habla de “empleados” sino de “*personas sometidas a la autoridad de los administradores o representantes de la persona jurídica*”, lo que amplía el ámbito de control de la persona jurídica a aquellas actividades que le preste determinado personal sin una relación laboral, pero sometido a la autoridad de la Entidad en diversos aspectos.

Según el artículo 2 de la Ley 26/2006, de 17 de julio, de Mediación de Seguros y Reaseguros Privados, “*Se entenderá por mediación aquellas actividades consistentes en la presentación, propuesta o realización de trabajos previos a la celebración de un contrato de seguro o de reaseguro, o de celebración de estos contratos, así como la asistencia en la gestión y ejecución de dichos contratos*”. Los mediadores de seguros son los que se manifiestan en la actividad de presentación y propuestas en función de las necesidades del cliente, previo a la firma del contrato, así como la gestión y ejecución de dichos contratos. Al fin y al cabo, la figura del mediador no es más que la de un intermediario que cuenta con la confianza de su cliente para conseguirle los mejores productos de acuerdo a sus necesidades y gestionar la vida de los mismos en defensa de los intereses de sus clientes cuando estos han sido contratados. Los riesgos surgirán en los comportamientos que puedan aprovecharse de esa necesaria confianza del cliente, así como el fraude en las obligaciones que el propio mediador tiene con la Administración pública. Así, se pueden identificar de un modo preliminar los siguientes riesgos penales que se manifiestan en el ámbito del ejercicio profesional del mediador:

- **Riesgo de estafa, apropiación indebida y administración de leal**
- **Riesgo de cohecho y tráfico de influencias.**
- **Riesgo de corrupción entre particulares.**
- **Riesgo de apoderamiento y revelación de secreto.**
- **Riesgo de delitos contra la intimidad personal y familiar.**
- **Riesgo de delitos contra la Hacienda Pública y la Seguridad Social.**
- **Riesgo de blanqueo de capitales.**

La actividad del mediador de seguros, como ya se ha dicho, se encuentra basada en una relación de confianza riesgos pudieran afectar a una compañía mediadora de seguros, pero resulta necesario acotar el ámbito de incidencia de los riesgos penales al sector de actividad y naturaleza de la mediación:

1. **Corrupción entre particulares Art.286 bis C.P.**
2. **Estafa. Art. 251.bis C.P. Apropiación indebida Art. 253 C.P. Art. 252 C.P. Apropiación desleal.**
3. **Cohecho Art. 427 C.P.**
4. **Tráfico de influencias art. 430. C.P.**
5. **Delito Contra la Hacienda Pública y la Seguridad Social. Art. 310. Bis C.P.**
6. **Blanqueo de Capitales. Art. 302. C.P. y Financiación del Terrorismo. art. 576 Bis C.P.**
7. **Apoderamiento y revelación de secreto. Arts. 278 a 280 C.P.**
8. **Delitos contra la intimidad 193.4 C.P.**

A continuación se analizará sucintamente los riesgos penales identificados y se incluirán algunos ejemplos que ilustren el modo y la forma en que dichos riesgos podrían afectar a **FRONTING**:

1. Corrupción entre particulares

Tradicionalmente, la corrupción en el ámbito privado no se ha considerado un comportamiento punible en España. Los regalos, viajes y otro tipo de atenciones a los posibles clientes era (y en gran medida sigue siendo) una práctica habitual en el ámbito comercial. No obstante, y derivada de la profunda preocupación surgida en el ámbito Europeo por escándalos de corrupción, se han desarrollado determinadas directivas que han desembocado en que todos los países de la Unión Europea castiguen los comportamientos de corrupción, incluso entre particulares. La “*corrupción pasiva*” se contempla en el segundo párrafo del artículo 286 bis C.P. En esta modalidad cometería el delito aquel que recibe el soborno en contra sus obligaciones profesionales. Así, cuando un directivo, administrador, empleado o colaborador de una empresa mercantil, o de una sociedad, asociación, fundación u organización solicita, acepta o recibe un beneficio o ventaja de cualquier naturaleza no justificada (soborno), con el fin de favorecer frente a terceros a aquel que se la ofrece u otorga, incumpliendo sus obligaciones en la adquisición o venta de mercancías o en la contratación de servicios profesionales.

2. Estafa y apropiación indebida y administración de leal

Lo que se castiga en la estafa, básicamente, es la articulación de un engaño suficiente por el que se consigue un beneficio, y se causa un perjuicio patrimonial a un tercero. La posibilidad inacabable de inventar nuevas formas de engaño, y por ende de estafa ha llevado al legislador a configurar el tipo penal de un modo genérico, exigiendo unos elementos que, conectados con la adecuada con relación de causalidad, constituyan el delito de estafa. En esencia, estos elementos son un engaño idóneo (bastante) articulado para producir error en otro, el cual motiva un acto de disposición patrimonial que, a su vez, provoca un perjuicio económico en su propio patrimonio o en el de un tercero. El Código Penal, en su artículo 248 contempla el delito de estafa del modo siguiente: 1. Cometén estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. 2. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujerén, poseyerén o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

El art. 253 del C.P , castiga como reos de apropiación indebida a *“los que, en perjuicio de otro, se apropiaren para sí o para un tercero, de dinero, efectos, valores o cualquier otra cosa mueble, que hubieran recibido en depósito, comisión, o custodia, o que les hubieran sido confiados en virtud de cualquier otro título que produzca la obligación de entregarlos o devolverlos, o negaren haberlos recibido”*

El art. 252 del Código penal que dispone que serán punibles los que, teniendo facultades para administrar un patrimonio ajeno, emanadas de la ley, encomendadas por la autoridad o asumidas mediante un negocio jurídico, las infrinjan excediéndose en el ejercicio de las mismas y, de esa manera, causen un perjuicio al patrimonio administrado.

3. Cohecho

El cohecho activo se materializa cuando un particular ofrece, promete o entrega dádiva o presente, a un funcionario o autoridad pública. Este ofrecimiento puede tener como finalidad que el funcionario o autoridad, lleve a cabo una actuación beneficiosa para el sujeto, o simplemente hacerlo en atención a su cargo. Es decir, el delito de cohecho cometido por un particular se perfecciona con el mero hecho de ofrecer, a un funcionario o autoridad por el mero hecho de serlo. No es necesario por tanto que el funcionario o autoridad lleve a cabo una actuación en beneficio del particular. Por lo tanto, el autor del cohecho puede ser tanto el particular que ofrece como el funcionario o autoridad que acepta u ofrece. A los efectos de entender perfeccionado el delito no es necesario que se produzca la aceptación o entrega de

dádiva, sino que el delito se consuma con el mero hecho de ofrecer. Asimismo, la resolución que se pretenda no tiene por qué ser contraria al ordenamiento jurídico, pero el mero hecho de intentar influir de una manera ilícita en la toma de decisiones de un funcionario o autoridad se considera punible en sí misma. El delito sólo podría cometerse de manera dolosa, es decir con conocimiento de la ilicitud del hecho.

4. Tráfico de influencias

En el ámbito de las relaciones con funcionarios público o autoridad, se circunscribe el delito de tráfico de influencias, donde se castiga influir sobre un funcionario o autoridad con la intención de conseguir una resolución que pueda generar directa o indirectamente un beneficio económico al sujeto activo del delito. En concreto, y a los efectos del Plan de prevención, conviene centrarse en el artículo 429 del C.P., el cual establece que: *“El particular que influyere en un funcionario público o autoridad prevaleándose de cualquier situación derivada de su relación personal con éste o con otro funcionario público o autoridad para conseguir una resolución que le pueda generar directa o indirectamente un beneficio económico para sí o para un tercero, será castigado con las penas de prisión de seis meses a dos años y multa del tanto al duplo del beneficio perseguido u obtenido. Si obtuviera el beneficio perseguido, estas penas se impondrán en su mitad superior”*. El autor del delito puede ser cualquier persona que utilice su situación de prevalimiento para influir en una toma de decisiones que le pueda beneficiar a él o a un tercero utilizando la relación personal que les une de parentesco, amistad, sentimental, etc. Para que el delito se perfeccione no es necesario que la resolución se llegue a tomar ni la efectiva producción del beneficio, pero sí que se cometa con la intención/esperanza de obtener un beneficio directo o indirecto. Este tipo delictivo sólo podrá llevarse a cabo de manera dolosa. El riesgo penal de tráfico de influencias surge en el momento que se tiene una relación profesional con un funcionario o autoridad pública que además une una relación personal (amistad, relación familiar), en los que, entre sus funciones y debido a la actividad profesional encomendada. Dicha relación, aun siendo necesaria y perfectamente legal, conviene que sea tratada con especial sensibilidad en el ámbito de prevención de riesgos penales al implicar una interrelación con las administraciones públicas que ha de establecerse por los cauces adecuados.

5. Fraude fiscal

Las obligaciones fiscales afectan tanto a las personas físicas como a las jurídicas, por lo que la elusión de impuestos supone un ámbito intrínseco de riesgo penal que afecta a cualquier sujeto que desarrolle una actividad lucrativa. La conducta tipificada en el artículo 305 C.P. castiga el hecho de defraudar a la Hacienda Pública, por acción u omisión, por un importe superior a 120.000 €. El citado artículo establece que: *“El que, por acción u omisión, defraude a la Hacienda Pública estatal, autonómica, foral o local, eludiendo el pago de tributos, cantidades retenidas o que se hubieran debido retener o ingresos a cuenta, obteniendo indebidamente devoluciones o disfrutando beneficios fiscales de la misma forma, siempre que la cuantía de la cuota defraudada, el importe no ingresado de las retenciones o ingresos a cuenta o de las devoluciones o beneficios fiscales indebidamente obtenidos o disfrutados exceda de ciento veinte mil euros será castigado con la pena de prisión de uno a cinco años y multa del tanto al séxtuplo de la citada cuantía, salvo que hubiere regularizado su situación tributaria en los términos del apartado 4 del presente artículo”*. La mera presentación de declaraciones o autoliquidaciones no excluye la defraudación, cuando ésta se acredite por otros hechos. *Además de las penas señaladas, se impondrá al responsable la pérdida de la posibilidad de obtener subvenciones o ayudas públicas y del derecho a gozar de los beneficios o incentivos fiscales o de la Seguridad Social durante el período de tres a seis años”*. El delito de defraudación tributaria se comete, en calidad de autor, por el sujeto pasivo de la relación jurídico-tributaria. El tipo contempla una acción u omisión defraudatoria concretada en comportamientos como eludir el pago de tributos, de cantidades retenidas o que se hubiesen debido retener, de ingresos a cuenta de retribuciones en especie, obtención indebida de devoluciones, disfrute indebido de beneficios fiscales, etc. El delito fiscal sólo puede cometerse de manera dolosa (con conocimiento e intención) y exige para su perfección un resultado típico, caracterizado en la producción de un perjuicio patrimonial a la Hacienda Pública en un quantum superior a 120.000€, referido a la cuota defraudada, y que esta situación no se hubiese regularizado de un modo voluntario antes del comienzo del proceso administrativo de comprobación o inspección, o de la interposición de denuncia o querrela contra el obligado tributario por delito fiscal

Fraude a la Seguridad Social

Las obligaciones que los empresarios tiene de contribuir a la Seguridad Social en la parte proporcional que les corresponde, tiene la consecuencia de que la defraudación a esta, en un importe superior a 50.000 € en cuota defraudada, podría provocar la responsabilidad penal de la persona jurídica, pues el hecho de eludir el pago genera un provecho esta. De manera similar el tipo penal expuesto en el epígrafe anterior, el artículo 307 contempla expresamente la acción u omisión de defraudar a la Seguridad Social como comportamiento punible. El artículo 307 C.P. establece que: *“El que, por acción u omisión, defraude a la Seguridad Social eludiendo el pago de las cuotas de ésta y conceptos de recaudación conjunta, obteniendo indebidamente devoluciones de las mismas o disfrutando de deducciones por cualquier concepto asimismo de forma indebida, siempre que la cuantía de las cuotas defraudadas o de las devoluciones o deducciones indebidas exceda de cincuenta mil euros será castigado con la pena de prisión de uno a cinco años y multa del tanto al séxtuplo de la citada cuantía salvo que hubiere regularizado su situación ante la Seguridad Social en los términos del apartado 3 del presente artículo”* El fraude a la Seguridad Social podría cometerse, tanto eludiendo el pago de las cuotas como por la obtención indebida de devoluciones o deducciones. Para que la conducta sea penalmente reprochable se ha de causar un perjuicio a la Seguridad Social superior a 50.000 €, por lo que se exige un resultado concreto y determinado, por lo que si se hubiera regularizado la situación - se haya, en términos del artículo 307.3 C.P., procedido completo reconocimiento y pago de la deuda antes de que se le haya notificado la iniciación de actuaciones inspectoras o se haya interpuesto denuncia o querrela contra la sociedad – no se castigaría penalmente este comportamiento. Este delito no admite la comisión imprudente, por lo que debe ser llevado a cabo con conocimiento e intención de ejecutarlo. Este delito se comete en concepto de autores por aquellos que legalmente estén obligados a efectuar el ingreso en la Seguridad Social o presentar documentación a los efectos de aplicarse devoluciones o deducciones. Según el artículo 104 de la Ley General de la Seguridad Social corresponde, *“el empresario es el único sujeto responsable del cumplimiento de la obligación de cotizar e ingresará las aportaciones propias y las de sus trabajadores en su totalidad”*. El riesgo penal de este delito se concentrará, por tanto, en los departamentos encargados de gestionar y calcular el pago debido a la Seguridad Social en función de los trabajadores empleados por persona jurídica, así como la procedencia de la aplicación de las bonificaciones.

6. Blanqueo de Capitales / Financiación del terrorismo

El delito de blanqueo de capitales se concreta, básicamente en realizar distintas acciones para ocultar el origen delictivo de los activos, y facilitar la incorporación al circuito legal de los bienes que, por su origen delictivo no podrían ser utilizados con apariencia de legalidad. La reforma del Código Penal ha incluido como conductas punibles los comportamientos de *“poseer y utilizar”* los bienes con origen delictivo, por lo que ha ampliado los comportamientos que podrían ser calificados como punibles, por lo que el mero hecho de poseer determinado activos con origen ilícito, según el tener literal del artículo, podría perfeccionar el hecho delictivo. Este riesgo tiene especial importancia en el sector de la mediación de seguros, ya que según la Ley 10/2010, de 28 de abril, de Prevención de Blanqueo de Capitales y de la Financiación del Terrorismo, serán sujetos obligados, entre otros, las entidades aseguradoras autorizadas para operar en el ramo de vida y los corredores de seguros cuando actúen en relación con seguros de vida u otros servicios relacionados con inversiones, con las excepciones que se establezcan reglamentariamente (art. 2.1.b). Ello conlleva una serie de obligaciones (identificación, comunicación operaciones sospechosas, etc) que en caso de ser incumplidas podrían suponer un ámbito de riesgo penal de blanqueo de capitales. Y ello es así porque el delito de Blanqueo de Capitales puede ser cometido por imprudencia grave, con lo que la desatención de las obligaciones impuestas por la Ley 10/2010 podría provocar la imputación de la persona jurídica, si un tercero ha blanqueado capitales utilizando los servicios contratados al mediador.

7. Delito de apoderamiento y revelación de secreto

La información reservada o confidencial de las personas físicas o jurídicas tiene un grado de protección penal, castigándose el hecho de apoderarse de tales secretos con la finalidad de revelarlo en el artículo 278 C.P. Si además de apoderarse, se llegara a revelar o utilizar la información reservada, se castigaría de un modo más grave la conducta. Secreto de empresa será cualquier aspecto de conocimiento reservado que afecte a la capacidad competitiva de la empresa. Se exige que el sujeto activo del delito – que puede ser cualquier persona – se apodere de secretos con la intención de descubrirlo. El apoderamiento puede ser físico de un modo subrepticio o de captación mental o intelectual de información confidencial plasmada en documentos escritos o electrónicos, soportes informáticos u otros objetos. Los secretos

pueden ser de distinta naturaleza, como la industrial (investigaciones en I+D, procedimientos específicos e fabricación, etc), los relativos al sector comercial (estrategias comerciales, productos innovadores, listado de clientes confidenciales, estudios de mercado, etc) o incluso referentes a la organización interna siempre que sea valiosa para los competidores (proyectos de reestructuración, situación financiera, etc).

8. Delito contra la intimidad

La intimidad personal y familiar encuentra su protección en el ámbito penal en el artículo 197 C.P., desde la privacidad de documentos y mensajes de texto o audio, hasta la utilización ilícita de datos en perjuicio de terceros, así como el acceso ilegítimo a sistemas informáticos. El derecho fundamental a la intimidad se encuentra contemplado en el artículo 18.1 C.E, y su protección penal se configura en el ámbito penal en el artículo 197 C.P. del modo siguiente: *“El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años”*. El artículo 197.1 C.P. castiga el apoderamiento de documentos y efectos personales, así como el control auditivo y/o visual clandestino por medio de interceptación de grabaciones o utilización de artificios técnicos de escucha. Son aptos para la comisión de este delito todos aquellos objetos que permitan un acceso ilícito al ámbito espacial de la intimidad de un tercero. Se tutelan datos, efectos personales, noticias, comunicaciones, etc, que deben quedar a reserva del conocimiento de los demás por voluntad expresa o tácita del titular. Este delito debe cometerse de un modo doloso, y requiere de un elemento subjetivo específico: la intención de descubrir o vulnerar la intimidad de otro. No obstante, la perfección del delito no requiere que finalmente se descubra el secreto, sino que la mera intención de llevarlo a cabo consumaría el delito. Las conductas típicas contempladas en el artículo 197.2 C.P. amplían el ámbito de protección a los datos personales. Así, se tipifican las acciones de apoderamiento, utilización o modificación, sin autorización para ello, de datos reservados de carácter personal que se hallen automatizados o que obren en cualquier tipo de archivo o registro público o privado. Para que el delito se perfeccione se requiere el perjuicio del titular de los datos o de un tercero.

Principales controles que pueden utilizarse para prevenir riesgos penales

En el ámbito de los controles de riesgo, ya sean penales o de otra clase, se establece un primer nivel, donde se sitúan los controles de ámbito general y que afectan a toda la organización, y un segundo nivel donde se encuentran los controles específicos, que han sido pensados y diseñados para prevenir y controlar riesgos concretos.

Como ejemplo de los controles de primer nivel, se pueden nombrar a modo de ejemplo, los siguientes:

- Código de conducta/ Código ético aplicable a todos los miembros de la empresa.
- Política y sistema de Control Interno de Riesgos.
- Canal de denuncia de comportamientos poco éticos de ámbito interno o externo.
- Política general anti fraude.
- Auditorias externas.
- Certificaciones de calidad.
- Responsable en la empresa del cumplimiento legal.
- Formación al personal.

Los controles de segundo nivel serán los específicos de cada riesgo identificado. Ello no quiere decir que los controles que a continuación se desarrollan sea los únicos aplicables, sino que se incluyen a los efectos de exponer un modo de controlar los riesgos penales identificados al mediador de seguro, y con ello desarrollar el debido control que el legislador exige al administrador y representante de las personas

jurídicas. En cualquier caso, como control principal **FRONTING** establecerá una formación continua al personal propio y a toda su red, incluyendo Directivos, empleados, socios, asociados, franquiciados y colaboradores.

Tipo de riesgos penales, Controles:

Cohecho Procedimiento interno que regule la relación con los funcionarios públicos y autoridades. Procedimiento de aceptación/entrega de regalos (incluyendo o no un límite en el valor del regalo).

Tráfico influencias. Norma interna que regule el modo de actuar ante la relación personal de un empleado y un funcionario encargado de dictar resolución que afecte a la empresa. Regulación expresa de las situaciones de conflicto de interés y pautas de actuación.

Estafa. Servicio de atención de las reclamaciones de los clientes a través de un canal específico (email, línea teléfono, etc) y de un encargado responsable de atender reclamaciones de un modo centralizado. Procedimiento de revisión de contratos por la asesoría jurídica y visos obligatorios de las áreas afectadas antes de proceder a su firma.

Apropiación indebida y administración desleal. Control de los sistemas de cobro y tramitación de pólizas, seguimiento de devoluciones de primas por parte de los colaboradores. Control de los acuerdos de Consejo y su cumplimiento, acceso restringido a poderes de disposición; establecimientos de sistemas mancomunados de gestión de cuentas.

Contra la intimidad. Procedimiento interno que regule el acceso y la supervisión del correo electrónico corporativo y el uso de internet por parte de la empresa (este procedimiento debe ser comunicado a los trabajadores con carácter previo al monitoreo de correos o vista de páginas) Auditorias externas bienales de tratamiento de datos personales. Documentos de seguridad de datos.

Blanqueo de Capitales/ Financiación Terrorismo Manual de Prevención de Blanqueo Capitales y Financiación Terrorismo. Prohibición de recibir pagos en metálico o aceptar transferencias de las que se desconozca su origen.

Apoderamiento/ revelación secreto. Norma interna que prohíba utilizar documentación de otras empresas que no sea pública. Anexo contrato trabajo donde se informe al trabajador que se va a contratar que la empresa no aceptará que se utilice documentación o información reservada obtenida en su anterior puesto de trabajo.

Delito fiscal Segregación de funciones respecto a las tareas contables y financieras. Adhesión al Código de Buenas Prácticas Tributarias

Delitos contra la seguridad social Segregación de funciones respecto a la información y pago a la Tesorería General de la Seguridad Social. Procedimiento interno pago cuotas Seguridad Social.

3.II. MAPA DE PROCESOS.

En este apartado se trata de identificar los proceso y sistema organizativo de **FRONTING** al objeto de identificar los riesgos y las personas implicadas en los mismos.

En los procesos de Gestión Comercial se entienden incluidos tanto al personal con vinculación laboral o mercantil directa con **FRONTING** como aquellos pertenecientes a su red. Es evidente que la responsabilidad penal de **FRONTING** no puede extenderse a las actividades ilícitas que puedan desarrollar sus Socios, Asociados, Franquiciados o los colaboradores de cualquiera de aquellos, ya que todos los citados son empresas independientes que han de velar cada una de ellas, por el escrupuloso cumplimiento de las normas legales por parte de sus directivos empleados y colaboradores. No obstante, dada la vocación de red empresarial de **FRONTING**, ésta asume la formación específica y la ayuda a los controles que sirvan para minimizer y en última instancia evitar cualquier tipo de riesgo penal en toda la red.

De esta forma, debemos añadir a los siguientes procesos que se detallan:

- Procesos de Dirección.
- Procesos de Gestión de Recursos Humanos.
- Procesos de Contabilidad.
- Procesos de Relación con Organismos Públicos.

La subcontratación de servicios obliga a determinar una serie de servicios externos como foco de riesgos, a saber:

- Servicios informáticos externos.
- Servicios externos de asesoría fiscal.
- Servicios jurídicos externos.
- Servicio externo de asesoría y tramitación laboral.
- Servicios de asesoría económica externa.

4.- SUPERVISIÓN Y DIFUSIÓN DEL MODELO

4.1. Supervisión y control del modelo

Es necesaria la supervisión continuada del modelo para asegurar su correcto funcionamiento. Dentro de esta supervisión continuada se hace fundamental establecer dos nuevos organismos que permitirán el efectivo funcionamiento del modelo (la composición, el funcionamiento y los procedimientos se detallan en el anexo I).

a) Órgano de Instrucción y control.

Se prevé la creación de un órgano de control de cumplimiento normativo, que pueda desarrollar las necesarias tareas de órgano de control del plan (actualización, supervisión), así como la instrucción de las posibles comunicaciones o denuncias que puedan llegar a él a través del canal ético. Esta tarea de instrucción será fundamental, pues deberá proporcionar al órgano de decisión de la empresa la información fiable y oportuna que le permita tomar las decisiones acordes a la ley, y que sean más convenientes para la sociedad y para su situación procesal.

Durante la instrucción deberá velar por el mantenimiento de los principios básicos que rigen el canal ético o de denuncias, con especial atención a la confidencialidad que debe regir el mismo. Deberá actuar con la celeridad que le permita su funcionamiento en el esclarecimiento de cuantos hechos tenga conocimiento y sean objeto de su competencia. La labor instructora deberá terminar en todo caso con un informe anual que contendrá, como mínimo, la siguiente información:

- Información descriptiva de la denuncia, fechas de interposición y principales hitos.
- Medidas de urgencia llevadas a cabo, motivación de la misma y efectos.
- Objetivación de la denuncia, análisis de la fiabilidad del denunciante y veracidad de la información.
- Valoración de si resulta necesario cualquier tipo de apoyo o asesoría externa, especialmente apoyo formativo
- Propuesta de actuación y de resolución.

Además de las funciones anteriormente descritas, el órgano de instrucción desempeñará las funciones de control de canal ético, clasificación de la información recibida a través de él, y dirección del sistema de gestión de denuncias.

b) Órgano de Respuesta.

Es el órgano encargado de tomar las resoluciones que conlleven una respuesta de cualquier tipo respecto a la posible materialización de un riesgo penal. Esta decisión se tomará en función de la información que se haya podido recibir desde el órgano de instrucción, con la exposición de los hechos, averiguaciones, y propuesta de resolución recibida.

El órgano de decisión será colegiado, recayendo el mismo sobre el Consejo de Admonstración. Para la toma de la decisión podrá recabar el apoyo de cualquier órgano o asesor, tanto interno o externo. Igualmente podrá apoyarse o asesorarse con el órgano instructor.

4.2. DIFUSIÓN DEL MODELO Y ACTUALIZACIÓN.

Este modelo de organización de **FRONTING**, en tanto que se encarga de la prevención de riesgos penales en la empresa y su red, estará disponible a través de un enlace en la página web corporativa, de forma que tanto los empleados como los terceros que tengan relación con la empresa, o aun sin tenerla, puedan conocer el interés de **FRONTING** por la prevención de delitos en su seno, y comunicar a través del cauce habilitado para ello, la posible comisión de delitos o conductos contrarias a la normativa vigente dentro de la empresa.

En cuanto a su actualización, toda vez que un modelo de prevención supone un programa de gestión dinámico, con carácter periódico se realizarán las oportunas revisiones del mismo, siendo esta periodicidad de un año, prestando especial atención a los cambios normativos que tengan directa relación con el plan, a las modificaciones de las líneas de negocio de la empresa, o a cambios en los procesos productivos que se han tenido en cuenta, que haría recomendable la revisión del programa. Esta tarea de revisión y verificación corresponderá al órgano de instrucción y control del cumplimiento normativo.

En todo caso, las tareas de revisión del modelo se instarán siempre y cuando se hayan modificado sustancialmente las normas legales que rijan el funcionamiento de la empresa o su sector de negocio o actividad, cuando cambien las condiciones de la empresa sobre las que se realizó este plan (al menos las que basaron la evaluación de los riesgos penales), o siempre que se reciban denuncias de incumplimientos de las normas del modelo o se detecten dichos incumplimientos.

5. CANAL ÉTICO / CANAL DE DENUNCIAS

5.I. Objeto y razón de ser.

A pesar de que actualmente la ley no determina claramente que sea una obligación normativamente hablando, resultaría difícilmente comprensible hablar de un modelo de prevención penal realmente eficaz sin que se establezca un procedimiento de recopilación de la información, en el que se reciban aquellos sucesos relativos a riesgos materializados, cerca de materializarse o bien sobre los que existan sospechas de haberse materializado. Para dar base a ese procedimiento de recopilación se crea un canal ético o canal de denuncias, que operará como estructura organizativa que hará posible que el modelo de respuesta pueda cumplir con sus objetivos, puesto que aportará la información necesaria sobre la posible comisión de un delito o materialización de un riesgo.

Este canal ético sustenta su funcionamiento sobre unos principios derivados de la finalidad perseguida, a saber:

- Integración en los procedimientos de la empresa.
- Sencillez para el comunicante.
- Diversidad de vías de acceso.
- Divulgación máxima de su existencia.
- Fiabilidad de la información.
- Confidencialidad

De estos principios, mención especial merece el último de los puntos, puesto que es el que más influye en sus características y uso. La confidencialidad del canal ético es su pilar fundamental, ya que garantiza al comunicante/denunciante que la información facilitada, así como sus datos personales serán tratados con total confidencialidad. En este punto, es necesario señalar que la confidencialidad del canal no implica necesariamente el anonimato. Así, la Agencia Española de Protección de Datos ha puesto en numerosas ocasiones sus objeciones a las denuncias anónimas, toda vez que el anonimato en las denuncias choca directamente con lo expuesto por ella en la “Guía de la protección de datos en las relaciones laborales” (AEPD, 2009). Por otra parte, la realización de una comunicación o denuncia no

implica más que un mecanismo de inicio de una actividad instructora o indagatoria por parte del órgano encargado del canal ético, en aras a averiguar cuanta información pudieran recabar para verificar los hechos comunicados/denunciados, siendo que de ese modo resultaría importante, por no decir imprescindible, que tanto para el comunicante como para el órgano encargado de la gestión fuese posible ponerse en contacto para ampliar o matizar las informaciones enviadas o recibidas, en función de las necesidades de la investigación realizada.

5.II Comunicación de infracciones.

A través del canal ético/canal de denuncias, cualquier persona podrá presentar sus dudas, sugerencias o quejas en relación al incumplimiento de los códigos internos de FRONTING. De igual forma, cualquier persona podrá presentar la oportuna comunicación/denuncia en caso de incumplimiento normativo alguno por parte de la empresa. Para su admisión y adecuada tramitación, las comunicaciones/denuncias deberán contener necesariamente los siguientes datos:

- Denunciante identificado con nombre y apellidos, y número de identidad.
- Exposición sucinta de los hechos o argumentos que sustenten la comunicación/denuncia.
- Persona o colectividad contra la que se dirige la denuncia.

Esta vía será la preferente para la puesta en conocimiento de FRONTING de cualquier posible incumplimiento normativo que se esté realizando o haya sido realizada. Sin embargo, dicha vía no es excluyente, por lo que en caso de que los órganos de la persona jurídica encargados del cumplimiento normativo tengan conocimiento efectivo por cualquier otro medio de la comisión de una conducta que pudiera ser constitutiva de un incumplimiento, iniciarán de oficio idénticas actuaciones idénticas a las que se pondrían en marcha ante la recepción de una comunicación por el canal de denuncias.

Como ya se ha señalado, en todo momento por parte del órgano instructor se mantendrá la confidencialidad del denunciante, salvo que dicha información sea requerida por autoridad competente para ello (judicial o administrative), en cuyo caso la empresa devendrá obligada a ceder dicha información al órgano requirente.

* Existiendo la posibilidad de que en el canal de denuncias se reciban, por alguno de los medios que lo permitan, algún tipo de comunicación donde no consten datos del denunciante, y a pesar de que el espíritu del canal es dar cumplimiento a lo expuesto por el gabinete jurídico de la A.E.P.D. de 2007, Informe para la Creación de sistemas de denuncias internas en las empresas (mecanismos de “whistleblowing”), de forma que en la medida de lo posible se eviten las comunicaciones anónimas, las mismas no serán automáticamente rechazadas, aunque nunca podrán servir como única prueba de la comisión de una irregularidad o un delito.

5.III. Comunicación y Tramitación.

La comunicación/denuncia se remitirá al órgano de control preferentemente por correo electrónico, en la dirección: prevenciónriesgospenales@fronting.es

Las denuncias que se reciban por otros cauces no serán desechadas, pero debido a que intervienen más factores y elementos ajenos a **FRONTING**, tanto en las comunicaciones postales como en las telefónicas, a pesar de que se realizará el máximo esfuerzo por velar por el mantenimiento de la confidencialidad de toda la información recibida, no es posible garantizar eficazmente dicho extremo. Por ello, se recomienda encarecidamente que la comunicación se realice directamente en el correo electrónico propuesto a tal fin, tanto por razón de temporalidad como de seguridad.

Recibida la comunicación/denuncia el órgano encargado de la gestión del canal ético iniciará las oportunas verificaciones y comprobaciones necesarias. En caso de que entre las personas afectadas por la comunicación/denuncia se encuentre alguna de las que formen parte del órgano instructor, esta deberá ser substituido por otro en las tareas de averiguación relacionadas directamente con la comunicación/denuncia en cuestión.

5.IV. Protección de datos y derecho a la intimidad.

En todo caso, se garantizará en todo momento la confidencialidad de la comunicación/denuncia. Las comunicaciones realizadas generarán un expediente que se registrará e identificará por una referencia, garantizándose el cumplimiento de lo previsto en la normativa de protección de datos. Todas las personas que intervengan en los posibles procesos de averiguación tienen la obligación de mantener la debida confidencialidad y mantener en secreto los datos e informaciones a que hayan tenido acceso, pudiendo en caso contrario ser sancionado.

ANEXO I.- ÓRGANO DE CONTROL Y ÓRGANO DE DECISIÓN.

I.- El Órgano de Control y Supervisión

1.- Funciones

Serán funciones del órgano de control el velar por el debido cumplimiento del modelo de prevención establecido, realizando las periódicas actualizaciones que puedan resultar necesarias.

El órgano de control y supervisión del modelo de prevención asumirá además entre sus funciones las labores de instrucción y gestión del canal en denuncias. En todo caso, mediante el uso de suplentes, se intentará mantener en la medida de lo posible el carácter colegiado del mismo, aún en casos de recusación o abstención de alguno de sus miembros por cualquier motivo.

2.- Composición.

Formarán dicho órgano,

- Asesor Jurídico
- Asesor contable
- Gerente

3.- Procedimientos relacionados con la gestión del Canal de Denuncias y la gestión de las Denuncias Recibidas.

El órgano de control y supervisión realizará las funciones de órgano de instrucción de las denuncias recibidas. Con relación a estas, el órgano tendrá encomendadas como mínimo las funciones de:

a) Gestión del canal de denuncias.

- 1.- Recepción de denuncias.
- 2.- Clasificación de denuncias.

b) Gestión de las denuncias recibidas.

- 1.- Instrucción de la denuncia.
- 2.- Redacción de informe dirigido al órgano de decisión.

Para realizar dichas funciones se detallan a continuación unas líneas básicas de carácter meramente orientativo en lo no relativo a las obligaciones legales, pudiendo el órgano de control estimar en cada caso concreto la realización de cuantas modificaciones considere procedentes en aras de una mejor consecución de sus objetivos.

a) Gestión del canal de denuncias.

En relación con la gestión de las denuncias recibidas por el canal de denuncias, corresponderá al órgano de instrucción tomar las decisiones debidamente justificadas correspondientes a los permisos de acceso, escritura, impresión, eliminación o bloqueo de datos almacenados, los plazos para su cancelación definitiva o las razones por las que se podrían acceder a datos bloqueados.

De conformidad con el artículo 15.1 de la LO 15/1999, el acceso a los datos almacenados por parte de un tercero interesado quedará limitado a los propios datos de carácter personal objeto de tratamiento, no pudiendo considerárselos datos de terceras personas como incluidos dentro de este derecho, de modo que tanto los datos del/los denunciante/s deberán mantenerse en todo caso bajo estricta situación de confidencialidad, así como cualesquiera otros datos relativos a terceros que consten en la comunicación recibida o en el expediente que se incoe.

Sobre la clasificación de las denuncias, esta función se corresponde con el análisis de las denuncias recibidas y la materialización de los riesgos que se den en la compañía, correspondiendo al órgano de control separar aquellas que realmente se corresponden a riesgos penales, y que por tanto deberán ser tramitadas por este órgano, de aquellas que responden a una casuística diferente, y que deberán ser dirigidas a los departamentos correspondientes si pudiesen ser de interés, o incluso desechadas directamente si no tuvieran trascendencia alguna. Para el caso de que la denuncia no tenga trascendencia penal, podrá el órgano de control omitir su incorporación al sistema de almacenamiento.

Toda denuncia o comunicación recibida con trascendencia penal implicará necesariamente el inicio de un expediente por parte del órgano de instrucción.

Para facilitar las tareas, tanto de clasificación como de instrucción, sería recomendable que cada denuncia devuelva un código de identificación a la persona que presenta una denuncia, de forma que se facilite al acceso a dicho expediente y la comunicación entre el órgano instructor y el denunciante, en caso de requerir nuevas comunicaciones entre las partes.

b) Gestión de las denuncias recibidas.

Iniciado el oportuno expediente, se analizará inicialmente el alcance de la información recibida, determinando si la información recibida afecta a alguna o algunas personas concretas. En caso de ser necesaria la recusación o abstención de alguno de los miembros que conforman el órgano de control, por verse afectados de forma directa por la información recibida, esta se producirá en este primer momento.

Para la instrucción de las denuncias el órgano podrá funcionar de forma colegiada o podrá el órgano, por designación, encomendar a uno de sus miembros la instrucción del procedimiento.

Iniciada la instrucción, el encargado de la misma podrá adoptar una serie de medidas urgentes, siempre motivadamente y con las siguientes finalidades:

- Paliar los efectos del riesgo materializado o por materializar.
- Ejecución de medidas urgentes para preservar las pruebas.
- Comunicación urgente, es su caso, de la información a los órganos de gobierno de **FRONTING**.
- Comunicación inmediata a los órganos policiales /judiciales en casos graves y flagrantes

Igualmente, si fuese necesario, podrá comunicar con el denunciante a los efectos de ampliar la información recibida, garantizando siempre la confidencialidad de identidad e información. Una vez realizada la instrucción, por el órgano de instrucción se aprobará una propuesta de resolución definitiva que se presentará al órgano de decisión un informe que contendrá:

- Información descriptiva de la denuncia, fechas de interposición y principales hitos.
- Medidas de urgencia llevadas a cabo, motivación de las mismas y efectos.
- Objetivación de la denuncia, análisis de la fiabilidad del denunciante y veracidad de la información.
- Valoración de si resulta necesario cualquier tipo de apoyo o asesoría externa.
- Propuesta de actuación y resolución, con proposición de las medidas ya adoptadas y que se deban mantener, la investigación del denunciante por deslealtad o por faltar dolosamente a la verdad, el envío de la información a los tribunales o agentes de la autoridad por ser delitos que no están dentro del ámbito de la persona jurídica.

Esta información será presentada a la mayor brevedad al órgano de decisión, a los efectos de que por **FRONTING** se pueda adoptar la decisión oportuna en el menor plazo posible.

4.- Procedimientos relacionados con la revisión del programa.

Los procedimientos y controles previstos en el modelo de prevención serán válidos en tanto se mantengan las idénticas condiciones sobre las que el mismo se diseñó, y mientras no se detecten fallos. También normativamente se establece esta obligación de revisión constante, puesto que la LO 1/2015 prevé expresamente la obligación de verificar de forma periódica el mismo.

Anualmente se realizará una revisión ordinaria del plan. En dicha revisión se valorará, como mínimo, los siguientes aspectos:

- La existencia de cambios o modificaciones sustanciales de normas legales que rijan el funcionamiento de la empresa o del sector o actividad de negocio, siempre que tenga entidad suficiente para afectar al plan de cumplimiento normativo.
- La existencia de cambios en las condiciones y estructura organizativa de la actividad de **FRONTING**, especialmente aquellas que fundamentaron la evaluación de los riesgos de este plan de cumplimiento normativo.

Si se detectara alguna de estas modificaciones con antelación a la revisión anual del plan, podrá esta adelantarse a los efectos de verificar la adecuación del plan a la nueva situación.

En todo caso, deberá instarse la revisión inmediata del plan en el momento en que por el órgano de control se detecte un incumplimiento de las conductas descritas en él.

* Actualmente las tareas relacionadas con este punto, de revisión y actualización del plan, se encuentran encomendadas por delegación a los servicios jurídicos de **FRONTING**, siendo este servicio el encargado de dichas tareas.

II.- El Órgano de Decisión.

1.- Funciones.

Corresponde al órgano de decisión la formación de la voluntad de la persona jurídica en respuesta a la posible comisión de un ilícito que afecte a la misma, y ello con fundamento en la presentación por parte del órgano instructor del oportuno informe detallado. Para la formación de dicha voluntad el órgano decisorio podrá solicitar asesoramiento de cuantos servicios externos sea necesario, así como cuantas aclaraciones requiera por parte del propio órgano de instrucción.

2.- Composición.

El órgano de decisión estará compuesto por los integrantes del Consejo de Administración de **FRONTING**.

Para la toma de decisiones, como ya se ha señalado, podrá asesorarse de cuantos servicios precise, tanto internos como externos.