Julio 2018
Asociación Europea
Abogados y Economistas
en Compliance

European Compliance & NEWS

La revista para los profesionales del Compliance editada por la Asociación Europea de Abogados y Economistas en Compliance

Entrevista

Entrevista a Don Emilio Ontiveros
Presidente de Analistas Financieros Internacionales
Catedrático de Economía de la Empresa de UAM

Noticias AEAEC

- Acuerdo estratégico con la International Compliance Association (ICA)
- Primer curso de auditor jefe en la norma UNE 19601:2017.
- Presentación del Software Compliance Protección de Datos (RGPD) desarrollado por la editorial Lefbvre-El Derecho.
- Presentación de la herramienta Gobertia para gestionar eficientemente el órgano de gobierno de las empresas.

ÍNDICE DE CONTENIDOS

PROMOVER - INFORMAR - FOMENTAR - APOYAR

*"**Ética y Compliance**: construyendo seguridad legal"*

Asociación Europea de Abogados y Economistas en Compliance
Passeig Mossen Jacint Verdaguer, 120- 08700 Igualada - Barcelona
Telf.: +34 938 049 038
info@aeaecompliance.com
Inscrita en el Registro Nacional de Asociaciones con número 609885

Redacción European Compliance & News
Cristina Vázquez Calo valencia@aeaecompliance.com / Luis Suarez Mariño asturias@aeaecompliance.com

EDITORIAL

Nuestro compromiso con los asociados
Avanzando en conocimientos y visibilidad

En el ánimo de servir a los asociados la AEAEC ha alcanzado en estos últimos meses dos acuerdos estratégicos de relevante importancia. Un acuerdo de colaboración con la International Compliance Association (ICA) y otro con ADOK

En virtud del convenio con la ICA los socios de la AEAEC pasan automáticamente a ser asociados de la ICA participando de los beneficios que conlleva ser socio de ambos asociaciones.

ICA es una asociación de compliance que actúa a nivel global, siendo el proveedor líder en materia de formación en compliance ofreciendo cursos de distinto grado en compliance, blanqueo de capitales, gobierno corporativo y muchas disciplinas más relativas al sector. Sus certificados están reconocidas en todo el mundo.

Cuenta con operadores regionales que ofrecen el apoyo a sus miembros, presentes en 130 países. A lo largo de su historia, ha otorgado más de 120.000 certificaciones en materia formativa. Además, cuenta con programas de servicios para empresas y eventos en los que se tratan materias de interés para los profesionales y las empresas ayudando a conocer las necesidades y tendencias en el mundo del compliance.

En paralelo a este acuerdo AEAEC ha alcanzado igualmente un acuerdo con ADOK. ADOK es una entidad acreditada para la certificación de sistemas de Gestión de la Calidad, Gestión Medioambiental, Seguridad y Salud laboral, Compliance Penal y es una de las siete entidades con designación provisional para expedir certificados de Delegados de Protección de Datos de conformidad con el Esquema AEPD-DPD.

Realiza auditorías y evaluaciones a medida en cualquiera de los ámbitos mencionados, bajo esquemas y requisitos de clientes o bien desarrollados por ADOK específicamente para el cliente: Evaluación de cumplimiento legal; auditorías de segunda parte; evaluación y calificación de proveedores; evaluación de franquicias y evaluaciones bajo especificaciones propias de cliente

Además ADOK Certificación cuenta con los derechos como Partner de la entidad alemana TUV HESSEN para su representación en exclusiva para España y Portugal. De este modo, sus clientes pueden optar a la certificación alemana con acreditación DAKKS, además de la acreditación de ENAC que como entidad española. Así sus clientes pueden ser certificados tanto con acreditación ENAC como DAKKS con el mismo equipo auditor.

En virtud del acuerdo alcanzado entre AEAEC y ADOK, los asociados de AEAC tienen la posibilidad de formarse como auditores jefe de la norma UNE 19601. Este mes se desarrolla en Madrid el primer curso en el que están participando quince socios de AEAEC.

Además en la medida que la auditoria de la UNE 19601 exige la participación de expertos en Derecho Penal, los asociados de AEAEC que cuenten con experiencia demostrada en esa rama del Derecho participaran en funciones auditoras de la mano de un auditor senior de ADOK.

Con estos Convenios la AEAC trata de cumplir su principal objetivo de potenciar las capacidades de sus socios en materia de Compliance para así reforzar la imagen de calidad, solvencia y profesionalidad de todos ellos.

ENTREVISTA A
Emilio Ontiveros Baeza

Emilio Ontiveros Baeza
Presidente de AFI, Analistas Financieros Internacionales

Tenemos la gran suerte de hablar hoy con Emilio Ontiveros Baeza, Presidente de Afi, Analistas Financieros Internacionales

Catedrático de Economía de la Empresa de la Universidad Autónoma de Madrid. Miembro del Grupo de Investigación Avanzada en Economía Internacional en 2005. Profesor invitado en varias universidades americanas. Autor de numerosos libros, artículos y colaboraciones en revistas especializadas y medios de comunicación. Director de la Revista Economistas desde su fundación hasta diciembre de 2011

Miembro de los Consejos de Redacción de varias publicaciones científicas y profesionales, y de los Consejos de Administración de varias empresas.

Gracias por recibirnos don Emilio. Me interesa especialmente la relación entre finanzas y ética y los programas de Compliance como medio de auto regulación.

Cuando la generalidad de los ciudadanos oyen hablar de sociedades de asesoramiento financiero e inversión, parece que les viene a la mente la figura del "lobo de Wall Street" **¿Se puede hacer compatible el trabajo profesional en el sector financiero e inversor con un comportamiento ético y la integridad personal y profesional como forma de entender y desarrollar esa actividad?**

Desde luego. El asesoramiento financiero es el resultado de la importancia y complejidad creciente que han cobrado las finanzas en las modernas economías. Nuestros trabajos siempre han combinado la presencia como consultores o asesores de entidades financieras (bancos y compañías de seguros, fundamentalmente), pero también como profesores, a través de nuestra Escuela de Finanzas. El rigor en la transmisión de conocimientos y experiencias puede y ha de ir asociado a la presencia de valores y referencias, no solo éticas, sino basadas en la honestidad profesional. Para que un sistema financiero funcione es necesario no solo la profesionalidad de sus participantes, sino el rigor y honestidad de todos.

Durante los años del boom inmobiliario hemos visto como la mayoría de entidades financieras ofrecieron swaps como seguros de cobertura de tipos de interés cuando en realidad eran productos financieros complejos

cuya contratación exigía, por parte del consumidor, un grado de conocimiento del mercado más elevado del que tenía la generalidad de los clientes a quienes se les ofrecieron. Por otra parte, la generalidad de las entidades ocultaron al consumidor sus datos internos sobre la perspectiva que tenían en relación al futuro devenir de los tipos de interés. **Cuando es la entidad quien ofrece un producto ¿no debería de actuar con total transparencia, asesorando al inversor conforme a su perfil, y haciéndole partícipe de sus propias prospectivas de futuro?**

Toda la oferta de productos y servicios financieros de cualquier tipo tiene que ir acompañada de la información suficiente sobre sus características y, desde luego, sobre el riesgo asociado. Junto a ello, la comercialización entre amplios consumidores requiere la verificación de que el inversor potencial dispone de elementos de juicio suficientes y de que su perfil de riesgo es el adecuado. Junto a todo ello, sería muy conveniente que, efectivamente, recibiera información rigurosa sobre los episodios que pueden condicionar el comportamiento de los instrumentos financieros. Con todo, más allá de las exigencias a los emisores de instrumentos financieros, o a sus comercializadores, es conveniente que los inversores se preocupen por disponer de las bases formativas necesarias. Aquí también es válida la proporción de "ser culto para ser libre".

Más tarde determinadas entidades ofrecieron como oportunidad acudir a la suscripción de ampliaciones de capital que luego han resultado desastrosas para el inversor.

¿Cómo diferenciar el riesgo propio de toda inversión financiera de que el inversor haya acudido a la misma sobre la base de una información precontractual que no respondía a la realidad o que al menos puede calificarse de dudosa?

Creo que es de todo punto necesario que con independencia de la información comercial o promocional de cualquier instrumento financiero el inversor revise detalladamente los folletos e información registrada de los mismos. Más allá de las palabras o del marketing financiero, hay que conocer el producto, la familia a la que perteneces y, con ello, la adecuación de su riesgo al perfil de cada inversor potencial. Todo ello, sin menoscabo de que las autoridades reguladoras y supervisora, ven por la calidad de las buenas practicas comerciales.

El 3 de enero de 2018 ha comenzado la aplicación del nuevo marco normativo sobre mercados e instrumentos financieros, basado en la directiva MiFID II y el reglamento MiFIR. La normativa pretende reforzar la protección del inversor, las condiciones de competencia en la negociación y liquidación de instrumentos financieros; así como mejorar la transparencia y la pervisión de los mercados financieros, incluidos los mercados de derivados.

¿Hasta qué punto las normas de conducta que impone esa norma impedirán este tipo de prácticas de que hablamos?

No la impedirán completamente, pero si su aplicación es correcta puede suponer un paso significativo.

¿En el fondo esas normas, se pueden calificar como normas éticas a las que se les ha dado valor de ley?

Normas de buen hacer, en general. De cumplimiento supranacional

¿Se puede decir que las entidades financieras tienen hoy unas obligaciones éticas legales, que les obligan a comportarse conforme a las reglas de la buena fe, la confianza y la transparencia con el consumidor?

Claro. Las normas existen desde siempre. Ahora se han mejorado y han asimilado la experiencia de la crisis. Pero, como es lógico, su eficacia depende de la forma de aplicación. Y de la cultura financiera de los inversores potenciales.

¿Hasta qué punto resultan las mismas un instrumento útil para desechar las malas prácticas de las que antes hablamos?

Claro que son útiles. Pero insisto que depende de más factores: la forma de aplicación y la formación de los clientes e inversores.

Parece hoy el pensamiento dominante aquél que dice que el capitalismo y el libre juego del mercado son los únicos sistemas económicos posibles y que la historia ha demostrado que son los que mejor han ayudado a la prosperidad de los pueblos. **¿En qué medida ello conjuga con el hecho de que las sociedades más prosperas sean aquéllas en que los Estados han establecido una regulación más exigente?**

La disposición de regulaciones adecuadas y bien supervisadas, e instituciones modernas y bien gestionadas, son un pilar básico del sistema económico. Y, en efecto, en el norte de Europa han avanzado bastante más que en el resto de los países.

Está claro que el capital se concentra, cada vez más, en menos manos y que las grandes corporaciones tienen cada vez mayor poder. **¿Hasta qué punto las mismas imponen a los Estados el marco regulatorio?**

Al menos lo intentan constantemente y los consiguen en ocasiones.

Hoy esta de moda el "Compliance" y la "autorregulación ética". **¿Hasta qué punto los programas de Compliance o cumplimiento normativo en las empresas financieras y el compromiso de las mismas con una cultura ética, producen beneficios positivos para las mismas?**

Claro que sí. A corto plazo deben llevar a cabo adaptaciones y quizás incurrir en costes adicionales, pero a medio y largo plazo hacer bien las cosas es rentable. Y esas exigencias de compliance van en esa dirección.

¿La cultura ética en las organizaciones es reflejo de la cultura ética de sus accionistas, directivos y empleados o viceversa?

No siempre, pero en muchas ocasiones es el activismo de los accionistas y la presión de los empelados la que acaba forzando esas adaptaciones.

¿Se puede concluir, o es demasiado pretencioso, que la ética es lo que hace eficaz al mercado, en virtud de su transparencia y por lo tanto de su confianza?

No solo la ética. Esta es una condición necesaria, pero no suficiente. Buena regulación, buena supervisión, adecuada formación de los empleados y clientes son igualmente condiciones para que se dé el círculo virtuoso.

¿Cómo convencer de ello a los operadores?

Convencer hoy, a tenor de las exigencias, no debe ser difícil. En todo caso, las autoridades y los clientes han de ser exigentes

¿Debe un Banco Central considerar las desigualdades sociales en la formulación de la política monetaria, y procurar la protección de quienes tienen menos capacidades de cubrirse de los efectos de la inflación y las crisis financieras?

No son los bancos centrales los que se han de preocupar preferentemente por la desigualdad, sino los gobiernos.

La humanidad tiene una agenda fabulosa en estos años venideros: asegurar la paz, el acceso de todos los seres humanos al agua potable y a los alimentos básicos; gestionar el cambio climático, caminar hacia la igualdad de oportunidades para todos - hombres y mujeres; países ricos y países pobres…-, procurar el acceso de todos los seres humanos a la vivienda, a la energía, a la educación, a las comunicaciones. **¿Son compatibles estos objetivos y la obtención del lucro lícito que busca el inversor financiero?**

Por supuesto que han de tratar de hacerlos compatibles. Para esos está la regulación y la supervisión. Si no es así, los clientes tendrán elementos para penalizar comportamientos poco adecuados.

¿Estamos adentrándonos en un sistema económico nuevo de la mano de la tecnología? ¿Qué caracteriza al mismo? Y según su criterio ¿qué deberíamos exigir del mismo en bien de la humanidad?

La tecnología, la digitalización creciente, el manejo inteligente de los datos pueden contribuir a mejorar la eficiencia del sistema económico, pero también a generar efectos no deseables socialmente. Para neutralizarlos han de estar atentos los gobiernos y los propios ciudadanos. El progreso tecnológico ha de ser compatible con el crecimiento inclusivo. Y si no es así, fallan los gobiernos.

Muchas gracias don Emilio, espero que la entrevista aporte a todos aquellos que trabajamos por un mundo mejor una luz de esperanza y confianza en el futuro.

“Compliance”

en el sector **público estatal**

Por Alberto Girón González
Economista, Interventor y Auditor del Estado
Técnico de Hacienda e Inspector de Hacienda del Estado

1. Introducción

“Compliance” es una de las palabras más usadas en la gestión empresarial y empieza a serlo en el ámbito de la gestión pública en España. Me han pedido un artículo divulgativo y por ello comenzaré aclarando que no es necesario introducir el “compliance” en el sector público porque existe desde tiempo inmemorial, cuestión distinta es que se puede mejorar y mucho.

Compliance significa en español cumplimiento de la normativa. Es decir “compliance” y cumplimiento normativo son lo mismo, aunque probablemente por razones comerciales se utiliza muchos más la palabra inglesa que la española, del mismo modo que por poner un ejemplo de algo similar es más común en el ámbito financiero utilizar la palabra inglesa swap, que la palabra española permuta. Obviamente el cumplimiento de la legalidad y la normativa en general es fundamental para el correcto funcionamiento del sector público. El Estado se dota de normas para regular su funcionamiento. Estas normas pueden tener distintas características en función de las características del propio Estado, democrático o autoritário. Pero todos los estados tienen normas, para regular entre otros aspectos su funcionamiento económico financiero y asegurar que los fondos públicos se dedican a las finalidades que hayan decidido quienes ostentan el poder político, y su gestión se adecúa a las normas que regulan dicha gestión. Si los políticos y los funcionarios no aplican las leyes o lo hacen a su antojo, no cumplen con su función. Esto es así mucho antes de que existieran los estados democráticos modernos, aunque obviamente cobra mucha mayor importancia en los estados democráticos porque para poder ser calificados como tales deben de estar sometidos a la Ley y al Derecho y perseguir el interés público. Por tanto, en los estados democráticos las ilegalidades son anomalías que debe ser limitadas al máximo, si bien obviamente es prácticamente imposible su erradicación total, como es imposible erradicar el crimen.

El cumplimiento legal no lo han inventado los anglosajones y no es algo que se ha inventado en el sector privado, que no existiera hace mucho tiempo en el sector público. Por el contrario, en el sector público existen desde tiempo inmemorial sistemas cuya finalidad es contribuir al cumplimiento de la legalidad. Esto puede parecer algo obvio para los que trabajamos en el sector público, pero no lo es para quien no lo conoce.

Por tanto, no se puede introducir el “compliance” en el sector público porque ya existe. Lo que sí se puede hacer es mejorar el cumplimiento normativo en el sector público. Y esta mejora desde luego no se va a producir tratando de exportar al sector público instrumentos que ni siquiera están suficientemente consolidados en el sector privado.

Obviamente para hacer propuestas útiles en ese sentido que puedan tener alguna posibilidad de ser viables, se debe partir del conocimiento de la organización cuyo sistema de cumplimiento legal o “compliance” se pretende modificar. Porque si lo que se pretende es exportar sin más a todo el sector público sistemas de organización diseñados para el sector empresarial el resultado probablemente sería un absoluto fracaso. Sería gastar dinero inútilmente porque lo importante no es tener un sistema de “compliance” sino que funcione y que funcione mejor que el que existe actualmente.

Profundizando algo más en el concepto de cumplimiento legal, podemos definir el “compliance” como función o como un conjunto de políticas, procedimientos y buenas prácticas. El Comité de Basilea define el “compliance” como una función independiente que identifica, asesora, alerta, monitorea y reporta los riesgos de cumplimiento en las organizaciones, es decir, el riesgo de recibir sanciones por, sufrir pérdidas financieras o pérdidas de reputación por incumplimientos de las leyes aplicables, las regulaciones, los códigos de conducta y los estándares de buenas prácticas (juntos “leyes, reglas y estándares”).

Desde otra perspectiva, se puede definir el “compliance” como un conjunto de políticas, procedimientos y buenas prácticas establecidas por una entidad para prevenir la realización por sus directivos, empleados, y terceros con los que mantiene relaciones comerciales o de otro tipo, de actuaciones contrarias a la legalidad, a su normativa interna y a los códigos éticos de los que se ha dotado a sí misma.

1. Causas del creciente interés por el cumplimiento normativo en el Sector Público

Hay varias razones para que últimamente se hable tanto del "compliance" o sea del cumplimiento legal en el Sector Público. A mi juicio las más importantes son las siguientes:

1·1 La progresiva sensibilización de la sociedad ante el fenómeno de la corrupción.

No todos los delitos que se pueden cometer en el sector público están relacionados con la corrupción, pero es indudable que la existencia de un buen sistema de cumplimiento legal dificulta, aunque no imposibilita la comisión de delitos de corrupción.

La R.A.E. define la corrupción:

"En las organizaciones, especialmente en las públicas, práctica consistente en la utilización de las funciones y medios de aquellas en provecho económico o de otra índole, de sus gestores"

Hay muchas definiciones de la corrupción pública. Utilizando elementos de las que me han parecido más interesantes he tratado de sintetizar el concepto en la siguiente: La corrupción en el sector público se puede definir como conducta realizada intencionadamente por un político o un empleado público en beneficio de intereses privados, propios o de terceros y en menoscabo del interés público. Asimismo, es corrupción pública el comportamiento de un tercero consistente en promover mediante la aportación de ventajas económicas o de otro tipo que el político o empleado público incumpla sus obligaciones en detrimento del interés público, y en beneficio de intereses privados no legítimos. La corrupción es lo contrario de la integridad que la OCDE define como la alineación con el cumplimiento de, los valores, principios y normas éticos compartidos, para mantener y dar prioridad a los intereses públicos, por encima de los intereses privados, en el sector público.

Las sociedades desarrolladas se ven afectadas por gravísimos casos de corrupción que minan los cimientos de la organización política y suponen un grave lastre para la economía. No es un fenómeno nuevo, pero en los últimos años se ha producido una creciente sensibilización de la población mundial informada sobre el fenómeno de la corrupción. Los gravísimos casos de corrupción en España son "prime time" todos los días y afectan a partidos políticos, instituciones y empresas estatales y por supuesto a empresas privadas, ya que no hay corruptos si no hay corruptores. Precisamente estos días hemos asistido a un cambio de gobierno en España mediante una moción de censura fundamentada en un caso de corrupción cuyo triunfo ha dado lugar a un cambio en el gobierno de España.

En la doctrina sobre la corrupción suele distinguirse entre la corrupción política y en la administrativa, en función de quienes son los sujetos afectados por la misma. En España el nivel de corrupción administrativa es muy bajo. Sin embargo, el nivel de corrupción política se ha convertido en uno de los problemas centrales del país, con graves consecuencias económicas difícilmente cuantificables y con gravísimas consecuencias políticas, cuyo análisis excede de este artículo. Sólo por incluir unas breves referencias las encuestas del CIS sitúan este problema sistemáticamente entre las grandes preocupaciones de la población. Por otra parte, en el último informe del Grupo de Estados contra la Corrupción (GRECO) se señala que de las once recomendaciones que se hicieron en el anterior informe para combatir la corrupción, España ha seguido siete de ellas de forma parcial, mientras que otras cuatro no las cumple en absoluto.

Pero siendo muy grave la corrupción en España, y afectando en mayor o menor medida según los casos a los principales partidos políticos y a las instituciones públicas, no es desde luego un problema en proceso de desaparición en países con un alto nivel de desarrollo.

Se trata de un fenómeno universal que afecta a todas las sociedades y a todas las economías, como así lo declara el Preámbulo de la Convención de las Naciones Unidas contra la Corrupción de 2003. Desgraciadamente estas consideraciones son de plena actualidad en 2.018. Si se hace un repaso de la prensa de los últimos meses descubre que autoridades de primer nivel de países como Brasil, Japón Francia, Israel o Sudáfrica están sometidos a procesos judiciales relacionadas con la corrupción.

Ahora bien, en España la repercusión mediática de determinados casos de corrupción derivada fundamentalmente de la gran relevancia pública de las personas a las que afectan junto con los recortes en los servicios públicos derivados de la crisis económica ha tenido la lógica consecuencia de una gran sensibilización de la población a la comisión de este tipo de delitos, hasta el punto de que la vida política española gira en buena medida sobre esta materia.

1·2 Las modificaciones del Código Penal que regulan la responsabilidad penal de las personas jurídicas que afectan a una reducida parte del Sector Público Estatal

En 2.003, mediante la Ley Orgánica 15/2.003 se modificó el Código estableciendo por primera vez la responsabilidad de la persona jurídica en determinados supuestos muy restringidos, pero fue en 2.010 cuando mediante una nueva modificación Del Código Penal se estableció la responsabilidad penal de las personas jurídicas de forma muy amplia, incluyendo en la misma los delitos más habituales del ámbito empresarial, estableciendo de manera muy difusa el atenuante de haber establecido antes del juicio oral, medidas para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica. En 2.015 mediante la Ley Orgánica 1/2.015 se vuelve a modificar el Código Penal estableciéndose las pautas sobre como tienen que organizarse las medidas eficaces para prevenir y descubrir los delitos que en el futuro puedan cometerse utilizando medios o bajo la cobertura de la persona jurídica, definiendo las características que deberían tener esas medidas para que en un eventual proceso judicial puedan ser consideradas como atenuantes o eximentes. Debe tenerse en cuenta a este respecto que el Código Penal establece que quién actúe como administrador de hecho o de derecho de una persona jurídica, o en nombre o representación legal o voluntaria de otra, responderá personalmente, aunque no concurran en él las condiciones, cualidades o relaciones que la correspondiente figura de delito requiera para poder ser sujeto activo del mismo, si tales circunstancias se dan en la entidad o persona en cuyo nombre o representación obre.

El ámbito de aplicación de esta reforma excluye a al Estado, a las Administraciones públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades Públicas Empresariales, a las

organizaciones internacionales de derecho público, así como a aquellas otras que ejerzan potestades públicas de soberanía o administrativas.

Sin embargo, si incluye a las sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, si bien solamente les podrán ser impuestas las penas consistentes en multas o intervención judicial. Esta limitación no será aplicable cuando el juez o tribunal aprecie que se trata de una forma jurídica creada por sus promotores, fundadores, administradores o representantes con el propósito de eludir una eventual responsabilidad penal.

Al igual que ha sucedido en el sector privado estas modificaciones legales han motivado a los directivos y consejeros de muchas empresas a modificar su organización para reducir el riesgo penal de las empresas y de ellos mismos, ya que el Código Penal establece que los administradores o los representantes legales responderán personalmente de los delitos que cometan las personas jurídicas, aunque no concurran e n ellos las condiciones, cualidades o relaciones que la correspondiente figura del delito requiera para poder ser sujeto activo del mismo. La exención de la responsabilidad de delitos cometidos en nombre y por cuenta de la empresa por sus representantes legales se produciría según el Código Penal si la empresa adopta una serie de medidas que trataré de sintetizar a continuación:

- El órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyan medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza que el cometido.

- La supervisión del funcionamiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y control o que tenga encomendada legalmente de supervisar los controles internos de la persona jurídica.

- Los autores individuales del delito lo han cometido eludiendo los modelos de organización y prevención.

- No se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se ha encomendado la supervisión del modelo de prevención.

> ***"Dependerá de la mayor o menor preparación de jueces y fiscales que sean capaces o no de detectar este tipo de sistemas cosméticos de compliance"***

En la implantación de sistemas de cumplimiento en el sector público o en el sector privado existe el riesgo, acerca del cual han advertido diversos fiscales, de que dichos sistemas tengan un carácter cosmético, es decir que se diseñen no para fomentar el cumplimiento normativo y prevenir la comisión de delitos, sino para tratar de dar la apariencia de que se tiene la voluntad de hacerlo. Dependerá de la mayor o menor preparación de jueces y fiscales que sean capaces o no de detectar este tipo de sistemas "cosméticos" de "compliance". Probablemente van a necesitar ayuda de expertos especializados si quieren llegar a conclusiones acertadas. En lo que respecta al sector de las sociedades mercantiles estatales puedo asegurar que hay múltiples maneras de aparentar la existencia de un buen sistema de "compliance", aunque en realidad sea pura apariencia porque en realidad no se quiere que funcione. Hay sistemas que es imposible que funcionen, por ejemplo, por falta de independencia de los responsables de cumplimiento o porque los principales responsables de la empresa lo consideran un simple requisito para evitar responsabilidades penales y que sobre el papel pueden estar incluso bien diseñados. Y desde luego es imposible que ningún sistema de cumplimiento funcione si la corrupción está instalada en los responsables de primer nivel o sin llegar a tanto, si su comportamiento dista mucho de ser ejemplar y abusan de su posición para obtener privilegios ilícitos. Desde mi punto de vista, la mejora de los sistemas de cumplimiento en las empresas no debe estar orientado ni exclusiva, ni fundamentalmente, a evitar la responsabilidad penal de las empresas y de sus administradores, sino a mejorar el cumplimiento de la normativa y a algo más amplio, a que la gestión económico financiera del sector público se realice respetando principios éticos y primando el interés público sobre cualquier otro. En ocasiones hay actuaciones que sin ser ilegales son contrarias a la ética que debe presidir la actuación de los responsables públicos.

La realidad es que desgraciadamente no ha existido un interés real en mejorar el cumplimiento en las sociedades mercantiles hasta que no se han producido las modificaciones del Código Penal que he mencionado anteriormente. En definitiva, existe un largo camino por recorrer.

2. **¿Cómo mejorar el cumplimiento normativo en el sector público?**

Obviamente para hacer propuestas útiles de mejora de la eficacia y eficiencia del "compliance" en el sector público que puedas tener alguna posibilidad de ser viables, se debe partir del conocimiento de la organización cuyo sistema de cumplimiento legal se pretende modificar, y efectuar una primera aproximación a cuál debe ser el sistema más idóneo a cada tipo de organización porque precisamente una de las características del sector público es la diversidad de las entidades que los componen. Nada tiene que ver un ministerio con una entidad pública empresarial, por ejemplo.

Si lo que se pretende es exportar sin más al sector público sistemas de organización diseñados para el sector empresarial el resultado probablemente sería un absoluto fracaso. Sería gastar dinero inútilmente porque lo importante no es tener un sistema de cumplimiento, sino que funcione y que funcione mejor que el que existe actualmente. Y para ello lógicamente hay que tener en cuenta las sustanciales diferencias que existen entre el sector privado y el sector público y entre las distintas entidades que conforman el sector público. En este documento por razones obvias de extensión solo es posible dar unas pinceladas no demasiado precisas de que es el sector público y sus características.

Espero que estas breves pinceladas sirvan al menos para transmitir la idea de la complejidad y heterogeneidad del sector público estatal español y aportar algunas ideas de cómo se puede mejorar el cumplimiento legal en ese sector.

2·1 ¿Qué es el Sector Público?

Como aproximación podemos decir que el sector público es el conjunto de entidades mediante los cuales el Estado hace cumplir la política o voluntad expresada en las leyes del país. El sector público como finalidad la satisfacción de los intereses generales. Por razones de espacio no puedo extenderme más sobre el asunto, ni comentar distintas definiciones existentes, entre las cuales la que me parece más completa es la de la OCDE, a cuya lectura invito, si se quiere profundizar sobre este tema. Aunque algunas de las consideraciones que efectuaré posteriormente son válidas a Comunidades Autónomas y Entidades Locales, a continuación, me voy a centrar en el Sector Público Estatal que es lo que me ha sido solicitado.

El Sector Público Estatal está formado por:

1. **Administración General del Estado**
2. **Sector Público Institucional**

a) Los organismos públicos vinculados o dependientes de la Administración General del Estado, los cuales se clasifican en:

1.º Organismos autónomos.
2.º Entidades Públicas Empresariales.

b) Las autoridades administrativas independientes.
c) Las sociedades mercantiles estatales.
d) Los consorcios.
e) Las fundaciones del sector público.
f) Los fondos sin personalidad jurídica.
g) Las universidades públicas no transferidas.

Además de los anteriores, existen otras entidades no incluidas en ninguna de las tipologías anteriores como: AEAT, Banco de España, CNI, Autoridades Portuarias y los Fondos sin Personalidad Jurídica.

Excede con mucho de la finalidad y posible extensión de este artículo apuntar simplemente las características de cada uno de ellos, pero si es imprescindible apuntar la enorme casuística existente en lo que respecta a:

El ejercicio o no de potestades administrativas.
Su organización.
Régimen económico, financiero y patrimonial.
Régimen de personal.
Régimen de contratación.
Régimen de control.

De la brevísima descripción del sector público estatal que he realizado en los párrafos anteriores se colige a mi juicio claramente su amplitud y complejidad.

El Sector Público está sometido en su actuación a la Ley y el Derecho. En este artículo divulgativo me voy a referir únicamente al cumplimiento de la normativa que regula la gestión económico-financiera. Pero debo advertir que la obligación de cumplimiento normativo del sector público no abarca únicamente a la normativa que regula la gestión financiera sino a otras normas que regulan aspectos como la prevención de riesgos laborales, la protección de datos, la prevención del blanqueo de capitales que afectan en general de las entidades del sector.

Y también hay entidades del sector público que tienen otras regulaciones específicas que cumplir como las que se refieren al juego o la de la seguridad ferroviaria, por poner algunos ejemplos.

Una de las características del Sector Público en España es la profusa y detallada regulación de la gestión económico-financiera y de otros aspectos de su funcionamiento interno. A continuación, figura una relación no exhaustiva de las normas con rango de Ley que regulan el Sector Público Estatal:

Ley General Presupuestaria.
Ley de Patrimonio del Estado.
Ley de Contratos del Sector Público.
Ley General del Subvenciones.
Ley de Régimen Jurídico del Sector Público.
Ley de Organización y Funcionamiento del Sector Público.
Ley Reguladora del Ejercicio del Alto Cargo.Ley de Incompatibilidades.
Estatuto del Empleado Público.
Ley de Transparencia y Buen Gobierno.

Todas las leyes anteriormente mencionadas y los reglamentos que desarrollan algunas de ellas contienen elementos de "compliance". Cada una de estas leyes, junto con la normativa que las desarrolla, regula distintos aspectos del funcionamiento de las entidades que conforman el sector público estatal, pero no lo hacen de manera uniforme sino atendiendo a las características de dichas entidades. Por poner unos ejemplos hay entidades públicas que tienen presupuesto limitativo y otras que lo tienen estimativo, hay entidades que están sujetas a la Ley de Contratos en su integridad, en tanto que otras únicamente lo están a sus principios, y otras a la denominada Ley de Sectores Excluidos. Hay entidades cuyo personal en su gran mayoría son funcionarios y otras cuyo personal es reclutado mediante sistemas de selección nada transparentes. Obviamente todas estas diferencias deben ser valoradas a la hora de proponer modificaciones a los sistemas de "compliance" existentes. En mi opinión las propuestas simplistas de importación de determinados elementos de "compliance" del sector privado, como el "compliance officer" no tienen ningún recorrido en la administración pública, aunque pueden ser objeto de estudio de cara a su posible implantación, previa regulación, en el sector público empresarial. Otros elementos de "compliance" como el análisis de riesgos pueden ser muy útiles en todo el Sector Público, y de hecho la Intervención General de la Administración ha empezado a impulsarlos, exigiendo a los gestores la entrega un documento de análisis de riesgos financieros en las auditorías de cuentas.

2·2 Claves para la mejora del cumplimiento en el Sector Público

Desde mi punto de vista las claves de cualquier sistema de cumplimiento normativo en el ámbito privado y en el público son las mismas, aunque la instrumentación de algunas de ellas *tienen que ser necesariamente distinta en ambos ámbitos.*

Aumentar la transparencia en la gestión pública.

Cuánta mayor transparencia existe en la gestión económico financiera pública, más difícil es realizar actos de corrupción sin dejar rastros que puedan dar lugar a investigaciones. Por eso la transparencia es fundamental para minimizar el riesgo de corrupción. El mayor o menos grado de transparencia en la gestión pública dependen de la voluntad de los políticos, que suelen estar más interesados en la transparencia en la gestión cuando están en la oposición que cuando están en el poder. De ahí el papel de la parte de la sociedad civil no mediatizada por intereses partidarios y de la prensa no sometida al poder político.

El establecimiento de la cultura de cumplimiento.

Se puede definir la cultura de cumplimiento como el conjunto de valores y de conocimientos que coadyuvan a que los miembros de una organización cumplan las leyes en el ejercicio de su actividad y en la

Establecer una cultura de cumplimiento consiste en transmitir a toda la organización la importancia de los valores éticos y los conocimientos necesarios para que esos valores y conocimientos soporten el funcionamiento de la organización

Va más allá de transmitir valores en abstracto, sino que tiene que ir acompañado de la formación de todos los empleados en la legalidad a aplicar y en los sistemas de control que permitan aplicarla.

El establecimiento de la cultura del cumplimiento es mucho más difícil si el reclutamiento de los empleados se realiza mediante procedimientos opacos en los que no se garantiza la aplicación de los criterios de mérito y capacidad. Desgraciadamente es práctica frecuente en el sector público empresarial y fundacional. El nepotismo es una forma de corrupción que facilita otras formas de corrupción.

La selección de los directivos de las organizaciones basándose en el mérito, la capacidad y probada honestidad.

En mi opinión la primera premisa para que cualquier sistema de cumplimiento legal funcione es que los directivos de las organizaciones sean de probada honestidad y que la selección de los mismo se base en el mérito y en la capacidad, y no en criterios arbitrarios como la pertenencia a un partido político o amistad, como desgraciadamente ocurre con muchísima frecuencia en nuestro país-. Ningún sistema de puede ser eficaz si los máximos responsables del sector público y de cada una de las entidades que lo conforman no son los primeros que están imbuidos de la cultura de cumplimiento y toman las decisiones necesarias para que el sistema funcione adecuadamente, entre otras liderar el sistema de cumplimiento y dotarle de medios.

Por otra parte, el efecto demostración es fundamental para que funcione el cumplimiento de una organización. Resulta algo obvio que los empleados de la empresa no se pueden en tomar en serio las medidas de cumplimiento si los directivos o altos cargos son los primeros en incumplir las reglas o si tienen comportamientos poco ejemplares abusando de su posición para obtener ventajas personales no legítimas.

Despolitización del control externo.

El control externo del sector público en España esta atribuido al Tribunal de Cuentas. Esta organización carece de credibilidad debido a la politización endémica. Los consejeros que dirigen la institución no son seleccionados en base a su competencia técnica en materia de fiscalización y auditoría, sino en base a criterios partidistas

Establecimiento de un sistema eficaz de control interno

La prevención de actos ilegales exige que la organización esté dotada de un buen sistema de control interno.

Existen muchas definiciones de control interno. En mi opinión una de las más claras y didácticas es la de INTOSAI 2004 (muy similar a la definición de COSO), que define el control interno del siguiente modo:

“El control interno es un proceso integral efectuado por la gerencia y el personal, y está diseñado para enfrentarse a los riesgos y para dar una seguridad razonable de que, en la consecución de la misión de la entidad, se alcanzarán los siguientes objetivos gerenciales:

Ejecución ordenada, ética, económica, eficiente y efectiva de las operaciones.
Cumplimiento de las obligaciones de responsabilidad.
Cumplimiento de las leyes y regulaciones aplicables.
Salvaguarda de los recursos para evitar pérdidas, mal uso y daño.

En el ámbito del sector público estatal en mi opinión existe mucho margen para la mejora de los sistemas de control interno. Excede de las posibilidades de este artículo describir la normativa que regula el control interno en el sector público estatal, las competencias de las distintas instituciones de control y los distintos procedimientos que se utilizan en función del tipo de entidades.

A mi juicio, en el sector público existe un sistema de control interno bastante robusto pero muy ineficiente y obsoleto. Sin entrar en detalle en la administración el sistema se realiza fundamentalmente, aunque no de forma exclusiva, mediante controles previos muy poco eficientes, existiendo una tendencia a neutralizarlos desviando actividades hacia el sector empresarial en el que los recursos dedicados al control son manifiestamente insuficientes, a pesar de que por la actividad que desarrollan las sociedades y entidades empresariales y forma de provisión de los puestos directivos e intermedios y los criterios más opacos de reclutamiento del personal, el riesgo de irregularidades es mucho mayor, como evidencia que la mayoría de los delitos de corrupción cometidos en el sector público no se cometen en la administración sino en el sector empresarial. A mi juicio, es necesaria una reforma integral del control interno en el sector público estatal inspirada en la implantación progresiva del modelo COSO, cuyas líneas fundamentales deberían ser las siguientes:

Separación absoluta de las funciones contables y de auditoría y de control financiero.

Debe atribuirse de forma exclusiva a los órganos gestores la responsabilidad sobre la adecuación a la legalidad de las operaciones de gestión económica, correspondiendo a los órganos de control la verificación posterior. Lo anterior debe ir acompañado de la eliminación progresiva de los sistemas de fiscalización previa, que se realizan acto a acto y sin valoración de riesgos. Estos sistemas que han sido abandonados en todos los países desarrollados y en la Comisión Europea por su ineficiencia y porque tienen el efecto perverso de descargar de responsabilidad a los responsables de la gestión.

Sustitución de los controles previos de la IGAE por auditorías de cumplimiento y operativas o controles financieros permanentes realizados por interventores u auditores del Estado y técnicos de auditoría, sin dependencia alguna del órgano gestor e integrados en la Intervención General de la Administración del Estado, a la que se debe garantizar una mayor independencia y de muchos

más recursos de los que ahora dispone. En los últimos años, se ha ido en la dirección contraria, debilitando este órgano de control.

Distribuir los recursos para el control del sector público estatal en función de los riesgos existentes., eliminando controles intensivos y anacrónicos sobre operaciones de muy escaso riesgo e intensificación de controles de operaciones de mayor riesgo como la contratación y ejecución de contratos de infraestructuras y de publicidad.

Incremento del control en el sector público empresarial. Actualmente se destinan en términos relativos muchos más recursos al control de la administración que a las entidades donde existe más riesgo, las empresas públicas estatales. En éstas el control es manifiestamente insuficiente.

Establecimiento obligatorio en la administración y en todas las entidades públicas de sistemas de evaluación de riesgos.

Publicación de los resultados más significativos de las auditorias, no solo de las de cuentas. Actualmente se está incumpliendo la Ley General Presupuestaria que obliga a la publicación de un informe anual comprensivo de dichos resultados.

Implantación de la cultura de la rendición de cuentas en los gestores y en los órganos de control.

Creación de órganos especializados en investigar el fraude.

En los últimos años hemos asistido a una sofisticación de los mecanismos para defraudar recursos públicos. De ahí la necesidad de que además de órganos de control generalistas existan órganos especializados en investigar indicios de fraude con suficientes recursos para realizar esa función.

Sistemas de denuncias y protección de los denunciantes

Al igual que sucede con otro tipo de delitos, los de corrupción que afectan al sector público son en muchas ocasiones muy difíciles de detectar y de ahí la colaboración inestimable que pueden ofrecer los denunciantes, siempre que dichas denuncias reúnan condiciones suficientes para ser investigadas. En mi opinión es un grave error no admitir denuncias por ser anónimas. Hay muchas personas que quieren contribuir a la legalidad de las operaciones de gestión económica pero que no están dispuestas a sufrir el calvario que actualmente sufren en España los denunciantes de corrupción, que por su condición de tales se enfrentan a personajes muy poderosos del ámbito político y empresarial.

Control interno
sobre la información financiera.

Hipólito Álvarez Fernández
Economista. Censor Jurado de cuentas (ICADE E-2)
Socio Director en Nexus Corporate

La información financiera constituye el elemento fundamental de comunicación con todos los interesados, directa e indirectamente, en la marcha de las empresas.

*En un entorno empresarial y social donde los requisitos de transparencia han evolucionado de forma muy importante, se hace imprescindible que los sistemas de control interno lo hagan de forma adecuada y sean capaces de proporcionar una **seguridad razonable** sobre la **fiabilidad** de la información financiera.*

Para enmarcar adecuadamente las cuestiones que vamos a abordar en este artículo, fijemos los siguientes conceptos:

Gestión de riesgos corporativos: proceso diseñado para identificar eventos potenciales que puedan afectar a la organización y gestionar los eventuales riesgos dentro de los umbrales aceptados, proporcionando un nivel de seguridad razonable sobre el logro de los objetivos.

Control interno: proceso efectuado por el consejo de administración, la dirección y demás personal de la organización con el objetivo de proporcionar seguridad razonable en la consecución de la eficacia y eficiencia de las operaciones, fiabilidad de la información financiera, cumplimiento de normas aplicables y salvaguarda de los activos.

El control interno forma parte íntegra de la gestión de riesgos corporativos y sus cinco componentes básicos, que deben estar relacionados a través de un proceso integrado, son los siguientes: (i) entorno de control; (ii) evaluación de riesgos; (iii) actividades de control; (iv) información y comunicación; y (v) supervisión.

Sistema de Control Interno de la Información Financiera (SCIIF): es una parte del control interno y se configura como el conjunto de procesos que el consejo de administración, el comité de auditoría, la alta dirección y el personal involucrado de la entidad llevan a cabo para proporcionar seguridad razonable respecto a la fiabilidad de la información financiera.

La información financiera incluye el balance, la cuenta de pérdidas y ganancias, el estado de cambios en el patrimonio neto, el estado de flujos de efectivo, la memoria y la información de naturaleza contable contenida en el informe de gestión. En lo normativo, su elaboración ha de cumplir los requisitos del Plan General de Contabilidad (PGC) y la Normas Internacionales de Información Financiera (NIIF), así como cualquier otro requisito legal aplicable.

Más allá de los aspectos formales y regulatorios, la información financiera, para ser útil, ha de caracterizarse por su fiabilidad.

Se considera que ha sido elaborada con fiabilidad si presenta las transacciones, hechos y demás eventos que afectan a la entidad. Para ello, el Sistema de Control Interno de la Información Financiera (SCIIF) debe asegurar que se cumplen cinco cuestiones básicas:

1. Existencia y ocurrencia: las transacciones, hechos y demás eventos recogidos por la información financiera efectivamente existen y se han registrado en el momento adecuado.

2. Integridad: la información refleja la totalidad de las transacciones, hechos y demás eventos en los que la entidad es parte afectada.

3. Valoración: las transacciones, hechos y demás eventos se registran y valoran de conformidad a la normativa aplicable.

4. Presentación, desglose y comparabilidad: las transacciones, hechos y demás eventos se clasifican, presentan y revelan de acuerdo con la normativa aplicable.

5. Derechos y obligaciones: la información financiera refleja, a la fecha correspondiente, los derechos y obligaciones a través de los correspondientes activos y pasivos, de conformidad con la normativa aplicable.

EL SCIIF debe proporcionar una seguridad razonable sobre la fiabilidad de la información financiera que las entidades difunden. Para ello, los elementos de un sistema de control interno - entorno de control, evaluación de riesgos, actividades de control, información y comunicación y supervisión - deben estar coordinados y operar de forma conjunta para **prevenir, detectar, compensar, mitigar o corregir errores con impacto material, o fraudes** en la información financiera.

Cuando el sistema está razonablemente diseñado y sus elementos funcionan de manera adecuada, se puede considerar que es eficaz y proporciona una seguridad razonable de que la información financiera se prepara de forma fiable.

No obstante, una debilidad manifestada en un elemento no implica necesariamente que el sistema de control interno sea inadecuado, siempre que esté compensada o mitigada por el efecto de otros elementos. Por tanto, evaluar la eficacia de un SCIIF requiere analizar una amplia variedad de aspectos y formas de actuación en la organización de la entidad, lo que exige, a su vez, **altas dosis de juicio profesional.**

En lo relativo a principios y buenas prácticas recomendadas en control interno, la referencia internacionalmente reconocida son los Informes COSO (COMMITTEE OF SPONSORING ORGANIZATIONS).

Cinco son los **componentes** esenciales:

1. Entorno de control de la entidad.

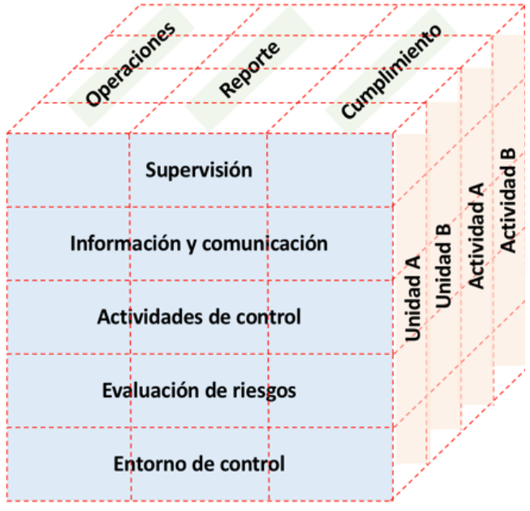
   Engloba factores tales como la integridad, los valores éticos, la competencia profesional, la filosofía de dirección y el estilo de gestión o la estructura organizativa. Marca las pautas de comportamiento de una organización y tiene influencia directa en el nivel de concienciación de personal respecto al control interno. De hecho, constituye la base de todos los demás elementos de control interno, aportando disciplina y estructura.

   Un porcentaje significativo de los recursos humanos de cualquier organización está involucrado, directa o indirectamente, en la elaboración de la información financiera. Los trabajos del área encargada de preparar los estados financieros dependen, en gran medida, de la información que le suministran el resto de los departamentos de la organización. Por tanto, el número de personas involucradas en la preparación de la información financiera es muy superior a los responsables de su elaboración.

2. Evaluación de riesgos de la información financiera.

   La evaluación de riesgos permite analizar el **impacto** de los potenciales eventos en la **consecución de objetivos** relacionados con la fiabilidad de la información financiera. Diversos riesgos pueden afectar a dicha fiabilidad, entre otros: errores de cálculo o de aplicación en las normas; fallos en los sistemas; fraudes contables; desconocimiento de información clave; estimaciones o proyecciones incorrectas; y otros de diversa naturaleza.

   Estos riesgos generales se traducen en aspectos concretos dentro de cada componente de la organización y en cada epígrafe y desglose de la información financiera, pudiendo variar de una entidad a otra. Por ejemplo, el riesgo de cometer errores en el registro de los ingresos será tratado de forma diferente por una entidad que utilice estimaciones sobre el grado de avance de los proyectos en curso, donde el control se centrará en los errores humanos y los procesos de supervisión para prevenir fraudes, que en otra entidad cuyas ventas dependan del registro diario de miles de transacciones, que pondrá el énfasis en la solidez de los sistemas informáticos.



El desconocimiento y la falta de actualización del proceso para identificar los riesgos de error pueden tener impactos relevantes en la información financiera y debilitar cualquier actividad de control. Este proceso es un pilar básico de un sistema de control adecuado y descansa, a su vez, en un **buen conocimiento de los negocios de la entidad** y de los procedimientos de preparación de la información financiera.

Por tanto, se puede esperar que la entidad disponga de un sistema, aprobado y supervisado por los niveles jerárquicos adecuados, que analice estos riesgos y sea la base del resto de componentes del SCIIF.

3. Actividades de control

   Las actividades de control tienen que realizarse en varios niveles de la organización para reducir los riesgos de incurrir en errores, omisiones o fraudes que puedan afectar a la fiabilidad en la información financiera. Estas actividades deben cubrir los riesgos que se hayan identificado en el inicio de las operaciones, su autorización, registro, procesamiento y divulgación de la información financiera.

   El **consejo de administración y la alta dirección** suelen utilizar, como herramientas de control de la gestión, análisis comparativos del rendimiento real con el previsto, indicadores de la evolución de los negocios y de la posición financiera, proyecciones presupuestarias y planes plurianuales. También revisan los juicios y asunciones realizados en aquellas áreas donde la complejidad de las transacciones y su impacto contable son más relevantes. En consecuencia, además de la autorización de transacciones significativas, las actividades de control típicas del consejo y la alta dirección se basan en procedimientos de revisión analítica de las estimaciones y proyecciones utilizadas, así como de los principales juicios asumidos en la preparación de la información financiera.

   En el **resto de la organización**, las actividades de control suelen consistir en procedimientos sistemáticos que requieren un menor conocimiento de la globalidad de las operaciones de la entidad. No obstante, estas actividades de control deben ser comunicadas por la alta dirección de manera que sean comprendidas por todos los empleados y desarrolladas de forma adecuada. La implantación del sistema de control en toda la organización permite al consejo de administración y la alta dirección limitar sus funciones a las actividades selectivas anteriormente mencionadas.

   Conviene diferenciar entre los controles cuyo objetivo es conseguir la eficacia y eficiencia de las operaciones, de aquéllos otros cuya finalidad es asegurar la fiabilidad de la información financiera:

   Las entidades disponen, normalmente, de una serie de procedimientos, controles y mecanismos de supervisión diseñados para garantizar el correcto desarrollo de las operaciones y el logro de los objetivos de la organización. Estos dispositivos se suelen denominar controles operativos.

   Las actividades de control del SCIIF incluyen aquellas que cubren riesgos asociados a la información financiera, entre las que figuran aquellas que, cumpliendo una función primordialmente operativa, tienen un impacto directo sobre dichos riesgos.

4. Información y comunicación

   Los **sistemas de información y comunicación** identifican, recogen, procesan y distribuyen la información sobre las transacciones, hechos y demás eventos que afectan a la entidad, en un periodo de tiempo que permita a las personas involucradas realizar las funciones que tienen asignadas.

Los **sistemas de información y comunicación** identifican, recogen, procesan y distribuyen la información sobre las transacciones, hechos y demás eventos que afectan a la entidad, en un periodo de tiempo que permita a las personas involucradas realizar las funciones que tienen asignadas.

Los sistemas de comunicación interna sirven para difundir a la organización los criterios, pautas, instrucciones y, en general, la información con la que deben contar sus miembros para desarrollar sus funciones y el tiempo que disponen para su desempeño. Los sistemas de información deben estar **diseñados para facilitar los datos necesarios, internos y externos, que puedan tener un impacto significativo** en los informes financieros.

La bondad de los sistemas de información y comunicación, interna y externa, es crítica para alcanzar los objetivos de la fiabilidad en la información financiera.

5. Supervisión del funcionamiento del sistema

   La supervisión del sistema es fundamental para mantener una seguridad razonable de que los riesgos por errores, omisiones o fraudes en la información financiera están siendo efectivamente controlados, ya sea por prevención, detección, mitigación, compensación o corrección. Un sistema de control interno, aunque haya sido adecuadamente diseñado, puede no estar funcionando, total o parcialmente, o no ser operativo en tiempo y forma, sin que tales circunstancias se revelen y se puedan corregir.

   El entorno en el que actúa la entidad es cambiante y los riesgos pueden variar, entre otras causas, por: (i) coyuntura económica; (ii) evolución del sector al que pertenece la entidad; (iii) avances en las tecnologías de la información; (iv) aparición de nuevos tipos de transacciones; y (v) modificaciones en las normas de preparación de la información.

Para cada uno de estos componentes, a continuación, se detallan algunas de las características que deberían reunir:

1. Entorno de control de la entidad.

a) Órganos y funciones responsables de la **existencia y mantenimiento** de un adecuado SCIIF, su implantación y su supervisión.

b) Departamentos y/o mecanismos encargados del diseño y revisión de la estructura organizativa, de definir claramente las **líneas de responsabilidad y autoridad** y de que existan **procedimientos** suficientes para su correcta difusión en la entidad.

c) Que existan, especialmente en lo relativo al proceso de elaboración de la información financiera, los siguientes elementos:

Código de conducta.
Canal de denuncias.
Programas de formación y actualización periódica para el personal involucrado en la preparación y revisión de la información financiera.

2. Evaluación de riesgos de la información financiera.

Principales características del proceso de identificación de riesgos, incluyendo los de error o fraude, en cuanto a:

Proceso **documentado.**

Que cubra la **totalidad de objetivos** de la información financiera: (existencia y ocurrencia; integridad; valoración; presentación, desglose y comparabilidad; y derechos y obligaciones).

Que esté **actualizado**.

Existencia de un proceso de identificación del **perímetro de consolidación**, teniendo en cuenta la posible existencia de estructuras societarias complejas, entidades instrumentales o de propósito especial.

Que el proceso tenga en cuenta los efectos de otras **tipologías de riesgos** (operativos, tecnológicos, financieros, legales, reputacionales, medioambientales, etc.).

Qué órgano de gobierno supervisa el proceso.

3. **Actividades de control.**

a) Documentación descriptiva de los **flujos de actividades y controles.**

b) Políticas y procedimientos de control interno sobre los **sistemas de información.**

c) Políticas y procedimientos de control interno destinados a supervisar la gestión de las **actividades subcontratadas** a terceros.

d) **Procedimientos de revisión y autorización** de la información financiera y la descripción del SCIIF.

4. **Información y comunicación.**

a) Existencia de una función específica encargada de definir y mantener actualizadas las **políticas contables.**

b) Manual de políticas contables actualizado y comunicado.

c) Mecanismos de captura y preparación de la información financiera con formatos homogéneos, de aplicación y utilización por todas las unidades de la entidad.

Será necesario identificar el perímetro de consolidación, teniendo en cuenta la posible existencia de estructuras societarias complejas, entidades instrumentales o de propósito especial

5. **Supervisión del funcionamiento del sistema.**

a) Disponer de una función de **auditoría interna.**

b) Contar con un **procedimiento de discusión** mediante el cual, los diferentes expertos puedan comunicar a la alta dirección y al comité de auditoría o administradores de la entidad las debilidades significativas de control interno identificadas durante los procesos de revisión de las cuentas anuales.

c) Alcance de la revisión del SCIIF, sus **resultados y plan de acción** que trate de corregir o mitigar las debilidades observadas.

d) Detalle de las eventuales **medidas correctoras y consideración de su impacto** en la información financiera.

> ***"La función de auditoria interna como elemento fundamental en la supervisión del funcionamiento del sistema"***

La **seguridad** a la que se debe aspirar es la razonable, en tanto siempre existirá el limitante del costo en que se incurre por el control, que debe estar en **concordancia con el beneficio que aporta.**

Debemos recordar que disponer de un adecuado sistema de control interno aporta, a las entidades, mucho más que seguridad y fiabilidad en la información que se prepara y elabora. Es un **instrumento de alta calidad y utilidad para la toma de decisiones** organizativas, operativas, estratégicas, financieras, comerciales, etc.

Hemos de tener en cuenta que la tendencia natural de las iniciativas empresariales es al crecimiento y ello conlleva un aumento progresivo de la distancia entre los accionistas, órganos de gobierno y la realidad diaria. Los medios que se empleen para reportar la verdadera situación y evolución de la organización deben aportar confianza, fiabilidad y seguridad. **Cuando shareholders y stakeholders tienen la garantía de que la información que se les aporta cumple todos estos requisitos, se genera un intangible de gran valor, una fuerte ventaja diferencial.**

El Delegado de Protección de Datos (DPD/DPO) y su comparativa con el Corporate Compliance Officer (CCO)

José Luis Colom Planas
Director de Auditoría y cumplimiento normativo en Audertis

> ***"En entornos de Compliance la coexistencia de ambos roles vendrá marcada por la ausencia de conflictos de interés."***

1. INTRODUCCIÓN AL COMPLIANCE

1.1 Aparición del término Compliance Officer

Si desde un punto de vista simplista nos limitamos a traducir el término anglosajón *Compliance por cumplimiento*, vemos que conceptualmente no es ninguna novedad ya que desde tiempos pretéritos la sociedad en su conjunto se organiza alrededor de normas y obligaciones de todo tipo que deben cumplirse, siendo las más relevantes las jurídicas.

No obstante, en los últimos años, el término Compliance se ha puesto en valor en entornos corporativos, quizá coincidiendo en España con la Ley Orgánica 5/2010, de 22 de junio, por la que se modificaba el Código Penal de 1995, introduciendo en nuestro país la responsabilidad penal de la persona jurídica. Posteriormente, con la última reforma en 2015 mediante la Ley Orgánica 1/2015, de 30 de marzo, se continuaba reconociendo en el Código Penal dicha responsabilidad, a la vez que se determinaba con mayor detalle cómo podía una organización verse exonerada de la misma. A partir del redactado del artículo 31 bis 2 CP, apareció indirectamente la función de Compliance Officer, a la que nos referiremos a menudo en este artículo como Corporate Compliance Officer (CCO).

Un hecho reseñable es que, entre ambas reformas, apareció la norma ISO 19600:2014, sobre Sistemas de Gestión de Compliance, que define: *"Compliance es el resultado de que una organización cumpla con sus obligaciones"*. Esta definición de amplio recorrido no circunscribe las obligaciones únicamente al ámbito penal, ni siquiera jurídico, sino que incardina dentro de Compliance las normas internas, las normas de adscripción voluntaria – como pueden ser las normas ISO - e incluso los requisitos contractuales, laborales o aquellos que puedan estar obligando a la organización. Naturalmente en los sistemas de gestión de Compliance basados en la norma ISO 19600:2014, partiendo de un completo análisis del contexto en el que opera la organización, debe determinarse el alcance del propio sistema, en base a seleccionar de qué marcos normativos u obligaciones se gestionará el cumplimiento. Este alcance delimitará sin duda las competencias específicas del CCO.

1.2 Aparición del término Delegado de Protección de Datos

El año 2016 fue aprobado el Reglamento (UE) 2016/679, de 27 de abril, *Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que*

que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, conocido como Reglamento General de Protección de Datos (RGPD) que ha finalizado el 25 de mayo de 2018 su período de vacatio legis, siendo actualmente de aplicación en todos los Estados de la Unión y ampara, después del Corrigendum de fecha 19 de abril de 2019, al tratamiento de datos personales de interesados "que se encuentren en la Unión", como acepción más amplia que la anterior de "residentes en la Unión". En el RGPD se introduce una nueva figura de cumplimiento normativo respecto a la protección de datos: El Data Protection Officer (DPO) referido en España como delegado de protección de datos (DPD).

Esta figura tiene mucho mayores atribuciones y exige mayor competencia que el rol de Responsable de Seguridad (DSO por sus siglas en inglés) que en España venía determinando por el derogado RD 1720/2007, Reglamento de aplicación de la anterior LOPD. Pensemos que las únicas competencias del DSO eran, según el artículo 5.2.l) RLOPD, coordinar y controlar las medidas de seguridad aplicables según se detallaban en el Documento de Seguridad. El DPD, en cambio, tiene una visión holística e integral de la protección de datos en la organización, para lo que se requieren conocimientos especializados del Derecho y práctica en protección de datos, que lo elevan a otro nivel profesional.

2. FUNCIONES ASIGNADAS

2.1 Funciones asignadas al CCO

Si nos ceñimos al ámbito penal, la condición segunda del apartado 2 del art. 31 bis CP dispone: *"2.ª la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica"*. Luego únicamente se explicitan como funciones del CCO la supervisión del funcionamiento del modelo de prevención (en la práctica del Sistema de Gestión del Cumplimiento) y la de su cumplimiento por parte de quienes están sometidos a él, junto a la supervisión de la eficacia de los controles internos de la organización.

Está claro que, si ampliamos el alcance del Compliance más allá de la RPPJ, las funciones pueden aumentar.

La norma UNE 19601:2017 sobre Sistemas de gestión de Compliance penal, trata las responsabilidades del CCO, y de la función de Compliance, en el apartado 5.1.2 Órgano de Compliance penal. Por su parte, la norma ISO 19600:2014 sobre Sistemas de gestión de Compliance, trata en el apartado 5.3.4 las responsabilidades de la función de Compliance en general.

2.2 Funciones asignadas al DPD

Según dispone el art. 39 RGPD, el DPD tendrá como mínimo las siguientes funciones que paso a resumir: a) informar y asesorar a la organización y a los empleados que se ocupen del tratamiento de datos personales; b) supervisar el cumplimiento de lo dispuesto en el RGPD y en otras disposiciones de protección de datos que sean de aplicación y de las políticas de la organización en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos (EIPD) y supervisar su aplicación de conformidad con el artículo 35; d) cooperar con la autoridad de control; e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

También ser interlocutor válido para los interesados que quieran ejercer sus derechos frente a la organización donde presta sus servicios, pudiendo resumir que mantiene contactos a tres bandas: con la Autoridad de Control, con el Responsable del Tratamiento dónde ejerce y con los interesados o afectados por los tratamientos.

2.3 Las tres líneas de defensa

La función de Compliance, ya estemos hablando del CCO, o más especializada en protección de datos como es el caso del DPD, debe tener suficiente grado de autonomía e independencia en sus funciones para no verse condicionada por intereses departamentales en conflicto con la cultura de cumplimiento corporativa. Ahora bien, al ser sus funciones principales las de vigilancia y control, por un lado, y de asesoramiento sobre cumplimiento, por otro, el contacto con las diferentes áreas funcionales o departamentos de la empresa ha de ser máximo. Esto viene reforzado por cuánto conocemos respecto a la elaboración del mapa de riesgos penales, que se extiende por todos los procesos de negocio de la empresa y todas las áreas funcionales, sin excepción, y por la teoría ampliamente aceptada de las tres líneas de defensa.

Esta teoría diferencia una primera línea consistente en la ejercida por los responsables de las diferentes áreas, puesto que la mayoría de circunstancias siempre suelen ocurrir en las áreas operativas; el poder supervisar y controlar en origen es condición necesaria para disponer de la suficiente agilidad para minimizar los incumplimientos y garantizar la eficacia de los controles. Una segunda línea la conforma la función de Compliance que vigila y asesora a las áreas operativas. También elabora los análisis de riesgos en su área de competencia en colaboración con dichas áreas que son las que conocen mejor que nadie los riesgos con los que conviven a diario. La tercera línea la constituye auditoría interna con sus evaluaciones, pero a menudo limitada en el tiempo a una única intervención anual para no agotar a los auditados.

3. ESTATUTO PROFESIONAL

3.1 Estatuto profesional del Compliance Officer

Actualmente no se dispone de un estatuto profesional del CCO, en lo que se refiere al ámbito de la RPPJ. De hecho, el Código Penal ni tan siquiera nombra a dicha figura, limitándose a señalar como hemos visto en la condición 2ª del art. 31 bis 2 CP que *"la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica"*.

Ha habido muchas voces que claman su promulgación y también esfuerzos encaminados a perfilar su posición por parte de determinadas organizaciones profesionales, que han elaborado documentos titulados "Estatuto del Compliance Officer" y "Libro blanco sobre la función de Compliance" que, aun siendo muy buenas aportaciones, carecen de valor jurídico. Esto nos lleva a que cada vez se considera más necesario disponer de un estatuto profesional para el CCO, o para la función de Compliance en general, que clarifique sus funciones, derechos y responsabilidades. Mientras llega, la mejor solución consiste en detallar como una adenda al contrato las funciones específicas del CCO en relación a su desempeño, dejando bien clara cualquier pretendida delegación de funciones desde la posición originaria de garante del administrador, aspecto que analizamos más adelante.

3.2 Estatuto profesional del Delegado de Protección de Datos

En cuanto al DPO, en lo formal tampoco se dispone de estatuto profesional, aunque si algo en lo material, deduciéndose de los artículos 37, 38 y 39 que constituyen la sección 4 sobre el Delegado de Protección de Datos del propio Reglamento (UE) 2016/679.

Como ejemplo citaré que tanto el responsable como el encargado del tratamiento respaldarán al DPD en el ejercicio de sus funciones (Art. 38.2 RGPD), garantizarán que no reciba ninguna instrucción en lo que respecta al desempeño de sus funciones, ni podrá ser destituido o sancionado por desempeñarlas (Art. 38.3 RGPD), también, pese a hacerlo de forma muy generalista, se explicitan sus requisitos de designación (Art. 37.5 RGPD) y la necesaria publicidad que debe darse al nombramiento (Art. 37.7 RGPD).

Por todo ello podemos afirmar a día de hoy que el desempeño profesional del DPD está más determinado y mejor protegido que el del CCO, no solo por tener las funciones más claramente delimitadas, sino por dedicarse al DPD tres artículos completos en el RGPD frente a ninguno respecto al CCO en el Código Penal, en lo que se refiere a su faceta de velar por la prevención de la RPPJ, como se ha visto en el apartado anterior.

4. DESIGNACIÓN DEL CCO Y DEL DPD

Podemos definir la justicia rogada como la petición dirigida a un órgano judicial para que éste dé a cada una de las partes, especialmente a la propia, lo que le corresponda o pertenezca. Desde este punto de vista, la exoneración de responsabilidad penal de la PJ deberá rogarse en justicia si se estima conveniente, no siendo obligatorios ni los modelos de prevención de delitos ni, en consecuencia, disponer de un CCO. En cambio, si extendemos el alcance del sistema de gestión de Compliance más allá de la RPPJ, debe estudiarse con detenimiento la necesidad, incluso la obligatoriedad, de determinadas funciones, como pueden ser la del Responsable de Prevención en PRL, el Representante ante el SEPBLAC en sujetos obligados por la LPBC/FT, el Delegado de Protección de Datos en la Administración pública y en determinadas circunstancias, etc. Dichas funciones cubren determinados aspectos de cumplimiento en las organizaciones, pudiendo actuar de forma independiente, aunque coordinada, o colegiados en un órgano general de cumplimiento.

En el caso del CCO, incluso, el apartado 3 del artículo 31 bis CP señala que *"En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2.ª del apartado 2 podrán ser asumidas directamente por el órgano de administración"*, estableciendo así un umbral de elusión en la independencia de la figura.

El caso del DPD es distinto al del CCO, ya que es su propia designación la que viene regulada por Ley. Concretamente, el art. 37.1 RGPD establece tres supuestos de obligatoriedad, que vienen desarrollados de forma práctica en el art. 34 del proyecto de nueva Ley Orgánica de Protección de Datos, determinando la necesidad de su designación en función del tipo de entidades de que se trate, detallando un numerus clausus o catálogo de 15 de ellas que van desde los colegios profesionales hasta la seguridad privada.

5. EL DEBER DE GARANTE

5.1 El deber de garante originario en las organizaciones

No escapa a la lógica de la razón admitir que, en el ámbito y en representación de la persona jurídica (PJ), el Administrador tiene los deberes propios de garante sobre la conducta de sus empleados.

Este poder lo ejerce de dos formas consecutivas:

Primero, desde la perspectiva in *eligendo,* estableciendo los controles adecuados en el proceso de selección de los trabajadores.

Después, *in vigilando*, supervisando su desempeño profesional, en la medida de sus posibilidades razonables, especialmente con los puestos más especializados.

Se puede decir que este poder de supervisión y control está orientado como:

Garante de protección, desde una perspectiva *ad intra,* evitando resultados lesivos para la propia empresa y sus empleados.

Garante de control, desde una perspectiva *Ad extra,* evitando resultados lesivos sobre terceros, externos a la organización, a partir de la actividad de los empleados.

En consecuencia, puede afirmarse que el Administrador de la PJ se encuentra en una posición de garante originaria, que le obliga a impedir la comisión de delitos por parte de subordinados con repercusión en bienes jurídicos de terceros.

Por ello, Los Administradores deben establecer los mecanismos de organización adecuados para evitar los riesgos de comisión de ilícitos en su seno o, en todo caso, mitigarlos hasta niveles tolerables por las circunstancias de la PJ. Ello, no obstante, no exonera al Administrador de su posición final de garante.

Dicho de otra manera, la comisión por omisión se dará en relación a los riesgos típicamente unidos a la actividad empresarial que tienden a descontrolarse, de no ponerse remedio, con el paso del tiempo y su inevitable evolución.

La propia norma UNE 19601:2017, en su apartado 5.3.2 sobre delegación de facultades, señala: *"En los casos en que la alta dirección delegue la toma de decisiones en ámbitos en los que exista riesgo penal mayor que bajo, la organización debe establecer y aplicar un procedimiento y un sistema de controles que garanticen que el proceso de decisión y el nivel de autoridad de los decisores sean adecuados y estén libres de conflictos de interés reales o potenciales. NOTA: La delegación de la toma de decisiones no exonera a la alta dirección de sus propios deberes y responsabilidades en cuanto a la prevención de los riegos penales. Tampoco transfiere a las personas delegadas las posibles responsabilidades legales en materia de supervisión o adopción de decisiones que les corresponda"*.

Citando el Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital, en su art. 236.1 señala: *"Los administradores responderán frente a la sociedad, frente a los socios y frente a los acreedores sociales, del daño que causen por actos u omisiones contrarios a la ley o a los estatutos o por los realizados incumpliendo los deberes inherentes al desempeño del cargo, siempre y cuando haya intervenido dolo o culpa"*, quedando como indelegable la responsabilidad que se deriva de su deber de garante originario. En consecuencia, sin perjuicio de las funciones propias del CCO, siempre corresponderá al Órgano de Administración establecer la política de control y gestión de riesgos de cualquier tipo de la organización y su supervisión, que en las sociedades cotizadas tiene la condición de facultad indelegable, conforme lo establece el art. 529 ter 1 b) de la referida Ley de Sociedades de Capital *"El consejo de administración de las sociedades cotizadas no*

podrá delegar las facultades de decisión a que se refiere el artículo 249 bis ni específicamente las siguientes: (…) b) La determinación de la política de control y gestión de riesgos, incluidos los fiscales, y la supervisión de los sistemas internos de información y control".

5.2 Transferencia del deber de garante al CCO y/o al DPD

¿Qué ocurre si la empresa delega varias de esas responsabilidades de garante originarias en una figura específica como puede ser el Delegado de Protección de Datos (DPD) o el Corporate Compliance Officer (CCO), cada una en su área de competencias?

La respuesta es que constituye un mecanismo de transferencia de la posición de garante porque, basándonos en esa delegación, el Administrador como delegante hace surgir una posición de garantía en el CCO o DPD, en calidad de delegado. Cabe decir que la posición de garante del Administrador no desaparece del todo, pudiendo pasar a ser residual, ya que la delegación correctamente efectuada modifica la posición jurídica del delegante liberándole de los deberes inherentes del ámbito competencial de que se trate, pues de lo contrario, carecería por completo de sentido que se llevara a cabo. Al administrador ya no le incumbe cómo se articulará el control de la fuente de riesgo, que le corresponde al CCO o al DPD, pero sí le compete la correcta selección, formación e información del responsable de cumplimiento, la dotación a esta figura de los medios necesarios para el cumplimiento de sus funciones y, especialmente, el deber de vigilancia sobre éste en el sentido de verificar su gestión.

Si llega a producirse un incidente motivado por una dejación de funciones del CCO o del DPD, la organización mantiene su responsabilidad última entendida en un caso como posible responsabilidad penal de la persona jurídica donde opera un CCO y, en otro, asumiendo su responsabilidad como Responsable, *Corresponsable o Encargado del Tratamiento* en relación a la protección de datos personales, donde opera un DPD.

Una prueba de que el administrador mantiene su responsabilidad última, pese a que CCO y DPD dispongan de autonomía, sería el hecho de estar facultado a destituirlos. Esto es así en el caso del CCO respecto a Compliance penal, dado que el art. 31 bis CP y concordantes no señala nada al respecto. En cambio, en el caso del DPD el art. 38.3 RGPD señala que *"No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones"*.

6. COEXISTENCIA DE AMBOS ROLES (CCO y DPD)

En entornos de Compliance la coexistencia de ambos roles vendrá marcada por la ausencia de conflictos de interés.

En el caso del DPD viene explicitado en el art. 38.8 RGPD que dispone: *"El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses"*.

En cambio, el Código Penal español nada dice al respecto del CCO, debiendo acudir a la Circular 1/2016 de la FGE, que señala: *"Para conseguir los máximos niveles de autonomía, los modelos deben prever los mecanismos para la adecuada gestión de cualquier conflicto de interés que pudiera ocasionar el desarrollo de las funciones del oficial de cumplimiento, garantizando que haya una separación operacional entre el órgano de administración y los integrantes del órgano de control que preferentemente no deben ser administradores, o no en su totalidad"*.

En consecuencia, caso de ausencia de conflictos de interés nada impide concentrar en pequeñas organizaciones ambos roles en la misma persona física. No obstante, debe garantizarse que concurran en el candidato las competencias necesarias para poder desempeñar ambos roles. Dicha concurrencia será poco habitual al requerirse profundos conocimientos jurídicos, técnicos y organizativos en protección de datos, seguridad de la información y gestión de riesgos para las funciones de DPD y de Derecho Penal, de gestión de riesgos y de muchas otras especialidades según el alcance adoptado de Compliance, para las funciones de CCO.

7. RESPONSABILIDAD Y PROTECCIÓN JURÍDICA DEL CCO Y EL DPD

7.1 En relación al deber de garante del CCO

La responsabilidad de cualquier desempeño en una organización radica en su "posición de garantía". Son el Administrador, o quienes tengan delegadas competencias de dirección general o alta dirección operativa, quienes serán poseedores de dicha posición. Bajo esa concepción será siempre el poder ejecutivo en la organización quien tiene el dominio de la fuente de riesgo, mientras que el CCO no posee en el mismo nivel dicha posición de garantía, concluyendo su responsabilidad - *prima facie* - con el deber de advertir, vigilar e informar de los riesgos propios de la actividad a la alta dirección operativa.

Dicho en otras palabras, el órgano de administración y, como máximo, la alta dirección operativa, conservan o en su caso adquieren, respectivamente, el deber de garante general originario respecto a la evitación de la comisión de delitos. En cambio, el CCO no se convierte en "garante" ya que el Código Penal únicamente le encomienda la función de *"supervisar la eficacia de los controles internos de la persona jurídica" y "funciones de supervisión, vigilancia y control"*, como se desprende del art. 31 bis 2 CP, pero no la posibilidad de contener y evitar la comisión del posible hecho delictivo, es decir, no posee el "dominio del hecho" propio del autor de un ilícito tipificado penalmente, incluso equiparando su desempeño a una posición directiva, como sucederá en múltiples ocasiones para legitimar y garantizar su comunicación directa con los órganos de gobierno corporativo. Adicionalmente, si tuviera conocimiento cierto de que va a cometerse, se está cometiendo, o se ha cometido un delito en el seno de la organización, su única responsabilidad es notificarlo al órgano de administración para que éste obre en consecuencia a su capacidad sancionadora, capacidad de la que adolece el CCO.

No obstante, el CCO podría ser responsable de un delito de omisión si incumple un deber especifico de actuación cuya observancia hubiera impedido o dificultado la comisión de un delito por parte de un tercero en el seno de la empresa.

Para poder atribuir responsabilidad a quién omite una acción se requiere dolo - intencionalidad o conocimiento cierto de que con su inactividad se contribuye al delito, equiparable a cómplice necesario o coautor- o dejación de funciones -comisión por omisión- concretándose este último supuesto en el Derecho Español mediante la necesidad de (1) Posición de garante: La existencia de una posición de garante en previsión de un hecho perjudicial; (2) Conexión: La existencia de alguna conexión entre omisión y responsabilidad; (3) Resultado: La producción de un resultado dañino íntimamente ligado al

hecho; (4) Previsibilidad: Que no se haya producido el hecho por la concurrencia de otros factores externos, imprevisibles o inevitables, ajenos a los que configuran la específica posición de garante, ya que éste factor imprevisible eximirá de cualquier responsabilidad al omitente que está situado como garante, al tener su origen el resultado lesivo en factores insalvables; (5) Posibilidad de actuar: la necesidad de que el omitente obligado estuviera en condiciones de realizar la conducta prevista. En caso de imposibilidad de actuar no surge responsabilidad por la inacción, eliminando la responsabilidad inherente a la situación de garante.

Ya el Tribunal Supremo ha señalado en la sentencia nº 797/2010, de 10 de septiembre, con MARCHENA GÓMEZ como presidente de la Sala Segunda del Alto Tribunal, referida a la realización omisiva de un ilícito penal en los delitos de resultado, indica en el FD 17 que: *"La jurisprudencia de esta Sala, si bien ha reconocido expresamente que la admisibilidad de una participación omisiva es de difícil declaración, ha aceptado ésta, asociando su concurrencia a la de los elementos propios del art. 11 del CP, entre ellos, que el omitente ocupe una posición de garante (STS 1273/2004, 2 de noviembre). De ahí que sea posible incluso en los delitos de acción, cuando la omisión del deber de actuar del garante haya contribuido, en una causalidad hipotética, a facilitar o favorecer la causación de un resultado propio de un delito de acción o comisión y que podría haberse evitado o dificultado si hubiera actuado como le exigía su posición de garante (cfr. SSTS 19/1998, 12 de enero, 67/1998, 19 de enero, 221/2003, 14 de febrero)".*

Para acabar este apartado, analizaré la referencia que hace la Circular 1/2016 de la FGE respecto a la posición del CCO en relación con su responsabilidad penal y la de la persona jurídica: *"Por un lado, el oficial de cumplimiento puede con su actuación delictiva transferir la responsabilidad penal a la persona jurídica a través de la letra a) puesto que, como se ha dicho, está incluido entre las personas que ostentan facultades de organización y control dentro de la misma. Por otro lado, puede ser una de las personas de la letra a) que al omitir gravemente el control del subordinado*

permite la transferencia de responsabilidad a la persona jurídica. En este supuesto, la omisión puede llevarle a ser él mismo penalmente responsable del delito cometido por el subordinado. Finalmente, si el oficial de cumplimiento omite sus obligaciones de control, la persona jurídica en ningún caso quedará exenta de responsabilidad penal (condición 4ª del art. 31 bis 2). De conformidad con este planteamiento, la exposición personal al riesgo penal del oficial de cumplimiento no es superior a la de otros directivos de la persona jurídica. Comparativamente, su mayor riesgo penal sólo puede tener su origen en que, por su posición y funciones, puede acceder más frecuentemente al conocimiento de la comisión de hechos delictivos, especialmente dada su responsabilidad en relación con la gestión del canal de denuncias y siempre que la denuncia se refiera a hechos que se están cometiendo y que, por tanto, el oficial de cumplimiento pueda impedir con su actuación".

7.2 El CCO como testigo o como investigado en la instrucción penal

El Juez del Juzgado Central de Instrucción n.º 5 de la Audiencia Nacional ha citado como investigados a siete CCO del Banco de Santander y BNP Paribas, en la pieza separada de entidades financieras de la lista Falciani, por delitos de blanqueo de capitales.

Alfredo Domínguez, socio de Derecho Penal y Coordinador de Corporate Compliance de Cuatrecasas, expuso en unas recientes jornadas que, a su juicio, se está *"muy cerca"* de vulnerar el derecho de defensa de la persona jurídica en la actual situación, *"si el representante de la organización se acoge a su derecho a no declarar y el fiscal o la acusación llama al CCO como testigo y le obliga a testificar". "La persona jurídica, al igual que la física, tiene derecho a definir su estrategia y aportar las pruebas que considere oportunas y necesite".*

No entramos aquí, pero también tuvo lugar hace poico en el ICAM una jornada sobre la responsabilidad civil del CCO. Se refuerza pues la necesidad de disponer de un estatuto profesional de la función de Compliance.

7.3 Responsabilidad del DPD

Buscando cierto paralelismo entre ambas figuras, DPD y CCO, según afirma Mar España, directora de la AEPD, *"La posición del DPD será próxima a los niveles jerárquicos más elevados dentro de una organización, de manera que aquellos a quienes reporte tengan capacidad de decisión en calidad de Responsables o Encargados del tratamiento. En ningún caso el DPD sustituirá al Responsable del Tratamiento en la toma de decisiones sobre los fines y alcance de los tratamientos, ni deberá asumir la carga de las posibles sanciones en las que pudieran incurrir los Responsables como consecuencia de tratamientos de datos no acordes con el RGPD".*

> ***"La persona jurídica, al igual que la física, tiene derecho a definir su estrategia y aportar las pruebas que considere oportunas y necesite".***

BIBLIOGRAFÍA

MACIÁ GÓMEZ, RAMÓN "La posición de garante en el Derecho español: concepto y estructura". Pórtico legal (Expansión). Enero de 2009.

SILVA SÁNCHEZ, JESÚS-MARÍA. "Fundamentos del Derecho Penal de la empresa". EDISOFER S.L.

SILVA SÁNCHEZ, JESÚS-MARÍA. "El delito de omisión: Concepto y sistema". Colección Maestros del Derecho Penal nº 12. Editorial IBdeF.

GOMEZ-ALLER, DOPICO. "Presupuestos básicos de la responsabilidad penal del Compliance Officer y otros garantes en la empresa". Actualidad Jurídica Aranzadi Nº 843, página 2. Año 2012.

COLOM, JOSE LUIS. "Compliance en la persona jurídica y las tres líneas de defensa". Blog "Aspectos Profesionales". 26 de enero de 2017.

MONZÓIN PÉREZ, HELENA. "La naturaleza de la relación laboral del delegado de protección de datos". UPF - IUSLabor 2/2017.

ANLLO, LINA y ALGUACIL, JIMENA. "¿Tiene el Compliance Officer responsabilidad penal?". Comisión Directiva del capítulo argentino de la WCA.

OSUNA, FERNANDO. "A vueltas con la responsabilidad penal del Chief Compliance Officer". LEFEBVRE – El Derecho. 05/10/2017.

ESPAÑA, MAR. "El Delegado de Protección de Datos: esquema de certificación, nombramiento, funciones y perfil requerido". LEFEBVRE - El Derecho. 01/08/2017.

Confederation on Data Protection Organizations (CEDPO). "Posición de CEDPO sobre el Delegado de Protección de Datos (DPO) en el Reglamento General de Protección de Datos (RGPD)".

¿Obligación o conveniencia de que las empresas denuncien o se autodenuncien, por los delitos detectados en su seno?

Bernardo del Rosal Blasco
Catedrático de Derecho Penal
Abogado de Urraza, Mendieta & Del Rosal Abogados
Socio Honorífico de la **AEAEC**

En el periódico "El Economista" del pasado día 15 de junio, se recogían unas manifestaciones del fiscal jefe de la Fiscalía Especial contra la Corrupción y la Criminalidad Organizada, Alejandro Luzón, hechas en el III Congreso Internacional del Compliance, quien, al parecer, dijo: *"la empresa que es capaz de descubrir un delito dentro de su organización y comunicarlo a la autoridad con una autodenuncia no tiene que pasar ni un minuto expuesta al procedimiento penal"*.

Así como en otros sistemas jurídicos esta afirmación puede ser cierta y su realidad casi cotidiana, en España, si la tomamos en su sentido literal, lamentable o afortunadamente –según se mire—, no lo puede ser, a la vista de cuál es la legislación penal y procesal vigente y cuál es la potestad que dicha legislación concede a las fiscalías para decidir acerca de la persecución penal de los individuos o de las empresas. De modo que, **con carácter general, no es posible decir que un fiscal se puede comprometer con una empresa a que si se autodenuncia no va a ser perseguida en el procedimiento penal que, a continuación, se incoe como consecuencia, precisamente, de esa autodenuncia. Cosa distinta es que la autodenuncia pueda beneficiar a la empresa, mitigando las consecuencias punitivas de la detección, en su seno, de un delito, cuando ésta trasciende y provoca la puesta en marcha de un procedimiento penal.** Voy a tratar de explicar las razones de estas reflexiones.

Tal y como disponen los vigentes arts. 124, núms. 1 y 2, de la Constitución española y arts. 100 y 105.1 de la Ley de Enjuiciamiento Criminal (en adelante "LECrim"), el ejercicio de la acción penal es público y obligatorio para el Ministerio Fiscal, cuya actuación está regida por el principio de legalidad y no por el principio de oportunidad. Es cierto que la reforma de la Ley Orgánica 1/2015, de 30 de marzo, introdujo, en la LECrim, en el procedimiento para el juicio sobre delitos leves (los castigados las penas leves del art. 33, núm. 4, del Código Penal), una nueva redacción en el art. 963, núm. 1, 1ª, de modo que:

> *"Recibido el atestado conforme a lo previsto en el artículo anterior, si el juez estima procedente la incoación del juicio, adoptará alguna de las siguientes resoluciones:*
>
> *1.ª Acordará el sobreseimiento del procedimiento y el archivo de las diligencias cuando lo solicite el Ministerio Fiscal a la vista de las siguientes circunstancias:*
>
> *a) El delito leve denunciado resulte de muy escasa gravedad a la vista de la naturaleza del hecho, sus circunstancias, y las personales del autor, y*
>
> *b) No exista un interés público relevante en la persecución del hecho. En los delitos leves patrimoniales, se entenderá que no existe interés público relevante en su persecución cuando se hubiere procedido a la reparación del daño y no exista denuncia del perjudicado.*
>
> *En este caso comunicará inmediatamente la suspensión del juicio a todos aquellos que hubieran sido citados conforme al apartado 1 del artículo anterior.*
>
> *El sobreseimiento del procedimiento será notificado a los ofendidos por el delito".*

Igualmente, y para los casos en los que el procedimiento se haya incoado por denuncia directamente presentada por el ofendido ante el Juez, el art. 964, núm. 2, apartado a), prevé que éste acuerde *"el sobreseimiento del procedimiento y el archivo de las diligencias cuando resulte procedente conforme a lo dispuesto en el numeral 1.ª del apartado 1 del artículo anterior"*.

Pero estos supuestos, de tímida posibilidad de ejercicio del principio de oportunidad por parte del Ministerio Fiscal, no están recogidos para los casos del procedimiento abreviado (enjuiciamiento de delitos castigados con penas no superiores a nueve años de prisión o con cualesquiera otras penas de distinta naturaleza, sea cual sea su cuantía y duración) ni para los casos del sumario ordinario (penas superiores a nueve años de prisión). Por tanto, si el delito no es leve, el fiscal no puede ofrecer a la empresa esa posibilidad de la que hablaba Alejandro Luzón; todo lo más, se podrán ofrecer los conocidos acuerdos de conformidad (véase, en este sentido, lo dispuesto en los arts. 779, núm. 1, 5ª, y 801 –juicios rápidos—, 784, núm. 3, y 787 de la LECrim), pero muy raro va a ser que la empresa pueda evitar el peregrinaje por la fase instructora, teniendo la condición de investigada en el proceso penal y teniendo que demostrar, en su caso, la eficacia de su programa de prevención.

A estos efectos de conseguir el acuerdo más beneficioso posible, o de mitigar las consecuencias penales tras el juicio oral, si tal acuerdo no es posible, es importante tener presentes las circunstancias atenuantes que, para las empresas, prevé el art. 31 quater del CP, a saber: haber realizado, con posterioridad a la comisión del delito y a través de sus representantes legales, las siguientes actividades: a) haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades; b) haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para esclarecer las responsabilidades penales dimanantes de los hechos; c) haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito; y d) haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica.

Por lo demás, en el caso del enjuiciamiento de delitos leves, sí es cierto que el fiscal, si la empresa se autodenuncia, le puede garantizar el sobreseimiento, obviamente, siempre que se den las condiciones de los preceptos antes transcritos, pero lo cierto es que el sobreseimiento también lo tiene garantizado ex lege la empresa, aunque sea el perjudicado el que denuncie, obviamente, siempre que se den los requisitos de los arts. 963, núm. 1, 1ª, y 964, núm. 2, apartado a), de la LECrim. Aparte de que estamos ante casos, el de los delitos leves, que no es tan frecuente que se den en las empresas, o que les resulten tan problemáticos a las empresas.

Es necesario establecer, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos

Por tanto, **a la hora de autodenunciarse, la empresa debe de ser consciente de que el Ministerio Fiscal no le puede garantizar, en absoluto, librarse del procedimiento penal, ni siquiera le puede garantizar librarse *pronto* del procedimiento penal; y, por supuesto, menos aún si no tiene implantado un eficaz programa de prevención de delitos. Eso sí, iniciado el procedimiento penal e iniciada la fase de instrucción, cuanto mejor esté implementado ese programa de prevención más posibilidades tiene la empresa de lograr el sobreseimiento antes del juicio oral.**

Dicho esto, a las empresas y a los *compliance officers* les suele preocupar mucho poder tener una respuesta clara a dos preguntas muy concretas: primera, ¿hay obligación de autodenunciarse o de denunciar cualquier delito que la empresa haya detectado y tiene el *compliance officer* que haya detectado un delito en la empresa, obligación de denunciar a la empresa?; segunda, aunque no exista esa obligación de denunciar los delitos o de autodenunciarse, ¿es conveniente formalizar denuncia ante la Fiscalía e intentar ir de la mano del Ministerio Fiscal en el peregrinaje penal que la denuncia pueda iniciar?

A la primera pregunta mi respuesta sería, sin ninguna duda, negativa.

El art. 259 de la LECrim impone la obligación de denunciar un delito a todo aquel que *presenciare su perpetración*, no a quien detectare su comisión, y, en cualquier caso, la infracción de ese deber se castiga con *"multa de 25 a 250 pesetas"*. Una infracción legal que tiene una respuesta coercitiva tan ridícula es una obligación prácticamente vacía de contenido. Por otra parte, el art. 450, núm. 1, del Código Penal castiga, con la pena de prisión de seis meses a dos años (si el delito fuera contra la vida) y la de multa de seis a veinticuatro meses (en los demás casos, salvo que al delito no impedido le correspondiera igual o menor pena, en cuyo caso se impondrá la pena inferior en grado a la de aquél) a aquel *"que, pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, no impidiere la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual"*. Además, según el núm. 2 de ese mismo precepto, *"en las mismas penas incurrirá quien, pudiendo hacerlo, no acuda a la autoridad o a sus agentes para que impidan un delito de los previstos en el apartado anterior y de cuya próxima o actual comisión tenga noticia"*. Luego la única obligación que, a este respecto, impone el CP, bajo amenaza de una pena, es la de impedir la comisión de un delito contra la vida, la integridad o la salud, la libertad o la libertad sexual, siempre que ello se pueda hacer sin riesgo propio ni de tercero, o acudiendo a la autoridad o sus agentes.

Finalmente, se debe de recordar que el art. 31 bis, núm. 5, del CP establece que para que el programa de prevención sea válido y eficaz, la empresa debe imponer, a sus empleados y dependientes, *"la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención"*, pero es ésta una obligación impuesta para beneficio del funcionamiento y la eficacia del programa, no a los efectos de la denuncia de las infracciones.

Problema completamente diferente, obviamente, es el de qué responsabilidad penal (o civil, en su caso) tiene un *compliance officer* que no ha cumplido con su cometido y ello ha permitido la comisión de un hecho delictivo.

Detectado, por tanto, un delito en la empresa y visto que, en principio, no parece existir una obligación legal de denuncia o autodenuncia, **¿es recomendable, no obstante, que la empresa proceda a esa denuncia o autodenuncia?**

En los últimos tiempos, en los que parece habernos invadido una especie de arrebato o entusiasmo ético, probablemente como reacción a tantísimos casos de corrupción que han trascendido, he podido detectar, como respuesta casi inmediata a esta pregunta, la afirmativa: la empresa debe denunciar los delitos que detecte porque eso acreditará, sin ninguna duda, que tiene una verdadera cultura ética empresarial. Porque, muchos, incluida la Fiscalía General del Estado, a través de su Circular 1/2016, piensan que, *"en puridad, los modelos de organización y gestión o corporate compliance programs no tienen por objeto evitar la sanción penal de la empresa sino promover una verdadera cultura ética empresarial"*. Es más, en dicha Circular, a la hora de plasmar los criterios para valorar la eficacia de los modelos de organización y gestión, se incluye un criterio sexto que dice:

"Si bien la detección de delitos no está expresamente incluida en la enunciación ni en los requisitos de los modelos de organización y gestión, forma parte, junto con la prevención, de su contenido esencial. Teniendo en cuenta que cualquier programa de prevención, por eficaz que sea, soportará un cierto riesgo residual de comisión de delitos, la capacidad de detección de los incumplimientos lucirá como un elemento sustancial de la validez del modelo. En consecuencia, los Sres. Fiscales concederán especial valor al descubrimiento de los delitos por la propia corporación de tal manera que, detectada la conducta delictiva por la persona jurídica y puesta en conocimiento de la autoridad, deberán solicitar la exención de pena de la persona jurídica, al evidenciarse no solo la eficacia del modelo sino su consonancia con una cultura de cumplimiento corporativo".

Por tanto, a la vista de estas manifestaciones, que la FGE hace a través de la Circular 1/2016, parece que no puede haber motivos para no recomendar a la empresa que denuncie los delitos que detecta en su seno o que, incluso, se autodenuncie. Y, sin embargo, sería partidario de enfriar un poco el *soufflé ético* y haría una llamada a la prudencia y a la reflexión a la hora de tomar decisiones de este tipo en las empresas.

En primer lugar, diré que me produce cierto rechazo que se asocie al Derecho penal con la consecución de determinados objetivos de regeneración ética o moral y, por tanto, no creo, en absoluto, que los modelos de organización y gestión o *corporate compliance programs* no tengan por objeto evitar la sanción penal de la empresa; es más, creo que ese es su fundamental objetivo. Otra cosa es que, además, la empresa asuma un compromiso de ética empresarial en la gestión que, sin duda, si lo cumple, le va a servir para evitar delitos.

Pero en ningún sitio del CP se les exige a las empresas que demuestren la asunción de una cultura ética empresarial, para quedar exentas de pena, entre otras cosas porque es casi imposible definir qué significa eso, más allá del estricto cumplimiento de la ley. Por tanto, no puede haber juez en el mundo que obligue a esa demostración imposible; sería tanto como exigirle a un individuo, para que se le pueda apreciar la eximente de legítima defensa, que demuestre que conduce su existencia de acuerdo con unos parámetros de ética ciudadana, parámetros que, en una sociedad compleja y diversa, nadie sabría muy bien cómo definir.

En segundo lugar, **una decisión de denunciar los delitos detectados en su seno, o de autodenunciarse por ellos, puede tener unas consecuencias irreparables para la empresa,** porque, como ya he dicho antes, en la mayoría de los casos la apertura de un proceso penal no se va a poder evitar. Y si eso es así, y si se tiene en cuenta, además, lo fácil que es que trasciendan al público los "problemas penales" de la empresa, el daño reputacional que ello comporta puede acabar con la empresa o perjudicarla muy severamente. Por eso, antes de interponer la denuncia, hay que pensarse muy bien cómo actuar.

Por otra parte, un procedimiento penal es un escenario, las más de las veces, imprevisible, en el que se sabe cuándo se entra, pero nunca cuándo sale, y el transcurrir de éste –al margen del daño reputacional que ya hemos mencionado– puede ser, en sí mismo, un elemento de perturbación muy importante para el normal funcionamiento de la empresa. Por ejemplo, puede alterar seriamente a los trabajadores el ver cómo un compañero es perseguido penalmente por la propia empresa; puede generar una severa retracción en el cumplimiento de sus obligaciones a los directivos el ver cómo a uno de ellos se le somete a una persecución penal; las sesiones del consejo pueden ser severamente conflictivas si unos consejeros descubren cosas que, hasta entonces, no se les trasladaba, etc. Y así, podría relatar experiencias personales infinitas vividas con mis propios clientes.

Así y todo, no estoy recomendando tajantemente no denunciar o no autodenunciarse; **lo que estoy recomendando es reflexionar, previa y pausadamente, sobre los pros y los contras de esa decisión. Y si el procedimiento penal es inevitable, porque se sabe que la denuncia la va a interponer un tercero ajeno a la empresa, o un socio, o un inversor, o un trabajador, entonces, la vía de la colaboración absoluta con la Justicia puede ser una opción.**

En cualquier caso, lo que **sí recomendaría seriamente es que las empresas, ante la menor sospecha, pongan en marcha una investigación interna** porque, en cualquier caso, para decidir hay que contar con la mayor información posible acerca de lo que ha sucedido en su seno.

El triunvirato entre Ética, Ley y Compliance.

Fernando Navarro García
Secretario General del Instituto de Estudios para la Ética y la Responsabilidad Social de las Organizaciones - INNOVAÉTICA
Autor de Responsabilidad Social Corporativa: teoría y práctica (ESIC, 2012)

Hace poco discutía con unos amigos sobre la transformación y *positivación* de la responsabilidad social de las organizaciones (RSO) y durante el debate surgió la eterna disyuntiva entre el deslinde cada vez menos diáfano entre la ética y la ley, muy especialmente tras la **Ley Orgánica 5/2010 que introdujo la Responsabilidad Penal de la Persona Jurídica** a través del artículo 31 Bis del Código Penal y la reciente trasposición de la Directiva europea al **Real Decreto-ley 18/2017 sobre Publicación Información No Financiera.** A medida que avanzábamos en el debate vimos claro que esa diferenciación entre ética y ley - que antes parecía tan clara- muchas veces puede distorsionar la valoración que hagamos de la responsabilidad social de una organización o, como nos recordaba hace poco Francisco Hevía en esta misma revista, de su Conducta Empresarial Responsable (RBC, por el acrónimo inglés de Responsible Business Conduct).

Para justificar la conveniencia de complementar ética, ley e instrumentos de aseguramiento normativo (legal o convencional) necesitaré en primer lugar explicar también sus diferencias. De entrada parece fácil asumir que **es legal todo aquello cuyo cumplimiento resulta obligatorio** y que **es ético todo aquello cuyo desempeño es voluntario.** La ley se acata, guste o no, porque en caso de no hacerse las instancias del Estado fuerzan su cumplimiento.

La ética, por el contrario, se aplica voluntariamente solamente porque se considera que es lo correcto y en ese sentido se trata de una convicción profunda que no se necesita de la coerción de ninguna ley que incite a actuar - o a no hacerlo - de tal modo.

¿Pero qué sucede cuando **la ley me obliga a acreditar que realmente hago lo que he declarado pública y voluntariamente** que quiero hacer (voluntariamente)? Casi parece un trabalenguas y hasta casi un contrasentido pues si hago algo obligado por una ley en realidad ya no sería un acto dentro de la esfera de la ética (que, como hemos visto, siempre es voluntaria) sino simplemente un acto legal (que siempre es obligatorio). Uno no declara públicamente que va a pagar los impuestos o que va a formalizar un contrato de trabajo para sus empleados, pues eso es algo a lo que nos obligan las leyes y se presume que la ley se acata. Lo que sí se puede y debe declarar públicamente es todo aquello que se hace sin existir obligación legal para ello. No se trata sólo de una disposición a la sinceridad, sino de que ésta adquiera **el rango de un compromiso público.** En ese sentido una empresa puede declarar que quiere que el 50% de sus proveedores sean entidades con algún tipo de sistema de gestión ética. La ley no obliga a ello (de momento) pero una organización, en su libertad y autonomía para seleccionar y contratar proveedores puede decidir incorporar ese criterio. Y si publica y difunde tal política de contratación (en su código ético, en sus políticas o manuales de procedimiento, etc) lo razonable será pensar que está dispuesta a responder, a "dar razones", de su aplicación.

> *"La ética es una convicción profunda que no necesita de la coerción de ninguna ley que incite a actuar"*

La ley entonces puede obligar a esa organización a responder de tal aplicación (¿qué ha hecho la organización para llegar a ese 50%? ¿cómo ha procedido?). Una parte sustancial del *compliance* se mueve en esa tierra de nadie en donde convergen ética y ley, en donde hay que acreditar el compromiso público.

Si nos limitáramos a pensar que son responsables aquellas organizaciones que respetan las leyes de un lugar y en momento dado, creo que estaríamos reduciendo enormemente el ámbito y el valor innovador de la RSO. Por supuesto que **lo primero que una organización debe hacer para poder llegar a ser calificada de "responsable" es respetar las leyes a las que está sujeta.** Sin ese condicionante ninguna organización puede pretender ser socialmente responsable, pues ni siquiera sería legal. Una organización que no cumpla con las leyes establecidas no puede ser una organización ética; a lo sumo será - parafraseando a Adela Cortina - una organización "cosmética", que emplea a modo de distracción ciertas buenas prácticas para ocultar su ethós intrínsecamente ilegal. En los años noventa del siglo pasado, la Fundación Etnor -pionera en España del estudio de la ética aplicada a las empresas- afirmaba irónicamente que "la ética lavaba más blanco".

Recordemos que la palabra ética deriva del *ethós* griego y que con ese término Aristóteles aludía al *carácter o modo de ser* de las personas. Y recordemos también que las organizaciones tienen su propio carácter y por esa misma razón las organizaciones tienen una ética o un modo de ser. Antes la denominábamos "filosofía de empresa" y hoy sistematizamos ese carácter (*ethós*) en la misión, visión y valores. El **mito de la empresa amoral** hace tiempo que ha pasado a la historia, aunque todavía continúe siendo defendido por intelectuales de la talla de Compte-Sponville (*El capitalismo ¿es moral?, 2004*).

El **carácter,** a diferencia del temperamento que nos viene genéticamente dado, puede ser construido -puede ser mejorado o perfeccionado- mediante la repetición de buenas prácticas, la proscripción o prevención de las malas y la **implantación de unos hábitos que a largo plazo sean desarrollados de forma instintiva.** Aristóteles tildaba al carácter de "Segunda Naturaleza" porqué podía transformar nuestra primera naturaleza, meramente genética (temperamento).

Pero ¡cuidado! los hábitos pueden ser buenos o malos. En filosofía moral se llaman **virtudes** a los hábitos buenos para alcanzar una meta (y al cabo para ser felices) y **vicios** a los hábitos malos (que nos alejan de la meta). Hay que habituarse a hacer buenas elecciones (tener un buen carácter) para lo cual resulta imprescindible el conocimiento previo de los fines y de los valores de la organización (misión, visión, valores). **Sin saber cuáles son nuestros valores, es imposible elegir bien** ¿Cómo vamos a llegar a la meta si no sabemos hacía dónde ir? Y el consenso internacional desde 1948 es que **la meta de cualquier organización solo puede lograrse dentro del estricto cumplimiento de los Derechos Humanos.**

En resumen, **la ética es un saber teórico y práctico que nos sirve para actuar racionalmente en el conjunto de la vida y que nos sirve para aclarar qué es moral (¿Qué?), fundamentarlo (¿Por qué?) y aplicarlo a los distintos ámbitos de la vida, incluida la práctica profesional (¿Cómo?).**

Es en ese sentido que **la ética ayuda a forjar el (buen) carácter mediante la toma de decisiones prudentes;** esto es, mediante la adopción de decisiones que han sido meditadas y reflexionadas, valorándose el impacto (externalidades) que tendrán en la propia organización y en sus restantes grupos de interés, incluso las generaciones aún no nacidas. Decisiones sobre las que la organización tendrá que responder. El catedrático de ética de la empresa García-Marzá llega a equiparar simbólicamente tal responsabilidad con la existencia de un **contrato moral.** Tal contrato es causa de **la ley de hierro de la responsabilidad** propugnada por Davis (*"Business Ethics: Five Propositions for Social Responsibility",* 1990): "La sociedad concede legitimidad y poder a la empresa. En el largo plazo, aquellos que no usan este poder de un modo que la sociedad considera responsable tienden a perderlo". Dicho en otras palabras, la actividad empresarial crea una serie de expectativas en los stakeholders. Esas expectativas se refieren al proyecto corporativo de la empresa, a la actividad que realiza **y a cómo la realiza.** Si la sociedad, la opinión pública formada a través de estos diferentes grupos de intereses, percibe que la organización responde y cumple *(compliance)* estas expectativas, aporta entonces la necesaria confianza.

Nada nuevo bajo el sol, salvo que tras más de dos milenios de reflexiones morales finalmente las empresas y otras organizaciones que operan e impactan en su entorno han decidido dar el paso de **normalizar la virtud y de tangibilizar** algo aparentemente tan intangible como son los valores (esos activos intangibles que son tan difíciles de piratear o plagiar).

Es ahora cuando las organizaciones están haciendo esfuerzos no solo para publicar o comunicar lo que consideran que es una buena forma de lograr sus objetivos (Kant llamaba a esto "ética de la publicidad") sino también para acreditar a una sociedad cada vez más cívica que realmente hacen lo que dicen. Y ese equilibrio entre lo que **digo** y lo que **hago** ofrece la medida de la **coherencia ética** de una organización y a mayor coherencia mayor **legitimación social** (la invisible "licencia para operar") y cuanta mayor sea esa legitimación más reservas tendrá la organización para competir y más "ahorrará en derecho" (en conflictividad laboral, en absentismo, en reclamaciones, etc). **La confianza es directamente proporcional a la capacidad de las empresas para hacer públicas y justificar discursivamente sus acciones, estrategias y políticas.**

Y es llegados a este punto cuando empieza a entenderse la fuerza creciente del **compliance,** entendido como el sistema de gestión y control establecido para garantizar y justificar el cumplimiento por parte de una organización no solo de las leyes y normativas de carácter legal sino también de todas aquellas que hayan sido adoptadas voluntariamente a modo de compromiso público (códigos éticos, políticas y reglamentos internos, guías y manuales de procedimiento, etc). En España el *compliance* se está implantando muy rápidamente y son ya muchas las organizaciones que lo están sistematizando, no solo empresas o entidades privadas.

Las leyes históricamente han ayudado a esa labor de concreción normativa, pero hasta mediados del siglo pasado se consideró que el ámbito de actuación de las empresas se debía limitar al estricto cumplimiento de las leyes y a veces ni siquiera eso en aras de la rentabilidad. No aludiré a la conocida afirmación de Milton Friedman en 1971 pues ha llovido mucho desde entonces y la ciudadanía de hoy ha ido forjando un carácter distinto a la de antaño, con una conciencia social y ecológica más elaborada y critica.

Por supuesto que el **acatamiento de la ley es el primer paso - pero no el único - para valorar la responsabilidad social de una organización.** Sin embargo, una vez acreditada su sintonía legal (su legalidad) será preciso seguir valorando otras prácticas voluntarias dentro del dominio de la ética (su *eticidad* o su responsabilidad). Y creo que este segundo paso de valoración moral - que no legal- de una organización es necesario porque muy a menudo las leyes son **incompletas** y además su gestación suele ser muy **lenta,** especialmente en los sistemas democráticos en donde el garantismo legislativo y judicial hace que la positivación de las costumbres (de la ética o del modo de ser de una sociedad) requiera un largo periodo de tiempo que algunos grupos de interés no están dispuestos a esperar.

Por lo tanto, **una organización que quiera acreditar su responsabilidad social no puede pretender fundamentarla solamente en el hecho de que cumple con las leyes; si estas no alcanzaran las expectativas legitimas de una parte de la ciudadanía a la que identificamos con sus grupos de interés.**

En esos casos una organización tiene la libertad -condicionante de la responsabilidad- de mejorar la ley en cierto grado. No afirmo con esto que una empresa o una organización no lucrativa tengan capacidad de legislar. Lo que sostengo es que - dentro del amplio marco de libertades que disfrutan - **pueden aplicarse voluntariamente normas de comportamiento interno más amplias que las impuestas por las leyes.**

Un ejemplo: *La Ley General de Derechos de las Personas con Discapacidad,* aprobada mediante el **Real Decreto Legislativo 1/2013**, establece que las empresas, ya sean públicas o privadas y con más de 50 trabajadores, están obligadas a disponer de una **cuota de reserva de discapacitados del 2%** del total de sus trabajadores. En este caso concreto, una empresa que solo reservara el 0,5% de su empleo a discapacitados sería una empresa ilegal; una empresa que reservara el 2% sería legal y una empresa que decidiera incorporar a su reglamento interno o a su código de conducta una reserva del 10% para discapacitados sería claramente una organización socialmente responsable ya que aumentado notablemente la exigencia legal (siempre dentro del ámbito concreto que he empleado como ejemplo; esto es, la inclusión laboral de personas con discapacidad)

Y afirmo que dicho acto voluntario, respetando la ley pero a la vez mejorándola, es un acto de responsabilidad social, pues la organización hace algo que responde a las expectativas legitimas de sus grupos de interés y lo hace anticipándose a las leyes, sin estar obligada a ello. Lo hace porque considera que debe hacerlo, independientemente de que el poder legislativo haya promulgado una ley al respecto o no. Obviamente una organización con buenos mecanismos de dialogo con stakeholders sabrá "adelantarse" a las leyes, ganando con ello, como ya hemos visto, no solo una mayor legitimación social sino también - y creemos que esto es muy importante - una mayor competitividad.

Del mismo modo, una organización que opere en terceros países en donde no se respeten o protejan los derechos humanos no puede ser socialmente responsable si aplica o respeta una ley *claramente inmoral* (por ejemplo, flagelación a trabajadores como castigo que aún es amparada por la legislación laboral de algunos países). Se trataría de dos situaciones muy concretas en donde quedaría patente **la superioridad de la RSO sobre la ley.**

La ley lo permite, pero la ética lo prohíbe y recordemos que algunos derechos son renunciables (por ejemplo, una empresa puede decidir libremente renunciar al derecho de discriminar por razón de sexo o credo en un país en donde la legislación permitiría hacerlo).

La RSO, por lo tanto, debe ser motor de cambio, de progreso y de mejora y debería servir de incentivo al legislativo y al ejecutivo (al menos en estados democráticos) para "ponerse las pilas" y mejorar sus leyes para situarlas a la "altura moral" de sus ciudadanos (que en democracia también son votantes). Por eso es tan importante fomentar desde todas las instancias - también desde las empresas- una ética cívica –como lleva décadas insistiendo Adela Cortina-, encarnada en una ciudadanía mayor de edad que sepa premiar o castigar a aquellos gobernantes que adecuen o no sus leyes y practicas a sus legitimas expectativas. Naturalmente, **para que la idea funcione es necesaria una sociedad civil vital y responsable, que no quede des-moralizada por la saturación mediática de malas prácticas y que** –parafraseando a Fromm- **viva sin miedo a la libertad.**

Pero no olvidemos que el **compliance,** al igual que sucede con la ética y con la ley, no es estático e inmutable. **La Moral Crítica Universal puede cuestionar las normas y principios vigentes**. El ámbito de la moral crítica es más amplio que el de las Leyes o el Derecho positivo y, al menos en los estados democráticos, suele inspirar sus cuerpos legales nucleares o constituyentes. Nadie concebiría hoy en Europa una Ley que consagrara expresamente ciertas discriminaciones raciales o religiosas; entre otras cosas porque no contaría con el apoyo de la gran mayoría del electorado. De ahí la importancia de las nuevas tendencias de RSO que, al cabo, no dejan de inspirar nuevas medidas legales tendentes a una adaptación de las Leyes a la "conciencia moral" de su sociedad. De ahí que el impulso político de la RSO no deja de ser también una retroalimentación para el saneamiento y mejora del gobierno y de la administración pública, aunque esto - como escribiría Kipling- ya es otra historia.

Resumiendo, creo que la **complementariedad entre Derecho y Ética** y su nexo de unión que es el **compliance** se fundamenta en las siguientes razones:

1. Las leyes no siempre protegen todos los derechos que son reconocidos por una moral cívica o crítica

2. Generalmente las "costumbres" evolucionan más rápidamente que el Derecho y a menudo lo inspiran a través de una ética dialógica (al menos en las sociedades abiertas y democráticas). Las reformas legales son lentas y una sociedad no siempre puede esperar a que una forma de actuación esté recogida por una ley para considerarla correcta. Por esa razón la ética muchas veces se anticipa y se superpone al derecho.

3. Las leyes no contemplan todos los casos particulares que, sin embargo, requieren una orientación; actuando en estos casos la ética como una "brújula" que indica el norte (Kant)

4. Positivar o juridificar todas las facetas de la vida no solo es lento sino también caro y, en ocasiones, un rasgo característico de los estados totalitarios o autoritarios como nos recordó Orwell con ese Gran Hermano que todo veía y regulaba en 1984.

> ***"La responsabilidad social de las organizaciones, debe ser motor de cambio, de progreso y de mejora"***

La correcta gestión de las contraseñas como elemento esencial de **seguridad de la información**

Francisco Menéndez Piñera
CEO en SIGEA.
Consultor en Seguridad, Privacidad y Gobierno TI

> ***Hay dos posibles puntos de fuga de información que pueden comprometer la seguridad: NOSOTROS y el SISTEMA DE INFORMACIÓN***

Los responsables de seguridad de las organizaciones mantienen, desde el origen de los tiempos informáticos, una lucha constante con los usuarios (y, en ocasiones, también con los administradores de sistemas) a propósito del correcto uso de las contraseñas. En este artículo voy a intentar explicar cómo funciona el proceso de autenticación y el porqué de la importancia de la correcta gestión de las contraseñas.

Nos pasamos el día accediendo a diferentes sistemas informáticos, ya sea para temas profesionales o privados. Para que el sistema nos deje acceder debe tener la seguridad de que quien llama a la puerta es quien dice ser. Para ello existe el subsistema de autenticación, que utiliza uno o varios de los siguientes elementos para comprobar que realmente somos quienes decimos ser:

Algo que sabemos
(por ejemplo, una contraseña)
Algo que tenemos
(por ejemplo, una llave)
Algo que somos
(por ejemplo, nuestra huella dactilar)

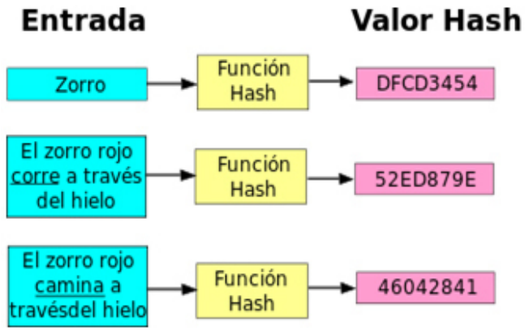
En la gran mayoría de los casos el sistema utilizado, por ser el más sencillo de gestionar, es el de autenticación por usuario y contraseña. El sistema nos pregunta primero nuestro usuario (¿quién eres?), y a continuación nos pedirá la contraseña de ese usuario.

Una vez que introducimos esta información, el sistema la compara con la que tiene almacenada en el subsistema de control de accesos, y decide si podemos o no acceder, y los permisos que tendremos en el sistema. La información que el sistema tiene almacenada es la que nosotros hemos introducido en el proceso de registro, o la que el administrador de sistemas ha generado al crear nuestra cuenta. En este último caso, lo primero que debemos hacer es cambiar la contraseña que nos han generado, para asegurarnos que solo la sabemos nosotros y el sistema, pero no los administradores de ese sistema, ya que las contraseñas se almacenan cifradas (o así debería ser).

De lo anterior, se deduce que hay dos entes que conocen nuestro usuario y contraseña, nosotros y el sistema de información. Por lo tanto, hay dos posibles puntos de fuga de información que pueden comprometer la seguridad.

Vamos a analizar primero cómo se intenta reforzar la seguridad por parte de los sistemas de información:

Como mencionaba anteriormente, las contraseñas se almacenan cifradas en bases de datos que gestiona el subsistema de control de accesos de los sistemas de información. Para ello, se suelen utilizar funciones HASH, funciones matemáticas que cifran la cadena de entrada en una cadena de salida de longitud fija y en formato hexadecimal. Este cifrado no es reversible; es decir, no es posible obtener la cadena de entrada a partir de la cadena de salida utilizando una función inversa. Cuando el usuario mete la contraseña durante el proceso de registro, se calcula su hash y es éste el que se almacena. Posteriormente, cuando un usuario quiere acceder, se calcula el hash de la contraseña introducida en ese momento y se compara con el hash almacenado. De esta forma, en el caso de que alguien consiga acceder a la base de datos de usuarios y contraseñas del sistema de información, lo que obtendrá será un conjunto de usuarios y los correspondientes valores hash de las contraseñas, que si son introducidos en el proceso de autenticación darán un error.



Parecería que, con este tipo de medidas, nuestras contraseñas están totalmente seguras por la parte de los sistemas de información. Pero no es así, en absoluto. Si "los malos" se hacen con una base de datos de contraseñas, tienen dos posibles maneras de atacarla:

Por diccionario: En un archivo se introducen miles de palabras y se calcula su hash. Posteriormente se busca ese hash entre los de la base de datos atacada y si se localiza ya tenemos la contraseña. Esta es la razón por la que se aconseja no utilizar palabras reales, que existan en el diccionario, como contraseña.

Por fuerza bruta: Se prueban todas las combinaciones posibles de caracteres alfanuméricos, calculando su hash y buscando éste en la base de datos atacada. Por este motivo, se aconseja el uso de contraseñas de una longitud mínima y complejas (que combinen números, letras minúsculas y mayúsculas, y caracteres especiales).

Veamos como influyen longitud y complejidad en dificultar ambos ataques, especialmente el de fuerza bruta:

El número de combinaciones posibles depende de dos factores: el número de caracteres utilizados (n) y el juego de caracteres posibles (c). La fórmula para saber el número total de combinaciones (T) es:

$$T = c^n$$

Si utilizamos contraseñas de cuatro caracteres y con un juego de caracteres solo numérico (como es el caso de los PIN de los teléfonos móviles), tendremos T=10^4 = 10.000 combinaciones posibles, del 0000 al 9999. Con la potencia actual de los ordenadores se tardaría unos pocos segundos en saber una contraseña de estas características por fuerza bruta.

Si en vez de utilizar solo caracteres numéricos, añadimos letras mayúsculas y minúsculas tendremos un juego de caracteres de 64 elementos (10 números, 27 mayúsculas y 27 minúsculas), con lo que ahora tendríamos T=64^4 = 16.777.216 combinaciones posibles. En este caso la fuerza bruta conseguiría su objetivo en aproximadamente un minuto.

Si a eso le añadimos los alrededor de 40 caracteres especiales que existen (@#$%_-*+[] ...), obtendremos T=104^4 = 116.985.856 combinaciones posibles, utilizando tan solo cuatro caracteres. En este caso la fuerza bruta conseguiría su objetivo en aproximadamente tres minutos.

Sin embargo, aumentando la longitud de la contraseña a 8 caracteres, y utilizando todo el juego de caracteres, obtendríamos T=104^8 = 13.685.690.504.052.700 combinaciones posibles, y un ataque por fuerza bruta necesitaría alrededor de 464 años para tener éxito.

Una vez conocido lo anterior, veamos qu**é podemos poner de nuestra parte** los usuarios para aumentar la seguridad de nuestra información.

Lo primero, las contraseñas son secretas. Ya sé que es obvio, pero no lo parece viendo los usos y costumbres de los usuarios. Nuestras **contraseñas solo las debemos saber nosotros** y no se dan a nadie, ni al administrador de sistemas ni al dueño de la empresa para la que trabajamos. Un caso habitual es que nos pidan la contraseña del correo del trabajo para que se pueda acceder a él mientras estamos de vacaciones. Nadie tiene que saber la contraseña de nuestro correo profesional, hay varias formas de solucionar ese problema; como, por ejemplo, la redirección de correos.

Debemos utilizar **contraseñas robustas,** con una longitud mínima de ocho caracteres y utilizando el mayor juego de caracteres posible (en algunos sistemas no admiten caracteres especiales, y en otros solo caracteres numéricos).

Las contraseñas que usemos **no deben ser palabras de uso común** que se pueden encontrar el diccionario español, inglés, etc.

Una buena opción es **utilizar frases** que, aunque utilizan palabras de uso común, son muy robustas por la longitud. Además, podemos realizar algunas sustituciones de caracteres. Las obvias (5 = S; 0 = O; 3 = E) son sencillas y conocidas, pero también ayudan a aumentar la complejidad. Por ejemplo, una contraseña que sea "Mi perro se llama Oscar" se transformaría en "Mi p3rr0 53 llama 05car"

Nuestras contraseñas deben ser **impersonales.** Es decir, nada que tenga que ver con nuestros datos personales: fecha de cumpleaños, nombre del perro (ya sé que lo he utilizado en el ejemplo anterior), números de teléfono, DNI, etc.

Debemos utilizar **contraseñas diferentes** para cada caso. Si utilizamos la misma contraseña para todas las redes sociales, y alguien descubre nuestro usuario y contraseña para una de ellas, lo primero que va a hacer es probar en el resto de redes sociales con el mismo usuario y contraseña. Una contraseña que tiene que

> ***"Nuestras contraseñas deben ser impersonales y diferentes para cada caso"***

ser espacialmente robusta (larga y compleja) es la de la cuenta de correo que utilizamos como cuenta principal, que es donde recibimos las confirmaciones de nuestros registros en los diferentes servicios, donde nos avisan si ha habido algún incidente con nuestras cuentas en las redes sociales, y que, habitualmente es el mismo correo que utilizamos como usuario en multitud de sitios. Esa cuenta de correo principal tiene que tener una contraseña robusta y diferente a las utilizadas en cualquier otro sitio.

Es especialmente importante no utilizar las mismas contraseñas **para temas personales y para temas profesionales.**

Mucho cuidado en **sitios públicos**, especialmente en las cafeterías. Una de las formas más habituales de robo de contraseñas sigue siendo la que se conoce como "shoulder surfing" (mirar por encima del hombro). Sobre todo con los móviles, cuyo PIN solo es de 4 dígitos; primero intentan averiguar el PIN observándote cuando lo introduces y, solo entonces, hacen todo lo posible por robártelo.

Las contraseñas **se deben cambiar** con una frecuencia que dependerá de su importancia. Las más importantes se deben cambiar con mayor frecuencia. Las de temas profesionales y la de nuestra cuenta principal de correo deberían cambiarse, al menos, cada seis meses; o inmediatamente cuando tengamos la sospecha de que alguien la pueda conocer.

Donde sea posible, y especialmente para las contraseñas más importantes, conviene utilizar el **doble factor de autentificación**. Al principio del artículo vimos que hay tres tipos de elementos para autentificarnos. Hasta ahora solo hemos hablado de "algo que sabemos", la contraseña.

En muchos sitios ya podemos añadir un segundo factor de autentificación que el servicio nos solicitará además de la contraseña. Este segundo factor ("algo que tenemos") puede ser un código que nos envíen al móvil, nuestro DNI electrónico, etc.

A estas alturas os estaréis preguntando cómo gestionar vuestras contraseñas con todos estos requisitos y con la cantidad de ellas que utilizamos a diario. Por supuesto, las contraseñas **no deben estar anotadas** en ninguna libreta, ni en esas famosas etiquetas amarillas que parecen diseñadas para ello. Lo adecuado es utilizar un **gestor de contraseñas** (existen varios gratuitos y de pago). Se trata de una aplicación que nos permite almacenar nuestras contraseñas de forma cifrada, y gestionarlas cómodamente. Eso sí, la contraseña utilizada para acceder a nuestro gestor tiene que ser especialmente robusta y, a la vez, fácil de recordar.

Como auditor de seguridad de sistemas de información, me encuentro habitualmente con muchos errores en la gestión de las contraseñas, tanto por parte de los usuarios como por parte de las organizaciones. Espero haber ayudado, con este artículo, a aclarar algunos conceptos y a la concienciación de la importancia de una correcta gestión de las contraseñas.

Del canal de denuncias como instrumento imprescindible de un programa eficaz de prevención de delitos y de la obligación de denunciar en las sociedades de capital

Luis Suárez Mariño
Abogado
Socio de Defensa y Compliance s.l.p.

De lo dispuesto en el artículo 31 Bis apartado 5, punto 4º del Código Penal, se infiere que una condición imprescindible para que el programa o modelo de prevención de delitos implantado en una sociedad de capital actúe, en su caso, como causa de exoneración de la responsabilidad penal de ésta, es que *"el mismo imponga la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención."*

1. ¿A quién se dirige la obligación de "informar"?

(El C.P. habla eufemísticamente de "informar" para referirse tanto a riesgos como a infracciones cuando en realidad para éste último caso podría haber sido más apropiado hablar de "denunciar").

Si atendemos a los términos utilizados por el propio art. 31 bis parece que dicha obligación se dirige:

a) **A los empleados: "Todos aquéllos que actuando en el ejercicio de actividades sociales por cuenta y en beneficio directo o indirecto de la sociedad estén sometidos a quien en la sociedad tiene autoridad". (cfr. art. 31bis. 1. b)**

El término "sometidos" que emplea el artículo 31 bis b, excluye –por tanto- del ámbito de los "obligados" a terceros ajenos a la sociedad, es decir contratados mercantiles, al carecer la sociedad sobre los mismos de poder de dirección, organización y control.

Cosa distinta es -como luego analizaremos- que el canal del que se dote la sociedad para facilitar la información de riesgos e infracciones (canal de denuncias en términos al uso) no se pueda y sea conveniente poner a disposición de dichos terceros (stackeholders), con el fin de que éstos puedan dar a conocer al órgano de cumplimiento de la propia sociedad, los riesgos o infracciones, por ellos observados en el proceso de contratación o ejecución del contrato, y que yendo más allá –incluso-, entre las propias condiciones contractuales que les vinculen a esos terceros con la sociedad, se les imponga la obligación de informar de los riesgos e infracciones observados por ellos en la contratación o ejecución del contrato, pactándose que el incumplimiento de dicha obligación pueda conllevar alguna penalización o incluso en los casos más graves la propia resolución del contrato.

b) **Desde luego, la obligación de "informar de riesgos o infracciones al órgano de cumplimiento" incluye entre todos los empleados, particularmente a aquéllos ligados por un contrato de alta dirección, a los que el propio código trata de manera particular en el art. 31 bis 1a) - estableciendo un régimen específico de responsabilidad - junto a los representantes legales de la sociedad y quienes integren el órgano de administración de la sociedad.**

Por lo que se refiere a la alta dirección, cuando se trate de riesgos o infracciones que afecten al propio departamento que se encuentre bajo su dirección, organización y control, serán esos mismos directores quienes deberan adoptar las medidas precisas para minimizar o evitar el riesgo o la infracción si ya se hubieran detectado (incluida la puesta en marcha del reglamento disciplinario frente al infractor), sin perjuicio de que los riesgos e infracciones por ellos detectados deban de ponerse en conocimiento del órgano de cumplimiento para que inicie el procedimiento de investigación necesario para determinar la autoría de la infracción (si éste no fuera conocido) y/o del órgano de administración para que apruebe la adopción de las medidas que se considerasen pertinentes precisamente para evitar o minimizar el riesgo o infracción detectados, incluidos los recursos necesarios para su implementación.

Lógicamente la política de compliance de la sociedad deberá de imponer a todos los miembros de la organización, incluidos -como es lógico- los miembros de la alta dirección-, el deber de informar al órgano encargado de vigilar el funcionamiento y observancia del modelo de prevención de aquellos riesgos o infracciones que lleguen a su conocimiento y afecten a otros departamentos distintos de aquéllos que dependan directamente de su poder de dirección, organización y control.

c) **Si el riesgo o la infracción fuera conocida por el propio órgano de cumplimiento** parece evidente que no resulta plausible que se le imponga la obligación de " informarse a si mismo" sino que directamente deberá, en cumplimiento de sus funciones, **instar la adopción inmediata de medidas previstas para minimizar o evitar el riesgo o la infracción detectada; iniciar los procedimientos de investigación regulados para determinar el autor de las mismas, instar el inicio del procedimiento reglamentario sancionador, y comunicar a la alta dirección y al órgano de administración la necesidad de implementar y aprobar las nuevas medidas que considerase pertinentes.**

d) **Si el riesgo o la infracción fueran cometidos en el ejercicio de la actividad social y fueran directamente conocidos por el órgano de administración, en el ejercicio de sus funciones específicas (el art. 225.2 de la LSC expresamente les impone la adopción de las medidas precisas para el control de la sociedad)**; en ese caso el órgano de administración deberá poner los riesgos o infracciones por ellos conocidos en conocimiento del órgano de control, analizar si el "riesgo o infracción" debía o podía haber sido conocido por éste -en el desempeño de su específica función-, o por los directores del departamento donde se produzca, y adoptar en su caso las medidas disciplinarias oportunas frente a ellos como frente a las personas implicadas directamente en las infracciones, o riesgos detectados, dando las oportunas órdenes para el cumplimiento inmediato de las medidas precisas ya aprobadas o adoptar las que se consideren pertinentes.

e) **Para el caso de que los propios miembros del órgano de administración pudieran conocer "riesgos o infracciones" de que fuera directamente responsable otro administrador** (falta de diligencia o dedicación adecuada al cargo, o infracciones de otra índole, incluso delitos) habría que analizar si el administrador conocedor de las posibles infracciones cometidas por otros miembros del órgano de administración y el administrador-infractor, son o no socios; la participación, en su caso, del administrador conocedor de la infracción así como la del infractor, en el capital social, para analizar cual debería de ser la conducta más adecuada y prudente: Si instar ante la Junta de socios el cese del administrador infractor, denunciarle a las autoridades o adoptar otro tipo de acciones, analizando la gravedad de los hechos y las repercusiones para la marcha de la sociedad y su imagen corporativa.

2. ¿Cuáles son las consecuencias de no informar o no denunciar un posible riesgo o infracción, para los empleados y para quienes ejercen el poder de dirección en virtud de un contrato laboral?

Partiendo de que el Código Ético y Reglamento Interno de Conducta de la empresa es parte esencial del modelo de prevención **(art. 31 bis 5 2º)**, al igual que el reglamento sancionador **(art. 31 bis 5 5º)**; el deber de informar o denunciar debe de ser conocido y aceptado como parte de las obligaciones y deberes contractuales por los empleados, -máxime por aquéllos ligados por un contrato de alta dirección- debiendo establecerse en el Código Ético -que forma parte de la Política de Compliance de la sociedad - la obligación de informar sobre riesgos o infracciones (obligación dimanante del deber de buena fe contractual) y en el Reglamento sancionador prever que el incumplimiento del "deber de informar" constituirá una infracción de del deber de buena fe –piedra de bóveda- de la relación laboral **(art. 5 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores)**, pudiendo llegar dicha infracción en caso de ser grave a ser causa de despido disciplinario **(art. 54.2 d)**

Como ha dicho en innumerables sentencias el Tribunal Supremo (por todas la **Sentencia de 19 Jul. 2010, Rec. 2643/2009)** *"la buena fe en su sentido objetivo constituye un modelo de tipicidad de conducta exigible, o mejor aún, un principio general de derecho que impone un comportamiento arreglado a valoraciones éticas, que condiciona y limita por ello el ejercicio de los derechos subjetivos (artículos 7 y 1258 del Código Civil), con lo que el principio se convierte en un criterio de valoración de conductas, al que ha de ajustarse el cumplimiento de las obligaciones, y que se traduce en directivas equivalentes a lealtad, honorabilidad, probidad y confianza; y es cierto también que en el Derecho Laboral hay mandatos legales que imponen un cumplimiento contractual de acuerdo con la buena fe -arts. 5-b) y 20-2 del Estatuto -, que obliga, al decir de la sentencia de esta Sala de 18 de diciembre de 1984 , que a su vez invoca una reiterada doctrina-, «a empresarios y trabajadores en el sentido de un comportamiento mutuo ajustado a las exigencias de la buena fe, como afirma también la sentencia del Tribunal Constitucional de 15 de diciembre de 1983, que matiza el cumplimiento de las respectivas obligaciones y cuya vulneración convierte en ilícito o abusivo el ejercicio de los derechos», hasta el punto de que la transgresión de la buena fe contractual constituye un incumplimiento que, cuando sea grave y culpable, es causa que justifica el despido -art. 54-2.d) del Estatuto -; -- que esta falta se entiende cometida aunque no se acredite la existencia de un lucro personal, ni haber causado daños a la empresa y con independencia de la mayor o menor cuantía de lo defraudado, pues basta para ello el quebrantamiento de los deberes de fidelidad y lealtad implícitos en toda relación laboral, deberes que han de ser más rigurosamente observados por quienes desempeñan puestos de confianza y jefatura en la empresa STS/Social 26-enero-1987 -infracción de ley)".*

Y en esa misma sentencia se incide en que *"la buena fe es consustancial al contrato de trabajo, en cuanto por su naturaleza sinalagmática genera derechos y deberes recíprocos"; siendo " el deber de mutua fidelidad entre empresario y trabajador una exigencia de comportamiento ético jurídicamente protegido y exigible en el ámbito contractual"; implicando siempre "la deslealtad una conducta totalmente contraria a la que habitualmente ha de observar el trabajador respecto de la empresa, como consecuencia del postulado de la fidelidad".*

3. ¿Qué personas pueden ser objeto de denuncia?

Parece claro que pueden ser objeto de denuncia cualquier persona "sometida" al poder de dirección y organización de la empresa (empleados); también los contratistas ligados por un contrato que así lo prevea; los propios directores o personas que tengan poder de organización, y control, e incluso los propios administradores o representantes legales de la sociedad, en el caso de que la supervisión del funcionamiento y del cumplimiento del modelo de prevención hubiera sido confiado a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica **(art. 31 bis 2 2ª).**

¿Puede ser denunciado el propio órgano de cumplimiento?; ¿a quién se dirigirán las informaciones de riesgos e infracciones del propio órgano de supervisión o control? Parece evidente que el órgano de supervisión y control puede y debe ser denunciado de cualquier riesgo o infracción existente en el ejercicio de sus funciones, siendo lógico que en ese caso la información o la denuncia se traslade directamente al órgano de administración de la empresa, del que funcionalmente depende.

¿Qué ocurre cuando el órgano de supervisión y control sea el propio órgano de administración conforme a la posibilidad que prevé el art. 31 bis 3.? El tema plantea más preguntas que respuestas. ¿Se podría comunicar al presidente del Consejo en caso de que la información afectase directamente a otro consejero?; ¿en caso de un consejo de administración con un secretario no consejero, se podría comunicar a éste?; ¿en el caso de una sociedad que hubiera nombrado auditor, podría ser éste la persona adecuada a quien trasladar la información comprometedora?; ¿qué ocurre en caso de pequeñas sociedades con un administrador único o varios solidarios que ostentan la condición de socios con igual participación en la sociedad?, y ¿en el caso de administradores mancomunados todos ellos afectados?

4. De las ventajas de establecer un canal de denuncias externo.

Todas estas respuestas tienen solución si el canal de denuncias se externaliza y su gestión se encomienda a una empresa externa, que tramite el contenido de las denuncias, garantice la indemnidad del denunciante para que no sufra represalia alguna por la denuncia, y le asesore en todo el proceso velando por que se preserven sus derechos durante la investigación a que pueda dar lugar la denuncia.

En un canal de denuncias externo, el denunciante puede ser cualquier persona vinculada a la sociedad, no solo accionistas, miembros del órgano de administración y dirección, empleados, colaboradores externos, proveedores, clientes o cualquier otra persona relacionada con la sociedad.

El canal de denuncias externo tiene pues como ventaja frente a un canal interno, que los posibles denunciantes sienten más seguridad de que se preserve su identidad, puedan ser asesorados y se sientan protegidos de cualquier represalia.

Para que esa externalización sea exitosa resulta necesario que todos los posibles denunciantes se hagan cargo del verdadero compromiso de la empresa con el modelo implantado al dejar en manos de tercero cuestión tan sensible como posibles riesgos o infracciones que puedan ser trascendentales desde el punto de vista legal y competitivo. Ello exige, como paso previo, que el órgano de administración y los directores de departamento sepan explicar adecuadamente ese compromiso empresarial como una decisión estratégica encaminada a establecer una verdadera cultura de cumplimiento en la empresa y un sistema de control adecuado.

La evidente ventaja del canal de denuncias externo es pues que su gestor se compromete a garantizar, utilizando las medidas de seguridad oportunas la confidencialidad del denunciante y del tratamiento de la denuncia; el asesoramiento jurídico al denunciante, así como la defensa y protección del mismo ante cualquier tipo de represalia, amenaza, acoso que sufra el denunciante por parte de un miembro, empleado, directivo o persona representante de la sociedad a consecuencia de una denuncia, conducta que en todo caso deberá de preverse en el reglamento sancionador de la entidad como una falta muy grave del reglamento de régimen interior.

La externalización del canal de denuncias:

a) **Facilita, que el denunciante aporte sus datos de identidad y se eviten denuncias anónimas; donde siempre es más fácil utilizar el medio con la simple base de un rumor, sino con fines directamente maledicentes.**

Ciertamente bajo la vigencia de la Directiva 95/46/CE, el Grupo Europeo del artículo 29 de Protección de Datos compuesto por un representante de la autoridad de protección de datos de cada Estado miembro de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea -creado al amparo de la misma- consideraba que los sistemas de denuncia de irregularidades

debían establecerse de tal manera que no fomentasen las denuncias anónimas como forma habitual de presentar una denuncia, pero aceptaba la denuncia anónima cuando el denunciante desease mantener el anonimato.

En el concreto caso español la Agencia española de Protección de datos en su Informe Jurídico 128/2007 (actualmente no disponible en su web) indicaba: que "a fin de garantizar el derecho de acceso deberá exigirse que el sistema únicamente acepte la inclusión de denuncias en que aparezca identificado el denunciante, sin perjuicio de las salvaguardas que se han señalado para garantizar la confidencialidad de sus datos de carácter personal, no bastando el establecimiento de un primer filtro de confidencialidad y una posible alegación última del anonimato para el funcionamiento del sistema".

Este criterio lo modifica el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal en cuyo artículo 24 considera lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.

En el mismo sentido la UNE 19601 - Sistemas de gestión de compliance penal. Requisitos con orientación para su uso-, desarrollada por AENOR como certificable a partir de los criterios de la ISO 19600 y el art. 31 bis. C.P.

Ello no significa, según entiendo, que la empresa no pueda decantarse por el sistema de denuncias confidenciales que proponemos, sin perjuicio de que si llega alguna denuncia anónima, el responsable externo del canal de traslado al Comité de cumplimiento de la relación circunstanciada de los hechos denunciados a efectos de que éste valore la conveniencia o no de iniciar una investigación interna.

b) **Hace más fácil que puedan ser denunciados miembros del órgano de administración, dirección y control (incluido el órgano de cumplimiento)** además de las personas que se encuentren bajo la dependencia de éstos, o los contratistas adheridos al sistema.

c) A mayor abundamiento **permite ser un medio de filtración de las denuncias,** si el responsable del canal asume el compromiso contractual de estudiar si los hechos revisten o no -prima facie- características de delito o infracción del Código Ético o del Reglamento de Régimen interior, o si los mismos no suponen infracción alguna, asumiendo la obligación de informar al denunciante, si da trámite a la denuncia previo asesoramiento o cual sea el canal adecuado para transmitir su queja en caso de que los hechos no sean constitutivos de infracción alguna.

En todo caso el responsable del canal deberá comunicar al órgano de cumplimiento de la empresa - preservando la identidad del denunciante- los hechos objeto de denuncia y el informe que haya elaborado considerando que los hechos denunciados no suponen un delito o infracción alguna del Código Ético o del Reglamento de régimen interior o de los controles establecidos en el programa de prevención de delitos.

d) Esos informes realizados por un tercero pueden ser **un medio idóneo de prueba en un proceso penal;** y si el sistema informático del responsable –lo que sería deseable- tiene las oportunas medidas implementadas, dar fehaciencia de la **fecha de interposición de la denuncia, del resultado de la misma, dejando trazabilidad de todo el proceso.**

e) Además, en caso de que, a juicio del responsable del canal de denuncias, los hechos denunciados revistan, prima facie, carácter de delito o infracción del Código Ético o del Reglamento de régimen interior, el responsable del canal podría igualmente asumir la función de **asesorar al denunciante** en el modo de plantear la denuncia, pruebas que debe incorporar o diligencias de investigación que debe proponer, a fin de que el denunciante una vez cumplimentado este trámite, ratifique la denuncia, de la cual se dará traslado, con el informe del responsable del canal, al órgano de cumplimiento de la empresa preservando la identidad del denunciante.

Esta decisión de externalizar el canal de denuncias y designar un responsable externo (persona física o jurídica) compete al órgano de Gobierno de la sociedad, que no olvidemos tienen dentro del deber general de diligencia, un específico deber de control (cfr.art.225.2 LSC).

5. De la denuncia y sus requisitos.

Será aconsejable que la denuncia se haga por escrito en el que conste:

- Los datos de identidad del denunciante: Nombre, apellidos, Documento Nacional de Identidad y una dirección de correo electrónico a efectos de la recepción de notificaciones.

El denunciante deberá identificarse al formular la denuncia.

- Los datos de identidad si son conocidos del denunciado.

- La relación circunstanciada de los hechos objeto de la denuncia, con indicación de la fecha, hora y lugar en que ocurrieron.

- También se indicarán si existieran testigos de los hechos y los datos de identidad de los mismos si son conocidos por el denunciante.

A la denuncia se debe facilitar que se acompañe cualquier documento, grabación de video, sonora o cualquiera otra prueba de los hechos, en soporte físico o telemático.

6. De la protección del denunciante.

Los datos del denunciante solo serán accesibles al responsable del canal de denuncias, quedando obligado éste al cumplimiento del principio de confidencialidad.

A tal efecto el responsable del canal de denuncia deberá eliminar todos aquellos datos que pudieran identificar al denunciante, manteniendo el resto de datos del documento de denuncia que será remitido al órgano de cumplimiento para la investigación de los hechos.

Igualmente el responsable del Canal de denuncias velará porque el denunciante, caso de ser descubierto en el transcurso de la investigación, no reciba ninguna represalia.

Si el denunciante fuera objeto de cualquier represalia o acoso, podrá dirigirse en amparo al responsable del canal de denuncias, que instará las medidas de protección oportunas, ante la alta dirección de la empresa, su órgano de administración y, si fuera preciso, ante la inspección de trabajo.

7. Derechos del denunciado.

El denunciado tiene derecho a conocer la denuncia.

El denunciado tiene derecho a conocer, en su caso, el resultado de la investigación realizada.

El denunciado tiene derecho a defenderse y proponer los medios de prueba que considere pertinentes para su defensa.

8. Protección de datos personales del denunciante, denunciado y de los terceros afectados.

El artículo 24 del Proyecto de Ley Orgánica de Protección de Datos prevé (art. 24.2 y 3) a este respecto que el responsable del canal deberá de garantizar que el acceso a los datos contenidos en el sistema de denuncias quede limitado exclusivamente a quienes, incardinados o no en el seno de la sociedad, desarrollen las funciones de control interno y de cumplimiento; adoptando las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

Los datos de quien formule la denuncia y de los empleados y terceros afectados por la información deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

Expresamente el Proyecto de Ley Orgánica de Protección de datos prevé en el art. 24.4 que "En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias", y que "Si fuera necesaria su conservación para continuar la investigación, podrán seguir siendo tratados en un entorno distinto por el órgano de la entidad al que competa dicha investigación. No siendo de aplicación a estos sistemas la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica".

> ***"El denunciado tiene derecho a defenderse y proponer los medios de prueba que considere pertinentes para su defensa."***

RSC CONECTADOS SIN BARRERAS

Metodología fomentando Inserción Laboral en mayores de 45 años y mejorando calidad de vida en nuestros mayores.

Óscar Bustos
Fundador Conectados Sin Barreras

> ***"Conectados sin barreras tiene como fin principal acercar la tecnología a las personas que actualmente no pueden beneficiarse de ella. "***

CONECTADOS SIN BARRERAS

INTRODUCCIÓN

El objetivo de crear Conectados sin barreras no fue sólo el de paliar las horas de soledad de nuestros mayores, sino también el de resaltar la figura de todos los abuelos y abuelas del mundo, y el de ayudar al prójimo, luchando constantemente por la igualdad de todos, y de los que más lo necesitan, como las personas con discapacidad, sin discriminación alguna.

Conectados sin barreras tiene como fin principal acercar la tecnología a las personas que actualmente no pueden beneficiarse de ella.

Nuestra misión es reducir paulatinamente la barrera tecnológica hasta derribarla por completo, integrando a todas las personas, independientemente de sus capacidades, en la era digital.

Es una manera de estar conectados y comunicados con nuestros mayores, y de paliar las barreras que les pone la vida a algunas personas con discapacidad, dados los altos grados de avance de la tecnología y el ritmo que la vida moderna nos hace llevar, que nos impide estar cerca de nuestros mayores y allegados tanto como quisiéramos.

A todo aquél que lea estas líneas, le animo a ser voluntario para formar parte de esta aventura, que no sólo trata de acompañar a nuestros mayores, sino de recuperar el valor y la dignidad que estos maestros de vida merecen.

NUESTRA VISIÓN

Queremos mejorar la vida de las personas mayores y ser referencia en servicios profesionales de Responsabilidad Social Empresarial aportando conocimiento e innovación en el mercado de habla hispana.

NUESTRA MISIÓN

Queremos ayudar a las organizaciones en su gestión sostenible, aportando servicios y soluciones que crean valor y beneficio económico, social y medioambiental, a través de la innovación y el conocimiento, tomando como base el compromiso con los grupos de interés.

¿POR QUÉ?

En el mundo empresarial se está despertando la conciencia del SER MAS Y MEJOR: Responsables, justos, transparentes, solidarios, participativos.

OBJETO DE NUESTRA ACTUACION:

Centramos nuestra actividad en los siguientes frentes:

1. **El programa de responsabilidad social empresarial (Programa la buena vida).**

Tiene por objeto tanto a micropymes, como a pymes y grandes empresas.

Su implantación tiene un coste relativamente bajo, y su objetivo con una efectividad cercana al 100% es mejorar la inserción laboral de mayores de 45 años y disminuir la brecha digital en la sociedad, así como favorecer herramientas de calidad de vida en el retiro activo.

En las grandes empresas desarrollamos programas de RSC para disminuir la brecha digital en la sociedad.

2. **Cursos de formación abiertos para mayores de 45 años.**

Nuestros cursos se dirigen a personas mayores de 45 años con el **objetivo de mejorar la calidad de vida, disminuir la brecha digital, generar programas de voluntariado intergeneracional y aumentar las probabilidades de encontrar un empleo.**

Los alumnos se forman sin coste alguno para que las empresas reviertan a la sociedad en concepto social la aportación que perciben d e la misma y de plan de comunicación (marketing emocional).

Este año vamos a formar a unas 1.000 personas en colaboración con diferentes entidades como Cruz Roja, Fundación Caja Círculo, Centro Comercial el Mirador, Camara Decimavilla, Hotel Almirante Bonifaz, Grupo Tiempo Activo, Asociación Abuelas de Gamonal, Cáritas, Construcciones Bubolta, Reyca-C, Regalos Gifts, Campofrío, etc.

Cursos abiertos durante todo el año:

Competencias Digitales 8h y 16h Smarthphone.

Competencias Digitales 8h y 16h PC

Programa a medida para grandes empresas y pymes (gestión personal interno)

Programa la Buena Vida (personal de grandes empresas)

Inteligencia Emocional 16h
Competencia Digital 16h

"Programa Manual de Nuevas Metas"

Digitalización de contenidos: Además de digitalizar contenidos formativos a medida de las necesidades de los clientes, creamos programas a medidas de las necesidades de las empresas, ya que al entrar en la empresa tenemos un Manual de Acogida, al finalizar la relación laboral con la empresa podemos tener también un manual. ¿Se pueden crear Herramientas y Programas para cumplir años con calidad de vida?.

https://www.conectados-sinbarreras.com/cursos/

3. Proyecto intergeneracional voluntariado.

Con el fin de unificar "Talento, Tecnología y Experiencia", hemos desarrollado los siguientes programas:

Un programa llamado "HERRAMIENTAS Y PROGRAMAS PARA CUMPLIR AÑOS CON CALIDAD DE VIDA"

Un lema nos inspira: 'Tanto aprende el joven del mayor, como el mayor del joven".

Se ha conseguido que una persona con 67 años imparta clases en la Universidad después de haber recibido el programa Conectados Sin Barreras en el módulo "Ocio y tiempo libre de calidad".

Un PROGRAMA UNIVERSITARIO DE VOLUNTARIADO NACIONAL E INTERNACIONAL:

Dirigido a:

Personas interesadas en programa intergeneracionales.

Estudiantes y graduados en titulaciones vinculadas con la educación y el desarrollo social y ocupacional (pedagogía, educación social, Terapia Ocupacional, etc.).

Profesionales del ámbito del acompañamiento, cuidad y desarrollo de personas mayores.

Temarios:

Bloque 1: Mantenimiento de la autonomía.

Bloque 2: Desarrollo de Calidad de Vida de las personas mayores.

Bloque 3: Programa Responsabilidad Social Corporativa Conectados Sin Barreras y su papel.

Bloque 4: Competencia Digital.

Bloque 5: La Buena Vida: Inteligencia Emocional.

Entrega de diplomas y clausura del curso.

Se reconocerá 0,5 créditos para los alumnos matriculados en los Títulos Oficiales adaptados al Espacio Europeo de Educación Superior (Grados). Los alumnos interesados deberán someterse al proceso de evaluación que será comunicado por la dirección del curso en la presentación del mismo. Asimismo todos los asistentes recibirán un certificado siempre y cuando se justifique una asistencia del 80%.

Los voluntarios de "Conectados Sin Barreras" también pueden ser personas con más de 30 años que cumplan el perfil para recibir el curso de Formador de Formadores en Competencias Digitales.

4. Plataforma tecnológica de emprendimiento social (programa embajadores e internalización latam)

Algunos de los conceptos que hemos trabajado para impartir cursos presenciales, con formación on line de calidad contrastada para los instructores son:

Plataforma Tecnológica de Emprendimiento Social con nuestro.

Programa de Embajadores para poder llevar a cada provincia y rincón de España, así como al medio rural el Proyecto RSE Conectados Sin Barreras.

Mitigar la soledad en los mayores.

Fomentar el emprendimiento social.

Del mismo modo desarrollamos dentro de la **Economía Colaborativa del proyecto con la empresa Socialmente Responsable Thalentia un Campus** de formación trabajando la digitalización de los contenidos desde el punto de vista **del aprendizaje digital y los contenidos psicopedagógicos.**

Algunos de los países objetivos de la Expansión son Chile, México, Colombia, Perú y Argentina entre otros.

Gracias al gran equipo multidisciplinar y varios colaboradores hemos conseguido realizar este gran proyecto de Responsabilidad Social Empresarial y Corporativa.

5. Video Marketing

Además promovemos la RSE en micropymes y pymes a través del Video Marketing y el testimonio de los alumnos generando empresas Socialmente Responsables como fuente de generación económica del proyecto.

Hemos desarrollado la metodología como concepto de los GEO DIGITAL CONGRESS donde hemos colaborado con ANVIMA *(www.anvima.orga)* y AJE MADRID *(www.ajemadrid.es)* donde los ponentes de Marketing Digital y sus empresas son socialmente responsables

http://geodigitalcongress.es/
http://geodigitalcongress.es/geopildoras

6. Entrevistas en plataforma de estudio virtual

Como punto final, se abordan entrevistas en Plató de Estudio Virtual entrevistas con responsables de RSC de grandes empresas, que nos indicaran el estado actual y los próximos pasos de la RSC a nivel nacional e internacional.

SEGUIMIENTO DE INDICADORES

Lo que no se puede medir no se puede gestionar, y para conocer si una metodología funciona o no, es conveniente disponer de algún indicador sobre la difusión o efectividad del mismo, como podría ser en este caso:

Acuerdos marco firmados: Actualmente tenemos 25 acuerdos marco firmados con Ayuntamientos, Asociaciones sin ánimo de lucro y Fundaciones que dan soporte a la difusión y al plan del comunicación del proyecto formativo.

Clientes actuales:

Grandes Empresas: Actualmente tenemos en marcha 6 proyectos con Grandes Empresas (Fundación Caja Círculo, GAES, Campofrío, Ascensores Zener y Caja Rural Viva).

Pymes: En marcha 4 proyectos Cámara Decimavilla (Adventis Solutions), Grupo Tiempo Activo, Grupo Julián y Maquinaria Cámara.

Micropymes: Más de 30 clientes actualmente.

Alumnos formados: Este año vamos a formar a unas 1.000 personas en colaboración con diferentes entidades tales como Cruz Roja y Cáritas.

Ponemos a disposición de los alumnos un canal para que los potenciales alumnos resuelvan las dudas que les surjan, como por ejemplo implementando:

Registro a través de la propia plataforma web, correo electrónico.

Registro plantear dudas y consultas sobre necesidades en mayores de 45 años.

Publicación de FAQ con publicación interna periódica, con la resolución de las principales consultas anónimas recibidas de forma general.

Encuesta de calidad al finalizar los curso. A fin de conseguir el objetivo de mejora continua en nuestros cursos, este año hemos implementado una encuesta de satisfacción, que respete el anonimato, y que se remita al cierre, nos puede ayudar a recoger aspectos de mejora en la gestión de los cursos.

SECCIÓN NOTICIAS

Primer curso de Auditor Jefe en la norma UNE19601:2017

realizado para los miembros de la AEAEC en colaboración con la entidad de certificación ADOK los días 9, 10, 11, 16 y 17 de Julio en Madrid.

Con este curso de 40 horas de duración los 15 alumnos participantes (asociados de AEAEC) han adquirido los conocimientos teóricos y prácticos necesarios para capacitarse como auditores jefe del sistema de gestión de compliance penal UNE 19601.

Con este curso los alumnos están en condiciones de planificar y realizar las auditorias de los sistemas de gestión de Compliance penal implantado conforme a los objetivos y requisitos de la norma UNE 19601.

El curso se dividió en dos partes: Una teórica relativa a los objetivos y requisitos de la norma UNE 19601, norma alineada tanto con los requisitos que el art. 31 bis del C.P. exige para que los programas de prevención de delitos puedan actuar como causa de exoneración de la responsabilidad penal de las personas jurídicas, como con las buenas prácticas ya reguladas en la UNE-ISO 19600 Sistemas de Gestión de Compliance. Directrices; en la UNE-ISO 37001 Sistemas de Gestión antisoborno y UNE-ISO 31000 Gestión del Riesgo.

Y otra práctica relativa a la Auditoría de sistemas de gestión conforme a la UNE-ISO 19011, donde se realizaron planificación de auditorías, redacción de informes y se analizaron los procesos de auditoria, y el comportamiento y responsabilidades de los auditores.

El curso fue impartido en su integridad por **Jorge Bonito Vera** Socio Director de Adok Certificación, Partner de la entidad alemana TUV HESSEN para su representación en exclusiva para España y Portugal.

La AEAEC alcanza un acuerdo estratégico con la International Compliance Association

Después de meses de contacto entre las directivas de ambas asociaciones, el pasado día 8 de junio la Asamblea General de la AEAEC adoptó por unanimidad de los socios asistentes, entre otros acuerdos de marcado componente estratégico, ratificar el convenio de colaboración con la International Compliance Association (ICA) alcanzado por sus directivas.

En virtud del convenio los socios de la AEAEC pasan automáticamente a ser asociados de la ICA participando de los beneficios que conlleva ser socio de ambos asociaciones.

Murray Grainger, director de Impact on Integrity empresa representante de la International Compliance Association (ICA), tuvo ocasión de explicar a los asistentes de la Asamblea general de la AEAEC el funcionamiento y actuaciones a nivel internacional promovidas por la ICA. ICA ostenta cuatro categorías de socios -denominadas Affiliate, Associate, Professional y Fellow- según la formación académica y experiencia profesional acreditada en el sector del compliance, contando todas ellas con diferentes beneficios y servicios a disposición del socio.

ICA INTERNATIONAL COMPLIANCE ASSOCIATION PARTNER

Presentación del software Compliance Protección de Datos (RGPD) desarrollado por la editorial Lefbvre-El Derecho.

Con motivo del curso de formación como auditores jefes en la UNE 19601 que Adok Certificación impartió a 15 asociados de la Asociación Europea de Abogados y Economistas en Compliacne | AEAEC durante la primera quincena de este mes de julio, D. Antonio Hurtado de Mendoza García, Director de formación, D. Julio Sainz, Director y responsable de la aplicación de Compliance y GDPR; y Dña. Ana Palicio, Gerente de Cataluña Lefebvre El Derecho, presentaron a los participantes del curso el software de "Compliance Protección de Datos (RGPD)" que ha desarrollado la prestigiosa editorial jurídica.

El programa presentado es un completo gestor documental diseñado para la correcta y sencilla implantación de un sistema de Prevención de riesgos penales conforme a los requerimientos de la UNE 19601, incluyendo sistemas de alertas y comunicación interna que facilitan el seguimiento y control de los procesos de gestión del programa, así como para la implantación de un programa de Protección de Datos Personales conforme a los requerimientos del RGPD.

Todos los asociados de AEAC podrán adquirir dicho programa en unas condiciones y ventajas especiales, tanto en términos económicos, como en la disponibilidad de la aplicación ADN Jurídico, una aplicación que permite al profesional mantenerse al día de las modificaciones en normativa.

Aprovechando este encuentro, responsables de AEAEC y el director de formación de la prestigiosa editorial, establecieron las bases para abrir canales de comunicación y futuras colaboraciones en materia de formación en Compliance entre la editorial jurídica y la AEAEC.

LEFEBVRE EL DERECHO

INTELIGENCIA JURÍDICA

Presentación de la herramienta gobertia

Eficiencia y Buen Gobierno

Solución que mejora la eficiencia, seguridad y coordinación de los órganos de gobierno a través de la digitalización

Aprovechando la presencia de 15 asociados de la AEAEC en el primer curso de auditor jefe en la norma UNE: 19601:2017, que tuvo lugar en Madrid la primera quincena de julio, la Compañía GOBERTIA presentó a los mismos su programa para la gestión de los órganos de gobierno de las personas jurídicas. Una herramienta tecnológica que permite acreditar a los miembros del órgano de gobierno la diligencia debida y dedicación adecuada de sus deberes legales y estatutarios, teniendo en cuenta las funciones atribuidas a cada uno de ellos; así como la adopción de las medidas precisas para la buena dirección y el control de la sociedad, y la solicitud a la misma de la información adecuada y necesaria para el eficaz cumplimiento de sus obligaciones.

La herramienta, presentada a los asociados de la AEAEC, por D. Guillermo Soto, y D Miguel Rull, a la sazón Director General y Responsable de Alianzas de GOBERTIA, es una aplicación multidispositivo que da acceso online y offline a las personas involucradas en el gobierno de la persona jurídica, facilitando la comunicación óptima entre los mismos y de éstos con la alta dirección, así como el proceso de toma de decisiones. El programa se adapta a las necesidades concretas de cada organización, atendiendo a su tamaño, procesos y procedimientos, lo que optimiza la eficacia de los órganos de gobierno, proporcionado además seguridad, autonomía y confidencialidad total en la gestión.

Los miembros de la AEAEC asistentes a la reunión intercambiaron opiniones con los responsables de GOBERTIA en relación con la utilidad de la herramienta como medio hábil para acreditar el cumplimiento de los órganos de gobierno en materia de Compliance penal, en cuanto que la misma tiene una importante misión de trazabilidad documental, que permite probar en un proceso penal la actuación de los miembros del órgano de gobierno, como responsables últimos del programa de cumplimiento penal, el liderazgo y la diligencia debida en la política y en el sistema de Compliance penal de la organización, así como en la revisión del sistema, para la mejora continua de la organización.

JURISPRUDENCIA COMPLIANCE

SENTENCIA TRIBUNAL SUPREMO 121/2017
DE FECHA 23/02/2017
Ponente: Monterde Ferrer, Francisco.

El caso enjuiciado versaba a la falta de alta de cotización y de alta en la Seguridad Social de nueve trabajadoras extranjeras dedicadas a la actividad de alterne en un pub.

La Sentencia del Supremo confirma la condena para el administrador único de la entidad que explota el club y declara a ésta como responsable civil subsidiaria.

En el recurso de casación se alega que en la sentencia no se resuelve nada sobre la circunstancia de que la sociedad mercantil titular de la explotación no haya sido acusada como entidad obligada a cursar el alta de las personas consideradas trabajadoras, los hechos y la responsabilidad por tal omisión. Y se llama la atención sobre que fue a dicha mercantil, y no al recurrente como administrador de la misma, a la que sancionó la inspección de trabajo por la falta de alta de las trabajadoras, como consta en el acta obrante a los folios 23 a 30.

El fundamento de derecho segundo de la sentencia desestima el motivo porque "El art. 851.3 de la LECr, señala que: *"También podrá interponerse el recurso de casación por la misma causa, cuando no se resuelva en ella (la sentencia) sobre todos los puntos que hayan sido objeto de la acusación y de la defensa."*.

"El recurrente –considera la sentencia- parte de un planteamiento equivocado. Ya vimos los términos en que la defensa del recurrente planteó sus conclusiones provisionales y definitivas. Además, la entidad Paradela SL. no puede ser acusada por este delito a tenor del art. 31 bis CP. El art. 318 no se remite al art.31bis. Lo que hace - mediante una cláusula que está vigente desde la LO 11/2003 y por ello con anterioridad a que se implantase la responsabilidad penal de las personas jurídicas por Lo 5/2010- es permitir la atribución de la pena en tales casos a los administradores y que quepa imponer alguna de las medidas del art. 129 CP a la persona jurídica; pero ésta no puede ser acusada como responsable penal.

Dice así el art. 318 CP: " Cuando los hechos previstos en los artículos de este título (Título XV, de los delitos contra los derechos de los trabajadores) se atribuyeran a personas jurídicas, se impondrá la pena señalada a los administradores o encargados del servicio que hayan sido responsables de los mismos y a quienes, conociéndolos y pudiendo remediarlo, no hubieren adoptado medidas para ello. En estos supuestos la autoridad judicial podrá decretar, además alguna o algunas de las medidas previstas en el artículo 129 de este Código."

De hecho, ha sido frecuente la crítica doctrinal sobre la no inclusión de los delitos contra los derechos de los trabajadores en el listado de delitos en los que cabe opere el art. 31bis.

Además, -como apunta el Ministerio Fiscal- la responsabilidad penal de la persona jurídica no condicionaría la de la persona física, ni viceversa conforme a los (arts. 31bis y ter) CP."

Por todo ello, el motivo ha de ser desestimado.

TRIBUNAL SUPREMO, SALA SEGUNDA, SENTENCIA Nº 374/2017
DE FECHA 24/05/2017, RECURSO Nº 1729/2016.
Ponente: Luciano Varela Castro.

La Sala Segunda del Tribunal Supremo, confirma la Sentencia de la Audiencia Provincial de Barcelona, por la que condena a Messi, por tres delitos fiscales contra la Hacienda Pública, por desviar el pago obligado del I.R.P.F. por los ingresos obtenidos por la explotación de sus derechos de imagen, los cuales fueron cedidos a sociedades sitas en paraísos fiscales a través de contratos ficticios.

Según los Hechos Probados de la Sentencia de la A.P. de Barcelona, el jugador no realizó la correspondiente declaración de la renta de los años 2007 a 2009. Para ello, previamente en el año 2005, inició la estrategia de ceder sus derechos de imagen a sociedades radicadas en paraísos fiscales. A la vez, estas empresas formalizan contratos de explotación de su imagen a sociedades radicadas en países sin convenio de doble imposición con España. Así el jugador tenía unos ingresos sin pasar por la Hacienda española.

A pesar de que el jugador, mantuvo una estrategia de defensa basada en el desconocimiento de la tributación fiscal de los ingresos, la Sala concluye que no es un error de tipo ni de prohibición, ni se puede esconder detrás de la responsabilidad del artículo 31 CP.; señalando la sentencia que el jugador sabía al firmar los contratos que ello le llevaba *"inexorablemente al insolidario resultado de la defraudación fiscal"*.

En cuanto al argumento esgrimido por el jugador de que confió el tema fiscal a asesores de su entera confianza, la Sala afirma que dicho argumento solo sería asumible si estuviéramos en un caso de *"ineludible «delegación», de quienes están en un escalón a favor de subordinados lo que se traduce en que queden excluidos de responsabilidad penal, si aquella confianza resulta legítima. Incluso, cuando la responsabilidad penal puede atribuirse, en los específicos casos así tipificados, a la persona jurídica, ésta puede resultar exenta de esa responsabilidad penal. Pero, eso sí, cuando la confianza en el gestor que actúa por ella se antecede de las precauciones del artículo 31 bis 2 del Código Penal* .

Pero, cuando la pluralidad de sujetos concurrentes a la producción delictiva se manifiesta en una especie de «asociación» horizontal, fuera del marco de una organización económica o jurídica compleja, y que puede dar lugar a responsabilidades penales plurales, ya de coautoría ya de participación, resulta extraño el concepto mismo de delegación. La «distribución de funciones» entre los partícipes acarrea entonces acumulación de responsables criminales. En ningún caso exoneración de ninguno."

En este sentido la Sala considera que también los acusados deberían haber sido acusados, pues el jugador acudió a ellos para evitar el pago de impuestos, en consecuencia, para cometer el delito. Los asesores deberían haber sido acusados como cooperadores. Indica la Sentencia: *"Cuando acude al despacho profesional no es para que éste le informe sobre cuál sea su obligación tributaria y cómo darle adecuado cumplimiento, sino para que le indiquen cómo lograr eludirlo, pues solamente desde este designio se comprenden los actos materialmente ejecutados por el acusado"*

La Sala es unánime en el castigo que se le impone al jugador y a su padre, excepto en considerar el delito fiscal como continuado o como tres delitos fiscales independientes. Le impone al padre una rebaja por haber devuelto la cantidad defraudada antes de juicio. Al jugador la Audiencia Provincial ya le había rebajado la pena, por resarcimiento del daño.

SENTENCIA TRIBUNAL SUPREMO Nº 455/2017
DE FECHA 21/06/2017
Ponente: Juan Saavedra Ruiz.

La Sentencia confirma la dictada por la Audiencia Provincial de Salamanca, por la que se condena al Consejero Delegado de una sociedad mercantil como autor responsable de un delito de malversación de caudales públicos; al quedar demostrado que dicho directivo (consejero delegado y propietario del 87,95% de las participaciones) se apropió el dinero que le fue entregado en el marco de ayudas públicas concedidas por el Ministerio de Industria, Turismo y Comercio para la persona jurídica a la que representaba.

En consecuencia, la misma se vio obligada a presentar concurso necesario de acreedores por no poder asumir todas las deudas a las que había caído la empresa.

Las sentencia resuelve la vulneración del principio acusatorio que se alega como infringido en el recurso por cuanto no se ha perseguido penalmente ex artículo 31 bis CP a la persona jurídica, hoy acusación particular, en quien concurre la cualidad de beneficiaria de las subvenciones, sosteniendo lo que podríamos denominar un impropio litisconsorcio pasivo necesario.

Según la Sala ello "carece de fundamento si tenemos en cuenta que la responsabilidad penal de la persona física (administrador o representante legal o persona que actúe individualmente o como integrante de un órgano de la persona jurídica) es autónoma de la del ente social; además la pretensión de haberse vulnerado el principio acusatorio por defecto tampoco es sostenible pues no existe el derecho a la condena de otro; y, por último, como señala el Ministerio Fiscal en su informe "los comportamientos de la persona física (acusado), no se realizaron en beneficio directo o indirecto de la sociedad, como exige el sino en todo caso en su perjuicio", con cita de la STS 154/2016."

El motivo octavo del recurso denuncia por la vía del artículo 849.1 LECrim la indebida aplicación del artículo 308 , 31 e inaplicación del 31 bis, todos ellos CP .

Sostiene el motivo que el acusado ha sido condenado como autor del delito del artículo 308.2 en base al artículo 31 CP "sin que se haya condenado a la persona jurídica", de forma que si el delito mencionado tiene naturaleza de especial propio y solo puede ser cometido por el que recibe la subvención, que tiene la obligación de devolverla o justificarla, ésta es la única obligada. Objeta también la infracción del primero de los artículos en la medida que no ha quedado acreditada la conducta típica realizada por el acusado porque para ello sería necesario conocer el proyecto para el cual se aprobó dicha subvención sin que ello conste en la causa. También afirma el desconocimiento de la subvención por parte del Tribunal siendo la primera a fondo perdido y la segunda un préstamo con un plazo de devolución de quince años y la Secretaría de Estado de Telecomunicaciones no ha declarado quebranto alguno del fin por el que se dio la subvención, por lo que se ha aplicado indebidamente el artículo 308 CP Igualmente objeta la fijación de la responsabilidad civil declarada.

La sentencia desestima el motivo con el argumento de que " *Efectivamente, la autoría del acusado, -que según el hecho probado era propietario y consejero delegado de la sociedad subvencionada y dispuso de las ayudas públicas recibidas, con independencia del retorno a la sociedad de las cantidades dispuestas, lo que es indiferente para la consumación del delito que tiene lugar cuando se aplican a fines distintos de aquéllos para los que la subvención o ayuda fue concedida-, corresponde a la extensiva prevista en el artículo 31 CP .*

Este artículo tiene su antecedente en el 15 bis derogado que fue introducido por la reforma de 25/06/1983, precisamente con el fin de evitar las lagunas punitivas que se daban en los delitos especiales propios relacionados con las personas jurídicas, cuando se requiere para poder imputar la autoría que concurran ciertas cualidades o condiciones personales en el sujeto activo que en algunos supuestos delictivos, como es el caso, solo se daban en la persona jurídica, pero no en la persona física que actuaba como su representante o administrador (como también es el caso). Para cumplimentar el principio de legalidad y

solventar los problemas que suscitaba alguna jurisprudencia que cubría las lagunas legales con criterios de analogía "contra reo", se dio vida al artículo 15 bis, integrado en sus aspectos sustanciales en el actual artículo31 CP. Sin embargo, ello no significa que para ser considerado autor del delito correspondiente baste con ocupar el cargo de administrador o representante de la sociedad vinculada al hecho delictivo, sino que además es preciso que el imputado incurra en una acción u omisión, siempre que en este último caso ocupe la posición de garante y se den los restantes requisitos del artículo 11 CP que aparezca recogida en el tipo delictivo que se le atribuye. Esta doctrina ha sido corroborada por el Tribunal Supremo y el Tribunal Constitucional (STC 253/1993).

Las condiciones para la aplicación del tipo de autoría por extensión de la del artículo 28 prevista en el que comentamos concurren en el caso enjuiciado. Ya hemos señalado que el acusado es propietario de la sociedad subvencionada y además consejero delegado, de la prueba practicada se deduce además que como tal disponía de los fondos de la sociedad; concretamente de las cantidades transferidas por la Administración, lo que significa que conocía su procedencia y finalidad, que no obstante ello no fueron aplicadas a los fines previstos en la resolución administrativa correspondiente y que la sociedad fue declarada en concurso necesario de acreedores por auto de 01/10/2012 como también se refleja en el hecho probado. Estos hechos son suficientes para subsumir la conducta del ahora recurrente en el tipo de autoría aplicado incluso aunque admitiésemos la comisión por omisión puesto que como propietario y consejero delegado era garante del buen fin del proyecto subvencionado. Es más si fuese cierto que las cantidades subvencionadas hubiesen retornado a la sociedad es inexplicable que no hubiesen sido invertidas en la consecución de los proyectos adjudicados."

SENTENCIA DEL TRIBUNAL SUPREMO Nº 583/2017 DE FECHA 19/07/2017

En esta Sentencia, la Sala resuelve varios recursos interpuestos contra la Sentencia de la Audiencia Nacional 29/2016, de 15 de julio

Ponente: Antonio del Moral García

El acusado, junto con sus familiares, iniciaron un entramado familiar y empresarial, con la intención de introducir en el mercado el dinero procedente de sus actividades ilícitas relativas al tráfico de sustancias estupefacientes, también protegiendo el patrimonio adquirido, para evitar la incautación por la justicia. La sentencia declara responsables penales a varias personas jurídicas, imponiendo penas que van desde multa al cierre de locales comerciales y suspensión de actividades hasta incluso la disolución jurídica y mercantil de una de las entidades.

El Alto Tribunal, repasa los elementos esenciales de la responsabilidad penal de la persona jurídica. Todo ello, según las pautas incluidas en el artículo 31 del CP, tanto en la redacción vigente en la fecha de la comisión del delito, así como de la posterior reforma del artículo. Recalca los requisitos por los que se puede condenar a una persona jurídica: actividad ilícita de los directivos de la persona jurídica; consecución de un beneficio directo o indirecto para aquella; y la ausencia de un programa de prevención de delitos.

"Se han acreditado –dice la sentenica- todos los elementos necesarios para que surja la responsabilidad penal de una persona jurídica . La atribución de responsabilidad penal de la persona jurídica, se ajusta, en efecto, a las exigencias contenidas en el art. 31 bis, tanto según la redacción vigente en el momento de los hechos, como en la emanada de la reforma de 2015.

a) Sus administradores y directivos (tanto de hecho como de derecho: actuando en representación de la empresa han llevado a cabo una continuada actividad encajable en el art. 301 CP que es precisamente una de las figuras delictivas en que el legislador prevé la imposición de penas para las personas jurídicas (art. 302 CP ; que en ese punto, por otra parte se adelanta a lo previsto en la propuesta de Directiva de 21 de diciembre de 2016 sobre la lucha contra el blanqueo de capitales mediante el Derecho Penal).

b) Concurre un innegable provecho o beneficio directo para la sociedad: Amadeo Pio realiza sucesivas inyecciones de dinero a la empresa, para introducir en el circuito económico lícito ganancias provenientes del tráfico de drogas; y adquiere para la Sociedad vehículos y maquinaria con metálico de idéntica procedencia.

c) Y, por fin, está cubierta también la faz negativa de esa atribución de responsabilidad: la persona jurídica carecía de un sistema efectivo de control implementado para anular o, al menos, disminuir eficazmente el riesgo de comisión en el seno de la empresa de ese delito. No exige esto aquí demasiados comentarios a la vista del panorama al que nos enfrentamos. Ni siquiera se hace necesario evocar lo que sobre este punto y en relación a esta entidad lo que razonó la STS 154/2016 . Es patente que en una empresa cuyos únicos administradores cometen de consuno dolosamente una infracción penal actuando en nombre de la entidad con la colaboración de la mayor parte de los titulares formales del capital social (también condenados por conductas dolosas), no es dable imaginar otra hipótesis que no sea la de compartida responsabilidad penal del ente colectivo. Lo destaca la sentencia de instancia: sería un contrasentido que quienes controlan la persona jurídica a la que utilizan para canalizar su actividad delictiva a su vez implantasen medidas para prevenir sus propios propósitos y planes."

La sentencia es de interés porque analiza varios problemas procesales en relación al derecho de defensa de la persona jurídica.

Una de las sociedades condenadas planteó la nulidad del juicio al no concedérsele la última palabra, obligando a retrotraer el procedimiento bien al trámite final, bien al comienzo del juicio oral.

La Sala desestimó el motivo con los siguientes argumentos, recordando el enfoque que daba a esta cuestión la STS 154/2016, de 29 de febrero:

"Nos enfrentamos - dice la Sala- ante un importante problema que la LO 37/2011, de 10 de Octubre, sobre medidas de agilización procesal, que introdujo las reformas en la Ley de Enjuiciamiento Criminal consideradas pertinentes para adaptar la regulación adjetiva a la presencia de la persona jurídica como eventual autora de delitos, no resolvió en su día.

Se trata en concreto de responder al interrogante acerca de cuál habrá de ser el régimen para designar la persona física que deba actuar en representación de esa persona jurídica en el procedimiento en el que

se enjuicie su posible responsabilidad penal, no sólo en el ejercicio de la estricta función representativa sino también a la hora de dirigir y adoptar las decisiones oportunas en orden a la estrategia de defensa a seguir como más adecuada para los intereses propios de la representada, lo que obviamente resulta de una importancia aún mayor.

La cuestión lógicamente se suscita especialmente en aquellos supuestos en los que pudiera existir un conflicto de intereses procesales entre los de quienes, en principio, estarían legalmente llamados a llevar a cabo tales funciones representativas (representantes y administradores) y los propios e independientes de la persona jurídica, que a su vez pudieren incluso afectar a los derechos de terceros, como sus trabajadores, acreedores, accionistas minoritarios, etc.

Más en concreto aún, cuando aquel a quien se encomiende tal tarea fuere, a su vez, posible responsable de la infracción que da origen a la condena de la representada, teniendo en cuenta, como se ha dicho, que su actuación se extiende también a las decisiones relativas a la estrategia de defensa a seguir, que incluirán la posibilidad de optar por un camino de colaboración con las autoridades encargadas de la persecución y castigo del delito cometido por la persona física en el seno de la colectiva, aportando datos y pruebas sobre la identidad de su autor y los hechos por él cometidos, con el fin de obtener para la persona jurídica los beneficios punitivos derivados de esa opción como consecuencia de la aplicación de la correspondiente atenuante (vid. art. 31 quáter b) CP).

En estos casos, dejar en manos de quien se sabe autor del delito originario, la posibilidad de llevar a cabo actuaciones como las de buscar una rápida conformidad de la persona jurídica, proceder a la indemnización con cargo a ésta de los eventuales perjudicados y, obviamente, no colaborar con las autoridades para el completo esclarecimiento de los hechos, supondría una intolerable limitación del ejercicio de su derecho de defensa para su representada, con el único objetivo de ocultar la propia responsabilidad del representante o, cuando menos, de desincentivar el interés en proseguir las complejas diligencias dirigidas a averiguar la identidad del autor físico de la infracción inicial, incluso para los propios perjudicados por el delito una vez que han visto ya satisfecho su derecho a la reparación.

Cuando además, de acuerdo con lo previsto en el art. 31 ter CP (anterior art. 31 bis. 2 CP), la persona jurídica responderá "...aún cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella" y, según apartado 3 del mismo precepto, incluso ante el "...hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia..." .

Semejante cuestión, de tanta trascendencia procesal como puede advertirse y que es resuelta en otros ordenamientos con distintas fórmulas, como la designación a estos efectos por el órgano jurisdiccional correspondiente de una especie de "defensor judicial" de la persona jurídica, la asignación de tales responsabilidades a un órgano colegiado compuesto por personas independientes junto con otras en representación de los intereses de terceros afectados por las posibles consecuencias sancionadoras derivadas del ilícito de la persona jurídica, etc. o como lo era también en nuestro propio país en el Borrador de Código Procesal Penal de 2013 (art. 51.1) mediante la atribución de esas funciones de defensa, con carácter prioritario, al "director del sistema de control interno de la entidad" (el denominado también como "oficial de cumplimiento"), evidentemente no puede ser resuelta, con carácter general, por esta Sala.

Sin embargo nada impediría, sino todo lo contrario, el que, en un caso en el cual efectivamente se apreciase en concreto la posible conculcación efectiva del derecho de defensa de la persona jurídica al haber sido representada en juicio, y a lo largo de todo el procedimiento, por una persona física objeto ella misma de acusación y con intereses distintos y contrapuestos a los de aquella, se pudiera proceder a la estimación de un motivo en la línea del presente, disponiendo la repetición, cuando menos, del Juicio oral, en lo que al enjuiciamiento de la persona jurídica se refiere, a fin de que la misma fuera representada, con las amplias funciones ya descritas, por alguien ajeno a cualquier posible conflicto de intereses procesales con los de la entidad, que debería en este caso ser designado, si ello fuera posible, por los órganos de representación, sin intervención en tal decisión de quienes fueran a ser juzgados en las mismas actuaciones...».

Preservando esas consideraciones generales que se vuelvan a asumir, ha de precisarse que su proyección al caso ahora examinado carece de viabilidad: difícilmente pueden apreciarse intereses contradictorios entre una empresa con forma de Sociedad limitada y una de las concretas personas físicas condenadas a quien la sentencia atribuye la total titularidad de facto de la mercantil; o aquellas otras que ostentan la mayoría de su capital social, al menos formalmente.

Dos órdenes de argumentos -uno en un nivel subjetivo y otro material- apuntalan la necesaria desestimación del motivo al que se han sumado otros recurrentes

a) Por una parte en el plano de identificar los reales intereses de la persona jurídica,….

Nos hallamos, ante una persona jurídica que viene a identificarse con personas físicas acusadas.

Por tanto no hay intereses contrapuestos. Terceros afectados por la pena impuesta a la persona jurídica (empleados, v.gr.), lo estarían igualmente por la condena del titular único de la empresa individual. No por eso han de ser traídos al proceso.

b) Desde el punto de vista material o de fondo, es decir desde la necesidad de indagar en qué medida puede anudarse algún género de indefensión a esa supuesta omisión (un trámite formal de última palabra a una persona jurídica que estaba defendida por letrado, cuyos titulares reales eran parte en el juicio, y que no había designado a nadie diferente para ostentar su representación, designación que en todo caso correspondía a esos propietarios reales también partes en el proceso y que por tanto lo conocían de sobra su existencia y vicisitudes), las conclusiones no pueden ser más contundentes: ninguna indefensión ha podido producirse.

Frente a la jurisprudencia más antigua que consideraba que la desnuda constatación de la ausencia de ofrecimiento al acusado del derecho a manifestar lo que conviniera al término del juicio bastaba para provocar la nulidad (STS 891/2004 entre otras) es doctrina común hoy que solo cuando esa omisión ha supuesto una efectiva privación de un medio de defensa con contenido real será planteable un desenlace anulatorio. Básica en este punto es la STC 258/2007, de 18 de diciembre : tras razonar que una irregularidad procesal o infracción de las normas de procedimiento sólo alcanza relevancia constitucion-

al cuando produzca un perjuicio real y efectivo en las posibilidades de defensa de quien la denuncie, concluye que la vulneración del derecho a la última palabra no se debe configurar como una mera infracción formal desvinculada de la comprobación de que se ha generado una indefensión material. Argumentar sobre esa indefensión material es carga procesal del recurrente. Solo habrá indefensión material con relevancia cuando no sea descartable que el trámite omitido hubiera sido decisivo en términos de defensa, en el sentido de que hubiera podido determinar un fallo diferente. Nada de eso se aduce aquí: ¿qué alegato distinto al efectuado por la defensa hubiese hecho un eventual representante procesal de la empresa que no se hubiese formulado ya o hubiese aparecido en el informe de la defensa o en las manifestaciones de quienes eran los titulares de la persona jurídica? Es patente el carácter puramente formalista y retórico de la queja.

La STS 490/2014, de 17 de junio , ante una protesta semejante (e incluso menos débil pues se trata de queja esgrimida por el acusado persona física), sienta este criterio: " ... la queja es más formal que sustancial. No se alega indefensión material. Para que el motivo pudiese tener alguna viabilidad tendría que alegarse en qué hubiese variado su defensa de haber contado con esa difícilmente posible traducción "simultánea". Nada se dice al respecto. Solo se sugiere que no pudo hacer uso con eficacia de su derecho a la última palabra . Pero no se explica por qué; es decir, no se dice qué es lo que hubiese dicho ahora que ya está en condiciones de conocer la sentencia y sus argumentos. Ni siquiera cuando tras la condena puede conocer las razones esgrimidas, arguye que de haber conocido el contenido de alguna declaración hubiese hecho una alegación que omitió precisamente por no habérsele informado de la misma. La nulidad exige una efectiva indefensión que ni se preocupa de intentar justificar. ¿Hubiese dicho algo distinto en el momento de su derecho a la última palabra ? ¿Qué? Este es el momento de demostrar que se vio efectivamente reducida su posibilidad de defensa.".

AUDIENCIA NACIONAL, SALA DE LO PENAL, SECCIÓN 3ª, AUTO Nº 351/2017 DE FECHA 15/09/2017.

Ponente: Barreiro Avellaneda, María de los Ángeles.

Caso Bankia por delito de falsedad contable.

La Sala confirma el sobreseimiento respecto del Banco de España y de la Comisión Nacional del Mercado de Valores, y la imputación de Deloitte, S.L., que era la auditora, pues en los informes de auditoría emitidos para salir a Bolsa, se refleja una situación que no concuerda con la real de Bankia, dándole una apariencia de solvencia de la que carecía.

El Auto de la Sección Tercera de la Sala de lo Penal de la Audiencia Nacional revoca el sobreseimiento del procedimiento en relación con la auditora Deloitte,. La Sala, admite parcialmente el Recurso interpuesto por la Confederación Intersindical de Crédito, y deja sin efecto el sobreseimiento de la sociedad consultora Deloitte, con el siguiente argumento:

"…, excluir la responsabilidad penal porque el vínculo entre el Sr. Pedro y Deloitte es de autonomía profesional, no puede tener acogida. Nos señala el artículo 10 de la Ley 19/1988., de 12 de julio, de

Auditoría de Cuentas, vigente hasta 1 de julio de 2011 que versa sobre las sociedades de auditoría tenía la siguiente previsión en su apartado 3: «la dirección y firme de los trabajos de auditoría realizados por una sociedad de auditoría de cuentas corresponderá, en todo caso, a uno o varios de los socios auditores de cuentas o a auditores de cuentas que pueden ejercer la actividad de auditoría en España y que estén designados por la sociedad, de auditoría para realizar la auditoría en nombre de la sociedad». Es decir, socio y sociedad constituyen la misma unidad jurídica, de modo que la firma cuenta con un Control de Calidad Interno, y un Manual de Cumplimiento Normativo que comprende Políticas generales para todas las líneas de servicio, y se alega que existen Políticas de nivel 2 para la línea de auditoria. Planteamiento teórico que por el- momento no puede dar lugar a aplicar la exención de responsabilidad prevista en el artículo 31 bis 2 del Código Penal, al desconocerse el grado de cumplimiento de esas políticas en el supuesto, pese a la incuestionable colaboración de la firma Deloitte explicando el tratamiento para detectar ilícitos penales, como se articula en el escrito de impugnación del recurso de apelación y en dos anteriores."

A fin de poder acreditar el beneficio directo o indirecto que el art. 31 bis exige para declarar la responsabilidad penal de una persona jurídica: El Auto determina el posible interés indirecto de la sociedad auditora en mantener al cliente.

El voto particular de uno de los componentes de la Sala se opone al sobreseimiento del caso para la cúpula del Banco de España y la CNMV. Aquella señala que: *"Existen indicios múltiples, concurrentes y razonables de criminalidad que permiten inferir que los máximos dirigentes del Banco de España y la CNMV avalaron y propiciaron con pleno conocimiento la falsedad contable más que detectada previamente a la salida a Bolsa de Bankia, a sabiendas del grave perjuicio que con ello se iba a causar a los inversionistas, que era evidente iban a ser minoritarios, en estada de inversores"*. Finalmente, no se les imputó ningún delito, pues, ni el uno ni la otra, decidieron la salida a Bolsa de la entidad bancaria, ni tampoco intentaron aparentar solvencia donde realmente no existía.

Para ello la Sala manifiesta que: *"La ley penal no castiga la ausencia de actividad de la autoridad competente".*

En este sentido la Sala, en línea con el juez instructor, considera que la elaboración de las cuentas es una obligación "exclusiva y excluyente" de los Administradores y la actuación del Banco de España como órgano supervisor nunca podría encajar en términos penales de cooperación o complicidad.

SENTENCIA TRIBUNAL SUPREMO 2498/2018,
DE FECHA 28/06/2018
Ponente: Vicente Almagro Serve

Hechos probados:

El acusado, mayor de edad y sin antecedentes penales, en su condición de administrador único de la entidad Hispanoucrán, constituyó en fecha 13 de febrero de 2007, junto con la sociedad italiana Energy Coal Spa, al 50% de participaciones sociales cada una de ellas, la empresa denominada Carbuastur S.L., actualmente Energy Fuel Asturias S.L., con domicilio social en C/ Lepanto s/ n de San Juan de Nieva - Castrillón- y cuyo objeto social era la comercialización de combustibles sólidos, productos carboníferos, que en la práctica se reconducía a la adquisición de carbón de importación, procedente principalmente de Ucrania, cuyo almacenaje se verificaba en las instalaciones de la Sociedad, ubicadas en el Puerto de Avilés, bajo el marco de depósito aduanero. El acusado, en su condición de administrador de la entidad por la que percibía una retribución, que en el año 2012 ascendió a 55.413 euros, cargo que pese a ser solidario con el otro administrador, quien no percibía retribución alguna, ejercía de manera individual, al encontrarse éste permanentemente en Italia, llevaba a efecto toda la gestión ordinaria y diaria de la empresa, causa por la que durante el periodo comprendido entre su nombramiento y su cese, por escritura pública otorgada en fecha 31 de agosto de 2013, cometió numerosas irregularidades en la gestión de la misma con el consiguiente perjuicio económico para Energy Fuel Asturias y así: 1.- Durante este periodo y sin el consentimiento del otro administrador solidario, procedió a realizar disposiciones en efectivo de "caja" y transferencias a su cuenta bancaria personal sin justificación alguna de su destino; asimismo periódicamente y sin conocimiento del otro administrador se fueron realizando transferencias bancarias a su cuenta personal por importe de 1.000 euros mensuales, ascendiendo el importe total a la suma de 126.976,96 euros. 2.- De idéntica manera y sin conocimiento ni autorización del otro administrador, procedió a domiciliar en las cuentas de la sociedad las facturas de sus gastos personales, correspondientes a sus teléfonos móviles, los de su familia -pareja e hijo-, sus empresas, a la televisión -gol televisión- de pago, cuotas de afiliación al partido político Foro Ciudadanos y de un club de fútbol, Sporting de Gijón, ascendiendo su importe a un total de 19.154,07 euros. 3.- En fecha 8 de marzo de 2010 el acusado como administrador de la sociedad recibió por parte del cliente, Emergicar S. L., la suma de 85.000 euros en metálico, ingresando en la cuenta de la sociedad la cantidad de 82.000 euros, restando por ingresar los restantes 3.000 euros, sin causa justificada. 4.- En fecha 22 de junio de 2009 el acusado constituyó una garantía en nombre de la sociedad en relación con la operación de un préstamo solicitando en el año 2006 por la empresa Sumara&Holtz, de la que era accionista y administrador único el acusado, operación que llevó a efecto sin conocimiento ni autorización del otro administrador.

La empresa Energy Fuel Asturias, S.L., tenía alquiladas unas instalaciones en el depósito aduanero del Puerto de Avilés, donde se almacenaba el carbón procedente de Ucrania y clasificaba para su posterior venta a los clientes, con unas ventajas fiscales por razón de tratarse de carbón procedente de países no pertenecientes a la Unión Europea y donde se prohibía, por ello, el almacenamiento de mercancías nacionales. El acusado sin conocimiento ni autorización del otro administrador procedió a utilizar dichas instalaciones para su uso personal, introduciendo carbón nacional procedente del Alto Bierzo, mezclándolo con el allí existente, con lo cual conseguía ofrecer a sus clientes -de la entidad Hispanoucrán S.L.- un producto de mejor calidad a un precio más bajo y, por el contrario, el mezclarse ambos carbones Energy Fuel vendía a sus clientes un producto de peor calidad a un precio más alto, todo ello con el consiguiente perjuicio para la empresa con quejas y pérdida de alguno de sus clientes y la correspondiente multa que le impuso la Agencia Tributaria de 606.770.99 euros más 92.534,13 euros en concepto de recargo y 11.683,86 euros en concepto de intereses de demora al detectar

"incumplimiento de las obligaciones a que quedan sujetas las mercancías sometidas a derechos de importación como consecuencia del régimen de depósito aduanero ... y que no habría presentado declaraciones de importación ni había ultimado el régimen de acuerdo con la normativa aduanera comunitaria". Finalmente el acusado procedió a quedarse con unos 9.040,16 toneladas de carbón suministradas por el socio Energy Coal Spa a Energy Fuel Asturias.

Calificación por el El Mº Fiscal:

-El ministerio público modificó sus conclusiones, calificando definitivamente los hechos como constitutivos de un delito de administración desleal del art. 295 del Cº Penal , en su redacción vigente al tiempo de los hechos, y un delito de apropiación indebida de los arts.252 en relación con el art. 250.1 y 5 del Cº Penal , en su redacción vigente al tiempo de la comisión de los hechos, considerando autor de los mismos al acusado, para quien, sin la concurrencia de circunstancias modificativas de la responsabilidad penal, solicitó la imposición de 3 años y 6 meses de prisión con la accesoria legal correspondiente por el delito de administración desleal, y la pena de 5 años de prisión con la accesoria legal y multa de 12 meses a razón de 20 euros día por el delito de apropiación indebida; asimismo interesó que el acusado indemnizara a Energy Fuel Asturias S.L. en la cuantía de los perjuicios causados realmente a la misma.

Sentencia de la Audiencia Provincial de Asturias (Seccc 2ª)

La Audiencia condenó al acusado como autor penalmente responsable de: 1.- Un delito continuado de apropiación indebida, ya definido, sin concurrir circunstancias modificativas de la responsabilidad penal, a la pena de dos años y nueve meses de prisión, con la accesoria legal de inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena y pena de 10 meses de multa a razón de 20 euros-día, con la responsabilidad personal subsidiaria del art. 53 del Cº Penal en caso de impago y 2.- Un delito de administración desleal, ya definido, sin la concurrencia de circunstancias modificativas de la responsabilidad penal, a la pena de tres años de prisión con la accesoria legal de inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena; imponiendo como responsabilidad civil ex delito la obligación al condenado de indemnizar, a la entidad Energy Fuel Asturias S.L. L. -antigua CARBOASTUR- en la suma de 2.043.877,01 euros, más los intereses legales del art. 576 de la L.E.Civil.

Recurrida la sentencia en casación la Sala Segunda del Tribunal Supremo conforme explicita en el Fundamento Jurídico 10º, aprecia que se ha penado por separado la continuidad delictiva en la apropiación indebida de la administración desleal y que la esencia del art. 74 CP debe llevarnos a

considerar la condena conjunta de la continuidad delictiva de ambos delitos con una condena de cuatro años de prisión en lugar de la condena por separado de los ilícitos cometidos de apropiación indebida y administración desleal, considerando más acorde con la realidad este marco punitivo.

Lo interesante de la sentencia en materia de Compliance es que en el fundamento de derecho UNDÉCIMO de la Sentencia que analiza el décimo motivo del recurso por infracción de precepto constitucional al amparo del artículo 5.4 de la Ley Orgánica del Poder Judicial y artículo 852 de la LECR, en relación con el 24 de la Constitución Española , por vulneración del derecho a la presunción de inocencia y tutela judicial efectiva, en que el recurrente trata de fundar básicamente en que no existe prueba de cargo que pueda sustentar una sentencia condenatoria, para lo que ha planteado hechos probados alternativos entendiendo que de la pericial no se evidencia la ilicitud objeto de condena, y que la pericial que aportó es clara prueba de descargo de la tenida en cuenta por el Tribunal y documentos tanto respecto a la falta de pesaje del carbón y la ausencia de una prueba clara y directa de esa pretendida apropiación de 9.040 toneladas de carbón por parte del recurrente; como con respecto al destino de las cantidades por las que se le condena por apropiación indebida al sostener el recurrente que resulta absolutamente coherente y se compadecen con el desenvolvimiento habitual de sociedades del sector que habitualmente existen diversos gastos, tales como sobresueldos, comisiones, gastos de "representación" de difícil justificación documental y que por ello no aparecerían reflejados en la contabilidad; **la Sala después de analizar la reiterada doctrina del propio Tribunal sobre el derecho a la presunción de inocencia y los requisitos constitucionalmente exigibles a la prueba para desvirtuar dicha presunción, para concluir que si ha habido prueba de cargo, y que el proceso de valoración de prueba del Tribunal no es arbitrario ni no ajustado a la práctica de la prueba,** pues la prueba de cargo con la que ha contado el Tribunal se refiere a datos evidentes, y que pese a que el recurrente pretenda justificar cada uno de los pasos que ha dado - pero que constituyen ilícitos penales- aun entendiendo que para cada actuación había una justificación y que todo ello se había realizado al amparo del asentimiento del administrador solidario, cuando la confianza del otro administrador societario con el recurrente es lo que dió lugar a la situación creada con perjuicios económicamente evaluables y que consta en la pericial, y apropiaciones de dinero sin justificar correctamente, ***añade obiter dicta que: "la justificación que ahora otorga el recurrente a cada uno de sus movimientos dista mucho de adecuarse a un normal desenvolvimiento de lo que se espera de un administrador societario que cumpla con los deberes y funciones que exige el Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital. Además, de haber existido un adecuado programa de cumplimiento normativo externalizado no se habrían dado estas circunstancias, o de haberse producido se habrían detectado de inmediato. Lejos de ello, la ausencia de un control adecuado y de una vigilancia ad intra por profesionales compliance officer no hubiera dado lugar al estado actual de la cuestión con perjuicios evaluables y el recurrente renunciando a sus cargos en las escrituras que refirió que no tienen otro efecto más allá de una voluntaria desvinculación de la sociedad, pero sin efectos exoneratorios de responsabilidad penal."***

DOMICILIO SOCIAL

Passeig Vergaguer, 120, Entlo. 4ª
Igualada (Barcelona)
Telf.: +34 938 049 038
info@aeaecompliance.com

VALENCIA
C/Barcas, 2, planta 4 - Valencia
Telf: +34 630 148 870
valencia@aeaecompliance.com

MADRID
O´Donnell, 12 - Madrid
Telf: +34 607 225 405
madrid@aeaecompliance.com

BARCELONA
P. Verdaguer, 120, ent 4º - Igualada
Telf.: +34 938 049 038
barcelona@aeaecompliance.com

GIRONA
Pza. Cataluña, 1, Entl. 3 – Blanes
Telf.: +34 972 33 44 05
girona@aeaecompliance.com

TENERIFE
C/ Molinos de Agua,10,1º
San Cristobal de La Laguna
Telf: +34 922 315 179
tenerife@aeaecompliance.com

MURCIA
C/ Platería,7 3ºD 30004 Murcia
Telf: +34 968 213 784
murcia@aeaecompliance.com

CÁDIZ
C/ Sociedad, 10, 1º-B Cádiz
Telf.: +34 956 264 806
cadiz@aeaecompliance.com

A CORUÑA
San Andres, 33 - 1a, A Coruña
Telf: +34 651 194 727
acoruna@aeaecompliance.com

ASOCIACION EUROPEA DE ABOGADOS Y ECONOMISTAS COMPLIANCE

CÓRDOBA
C/José Cruz Conde, 30, 3º 1ª - Córdoba
Telf: +34 957 496 501
cordoba@aeaecompliance.com

GUADALAJARA
C/Enrique Benito Chávarri, 6, 2º - Guadalajara
+34 949 22 00 73
guadalajara@aeaecompliance.com

MALLORCA
C/de Velázquez, 10 - Mallorca
Telf.: +34 689 19 19 55
mallorca@aeaecompliance.com

ASTURIAS
C/ San Bernardo, 3 - Avilés
Telf.: +34 984 835 245
asturias@aeaecompliance.com

CASTELLÓN
C/ Poeta Verdaguer, 1, Ento.
Telf.: +34 644 01 56 01
castellon@aeaecompliance.com

ANTEQUERA
C/ Carreteros, 1, Antequera
Telf.: +34 952 194 017
antequera@aeaecompliance.com

SEVILLA
C/ Caños de Carmona, 9-1º-A, Sevilla
Telf: 34 954 707 700
sevilla@aeaecompliance.com

MÁLAGA
C/ Tomás Heredia, 23 - 2º Izq., Málaga
Telf: +34 957 498 050
malaga@aeaecompliance.com