Evaluación de Programas de Corporate Compliance. Nuevo documento del Departamento de Justicia de EEUU

El 30 de abril de 2019, el Departamento de Justicia de los Estados Unidos a través de su *"Criminal Division"* que engloba entre otros a la Fiscalía y al FBI, ha publicado una versión actualizada de las directrices para fiscales sobre ***«Evaluación de programas de corporate compliance»***.

Es una guía de obligado cumplimiento para todos los fiscales norteamericanos a la hora de evaluar si el programa de cumplimiento normativo, es suficiente o no.

Su propósito principal es garantizar que los fiscales "*evalúen la efectividad del cumplimiento de una manera rigurosa y transparente"*, conviene que esta nueva versión actualizada se tenga en cuenta por las empresas, especialmente por aquellos que hagan negocios con los EE. UU. o con empresas de los EE. UU. Por lo que recomendaríamos a quien haga negocios con EE.UU y a sus responsables de compliance, un análisis del documento. (VER documento Evaluación de Programas de Corporate Compliance).

Esta nueva Guía sobre la Evaluación del Corporate Compliance, aborda tres temas principales relacionados con la efectividad:

1.) ¿Está bien diseñado el programa de cumplimiento?
2.) ¿Se está aplicando el programa adecuadamente y de buena fe?
3.) ¿Funciona, en la práctica, el programa de cumplimiento?

El documento, plantea diferentes preguntas que se abordan para comprender cuándo un programa de compliance es simplemente un *«compliance paper»* o si realmente se está implantando de manera efectiva.

Destacaríamos preguntas que nos podemos hacer para analizar si la implantación del sistema de gestión de compliance la estamos realizando de manera adecuada y efectiva**:**

1) Evaluación de riesgos:

- ¿Qué metodología ha utilizado la empresa para identificar, analizar y abordar sus riesgos particulares, teniendo en cuenta el sector de la industria, la ubicación, el mercado, los socios comerciales y las relaciones con terceros?
- ¿Se revisan periódicamente los riesgos y se dedican recursos para monitorear las áreas de riesgo?

2) Políticas y procedimientos de compliance:

- ¿La administración y las unidades de negocio participaron en la creación de políticas o estas son, más bien *un, copia y pega* de materiales comunes del sector?
- ¿Qué esfuerzo está haciendo la compañía para vigilar la implantación de las políticas de compliance… si las hay?
- ¿Qué está haciendo la compañía para comunicarse y asegurar que las políticas y procedimientos estén disponibles para los empleados y no existan barreras lingüísticas? ¿Los empleados realmente entienden de qué tratan las políticas y los procedimientos de compliance?

3) Formación y comunicación:

- ¿La formación es realmente efectiva y se adapta en sus formas y contenidos a diferentes audiencias, y se ha diseñado en función de las áreas de control de riesgo y relevantes, o es más bien un repositorio *on-line* barato sobre reglas corporativas?
- ¿La formación está basada en ejemplos prácticos reales del sector, que pueden comprender fácilmente todos los empleados o se trata solo de jerga legal sobre delitos, sin importar si estos pueden ocurrir en la empresa o no?
- ¿Se está midiendo el impacto de la formación que se realiza? ¿Cómo? ¿Cuáles son los recursos realmente gastados en formación y comunicación en materia de compliance y cómo comparan frente a otros gastos de formación?

4) Informes e Investigación:

- ¿Existe un proceso de gestión de denuncias en el que puedan confiar verdaderamente todos los empleados, e incluso terceras partes, sin temor a represalias? ¿Es realmente seguro el canal de denuncias y es confidencial o es un número de teléfono del oficial de cumplimiento o un correo electrónico de un director de un área de la empresa?
- ¿Cómo garantiza la compañía que los empleados y terceros conozcan cuál es el canal de denuncias y cómo funciona?
- ¿Existe un proceso de investigación y los resultados de las investigaciones se informan adecuadamente al más alto nivel para que exista una adecuada rendición de cuentas?
- ¿La investigación y los informes son adecuadamente financiados con recursos de compliance que aseguren en todo caso que la información se recopila y analiza y permite revisar de modo efectivo las debilidades del Sistema de Cumplimiento?

5) Gestión de terceros:

- ¿Se implementan controles adecuados para garantizar que los terceros también cumplan o se trata solo de listas de verificación que con posterioridad nadie revisa?
- ¿El análisis de riesgos de terceros está realmente integrado en el sistema de compras o es solo una redacción legal que garantiza que las auditorías se pueden llevar a cabo, pero estas nunca se hacen?
- ¿La compañía rastrea *red flags* y se asegura de que los proveedores y terceros que no pasen la prueba de diligencia debida no sean contratados o vueltos a contratar posteriormente?

6) Liderazgo y compromiso:

- ¿Qué acciones específicas ha adoptado la alta dirección para demostrar liderazgo en el cumplimiento de la compañía? ¿Los gerentes han alentado o tolerado en algún momento los riesgos de cumplimiento para obtener mejores resultados comerciales?
- ¿Qué experiencia en materia de compliance existe a nivel Consejo de Administración? ¿Cuenta el Consejo de Administración con apoyo externo e independiente experto en compliance?
- ¿La alta dirección y el Consejo revisan el programa de cumplimiento de vez en cuando y solicitan evidencias o informes de su implantación efectiva?

7) Recursos:

- ¿Dónde se encuentra ubicada la función de compliance y a quién reporta? ¿Funciona con suficiente autonomía? ¿Reporta directamente al Consejo?
- ¿Cómo se compara la función de compliance en términos de *seniority*, nivel de compensación, líneas de *report*, estructura y recursos a otras funciones estratégicas de la empresa?
- ¿Cuál es el papel que desempeña la función de compliance en las decisiones estratégicas y operativas de la organización?
- ¿El personal dedicado a compliance tiene experiencia y cualificaciones adecuadas para sus roles y responsabilidades?
- ¿Hay suficiente personal para que los esfuerzos en materia de compliance se mantengan a lo largo del tiempo?
- ¿La empresa subcontrata algunas de las funciones de cumplimiento a expertos externos independientes?

8) Incentivos y desincentivos para el compliance:

- ¿Existen incentivos / recompensas por mejorar el sistema de compliance?
- ¿Las medidas disciplinarias se aplican de manera consistente o, a veces, las violaciones de normas se tratan como si “no pasara nada”?

9) Mejora continua y cultura de cumplimiento:

- Del mismo modo, bajo las normas ISO19600, la mejora continua es un hito relevante para el D.O.J ¿Con qué frecuencia se realiza una auditoría independiente interna o externa del sistema de gestión de compliance? ¿Los informes de auditoría son revisados por el Consejo? ¿La

empresa realiza alguna prueba periódica de sus controles de cumplimiento incluido su canal de denuncias?
- ¿Se revisan las políticas y la evaluación de riesgos de vez en cuando?
- ¿Cómo mide la compañía su cultura de cumplimiento? ¿Se pide opinión de la gerencia y de los empleados sobre el sistema de compliance?

10) Acciones correctivas:

- ¿Se dispone de mecanismos para la investigación independientes y de expertos cuando es necesario identificar vulnerabilidades del sistema o causas de incumplimientos legales?
- ¿Las investigaciones se basan en análisis independientes de hechos y resultados o evidencias?
- ¿La empresa analiza las causas de los incumplimientos y mejora los procesos para evitar que se repitan en el futuro?
- ¿Qué cambios se llevaron a cabo después de una conducta indebida y qué medidas disciplinarias se adoptaron en otros casos? ¿Qué medidas se han tomado con proveedores si estos participaron en la violación de normas?

Directiva Whistleblowing

El pasado 16 de abril, el Parlamento Europeo aprobó la Directiva del Parlamento Europeo y del Consejo relativa a la protección frente a represalias, de las personas que informen sobre **infracciones del Derecho de la Unión, conocida como *Directiva Whistleblowing*** con el objetivo de garantizar la protección de las personas que denuncien infracciones de empresas y organizaciones.

La Directiva europea ahora aprobada establece, la necesidad y obligación de implementar **cauces y procedimientos internos de denuncia y de tramitación de denuncias**. Esta obligación existirá tanto para las entidades públicas, como para las **empresas del sector privado que tengan más de 50 trabajadores**.

Se contemplan como denunciables, entre otras, infracciones relacionadas con:

a.) La contratación pública.

b.) Los servicios, productos financieros y blanqueo de capitales.

c.) La seguridad en los productos y en el transporte.

d.) La protección del medio ambiente, la salud y los consumidores

e.) La protección de la intimidad.

Para la efectiva implementación de los **canales de denuncia internas**, la Directiva prevé que estos sean negociados con la representación legal de los trabajadores cuando así lo establezca la normativa nacional, y establece de manera específica el alcance y contenido de los procedimientos y tramitación de denuncias.

Los canales de *denuncia* deben permitir la posibilidad de formular denuncias tanto por escrito como verbalmente, así como por vía telefónica u otros sistemas de mensajería de voz y, también de manera presencial si así lo solicita el denunciante.

Obligación de acusar recibo de la denuncia en un plazo máximo de 7 días.

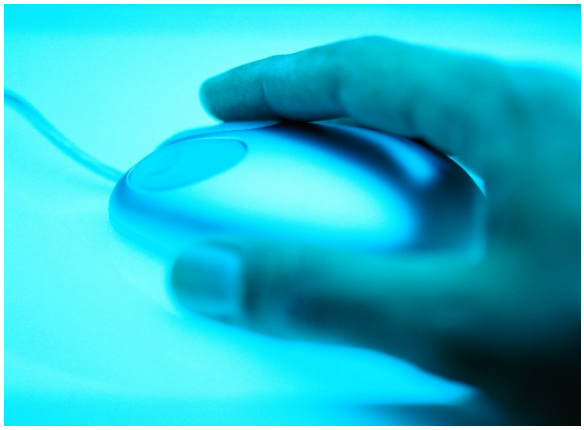
Designación de una persona o servicio imparcial que sea competente para tramitar las denuncias, que podrá ser la misma persona o servicio que recibe las denuncias y que mantendrá la comunicación con el denunciante y, en caso necesario, se encargará de solicitarle información adicional y de darle respuesta.

Tramitación diligente de todas las denuncias incluidas las anónimas.

Plazo máximo de 3 meses para dar respuesta al denunciante sobre la tramitación de la denuncia, a contar desde el acuse de recibo o, si no hubo acuse de recibo, desde el vencimiento del plazo de siete días desde la presentación de la denuncia.

España ya empezó a regular estos canales a través del artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que establece la posibilidad de que las empresas privadas puedan crear y mantener canales de denuncia a través de los cuales los trabajadores y terceros externos pudieran denunciar, incluso de manera anónima, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.

A pesar de que la Directiva tiene un plazo de transposición de dos años desde su publicación, los **planes de *compliance* ya recomiendan contar con estos canales**, Por lo que es recomendable que las empresas implanten y mantengan canales de denuncia con plenas garantías y que cumplan con las directrices establecidas por la nueva normativa europea.



Circular 7/2019 de la Fiscalía General del Estado. Delitos de odio

El **Boletín Oficial del Estado** publicó el pasado de 14 de mayo, la Circular 7/2019, de la **Fiscalía General del Estado**, sobre pautas para interpretar los delitos de odio tipificados en el artículo 510 del **Código Penal**.

La circular de la fiscalía tiene por objeto la fijación de pautas interpretativas de las distintas figuras delictivas englobadas en el nuevo artículo 510 del Código Penal tras la reforma llevada a cabo por la Ley Orgánica 1/2015, que entró en vigor el 1 de julio de 2015 y en concreto los delitos de odio. Se pretende ofrecer a los Fiscales unas pautas de actuación que sean lo suficientemente generales como para facilitar soluciones a los distintos problemas que estas figuras delictivas puedan plantear en la práctica.

Según detalla la circular, los delitos de odio afectan a un sujeto pasivo que presenta unas características propias que diferencian estas conductas de otras idénticas o similares. “Una agresión o una vejación se configuran como delito de odio si se dirigen contra un determinado grupo o individuo, precisamente por formar parte del mismo”, recoge el comunicado dirigido a los fiscales.

Ello enlaza con la motivación discriminatoria que, en realidad, es lo que define la esencia del delito de odio.

En ese sentido, la fiscalía determina que, a pesar de que el origen del delito está relacionado con la protección a los colectivos desfavorecidos, no tiene que analizarse desde un juicio de valor previo ni tampoco lo es el valor ético que pueda tener el sujeto pasivo.

Prevención Blanqueo de Capitales. Reglamento Delegado (UE) 2019/758

El Reglamento Delegado (UE) 2019/758 de la Comisión, de 31 de enero de 2019, por el que se completa la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo("Cuarta Directiva") en lo que respecta a las normas técnicas de regulación sobre las medidas mínimas y el tipo de medidas adicionales que han de adoptar las entidades de crédito y financieras para atenuar el riesgo de blanqueo de capitales y financiación del terrorismo en determinados terceros países quedó aprobado el pasado 31 de enero de 2019, si bien no entrará en vigor hasta el **3 de septiembre de 2019**. Conviene recordar que, en tanto que Reglamento Delegado, entrará en vigor **de forma directa** en la Unión Europea, sin necesidad de transposición o desarrollo en las normativas nacionales de los Estados miembro.
Este reglamento viene a dar respuesta a una cuestión no resuelta por la Cuarta Directiva: ¿cómo pueden gestionar el riesgo de blanqueo de capitales o financiación del terrorismo aquellas entidades de crédito o financieras que tengan sucursales o filiales con participación mayoritaria en países cuya legislación no permita la aplicación de las medidas a nivel de grupo previstas en la Cuarta Directiva? Esta situación puede producirse, por ejemplo, si el Derecho del tercer país en materia de protección de datos o de secreto bancario limita el acceso a información relativa a los clientes de la sucursal o filial.

La solución ofrecida por el reglamento pasa por la aplicación de políticas y procedimientos adicionales a las medidas ordinarias de prevención en los supuestos de riesgo específicos, primando la obtención del consentimiento de los clientes o titulares reales para salvar las restricciones normativas si la legislación del país de destino lo permite. Las medidas concretas se determinarán mediante un enfoque basado en el riesgo real, en consonancia con los principios de la Cuarta Directiva, y también teniendo en cuenta las directrices conjuntas de la Autoridad Bancaria Europea (ABE), la Autoridad Europea de Seguros y pensiones de Jubilación (AESPJ) y la Autoridad Europea de Valores y Mercados (AEVM).

Como obligación general, se exige **evaluar el riesgo del grupo en cada tercer país** y documentar la evaluación realizada en un registro que deberá mantenerse actualizado y a disposición de las autoridades competentes. Además, se deberá tener en cuenta el riesgo detectado en las procedimientos y políticas internas a nivel de grupo, obtener autorización de la alta dirección del grupo en relación con la mencionada evaluación del riesgo y su gestión en las políticas y procedimientos internos, así como de impartir formación específica al personal del país del que se trate para que pueda reconocer los indicadores de riesgo establecidos.
Los **supuestos de riesgo específicos** en los que hay que adoptar cautelas específicas son los siguientes, consistentes en que el Derecho del tercer país prohíba o restrinja:

- El acceso a la información del cliente y su titularidad real o la utilización de la misma para aplicar **medidas de diligencia debida** en una relación de negocios o transacción ocasional;
- El **intercambio o tratamiento de datos** de clientes dentro del grupo para la lucha contra el blanqueo y la financiación del terrorismo;
- El intercambio de información relativa a **transacciones sospechosas;**
- La **transferencia de información** relacionada con los clientes de la sucursal o filial a un Estado miembro a efectos de **supervisión** para la lucha contra el blanqueo y la financiación del terrorismo; o
- La aplicación de medidas de **conservación de documentos** equivalentes a las de la Cuarta Directiva.

Con la aprobación del reglamento, el círculo de la prevención se cierra un poco más, pues se completa a la Cuarta Directiva en lo que a la aplicación de medidas de diligencia a nivel de grupo se refiere (directiva que, no lo olvidemos, ha sido recientemente modificada por la Quinta Directiva con el fin de combatir más eficazmente la financiación del terrorismo). No obstante, los cambios legislativos en esta materia serán siempre continuos para combatir las nuevas operativas y riesgos que se vayan detectando.