

biblioteca
COMPLIANCE

WORLD
COMPLIANCE
ASSOCIATION



biblioteca
COMPLIANCE

02

ESTRUCTURA DE UN PROGRAMA DE COMPLIANCE

Marzo 2021

La **World Compliance Association (WCA)** es una asociación internacional sin ánimo de lucro formada por profesionales y organizaciones interesadas en el mundo del *compliance*. La asociación tiene, entre sus objetivos, la promoción, reconocimiento y evaluación de las actividades de cumplimiento en las organizaciones (con independencia de su forma jurídica), así como el desarrollo de herramientas y procesos para una correcta protección frente a determinados delitos/infracciones cometidas por sus empleados, colaboradores o cualquier otra persona relacionada con ella.

La **Biblioteca Compliance** es un proyecto que tiene por objetivo desarrollar contenidos bajo un enfoque práctico a través de documentos de buenas práctica sobre cinco ejes principales alrededor del *compliance*:



Todos los documentos están disponibles en
www.worldcomplianceassociation.com



ESTRUCTURA DE UN PROGRAMA DE COMPLIANCE

Marzo 2021

María Torres Robles
JEFA DE EQUIPO DE COMPLIANCE, MANAGEMENT SOLUTIONS
PROFESORA DEL MÁSTER DE DIRECCIÓN DE COMPLIANCE & PROTECCIÓN
DE DATOS, ESCUELA INTERNACIONAL DE POSGRADO

COAUTORES

Liliana Calderón, Danitza Echeandia, Paola Ximena Molina, Verónica Flores,
César José Fernández, Juan Rodrigo Durán, Teresa Serrano, Irene Macein,
Antonio Ávila, Jensen Samayoa Estrada, Manuel Letzkus Palavecino,
Carlos Andrés Abarca, Alfonso Vicens, María Torres



ESTRUCTURA
DE UN PROGRAMA
DE COMPLIANCE

A los coautores de este fascículo, que son seguidores de reglas por naturaleza, y que valoran la integridad, la justicia y el buen hacer.

A la WCA por la oportunidad de escribir, leer y compartir este fascículo, pues sólo a través de la compartición del conocimiento podremos contribuir al desarrollo de la comunidad de Compliance.

MARÍA TORRES ROBLES

Te invitamos a formar parte de la Red Mundial para el Cumplimiento.

La World Compliance Association (WCA) es una asociación internacional sin ánimo de lucro formada por profesionales y organizaciones interesadas en el mundo del compliance. La asociación tiene, entre sus objetivos, la promoción, reconocimiento y evaluación de las actividades de cumplimiento en las organizaciones (con independencia de su forma jurídica), así como el desarrollo de herramientas y procesos para una correcta protección frente a determinados delitos/infracciones cometidas por sus empleados, colaboradores o cualquier otra persona relacionada con ella.

La pertenencia a la WCA muestra por sí misma un interés y un compromiso real con el mundo del compliance. Está abierta a personas y organizaciones con interés en participar, impulsar y ampliar su conocimiento y red de trabajo y colaboración en el mundo del compliance corporativo. Además nuestro socios profesionales están cubiertos por un Seguro de Responsabilidad Civil en sus actividades como compliance officer, consultor y/o auditor de compliance.

01 CONTENIDOS EXCLUSIVOS
02 PARTICIPACIÓN PRIVILEGIADA
03 CRECIMIENTO PROFESIONAL
04 PRIVILEGIOS EXCLUSIVOS
Y VENTAJAS ADICIONALES PARA ASOCIADOS CORPORATIVOS

CUOTA DE ADHESIÓN

Categoría Socio	Profesional		Corporativo
	Fuera de España	España (seguro RC)	
Cuota Semestral	70 €	110 €	195 €
Cuota Anual	120 €	195 €	295 €



WCA Internacional
Paseo Castellana 79, 7ª Planta (Lexington Center)
28046 Madrid - España Tlf: +34 917 91 66 16
info@worldcomplianceassociation.com
www.worldcomplianceassociation.com



ÍNDICE

1. INTRODUCCIÓN SOBRE PROGRAMAS DE COMPLIANCE Y SUS ELEMENTOS ESENCIALES	08
2. LIDERAZGO Y CULTURA DE CUMPLIMIENTO	10
3. DESIGNACIÓN DE RECURSOS	12
4. EVALUACIÓN DE RIESGOS	14
5. IMPLANTACIÓN DE MECANISMOS DE CONTROL	20
6. FORMACIÓN, CONCIENCIACIÓN Y COMUNICACIÓN	23
7. MONITORIZACIÓN	28
8. SISTEMA DISCIPLINARIO	31
9. CONCLUSIÓN	35
10. BIBLIOGRAFÍA	36

1. INTRODUCCIÓN SOBRE PROGRAMAS DE COMPLIANCE Y SUS ELEMENTOS ESENCIALES

La expansión de las actividades económicas a nivel mundial, los avances científicos, así como la explosión de la tecnología, generan nuevos riesgos para la sociedad en su conjunto. Es por ello que, las empresas, promotoras en buena medida de dichos riesgos, deben implementar mecanismos idóneos para controlarlos y mitigarlos.

En esa línea, el programa de *compliance* o *compliance program*, es un conjunto de normas internas, procesos, procedimientos, buenas prácticas y políticas que las empresas implementan, en el ejercicio de su autorregulación, para identificar, evaluar y mitigar los riesgos legales asociados a las actividades económicas que realizan, contribuyendo así al desarrollo de una cultura de cumplimiento en el interior de las organizaciones.

El programa de *compliance* termina siendo un mecanismo que les otorga a las empresas, no solo la posibilidad de evitar el incumplimiento de la normativa de carácter obligatorio

y voluntario, sino que les permitirá generar un valor agregado en términos de sostenibilidad en el tiempo y mejora reputacional.

Si queremos hablar sobre el origen del *compliance*, debemos remontarnos a Estados Unidos en 1970. A mediados de la década de 1970, diversas empresas estadounidenses y trasnacionales del sector de la electricidad comenzaron a adoptar *compliance programs* con la finalidad de detectar y evitar infracciones legales, vinculadas con la libre competencia y antimonopolio (*antitrust*), así como actos de corrupción (*bribery laws*), los cuales cobraron mayor relevancia y enforcement a partir de la dación del FCPA (*Foreign Practices Corrupt Act*).

El *compliance* se fue expandiendo a otros países y, por ende, a otros sectores relevantes, como el caso del rubro bancario. En el año 2005, el Comité de Basilea emitió el documento denominado "El cumplimiento y la función de cumplimiento en

los bancos", en el que se mencionan diez principios esenciales para el desarrollo del *compliance* dentro del sistema bancario. De igual forma, la *International Organization of Securities Commissions* (IOSCO) también ha emitido publicaciones vinculadas al *compliance*.

De otro lado, en el año 1998, se emitió el *Australian Standard for Compliance Programs* -AS 3806-1998, primer intento específico para desarrollar de modo objetivo programas de cumplimiento dentro de una empresa, que tuvo gran aceptación tanto en Australia como en otras jurisdicciones. Por su parte, el Reino Unido reguló, a través de su parlamento, el *UK Bribery Act* (2010), normativa que, si bien dispuso sancionar de manera muy drástica los actos de soborno público y privado cometidos por las empresas, también estableció, como mecanismo de exclusión de responsabilidad penal, el haber implementado un efectivo programa de cumplimiento dentro de la organización. Esta norma, al igual que la FCPA, es aplicable -bajo el principio de extraterritorialidad- a las empresas que realicen sus actividades tanto fuera como dentro de Reino Unido (en el caso del FCPA, aplicable a empresas que operan dentro y fuera de los Estados Unidos).

Los mencionados instrumentos han servido de respaldo para la generación de las normas ISO 37001 de Sistemas de gestión antisoborno e ISO 19600 de Sistemas de gestión de *compliance* que, además de tener gran aceptación a nivel internacional, cuentan con una serie de principios comunes y se basan en una metodología denominada estructura de alto nivel (*high level structure*)¹. Por su parte, el estándar ISO 19600 nace como resultado de un proyecto de normalización que concluyó en el año 2014. Esencialmente, esta norma busca articular el *compliance* como un sistema de gestión dentro de los diversos ámbitos de la actividad empresarial, permitiendo una adecuada supervisión y coordinación de varias áreas a la vez (protección de datos, competencia, laboral, etc.), y convirtiéndose en un mega sistema de gestión².

La expansión y evolución del *compliance*, así como las distintas normativas que hemos mencionado, nos permiten identificar, a nivel macro y con vocación de generalidad, los componentes o elementos esenciales de un programa de *compliance*. A través del presente fascículo, delinearemos las características más relevantes de los siguientes elementos:

La expansión del *compliance* permite identificar los elementos esenciales de un programa de *compliance*: liderazgo, designación de recursos, evaluación de riesgos, mecanismos de control, formación, concienciación y comunicación, monitorización y sistema disciplinario.

El programa de *compliance* es un conjunto de normas internas, procesos, procedimientos, buenas prácticas y políticas que las empresas implementan para identificar, evaluar y mitigar los riesgos legales asociados a sus actividades.

- Liderazgo y cultura de cumplimiento
- Designación de recursos
- Evaluación de riesgos
- Implantación de mecanismos de control
- Formación, concienciación y comunicación
- Monitorización
- Sistema disciplinario

2. LIDERAZGO Y CULTURA DE CUMPLIMIENTO

En la actualidad, las organizaciones, alrededor del mundo, se enfrentan cada día a nuevas regulaciones y nuevos estándares surgidos tanto en el ámbito nacional como internacional, que les exigen activar mecanismos idóneos para dar cumplimiento integral a la regulación que les aplique, identificando los riesgos según el sector, mercado y geografía, entre otros, a través de sistemas de gestión del riesgo enmarcados dentro de programas de *compliance*.

Si bien deben preocuparse por cumplir sus metas, generar márgenes al negocio y utilidades a sus accionistas, también, y no menos importante, es su deber de garantizar que ese cumplimiento se realice bajo el estricto seguimiento a las normas que regulen su actividad económica, permeado por el componente ético que enmarque los valores de la

organización. Es, entonces, un pilar fundamental tanto para sus accionistas, como sus inversionistas, gobierno y la sociedad en general, evitando ser objeto de escándalos que afecten su reputación y, en muchos casos, que conlleven a responsabilidad penal de la persona jurídica en los países en los que esta figura ya se encuentra regulada.

De esta manera, para que un programa de *compliance* sea efectivo, se considera como elemento esencial que se estructure acompañado de los valores empresariales enmarcados en el código de ética y en el compromiso y liderazgo activo de la alta dirección, que es la llamada a crear, mantener y fortalecer una cultura de cumplimiento desde la integridad y coherencia en su discurso.

Con esto, se busca mantener, en

todas las etapas de estructura e implementación del programa de *compliance*, la promoción de la cultura de cumplimiento, acreditando ante entidades estatales y terceros que la organización actúa en todo momento con la debida diligencia esperada en el cumplimiento de sus disposiciones legales, no solo con el fin de evitar que sea incluida en investigaciones que conlleven sanciones económicas y/o responsabilidades penales, sino para proteger la reputación, valor que, una vez perdido, es difícil de recuperar.

Así, es claro que la creación y mantenimiento de la cultura de cumplimiento no puede quedar en cabeza exclusiva del líder de *compliance*. Es fundamental y esencial el compromiso, liderazgo y empoderamiento de la alta dirección, de quienes se espera una declaración constante y real frente al cumplimiento de las normas; declaración que no puede quedar en papel solo para dar cumplimiento a un requisito del programa.

De igual manera, la activación del discurso de la alta dirección en conexión con el código de ética para soportar una exitosa consecución de la estructuración del programa de *compliance*, tiene como fin construir

las bases de su efectividad y eficacia, enviando un mensaje de coherencia en los valores corporativos y la ejecución de programa a todos sus destinatarios.

Por tanto, la materialización de la cultura de cumplimiento a través de la puesta en marcha de los valores éticos en el discurso y actividades propias de la alta dirección es el inicio para construir y fortalecer constantemente el programa de *compliance* y la labor del oficial de cumplimiento, toda vez que el liderazgo en la materia será visible para el personal de la empresa, activando lo que se conoce como "*tone at the top*", de tal forma que la conducta y el cumplimiento de las normas al interior de la organización se realice, no por obligación, sino a favor de la integridad de la compañía y de cada una de las personas que hace parte de ella, beneficiando los buenos resultados.

Esto es fundamental, porque se puede construir un programa de *compliance* integral donde se pueda demostrar la debida diligencia, el cual refleje lo expresado en el código de ética y las políticas que lo desarrollan en las diversas materias a regular desde el aspecto legal, permeados de manera transversal a todas las áreas que conformen la compañía.

Así, es claro que la creación y mantenimiento de la cultura de cumplimiento no puede quedar en cabeza exclusiva del líder de *Compliance*. Es fundamental y esencial el compromiso, liderazgo y empoderamiento de la alta dirección, de quienes se espera una declaración constante y real frente al cumplimiento de las normas; declaración que no puede quedar en papel solo para dar cumplimiento a un requisito del programa.

Se espera que la empresa, a través del máximo órgano, sea lo suficientemente visionaria, teniendo, en la misma línea de prioridades, tanto su estrategia, como su programa de *compliance*, en el cual su liderazgo será la base para consolidar los valores éticos que las rigen en todas sus actuaciones por medio de la manifestación de la cultura de cumplimiento.

Lo anterior puede ser realizado siempre y cuando se mantenga el "*tone at the top*" en todas las actuaciones de la alta dirección, de tal manera que todas las decisiones se realicen bajo parámetros de integridad que protejan en todo momento la

reputación de la compañía, haciendo que su discurso sea coherente con lo dispuesto en la norma, el programa de *compliance* y el mismo código de ética.

El compaginar el programa de *compliance* con los estándares éticos definidos por la organización, siendo ambos, parte del discurso de la alta dirección, conducirá a que las decisiones del personal estén siempre orientadas a minimizar los riesgos, proteger la reputación, reconociendo en todo momento que estas deben respaldar los intereses de la compañía, y, por ende, sus resultados financieros y su competitividad sin violar normas éticas y legales.

3. DESIGNACIÓN DE RECURSOS

La Norma Internacional ISO 19600 de Sistemas de gestión de *compliance* establece en el punto 7.1, bajo el título "Recursos", que la organización debe determinar y proporcionar los recursos necesarios para el establecimiento, desarrollo, implementación, evaluación y mejora continua del sistema de gestión de *compliance*. Aunado a ello, impone como una de las responsabilidades de la alta dirección, el "*asignar recursos adecuados y apropiados para*

establecer, desarrollar, implementar, evaluar, mantener y mejorar el sistema de gestión de compliance y los resultados del desempeño".

Sin embargo, ¿qué significa recursos necesarios? Básicamente, es el dotar de recursos financieros y humanos suficientes a la función de *compliance* para el desarrollo de los contenidos esenciales del programa de cumplimiento³. Así, por recursos humanos se entiende la asignación de

personal idóneo y suficiente para el despliegue de la función de *compliance*. No se trata de una reasignación de funciones del personal, ni tampoco darles sobrecarga laboral; sino el poder contar con personal que se encargue de desarrollar la función de *compliance* de una manera eficiente y adecuada. Indudablemente, el recurso humano dependerá de las características de la organización (tamaño, riesgos, sector, entre otros). No se puede esperar que la función de *compliance* de una gran organización sea la misma que de una pequeña organización.

Por otro lado, en relación a los recursos financieros, se entiende el asignar un presupuesto propio a la función de *compliance*, el cual deberá ser destinado a la formación, comunicación, asesoramiento e implementación de aplicaciones informáticas propias que coadyuven al control de los procesos internos del negocio y registro de las decisiones, entre otras funciones⁴. En pocas palabras, es brindar a la función de *compliance* de recursos económicos suficientes que le permitan desarrollar su propósito sin ninguna contingencia y con total libertad.

Indudablemente, al ser la función de *compliance* un área que supervisará

el adecuado funcionamiento del programa de prevención, deberá contar con los recursos suficientes (sea personal adecuado o sea recursos económicos) para desarrollar dicha labor con total tranquilidad y sin depender de ningún área de la organización. Precisamente, por ello, reviste la necesidad de dotarla de un presupuesto propio y sobre el cual pueda decidir libremente. Claro está, ello no quita que la adecuada administración de dicho presupuesto sea auditada.

Sobre este aspecto, es oportuno precisar que el *U.S. Department of Justice Criminal Division*, en junio del 2020, elaboró un manual donde describe aquellos factores fundamentales que deben ser considerados al momento de evaluar la idoneidad y eficacia de los programas de *compliance*. Este manual es una guía para que, los Fiscales puedan determinar al interior de una investigación, si determinado programa de *compliance* es verdaderamente eficiente y eficaz; o en su defecto, si es de una "mera fachada" para que la organización pueda atenuar su responsabilidad.

Precisamente, dentro de estos criterios a considerar, se encuentra el verificar si el programa de *compliance* cuenta con los recursos adecuados

Es responsabilidad de la alta dirección el asignar recursos financieros y humanos adecuados y apropiados para establecer, desarrollar, implementar, evaluar, mantener y mejorar el sistema de gestión de *compliance* y los resultados del desempeño.

para que, pueda funcionar. En este caso, el *U.S. Department of Justice Criminal Division* especifica que se trataría de recursos humanos y recursos financieros.

Sin embargo, el análisis a realizar no se limita en la sola asignación de recursos (sea humanos o financieros) sino también, comprende aquellas solicitudes de recursos que fueron negadas a la función de *compliance*. Por lo que, en estos casos, se deberá

analizar los motivos por los cuales se dio esta negativa; lo cual, servirá como criterio para evaluar el programa de cumplimiento.

Entonces, por todo lo expuesto, se tiene que la asignación de recursos resulta ser una pieza fundamental para un programa de *compliance*; pues de ella dependerá, entre otros factores, si una organización lo está implementado de manera adecuada y eficiente.

4. EVALUACIÓN DE RIESGOS

Dentro del proceso de gestión del riesgo en la organización, es importante establecer el contexto o entorno, tanto interno como externo, en los que opera la empresa. El contexto interno y externo son el entorno de la organización en el que busca definir y lograr sus objetivos.

El **contexto interno** en una organización está condicionado por unos

factores que afectan a su desempeño y repercuten en esta con objeto de cumplir sus obligaciones, en este caso en materia de *compliance*. Para ello, debemos considerar factores relativos a los valores, la cultura en la organización, estructura, normas y objetivos los recursos, la propia gobernanza de la organización y las necesidades y/o expectativas de los *stakeholders* internos⁵:

CONTEXTO INTERNO: FACTORES A CONSIDERAR	
Cultura de la organización.	Recursos y conocimiento. Recursos humanos, recursos financieros, tecnológicos y redes. Conocimiento propiedad intelectual, propiedad industrial, procesos y sistemas.
Estructura organizativa y roles de cada función.	Gobernanza.
Normas y objetivos, normas, directrices y modelos adoptados por la organización, así como, la misión, la visión y los valores de esta.	Necesidades y/o expectativas de los stakeholders internos, relaciones entre ambos, percepciones y valores de estos.

CONTEXTO EXTERNO: FACTORES A TENER EN CONSIDERACIÓN	
Factores legales, reglamentarios, económicos, financieros sociales, culturales, políticos, ambientales, tecnológicos	
Niveles de corrupción	
Cultura: cultura de cumplimiento en el entorno geográfico y productivo	
Entorno regulatorio	Relaciones contractuales y compromisos.
Internalización	Necesidades y/o expectativas de los stakeholders externos

En cuanto al **contexto externo**, cada organización se relaciona y participa en un entorno externo determinado. Para ello, debemos considerar cuestiones legales, de mercado, económicas, culturales, sociales y tecnológicas⁵: *(tabla superior)*

Además de conocer el contexto, tanto interno como externo, se deben tener en cuenta las necesidades de las **partes interesadas o stakeholders**, entendidas como aquella persona, personas u organizaciones afectadas por las actividades y las decisiones de una organización, o que se pueda o puedan sentirse afectada/s por estas actividades o decisiones⁶⁷⁸.

La organización debe determinar los *stakeholders* que son relevantes para el programa de *compliance*. Cada organización tiene sus *stakeholders*, y podemos categorizarlos como *stakeholders* activos y pasivos⁵:

- **Stakeholders activos:** Aquellos

que trabajan o se relacionan directamente con la organización.

- **Stakeholders pasivos:** Aquellos que no tienen relación directa con la organización.

Debemos:

- Identificarlos. De forma individual o en conjunto, bien sea por sus características u obligaciones: **¿quién?**
- Comprender sus intereses, actitudes, expectativas y su influencia en la organización: **¿qué?**
- Analizar la relación con la organización: **¿cómo?**
- Planificar su control: **¿cuándo?**

SKATEHOLDERS	
Interno	Trabajadores
	Organizaciones sindicales
	Accionistas
	Titulares participaciones societarias
	Socios en los negocios

SKATEHOLDERS	
Externo	Cientes
	Proveedores
	Administraciones
	Organizaciones no Gubernamentales
	Organizaciones ciudadanas

Por su parte, la apreciación del riesgo comprende los elementos centrales del proceso de gestión del riesgo⁸. La finalidad de la apreciación del riesgo consiste en proporcionar evidencias basadas en la información y el análisis para la toma de decisiones informadas sobre cómo tratar los riesgos en el programa de *compliance*.

Uno de los errores más comunes en los programas de *compliance* es la determinación de forma genérica del contexto de la organización. Ahora bien, el éxito en la apreciación del riesgo depende del establecimiento de comunicaciones y sobre todo consultas con los *stakeholders*.

En este sentido, al comunicar y consultar a los *stakeholders*, no solo ya tienen conocimiento de que estamos implementando o modificando el programa de *compliance* de nuestra organización, sino que lo hacemos participe de este y además trasladamos una imagen más “real” de la organización en el proceso de gestión del riesgo.

Establecimiento contexto gestión del riesgo
Definir y establecer la metodología de apreciación del riesgo
Definir y establecer los criterios de riesgo
Establecer el método de evaluación del desempeño en la gestión del riesgo
Definir y establecer los criterios de riesgo

Criterios determinación criterios de riesgo
Los requisitos legales
El apetito por el riesgo de la organización
Los objetivos de proceso adoptados previo acuerdo

En cuanto a la **identificación de riesgos**, se puede definir como el proceso con el que se descubren, reconocen y se registran los riesgos. Para llevar a cabo esta tarea, contamos con distintos métodos como son, entre otros: la identificación de riesgos por áreas de trabajo, la identificación de riesgos por actividades y la identificación de riesgos por áreas geográficas. Veamos a continuación el siguiente ejemplo: [\(tabla superior pág.17\)](#)

A continuación, se muestra una tabla de riesgos identificados tomando como referencia los riesgos penales que pueden dar lugar a la responsabilidad penal de la persona jurídica en España, de acuerdo a la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal: [\(tabla inferior pág.17\)](#)

ÁREA	RIESGOS DE CONDUCTAS
RECURSOS HUMANOS	Contra los trabajadores. Odio. Contra la Seguridad Social. Contra la Hacienda Pública. Derechos fundamentales. Frustración en la ejecución.
COMERCIAL	Estafa. Corrupción. Contra la propiedad industrial. Contra la propiedad intelectual.
COMPRAS	Corrupción. Estafa. Blanqueo de Capitales.
COMPRAS	Corrupción. Estafa. Blanqueo de Capitales.

DELITO PENAL	DIRECCIÓN	GERENCIA	RRHH	FINANZAS	DESARROLLO	GESTOR PROYECTOS
Trata de Seres Humanos (177 bis 7 CP)	X	X	X		X	X
Prostitución, explotación de menores y corrupción (189 bis CP)	X	X	X		X	X
Descubrimiento y revelación de Secretos. Protección de Datos (197,197bis, 197ter CP)	X	X	X	X	X	X
Estafas y Defraudaciones. (251 CP)	X	X	X	X	X	X
Daños informáticos. (264 quater CP)	X	X				
Relativos a la Propiedad Intelectual, industrial, al mercado y a los consumidores. (270,271,273,274,275,276,283,285 286 CP)	X	X			X	X
Corrupción en los Negocios y financiación ilegal de los Partidos Políticos. (277,278,279,280,281 y 282 CP)	X	X		X	X	
Delitos Societarios. (290 a 297 CP)	X	X		X	X	
Receptación y Blanqueo de Capitales. Financiación al Terrorismo. (301 y 302 CP)	X	X		X	X	X
Contra la hacienda Pública y la Seguridad Social. (310 bis CP)	X	X	X	X	X	X
Contra los Derechos de los trabajadores. (318 CP)	X	X	X		X	X
Contra los Recursos naturales y el Medio Ambiente. (328 CP)	X	X			X	X
Contra el Ejercicio de los Derechos Fundamentales y Libertades Públicas. (510 bis CP)	X	X	X		X	X
Riesgos provocados por Explosivos y Otros agentes. (348.3 CP)	X	X			X	X
Cohecho. (427 bis CP)	X	X	X	X	X	X
Tráfico de Influencias. (430 CP)	X	X	X	X	X	X

En cuanto al **análisis de riesgo**, este implica desarrollar una comprensión del riesgo. El riesgo nace de las conductas, sin conductas no hay exposición al riesgo⁹.

El análisis del riesgo proporciona un elemento de entrada para la apreciación del riesgo: la toma de decisiones para un necesario tratamiento del riesgo y para el establecimiento de estrategias y de los

MÉTODO	CONCEPTO	NIVELES
CUALITATIVOS	Define las consecuencias, la probabilidad y el nivel de riesgo	Bajo Medio Alto
SEMICUANTITATIVOS	Utiliza escalas de valoraciones numéricas para las consecuencias y la probabilidad, y las combina para determinar el nivel de riesgo	Lineales Logarítmicas Otras fórmulas
CUANTITATIVOS	Estima valores realistas para las consecuencias y sus probabilidades, obteniendo valores de nivel del riesgo en unidades específicas	N/A

métodos de tratamiento de riesgos más adecuados. Por su parte, este análisis de riesgo también implica considerar las causas, las fuentes del riesgo, las consecuencias y la probabilidad de que las consecuencias puedan ocurrir. [\(tabla superior\)](#)

El **análisis de las consecuencias** de la materialización del riesgo determina la naturaleza y el tipo de impacto que se podría producir asumiendo que ha ocurrido un suceso, situación o circunstancia particular. Un suceso puede dar lugar a una gama de impactos de diversas magnitudes, y puede también llegar a afectar a una gama de diferentes objetos y *stakeholders*. Un ejemplo de tabla de consecuencias (C) sería el siguiente:

CONSECUENCIAS	CRITERIO	VALOR (C)
INSIGNIFICANTES	La repercusión de la materialización del riesgo (sanciones, reputación de la organización, etc) no representa ningún impacto significativo (sanciones, reputación para la organización, etc) para la organización	1
BAJAS	Si bien la repercusión de la materialización del riesgo del incumplimiento representa un perjuicio para la organización, el impacto (sanciones, reputación, etc) es asumible por esta.	2
MODERADAS	La repercusión de la materialización del incumplimiento representa un perjuicio que pone en riesgo la supervivencia y/o continuidad de la organización	3
INTOLERABLES	La repercusión de la materialización de incumplimiento impediría la continuidad de la organización.	4

Para llevar a cabo la estimación de la probabilidad, se emplean normalmente tres variables o factores que son:

- La utilización de datos históricos importantes para identificar sucesos o situaciones que han ocurrido en el pasado y que permiten extrapolar la probabilidad que vuelvan a ocurrir en el futuro.
- Los pronósticos de probabilidad, que utilizan técnicas de predicción tales como el análisis de árbol de fallos y análisis del árbol de sucesos.
- La opinión de un experto, que se puede utilizar en procesos

EXPOSICIÓN	DEFINICIÓN	VALOR (E)
BALADI	La actividad que puede dar lugar al incumplimiento en principio no tiene porqué realizarse en su funcionamiento habitual	1
BAJAS	La actividad que puede dar lugar al incumplimiento se realiza de forma ocasional (por ejemplo: alguna vez al año)	2
MEDIA	La actividad que puede dar lugar al incumplimiento se realiza de forma irregular (por ejemplo: alguna vez al trimestre)	3
ALTA	La actividad que puede dar lugar al incumplimiento se realiza de forma frecuente (por ejemplo: alguna vez al mes)	4

sistemáticos y estructurados para determinar la probabilidad.

Se expone a continuación un ejemplo de tabla de probabilidad (P):[\(tabla superior\)](#)

En la etapa de valoración y tratamiento de los riesgos, una vez identificado y analizado el riesgo, se debe proceder a su evaluación y posterior tratamiento. La **evaluación del riesgo** es la actuación que implica la comparación de niveles estimados de riesgo con los criterios obtenidos durante el análisis del riesgo definido, cuando se estableció el contexto, con objeto de determinar la importancia del nivel y tipo de riesgo.

Es importante tener en cuenta que,

TRIVIAL (T)	No se requiere acción específica
TOLERABLE (TO)	No se necesita mejorar los controles existentes salvo que el coste se reducido. Se requieren comprobaciones periódicas para asegurar que se mantiene la eficacia de las medidas de control
MODERADO (M)	Se deben hacer esfuerzos para reducir el riesgo, determinando los controles. Las medidas para reducir el riesgo deben implantarse en un periodo determinado
IMPORTANTE (I)	Se deben hacer esfuerzos para reducir el riesgo, determinando los controles. Deben implantarse en un tiempo inferior al de los riesgos moderados.
INTOLERABLE (IN)	Debería paralizarse la actuación que genera el factor del riesgo hasta el establecimiento de los controles.

en la evaluación del riesgo, se aplica el conocimiento del riesgo obtenido durante el análisis, para tomar decisiones para acciones futuras. Ejemplo de opciones en la evaluación del riesgo: [\(tabla inferior\)](#)

En cuanto al tratamiento del riesgo, es el proceso que consiste en seleccionar e implementar opciones para abordar el riesgo. Las opciones con que cuenta una organización, de acuerdo con la UNE-ISO 31000:2018 de Gestión del riesgo para realizar el tratamiento del riesgo, son las siguientes:

- Evitar el riesgo decidiendo no iniciar o no continuar con la actividad que genere el riesgo.

- Aceptar o aumentar el riesgo en aras de una nueva oportunidad
- Eliminar la fuente de riesgo.
- Modificar la probabilidad
- Modificar las consecuencias
- Compartir el riesgo
- Retener el riesgo en base a una decisión informada

El riesgo residual debe ser documentado y ser objeto de seguimiento y revisión. Además, cuando sea necesario, le será realizado un tratamiento adicional.

Los planes de tratamiento del riesgo consisten en especificar la manera en la que se implementarán las opciones elegidas para el tratamiento del riesgo. Estos se deberán integrar en los planes y procesos de gestión

de la organización, en consulta con los *stakeholders*. A continuación, se muestra la información mínima que deberá comprender el plan del tratamiento del riesgo:

LA INFORMACIÓN PROPORCIONADA POR EL PLAN DE TRATAMIENTO DEL RIESGO DEBERÁ INCLUIR AL MENOS:
La fundamentación de la selección de las opciones para el tratamiento
Las personas encargadas de rendir cuentas y aquellas responsables de la aprobación e implementación del plan de tratamiento del riesgo
Las acciones propuestas
Los recursos necesarios para su ejecución
Las medidas de desempeño
Las restricciones
Los informes y seguimientos requeridos
Los plazos previstos para la realización y la finalización de las acciones

El seguimiento y la revisión deberían tener lugar en todas las etapas del proceso, y deben incluir la planificación, recopilación y análisis de la información, registro de los resultados y proporcionar su retroalimentación.

5. IMPLANTACIÓN DE MECANISMOS DE CONTROL

Bajo un enfoque de procesos, la implantación de mecanismos de control corresponde a acciones que la organización desarrolla de manera

posterior a la evaluación de riesgos. Cabe preguntarse: ¿qué son los mecanismos de control?, o en forma aún más específica, ¿qué implica el

control como función dentro de una organización?

Una buena definición de control es "(proceso de) medición y corrección del desempeño para garantizar que los objetivos de la empresa y los planes diseñados para alcanzarlos se logren"¹⁰. Es importante considerar que tanto los objetivos como planes deben estar convenientemente respaldados como información documentada.

De la definición anterior, podemos deducir que el control, entendido como un sistema o proceso de la organización, deberá desarrollarse considerando tres instancias básicas:

1. Determinación de estándares.
2. Evaluar el grado de cumplimiento de los estándares.
3. Enmendar eventuales desviaciones de los estándares.

Resulta de capital importancia considerar que, la implantación de los mecanismos de control o, en otras palabras, el establecimiento del proceso de comprobación y regulación de nuestro sistema de *compliance*, debe tener un enfoque preventivo, ya que su propósito esencial es anticipar

eventuales daños o perjuicios a la organización relacionados con distintos incumplimientos de carácter legal, ético, financiero, medioambiental, laboral, etc. Asimismo, en aquellos casos en que no se logre prevenir, su objetivo es minimizar los efectos negativos de tales incumplimientos.

Además del carácter anticipatorio de los mecanismos de control, al momento de llevar a cabo su implantación, debemos considerar otros elementos tales como la complejidad, tamaño y cultura de la organización, la naturaleza y nivel del riesgo al que está asociado y los requisitos y expectativas de las partes interesadas.

Con todos los conceptos antes descritos como datos de entrada, y liderado por personal con autoridad suficiente dentro del sistema de *compliance*, el proceso de implantación de los mecanismos de control debe ser planificado y comunicado a todo el personal relevante de la organización, y quedar convenientemente formalizado como información documentada, a través de manuales, procedimientos, códigos de conducta, políticas, programas de capacitación, etc.

En todos los modelos de gestión estandarizados, se aplica el llamado

El control es el proceso de medición y corrección del desempeño para garantizar que los objetivos de la empresa y los planes diseñados para alcanzarlos se logren.

enfoque de procesos. En este punto, quiero establecer que, tanto el carácter preventivo como la naturaleza organizacional complejidad, tamaño y cultura de la organización, tipos de riesgos y requisitos de las partes interesadas, son *input* para el siguiente proceso, que es establecer los mecanismos de control:



Veamos lo anterior en casos hipotéticos:

Supongamos que la compañía (A) con una dotación total de 10 personas establece que existe un nivel de riesgo alto de fraude en su proceso de adquisiciones. Los mecanismos de control podrían estar dados por:

- Mayores exigencias al momento de la contratación del personal del área.
- Capacitación mensual impartida directamente por del dueño de la compañía.

Ahora, supongamos que la compañía (B) es una empresa con más de 500 trabajadores, con múltiples faenas y oficinas en distintas ciudades, en todas las cuales hay personal de adquisiciones. En esta organización, se ha identificado el mismo riesgo (fraude en el proceso de adquisiciones), pero su nivel de riesgo es considerado bajo.

Como consideración inicial, a pesar de contar la compañía (B) con un nivel menor de riesgo de fraude en el proceso de adquisiciones, la diferencia de tamaño entre ambas organizaciones hace que las medidas de control definidas para la compañía (A) no resulten suficientes. Por ello, algunos ejemplos de mecanismos de control para la compañía (B) podrían ser:

- Inclusión de un anexo en el contrato de todo el personal de adquisiciones explicitando los requisitos de *compliance* de la organización.

- Auditorías internas periódicas a todas las áreas de adquisiciones.
- Capacitación mensual impartida por la oficina de *compliance* corporativa.

Como corolario y acorde al conocido ciclo de mejora continua, este proceso debe continuar con la evaluación del grado de efectividad de los mecanismos de control. En efecto,

las medidas implementadas en una primera instancia podrán ser o no apropiadas y, por ello, resulta indispensable medir lo anterior, así como su capacidad para lograr el efecto deseado (reducir los riesgos de fraude en el ejemplo anterior). Esta evaluación determinará si debemos mantener, mejorar, aumentar o incluso eliminar determinados mecanismos de control.

6. FORMACIÓN, CONCIENCIACIÓN Y COMUNICACIÓN

La formación en el ámbito de *compliance* es un aspecto que, en determinados casos, está regulado, resulta obligado o altamente recomendable por el marco normativo vigente en cada momento. Este es el caso, por ejemplo, de la prevención del blanqueo de capitales y de la financiación del terrorismo, de las obligaciones de conocimiento continuado en determinados bloques de materias para el personal que asesora o informa en productos o servicios de inversión y respecto de la protección de datos de carácter personal. Con independencia del matiz de obligado o recomendable

por normativa, la formación ha de ser aprovechada como la herramienta adecuada para transmitir a la organización un mensaje claro de la relevancia del cumplimiento normativo (*compliance*) y del compromiso asumido a nivel corporativo en poner la ética en el centro de las decisiones empresariales.

Dicho mensaje, no solo ha de proceder del departamento de cumplimiento normativo, sino que debe, en primera instancia, estar apoyado por la alta dirección. Ello es así en la medida en la que el tono de *compliance*

El proceso de implantación de los mecanismos de control debe ser planificado y comunicado a todo el personal relevante de la organización y quedar convenientemente formalizado y documentado.

debe estar "arriba" para poder transmitirse en cascada al resto de la compañía. *"Vale más un ejército de ovejas dirigidas por un león, que un ejército de leones dirigido por una oveja"* (frase atribuida a Vasco de Gama). En este sentido, el *"tone at the top"* por parte del máximo o los máximos responsables de la gobernanza de una organización (los líderes de la misma) resulta clave para el éxito de una cultura de cumplimiento. En definitiva, resulta fundamental obtener el compromiso de los consejeros y de la alta dirección.

Tomando como referencia la UNE-ISO 19600 de Sistemas de Gestión de *Compliance*, de abril de 2015, en todo programa de formación de *compliance* deberían tenerse en cuenta los siguientes condicionantes¹¹:

1. Atender a las obligaciones y riesgos de *compliance* a los que los empleados están expuestos según los roles y nivel de responsabilidad de cada uno.
2. Responder a los resultados de la evaluación de desempeño de los empleados en la medida en la que, en aquella, se hayan identificado carencias de conocimientos y competencias de los mismos.

3. Situar el punto de arranque en el inicio de la relación del empleado con la organización, para posteriormente realizar cursos de forma continuada.
4. Considerar el programa de formación de la organización como punto de referencia con el que estar alineado.
5. Ser relevantes para el trabajo diario de los empleados y de aplicación en el sector de actividad correspondiente. El objetivo reside en formar personas que sepan que, llevando a cabo su trabajo de modo correcto, cumplen con la normativa. En este sentido, resulta relevante recordar que, en España, la Ley 30/2015, de 9 de septiembre, por la que se regula el sistema de formación profesional para el empleo en el ámbito laboral, establece que la formación programada para empresas ha de guardar correspondencia con la actividad empresarial y atender a las necesidades de las empresas y de sus trabajadores. De ahí, que los itinerarios formativos de cada empresa hayan de estar precedidos de un análisis que detecte las necesidades reales.

6. Ser flexible para adaptarse, según las necesidades de la compañía, a los distintos formatos de *e-learning* y presencial.
7. Ser susceptibles de evaluación, de modo que los miembros de la organización puedan realizar un test o ejercicio de evaluación al final, idealmente, de cada actividad formativa.
8. Ser objeto de actualización y revisión periódica, a fin de tener en cuenta los cambios en la organización tanto de estrategia, como de desarrollo de nuevos productos o servicios, o de procedimientos, etc.
9. Ser objeto de registro y conservación. En particular, las acciones formativas y sus correspondientes evaluaciones.
10. Recoger la normativa general y sectorial más relevante que los miembros de la organización deben conocer, con un enfoque aplicado a la compañía y al sector en el que opera.

En una estrecha relación con el programa de formación de *compliance*, se encuentra la función de asesoramiento, que reside en el ADN de

esta función, y que resulta parte de la responsabilidad del *compliance officer*. En particular, esta función de asesoramiento afecta a la alta dirección, ya citada antes, así como a las distintas líneas de negocio y de soporte de la organización respecto de las leyes, reglas y estándares de cumplimiento.

Por tanto, el responsable de *compliance*, así como todo miembro de dicho equipo, son correa de transmisión del marco regulatorio que aplica a la compañía por ser una sociedad mercantil y por operar en un determinado sector de la actividad económica. En este sentido, existen ejemplos como los planes de prevención de riesgos laborales y los modelos de organización y gestión de los riesgos penales, cuyo conocimiento es imprescindible dentro de la compañía, independientemente del sector en que se opere.

En el primero de los ejemplos, cabe destacar que, en España, la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales, que crea un nuevo ámbito normativo en materia de protección de la seguridad y salud de los trabajadores, consagrando la obligación de todo empresario de velar por el cumplimiento de dicho marco.

Se hace imprescindible, no solo dar a conocer las políticas, procedimientos y códigos de conducta, sino también dejar constancia de la comprensión de los mismos y de su aceptación por los miembros de la organización.

Para que la formación y la concienciación puedan ser correctamente articuladas por el *compliance officer*, la comunicación (tanto la interna como la externa) resulta un factor clave.

En el segundo ejemplo, la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal español (en sus conocidas reformas de los años 2010 y 2015) establece que *"los modelos de organización y gestión que incluyen medidas de vigilancia y control son idóneos para prevenir delitos o reducir de forma significativa el riesgo de su comisión"*. Se hace imprescindible, por tanto, no solo dar a conocer las políticas, procedimientos y códigos de conducta a través de los que se articula todo lo anterior, sino también dejar constancia de la comprensión de los mismos y de su aceptación, dado que la desviación del marco aplicable supone que se desencadenen las medidas arbitradas por el sistema disciplinario correspondiente.

Por tanto, los modelos de gestión que resulten de aplicación dentro de la compañía deben establecer los protocolos y procedimientos que aterricen los procesos de formación de voluntad de la persona jurídica. Lo anterior pasa por documentar toda política que se implante dentro de la empresa y por informar y formar a todos los miembros de la organización, en la medida en la que adicionalmente se contará con un sistema disciplinario que sancione los incumplimientos de los protocolos acordados.

Puede afirmarse, por tanto, que la formación y la concienciación (*"awareness"*) o asesoramiento son elementos clave en la implantación de la cultura de *compliance* y están en el centro de la función de *compliance*. Para que ambos aspectos puedan ser correctamente articulados por el responsable de *compliance* o cualquier *compliance officer* del departamento, la comunicación resulta un factor clave. Este nuevo concepto nos lleva a distinguir dos tipos que pueden definirse del modo que sigue¹²:

- **Comunicación interna:** conjunto de actividades efectuadas por la organización para la creación y mantenimiento de buenas relaciones con y entre sus miembros, a través del uso de diferentes medios de comunicación. El objetivo reside en mantenerse informados, integrados y motivados para contribuir al logro de los objetivos organizacionales.
- **Comunicación externa:** conjunto de mensajes emitidos por la organización hacia sus diferentes públicos externos, *stakeholders* o grupos de interés, dirigidos a mantener o mejorar sus relaciones con ellos, a proyectar una imagen favorable o a promover sus productos o servicios. Este

tipo de comunicación incluye al área de relaciones públicas y de publicidad.

Dentro de la comunicación interna, cabe establecer una subclasificación que distingue entre vertical hacia abajo (flujo de información desde la alta dirección a todos los empleados de la entidad, teniendo en cuenta la estructura formal de cada empresa, incluyendo transmisión de objetivos de trabajo, procedimientos, instrucciones, evaluación, etc.) o hacia arriba (flujo de información que va desde áreas con menor autoridad, a aquellas que tienen mayor autoridad o poder de decisión a fin de informar sobre resultados de trabajo, quejas, consultas, incidencias, etcétera, si bien también debería utilizarse como herramienta de mejora continua) y comunicación horizontal o comunicación entre personas del mismo nivel jerárquico o similar (flujos de información entre dos empleados, dos responsables, dos departamentos, etcétera, para coordinarse mejor entre los participantes de un proceso).

En el ámbito del *compliance*, es importante transmitir cualquier materia, si bien cabe destacar las siguientes materias que pueden ser susceptibles de comunicarse al resto de la entidad: materiales relativos

al funcionamiento del departamento o área de cumplimiento normativo (por ejemplo, política de la función de cumplimiento); políticas, protocolos y procedimientos sobre operaciones o actividades concretas afectas por la normativa externa y/o interna, en los que se diga las obligaciones de los empleados; listados de operativas sospechosas o de casos prácticos sobre buenas prácticas de cumplimiento, y ejemplos de incumplimientos o qué no se debe hacer.

Antes de llevar a cabo una comunicación, han de seguirse unos pasos previos. Por ejemplo, antes de comunicar una política, esta ha debido ser aprobada por el consejo de administración y tratada con la alta dirección para que se analicen los impactos organizativos. En consecuencia, en la elaboración de la política, es relevante la comunicación horizontal entre departamentos para poder ajustarse lo mejor posible a sus actividades. En este sentido, se trabaja de manera puntual con el departamento impactado o mediante el uso de equipos multidisciplinares, que ayudan a tener una visión más amplia del problema. Una vez aprobada y tratada, se debe comunicar al resto de empleados toda la información y los datos de fechas y medios en la implantación.

Se destaca entre las materias susceptibles de ser comunicadas: materiales relativos al funcionamiento del departamento de cumplimiento, las políticas, protocolos y procedimientos, y el listado de operativas sospechosas o casos prácticos sobre buenas prácticas de cumplimiento.

Siguiendo en esta misma línea, las directrices de la ISO 19600 de Sistemas de gestión de *compliance* finalizan indicando: *"La comunicación debería indicar claramente [...] cuáles son los incumplimientos que se espera que sean escalados, en qué circunstancias y a quién"*. Por tanto, también es importante que el receptor de esta comunicación sea conocedor, en caso de realizar un incumplimiento o ser conocedor del mismo por parte de un tercero, de cómo debe escalar dicha información. En este aspecto, esto no es algo que tenga que ir explícito en una comunicación de una operativa concreta. Más bien, está información debe ser conocida por toda la entidad dentro del marco de la función de cumplimiento normativo y las actuaciones básicas que deben realizar.

Entre estas, deben estar la de cumplir con todas las normas externas e internas, informarse y poner todos los medios para actualizarse en este sentido, e informar o denunciar en caso de ser conocedor de una actuación que incumple la normativa.

Las directrices de gestión de *compliance* de la ISO 19600 de Sistemas de gestión de *compliance* también establecen para **comunicaciones externas**: *"Se debería adoptar un enfoque práctico de comunicación externa, dirigido a todas las partes interesadas, de acuerdo con la política de la organización. Las partes interesadas pueden incluir, pero no están limitadas a, organismos reguladores, clientes, contratistas, proveedores, inversores, servicios de emergencia, ONGs y vecinos"*.

7. MONITORIZACIÓN

Monitorizar los sistemas de gestión de *compliance* es tan importante como un buen diseño y su implantación. Es por ello que, uno de los elementos clave que determinan la eficacia de un programa o sistema de *compliance*, es la monitorización del mismo, así como su mejora continua.

William Thomson Kelvin (Lord Kelvin), físico y matemático británico (1824

–1907) dijo que *"Lo que no se mide, no se puede mejorar. Lo que no se mejora, se degrada siempre"*. Por tanto, debemos someter a nuestros sistemas o programas de *compliance* a una continua monitorización y mejora continua. La monitorización consiste en:

1. Recoger y analizar la información y documentación del sistema.

2. Analizar los indicadores y verificar el cumplimiento de los procedimientos de control.
3. Elaborar los informes de cumplimiento junto con las recomendaciones de mejora y planes de acción.

Una de las partes esenciales de la monitorización es la auditoría, por medio de la cual se puede verificar tanto el diseño como la efectividad de los procedimientos de control establecidos. Al igual que el resto de la información, ha de quedar adecuadamente registrada.

La implementación de programas de *compliance* conlleva una serie de actividades, acciones y controles propios de la implementación de cualquier proyecto que tenga una finalidad y un objetivo propio. Es por eso que, de esta implementación, se deriva la máxima de las 5C en el área de *compliance*, y estas son:

- Cumplir
- Control
- Capacitación
- Constancia
- Comunicación

El control es una de las herramientas del *compliance* donde la efectividad

puede ser medida, de ahí que los informes que se generan son un pilar fundamental dentro de la actividad propia que genera un oficial de cumplimiento.

Los informes que se consideran como parte de la labor del oficial de cumplimiento son:

- Reportes operativos.
- Memorias anuales.
- Comunicaciones urgentes.
- Reportes forenses.

Los informes de cumplimiento deben de estar alineados a la política de *compliance*, en la que existen informes periódicos establecidos. Sin embargo, cuando existen materias significativas, se debe de informar de manera inmediata.

Estos informes o reportes permitirán conocer siempre la función y evolución que el programa de cumplimiento está teniendo, y establecer los momentos de la auditoría que todo programa debe tener, así como la eficiencia a través del tiempo. De ahí que, una de las frases tantas veces repetidas en *compliance*, radica en "es mejor prevenir, que combatir".

La mejora de los programas de *compliance* tiene aplicación real, práctica

La monitorización consiste en recoger y analizar la información y documentación del sistema; analizar los indicadores y verificar el cumplimiento de los procedimientos de control; y elaborar informes de cumplimiento con las recomendaciones de mejora y planes de acción.

e intensiva si existe una cultura de todos los integrantes de la organización, que se oriente a la resolución de problemas y aplicación de un sistema de gestión *lean manufacturing*. Se trata de una metodología de gestión que consiste en la aplicación de diferentes herramientas para el mejoramiento continuo, bajo la filosofía de calidad perfecta a la primera vez, es decir, cero defectos y detección, y solución de los problemas desde su origen, evaluando los resultados de manera constante, tomando decisiones para corregir y controlar los procesos, mejorando sustancialmente la comunicación e incidiendo con efectividad en el control del *compliance*.

Todo sistema de cumplimiento debe incorporar indicadores QCD (calidad, costo, entrega) extendidas a otras variables de interés. En este caso, el programa de *compliance* empresarial/ organizacional incorpora indicadores clave de rendimiento (KPI), referido al *compliance* propiamente como tal (QCDC). Hablamos de métricas que miden la capacidad del programa para mantener una organización en línea con las políticas, tanto internas como externas, así como con las regulaciones gubernamentales.

Los indicadores de gestión de

cumplimiento ayudan a la alta dirección a tomar decisiones oportunas en base a datos objetivos y valiosos para articular la mejora continua del programa, según los KPI definidos y adoptados (por ejemplo, el número de problemas de cumplimiento identificados, tiempo de ciclo de investigación de cumplimiento, porcentaje de auditorías internas completadas a tiempo, etc.). *Lean manufacturing* incluye una metodología de solución de problemas, una de prevención y una de mejora, las cuales utilizan herramientas y técnicas para diferentes necesidades y propósitos¹³. Uno de estos es el mantenimiento y control del *compliance*.

Algunas de las herramientas más utilizadas y recomendadas son las siguientes:

Gemba y Gerencia diaria	Benchmarking
Estandarización	Los 5 ¿Por qué?
Kaisen	Hoshin Kanri
Jidoka	Seis Sigma
Poka Yoke	A3

Respecto a herramientas de gestión y mejora de la calidad, las herramientas de gestión y administración propuestas por la Asociación Japonesa de Científicos e Ingenieros (JUSE) son las siguientes:

Diagrama de Afinidad	Matriz Priorización
Diagrama de Relaciones	Diagrama de Proceso de Decisión
Diagrama de árbol	Diagrama de Flechas
Diagrama de Matriz	

8. SISTEMA DISCIPLINARIO

Uno de los puntos más controvertidos y que generan más opiniones encontradas relacionados con la estructura de un programa de *compliance* es el llamado sistema disciplinario.

De manera generalizada, la mayoría de las legislaciones de los distintos ordenamientos jurídicos consideran que, para que la persona jurídica pueda quedar exenta de responsabilidad, una de las condiciones que deben cumplir los programas de *compliance* es establecer un sistema disciplinario.

Concretamente, en el ordenamiento jurídico español, dicha condición viene recogida en su vigente Código Penal, concretamente en su artículo 31 bis. 5. 5º, que literalmente dispone que:

5. Los modelos de organización y gestión a que se refieren la condición 1.ª del apartado 2 y el apartado anterior deberán cumplir los siguientes requisitos:

5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

Consecuencia de este deber disciplinario del programa de *compliance*, las organizaciones podrán aplicar sanciones y medidas correctoras a los incumplimientos de su personal en esta materia. Las conductas sancionables deberán ser graduadas y, por tanto, tipificadas en función de su gravedad atendiendo a un esquema perfectamente delimitado.

En el marco del programa de *compliance*, serán consideradas faltas del personal aquellas conductas que contravengan el programa y supongan un incumplimiento o la materialización de un riesgo cuya responsabilidad sea susceptible de ser derivada a la organización.

Si analizamos el entorno internacional y las más destacadas normas que versan sobre los distintos sistemas

Los indicadores de gestión de cumplimiento (KPI) ayudan a la alta dirección a tomar decisiones oportunas en base a datos objetivos y valiosos para articular la mejora continua del programa

Serán consideradas faltas del personal aquellas conductas que contravengan el programa de *compliance* y supongan un incumplimiento o la materialización de un riesgo.

disciplinarios, podemos encontrar ejemplos que nos muestran la importancia de establecer un sistema disciplinario dentro de los programas de *compliance*. Algunos de los ejemplos son los siguientes:

- UNE 19601 de Sistemas de Gestión de *Compliance* penal, cuando en su apartado 7.3.2.1 "Diligencia debida común a todos los miembros de la organización", señala que *"se deben establecer, implementar y mantener actualizados procedimientos tendentes a que: d) Se adopten acciones disciplinarias proporcionales contra aquellos miembros de la organización que incumplan los requisitos derivados de la política de compliance penal o del resto del sistema de gestión de compliance penal"*.
- *U.S. Department of Justice*, al informar de que *"otro sello distintivo de la implementación efectiva de un Programa de Compliance es el establecimiento de incentivos para el cumplimiento y desincentivos para el incumplimiento"*, en la actualización de su *"Evaluation of Corporate Compliance Programs"* de junio de 2020.
- La chilena Ley 20.393, de 25 de noviembre de 2009, que

establece la responsabilidad penal de las personas jurídicas en los delitos que indica. En su artículo 4, indica que, *"el encargado de prevención, en conjunto con la administración de la persona jurídica, deberá establecer un sistema de prevención de delitos para la persona jurídica, que deberá contemplar a lo menos lo siguiente: d) La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades pecuniarias en contra de las personas que incumplan el sistema de prevención de delitos"*.

- En derecho comparado, existen diversidad de sistemas disciplinarios y de estructuras, más o menos comunes, generalmente aceptadas por los ordenamientos jurídicos internacionales. Podemos plantear un ejemplo ilustrativo con la siguiente estructura:

CALIFICACIÓN DE LAS INFRACCIONES:

- **Infracciones leves.** La falta de asistencia esporádica, puntual e injustificada a las formaciones programadas para personal en materia de prevención de delitos.

- **Infracciones graves.** El incumplimiento de las políticas corporativas aprobadas por la organización en el programa de *compliance*.
- **Infracciones muy graves.** La comisión directa o colaboración, incluso en grado de tentativa, de cualquier conducta delictiva regulada en el programa de *compliance*.

RÉGIMEN DE SANCIONES:

- **Faltas leves.** Amonestación verbal. Si fueran reiteradas, amonestación por escrito.
- **Faltas graves.** Suspensión de empleo y sueldo hasta X días cuando exista reincidencia.
- **Faltas muy graves.** Despido disciplinario.

RÉGIMEN DE NOTIFICACIONES:

Cuando la organización tenga conocimiento de la comisión de una infracción regulada en el programa de *compliance*, se actuará de la siguiente forma:

- Notificación personal y por escrito.
- Acuse de recibo de la notificación.
- Información detallada de los hechos constitutivos de la infracción y propuesta de eventual subsanación.
- Propuesta de sanción.
- Pliego de descargos. La persona dispondrá de tres días para alegar lo que estime conveniente.
- Silencio. La ausencia del escrito de descargo se entenderá como voluntad de permanecer en silencio.
- Instrucción del pliego de descargos.
- Resolución y comunicación.

Otra de las partes esenciales en la estructura de un programa de *compliance* y que, además, puede considerarse un instrumento con estrecha vinculación al sistema disciplinario, es el canal de denuncias.

El canal de denuncias supone la vía u oportunidad para que el personal de la organización pueda participar

Existen diversidad de sistemas disciplinarios y de estructuras. Un ejemplo sería:
 1) Calificación de las infracciones (leves, graves y muy graves),
 2) Régimen de sanciones (leves, graves y muy graves),
 3) Régimen de notificaciones.

Por medio del canal de denuncias, la organización recibe y gestiona la información sobre conductas contrarias al código ético, a las políticas corporativas, o a la normativa que es de aplicación a la organización.

en la prevención de los riesgos. Es el instrumento por medio del cual la organización recibe y gestiona la información aportada por el personal sobre conductas contrarias al código ético, a las políticas corporativas aprobadas por la organización, o a la normativa que es de aplicación a la organización.

Las formas que puede adoptar un canal de denuncias pueden ser varias, por ejemplo:

- Dirección de correo electrónica.
- Dirección postal física.
- Buzón físico en el interior de las instalaciones de la organización.

Como conclusión, podemos afirmar que la facultad disciplinaria del administrador de la organización deriva de sus poderes de control y vigilancia y que, con ocasión de los programas

de *compliance*, se convierten en deberes en lo que respecta al cumplimiento de aquellas obligaciones de prevención de riesgos establecidas en las distintas normativas sobre la materia.

Establecer un sistema disciplinario no es tarea fácil para la persona jurídica, pues la facultad disciplinaria no es ilimitada, al contrario, está perfectamente definida por la legislación vigente en cada país (en España, por ejemplo, concretamente en la Constitución Española, en el Estatuto de los Trabajadores y los convenios colectivos de aplicación), por lo que cualquier acción tendente a sancionar conductas del personal de la organización contrarias al código ético y de conducta deberá guardar una perfecta consonancia con la legislación antes referida pues, de lo contrario, el aplicar sanciones no contempladas o desproporcionadas podría constituir, en sí mismo, un ilícito.

9. CONCLUSIÓN

Cada vez son más los ordenamientos jurídicos que establecen como requisito a las organizaciones la implantación de un programa de *compliance*, de cara a evitar sanciones o reducir el alcance de las mismas ante un

hipotético incumplimiento, así como para promover la existencia de una cultura de integridad, de ética y de cumplimiento normativo dentro de las mismas.

Lo fundamental a la hora de implantar y mantener un programa de *compliance* es que el mismo sea eficaz. Un programa de *compliance* eficaz y efectivo se reconoce en la activación real de la cultura de cumplimiento al interior de las empresas, a través de la puesta en marcha de las normas internas, políticas, procesos, procedimientos y buenas prácticas.

En este sentido, y para que el programa de *compliance* sea eficaz, no solo deben coexistir los elementos expuestos en este fascículo, sino que, además, el mismo debe estar adaptado a las características de cada organización. Es decir, las organizaciones deben implantar programas de *compliance* hechos a su

medida, ad hoc, de manera que no se trate de "*paper compliance*" (adoptar programas de *compliance* copiados de otras organizaciones). Por ello, las organizaciones se enfrentan al desafío de diseñar, construir y mantener programas sólidos de cumplimiento adecuados para ellas mismas.

Estos programas deben fomentar una cultura de cumplimiento que comience en la alta dirección y que pueda calar en todos los miembros de la organización. Un programa de *compliance* robusto y eficaz, liderado por un equipo de cumplimiento con recursos financieros y humanos y una alta dirección comprometida "*tone at the top*", es un *must* para la rentabilidad y sostenibilidad de la empresa.

10. BIBLIOGRAFÍA

1. Casanovas, A. (2013) *Legal Compliance. Principios de cumplimiento generalmente aceptados*. Madrid: Difusión Jurídica
2. Argüello, S. (2018) *El responsable de cumplimiento debe rendir cuentas sobre el adecuado destino de recursos asignados* [en línea] disponible en <<https://www.eleconomista.es/ecoley/buen-gobierno/noticias/9033757/03/18/El-responsable-de-cumplimiento-debe-rendir-cuentas-sobre-el-adecuado-destino-de-recursos-asignados.html>> [consulta diciembre 2020]
3. Rodríguez, C. (2016) *El modelo de Compliance ideal en la empresa: asignación de presupuesto y adaptación a las pymes y micro-pymes* [en línea] disponible en <<http://protocolopreencionpenal.com/asignacion-presupuesto/>> [consulta diciembre 2020]
4. Casanovas, A. (2017) *Métrica comparativa en los recursos de Compliance* [en línea] disponible en <<https://www.tendencias.kpmg.es/2017/04/metrica-comparativa-en-los-recursos-de-compliance/>> [consulta diciembre 2020]
5. UNE (2018) UNE - ISO 31000:2018 *Gestión del riesgo. Directrices*
6. UNE (2011) UNE-EN 31010: 2011 *Gestión del riesgo. Técnicas de apreciación del riesgo*
7. UNE (2017) UNE 19601: 2017 *Sistemas de gestión de compliance penal. Requisitos con orientación para su uso*.
8. Bajo, J.C. (2017) *Manual para la evaluación de riesgos Compliance*. Madrid: Ampell consultores
9. Kuntz, H., Weihrich, H. y Cannice, M. (2012) *Administración general Una Perspectiva global y empresarial*. Ciudad de México: Mc Graw Hill
10. UNE (2015) UNE - ISO 19600:2015 *Sistemas de Gestión de Compliance. Directrices*
11. Andrade, H. (2015) *Comunicación organizacional interna: proceso, disciplina y técnica*. Madrid: Netbiblo
12. Socconini, L. V. (2019) *Lean Company: más allá de la manufactura*. Barelona: Marge Books
13. López Lemos, P. (2016) *Herramientas para la mejora de la Calidad: Métodos para la Mejora Continua y la solución de problemas*. Madrid: FC Editorial

“Nuestra estrategia, el Desarrollo Competitivo.”

El entorno legislativo en el que la empresa desarrolla sus actividades es cada vez más complejo. El nivel de exigencia de las autoridades y organismos regulatorios es cada vez mayor, y el impacto de la legislación es más intenso que nunca.

Por ello, y por los recientes escándalos societarios y el innegable incremento de la sensibilidad social respecto de la ética de los negocios, **un mayor número de organizaciones públicas y privadas integran estándares éticos y legales como protocolos de buen gobierno de obligado cumplimiento.**

Curso de Experto Universitario Compliance Officer

Modalidad > 450 horas, e-Learning

Titulación > Experto Universitario Compliance Officer emitido por la Universidad de San Jorge. Compliance Officer Certificado por la World Compliance Association. Experto Compliance Officer emitido por Intedya

Curso Universitario de Protección de Datos Data Protection Officer

Modalidad > 200 horas, e-Learning

Titulación > Curso Universitario de Protección de Datos – Data Protection Officer.

Data Protection Officer & Compliance Officer

Modalidad > 650 horas, e-Learning

Titulación > Experto Universitario Compliance Officer + Compliance Officer Certificado por la World Compliance Association. Curso Universitario de Protección de Datos – Data Protection Officer

Más información en:

T. 984 395 152 | info@intedya.com | www.intedya.com



“Cuando la especialización e independencia SON VALORES IMPRESCINDIBLES”

Las certificaciones profesionales de la WCA son conformes con la **norma internacional ISO 17024 para organismos que realizan la certificación de personas**, aportando, un reconocimiento internacional a través del sistema de evaluación de la conformidad establecido y convirtiéndose en una herramienta para diferenciar los distintos niveles de capacitación de los profesionales.

Categorías de Certificaciones Profesionales:

01 | COMPLIANCE OFFICER.

02 | AUDITOR COMPLIANCE.

03 | EXPERTO EN PREVENCIÓN DEL FRAUDE.

04 | EXPERTO EN PROTECCIÓN DE DATOS (DPO).

05 | EXPERTO EN PREVENCIÓN DE BLANQUEO DE CAPITAL Y FINANCIACIÓN DEL TERRORISMO.

La alianza internacional para **la difusión de la ética y el cumplimiento** en las organizaciones.



WCA Internacional

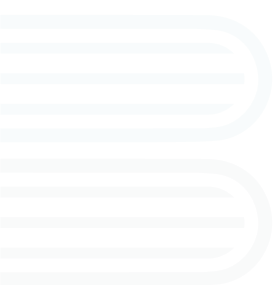
Paseo Castellana 79, 7ª Planta (Lexington Center)

28046 Madrid - España Tlf: +34 917 91 66 16

info@worldcomplianceassociation.com

www.worldcomplianceassociation.com





World Compliance Association

Paseo de la Castellana, 79, 7º planta · 28046 Madrid · España

Tel.: 91 791 66 16 · www.worldcomplianceassociation.com

Diseño y maquetación: Equipo de diseño **WCA**

© **World Compliance Association**. 17-03-2021. Todos los derechos reservados.

Se permite la reproducción total o parcial y la comunicación pública de la obra, siempre que no sea con finalidades comerciales, y siempre que se reconozca la autoría de la obra original. No se permite la creación de obras derivadas.

WORLD COMPLIANCE ASSOCIATION



biblioteca
COMPLIANCE

Para evitar un “paper compliance”, la organización debe promover la implantación de un Programa de *Compliance ad hoc*. Para cumplir este objetivo, y contar con un Programa de *Compliance* efectivo, con validez a nivel global, la función de *Compliance* deberá tener en cuenta los elementos expuestos en este capítulo: liderazgo, designación de recursos, evaluación de riesgos, implantación de mecanismos de control, formación, concienciación y comunicación, monitorización y sistema disciplinario.

