TEMA 1:

Introducción a la normativa de ciberseguridad

ÍNDICE

1. INTRODUCCIÓN AL CUMPLIMIENTO NORMATIVO

La normativa sobre ciberseguridad es transversal: no se centra en un solo sector o área, sino que afecta a diversos sectores y áreas, que son todas las relacionadas con las tecnologías de la información y comunicación.

Esta normativa surge por las nuevas necesidades derivadas de la protección de los sistemas y redes de información. Dicha normativa tiene como finalidades:

- Fijar las directrices generales del uso seguro del ciberespacio.
- Conseguir un adecuado marco normativo que proporcione una mayor confianza en el uso de las tecnologías de la información y comunicación.

El objetivo es que al realizar una gestión eficaz de los riesgos derivados del ciberespacio se pueda edificar una sólida cultura de ciberseguirdad. Esta materia resulta imprescindible para lograr una adecuada protección de:

- Instituciones (sector público)
- Empresas (sector privado)
- Ciudadanos (particulares personas físicas)

Y prevenir y perseguir ***ciberdelitos*** en todos estos ámbitos.

1.2. CUMPLIMIENTO LEGAL

El legal compliance o cumplimiento legal hace referencia al establecimiento de los requisitos y normas necesarios para asegurar que, en el seno de una empresa u organización, se cumple con el marco normativo que sea de aplicación. Este concepto tiene más de cincuenta años de antigüedad y surge, originariamente, en el mundo anglosajón. En sus inicios, estuvo vinculado al ámbito financiero, pero, poco a poco, se fue expandiendo a todos los ámbitos empresariales y gubernamentales.

En España, el concepto de cumplimiento de requisitos legales ha llegado recientemente y, en especial, se ha puesto en marcha en empresas con matrices en el extranjero. Poco a poco, esta tendencia se va ampliando también a empresas de ámbito nacional, pero que tienen una amplia proyección internacional. Si bien, en un principio, era una figura mucho más vinculada a las grandes empresas, con el paso del tiempo, se ha ido usando también en empresas de tamaño mediano o pequeño. Esto ha venido impulsado por el hecho de que la normativa que establecía obligaciones para las empresas se ha ido incrementando paulatinamente y haciendo cada vez mayores las exigencias legales en todos los niveles de las organizaciones.

Tal como señalaba Marsh&McLennan en su "MMC Cyber Handbook 2018. Perspectives on the next wave of cyber", a medida que los ataques contra sistemas informáticos han ido aumentando en los últimos años (en los últimos ocho han quedado expuestas, por estos motivos, más de 7,1 billones de identidades), los poderes públicos han ido reforzando y construyendo un marco legal cada vez más exigente en materia de ciberseguridad.

Las obligaciones de protección de la seguridad de la información, como tal, se han ido introduciendo progresivamente para distintos ámbitos y operadores. En un primer momento, se exigió en los ámbitos afectos a la seguridad nacional e infraestructuras críticas de los Estados, posteriormente a servicios de seguridad privada, a proveedores de servicios electrónicos de confianza (firmas, sellos y certificados digitales), o a operadores de servicios de comunicaciones electrónicas, finanzas, seguros y tratamiento de datos personales en cualquier ámbito.

Estas normas de protección de datos (en su sentido amplio, no solo personales) y otro tipo de activos (como infraestructuras críticas), incluyen una parte importante de controles de ciberseguridad que aseguren dicha protección, junto con una serie de medidas de ámbito más legal y administrativo.

1.2.1. Definición de compliance

Existen diferentes definiciones a la hora de explicar qué es el compliance. Así, la World Compliance Association lo considera como un ***conjunto de procedimientos y buenas prácticas que las organizaciones adoptan con el fin de "identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos***".

Hace referencia a las normas establecidas por las empresas en los ámbitos interno y externo (*mejores prácticas, Código Ético, anticorrupción, prevención de riesgos en el lugar de trabajo, protección de datos, blanqueo de capitales, etc.*). El cumplimiento de estas normas creadas por y para las empresas es una forma de prevenir y evitar cualquier conducta ilícita.

España también contempla el concepto de compliance en su sistema legal a través de varias leyes, en particular en materia de protección de datos y blanqueo de capitales.

Más recientemente, la reforma del Código Penal español ha puesto énfasis en la importancia de este concepto. De hecho, con el objetivo de regular la responsabilidad penal de las personas jurídicas, el Código especifica la obligación de vigilancia que pesa sobre las empresas y cuyo incumplimiento puede dar lugar a la responsabilidad penal jurídica.

La importancia del concepto de cumplimiento normativo se evalúa en varios niveles:

Nivel legal: respeto a la ley

La empresa debe conocer los cambios introducidos en la legislación y su obligación de actuar conforme a las nuevas normas legales.

De hecho, las consecuencias jurídicas de una actuación ilícita por parte de directores o empleados que violen las normas recaerán sobre la empresa, a menos que ésta pueda demostrar que ha puesto en marcha los mecanismos necesarios para prevenir dichas conductas.

Para no verse comprometida, la empresa debe:

- Unificar los criterios de actuación
- Organizar la capacitación de su personal
- Establecer un sistema de monitoreo
- Identificar las fuentes que aumentan el riesgo de delitos
- Trabajar conjuntamente con el departamento legal

Nivel de regulación: observación de las normas técnicas, medioambientales, de seguridad del producto, etc.

Responsabilidad social: actuar de acuerdo con el código de buenas prácticas, establecer procedimientos de autorización, supervisión, ejecución, información y control

En este nivel, el cumplimiento normativo requiere que las empresas no sólo cumplan con la normativa, sino también con el espíritu y propósito de la misma. La responsabilidad social está estrechamente ligada al concepto ético que pretende evitar el uso de la ley para propósitos distintos.

De esta forma, se puede considerar el cumplimiento como una función específica dentro de las empresas, encaminada a detectar y gestionar los riesgos de incumplimiento de las obligaciones regulatorias bajo las que opera. El incumplimiento de una ley, o de determinada normativa, puede suponer una pérdida de reputación para una compañía. Además, también puede suponerle sanciones económicas, o la exclusión de licitaciones o subvenciones públicas, entre otras.

Así, la función de compliance se encarga de ***establecer estándares y procedimientos adecuados para evitar incumplimientos.*** Además, supervisa y controla que éstos se cumplan en toda la organización.

El Compliance en muchos casos, y a tener de la evolución del marco legal a nivel mundial y la clara tendencia en este sentido, ha dejado de ser una opción voluntaria para muchas organizaciones y ha pasado a ser un requisito a integrar dentro de su estrategia y estructuras internas a fin de dar cumplimientos a los preceptos legales o bien poder protegerse ante situaciones de riesgo que pondrían en serios problemas la estabilidad y continuidad de la actividad de la organización.

Ejercicio:

Buscar un artículo en el cual el tema base es cuando falla el compliance.

Escribir un ensayo describiendo: el caso en el que ocurrió, cuáles fueron las repercusiones y qué se debía haber hecho para no incurrir en el delito.

Incluye tu opinión personal al respecto.

Guárdalo en un archivo con el nombre de: norT1P1_nombre_apellidos y súbelo a la plataforma.

2. PRINCIPIOS DEL BUEN GOBIERNO Y LA ÉTICA EMPRESARIAL

El equilibrio entre la búsqueda de oportunidades del mercado, y el mantenimiento de la contabilidad y la integridad éticas ha demostrado ser un reto determinante para la empresa comercial desde la llegada de las sociedades anónimas en los primeros años de industrialización.

La transparencia y la responsabilidad de la empresa comercial se ven constantemente cuestionadas. Los fallos manifiestos del gobierno corporativo y la ética empresarial en la crisis financiera global han incrementado la urgencia de buscar un marco ético y de gobierno mejor para los negocios.

El aumento sustancial que se ha producido en el ámbito, la trascendencia y el impacto de las iniciativas sociales y ambientales corporativas en estos últimos años sugiere la creciente importancia de adoptar un enfoque más fundado desde una perspectiva ética. Hay más indicios que ponen de manifiesto que las grandes corporaciones están asumiendo con mayor seriedad sus responsabilidades sociales y ambientales, así como de que estos asuntos están cobrando mayor importancia en la agenda empresarial.

2.1. PRINCIPIOS DEL BUEN GOBIERNO EMPRESARIAL O BUENAS PRÁCTICAS

Cuando los Gobiernos, reguladores e instituciones financieras estudiaron qué había fallado durante la crisis, se extendió una nueva idea de la **importancia de una regulación sólida, un gobierno corporativo atento y unas directrices éticas más fuertes**. De hecho, lo que emerge en la actualidad es una integración del gobierno corporativo, la responsabilidad social corporativa y la sostenibilidad corporativa, lo cual ofrece potencialmente un nuevo marco para los negocios éticos.

Este nuevo marco ético emergente para los negocios proporciona una base más sólida para el ejercicio de los valores morales y el razonamiento ético. "*Los empresarios tienen una responsabilidad en última instancia como individuos, pero se trata de una responsabilidad individual en un entorno corporativo en el que sus responsabilidades, al menos parcialmente, se definen por sus papeles y funciones dentro de la empresa… a su vez, las empresas se definen por su(s) papel(es) y responsabilidades como parte de una comunidad mayor*" (Solomon 1992, 320). Esto sugiere una alineación ética de individuos, empresas y el sistema económico, que aparece recogida en la definición de gobierno corporativo que ofrece Cadbury y que ha sido adoptada por el Banco Mundial:

El gobierno corporativo se centra en mantener el equilibrio tanto entre los objetivos económicos y sociales como entre los individuales y colectivos. El marco de gobierno existe para fomentar el uso eficiente de los recursos, así como para exigir la responsabilidad en la administración de los mismos. La meta es alinear en todo lo posible los intereses de los individuos, las empresas y la sociedad.

Por lo que podríamos decir, que el Buen Gobierno Corporativo ***es el conjunto de normas, principios y procedimientos que regulan la estructura y el funcionamiento de los órganos de gobierno de una empresa. Establece las relaciones entre la junta directiva, el consejo de administración, los accionistas y el resto de partes interesadas, y estipula las reglas por las que se rige el proceso de toma de decisiones sobre la compañía.***

Esta definición resalta la importancia del gobierno corporativo para proporcionar:

- Los incentivos y medidas necesarias para lograr el éxito en los negocios,
- La rendición de cuentas y transparencia necesarias para garantizar la distribución equitativa de la riqueza resultante.
- La importancia del gobierno corporativo a la hora de fortalecer la estabilidad y equidad de la comunidad general reconoce un papel más positivo y proactivo a las empresas.

No es que el gobierno corporativo y la regulación sean inherentemente restrictivos, sino que pueden representar una forma de facilitar que las empresas logren sus objetivos más altos. De igual modo, se puede imaginar un enfoque más positivo respecto a la ética empresarial

La idea del buen gobierno está muchas veces conectada con el concepto de "Compliance", gestión de riesgos y cumplimiento normativo. Y, iclaro que tiene mucho que ver! el cumplimiento normativo es la base de la que partimos para poder hablar de buen gobierno, sin embargo, estamos hablando de mínimos. El buen gobierno honesto y eficaz no busca sólo cumplir la ley y gestionar los riesgos, sino una gestión responsable basada en sólidos criterios éticos. Hablar de ética, es hablar de máximos.

2.1.1. Buenas prácticas en la Seguridad de la Información

Aunque de forma generalizada (y errónea) se cree que las buenas prácticas son solo aquellas que atienden al sentido común y a la reflexión del usuario y que, mientras se usen de manera racional y coherente, pueden garantizar una mejor concienciación sobre seguridad en las organizaciones.

En realidad, esta interpretación, al igual que ha sucedido con toda la teoría y documentación sobre Seguridad de la Información también ha evolucionado. Y con la llegada de flujos de gestión de riesgos y Sistemas de Gestión de la Seguridad de la Información (SGSI), los manuales de Buenas Prácticas son auténticos reglamentos sobre el correcto uso de las tecnologías de la información. Con lo cual, con su conocimiento e integración en una organización, básicamente habremos derribado todos los muros y allanado el camino para que los conjuntos de mecanismos operativos necesarios puedan llegar a la empresa también.

Existen varios enfoques principales que recogen el conjunto de buenas prácticas sobre el correcto uso de los servicios de las tecnologías de la información. Cada uno de ellos ofrece una visión diferente sobre qué hacer o cómo hacerlo. Por tanto, sus objetivos son diferentes. Entre los cuatro enfoques principales que vamos a explicar repasaremos los fundamentos de COBIT y del NIST 800-53 y la ISO 27002 pero ahondaremos más en ITIL cuya naturaleza proporciona mayor interés y nos permitirá adquirir un extenso conocimiento de la importancia de las buenas prácticas en Seguridad de la Información.

2.1.2. Enfoques de Buenas Prácticas

- **COBIT** (Control Objective over Information and related Technology)

  COBIT en español significa Objetivos de Control para Información y Tecnologías Relacionadas, en conjunto es define una guía con las mejores prácticas sobre el gobierno, control y supervisión de las tecnologías de la información, que se presentan en forma de marco de trabajo.

  Actualmente ofrece su versión COBIT 5 y está mantenida por el ISACA (Information Systems Audit and Control Association), asociación internacional muy conocida que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

  Entre otras funciones, COBIT se encarga de:

  - Ayuda a reducir los perfiles de riesgo de las organizaciones a través de la administración de seguridad, orientada a transmitir la mayor confianza posible hacia el exterior.
  - Establecer unas fases para investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información, incorporando perfiles de autorización, estableciendo una capacidad natural para la actualización y generando una concienciación vertical de los Sistemas de Información de cara a los auditores, gestores y directivos.
  - Ayudar a precisar el nivel de seguridad y control necesario para proteger los activos de las compañías mediante un modelo de administración de las tecnologías de la información.

  En definitiva, ***COBIT ayuda a decir qué debe cambiar en la organización***.

- ## NIST 800-53 Revisión 5

El NIST (National Institute of Standards and Technology) es el Instituto Nacional de Estándares y Tecnología, una agencia estadounidense destinada a promover la innovación y la competencia industrial mediante avances en métricas, normativas y generación de tecnologías que proporcionen ventajas al sector económico de los EEUU. Sin embargo, el peso a nivel internacional ejercido por este organismo junto a la proximidad de éste con el tejido científico e investigador, lo han convertido en un referente al respecto de sus formalismos sobre reglamentos, metodologías y estándares a seguir. Y uno de ellos es el ***800-53, actualmente en quinta revisión, que define los Controles de Seguridad y Privacidad para los Sistemas de la Información y las Organizaciones***. Necesario para el cumplimiento de la ley federal impuesta en los EEUU al respecto de la ciberseguridad en sus agencias gubernamentales, bajo el nombre de FISMA (Federal Information Security Management).

El 800-53 presenta un enfoque completamente holístico a la Seguridad de la Información y la gestión de riesgos al proveer de los controles necesarios para fortalecer todos los sistemas que pueden ser objetivo de ciberataques y otras amenazas.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

La máxima del NIST al respecto ***se centra en el Diseño Seguro junto a una Monitorización continua que permita a las organizaciones reaccionar y tomar decisiones ante eventos que pongan en riesgo la resistencia de sus sistemas de información***. Por tanto, este enfoque aborda aspectos técnicos de la gestión de riesgos, de cara a cumplir con los requisitos necesarios para una futura adopción de un SGSI por parte de la organización. Está más próximo a los sistemas informáticos que COBIT e implica un árbol de dependencias bastante amplio a la hora de ser desplegado en un entorno real.

https://www.nist.gov/cyberframework/resources

- ## ISO 27002

A efectos comparativos debemos mencionar esta norma internacional que establece el código de mejores prácticas para apoyar la implantación de los SGSIs en las organizaciones.

A través del suministro de una guía completa de implementación, esa norma describe cómo se pueden establecer los controles, que serán elegidos en base a una evaluación de riesgos de los activos más importantes de la empresa. La ISO 27002 se puede utilizar para apoyar la implantación del SGSI en cualquier tipo de organización, pública o privada, de pequeño o gran porte, con o sin fines de lucro; y no sólo en las empresas de tecnología.

El principal objetivo de la ISO 27002 es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

https://www.iso27000.es/iso27002.html

- ## ITIL

ITIL (Information Technology Infrastructure Library) es la **Biblioteca de Infraestructura de Tecnologías de Información** que surgió en los años 80 cuando las organizaciones que cada vez hacían un uso mayor de los sistemas de información comenzaban a definir sus propios mecanismos de gestión de las tecnologías de la información, ante la falta de estándares unificados. Por tanto, ***ITIL surgió para abanderar esa recolección de buenas prácticas y para validar qué técnicas producían los mejores resultados.*** Y desde sus inicios ITIL fue puesta a disposición del público en forma de un conjunto de libros, de ahí su nombre, para que las organizaciones de todo el mundo pudieran adoptarlo

ITIL no solamente recopiló, almacenó y manejó estos materiales, sino que, con el tiempo, ha llegado a convertirse en una metodología ejemplar para la gestión de servicios del campo de las Tecnologías de la Información (TI), convirtiéndose en el parámetro global de excelencia para aquellos que trabajan con dichas tecnologías.

ITIL proporciona una metodología enfocada a la gestión de servicios TI, dando descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr mayor calidad y eficiencia en las operaciones de TI. Por tanto, hay que tener claro, que el conductor de ITIL es el servicio y la forma de proveer dicho servicio de la mejor forma, adecuado a las capacidades de la organización y de la empresa y satisfaciendo las necesidades de los clientes.

ITIL v3 es la última versión liberada en 2007 y actualizada en el 2011 donde además de correcciones se formalizaron una serie de flujos que no habían sido concretados antes, por ejemplo, modelos de gobernanza o la generalización de uso de tecnologías en la nube. Con una nueva revisión esperada para comienzos de 2019 han surgido muchas dudas respecto a los cambios y necesidades que puede generar a la comunidad, hasta entonces no será necesario adquirir las capacidades de esta futura ITIL 4 certificándose de nuevo. Así que de momento la vitente ITIL v3 divide el contenido en 5 libros que definen el Ciclo de vida ITIL:

1. ITIL v3 Service Strategy (SS) – Estrategia de Servicio
2. ITIL v3 Service Design (SD) – Diseño de Servicio
3. ITIL v3 Service Operation (SO) – Operación de Servicio
4. ITIL v3 Service Transition (ST) – Transición de Servicio
5. ITIL v3 Continual Service Improvement (CST) – Mejora constante de Servicio

ITIL está basada en procesos puestos en marcha y recopilados en estos volúmenes, la documentación no tiene derechos de uso ya que no son prácticas personales o empresariales únicas. Por tanto, es de libre utilización. Cualquiera, independientemente de las características de la entidad, puede ponerlo en práctica, incluso únicamente las partes que le apliquen. Además, ITIL se plantea como estándar internacional de los conceptos, lenguaje, estructura y formas de trabajo de las organizaciones en todo el mundo con respecto a las TI. Tratando de respetar una estructura común del lenguaje y su terminología, así como de la tipología de documentos que se utilizan actualmente en el mundo empresarial.

El enfoque ITIL trata de crear un nexo de unión y acercamiento de la gestión de las TI con el mundo de la gestión empresarial, por lo cual comparte muchos elementos y se inspira de otros estándares como la ISO, COBIT o similares. Por tanto, otras normas o modelos de trabajo permitirán cumplir con una gran parte de las buenas prácticas de ITIL simplemente con su implantación.

El modelo de aplicación de mejores prácticas ITIL tiene, como cualquier otro modelo o norma internacional de gestión, un comité rector que actualiza, verifica, mejora la librería, evalúa nuevas mejores prácticas y además certifica qué personas pueden asesorar a las organizaciones en cuestiones de ITIL. Existen por tanto distintas certificaciones que pueden obtenerse según el nivel de profundización en la materia.

Sin llegar a hacer un análisis exhaustivo de ITIL repasaremos las 5 fases de actuación para conocer los fundamentos de acción de cada una de ellas y entender cómo se trasladan las buenas prácticas a las empresas. El objetivo es comprender como las buenas prácticas no son únicamente recomendaciones de uso, sino principios básicos que definen todos los procesos necesarios para ofrecer servicios de calidad a los clientes.

Ejercicio:

Explica cada una de las etapas del ciclo de vida de ITIL. Describe y desarrolla cada una de las gestiones que se deben hacer en cada etapa.

Guárdalo en un archivo con el nombre de: norT1P2_nombre_apellidos y súbelo a la plataforma.

2.1.3. Resumen de metodologías de buenas prácticas

METODOLOGÍA	FUNCIÓN	CARACTERÍSTICAS
COBIT	Establece el qué se debe hacer y los procesos afectados respecto a la gestión de la Seguridad de la Información	✔ Marco de trabajo excesivamente amplio ✔ Próximo a directivos y cargos administrativos ✔ Actualizado y alineado con el estado actual de las tecnologías de la información.
NIST	Selecciona los controles necesarios para fortalecer los sistemas de cara a la gestión de riesgos de seguridad.	✔ Cercano a los sistemas informáticos y orientado a empresas de índole TIC ✔ Definidos en términos propios de las agencias federales de los EEUU. ✔ Controles demasiados exhaustivos
ISO 27002	Define los requisitos para establecer, implementar, mantener y mejorar de forma continua un SGSI.	✔ Se adentra en el plano de la implementación ✔ Muy centrado en la Seguridad de la información ✔ Estándar Internacional ✔ Estrictamente vinculado a la ISO 27001
ITIL	Metodología para la gestión y provisión de servicios de TI desde un plano global para la organización	✔ Carece de detalles sobre la implementación, pero detalla todas las actuaciones. ✔ Marco de trabajo amplio orientado a los servicios basado en lecciones aprendidas. ✔ La seguridad es solo uno de sus elementos de gestión entre los múltiples a considerar

2.2. Normativa que regula el Buen Gobierno o Buenas Prácticas

2.2.1. Normativa Internacional

En el contexto **internacional** existen una serie de documentos e iniciativas que son elementos reguladores de esta materia del buen gobierno corporativo, entre ellas:

- Las Líneas Directrices de la OCDE para Empresas Multinacionales
- Los 10 principios de Pacto Mundial de la ONU
- Los Principios rectores de la ONU sobre Empresas y Derechos Humanos
- La Estrategia renovada de la UE (2011-2014) sobre RSE
- La ISO 26000
- El Grupo de Países del Consejo de Europa contra la Corrupción (GRECO)
- Comunicación de la Comisión al Parlamento Plan de acción: Derecho de sociedades europeo y gobierno corporativo

- Directiva Europea 2014/95 sobre divulgación de Información no financiera e información sobre diversidad

2.2.2. Normativa Nacional

A nivel **nacional** podemos destacar las siguientes iniciativas en materia de regulación:

- Código de Buen Gobierno – CNMV
- Estrategia Española de RSE
- Ley 31/2014, de 20 de julio, de Sociedades de Capital para la mejora del Gobierno Corporativo
- Ley 22/2015, de 3 de diciembre, de Auditoría de Cuentas
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la información pública y Buen Gobierno

La Estrategia española de RSE incluye el buen gobierno y la transparencia dentro de sus 10 líneas de actuación. El buen gobierno y la transparencia son instrumentos para el aumento de la confianza y **la confianza es el motor fundamental de la economía**.

2.3. ÉTICA EMPRESARIAL

Conviene recordar que las empresas no tienen ninguna responsabilidad respecto a la ética, al menos responsabilidad legal. Pero regirse por criterios éticos es muy recomendable y es la mejor brújula hacia la excelencia y la sostenibilidad a largo plazo.

El 60% de las empresas españolas está implantando soluciones de inteligencia artificial para automatizar procesos, pero en los modelos de automatización no se conseguirá el verdadero éxito si no se implanta la tecnología de manera responsable. Y la seguridad y la ética son muy importantes para conseguirlo.

Ética y tecnología o ¿qué está bien y qué no lo está cuando hablamos de usos de la tecnología?, es un tema que lleva ya un tiempo debatiéndose a nivel empresarial,

Las compañías son conscientes de los retos éticos que suponen o supondrán el futuro el desarrollo de la IA y el uso de datos en diferentes disciplinas, por ejemplo, las relacionadas con la salud. El presidente de Samsung, Young Sohn, ya plasmó en una entrevista concedida a Bussines Insider la posibilidad de que en el futuro (no muy lejano) se pudiera recopilar información del ADN, ser analizada y clasificada en aras de la investigación científico, reconociéndose preocupado respecto a las implicaciones éticas que el uso de este tipo de herramientas podrían tener, subrayando la necesidad que deberían estar guiadas por principios y ser empleadas con propósitos claros y no con el único objetivo de sacar provecho.

Las empresas deben hacerse responsables en el uso de las nuevas tecnologías y los fines con los que aplican estas, formar sus propios equipos de trabajo para explorar los cambios y aportar una visión global de la ética digital de en la empresa.

En ese sentido, algunas compañías ya están siguiendo los pasos de universidades como la Oxford o la de Loyola en Chicago, que cuentan con sus propios laboratorios digitales para promover el diálogo y la investigación con el objetivo de comprender los nuevos hábitos en ambientes digitales.

La ética tiene que ver con la capacidad de decidir de las empresas, con la correcta toma de decisiones. Desgraciadamente son muchos los casos en los que los escándalos de soborno, información privilegiada, o fraude, se asocian con el fracaso de la ética en los negocios.

3. COMPLIANCE OFFICER: FUNCIONES Y RESPONSABILIDADES

El Compliance Officer o en castellano, Oficial de Cumplimiento es, dentro de la empresa, **el encargado de asegurar el cumplimiento de la normativa de aplicación** o de cualquier tipo de legislación relacionada con el sector.

Es más, a lo largo de los años, ha ido aumentando la preocupación e importancia en torno a esta figura, hasta el punto de publicarse la norma ISO 19600, sobre los Sistemas de Gestión de Compliance. Si bien la mayoría de las empresas han realizado grandes esfuerzos por llevar adelante las directrices, es precisamente en este ámbito de incertidumbre, donde surge el riesgo de sufrir sanciones por el incumplimiento de las regulaciones.

La supervisión del funcionamiento y del cumplimiento del modelo de cumplimiento normativo debe confiarse a un órgano de la persona jurídica con poderes autónomos de iniciativa y control o que tenga encomendada la función de supervisar la eficacia de los controles internos de la persona jurídica. En el caso de las PYMES, la función será ejercitada directamente por el órgano de administración.

Las empresas deben definir claramente cuál es el rol que jugará el Compliance Officer, estableciendo sus responsabilidades y por encima de todo dotándolo de las atribuciones suficientes para que pueda ejercer la función encomendada que no es otra que la supervisión o vigilancia respecto al cumplimiento normativo de la empresa.

3.1. CARACTERÍSTICAS DE UN COMPLIANCE OFFICER

La decisión de designar a una persona que ya ejecute otra función en la empresa, crear un nuevo cargo, instaurar un comité o contratar a un externo que se encargue del tema, dependerá de la complejidad organizativa y tamaño de la empresa, teniendo en consideración sus singularidades y resultaría difícil recomendar a priori alguna estructura específica.

Es habitual que las empresas pequeñas designen a una sola persona para ejercer estas funciones, como también lo es que decidan asignar estas responsabilidades a otra persona que ejerce labores de supervisión dentro de la empresa. Sin embargo, esta última alternativa, aunque aceptable en unos casos, tiene sus riesgos en tanto pueda generarse un conflicto de intereses o no se dote de una verdadera autonomía al Compliance Officer, poniendo en duda uno de los principios que debe regir la función.

Mención aparte para las personas jurídicas de pequeñas dimensiones, que, por estar autorizadas para dejar la supervisión y vigilancia en manos del órgano de Administración, pueden incurrir no sólo en un conflicto de intereses (al estar sujetos a revisar sus propias actuaciones), sino en una falta de autonomía que podría hacer ineficaz el modelo. Es por ello que, en este supuesto, ***lo recomendable es que quien ejerza la función sea un director o administrador que no esté directamente vinculado con el área operativa, de manera que su labor no esté sujeta a la manera como se ejecutan los procesos.***

Por lo cual, un compliance officer debe cumplir las siguientes características:

- Función independiente de identificación, evaluación, consejo, control y auditoría del riesgo de cumplimiento de la entidad. Recordemos que la función del Compliance será la que asuma esta figura, en todas sus vertientes de asesoramiento, confección, formación e implantación.
- Se debe nombrar formalmente a la persona o departamento que ocupará la función del Compliance Officer. Esto podrá realizarse a través de un acta de la Junta de la empresa o cualquier otro tipo de documento en el que se precise de modo expreso quien ostentará las funciones que aquí describimos y la garantía de su independencia y autonomía.
- Debe existir un canal de comunicación abierto, sin dificultades, entre el Compliance Officer y los órganos de dirección y administración de la empresa.
- Perfil profesional cualificado al efecto, con la experiencia necesaria para gestionar sus obligaciones exclusivas de vigilancia del cumplimiento normativo.
- Buen criterio de imparcialidad y proporcionalidad, pues el objeto de su trabajo consiste en moverse por escenarios de amplia ambigüedad, en los que existen muchas vicisitudes y decisiones que tomar.
- Perfil honesto y firme en la toma de decisiones, para lo cual es aconsejable que no desarrolle relaciones de amistad extraprofesionales.

3.2. Funciones de Compliance Officer

Las responsabilidades del Compliance Officer en España ***parten del deber de informar los posibles riesgos e incumplimientos***, pero no se limitan a ello. Se trata de una función que para poder cumplir cabalmente con ese deber y ser eficaz en su gestión, requiere ejecutar una serie de tareas de seguimiento, control, implementación, capacitación y notificación a los órganos de gobierno de la empresa.

Si bien no hay un consenso sobre todas las responsabilidades del Compliance Officer, que pueden variar de empresa a empresa según su organigrama y sector, sí existen unas líneas generales de actuación comunes para la función que vienen recogidas recientemente en la Norma ISO 19600.

De manera enunciativa, destacan las siguientes:

- **Debe identificar las obligaciones a que están sujetas las empresas**, tanto desde el punto de vista legal como también aquellas directrices que deriven de Códigos Sectoriales o de sus propias políticas o de Códigos Éticos. La doctrina refiere estos dos tipos de obligaciones como Hard Law y Soft Law, siendo las primeras aquellas que derivan de un mandato jurídico cuyo incumplimiento representa una infracción, mientras que las últimas son aquellas que voluntariamente decide cumplir la empresa como buenas prácticas sectoriales o de desarrollo de buen gobierno.
- **Debe comprender los procesos y procedimientos de la empresa**, de manera que pueda integrar el desarrollo de los mismos con las obligaciones en materia de cumplimiento normativo.

- **Frente a los empleados, será el responsable de proveer o coordinar los entrenamientos continuos en materia de cumplimiento normativo,** así como la figura que dará soporte en el caso de dudas sobre cómo proceder o si cierta conducta constituye o no una infracción al Compliance de la empresa.
- **Responderá por la adecuada comunicación del programa de Compliance a los empleados**, debiendo divulgar cualquier información relevante en materia de cumplimiento a las empresas y hacer entrega del Código de Conducta y las políticas a que estará sujeto el personal.
- **Deberá también contribuir en la descripción de las obligaciones de Compliance que sean inherentes a cada área o cargo dentro de la empresa,** como parámetro objetivo en la evaluación de desempeño del personal.
- **Debe implementar las medidas y controles que le permitan conocer oportunamente los riesgos e incidencias**, bien sea a través del personal o inferidas de la propia documentación que recaba a través de procesos internos. Ejemplo de ello son:
    a) Sistema de denuncias,quejas y soporte telefónico o mediante correos electrónicos.
    b) Reuniones periódicas con los responsables de procesos.
    c) Informes periódicos de reporte de incidencias.
    d) Mecanismos de soporte directo a los empleados que tengan dudas sobre si una conducta o no representa un riesgo, antes de ejecutarla.
    e) Checkpoints y controles de procesos en los casos en que se exceda de los parámetros normales de operación en los cuales se requiera la aprobación del Compliance Officer (Por ejemplo: Firma de contratos que excedan determinado monto, autorización de obsequios corporativos).
    f) Indicadores de desempeño y de cumplimiento de las medidas establecidas para garantizar el cumplimiento normativo y que reflejen la evolución del sistema de prevención de riesgos.
- **Identificar y atender los riesgos derivados de sus relaciones** con clientes, proveedores, distribuidores y comerciales externos, así como con cualquier colaborador que pudiese ser considerado representante de la empresa.
- **Monitorear el funcionamiento del sistema de prevención de riesgos** y tomar las medidas preventivas y correctivas que garanticen su eficacia y asegurar la revisión en los intervalos planificados.
- **Proveer asesoría a la organización en materia de Compliance**, bien sea directamente o a través de expertos externos.

Como se puede apreciar, se trata de un conjunto de responsabilidades importantes no sólo para el cargo sino que puede incidir sobre la actividad de la empresa, y es por ello que se debe garantizar que quien funja como Compliance Officer o conforme un Comité a tales fines, sea una persona que demuestre valores como

integridad, compromiso, liderazgo, comunicación efectiva, la habilidad para insistir y convencer sobre la aceptación de sus recomendaciones y un conocimiento profundo (o el acceso a expertos en la materia) en temas de cumplimiento normativo.

Cabe destacar que el incumplimiento de estas responsabilidades puede acarrear no sólo las sanciones penales que establece el Código Penal para la empresa, sino también responsabilidades personales para el Compliance Officer que no haya ejercido su deber de vigilancia diligentemente.

Aunque por lo novedoso del tema en España no tenemos aún pronunciamientos judiciales, existen precedentes en el entorno europeo, como el de un Tribunal Federal en Alemania que condenó a la Compliance Officer de una empresa de basura de Berlín en el año 2009 por haber incurrido en omisiones respecto a su deber de supervisión y vigilancia a pesar de haber notificado el incumplimiento. Caso que, desde luego, será el espejo en el que se mirarán nuestros tribunales en breve como viene sucediendo en materia de Derecho Comunitario de la Unión Europea.

4. COMPLIANCE Y TERCERAS PARTES

El Código Penal establece que la persona jurídica es responsable de determinados hechos delictivos cometidos por sus representantes legales, por quienes ostenten facultades de organización y control dentro de la misma o por quienes están sometidos a la autoridad de cualquiera de ellos.

Sin embargo, toda empresa tiene una proyección externa ya que interviene en el tráfico mercantil y se relaciona con terceras partes, lo que provoca que su responsabilidad penal pueda producirse no sólo por los delitos que cometan sus representantes legales o empleados, sino también por los que puedan cometer los terceros que estén integrados en el perímetro de su dominio social: autónomos, trabajadores subcontratados, clientes, proveedores o socios de negocio. Es decir, los actos de todos estos terceros con los que la empresa se relaciona en el ejercicio de su actividad generan un riesgo tan significativo como el que pueda emanar de la propia empresa.

No olvidemos que la circular 1/2016 de la Fiscalía General del sobre la responsabilidad penal de las personas jurídicas, advierte que no es necesario que quien cometa un delito tenga una vinculación formal con la empresa a través de un contrato laboral o mercantil, quedando incluidas terceras partes.

Por tanto, toda empresa no sólo debe cumplir con sus propios compromisos legales y éticos sino que debe, además, conseguir que dichos compromisos sean respetados por los terceros con los que se relaciona. De lo contrario, puede verse afectada económica y/o reputacionalmente por la conducta de terceros con los que se vincula. ***Es el llamado riesgo de "contaminación o "contagio".***

Es aquí donde entran en juego los procedimientos de "diligencia debida" (due diligence) que, en el ámbito del Compliance, tratan de prevenir estos riesgos evitando comportamientos de los terceros contrarios a los principios del cumplimiento normativo.

Los procedimientos de "diligencia debida" procuran, en definitiva, una adecuada selección y supervisión de las personas que se relacionan con la empresa de forma que su comportamiento se ajuste a los principios y valores de aquélla. Ello exige el cumplimiento de un proceso en el que cabe distinguir tres etapas:

a) En primer lugar, una adecuada selección del tercero con el que la empresa se va a relacionar, valorando información de todo tipo: financiera, antecedentes frente a la administración (posibles sanciones), antecedentes frente a los tribunales (posibles condenas), relación con escándalos, …
   Se trata de comprobar si la trayectoria y el comportamiento del tercero se ajusta y es compatible con los valores y principios de la empresa. De este modo evitaremos "contagiarnos" de terceros con antecedentes de malas prácticas o con mala reputación.
b) En segundo lugar, una correcta formalización de la relación con el tercero a través de un contrato en el que se fijen cláusulas relativas a los compromisos del Compliance: veracidad de la información facilitada y de la legalidad en el uso de los productos o servicios contratados, sometimiento a los valores de la organización (especialmente al Código Ético), asumir compromisos de vigilancia y control, asumir la posibilidad de ser auditado….
c) En tercer lugar, la última etapa consiste en el seguimiento de la evolución del tercero, valorando y actualizando periódicamente la información que dio lugar a su selección.

Finalmente, señalar que, sin perjuicio del cumplimiento de las medidas referidas anteriormente, para evitar posibles responsabilidades penales las empresas deben comenzar a exigir por contrato a los terceros con los que se vinculan que dispongan de Sistemas de Gestión de Compliance Penal, exigencia absolutamente normalizada en el mundo anglosajón y que en España ya ha puesto en práctica tanto las grandes firmas como la Administración Pública.

4.1 Gestionar diligencias a través de un sistema de Gestión Compliance

Toda organización tiene una proyección externa que la relaciona con terceras partes. Esto provoca que su responsabilidad penal no solo dependa de si misma, sino también de terceros que estén integrados en el entorno de su dominio social: autónomos, trabajadores subcontratados, clientes, proveedores o partners y socios de negocio.

Esto quiere decir, que las actividades de todos estos agentes con los que una empresa o institución se relaciona en el ejercicio de su actividad pueden provocar una serie de riesgos tan significativos como los que puedan provocarse desde la propia organización.

Este tipo de riesgos, conocidos como riesgos por contaminación o contagio legal deben de ser debidamente controlados, ya que se pueden producir en cualquier momento. Para tener un perfecto control de ellos habrá que conocerlos, documentarlos y controlarlos a la perfección. La implantación de un sistema de gestión compliance contribuirá a que las organizaciones puedan controlarlos debidamente.

¿Cómo gestionar las debidas diligencia a través de un sistema de gestión compliance?

La debida diligencia es el proceso que procura una correcta y acertada selección de aquellas personas, proveedores u otros agentes que se relacionan o son susceptibles de relacionarse con la una determinada organización. El objetivo final es que su comportamiento y actuaciones estén alineadas legal y éticamente con las suyas. La implantación de un sistema de gestión compliance permitirá categorizar este procesos en etapas, pudiendo distinguir tres fundamentales:

a) Una correcta selección de terceros con el que la empresa se va a relacionar, valorando aspectos como: la situación financiera, sus antecedentes administrativos y judiciales, su posible relación con escándalos públicos, etc. Esto ayudará a establecer un primer filtro que evitará con una simple investigación cualquier «riesgo por contaminación».
b) Llevar a cabo una formalización documental que aclare cómo van a ser las relaciones con terceros a través de un contrato. En este se deberán de recoger aspectos relativos al cumplimeinto legal: veracidad de la información facilitada, la legalidad en el uso de los productos o servicios contratados, sometimiento a los valores de la organización, valores éticos, etc.
c) Llevar a cabo un seguimiento periódico de estos agentes terceros para poder ir chequeando que se siguen cumpliendo los requisitos que se plantearon en la primera fase de selección.