APUNTES 01

PUNTOS PRINCIPALES SOBRE EL CUMPLIMIENTO NORMATIVO

NORMATIVA DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

En esta unidad se va a desarrollar una serie de conceptos sobre el cumplimiento normativo con el objetivo de:

1.- Identificar las bases del cumplimiento normativo a tener en cuenta en las organizaciones.

2.- Conocer los principios del buen gobierno y su relación con la ética profesional.

3.- Construir un conjunto de políticas y procedimientos, asi como una estructura organizativa que establezca la cultura de cumplimiento normativo dentro de las organizaciones.

4.- Describir las funciones y competencias del responsable de cumplimiento normativo.

5.- Establecer las relaciones con terceros para un correcto cumplimiento normativo.

Esta unidad está enfocada en elementos introductorios, por lo que se van a desarrollar los siguientes contenidos:

1.- Introducción al cumplimiento normativo (Compliance: objetivo, definición y conceptos principales).

2.- Principios del buen gobierno y ética empresarial.

3.- Compliance Officer: funciones y responsabilidades.

4.- Relaciones con terceras partes dentro del Compliance.

1.- INTRODUCCIÓN AL CUMPLIMIENTO NORMATIVO

Definición, objetivo y función del cumplimiento normativo

El cumplimiento consiste en establecer una serie de procesos en una organización, que, acompañados de un conjunto de políticas y procedimientos consigan asegurar que se respeten todos los requerimientos legales, normativos y compromisos internos y con terceros que sean de aplicación a la organización.
El principal objetivo del cumplimiento -también denominado compliance- es, en definitiva, el de garantizar que una organización cumple con sus obligaciones adquiridas como consecuencia del funcionamiento de su negocio.

La función de compliance implica la adopción dentro de la organización de diferentes componentes que soportan su función, tales como:

- Un código ético, como un conjunto de principios y pautas de conducta que conforman la cultura organizacional de una empresa.
- Un conjunto de buenas prácticas, que, siendo ya adoptadas y probadas de ocasionar beneficios en organizaciones, están demostradas y reconocidas para proporcionar beneficios en organizaciones similares.
- Una identificación de compromisos a dividir en: legales, normativos, contractuales, organizacionales.
- La existencia de un responsable de cumplimiento, encargado de asegurar que se respeten, las normas, leyes, y por lo general, compromisos adquiridos por la organización, y, que supervise el buen funcionamiento del sistema de gestión de cumplimiento.
- La existencia de un canal de denuncias, para articular la comunicación anónima de cualquier tipo de violación de las normas existentes.
- Actividades de formación para concienciar a la organización sobre los deberes y obligaciones sobre el cumplimiento y para la creación de una cultura organizacional de cumplimiento.
- La existencia de un sistema de gestión de cumplimiento, para operar y asegurar la mejora continua del proceso de cumplimiento.

Como se ha comentado, el cumplimiento normativo implica el diseño de una serie de políticas, procesos y procedimientos que deberán respetarse durante el funcionamiento del negocio para impedir actuaciones delictivas y sanciones por infringir la ley, no obstante, no debe limitarse únicamente a las leyes aplicables, sino que debe tener en cuenta diferentes elementos como políticas internas, compromisos contractuales con clientes, proveedores o terceros, además, también debe contar con un enfoque ético, ya que el funcionamiento negocio de acuerdo a la legislación no siempre es acorde a un código ético.

Compromisos de las organizaciones

Los compromisos adquiridos por una organización, se pueden clasificar en dos categorías distintas, por un lado, aquellos que pueden ser de obligado cumplimiento, como puede ser la legislación vigente, sentencias de un tribunal o un juez, o imposiciones bajo contrato con un tercero. Por otro lado, se podría definir una categoría de compromisos voluntarios que la empresa decide asumir, tales como códigos éticos, estándares, normativas o buenas prácticas.
A continuación, se presentan algunos de los compromisos posibles que pueden ser adquiridos por una organización:

- **Compromisos de obligado cumplimiento:**

En este tipo de compromisos implica un alto nivel de riesgo más elevado para la compañía, ya que en caso de incumplimiento, pueden existir sanciones económicas y penales, se podrían poner en riesgo contratos firmados con clientes, con la consiguiente perdida de negocio, asi como ocasionar pérdidas en la imagen y reputación de la compañía.

- Legislación vigente:

Cualquier empresa está sometida a una legislación por el mero hecho de mantener su función. El cumplimiento legislativo esta también asociado a uno de los principales riesgos a los que se ve sometido una organización, el riesgo penal, financiero y reputacional. Éste deberá ser tenido en cuenta a la hora de identificar, analizar y gestionar los riesgos dentro del plan de gestión de cumplimiento.

Cualquier empresa que tenga su actividad en España debe respetar, por ejemplo, las siguientes leyes:

Ley de Sociedades de Capital: es la ley que regula las sociedades en España. Todas las personas que creen una sociedad empresa deben conocer que derechos y obligaciones tienen como socios y administradores, y las consecuencias sobre su propio patrimonio podría tener el no actuar de acuerdo a la legislación.

Ley de impuesto de sociedades: es la legislación sobre la tributación de las actividades económicas de una sociedad. Regula los impuestos sobre los rendimientos de negocio y las deducciones, bonificaciones y tipos impositivos, algo similar al IRPF, pero para empresas.

Ley del Impuesto sobre el Valor Añadido: se trata de la ley que regula los impuestos sobre los productos y servicios que presta la empresa hacia el consumidor final, esta ley establece que, como proveedora y consumidora de productos y servicios, una organización debe soportar y repercutir el Impuesto de Valor Añadido (IVA), en caso de que el IVA repercutido sea mayor que el soportado, el empresario debe pagar a hacienda la diferencia en concepto de IVA.

Ley de marcas: es la legislación para la protección de los elementos distintivos de una empresa, a través de ella se regirán los derechos sobre las marcas y los nombres comerciales de productos y servicios de una empresa española. La solicitud y tramitación de las marcas en España, se realiza a través de la Oficina Española de Patentes y Marcas, y deben especificar las tipologías de productos y servicios que se desea identificar. Éstas, pueden ser renovadas de manera indefinida o por periodos de diez años.

Ley de Servicios de la Sociedad de la Información y de comercio electrónico (LSSI-CE): Se trata de la ley que regula las actividades comerciales realizadas a través de internet. Principalmente define los requisitos que deben cumplir los sitios web de comercio electrónico de todas aquellas empresas registradas en España. En ella, se establece que en los sitios de comercio electrónico tiene que constar el nombre del dominio de Internet, ofrecer información sobre la empresa, colaborar con las autoridades y retener los datos concernientes a comunicaciones electrónicas.

Reglamento General de Protección de Datos (RGPD): Establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. Además, protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. Por último, regula la libre circulación de los datos personales en la Unión, que no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPD): Es la adaptación a la normativa local española al Reglamento Europeo de Protección de Datos (RGPD), el objetivo de esta ley es proporcionar una base legal para el tratamiento de los datos personales de las personas físicas, además, en la normativa nacional se incluyen artículos enfocados en la garantía de los derechos digitales tales como la desconexión digital, derecho al olvido, seguridad digital, protección de menores.

- Obligaciones por mandamiento judicial, tribunales o sentencias judiciales:

En este tipo de obligaciones, implica una acción por parte de la organización que los recibe, estas acciones podrían ser, desde la proporción de cierta información a un judgado o a fuerzas y cuerpos de seguridad del estado, hasta el pago de multas o sanciones, incluso la modificación de su modelo de negocio, hasta el punto de la rescisión de las licencias que permiten ejecutar la actividad de la organización. Este tipo de obligaciones pueden implicar grandes riesgos para las organizaciones y tienen que ser tenidas en cuenta en el momento de construir los sistemas de gestión de cumplimiento.

- Obligaciones por contrato de terceros:
En ocasiones, las organizaciones se comprometen en el cumplimiento de ciertas normas como forma de garantizar sus servicios, por lo general se trata de condiciones que podrían clasificarse como compromisos voluntarios, pero, al ser incluidas en los contratos de prestación de servicios, se convierten en compromisos de obligado cumplimiento.
Una muestra de este tipo de obligaciones pueden ser los compromisos contractuales de certificación en normas ISO, como puede ser la 9001 sobre sistemas de gestión de la calidad, 14001 sobre sistemas de gestión ambiental, 20001 sobre gestión de servicios de TI, e ISO 27001 sobre sistemas de gestión de seguridad de la información.

- **Compromisos voluntarios:**

Los compromisos voluntarios tienen un menor nivel de riesgo en cuanto a las consecuencias directas derivadas de su incumplimiento, ya que en el corto plazo estas serán muy leves y podrían limitarse a daños reputacionales, no obstante, este tipo compromisos significan un mejor funcionamiento para la organización, pudiendo implicar en función de los esfuerzos realizados, un funcionamiento más eficiente, seguro y respetuoso con la sociedad y medio ambiente. Estos pueden ser:

- Políticas y procedimientos:
Las políticas y procedimientos integran las normas, reglas y directrices a través de las cuales se debe regir una organización.
Las políticas deben ser específicas para cada organización y establecer los principios y el modo de comportamiento de las mismas. Estos documentos, son por lo general escritos en lenguaje de alto nivel sin incluir detalles técnicos ya que son directrices, estratégicos. Las políticas de una organización tienen varios objetivos, principalmente ayudan a conseguir los objetivos estratégicos de una organización, ahorrar tiempo y costes en la toma de decisiones rutinarias, implementar sistemas normativos de gestión empresarial (calidad, medio ambiente, seguridad de la información), reducen los riesgos empresariales y ayudan a mejorar el control directivo, administrativo y operativo de la compañía.
Si bien las políticas son documentos estratégicos, los procedimientos, son los documentos que definen las tácticas a través de las cuales se van a conseguir los objetivos de la compañía. Por lo general son documentos con un nivel de detalle más elevado, que describen una manera de ejecutar una actividad o un proceso dentro de la empresa. El procedimiento puede describir un proceso empresarial completo, describiendo paso a paso las actividades que lo comprenden.

- Normas y estándares:
Una norma es una forma comúnmente aceptada de llevar a cabo una actividad. Por lo general, puede tratarse de cualquier proceso empresarial, no obstante, en relación a tecnologías de información, se pueden definir como formas de gestionar los sistemas y tecnologías de información y comunicaciones de una organización.
El ejemplo más conocido son las ISO (International Organization for Standardization), que, aunque no estén limitadas a la gestión de procesos de IT si son las mas generalizadas, por ejemplo, la norma ISO 20000 de gestión de servicios TI, la ISO 27001 de gestión de seguridad de la información o la ISO 22301 sobre continuidad de negocio. En España, la transposición a estos estándares son las normas UNE (Una Norma Española), publicadas por la Asociación Española para la NORmalización y Certificación (AENOR).

- Buenas Prácticas y Mejores prácticas:
Las buenas prácticas son acciones recomendadas para llevar a cabo una actividad que han resultado satisfactorias para la organización, estas actividades, deben ser documentadas con el fin de crear guías, procedimientos, directrices o manuales de ejecución de un proceso.
Las mejores prácticas son acciones, que, si bien han demostrado ser satisfactorias para la organización, han sido monitorizadas y optimizadas para obtener los mejores resultados en ejecución y eficiencia en los objetivos de una organización. Las mejores prácticas son fruto del análisis y aplicación de conocimientos y procesos empresariales de los resultados obtenidos de los mismos, de lo que se ha identificado es beneficioso para la organización, de las lecciones aprendidas tras incidencias, y en definitiva tras la reflexión sobre resultados y aprendizaje continuo.

- Marcos de trabajo o Frameworks:
Los marcos de trabajo se enfocan en el cómo implementar una serie de procesos en una organización, éstos pueden ser construidos basándose en normas existentes, pero desarrollando un conjunto de procesos y buenas prácticas que marcan los pasos para desarrollar ciertas funciones dentro de una compañía. Estableciendo técnicas

estandarizadas de operación incrementando el valor y la eficiencia del los procesos TI y por tanto, del negocio. Ejemplo de marcos de trabajo son:

ITIL: Acrónimo en inglés de "Biblioteca de Infraestructura para las Tecnologías de la Información", consiste en una serie de libros que recogen las procesos y buenas prácticas para la gestión de las tecnologías de información obtenidas de diversas fuentes. La última versión de ITIL (v4) publicada en el 2019, se enfoca en la automatización de servicios IT, la gestión de los servicios, y la integración de las áreas de IT en el negocio de la organización.

Objetivos de Control para Tecnologías de la Información y Relacionadas (COBIT, por sus siglas en inglés): Es un marco desarrollado por ISACA cuyo objetivo de desarrollar estrategias de gestión y gobierno de la información y además incluye herramientas para construir, supervisar y mejorar procesos IT tras su implementación y proveer de soluciones para la gestión de riesgos. Cobit incluye 40 objetivos de gestión para ayudar a las organizaciones, para conseguir los siguientes objetivos:

Alinear los objetivos empresariales con los objetivos informáticos
Establecer un marco de gobernanza sólido
Navegar por el gobierno de la información, la gestión de riesgos y la seguridad

- Código ético:

El código ético es el conjunto de valores, principios y pautas a través de las cuales se debe regir la cultura de una organización. Asociado al código ético de la organización, podemos encontrar el código de conducta, en el cual se establecerán las directrices comportamentales que deben regir la manera de actuar de los profesionales que componen la organización.

Bajo el ámbito del código ético de la empresa, pueden establecerse elementos como las relaciones entre personas, la discriminación, el medio ambiente, el soborno y el uso de información privilegiada y la responsabilidad social corporativa. El código ético permite tomar decisiones a los integrantes de la organización en relación a la realización de su trabajo y en sus relaciones con otras personas y organizaciones, estableciendo cual debe ser su comportamiento más apropiado.

El código ético va más allá de la legislación y de los compromisos obligatorios de una organización. Las actividades de una empresa pueden ser consideradas legales, y sin embargo, estas mismas actividades, pueden de dudosa eticidad. Por ejemplo: Es legal que un deportista que participa en un torneo pueda cobrar una comisión por la organización de dicho torneo en un país extranjero, sin embargo, no es ético el cobro de dicha comisión debido principalmente a: 1) la participación del deportista en la competición que ha ayudado a organizar, 2) llevar a cabo una acción que tiene impacto sobre uno o varios grupos para lograr un beneficio individual o de muy pocos individuos, 3) cobrar una comisión elevada, 4) el agravio comparativo en la remuneración del resto de deportistas, 5) el impacto que puede ocasionar en costes logísticos para el resto de deportistas y clubs que forman parte de la competición, 6) el coste medioambiental que implica trasladar una competición a otro país a varios miles de kilómetros de distancia.

1.1.- PRINCIPIOS DEL BUEN GOBIERNO Y ÉTICA EMPRESARIAL

El buen gobierno corporativo

El gobierno corporativo tiene que ver con la toma de decisiones por parte de la dirección de la empresa y de su estrategia corporativa.

Para obtener soporte a este tipo de decisiones, se establecen procesos de buen gobierno corporativo que consisten en el conjunto de reglas, procesos y principios utilizados por los consejos de gobierno de las empresas para tomar decisiones que afecten a la empresa y a su relación con todos los actores involucrados y partes interesadas.

Las decisiones tomadas por las empresas de gran tamaño pueden tener una gran repercusión en la sociedad, por este motivo conviene tener unas normas y pautas de actuación que ayuden a tomar decisiones en las organizaciones, y especialmente en lo relacionado a elementos como estrategia de la compañía e inversiones, pero también en otros elementos como fusiones y adquisiciones.

Los procesos de buen gobierno corporativo tienen como objetivo principal mejorar la credibilidad de las organizaciones introduciendo elementos que garanticen la veracidad, transparencia y responsabilidad social corporativa en las decisiones de gestión empresarial tomadas por las cúpulas directivas.

Dentro de estas pautas, cabe la existencia de herramientas de control corporativo, que sean utilizadas para medir las decisiones de la organización desde el punto de vista económico, social o estratégico.

Otro elemento del buen gobierno implica el concepto de cumplimiento normativo, y como consecuencia, el cumplimiento de la ley vigente y la reducción del riesgo de cualquier consecuencia penal o económica para la compañía y su dirección.
Asimismo, otro objetivo consiste en vigilar y controlar los comportamientos de la compañía, de las áreas de negocio y de sus integrantes, estableciendo derechos y obligaciones de las mismas y vigilando su cumplimiento.
Las actividades relacionadas con el buen gobierno corporativo pueden ser interpretadas por el mercado como una ventaja competitiva, por ello, son utilizadas como una métrica de situación con respecto a la competencia, y una manera de llevar a cabo acciones de mejora que principalmente estarán relacionadas con los mayores beneficios generados por el buen gobierno, como el aumento de la confianza del mercado, la mejora de los procesos internos de la compañía y la garantía de funcionamiento dentro de los márgenes de la ley, como ejemplo, uno de los elementos que mas hincapié se realiza dentro de las políticas de buen gobierno corporativo son la prevención de delitos fiscales y blanqueo de capitales, existiendo otros más relacionados con el estricto cumplimiento normativo más enfocados a la prevención de la financiación del terrorismo.
Durante los últimos años, todas las compañías se han visto inmersas de alguna u otra forma en procesos de digitalización. El uso de herramientas digitales, de tecnologías de comunicación y de apertura a internet, conlleva inevitablemente un aumento de los riesgos de las organizaciones. Por ello, y cada vez más, las organizaciones centran sus esfuerzos en el control de sus sistemas de información, y por tanto la protección de su infraestructura tecnológica contra ciberincidentes que puedan tener impacto en la confidencialidad, integridad y disponibilidad de su información y por tanto en sus procesos de negocio.
En la actualidad, una de las normativas con mayor impacto para las empresas es la Ley Orgánica de Protección de Datos nacional (LOPD), y a nivel europeo la Regulación General de Protección de Datos (RGPD), cuya finalidad principal es el aumentar el control de las compañías con respecto a la información que manejan, y en especial el de los datos de sus clientes.
El buen gobierno corporativo tiene parte también en elementos más relacionados con la ética y no tanto con las limitaciones legales o normativas, como pueden ser las retribuciones de sus consejeros. Las empresas cotizadas deben realizar un informe de retribución de sus consejeros con carácter anual. Esta retribución debe ser sometida a votación y aprobada en junta de accionistas para evitar que los comités de dirección de las compañías tengan retribuciones alejadas de la realidad del mercado y además garantizar la transparencia para con sus clientes y actores relacionados.
Como parte de las actividades relacionadas con el buen gobierno corporativo, se ha de realizar un informe anual de evaluación de cumplimiento de objetivos, la finalidad de este proceso es establecer un plan de cumplimiento, midiendo las acciones realizadas y estableciendo planes de acción correctiva en caso necesario, el informe cubre de manera anual las actividades de un proceso de revisión, como son:

- Diseño:
  - Análisis del negocio y aspectos a evaluar.
- Evaluación:
  - Cuestionario de evaluación.
  - Análisis de la documentación interna y externa de la organización.
  - Entrevistas con la dirección.
- Diagnóstico:
  - Conclusiones y recomendaciones.
- Respuesta:
  - Plan de acciones correctivas.

El buen gobierno corporativo esta íntimamente relacionado con el cumplimiento normativo dado a que uno de los principales elementos que ha de tener en cuenta el buen gobierno, tiene que ver con la buena ejecución de un proceso de cumplimiento normativo. Esta relación se hace cada vez más necesaria a partir del año 2010 en el cual, el código penal recoge responsabilidades penales para personas jurídicas. Además, la ley de sociedades de capital, también requiere desde ese mismo año la introducción de políticas de buen gobierno corporativo tanto a compañías cotizadas como a compañías que no lo están. 29/8/22, 17:22 Puntos principales sobre el cumplimiento normativo.
Precisamente, existen diversas funciones que tienen que ver tanto con el buen gobierno corporativo como con el cumplimiento normativo, entre ellas:

- La aprobación de lo planes estratégicos, planes de negocio, presupuestos corporativos, y la política de responsabilidad social corporativa, entre otros.
- Definición de políticas de gestión de riesgos que cubran además de los riesgos del propio negocio, aquellos relacionados con el incumplimiento legal, fiscal, y sanciones penales.

- Establecimiento de los gobiernos corporativos, y funciones relacionadas con la toma de decisiones sobre
- Definición de códigos éticos, políticas de transparencia y de cumplimiento legal que den soporte a la toma de decisiones.
- Toma de decisiones relacionadas con los sistemas de gestión de compliance.

Elementos con los que debe contar una política de buen gobierno corporativo:

- **Cultura, valores y principios de la organización**.

- Existencia de misión y visión de la organización.
- Existencia de un código de conducta.
- Canal de denuncias abierto y anónimo.
- Régimen sancionador ante incumplimientos del código de conducta.
- Principios éticos de comportamientos y toma de decisiones.

- **Supervisión del entorno de control de la organización.**

- Definición de los equipos de supervisión del sistema de control interno (auditoría interna, reportando directamente al comité de dirección).
- Existencia de consejeros externos e independientes.
- Independencia de los consejeros en función con roles o negocios previos.
- Formación de los consejeros en políticas de control interno y gestión de riesgos.

- **Estructura organizativa de la empresa:**

- Existencia de un organigrama con el detalle de líneas de negocio, funcionales, geográficas, auxiliares y divisiones por entidades legales.
- Definición de roles y responsabilidades para cada función.
- Segregación de roles y responsabilidades.
- Reporte coherente a la estructura organizativa.

- **Políticas y procedimientos** de recursos humanos:

- Procedimientos de altas y bajas de empleados y documentación de formación para las nuevas incorporaciones que introduzca la cultura corporativa de la organización.
- Establecimiento de programas formativos, de evaluación de desempeño, remuneración y políticas sancionadoras.
- Definición de programas de medición de desempeño y alineamiento con los objetivos de la organización.
- Identificación las funciones críticas de la organización.
- Existencia de un plan de sucesión para las funciones críticas.
- Definición de planes formativos que cubran los aspectos sin sucesión en funciones críticas.

- **Modelos de asignación de autoridad** y responsabilidad para la toma de decisiones.

- Existencia de un modelo formal de asignación de autoridad según objetivos de la organización.
- Definición de protocolos de asignación de autorizar en función de la criticidad de la decisión a tomar.
- Definición de procedimiento de revisión periódica del modelo de decisión en función de cambios en la organización y la inclusión de nuevas casuísticas a integrar.
- Existencia de procesos de validación por parte de auditoría interna.

- **Sistemas de gestión del cambio.**

- Definición de procesos de estrategia empresarial a medio y largo plazo.
- Establecimiento de recursos y herramientas para la monitorización del cambio y sus consecuencias.
- Existencia de procesos de monitorización de factores externos (legislación, competencia, mercado, economía, geopolítica) y análisis de los impactos en el negocio para establecimiento de procesos de innovación.
- Revisión de cambios en la organización y las funciones clave en la organización.
- Existencia de políticas de gestión de riesgos y de continuidad de negocio ante cambios.

Principios de la ética empresarial

La ética empresarial es el código que sigue una organización a la hora de realizar su actividad, tomar decisiones, gestiona a sus recursos humanos y desarrollarse en una comunidad. Define los límites que una empresa decide ponerse, directrices a seguir, metas a alcanzar a nivel social y medioambiental, siendo estos generalmente más restrictivos que las normas y leyes. Todo este conjunto de elementos conforma una serie de valores y principios que a su vez constituyen la cultura de la empresa.

Asimismo, la ética empresarial rige el modo en que la organización se relaciona con sus clientes, proveedores, y trabajadores con el objetivo de ejercer un impacto positivo en la sociedad.

La ética empresarial es una manera de atraer talento y generar un ambiente laboral beneficioso para los empleados de la organización, además, generará más confianza tanto en clientes como en inversores, lo cual indirectamente repercutirá en un aumento de la rentabilidad. Este tipo de actividades genera atracción hacia las empresas de un mayor volumen y cualificación de profesionales que quieren crecer en organizaciones en las que confían y que cuentan en proyectos en los que creen.

Aunque los objetivos de las empresas pueden ser distintos, la ética gira entorno a aspectos que por lo general tienen que ver con la mejora del entorno y clima laboral, promover la igualdad, el respeto a los derechos, etc.

Este tipo de actividades no solo se limitan a destinar parte del presupuesto anual a una iniciativa específica, sino que también suponen una serie de actuaciones en las que la organización puede mejorar en aspectos no directamente relacionados con el negocio, por ejemplo, en diversidad en el puesto de trabajo, en reciclaje, conciliación, etc...

Las iniciativas relacionadas con ética empresarial pueden tener multitud de objetivos, no obstante, los siguientes se plantean como los más relevantes, o frecuentes:

- Respeto al medio ambiente. Todas las empresas tienen de alguna manera u otra un impacto medioambiental debido al consumo energético, emisiones o producción de deshechos, por ello, la mayoría de las organizaciones tratan de optimizar sus modelos de producción para reducir sus impactos medioambientales, por ejemplo, haciendo más eficiente su consumo energético o utilizando energías renovables.
- Responsabilidad social corporativa. Consiste en iniciativas que tendrán impacto actual o futuro en la sociedad, se trata de llevar a cabo acciones que mejoren las condiciones de vida de las zonas en las que trabaja la organización, impulsando iniciativas que favorezcan el crecimiento de la comunidad. También hace referencia a iniciativas que solucionen problemas existentes en la sociedad que no tienen necesariamente que ver con el producto o servicio que presta la compañía.
- Competencia desleal. La ética empresarial también tiene en cuenta iniciativas que eviten la competencia desleal entre organizaciones, como puede ser, la venta por debajo de coste, la comparación, las comunicaciones agresivas, la crítica o la desinformación.
- Calidad, pese a que este es un aspecto directamente relacionado con el producto, la calidad tiene también un componente ético, evidentemente las empresas deben cumplir unos estándares de calidad mínimos, no obstante, se trata de poner atención en el aumento de los niveles de excelencia de los clientes para mejorar la confianza en los mismos, además de, por ejemplo, se consiga evitar que estos sean sustituidos en un corto espacio de tiempo, con los impactos que ello pueda acarrear.
- Publicidad engañosa, haciendo de la comunicación hacia los clientes una herramienta para la generación de confianza sin utilizar argumentos de venta inválidos o incorrectos. Mejorar la transparencia de la organización a través de la publicación de las cuentas económicas de la empresa.
- Gestión de los recursos humanos, fomentando un buen ambiente laboral desarrollando valores positivos de respeto por los empleados y sus familias, como la conciliación.
- Creación e innovación, como herramienta de mejora de eficiencia y mejora en impactos ambientales y rentabilidad, mejora en la imagen de la organización y en la competitividad.

Motivos para construir un código ético empresarial:

1.- Mejora de la imagen y reconocimiento empresarial entre empleados, clientes, proveedores competencia, lo cual se traduce en un aumento de la confianza en todas las partes interesadas.

2.- Reducción de los riesgos por incumplimiento legal y por tanto de sanciones económicas y penales. La ética empresarial pone el listón del cumplimiento en una posición más elevada que la de las obligaciones legales.

3.- Obtención de beneficios fiscales por la ejecución de actividades relacionadas con la ética empresarial. Por ejemplo, a través de proporción de seguros médicos y planes de pensiones a empleados.

4.- Aumento de la lealtad de los trabajadores a través de la creación de iniciativas de conciliación y generación de ambientes seguros tras la definición de normas de convivencia y respeto a los trabajadores.

5.- Mayor atracción a inversión debido a un aumento de la imagen corporativa en la sociedad.

Llegados a este punto ya conocemos los objetivos y motivos de una organización para definir un código ético empresarial, pero, ¿Qué debe contener dicho código? A continuación, se presentan una serie de características con la que debe contar una política de ética empresarial.
El código ético siempre debe contar con los valores corporativos como base.
Además, debe girar en torno a principios éticos universales, como son la justicia, igualdad, legalidad, responsabilidad y solidaridad.
Debe contener una enumeración de las obligaciones legales a las que está sometida la empresa.
En él, se deben tener en cuenta posibles aspectos conflictivos de la organización que permitan tomar decisiones, como por ejemplo una política de retribución justa y equitativa, asimismo, debe establecer el código comportamental de los empleados de la organización.
Debe estar descrita en un lenguaje accesible para todos los destinatarios de la misma tanto a nivel interno como externo y debe aplicar a todos los empleados de la organización.
Su construcción debe contar con personal de diferentes partes de la organización para obtener el mayor volumen de información y representación posible.
Y, finalmente debe ser un documento vivo, que se revise y actualice con cierta frecuencia.

1.2.- COMPLIANCE OFFICER: FUNCIONES Y RESPONSABILIDADES

El compliance officer

El compliance officer es la persona encargada de velar por el cumplimiento de los requisitos legales y normativos de una organización, se encarga de identificar los riesgos regulatorios y asegura la existencia de controles internos para la medición y gestión de los mismos.
Debe promover una conducta ética y una cultura de cumplimiento normativo y debe trabajar para garantizar que la actividad de la empresa se realice de acuerdo a la ley, a los compromisos adquiridos con clientes y a la normativa interna.
Como responsable de cumplimiento, debe estar al tanto de las últimas leyes, normativas y reglamentos que se han de cumplir, y debe conseguir transformarlos a requisitos y procedimientos dentro de la organización.
Si bien la figura de compliance officer no está definida en la legislación española, éste, puede llegar a tener responsabilidad penal sobre cualquier tipo de actividad ilícita desarrollada dentro de la organización, ya sea por su participación en la misma, o de manera indirecta, únicamente con el conocimiento de las actividades ilegales de la organización, o, por desconocimiento por la omisión en sus responsabilidades como supervisor del cumplimiento en la organización. Las funciones de supervisión y vigilancia si están contempladas en la legislación.

Tras la reforma del Código Penal operada por la Ley Orgánica 1/2015, se establece:
“ 2.ª la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica;” (…)
“ 4.ª no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2.ª”

Si bien el artículo 2 no hace referencia explícita al compliance officer, se puede interpretar su figura en las la definición de “órgano de la persona jurídica con poderes autónomos de iniciativa y de control”, así como las herramientas y obligaciones con las que debe contar esta figura para ejercer su función, como son:
Poderes para realizar de manera autónoma y proactiva controles sobre el negocio, o una función legalmente establecida de supervisión sobre el mismo.
Que no exista una omisión o insuficiencia de las funciones de compliance officer. Debe ejecutar sus funciones con diligencia y determinación. Que informe obligatoriamente de posibles incumplimientos legales y los riesgos asociados.
Dentro de la organización tanto el responsable de cumplimiento como el comité de administración tienen dentro de sus funciones el cumplimiento legal y normativo, no obstante, mientras la función del comité se centra en la consecución de los objetivos comerciales respetando la ley pero defendiendo los intereses de la empresa, el compliance officer tiene como como objetivo el cómo respetar la ley, diseñando procesos organizacionales para cumplirla, fomentando la cultura y concienciación en cumplimiento, y estableciendo objetivos más estrictos a través de los códigos éticos y de buena conducta.
Asimismo, cabe destacar la figura del responsable de cumplimiento con respecto a la del delegado de protección de datos. Si bien el primero se encarga del cumplimiento de la normativa a nivel general, el segundo se enfoca únicamente en el cumplimiento normativo en materia de protección de datos y en los procesos asociados a dicho

cumplimiento tales, como el registro de actividades de tratamiento, el análisis de riesgos de privacidad, las evaluaciones de impacto en privacidad, los compromisos de confidencialidad y los documentos de requisitos de seguridad.
Ambas figuras están estrechamente relacionadas ya que la normativa de protección de datos es una de las más relevantes y de las que mayores riesgos y sanciones supone a las organizaciones. Funciones del compliance officer

Funciones del compliance officer
A continuación, se describen las funciones principales que son desarrolladas por el responsable de cumplimiento de una organización:

- Entender el funcionamiento de la organización y del negocio: La primera función del compliance officer es la de entender el negocio de la organización y los procesos y procedimientos de la empresa, de tal manera que pueda identificar los requisitos y obligaciones de los mismos e integrarlos en el sistema de cumplimiento normativo.
- Operación de los sistemas de gestión de cumplimiento: Debe definir y asegurarse el despliegue de las medidas y controles que permitan identificar y gestionar los riesgos e incidencias relacionadas con el cumplimiento, bien sea a través del personal o a través de herramientas internas o externas a la organización, tales como:
    - Sistemas de denuncias.
    - Reuniones con responsables de procesos.
    - Reportes de incidencias.
    - Comunicación y soporte hacia empleados ante la duda de que una actividad suponga un riesgo para la organización.
    - Revisión de nuevos procesos de la organización o modificación de los existentes.
    - Métricas e indicadores de desempeño y cumplimiento
- Desarrollar una cultura de cumplimiento en la organización: El compliance officer debe promover los procesos de cumplimiento dentro de la organización, comunicarlos y supervisarlos, con el objetivo de que sus integrantes los conozcan y los tomen en cuenta. Deben ser comunicados y recordados con frecuencia. En caso de que exista madurez en cuanto a la cultura de cumplimiento de la organización, el compliance officer será consultado a la hora de establecer nuevos procesos de negocio en la organización, y éste ayudará a diseñarlos dentro de lo limites legales.
- Asesoramiento legal y regulatorio: Debe encargarse de conocer las leyes y regulaciones que afectan al negocio de la organización y debe mantenerse actualizado sobre todas las modificaciones o nuevas regulaciones que puedan surgir. Además, deben conocer los posibles impactos que puede ocasionar su incumplimiento, por lo que son consultados ante el lanzamiento de nuevos productos o servicios.
- Supervisión de los procesos de la organización: Debe asegurarse de la monitorización proactiva de los procesos de la organización con respecto al cumplimiento legal o normativo. Para este tipo de seguimientos se realizarán revisiones periódicas con una frecuencia determinada evaluando el proceso y a sus integrantes.
- Contacto con el regulador: El responsable de cumplimiento debe ser el punto de contacto a través del cual se lleven a cabo las comunicaciones con regulador. Es el encargado de comunicar a la empresa cualquier tipo de requerimiento con origen en alguna ley o en el propio regulador, asimismo, también es el responsable de transmitir información hacia el regulador, comunicando requerimientos, solicitudes de información, sugerencias, dudas y consultas.
- Gestión de incidencias: Como responsable de un proceso de riesgo para las organizaciones, el compliance officer debe ser capaz de reaccionar a cualquier incidencia relacionada con el cumplimiento, bien a través de denuncias o a través de sanciones, debe tener las herramientas necesarias para poder detener una situación de riesgo para la compañía y mitigar cualquier vulnerabilidad que pueda ocasionar sanciones o multas.
- Concienciación: Debe tener la capacidad de comunicar los procesos de gestión de compliance, pero además debe llevar a cabo actividades de concienciación sobre cumplimiento normativo a los empleados con frecuencia, el objetivo de estas formaciones es principalmente mitigar los riesgos de incumplimiento, pero también actualizar a los empleados ante la aparición de nuevas normativas o requisitos legales y mantener la comunicación entre el negocio y el área de cumplimiento.
- Asegurar el cumplimiento en terceras partes: El compliance officer debe tener en cuenta también el cumplimiento legal y normativo en los productos y servicios contratados a terceras partes, y ser capaz de identificar y gestionar los riesgos que surgen de la relación con sus clientes, proveedores y en general con cualquier tercero relacionado con la organización.

Se debe tener especial atención a las responsabilidades de cumplimiento, ya que, en caso de externalizar un servicio, y acontezca una incidencia por algún tipo de incumplimiento legal con el proveedor, la empresa contratante, no está eximida de responsabilidad sobre dicho servicio, estos casos son especialmente relevantes, por ejemplo, en procesos relacionados con la protección de datos.

1.3.- RELACIONES CON TERCERAS PARTES EN COMPLIANCE

Riesgos de cumplimiento con terceros

Hoy en día todas las empresas tienen relación con terceros que forman parte de manera directa o indirecta de su negocio. Los terceros relacionados, pueden ser entre otros, proveedores, socios, distribuidores, intermediarios, empresas colaboradoras, y también clientes.

Como hemos visto en el apartado anterior, el código penal establece que una empresa (persona jurídica) es responsable de los actos delictivos cometidos por sus representantes legales o por quienes ostenten facultades de organización y control dentro de la misma. En este punto estamos incluyendo “sus representantes legales”, es decir, los terceros relacionados.

Por este motivo, cobra tanta relevancia la gestión del cumplimiento en terceras partes y los riesgos asociados a los servicios prestados por terceras partes. Por este motivo el compliance no se debe limitar a la organización, sino que se trata de que todos los terceros relacionados con la empresa respeten también sus compromisos. De lo contrario, su actividad económica se puede ver afectada, y también su reputación.

El riesgo de corrupción relacionado con terceros es estadísticamente elevado, ya que, en la mayoría de los casos, los pagos de sobornos son gestionados a través de terceros, siendo este foco en la identificación de los riesgos relacionados con sobornos y corrupción en las transacciones comerciales.

¿De qué manera se puede controlar el cumplimiento en terceras partes?

Para esta tarea existen procedimientos denominados de “diligencia debida” cuyo objetivo es llevar a cabo una adecuada selección y supervisión de las empresas que colaboran con la organización, de tal manera que se ajusten a los principios, valores y conductas de la organización. Asimismo, sirve para conocer el nivel de compromiso ético y de cumplimiento legal de los terceros.

Tal es la importancia de este tipo de procesos que organismos como la Organización para la Cooperación y el Desarrollo Económico (OCDE) ha publicado una guía de debida diligencia para una conducta empresarial responsable, teniendo en cuenta especialmente lo siguientes elementos a analizar, que forman parte de la Conducta Empresarial Responsable.

- Derechos humanos.
- Empleo y relaciones laborales.
- Medio ambiente.
- Lucha contra la corrupción, soborno y extorsión.
- Intereses de los consumidores.
- Divulgación de información.

Procesos de diligencia debida

Los procesos de diligencia debida se pueden articular a través de tres fases:

1.- Evaluación del comportamiento del tercero a contratar, a través del análisis de sus antecedentes, valorando información financiera, responsables de las organizaciones, relaciones con la administración pública, problemas con la administración o problemas legales previos o existencia de noticias negativas previas.

2.- Formalización detallada de la relación con el tercero, servicio a proveer, elemento que va a ser objeto de una transacción económica, o cualquiera que sea el objeto del contrato, debe quedar claramente definido y delimitado. En el contrato se deben establecer clausulas relacionadas con el cumplimiento, la legalidad de los productos o servicios provistos, la veracidad de la información provista por el tercero, los valores de la organización, y la existencia de procesos de gestión de cumplimiento tales como vigilancia y control, además de posibilidad de ser auditado. Asimismo, se deben evaluar los pagos a realizar, los motivos de los mismos y la razonabilidad de las cantidades relacionadas con los servicios o productos objeto del contrato.

3.- Monitorización de los terceros relacionados con la organización, no limitando el estudio al proceso de contratación, sino analizando a los terceros de manera como parte de un proceso, con una frecuencia determinada la información provista por los terceros en relación al compliance y el cumplimiento de los compromisos definidos en el contrato.

Autoevaluación I:

1- ¿Cuál de los siguientes elementos está considerado siempre dentro del compliance?
   a) Códigos éticos
   b) Legislación vigente
   c) Calidad
2- ¿Cuál de los siguientes es un compromiso obligatorio para una organización?
   a) Las políticas y procedimientos internos
   b) Las condiciones establecidas en la cláusula de un contrato
   c) Los estándares ISO
3- De los siguientes elementos. ¿Cuál supone una mayor esfuerzo en cumplimiento para una empresa?
   a) Los códigos éticos
   b) Legislación vigente
   c) Las obligaciones contractuales

Autoevaluación II

Los procesos de buen gobierno corporativo…

1- Pueden servir para definir planes formativos para los empleados
   a) Verdadero
   b) Falso
2- Pueden servir para establecer los horarios de los empleados.
   a) Verdadero
   b) Falso
3- Pueden servir para regular el salario de los empleados.
   a) Verdadero
   b) Falso

Autoevaluación III

1- ¿Cuáles de las siguientes son funciones del compliance officer?
   a) Generar políticas y procedimientos de Seguridad IT.
   b) Velar por el cumplimiento de la ley en la organización.
   c) Estar actualizado sobre las últimas leyes, normativas y reglamentos que afecten a la organización.
   d) Negociar el convenio colectivo corporativo con el comité de dirección
2- ¿Qué derechos y obligaciones tiene un compliance officer?
   a) Poderes para realizar revisiones de cumplimiento de manera autónoma y proactiva.
   b) Obligación de desempeñar su función de manera diligente y con determinación.
   c) Obligación a informar los incumplimientos detectados.
3- ¿Qué herramientas tiene un compliance officer para operar los sistemas de gestión de cumplimiento?
   a) La comunicación e influencia hacia la dirección para obtención de recursos.
   b) Métricas e indicadores de cumplimiento.
   c) Sistemas de comunicación de hechos delictivos.
   d) Revisiones sobre procesos de la organización.
4- ¿Cuál de las siguientes NO es una función del compliance officer?
   a) Desarrollar una cultura de cumplimiento en la organización.
   b) Establecer políticas y procedimientos de privacidad.
   c) Asegurar el cumplimiento normativo en terceras partes.
   d) Supervisar el cumplimiento legal de los diferentes procesos de negocio.

Autoevaluación IV

1- ¿Qué riesgos de cumplimiento puede ocasionar el externalizar un producto o servicio? Pregunta de Selección Múltiple.
   a) Que el tercero ejecute su función sin la calidad suficiente.
   b) Que el tercero ejecute su función fuera de los límites legales.
   c) Que el tercero ejecute su función utilizando prácticas de dudosa eticidad.
   d) Que el tercero no tenga en cuenta los requisitos contractuales de la organización.
2- ¿Cuáles son las fases de un proceso de diligencia debida?
   a) Evaluación, formalización, corrección.
   b) Definición, revisión, resultado.
   c) Evaluación, formalización, monitorización.
   d) Planificación, ejecución, revisión.

TEST

1- Los códigos éticos mejoran la percepción que tienen las personas sobre las empresas. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

2- El único estándar de seguridad de la información es ISO 27001. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

3- ACME se compromete con un cliente a contar con la certificación ISO27001, este compromiso es:
   a) Obligatorio contractual.
   b) Buena práctica.
   c) Obligatorio.
   d) Voluntario.

4 -La transposición de las normas ISO en España son las normas UNE (Una Norma Española) ¿Verdadero o falso?
   a) Verdadero
   b) Falso

5- El compliance officer:
   a) Debe ser consciente de la legislación vigente que afecta a la organización.
   b) Debe tener potestad de rescindir el contrato de un empleado.
   c) Debe tener conocimientos de seguridad informática.
   d) Debe tener un salario elevado para evitar sobornos.

6- Un proceso de diligencia debida puede implicar la rescisión de un contrato con un tercero. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

7- El compliance officer puede tener responsabilidad penal sobre un incumplimiento legal. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

8- El único compromiso legal que tienen las empresas es la normativa de protección de datos. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

9- Un código ético incluirá elementos para:
   a) Establecer los principios y valores que rijan a una organización.
   b) Conseguir salarios equitativos para todos los empleados.
   c) Establecer una correcta climatización del lugar de trabajo.
   d) Especificar las medidas de protección de la información posibles.

10- Las buenas prácticas son:
   a) Acciones que salen bien tras intentos de ejecución reiterados.
   b) Acciones que es probable sean positivas para la organización.
   c) Acciones recomendadas para llevar a cabo una actividad que han resultado satisfactorias para la organización.
   d) Acciones que han salido bien en otras organizaciones.

Solución:
Autoevaluación I: 1 b), 2 b), 3 a)
Autoevaluación II: 1 a), 2 b), 3 a)
Autoevaluación III: 1 b) c), 2 a) b) c), 3 b) c) d), 4 b)
TEST 1 a), 2 b), 3 a), 4 a), 5 a), 6 a), 7 a), 8 b), 9 a), 10 c)

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.
ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.
ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.
Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO 27001 en los servicios de comunicaciones.
La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.
Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.
La dirección de la organización está planteándose mejorar su imagen y competitividad, por lo que nos ha solicitado el desarrollo de una propuesta de código ético para la compañía.

Apartado 1: Compromisos de la organización.
¿Podrías describir al menos cuatro compromisos que tiene ACME en cuanto al cumplimiento por el funcionamiento de su negocio?
Las organizaciones, como ACME S.A. deben cumplir una serie de requisitos esenciales para garantizar el correcto funcionamiento de su empresa, siguiendo los requerimientos legales, normativos y los propios compromisos. En caso de esta empresa destacan los siguientes compromisos:

1) Como compañía que tiene su actividad en España y cuenta con 300.000 clientes, debe garantizar de manera obligatoria la protección de la privacidad y la seguridad de los datos personales de todos sus clientes. Siguiendo con la normativa europea y española que viene definida en el "Reglamento general de protección de datos" (RGPD) y la "Ley orgánica de protección de datos y garantía de los derechos digitales" (LOPD), no respetarlas puede implicar sanciones y problemas legales.
2) Uno de los compromisos obligados por contrato de terceros que se mencionan en la empresa, es el requisito de tener el certificado ISO 27001 en los servicios de comunicaciones. Necesario para gestionar los sistemas de gestión de la seguridad de la información, impuesto como requisito por una entidad bancaria que tiene como cliente.
3) La compañía también asume compromisos voluntarios, apostando por la sostenibilidad y responsabilidad social, a través del uso de paneles solares, creación de parques públicos… que les ayuda a mejorar su imagen y a su vez contribuyen al bienestar de los trabajadores/clientes.
4) Se menciona que la empresa ha solicitado el desarrollo de un codigo etico para reforzar su imagen y la competitividad. En este documento se incluirán valores y principios de conducta para mejorar la cultura y la ética empresarial de la organización, siendo un compromiso voluntario.

Estos compromisos permiten a la compañía ACME operar de manera responsable y competitiva, respetando las exigencias de los clientes y la sociedad, así como el cumplimiento legislativo.

Apartado 2: Principios del buen gobierno y ética empresarial.
¿Podrías identificar qué actividades ha realizado ya ACME como respuesta a sus principios de ética empresarial?¿Qué siete ejemplos incluirías en el código ético de ACME?
La compañía ACME, según la información proporcionada ha mostrado un compromiso a nivel de responsabilidad social corporativa, haciendo parques públicos con sus terrenos para ser utilizados por los residentes de la zona, además de acondicionar y reasfaltar los accesos por carreteras. Todo ello para mejorar el bienestar de la comunidad, mejorando el entorno.
Otro de los principios que ya cumple la empresa sería el respeto al medioambiente, realizando actividades como la climatización inteligente, jardines en las azoteas, aprovechar el agua de la lluvia, la utilización de paneles solares, entre otras, para demostrar su compromiso con la sostenibilidad y reducir el impacto medioambiental.
Por último, ACME ha obtenido la certificación ISO 27001 en los servicios de comunicaciones para uno de sus clientes con altos estándares de seguridad, lo que refleja el compromiso en cuanto a la calidad de sus servicios y la seguridad que ofrecen, para generar una confianza en sus clientes actuales y potenciales.
En resumen, Acme ya ha implementado medidas significativas en algunas áreas clave de la ética empresarial lo que mejora su imagen y competitividad. Ahora hablaremos de 7 ejemplos que la empresa podría incluir en su código ético:

1) Compromiso con el medioambiente, que la empresa minimice el impacto medioambiental con prácticas más sostenibles y eficientes, como el reciclaje de residuos, utilización de energías renovables…

2) Igualdad, que se promueva el entorno laboral inclusivo y diverso dando las mismas oportunidades a todos los trabajadores sin importar ideologías, razas, orientación sexual, edad…
3) Sinceridad y transparencia, garantizar la honestidad en las comunicaciones, evitando ocultar información, dar publicidad engañosa, comunicando decisiones estratégicas y operaciones, cuidando que la información sea clara y veraz.
4) Protección de la información, comprometerse con la protección de la información de sus clientes y empleados teniendo los mejores estándares de protección de datos.
5) Condiciones laborales, proponer condiciones laborales dignas para sus empleados, dando espacio a la conciliación entre la vida laboral y personal, respetando los derechos humanos en todo momento.
6) Competencia, promover una competencia leal en el mercado, evitando prácticas desleales (venta productos por debajo de su precio, descalificar a los competidores…)
7) Innovación, promover la creación de soluciones tecnológicas, que ayuden a la mejora de la eficiencia de sus operaciones, tanto para el sector como para sus procesos internos.

Apartado 3: Relaciones con terceras partes.

ACME quiere contratar los servicios de un call center para cubrir el servicio de atención telefónica de su centro de atención al cliente. ¿Qué elementos tendrías en cuenta dentro de un proceso de diligencia debida?

En el proceso de diligencia para contratar los servicios de un call center, ACME debería tener en cuenta los siguientes elementos:

1) Analizar la situación financiera del call center, sus balances, liquidez, capacidad de pago… para asegurar que sea confiable.
2) Evaluar la infraestructura, así como el personal y la tecnología para verificar que el call center pueda manejar el volumen de trabajo requerido, manteniendo la calidad y la eficiencia del servicio
3) Investigar acerca de la opinión sobre el call center, opiniones de clientes, experiencias, campañas publicitarias, artículos en los medios de comunicación…
   Basándose en los responsables, en casos de posible corrupción o antecedentes legales para estar enterado de posibles malas situaciones en las que se hayan podido ver afectados
4) Verificar que cumple las leyes relacionadas con el trabajo tanto nacionales como internacionales en normativas del sector. Asegurando que respete los derechos laborales de los empleados, unas condiciones laborales justas y evitando la dicriminación y que no incentiven el trabajo forzoso o infantil.
5) Comprobar si cuenta con certificaciones que garanticen un nivel adecuado de la gestión y seguridad de los servicios (ISO) así demuestran el compromiso con los estándares.
6) Investigar si el call center implementa procesos de mejora en sus servicios, como implementar la inteligencia artificial, análisis de datos o innovación para mejorar la experiencia del cliente. Esto asegura que evolucione junto con la empresa.
7) Comprobar si el call center tiene prácticas responsables con el medioambiente que coincidan con la misma mentalidad de nuestra empresa, como el reciclaje, uno eficiente de energía, reducir el número de residuos…
8) Evaluar los mecanismos de control interno del call center para identificar y mitigar riesgos de seguridad informática y protección de datos. Establecer la posibilidad de hacer auditorías periódicas y recibir informes del cumplimiento con el objetivo de detectar posibles amenazas.
9) Evaluar la tecnología para asegurar que sea moderna, segura y eficiente para manejar los datos del cliente, incluyendo herramientas de comunicación, almacenamiento y seguridad.
10) Asegurar que el call center tenga un plan de contingencia o continuidad de negocio, que le permita responder de manera eficiente ante interrupciones, desastres naturales o ciberataques.

Realizar un proceso de diligencia debida permitirá a la compañía ACME garantizar que el call center seleccionado cumpla con los estándares legales, éticos y operativos para así minimizar los riesgos y fortalecer su compromiso de la calidad y la innovación entre otros requisitos.

Se deberá llevar a cabo un análisis detallado de todos los requisitos anteriores sobre la empresa, después se redactará el contrato con los puntos claramente indicados, incluyendo cláusulas y todos los requisitos que se quieran seguir, sobre legalidad, valores éticos, medidas de control… Finalmente la empresa debe realizar un seguimiento continuo para asegurar que el call center mantenga los compromisos asumidos, de modo que se minimicen los riesgos y se proteja la reputación y a los clientes.