UNIVERSIDAD DE ZARAGOZA

IMPLEMENTACIÓN DE UN MODELO DE COMPLIANCE

Carlos Vera del Ruste

15/12/2017

Trabajo de Fin de Máster realizado bajo la supervisión del Dr. Luis Gracia Martín

Índice

ABREVIATURAS

B

- *BBDD:* Bases de Datos.
- *BYOD:* Hace referencia a la tendencia actual de que los empleados lleven sus propios dispositivos personales a la empresa para acceder a determinados recursos. BYOD, por sus siglas en inglés Bring Your Own Device.

C

- *CE:* Constitución Española de 1978.
- *CP:* Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- *CPD:* Centro de Procesamiento de Datos.

D

- *DPT:* Descripción del Puesto de Trabajo.

E

- *ERP:* Hace referencia a los sistemas de planificación de recursos empresariales, por sus siglas en inglés, Enterprise Resource Planning.

G

- *GDPR:* Reglamento (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Por sus siglas en ingles, GDPR.
- *GHC:* Hace referencia al ERP de SPYNET en el supuesto de hecho planteado.

I

- *IA:* Inteligencia Artificial.
- *IDS:* Sistema de Detección de Intrusos. Por sus siglas en inglés, Intrusion Detection System.
- *ISO:* Hace referencia a la Organización Internacional de Normalización conocida por sus siglas en inglés, derivadas de International Organization for Standardization.

- *IoT:* Hace referencia al Internet de las Cosas, por sus siglas en inglés, Internet of Things.

L

- *LSSI:* Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

N

- *NDA:* Contrato de Confidencialidad, por sus siglas en inglés Non Disclosure Agreement.
- *NAS:* El almacenamiento conectado en red, por sus siglas en inglés Network Attached Storage.

S

- *SEO:* Search Engine Optimization
- *SEM:* Seach Engine Marketing
- *STJUE:* Sentencia del Tribunal de Justicia de la Unión Europea.

T

- *TFM:* Trabajo de Fin de Máster.
- *TIC:* Tecnologías de la Información y la Comunicación.

V

- *VPN:* Sistema que permite el acceso lógico a una red privada desde un punto distinto a la misma. Deriva de las palabras en inglés Virtual Private Network.

PARTE I: INTRODUCCIÓN

I. OBJETO DEL TRABAJO

A causa de lo que algunos autores han denominado la colonización de los ordenamientos jurídicos continentales, han surgido nuevas figuras jurídicas originarias del derecho angloamericano que, pese a ser tremendamente debatidas por la doctrina, han sido aceptadas por el legislador y han pasado a formar parte de los ordenamientos continentales.

Una de las integraciones más destacables ha sido la consagración de la responsabilidad penal de la persona jurídica[1], derogándose de esta forma el principio tradicional «societas delinquere non potest» originario del derecho romano. Esta nueva óptica trata de evitar que la comisión de determinados delitos, por un defecto estructural en los modelos de gestión, vigilancia y supervisión[2], quede impune por la dificultad de esclarecer responsabilidades individuales en el desempeño de ciertas actividades a través de la opacidad organizativa que puede ofrecer la persona jurídica. No obstante, el objeto último de esta figura no es meramente el de castigar aquellas conductas reprochables, sino el de generar una cultura de cumplimiento en el tejido empresarial fundamentalmente.

Para promover esta cultura el legislador ha establecido como causa de exención de la responsabilidad penal la adopción de un modelo de organización y gestión[3] (Compliance Penal) que reduzca significativamente el riesgo de comisión de delitos en el marco de actuación de la persona jurídica. Ante esta situación muchos despachos de abogados y consultorías ofertan actualmente diversos tipos de productos (modelos de Compliance, herramientas de gestión del riesgo, o incluso carpetas de políticas y procedimientos estándar) que en ocasiones sirven para favorecer el lucro de los propios ofertantes, pero que no contribuyen al desarrollo de una verdadera Cultura de

[1] «En opinión de ZUGALDÍA ESPINAR debe entenderse que el debate sobre si se debe (desde el punto de vista político-criminal), y si se puede (desde el punto de vista dogmático), exigir responsabilidad criminal a las personas jurídicas pertenece al pasado y se encuentra superado desde hace tiempo y resuelto en sentido afirmativo». ZUGALDIA ESPINAR, J.M., *Aproximación teórica y práctica al sistema de responsabilidad criminal de las personas jurídicas en el derecho penal español*. Centro de investigación Interdisciplinaria en derecho Penal Económico (CIIPE). 2010.

[2] Sentencia 154/2016, dictada el 29 de febrero por la Sala de lo Penal del Tribunal Supremo.

[3] Según la dicción dada por el Código Penal a estos modelos.

Cumplimiento, no son efectivos y por tanto, no eximirían de responsabilidad penal a la persona jurídica[4].

El presente trabajo tiene por objeto esbozar[5] la deontología de implementación de un modelo eficaz de *Compliance Penal*[6]. Para ello, se plantea un supuesto de hecho ficticio tomando como referencia la estructura organizativa de una empresa tecnológica, a partir del cual se identificarán sucintamente los problemas jurídicos, técnicos y organizativos a los que potencialmente se enfrenta una empresa de este sector en la adopción de un programa de Compliance.

A lo largo del trabajo, se propondrán una serie de estrategias que pueden resultar de interés en las distintas fases de implementación del modelo de Compliance:

- La Fase de Diagnostico, que consiste esencialmente en la identificación de los riesgos existentes, concluirá con un breve dictamen sobre la situación actual de la empresa y la conveniencia de iniciar o no la comercialización de un producto muy particular de Inteligencia Artificial;
- La Fase de Diseño, donde se propondrán medidas correctivas para reducir la probabilidad de comisión de los riesgos identificados; y
- Las Fases de Implantación y Revisión, que en este trabajo, se han decidido mencionar transversalmente únicamente de forma teórica debido a su componente eminentemente casuístico.

II. ¿QUÉ ES COMPLIANCE?

El término inglés "*Compliance*" (Cumplimiento Normativo, en español), importado del derecho angloamericano, como se expondrá a continuación, se utiliza actualmente de forma consensuada conservando su nomenclatura original para referirse al conjunto de estrategias corporativas que debe o puede adoptar la persona jurídica para cumplir con

[4] Pues como señalaba la Fiscalía General del Estado en su Circular 1/2016 al establecer los criterios para valorar la eficacia de los modelos de Compliance «Ha de evitarse, por lo tanto, que la mera adopción de estos modelos, que profusamente ofrece el mercado especializado, constituya un salvoconducto para la impunidad de la persona jurídica blindándola».

[5] Conscientemente utilizo el término esbozar debido a la imposibilidad de plasmar en el presente trabajo todos aquellos procesos y esfuerzos que requiere la implementación de un modelo de Compliance. El objetivo fundamental es proponer metodologías sobre el deber ser de este tipo de sistemas que puedan servir de referencia. No es por tanto objetivo de este trabajo encontrar el modelo definitivo, ni tampoco redactar un informe ejecutivo que contemple todos los matices que tendría una implantación real en la que necesariamente habría que considerar múltiples adaptaciones a la naturaleza y tamaño de la concreta persona jurídica, además de acudir a la normativa sectorial correspondiente.

[6] Véase punto II.2 del presente trabajo "MODELOS DE COMPLIANCE".

aquellas normas que según el ámbito de actuación debe cumplir con objeto prevenir o evitar la comisión de determinadas infracciones propias de su sector.

Por tanto, cuando hablamos de Compliance no hablamos de cumplimiento, ni tampoco únicamente del ámbito penal, sino de todas aquellas actuaciones y compromisos que en cumplimiento del derecho positivo (conocido como *hard law*) o de los estándares y códigos éticos que de forma voluntaria son asumidos por la organización (*soft law*) con objeto de contribuir a propiciar y satisfacer las obligaciones de cumplimiento que atañen a la persona jurídica.

¿Qué no es Compliance?[7]

NO ES un modelo destinado exclusivamente a la prevención de delitos, pues un modelo de Compliance tiene por objetivo primario generar una Cultura de Cumplimiento[8], y con ello se busca proteger a la organización frente a cualquier tipo de Responsabilidad Legal[9].

NO ES un modelo destinado a prevenir cualquier tipo delictivo, sino sólo aquellos de los que la persona jurídica puede resultar responsable.

NO ES un entregable. Es decir, no basta con que se encargue a un despacho especializado la realización de un modelo de Compliance si luego no se ponen todos los medios necesarios para que el Código Ético y el Manual de Prevención de Delitos junto con sus políticas y procedimientos sean efectivamente aplicados en la organización.

NO ES exclusivamente asesoría jurídica. La función Compliance fomenta el cumplimiento de las leyes y de todos aquellos estándares adoptados voluntariamente por la organización a nivel interno.

NO ES un molde, es un modelo y como tal debe diseñarse a medida ajustándose a las particularidades propias de cada organización.

1. ORÍGENES DEL COMPLIANCE:

1.1. Nacimiento de la figura jurídica:

Tradicionalmente en el Derecho continental la responsabilidad penal del hecho delictivo ha sido exclusivamente imputable a las personas físicas, debido esencialmente a su consideración como único sujeto con capacidad de acción. Sin embargo, en el Derecho

[7] SÁIZ PEÑA, C.A.; (Coord.), Compliance: Cómo gestionar los riesgos normativos en la empresa. Thompson Reuters Aranzadi. Pamplona, 2015. Pp. 39 - 45.

[8] Circular 1/2016 de la Fiscalía General del Estado, de 22 de enero de 2016, Pg. 39. Refiriéndose a ello como «Cultura ética empresarial»

[9] Entiéndase Responsabilidad Criminal, Responsabilidad Civil (contractual y extracontractual) y Responsabilidad Administrativa.

angloamericano, ya en 1909 el Tribunal Supremo de los Estados Unidos[10], consagró en la jurisdicción federal, un modelo de imputación de la responsabilidad penal de las personas jurídicas basado en la doctrina del *respond at superior* -importada del ámbito civil-, conforme al cual, se atribuye responsabilidad penal a la persona jurídica por aquellos delitos cometidos por sus directivos o empleados, cuando estos actúen en el ejercicio de sus funciones y con la intención de producir un beneficio para la organización.

Algunas décadas después, con *la Sentencing Reform Act*, se reforma en 1984 el sistema judicial estadounidense estableciéndose la posibilidad de atenuar la responsabilidad penal de aquellas organizaciones que previamente a la comisión del delito hubiesen adoptado y aplicado efectivamente un *Compliance and Ethics Program* (Programa de Prevención de Delitos).

Progresivamente esta idea fue calando en el Derecho Continental[11] generándose una conciencia en la sociedad europea cada vez mayor sobre la necesidad de aceptar estos modelos de responsabilidad penal de la persona jurídica con el fin de evitar de este modo graves perjuicios para el interés general.

1.2. Evolución legislativa en España:

Hasta la reforma del Código Penal de 2010[12], nuestro sistema de imputación penal era de aplicación exclusivamente a la persona física. En el caso de delitos cometidos a través de personas jurídicas, la responsabilidad penal se imputaba al administrador persona física que, en tal condición, fuese autor de un determinado delito. Complementariamente, el Código Penal preveía la posibilidad de imponer a la persona moral (con o sin personalidad jurídica) las llamadas *"consecuencias accesorias"* recogidas en el artículo 129 del Código Penal, de forma conjunta con la pena al autor.

En 2010 influenciada por las recientes reformas acaecidas en países vecinos (Italia 2001 y Reino Unido 2010), se reforma el Código Penal estableciéndose en el artículo 31 bis del Código Penal que «las personas jurídicas serán penalmente responsables de los delitos cometidos en nombre o por cuenta de las mismas, y en su provecho, por sus representantes legales y administradores de hecho o de derecho», consagrándose por

[10] Sentencia Hudson. Dictada en 1909 en el caso *New York Central y Hudson River Railroad vs. United States*, por el Tribunal Supremo de los Estados Unidos.

[11] La primera referencia normativa que encontramos en Europa es la Directiva 2004/39/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a los mercados de instrumentos financieros.

[12] Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

primera vez en nuestro país la responsabilidad penal de la persona jurídica con la finalidad de ofrecer mayores garantías y seguridad jurídica esencialmente en materia de blanqueo de capitales y protección de datos de carácter personal.

Posteriormente con el propósito de reforzar la transparencia de la actividad de la administración pública y mejorar la eficacia de los instrumentos de control de los ingresos y del gasto público, se extiende en 2012[13] el régimen general de responsabilidad penal de las personas jurídicas, incluyendo en él partidos políticos y sindicatos. Asimismo, la reforma de 2012 supuso una profunda revisión de los delitos contra la Hacienda Pública y contra la Seguridad Social, regulados en el Título XIV del Código Penal.

Más tarde, en julio de 2015, el Código Penal «es objeto de una completa revisión y actualización, en la conciencia de que el transcurso del tiempo y las nuevas demandas sociales evidencian la necesidad de llevar a cabo determinadas modificaciones de nuestra norma penal. En general, se revisa el régimen de penas y su aplicación, se adoptan mejoras técnicas para ofrecer un sistema penal más ágil y coherente, y se introducen nuevas figuras delictivas (delitos leves esencialmente). Del mismo modo, se modifican tipos penales ya existentes, con el fin de ofrecer una respuesta más adecuada a las nuevas formas de delincuencia (especialmente delitos informáticos y relacionados con redes de comunicaciones); del mismo modo se suprimen aquellas otras infracciones que, por su escasa gravedad, no merecen reproche penal (se suprimen las faltas, incluyéndose algunas de ellas en el catalogo de delitos leves). Gran parte de la reforma está también orientada a dar cumplimiento a los compromisos internacionales adquiridos por España»[14].

Asimismo, con la entrada en vigor de la última reforma del Código Penal[15], el régimen de responsabilidad penal de la persona jurídica, fuertemente criticado desde su consagración en 2010 por un amplio sector doctrinal, que lo consideró incompleto y confuso en muchos de sus aspectos esenciales, es modificado de manera significativa en su revisión del art. 31 bis. A su vez, se reforma parcialmente el art. 66 bis y se introducen tres nuevos artículos, 31 ter, 31 quater y 31 quínquies. Entrando un poco más en detalle, las modificaciones más importantes consistieron en:

[13] Ley Orgánica 7/2012, de 27 de diciembre, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal en materia de transparencia y lucha contra el fraude fiscal y en la Seguridad Social.
[14] Preámbulo Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
[15] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

- La posibilidad de limitar (eximir o atenuar) la responsabilidad penal de aquellas personas jurídicas cuyo órgano de administración, antes de la comisión del delito, hayan adoptado y ejecutado eficazmente de modelos de organización y gestión que incluyan medidas de vigilancia y control idóneas para prevenir delitos o reducir significativamente su comisión[16].
- La creación de un órgano de cumplimiento: La exención de la responsabilidad será de aplicación siempre y cuando la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado haya 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, esto es, la figura del *Compliance Officer*. Por ende, se establecen como requisitos necesarios para eximir la responsabilidad que los autores individuales hayan cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención y no se haya producido una omisión o un ejercicio insuficiente de las funciones de supervisión, vigilancia y control por parte del órgano de cumplimiento.
- La extensión del régimen de responsabilidad penal a las sociedades mercantiles estatales que ejecuten políticas públicas o presten servicios de interés económico general.

2. MODELOS COMPLIANCE:

Los modelos de gestión y organización tratan de dar cumplimiento a los diferentes bloques normativos a los que las personas jurídicas están obligados, como pueden ser previsiones en materia de prevención de delitos, riesgos laborales, protección de datos de carácter personal, propiedad intelectual e industrial, derecho de la competencia, blanqueo de capitales, seguridad de la información, etc. Esta diversidad de materias en muchas ocasiones es afrontada por parte de las organizaciones de manera segmentada, es decir, delegando las funciones de cumplimiento en distintas áreas de la empresa. Esta fragmentación de la gestión de cumplimiento deriva, no en raras ocasiones, en políticas y procedimientos repetidos que debido a la falta de comunicación entre departamentos pueden ser incoherentes entre sí o incluso obviar aspectos importantes al creer comprendidos dentro de otro modelo de gestión.

[16] Nótese que el precepto utiliza la expresión «delitos cometidos» lo que según la Fiscalía General del Estado permite incluir, además de las diferentes formas de autoría y participación, el delito intentado.

El término Compliance abarca todos los modelos de organización y gestión asumidos por la empresa para propiciar el cumplimiento normativo, por tanto, podemos referirnos a modelos de Compliance de muy diverso índole, por ejemplo: IT Compliance, Legal Web Compliance, Finance Compliance, o Compliance Penal, de Riesgos Laborales, de Protección de Datos, de Competencia Desleal, etc. Aunque también podríamos referirnos a todos estos de forma conjunta al hablar de modelos de *Corporate Compliance*, los cuales, se encargarían de coordinar todos estos aspectos.

En el presente trabajo hablaremos de un sistema de Compliance Penal en el que, además de las consideraciones necesarias para la prevención de delitos, se tratarán de forma transversal otros bloques normativos, o incluso, aspectos meramente organizativos que en base a la diligencia vengan a disuadir una posible responsabilidad civil empresarial frente a clientes (véase supuesto de hecho).

2.1. ¿Qué requisitos debe cumplir un sistema de Compliance?

El Código Penal establece en su artículo 31.2 bis las condiciones por las que la persona jurídica quedará exenta - o atenuada en su caso- de responsabilidad penal, siendo en síntesis las siguientes:

- Que se haya adoptado y ejecutado eficazmente por parte del órgano de administración, antes de la comisión del delito, un modelo de Compliance que sirva para prevenir delitos de la misma naturaleza que el cometido o, al menos, para reducir significativamente el riesgo de su comisión. Debiendo cumplir los requisitos establecidos en el artículo 31.5 bis Código Penal (Se analizarán más adelante conforme a las directrices de la Fiscalía).
- Que se hayan observado suficientemente los deberes de supervisión y revisión del funcionamiento y cumplimiento del modelo implantado, por parte del órgano de control nombrado, que salvo en las sociedades de pequeñas dimensiones, deberá ser un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o una persona externa designada legalmente para ello.
- Que los autores individuales hayan cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención adoptados.

Sin embargo, a pesar de que la redacción que ofrece nuestro Código Penal en esta materia es más detallada de lo habitual, el precepto presenta dificultades técnicas demasiado abiertas a interpretación. Es por ello que la Fiscalía General del Estado emite

en enero de 2016 la CIRCULAR 1/2016[17], con el fin de establecer unos parámetros de interpretación claros sobre la responsabilidad penal de la persona jurídica (modelo de autorresponsabilidad) y unas pautas mínimas de referencia sobre la deontología de los modelos de organización y gestión a que se refiere el Código Penal.

En síntesis, las pautas de interpretación dadas por la Fiscalía sobre los seis requisitos del apartado 5 del artículo 31 bis del Código Penal, (reproducidos a continuación) son los siguientes[18]:

1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.

En este sentido la Fiscalía dijo que «Los programas deben ser claros, precisos y eficaces y, desde luego, redactados por escrito». De estas tres cualidades la más difícil de interpretar podría ser la eficacia[19], la cual parece tener que entenderse como la capacidad de acreditar su grado de adecuación para prevenir o reducir significativamente el riesgo de comisión, pues la comisión del delito no implica necesariamente la innidoneidad del modelo. Corresponde al juez valorar dicha capacidad teniendo en cuenta la idoneidad del contenido del programa en relación con la infracción.

Por este motivo, quiere advertir la fiscalía la importancia de que los modelos sean originales y el diseño se haya realizado a media adaptando el modelo a la persona jurídica y a sus concretos riesgos. Es decir, que no copien los modelos de otras empresas/organizaciones, pues «esta práctica suscita serias reservas sobre la propia idoneidad del modelo adoptado y el verdadero compromiso de la empresa en la prevención de conductas delictivas».

En cuanto a la precisión, cabe deducirse la necesidad de realizar evaluaciones previas al diseño del modelo que permitan identificar los riesgos reales y potenciales derivados de las actividades de la organización (fase de diagnostico), para ello «el análisis identificará y evaluará el riesgo por tipos de clientes (entiéndanse personas físicas, sociedades mercantiles, administraciones públicas), países o áreas geográficas (ámbito de actuación y ubicación), productos, servicios, operaciones, etc., tomando en consideración variables como el propósito de la relación de negocio, su duración o el

[17] CIRCULAR 1/2016, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, de 22 de enero de 2016.
[18] Circular 1/2016 de la Fiscalía General del Estado de fecha 22 de enero de 2016, apartado 5.3
[19] Para más información véase el apartado 5.6. de la Circular 1/2016 sobre Criterios para valorar la eficacia de los modelos de organización y gestión.

volumen de las operaciones». En este sentido entiendo igualmente necesario considerar el modo en el que se desarrolla la actividad con las particularidades propias del caso concreto. Por ejemplo; en la suscripción de contratos con fines lícitos habrá de identificar si el firmante tiene o no poderes.

Asimismo, se destaca la importancia de contar con aplicaciones informáticas que controlen «con la máxima exhaustividad los procesos internos de negocio de la empresa». Estas herramientas son especialmente útiles para acreditar el cumplimiento mediante el almacenamiento de evidencias, para realizar las funciones de supervisión encomendadas al órgano de cumplimiento o, por ejemplo en modelos de Compliance de Protección de Datos, pueden tener otras funcionalidades como dar respuesta al ejercicio de derechos GDPR como el derecho a la portabilidad.

2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.

Estos protocolos y procedimientos a que se refiere el precepto «deben garantizar altos estándares éticos, de manera singular en la contratación y promoción de directivos y en el nombramiento de los miembros de los órganos de administración. Además de la obligación de atender a los criterios de idoneidad fijados por la normativa sectorial y, en defecto de tales criterios, la persona jurídica debe tener muy en consideración la trayectoria profesional del aspirante y rechazar a quienes, por sus antecedentes carezcan de la idoneidad exigible». Personalmente considero que la Fiscalía no ha sido suficiente clara en este aspecto. Entiendo que la finalidad de estas pautas es evitar que la contratación y promoción interna este influenciada por favoritismos a familiares o amigos, o incluso la figura del testaferro u "hombre de paja", pero ¿deben concretarse estos estándares éticos en una política que establezca pautas de contratación y promoción?, ¿bastaría con llevar a cabo una contratación diligente?, ¿si existen criterios de idoneidad en normativa sectorial deben necesariamente tenerse en cuenta para considerarse contratación diligente? Mi recomendación sería tratar de prever lo máximo posible en políticas escritas donde se estipulen una serie de criterios objetivos que valoren el merito y la capacidad del trabajador, permitiendo cierto margen de valoración subjetiva que corresponderá al responsable de la contratación.

3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.

La Fiscalía no se pronuncia a este respecto. El propio precepto parece sugerir el uso de herramientas informáticas que garanticen la trazabilidad de los movimientos financieros, la observancia de la normativa en blanqueo de capitales y en definitiva la identificación del dinero de la organización.

4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

En la interpretación de este apartado la Fiscalía aprovechó para extender el criterio de la eficacia, el cual, además de permitir la prevención de delitos «debe posibilitar la detección de conductas criminales». Para ello, se hace necesaria la existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas, que permitan a los trabajadores cumplir con su obligación de informar de riesgos e incumplimientos. «Ahora bien, para que la obligación impuesta pueda ser exigida a los empleados resulta imprescindible que la entidad cuente con una regulación protectora específica del denunciante (*whistleblower* – persona que "hace sonar el silbato", que alerta), que permita informar sobre incumplimientos varios, facilitando la confidencialidad mediante sistemas que la garanticen en las comunicaciones (llamadas telefónicas, correos electrónicos…) sin riesgo a sufrir represalias».

Esta interpretación me parece adecuada y necesaria, sin embargo, veo ciertos problemas en su aplicabilidad. En empresas de cierto tamaño donde las relaciones entre trabajadores y directivos es relativamente distante es cierto que podrán establecerse estos canales de denuncia y funcionar correctamente, pero en empresas que aun siendo de tamaño medio (pongamos 40-60 trabajadores) las relaciones entre trabajadores y directivos son cercanas y basadas en la confianza, estos canales no son del todo bien recibidos y la confidencialidad de la denuncia probablemente sea difícil de garantizar, sustancialmente por la facilidad para identificar funciones y conocimientos del hecho.

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

La Fiscalía aclaró que el sistema disciplinario debe establecerse en un código de conducta donde se contemplen las obligaciones de directivos y empleados, así como un catalogo de infracciones y sanciones. Igualmente el código deberá contemplar «aquellas conductas que contribuyan a impedir o dificultar el descubrimiento de estas infracciones así como la infracción del deber específico de poner en conocimiento del órgano de control los incumplimientos detectados».

6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

El precepto establece claramente el deber de verificar periódicamente la eficacia del modelo. La fiscalía en este sentido señala la necesidad de contemplar expresamente en el modelo de Compliance el plazo y el procedimiento de revisión que se llevará a cabo por parte del órgano de cumplimiento. A si como, establecer el deber de revisarlo inmediatamente cuando concurran circunstancias que puedan influir en el análisis del riesgo u otras que lo alteren significativamente como por ejemplo modificaciones en el Código Penal o normativa sectorial aplicable que afecten a la actividad de la corporación.

Sintetizando, los modelos de Compliance deben:

- Constar por escrito.
- Ser claros, precisos, eficaces, diseñados a medida e idóneos para prevenir o reducir significativamente el riesgo de comisión de delitos.
- Supervisarse periódicamente por el correspondiente órgano de cumplimiento.
- Actualizarse y poner las medidas necesarias para garantizar su eficacia por parte del órgano de gobierno de la persona jurídica.
- Contar con canales de denuncia anónima para garantizar el correcto ejercicio de las obligaciones de información a las que refiere el art.31.5.4º bis CP.
- Establecer un catalogo con las infracciones y sanciones aplicables por la inobservancia del modelo.
- Aplicar efectivamente el sistema disciplinario.

3. LA FUNCIÓN COMPLIANCE:

Como ya se ha ido exponiendo a lo largo de este trabajo, la función esencial de todo modelo de Compliance no es la de eximir de responsabilidad a la persona jurídica[20] sino la de adoptar una autentica y efectiva Cultura de Cumplimiento que sea observada por toda la organización. Con el término "cultura" nos referimos a la profunda creencia de que toda la actividad de la persona jurídica tiene que observar de forma rigurosa toda aquella norma que le sea de aplicación, ya tenga origen en el derecho positivo (*hard*

[20] En caso de comisión de delito la exención o atenuación de la pena que correspondería a la persona jurídica debe ser una causa de la efectiva adopción y cumplimiento de un modelo de Compliance, pero no su fin último.

law) y carácter imperativo o haya sido adoptado voluntariamente por la organización a nivel interno (*soft law*). Sin embargo, para garantizar el cumplimiento en la organización, la función Compliance, además de generar una conciencia ética empresarial orientada a prevenir la comisión de infracciones y delitos, debe necesariamente ser capaz de detectar esas conductas infractoras/delictivas y reaccionar ante ellas, tratando de individualizar responsabilidades identificando al infractor, contemplando incluso en sus propios procedimientos internos la colaboración con el sistema de enjuiciamiento penal en el caso de comisión de delitos.

La eficacia de los modelos de Compliance y la garantía de su función queda supeditada sin embargo a la interacción del modelo con otras funciones de la organización que requieren la necesaria colaboración de distintas áreas de la persona jurídica, empezando por el órgano de gobierno que debe dotar de independencia y autonomía al órgano de cumplimiento, así como facilitar y comunicar la incorporación de las obligaciones que se desprendan de las políticas y procedimientos del modelo a las distintas actividades de la persona jurídica. Asimismo, como se expondrá en el apartado relativo a la Fase de Diseño, se hace necesaria la colaboración con otras áreas que puedan tener encomendadas funciones que impliquen necesidad de políticas y procedimientos para cumplir con obligaciones legales como recursos humanos, administración, legal, etc, evitando de esta forma los problemas de la gestión segmentada mencionados anteriormente al hablar de los modelos de Compliance.

III. LA RESPONSABILIDAD PENAL DE LA PERSONA JURIDICA

No es objeto de este trabajo entrar a analizar la corrección o no del régimen de responsabilidad penal de la persona jurídica en la doctrina científica[21]. Pues se trata de un debate superado que en el marco de este trabajo y en relación con su objeto carecería de sentido plantear. El problema de la responsabilidad criminal de las personas jurídicas radica actualmente en la necesidad de establecer los criterios normativos de imputación[22], tarea que resultaría demasiado ambiciosa en este momento, especialmente si recordamos que todavía nos encontramos en la introducción del trabajo. Por ello, conviene ahora exclusivamente señalar que la eventual responsabilidad criminal de la

[21] Sobre la discusión doctrinal de la cuestión, véase Gracia Martín, Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica", recpc 18-05 (2016).

[22] ZUGALDIA ESPINAR, J.M., Aproximación teórica y práctica al sistema de responsabilidad criminal de las personas jurídicas en el derecho penal español. Centro de investigación Interdisciplinaria en derecho Penal Económico (CIIPE). 2010.

persona jurídica puede derivarse si concurren los requisitos señalados en el art.31 bis del Código Penal, estos son sustancialmente: que el delito se haya cometido en nombre o por cuenta de la organización y en beneficio directo o indirecto de la misma. Requisitos que deben valorarse de forma acumulativa, no excluyente[23].

En cuanto a la configuración del tipo de responsabilidad penal dado por nuestro legislador, la Exposición de Motivos de la LO 1/2015 despeja «las dudas interpretativas que había planteado la anterior regulación, que desde algunos sectores había sido interpretada como un régimen de responsabilidad vicarial», y explica concienzudamente que «la reforma lleva a cabo una mejora técnica en la regulación de la responsabilidad penal de las personas jurídicas, introducida en nuestro ordenamiento jurídico por la Ley Orgánica 5/2010, de 22 de junio, con la finalidad de delimitar adecuadamente el contenido del «debido control», cuyo quebrantamiento permite fundamentar su responsabilidad penal». De esta puntualización según la Fiscalía General del Estado[24] puede extraerse que «el propósito de la Ley no sería modificar el régimen de responsabilidad de las personas jurídicas sino aclarar el modelo establecido en 2010 que, conforme al Preámbulo de la LO 5/2010, consagraba en el segundo párrafo del art. 31 bis.1 una responsabilidad directa o autónoma de la persona jurídica», esto es, un modelo de responsabilidad por el hecho propio. El fundamento de imputación de la persona jurídica reside por tanto en la defectuosa organización que provoca la comisión del delito o, que al menos, favorece la comisión por parte del individuo.

En el supuesto de hecho del presente trabajo se plantean una serie de elementos que podrían dar lugar distintos tipos de responsabilidades. Asimismo, el modelo de Compliance planteado tiene por objetivo principal generar una Cultura de Cumplimiento, y con ello se hace referencia a identificación de riesgos, diseño de distintas propuestas de organización y medidas preventivas (adopción de políticas, procedimientos, códigos éticos, etc), e implantación de estas medidas con la finalidad de cumplir con aquellos aspectos legales y corporativos que consecuentemente previenen de responsabilidad penal en caso de comisión de delito y concurrencia de los elementos del tipo del art. 31 bis Código Penal, o en caso de no concurrir de responsabilidad civil.

[23] SÁIZ PEÑA, C.A. (Coord.); PÉREZ BES, F., (Coord.), La Responsabilidad Legal de las Empresas Frente a un Ciberataque. ISMS Forum Spain – ENATIC. Madrid.
[24] Circular 1/2016. Ver Legislación.

PARTE II: DESARROLLO DEL TRABAJO

I. SUPUESTO DE HECHO

El supuesto de hecho que se presenta a continuación no es real, con él se pretende ilustrar la necesidad e importancia de tomar en consideración las particularidades propias del caso concreto durante todas las fases de implementación de un modelo de Compliance. Asimismo, se ha querido aprovechar el marco de este trabajo para exponer el alcance y la complejidad de los nuevos escenarios que plantea el desarrollo de la tecnología, especialmente en el ámbito de la Inteligencia Artificial, cada vez más presente y donde el control de la empresa sobre sus productos puede llegar a ser cuestionable.

Con la intención de acercar el supuesto de hecho lo máximo posible a la realidad, los hechos planteados son expuestos desde dos perspectivas, distintas pero complementarias entre sí para el propósito de este trabajo. Por un lado, se presenta una breve descripción de la empresa y de las particularidades objetivas[25] del supuesto, desde una óptica digamos «académica». Y por otro lado, desde una visión llamemos «ejecutiva» se presentan los hechos mediante una ficción de entrevistas, de modo que se reflejan tal y como podrían haber sido contados los interlocutores de la empresa. De esta forma se pretende exponer cómo sería la fase de diagnostico de esta compañía y el informe donde se reflejaría.

1. DESCRIPCIÓN DE LA EMPRESA Y ENCARGO DEL SERVICIO:

I. SPYNET S.L., es una compañía española especializada en la prestación de servicios tecnológicos e investigación y desarrollo de Inteligencia Artificial, líder en el sector de las TIC (Tecnologías de la Información y Comunicación), domiciliada en Zaragoza, con presencia en varias ciudades españolas (Zaragoza, Madrid y Guadalajara) y más de 400 trabajadores en nómina.

II. SPYNET cuenta con cuatro grandes divisiones de negocio:

1. *Guardian*: Servicios de Hosting y Back up. Prestan servicios de soporte y gestionan los recursos IT de toda la compañía (Zaragoza y Guadalajara).

[25] Objetivas en el sentido de que esos hechos deben ser tomados como reales, cómo algo cierto que ocurrió de ese modo y no da lugar a interpretaciones subjetivas. Hechos que en una situación de implementación real siempre son conocidos a través de un interlocutor de la empresa, por lo que su objetividad puede ser discutida.

2. *Impulsa*: Desarrollo, gestión y soporte de plataformas web (Madrid).
3. *Code Monkey*: Desarrollo de software (Zaragoza).
4. *IA Service*: Investigación y desarrollo de Inteligencia Artificial (IA) (Zaragoza).

III. Los principales clientes de SPYNET son grandes empresas tanto nacionales como extranjeras ubicadas en España. Sin embargo, con la salida al mercado del nuevo producto de IA Service, el P3CO[26], esperan que el grueso de sus clientes comiencen a ser los particulares.

IV. Ante este escenario SPYNET contacta con HLT & CyberSec, consultoría legal especializada en derecho tecnológico y seguridad de la información, solicitando asesoramiento legal y la prestación de su servicio de Compliance Penal con el objetivo de conocer sus necesidades de cumplimiento y especialmente las medidas a adoptar para garantizar la correcta comercialización de su novedoso producto.

2. PARTICULARIDADES DEL SUPUESTO:

2.1. El Robot:

I. IA Service tras varios años de investigación ha desarrollado a "P3CO", un robot con apariencia humana diseñado para servir en las tareas del hogar y encargarse del cuidado de los niños mientras los padres trabajan. Este robot ha sido programado con una serie de conocimientos sobre cocina, limpieza e higiene, cuidado y alimentación de personas, primeros auxilios y psicología básica. P3CO ha sido inicialmente programado para hablar solamente en español.

II. En las primeras versiones del robot los desarrolladores invirtieron grandes esfuerzos tratando de conseguir que P3CO se pudiese comunicar de forma correcta y eficiente. Consiguieron que el robot hablase un perfecto español, sin embargo, observaron que las normas de lenguaje que le habían dado no eran suficientes para lograr la calidad de producto que buscaban. P3CO era capaz de hablar y mantener una conversación en función de las preguntas que se le formulasen siempre que estas no fuesen demasiado complejas. No obstante, no tenía capacidad para entender palabras que no estuviesen en su vocabulario, tenía dificultades para distinguir determinados registros lingüísticos, y no era capaz de relacionar algunos conceptos.

III. Con la intención de que el robot pudiese mantener una conversación más natural los desarrolladores consiguieron dotar al robot de la capacidad de auto-aprendizaje.

[26] Véase el apartado 2.1 del apartado "Particularidades del supuesto".

Desarrollaron un complejo software basado en Inteligencia Semántica e Inteligencia Computacional Cognitiva que permitía a P3CO relacionar conceptos, entender situaciones complejas y aprender de forma autónoma nuevas funcionalidades y formas de comunicación a través de la observación.

IV. En fase de pruebas se descubrió que este aspecto podía traer consecuencias negativas. Se sometió a grupos de robots a distintos tipos de estímulos y se evidenció que en función de los estímulos que recibiesen los robots podían variar su comportamiento. Sometidos a mensajes que fomentaban la educación, el respeto, la amabilidad, la generosidad, o ayuda desinteresada, los robots se mostraban agradables y respetuosos con todo el mundo. En cambio, en ambientes donde estaban expuestos a mensajes que fomentaban e incitaban directa o indirectamente al odio, la hostilidad, la discriminación o la violencia contra determinado grupo de personas, los robots se mostraban reaccionarios ante personas de ese colectivo.

V. Asimismo, algunos técnicos alertaron que la falta de adecuadas medidas de seguridad en los robots los hacía fácilmente vulnerables ante ataques informáticos. Lo cual podía comprometer la confidencialidad de la información generada por los robots derivándose graves consecuencias para los clientes del P3CO.

VI. A pesar de la identificación de estos riesgos y de las múltiples advertencias del equipo de IA Service, SPYNET decide lanzar al mercado español su primera versión de P3CO.

2.2. El Encargado del Tratamiento:

I. Data&Coins Inc., es una compañía estadounidense del sector TIC especializada en BigData. Asimismo, presta servicios de "Hosting" (almacenamiento de datos) y "Back up" (copia de seguridad) a cientos de empresas de diversas nacionalidades, pues gracias a la gran red de servidores que tienen distribuida por todo el planeta han conseguido dar cobertura a una gran cartera de importantes clientes.

II. A mediados de 2015 la compañía se vio envuelta en grandes escándalos reputacionales tras recibir numerosas denuncias de empresas americanas por cesión de datos no consentida con fines comerciales (cesión de bases de datos personales, elaboración de perfiles con fines publicitarios, venta de información confidencial y secretos de empresa, etc.).

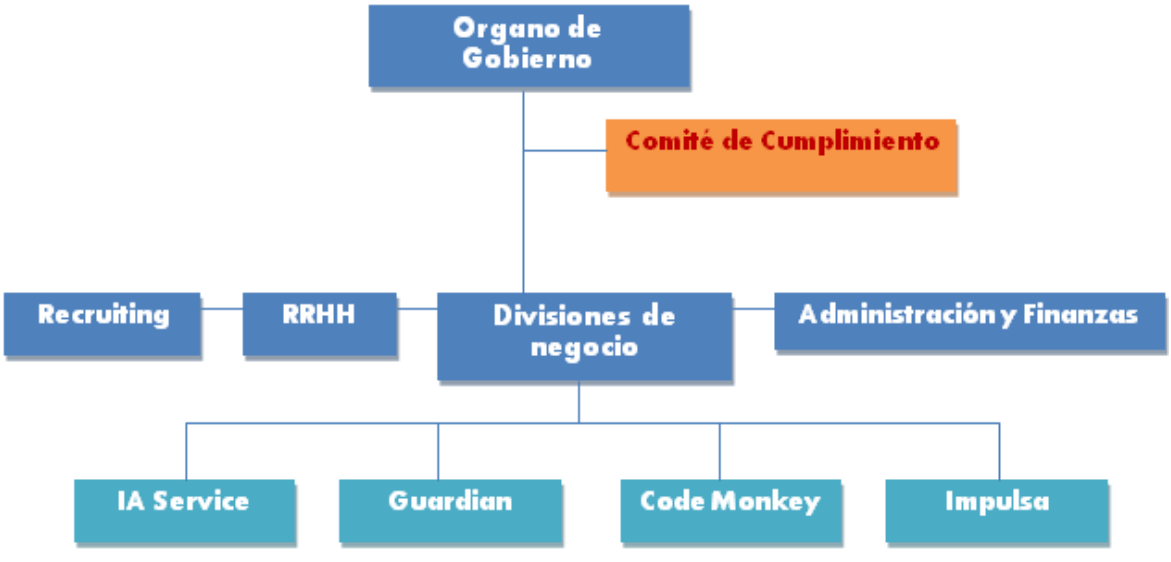
III. El escándalo finalmente no fue muy conocido en Europa, sin embargo terminó con la condena al pago de una elevada indemnización a las empresas afectadas.

IV. Desde 2016 Data&Coin presta servicios de "Hosting" y "Back up" a SPYNET. De tal forma que SPYNET almacena cada año millones de datos en los servidores de la americana, pues aloja tanto los generados por aplicaciones de clientes que quieren un servidor para almacenar sus datos, como los datos de los propios clientes que almacenan algunos productos de IA Service de los que SPYNET es Responsable del Tratamiento.

V. Entre estos productos desarrollados por IA Service se encuentra "Cynthia", un robot-aspiradora (IoT)[27] que es programable a través de una app que los clientes pueden descargarse en su móvil para disponer de las diferentes funciones del robot. Entre las cuales está programarlo para que limpie a la hora deseada, configurar los distintos modos de limpieza, controlarlo a distancia, recibir avisos de falta de batería, etc.

VI. Este robot para su mejor funcionamiento y optimización crea un plano de la casa de forma automática, así como un registro de las personas que viven en la casa y de los horarios que suelen llevar mediante un novedoso sistema denominado "CleaningESCAN[28]". Es decir, desde 2015 SPYNET ha estado enviando datos personales de sus clientes a un tercero Encargado del Tratamiento.

3. ORGANIGRAMA DE LA EMPRESA:



[27] Internet of Things, por sus siglas en inglés "IoT". Hace referencia a todos aquellos productos conectados a Internet.
[28] Se trata de un sistema ficticio, inventado para este supuesto con objeto de analizar los riesgos penales que derivarían del tratamiento de los datos personales generados por la máquina.

El órgano de Gobierno de SPYNET está compuesto por cinco socios que ostentan cada uno un 20% de las participaciones de la empresa.

El Comité de Cumpliento está compuesto por tres personas: la responsable de Recursos Humanos, el responsable de Administración y Finanzas y yo como abogado contratado para llevar a cabo las funciones de cumplimiento *As a Service*.

Las áreas señaladas en azul oscuro operan de forma transversal en todas las divisiones de negocio.

II. FASES DEL SISTEMA DE COMPLIANCE PENAL

1. DIAGNOSTICO DEL SISTEMA

En toda implementación de un Sistema de Gestión, sea de la índole que sea, resulta necesario realizar, previamente a cualquier otra acción, un estudio de la entidad dónde se va a implantar el sistema, con el fin de conocer su estructura, organización, funcionamiento interno y partes implicadas entre otros. Asimismo, resulta fundamental para el diseño del Sistema y posteriores fases de implantación y revisión, realizar un Diagnostico del Sistema, esto es identificar los riesgos, definir sus causas, conocer sus consecuencias, valorar la probabilidad y la existencia de factores que pueden mitigar las consecuencias del riesgo, o la probabilidad de que éste se materialice. La fase de Diagnostico, por tanto, puede entenderse como un proceso divisible en tres partes[29]:

En primer lugar, **la Identificación del riesgo:** se trata de detectar, reconocer y describir los riesgos, de forma que con posterioridad, sean fácilmente identificables tanto los nuevos riesgos detectados como los ya conocidos sobre los que se hayan implantado medidas correctivas. Para la realización de esta primera parte, deberán analizarse todas las actividades de la empresa, las habituales y las nuevas que se puedan producir. Se trata de obtener una relación detallada de los acontecimientos o de los escenarios que, en caso de que sucedieran, podrían dar lugar a pérdidas económicas, financieras o reputacionales como consecuencia del incumplimiento de las normas[30].

Para ello, es aconsejable reunirse con los responsables de aquellas áreas de la organización que manejen flujos económicos, contractuales, de personal, o de información, ya sean de la propia organización, de clientes o de proveedores.

---

[29] SÁIZ PEÑA, C.A.; (Coord.), *Compliance: Cómo gestionar los riesgos normativos en la empresa*. Thompson Reuters Aranzadi. Pamplona, 2015. Pp. 534 y ss. Bloque III: Fases de implantación de un Programa de Compliance.

[30] GONZÁLEZ RUISÁNCHEZ S., *Compliance: Sistemas de Cumplimiento y Gestión del Riesgo empresarial*. Universidad de Salamanca. Máster Compliance. Salamanca.

En segundo lugar, **el Análisis del nivel riesgo:** a partir de los riesgos identificados en las Entrevistas de Evaluación mantenidas con los responsables de las distintas áreas de la organización se analiza el nivel de los riesgos existentes con objeto de poder evaluar posteriormente la prioridad en su gestión. El nivel de riesgo se obtiene calculando la probabilidad de su concurrencia por su nivel de impacto, diferente en cada organización (se explicará en el apartado 1.2 Análisis del nivel Riesgos Compliance SPYNET).

Y en tercer lugar, **la Evaluación del riesgo:** se trata del proceso de decisión sobre cómo se van a gestionar los riesgos identificados teniendo en cuenta factores como si son asumibles, si son transferibles, si son mitigables cómo y en qué medida.

En los siguientes sub-apartados se ha tratado de reflejar cómo podría ser el desarrollo de esta primera fase de Diagnostico de acuerdo a los hechos planteados.

La información contenida a continuación no es real, todos los hechos, nombres, marcas, referencias y cualquier otro dato son ficticios y han sido inventados para la realización de este trabajo. Salvo referencias a empresas o productos reales de las mismas, que por ser notoriamente conocidos se incluyen únicamente con la finalidad de contextualizar el supuesto, no prendiéndose en ningún momento comprometer su reputación.

1.1 Entrevistas de Evaluación con las cuatro divisiones de negocio:

A continuación se presenta lo que serían los resúmenes de las entrevistas de evaluación con los responsables de las cuatro divisiones de negocio del supuesto de hecho planteado. En un supuesto de implementación real deberían examinarse también aquellas áreas que afecten de forma transversal a la organización como podrían ser Recursos Humanos (elaboración de contratos de trabajadores, gestión de altas y bajas, contratación con los trabajadores etc), Recruiting[31] (procesos de captación y gestión del talento), Administración o contabilidad y finanzas (presupuestos de la empresa), u otros como Comercial, Marketing, etc, que pueden ser comunes en la empresa o particular de cada división de negocio.

[31] En empresas de cierto tamaño, o sectores especializados dónde es esencial el capital humano y cuesta encontrar y atraer trabajadores es común la existencia de un departamento de Recruiting.

En el presente trabajo se quiere ejemplificar cómo se podría implementar un modelo de gestión y organización eficaz, por lo que en relación con este objeto, se ha decidido exponer únicamente la evaluación a las cuatro divisiones de negocio por ser dónde, de acuerdo con el supuesto planteado, existirían más riesgos penales. El objetivo de la plasmación de estas entrevistas es múltiple:

(i) realizar una aproximación al tipo de cuestiones que se deberían considerar durante la fase de diagnostico de una implementación real;

(ii) introducir hechos nuevos con el fin de completar el supuesto;

(iii) exponer algunos aspectos fundamentales a tener en cuenta al analizar una empresa tecnológica;

(iv) poner de manifiesto la dificultad de identificar durante la fase de diagnostico los hechos relevantes de los accesorios;

(v) poner de manifiesto la dificultad de identificar la información veraz a tener en cuenta, ante las incoherencias que sobre el mismo aspecto suelen derivarse de las entrevistas con un responsable y otro.

En relación con este objetivo, durante la entrevista A) se describen algunos aspectos que no aportan información relevante al supuesto, o que cuanto menos, no son tan necesarios para evidenciar los riesgos penales que en este trabajo se quieren comentar. En las siguientes entrevistas solo se incluirá información relevante para desarrollar el supuesto.

A) Entrevista con el responsable de IA Service:

Compañía: SPYNET S.L.

Número de empleados: 400 en nómina aprox.

Cargo: Responsable de IA Service

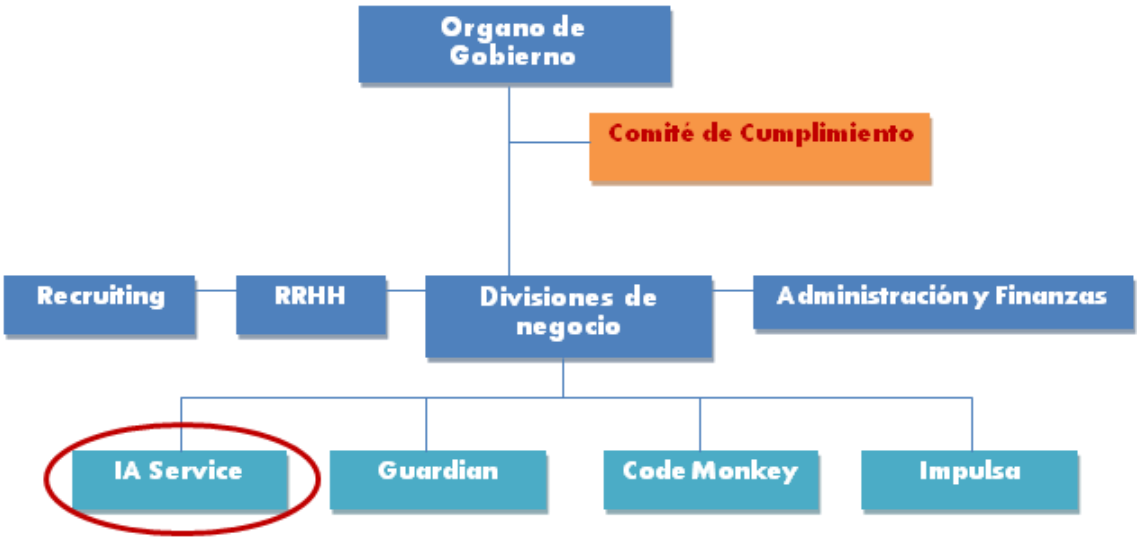
Nombre y apellidos: Francisco Asimov

Correo electrónico: fasimov@spynet.com

Recibí. Firma y Fecha.

X

Francisco Asimov
Director IA Service



Ubicación del área: Zaragoza (España).

Ámbito de actuación: Nacional.

Certificaciones: ISO 9001 de Calidad.

Descripción del área: Desde 2012 el área cuenta con autonomía e independencia tanto económica como organizativa para investigar y desarrollar productos de Inteligencia Artificial (en adelante, IA). Actúa como empresa independiente en todo el proceso de investigación y desarrollo, no obstante, la producción y comercialización de todos los productos, así como las condiciones de entrada al mercado es decidida de forma unilateral por la dirección de SPYNET.

El área se divide en tres grandes departamentos:

- Desarrollo e Investigación
- Diseño
- Testeo & Feedback

Recursos Humanos del área: El área actualmente está compuesta por unos 25 trabajadores aproximadamente.

Facultades de organización y control: Francisco Asimov es el máximo responsable del área, tiene facultades de organización y control sobre todo el personal de IA Service. Sin embargo, no tiene atribuida ninguna facultad de organización sobre el resto del

personal de SPYNET, su trabajo consiste coordinar los tres departamentos de IA Service y controlar toda la cadena de desarrollo del producto.

Poderes: Francisco tiene poderes para actuar en nombre y representación de SPYNET como director de IA Service. Se solicita evidencia de tales poderes.

DPTs (Descripción del puesto de trabajo): Existen DPTs y se actualizan cada año para poder obtener la 9001. Se solicita como evidencia un DPT de cualquier trabajador con los datos tachados.

Sistema de Reporting: Todos los trabajadores de IA Service reportan a Francisco cualquier tipo de incidencia o problema que tengan en el desarrollo del producto. Todos estos reportes se registran en la herramienta de Ticketing (INFORMER, herramienta propia). En ocasiones Francisco envía estos tickets al responsable de Code Monkey, solicitando apoyo de especialistas de su área. En caso de no poder resolver el reporte Francisco informaría a Dirección de SPYNET.

Reuniones en las que participan: Semanalmente o cuando sea necesario Francisco participa en reuniones con los responsables de los tres departamentos del área. Cada mes aproximadamente se reúne con Dirección de SPYNET e informa de los resultados de los nuevos proyectos.

Almacenamiento de la información de los proyectos: Toda la información generada en el desarrollo de nuevos productos de IA Service se almacena en el CPD (Centro de Procesamiento de Datos) de Guardian en Zaragoza. Las copias de seguridad en cambio se almacenan en los servidores de Guadalajara.

Almacenamiento de la información económica y contable: Toda la información económica relacionada a los presupuestos del área se encuentra en GHC, software licenciado con mantenimiento almacenado en el CPD de Guardian en Zaragoza. La contabilidad es realizada directamente por Administración y Finanzas. El pago de nominas se realiza directamente por RRHH de SPYNET.

Acceso a información económica de la empresa: Francisco solo tiene acceso a los presupuestos que cada año se le asignan desde Dirección. El resto de la información económica de la empresa es gestionada exclusivamente por Administración y Finanzas.

Autorización de gastos y pagos: Francisco tiene autorización para realizar con plena autonomía todo tipo de pagos y hacer frente a cualquier gasto necesario para el desarrollo de los productos de IA Service, teniendo como único limite el presupuesto anual.

Documentación de los pagos: Francisco justifica a través de GHC cada gasto, siendo Administración quien realiza un control de los mismos. Todos los gastos que se realizan en el área se hacen con su consentimiento.

Manejo de dinero en metálico: Francisco nos comenta que si en algún momento resulta necesario realizar algún pago en metálico, él u otra persona que tenga que hacer el pago, lo realiza y posteriormente con el ticket de compra correspondiente pide a Administración que se le abone en su nomina a final de mes.

Tarjetas de crédito: Francisco tiene tarjeta propia de empresa. Los responsables de los distintos departamentos del área tienen los datos de esta tarjeta y si necesitan realizar algún pago piden autorización a Francisco y éste autoriza el gasto.

Proveedores: SPYNET realiza la contratación de todos los proveedores de las distintas áreas. La producción de los productos de IA Service se ha externalizado y se ha contratado con Zaragoza Productora Industrial S.L., (en adelante, ZPI) la fabricación de todos los componentes de los diferentes productos así como el ensamblaje y empaquetado final, que es realizado por SONBEL S.A, a través de una subcontrata con ZPI. Se solicitan como evidencia ambos contratos.

Datos de los proveedores: Los datos de estos proveedores se almacenan en GHC en el CPD de Zaragoza.

Reputación de los proveedores: No se ha analizado la reputación de ninguno de ellos, se confía en ellos por su marca y por la buena experiencia que han tenido durante los años en los que han colaborado.

Software utilizado en el área:

Herramienta	Función	Licencia

Paquete Office	Diversas funciones	No todos los programas están licenciados
INFORMER	Ticketing	Software propio
GHC	ERP Contabilidad, Proveedores, recursos, etc.	Sí
Intranet de SPYNET	Correos electrónicos	Software propio
Autocad	Diseño de productos	Sí
Corel	Diseño de productos	No

Todas las herramientas que utilizan en el área almacenan su información en el CPD de Zaragoza. La Intranet y las copias de seguridad de producción se almacenan en los servidores de Guadalajara. El Paquete Office se aloja en local en cada equipo de los trabajadores.

Software ilegal: Hay programas que no están licenciados, sabe que el paquete Office es pirata ya que no se usa mucho y otros programas como el Corel que se usan de forma puntal aunque habitual provienen de una remesa de licencias que se adquirieron hace unos tres años pero que ya expiró. No hay un registro de los programas licenciados ni una política de renovación de licencias. Las licencias se adquieren desde Administración por orden directa de Dirección.

Auditorias: No se han realizado auditorias de software por lo que no se tiene constancia de los programas que pueda haber instalados en cada equipo. Cada usuario tiene permisos de administrador sobre su propio equipo.

Activos de la empresa: SPYNET facilita todos los activos necesarios para la realización del trabajo. Cada usuario cuenta con un equipo portátil que se le entrega en el momento de su incorporación. Este ordenador se asocia a la dirección de correo corporativo del trabajador. Sólo los responsables de cada área tienen móviles de

empresa. No hay una política que prohíba llevarse los equipos a casa, sin embargo casi nadie lo hace ya que los equipos no pueden almacenar información en local por configuración (salvo archivos Office). En alguna ocasión por cuestiones de eficiencia se ha creado una VPN para que algún trabajador pueda acceder a la red de SPYNET a distancia y así seguir trabajando en algún viaje.

Inventario de activos: Todos los ordenadores se encuentran debidamente registrados en un inventario gestionado por Guardian. Sin embargo, no hay ninguna política que regule tal inventario. La forma de actuación normal nos comenta el responsable es registrarlo en el momento de entrega, aunque debería verificarse con el responsable de Guardian.

BYOD: No existe una política de BYOD que regule en uso de dispositivos propios en la empresa. Los trabajadores tienen permitido tener en su móvil personal el correo corporativo. No se restringe tampoco el uso de los mismos en la empresa.

Correo corporativo: Los correos corporativos son gestionados desde la Intranet de SPYNET. Guardian se encarga de crear y eliminar las cuentas de correo electrónico.

Medidas de seguridad: El responsable del área desconoce las medidas de seguridad que aplican sobre las herramientas que utilizan en el área. Tampoco conoce las aplicadas sobre el correo electrónico y la red de la empresa. Deberá preguntarse al responsable de Guardian. Reconoce que pese a ser necesario no se aplican medidas de ciberseguridad específicas sobre los productos de IA Service, únicamente se realizan análisis estáticos en la fase de implementación (*in-programming*), pero no se realizan análisis estáticos en fase de pruebas, análisis dinámicos ejecutando el programa[32], ni se realizan pentestings[33] en situación de funcionamiento real para descubrir vulnerabilidades. El nuevo producto, P3CO presenta importantes vulnerabilidades en su diseño que por plazos de lanzamiento impuestos por Dirección de SPYNET no han

[32] MOOC: *Ciberseguridad entender los ataques para desplegar contramedidas. Módulo 5 Contramedidas a nivel de servicios, aplicación y metodologías*. Universidad Rey Juan Carlos. Madrid. «A la hora de desarrollar un programa se hace necesario analizar el código para detectar posibles errores que deriven en un fallo de seguridad. [...] Podemos realizar el análisis del código sin ser ejecutado (análisis estático) o durante su ejecución (análisis dinámico)»

[33] Test de penetración o de intrusión, son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar.

podido ser subsanados. Se identifica como riesgo alto el lanzamiento de P3CO esencialmente por los datos personales a los que va a tener acceso.

Notificación brecha de seguridad: No hay implementado ningún canal ni se ha adoptado ninguna política de notificación de incidencias de seguridad. En caso de ocurrir los trabajadores reportarían a Francisco y este reportaría a Guardian a través de la herramienta Ticketing o dependiendo de la gravedad por teléfono y posteriormente se registraría en INFORMA.

Robo/perdida de activos: Tampoco se ha adoptado ninguna política que regule este aspecto. En caso de que un algún responsable perdiese un móvil de empresa o un ordenador portátil Francisco reportaría a Guardian para el cambio de contraseña del correo.

Destrucción de activos: Cuando un equipo deja de funciona o decide destruirse por la razón que sea, se envía a Guardian y ellos se encargan de la destrucción. Deberá hablarse de esto con ellos.

Sistema de Back up: Ningún trabajo de IA Service se almacena en local. Se trabaja en local, pero toda la información generada se almacena automáticamente en el NAS de SPYNET (Intranet) alojado en el CPD de Zaragoza. Esta información se vuelca semanalmente en los servidores de Guadalajara a través de copias incrementales. Cada dos meses se realizan copias completas del servidor de Zaragoza a los de Guadalajara. No existe una política que regule cómo deben realizarse estas copias.

Data Loss Prevention: No se cuenta con ningún sistema de detección de fugas de información. Deberá hablarse con Guardian.

VPN: Salvo casos excepcionales los trabajadores no tienen conexión VPN a la red corporativa ni a las herramientas de producción.

EVIDENCIAS SOLICITADAS:

- Poderes de Francisco
- DPT
- Contratos con los Proveedores del área

- Relación de funciones de los productos de IA Service que presentan riesgos para la protección de datos.

B) Entrevista con el responsable de Guardian:

Compañía: SPYNET S.L.

Número de empleados: 400 en nómina aprox.

Cargo: Responsable de Guardian

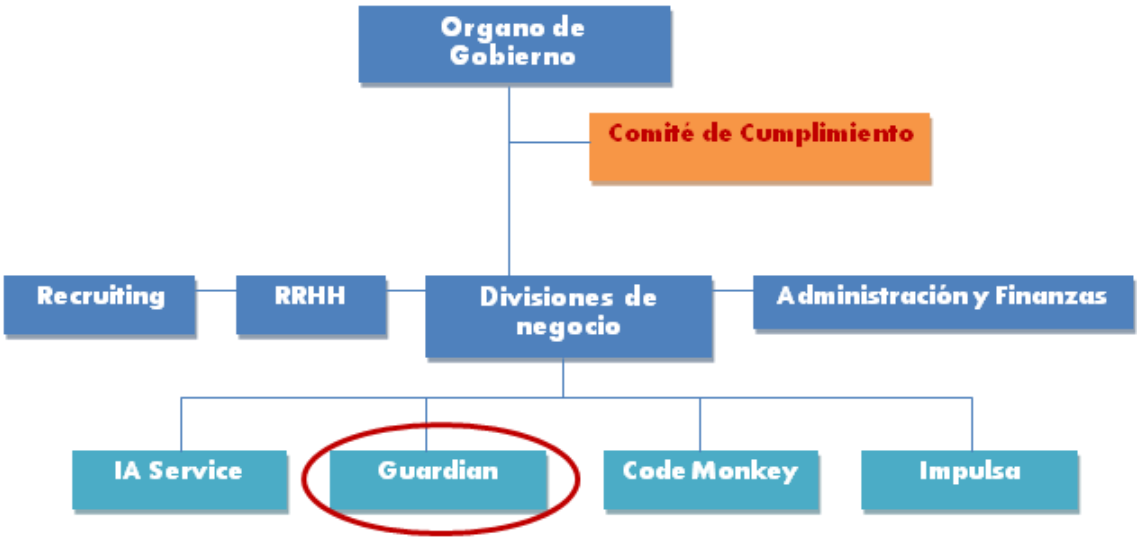
Nombre y apellidos: Pelayo Hurtillo

Correo electrónico: phurtillo@spynet.com

Recibí. Firma y Fecha.

X

Pelayo Hurtillo
Director Guardian



Ubicación del área: Zaragoza y Guadalajara (España).

Ámbito de actuación: Nacional.

Certificaciones: ISO 9001 de Calidad. Se quiere implantar la ISO 27001 de Sistemas de Gestión de Seguridad de la Información pero todavía tiene que aprobarlo Dirección.

Descripción del área: Presta servicios de almacenamiento (Hosting) y copia de seguridad (Back up) tanto a las distintas áreas de SPYNET como a múltiples clientes. Asimismo, se ocupa de la gestión de todos los activos de la compañía, de la intranet (correos electrónicos, NAS y reserva de salas, entre otros), de prestar soporte

informático a los trabajadores y de garantizar un nivel de seguridad en los servidores y en la red corporativa.

El área cuenta con los siguientes departamentos:

- CAU: Centro de Atención al Usuario
- Servicios Gestionados
- Comercial

Recursos Humanos del área: El área actualmente está compuesta por unos 90 trabajadores aproximadamente.

Facultades de organización y control: Pelayo Hurtillo es el máximo responsable del área, tiene facultades de organización y control sobre todo el personal de Guardian. No tiene sin embargo, estas facultades sobre otras áreas de la empresa, salvo en caso de reporte de brecha de seguridad, en ese caso, todos los trabajadores deberían seguir estrictamente sus instrucciones.

DPTs (Descripción del puesto de trabajo): Existen DPTs y se actualizan cada año para poder obtener la 9001. (No se solicita el DPT, ya que consideramos que con el de IA Service es suficiente).

Sistema de Reporting: Todos los trabajadores de SPYNET reportan a Pelayo cualquier tipo de incidencia de seguridad o problema informático que tengan en relación con sus equipos o el correo corporativo. Todos estos reportes se registran en INFORMER. En caso de no poder resolver el reporte, Pelayo informaría a Dirección de SPYNET.

Reuniones en las que participan: Diariamente se reúne con responsables de Servicios Gestionados, periódicamente Pelayo también participa en reuniones con los responsables de los tres departamentos del área, y con otros responsables de SPYNET. En raras ocasiones trata directamente con clientes, pero normalmente estas funciones son realizadas por el departamento Comercial de Guardian. En cambio, el cierre de contratos con proveedores (encargados del tratamiento, proveedores de sistemas, material informático, etc.) corresponde a Pelayo en última instancia.

Almacenamiento de la información de los proyectos: La principal actividad de Guardian consiste en la prestación de servicios de Hosting a clientes de SPYNET, sin

embargo, es también el área encargada de almacenar y custodiar toda la información de la propia empresa. Guardian funciona del siguiente modo:

- **Información de clientes**: Los clientes de Guardian son en su totalidad clientes de SPYNET. Algunos clientes provienen de labores de captación realizadas por el departamento comercial de Guardian, en nombre de SPYNET, pero en la mayoría de los casos son clientes de SPYNET a los que previamente se les ha prestado algún servicio desde Impulsa o aplicaciones desarrolladas por Code Monkey. Esta información de clientes normalmente es almacenada en el CPD de Guadalajara, sin embargo, desde 2016 se ha comenzado a almacenar datos en el hierro de terceros (Amazon, Linode, y Data&Coin). Se solicita evidencia de los contratos con estos sub-encargados del Tratamiento.
- **Información de SPYNET**: Toda la información generada durante la producción de proyectos en SPYNET es almacenada en los servidores de Guardian. Durante muchos años el almacenamiento se hacía siempre de la misma forma: todos los datos de producción se almacenaban en Zaragoza y las copias de seguridad se hacían siempre en los servidores de Guadalajara. Sin embargo, algunos de los últimos proyectos han requerido externalizar las copias de seguridad a diversos Encargados del Tratamiento (Amazon, Linode y Data&Coin). Por otro lado, SPYNET es el Responsable del Tratamiento de todos los datos generados en sus propios productos IoT (Internet of Things) desarrollados por IA Service. Estos productos generan gran cantidad de datos que se hace necesario externalizar, actualmente se ha contratado con Data&Coin el almacenamiento de todos los datos generados por estos productos. Se solicita evidencia de dicho contrato.

Almacenamiento de la información económica y contable: Toda la información económica relacionada a los presupuestos del área se encuentra en GHC, software licenciado con mantenimiento almacenado en el CPD de Guardian en Zaragoza. La contabilidad es realizada directamente por Administración y Finanzas. El pago de nominas se realiza directamente por RRHH de SPYNET.

Autorización de pagos: Pelayo tiene autorización para realizar pagos en nombre de SPYNET, normalmente derivan de contratos con Proveedores. En ocasiones Pelayo delega en sus trabajadores la realización de ciertos pagos, pero todos los pagos que se realizan en el área se hacen con su consentimiento.

Documentación de los pagos: Pelayo justifica a través de GHC cada gasto, siendo Administración quien realiza un control de los mismos.

Tarjetas de crédito: Pelayo tiene tarjeta propia de empresa. Los responsables de los distintos departamentos del área tienen los datos de esta tarjeta y si necesitan realizar algún pago piden autorización a Pelayo y éste, previa consulta con Administración, autoriza el gasto.

Firma electrónica: Pelayo tiene firma electrónica para representar a SPYNET como Director de Guardian.

Proveedores: Todos los contratos con proveedores se realizan en nombre de SPYNET. En Guardian corresponde a Pelayo buscar los proveedores y gestionar los contratos con ellos. Los principales proveedores del área son BlueComputer S.L., y Zgz Sistem S.L., con quienes se tiene contratada la compra de equipos informáticos y otros activos. Se solicita evidencia de estos contratos.

Desde 2016 la empresa se ha visto obligada a externalizar el almacenamiento de muchos datos de clientes y de las propias aplicaciones y productos de SPYNET ofrecidos a clientes (numerosas bases de datos de aplicaciones desarrolladas para clientes, páginas web, o incluso "Cynthia" y otros servicios de IA Service). Se prevé que todos los datos generados por P3CO, el nuevo robot de IA Service sean almacenados en los servidores de Data&Coin. Entre estos datos según comenta Pelayo, seguramente haya numerosos datos especialmente protegidos[34] (imagen/voz de menores, gustos y preferencias, aficiones, enfermedades, historial médico, etc.) ya que el robot tiene como función principal el cuidado de niños.

Datos de los proveedores: Los datos de estos proveedores se almacenan en GHC en el CPD de Zaragoza. Guardian guarda un registro de todos los proveedores y Encargados del Tratamiento con los que trabaja.

Reputación de los proveedores: No se analiza la reputación de ninguno proveedor, se tienen en cuenta las condiciones económicas y los servicios ofrecidos. Muchas veces el

[34] El Reglamento General de Protección de Datos (UE) (GDPR, por sus siglas en inglés), ya no clasifica los datos en datos de nivel alto, medio, bajo, como hacía la LOPD del 1999. Ahora se distingue entre datos básicos y datos especialmente protegidos.

precio que damos al cliente final determina conseguir o no ese cliente, explica el responsable del área.

Software utilizado en el área:

Herramienta	Función	Licencia
Paquete Office	Diversas funciones	No todos los programas están licenciados
INFORMER	Ticketing	Software propio
GHC	ERP Contabilidad, Proveedores, recursos, etc.	Sí
Intranet de SPYNET	Gestión de Correos electrónicos	Software propio
XcL Power	Firewall Perimetral y otras medidas de seguridad	Sí
Diversos software propios	Medidas de seguridad (cifrado red, pasarela correo, etc).	Software propio

Software ilegal: Hay programas que no están licenciados, sabe que el paquete Office es pirata ya que no se usa mucho. Todos los programas que usa la unidad cree que están licenciados, no obstante las licencias las gestiona Administración. Todos los programas de XcL Power para las medidas de seguridad sí que están licenciados y se renuevan cada año.

Auditorias: No se han realizado auditorias de software. Cada usuario en SPYNET tiene permisos de administrador sobre su propio equipo.

Activos de la empresa: Cuando se incorpora un nuevo trabajador desde Guardian se le entrega un equipo portátil. Este ordenador se asocia a la dirección de correo corporativo que le corresponda al trabajador. Todas las personas del departamento comercial tienen móvil de empresa.

Inventario de activos: Todos los ordenadores se encuentran debidamente inventariados según modelo, número de serie, sistema operativo, configuración y persona asignada. No hay ninguna política que regule tal inventario, pero se actualiza cada año con el cierre de presupuestos.

Correo corporativo: Guardian gestiona los correos corporativos desde la Intranet de SPYNET, asigna una dirección de correo electrónico a cada trabajador al incorporarse en la empresa y les da de baja cuando estos dejan la empresa.

Medidas de seguridad: Verificadas las medidas de seguridad implementadas por Guardian para garantizar la seguridad de la información en SPYNET, se observa un alto nivel de seguridad tanto lógica como física en el almacenamiento de los servidores de propios de Guardian, en los equipos (cifrados en local) y en el tránsito de información en la Red (cifrada con software propio) e Intranet de SPYNET mediante firewall perimetral, una pasarela de correo (filtrado de virus, spam etc.), y un *Apliance* que desecha todo el contenido no deseado y genera un informe de actividades.
No obstante, se observan ciertos vacios regulatorios en cuanto a la seguridad de los accesos lógicos a servidores y plataformas gestionadas por parte del personal de Guardian, teniendo todas las personas del departamento acceso sin restricción a toda la información almacenada por la empresa, tanto propia como de terceros, sin guardar trazabilidad de los accesos y operaciones en estas plataformas.
Asimismo, se evidencia la necesidad de tener identificadas las medidas de seguridad aplicadas por los terceros a los que se transfieren datos de SPYNET, tanto en el almacenamiento primario como en copia de seguridad. Lo que hace fundamental comprobar la idoneidad de las medidas de seguridad adoptadas por el encargado de realizar las copias de seguridad.

Notificación brecha de seguridad: No hay implementado ningún canal ni se ha adoptado ninguna política de notificación de incidencias de seguridad. En caso de ocurrir los trabajadores reportarían a Pelayo a través de la herramienta Ticketing. No

hay previstos procedimientos para realizar notificaciones en caso de brecha de seguridad a afectados ni a autoridades de control.

Robo/perdida de activos: No hay ninguna política que regule este aspecto. En caso de que un algún responsable perdiese un móvil de empresa o un ordenador portátil y se lo reportase a Pelayo, éste o alguna persona delegada cambiaria la contraseña del correo corporativo.

Destrucción de activos: No se ha contratado ningún servicio de destrucción de activos con terceros especializados. Todas las áreas de SPYNET remiten a Guardian los equipos que ya no sirven y alguna persona del área se encarga de hacer la destrucción física de los discos duros (se taladran), y posteriormente se llevan al punto limpio.

Sistema de Back up: Toda la información de producción generada en SPYNET se almacena automáticamente en el NAS de SPYNET (Intranet) alojado en el CPD de Zaragoza. Esta información se vuelca semanalmente en los servidores de Guadalajara a través de copias incrementales. Cada dos meses se realizan copias completas del servidor de Zaragoza a los de Guadalajara. La información de los clientes, y la generada por los productos comercializados se almacena en muchas ocasiones en servidores de terceros, las copias de seguridad principalmente están contratadas con Data&Coin.

Data Loss Prevention: SPYNET no cuenta con ningún sistema de detección de fugas de información en servidores, sin embargo, se cuenta con un software propio que informa sobre intentos de accesos maliciosos a la Red corporativa.

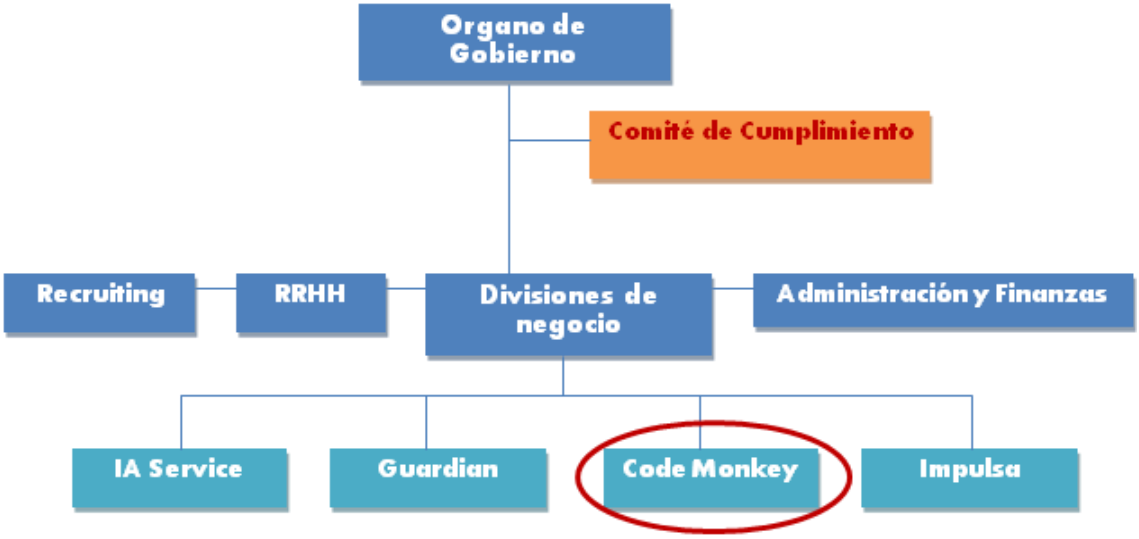
VPN: Salvo casos excepcionales los trabajadores no tienen conexión VPN a la red corporativa ni a las herramientas de producción. Estas VPN están cifradas.

C) Entrevista con el responsable de Code Monkey:

Compañía: SPYNET S.L.
Número de empleados: 400 en nómina aprox.
Cargo: Responsable de Code Monkey
Nombre y apellidos: José María Marrano
Correo electrónico: jmmarrano@spynet.com
Recibí. Firma y Fecha.

X

José María Marrano
Director Code Monkey



Ubicación del área: Zaragoza (España).

Ámbito de actuación: Nacional.

Certificaciones: ISO 9001 de Calidad.

Descripción del área: La principal línea de trabajo de Code Monkey consiste en el desarrollo de software por encargo de clientes. Se trata de proyectos muy grandes en los que se parte de cero y el cliente quiere un producto concreto sobre el que tener el control absoluto. No obstante, es también bastante común realizar proyectos a partir de software de terceros. Por ejemplo, proyectos de e-commerce a partir de los patrones de Magento. Habitualmente se trabaja en el desarrollo de software propio de SPYNET para otros departamentos especialmente IA Service, suele requerir proyectos bastante complejos, e Impulsa para proyectos más sencillos.

Recursos Humanos del área: El área actualmente está compuesta por unos 130 trabajadores aproximadamente.

Facultades de organización y control: José María es el máximo responsable del área, tiene facultades de organización y control sobre todo el personal de Code Monkey. Sin

embargo, no tiene atribuida ninguna facultad de organización sobre el resto del personal de SPYNET.

Almacenamiento de la información de los proyectos: Toda la información generada en el desarrollo de nuevos productos de Code Monkey se almacena en el CPD (Centro de Procesamiento de Datos) de Guardian en Zaragoza. Las copias de seguridad se almacenan en los servidores de Guadalajara y en los de Data&Coin.

Acceso a información económica de la empresa: José María no tiene acceso a información económica de la empresa. Toda la información económica de la empresa es gestionada exclusivamente por Administración y Finanzas.

Autorización de gastos y pagos: José María no tiene autorización para realizar pagos en nombre de SPYNET, cuando necesita realizar algún pago solicita autorización a Administración general.

Proveedores: Toda la contratación con proveedores se realiza en nombre de SPYNET. Los únicos proveedores del área son BlueComputer S.L., y Zgz Sistem S.L., con quienes se tiene contratada la compra de equipos informáticos y otros activos. Se solicita evidencia de estos contratos

Datos de los proveedores: Administración tiene estos datos.

Reputación de los proveedores: El responsable desconoce si se ha analizado la reputación de los proveedores.

Software utilizado en el área:

Herramienta	Función	Licencia
Paquete Office	Diversas funciones	No todos los programas están licenciados
INFORMER	Ticketing	Software propio
Intranet de SPYNET	Correos electrónicos	Software propio
Magento	Desarrollo e-commerce	No en todos los equipos

Python	Desarrollo de código	Open Source
OpenJDK	Desarrollo de código	Open Source
Java	Desarrollo de código	No
C	Desarrollo de código	No
Otros programas	Desarrollo de código	Open Source/No

Software ilegal: No hay un registro de los programas licenciados ni una política de renovación de licencias. Se usan muchos programas de código abierto sin embargo, hay muchos que no están licenciados. En ocasiones, para un proyecto es necesario utilizar un programa concreto para una función concreta y puntual, en estos casos, el responsable de proyecto suele autorizar que los trabajadores descarguen software pirata, aunque en muchas ocasiones los trabajadores lo hacen por su cuenta si se trata de gestiones rapidas.

Auditorias: No se han realizado auditorias de software por lo que no se tiene constancia de los programas que pueda haber instalados en cada equipo. Cada usuario tiene permisos de administrador sobre su propio equipo.

D) Entrevista con el responsable de Impulsa:

Compañía: SPYNET S.L.

Número de empleados: 400 en nómina aprox.

Cargo: Responsable de Impulsa

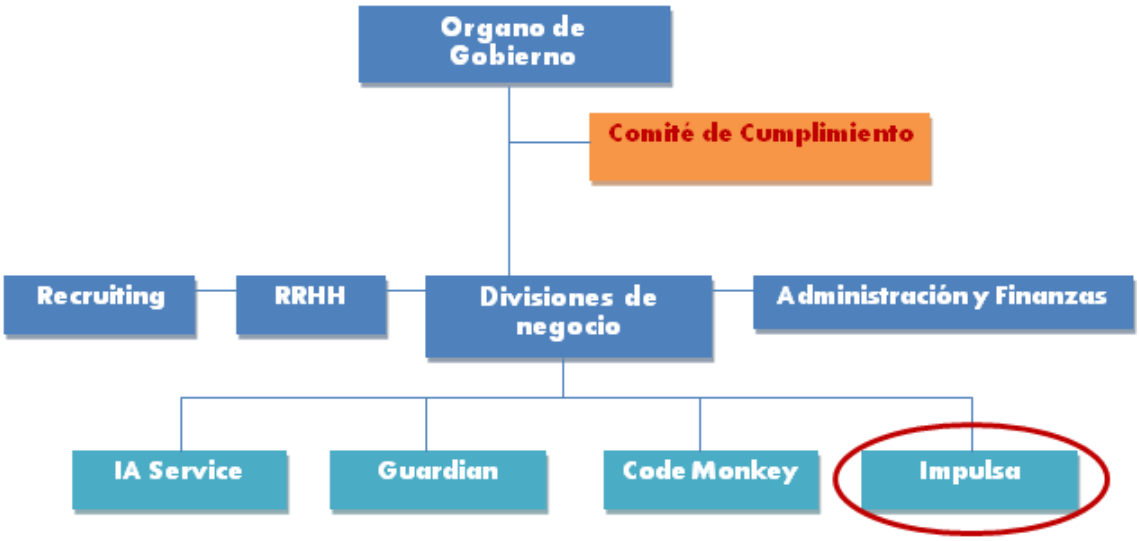
Nombre y apellidos: Eduardo Rolpán

Correo electrónico: erolpan@spynet.com

Recibí. Firma y Fecha.

X

Eduardo Rolpán
Director Impulsa



Ubicación del área: Madrid (España).

Ámbito de actuación: Nacional.

Certificaciones: ISO 9001 de Calidad.

Descripción del área: Desarrollo, gestión y soporte de plataformas web y aplicaciones informáticas. El departamento tiene como objetivo "impulsar" empresas en el ámbito digital, para ello se trabaja en toda la estrategia de integración digital, desde la creación de una página web desde cero, hasta la optimización en buscadores, elaboración de la estrategia de marketing, refuerzo de la imagen corporativa etc.

El valor añadido del servicio reside esencialmente en los diseños y en el posicionamiento en buscadores que Impulsa consigue.

Recursos Humanos del área: El área actualmente está compuesta por unos 55 trabajadores aproximadamente.

Facultades de organización y control: Eduardo Rolpán es el máximo responsable del área, tiene facultades de organización y control sobre todo el personal de Impulsa. Sin embargo, no tiene atribuida ninguna facultad de organización sobre el resto del personal de SPYNET.

Software utilizado en el área:

Herramienta	Función	Licencia

Paquete Office	Diversas funciones	No todos los programas están licenciados
INFORMER	Ticketing	Software propio
GHC	ERP Contabilidad, Proveedores, recursos, etc.	Sí
Intranet de SPYNET	Correos electrónicos	Software propio
Drupal	Diseño web	Open Source
Magento	Desarrollo e-commerce	Sí
Wordpress	Diseño web	Open Source
MySQL	BBDD	Open Source

Software ilegal: Hay programas que no están licenciados, sabe que el paquete Office es pirata.

Auditorias: No se han realizado auditorias de software por lo que no se tiene constancia de los programas que pueda haber instalados en cada equipo. Cada usuario tiene permisos de administrador sobre su propio equipo.

Gestión de dominios: El área se encarga de gestionar los dominios de las webs que desarrollan para los clientes. Realizan la inscripción por encargo y en nombre de los clientes y bajo los términos que ellos establezcan. Los .com se realizan en Whois, y los .es en Red.es.

Marketing digital. Infracción derechos marcarios: Cuando un cliente contrata el desarrollo de una página web, de un e-commerce o de cualquier otra plataforma quiere que esta posicione correctamente en los motores de búsqueda. Para ello, en primer lugar, se crea una estrategia de SEO (Search Engine Optimization) desde el diseño en todo proyecto. Es decir, se tiene en cuenta factores como la densidad de las palabras que

aparecen en cada página, la prominencia de las palabras (uso de negritas, títulos, anchor text, breadcrumbs, etc.), la estructura de la web, la velocidad del sitio, los enlaces que se indexan, etc. Habitualmente, se incrustan *meta tags*[35] en el código fuente para conseguir un mejor resultado. En ocasiones se ha usado el nombre de una marca o de un producto de la competencia que pudiera interesar para relacionar la web a ese contenido.
En segundo lugar, cuando un cliente contrata servicios de SEM (Search Engine Marketing) se realizan campañas de *adwords*[36] utilizando las *keywords* más buscadas para ese tipo de servicios, o incluso haciendo referencia a marcas o productos de la competencia.

1.2 Análisis del nivel Riesgos Compliance SPYNET

En este apartado se presenta de forma muy resumida lo que sería un informe de los riesgos penales que pueden afectar a SPYNET en el desempeño de su actividad. Como ya se ha comentado, el nivel de riesgo se obtiene calculando la probabilidad de su concurrencia por su nivel de impacto en la organización. Es importante ser meticuloso en este aspecto e ir al caso concreto, debido esencialmente a que, por ejemplo, los daños reputacionales derivados de un delito de revelación de secretos del 197 CP no serían iguales en una empresa como SPYNET que almacena millones de datos personales, que en una fábrica de piezas suministradas donde difícilmente se vería afectada la intimidad de personas. Asimismo, algunos delitos no aplicarán pues no va a ser igual la probabilidad de tráfico de órganos en un hospital que en una empresa como SPYNET.

En un supuesto de implementación real se hace necesario, o al menos muy recomendable, el uso de herramientas informáticas especificas que permitan evaluar exhaustivamente la probabilidad e impacto de cada tipo delictivo aplicable, guardando

[35] LÓPEZ-TARRUELLA MARTÍNEZ A., (Direc.); GRACÍA MIRETE C.M. (Coord.), "*DERECHO TIC: Derecho de las tecnologías de la información y de la comunicación*" TIRANT LO BLANCH. Valencia, 2016. Pg. 114. «Son palabras clave incluidas en el código fuente de una página web (y por tanto invisibles para la inmensa mayoría de los usuarios) que describen su contenido para ayudar a los motores de búsqueda a identificarlo y dirigir el tráfico online atendiendo a las diferentes búsquedas llevadas a cabo por los usuarios».

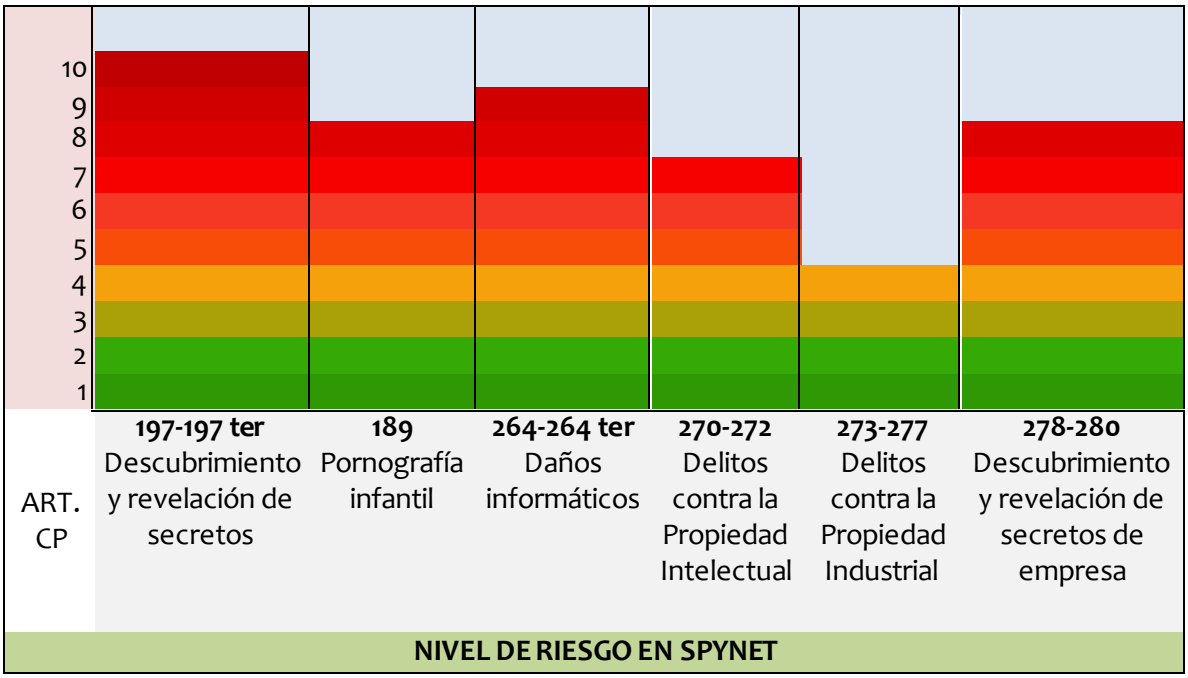
[36] LÓPEZ-TARRUELLA MARTÍNEZ A., (Direc.); GRACÍA MIRETE C.M. (Coord.), "*DERECHO TIC: Derecho de las tecnologías de la información y de la comunicación*" TIRANT LO BLANCH. Valencia, 2016. Pg. 107. «En términos estrictos, el término *adwords* se emplea para denominar un sistema de publicidad empleado por Google y otros operadores que permite a un determinado agente económico (anunciante) "reservar" una serie de palabras clave o *keywords* de tal modo que cuando un internauta introduce dichas palabras clave en el motor de búsqueda, en una sección concreta de los resultados que le son devueltos (anuncios patrocinados) aparecen referencias directas al anunciante en cuestión. Por su parte, cada vez que un usuario hace clic en el anuncio patrocinado, y accede a la página web de la empresa que ha contratado el servicio, ésta paga a Google, o al operador correspondiente, un precio acordado de antemano».

una evidencia del nivel de riesgo que, en primer lugar, facilite la elaboración del informe entregable al cliente, y en segundo lugar, permita llevar un control de los riesgos identificados y medidas aplicadas para poder ser mejoradas por el Comité de Cumplimiento o por el *Compliance Officer* en posteriores revisiones. No obstante, debido a que esto es un trabajo de fin de máster se ha preferido no utilizar ni hacer mención de ninguna herramienta de terceros, sin embargo, para ofrecer una visión más completa del resultado de este análisis se incluyen dos gráficas representativas del nivel de riesgo, una a nivel global de la compañía y otra según el nivel de riesgo de cada área funcional evaluada.

A) Riesgos identificados en SPYNET:

Analizadas las Entrevistas de Evaluación mantenidas con los responsables de las diferentes áreas de negocio se han identificado como potenciales riesgos penales los reflejados en el mapa de riesgos que se presenta a continuación. De estos delitos advertidos como aplicables se ha estudiado de forma individualizada la valoración del nivel riesgo teniendo en cuenta la probabilidad de su comisión y su nivel de impacto en la organización, considerando los eventuales daños reputacionales, económicos y la responsabilidad civil que pudiera derivar del delito de conformidad con el art. 120. 4º CP.

El nivel de riesgo se mide del 1 al 10 siendo el 1 la menor probabilidad de impacto y 10 el máximo.



Para obtener el nivel de riesgo existente en SPYNET se han analizado individualmente los riesgos advertidos en cada una de las áreas de negocio referidas en la Fase de Diagnostico, teniendo en consideración la probabilidad e impacto de los mismos a través de factores como: la actividad de SPYNET, el historial de la empresa y sus proveedores, la cultura de cumplimiento existente, y otros aspectos relacionados con el personal que pueden extraerse de las Entrevistas de Evaluación.

Los riesgos identificados/expuestos en este trabajo resultan suficientes para cumplir con el propósito didáctico de este trabajo. No obstante, debe señalarse que en un supuesto de implementación real deberían analizarse igualmente las áreas que operan transversalmente en SPYNET, véase RRHH, Administración y Finanzas, Recruiting y Dirección General. Asimismo, podrían concurrir otros riesgos como delitos contra los derechos de los trabajadores, estafas, frustración a la ejecución, negativa a actividades inspectoras, etc, que se ha preferido dejar al margen del presente trabajo.

Expliquemos a grandes rasgos porqué se ha considerado que existe riesgo de comisión de estos delitos:

- **Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio como el descubrimiento y revelación de secretos (197-197 ter CP):**

Estudiadas la Entrevistas de Evaluación y las evidencias solicitadas a los responsable de las diferentes áreas, se verifica que no existen contratos de Encargado del Tratamiento adaptados a las exigencias del GDPR, lo que, por un lado, podría derivar importantes perjuicios económicos para SPYNET, con multas administrativas de hasta 10.000.000 EUR o, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía[37]. Por otro lado, muy probablemente de ese defecto organizativo podría derivar responsabilidad penal o civil de SPYNET. Quien, en nuestra opinión, concurre una absoluta falta de diligencia *in eligendo*, esencialmente por haber elegido como principal Encargado el Tratamiento a Data&Coin Inc., y externalizar en esta empresa, todo o gran parte, de su sistema de copias de seguridad, sin realizar ningún tipo de verificación

[37] Art. 83.4 del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (por sus siglas en inglés GDPR).

sobre las medidas de seguridad que ésta aplica sobre los datos transmitidos, ni dar ningún tipo de directriz sobre el tratamiento de los mismos.

Situación que se agrava considerablemente debido a que Data&Coin se vio en 2015 involucrada en varios escándalos por cesión de datos no consentida con fines comerciales (cesión de bases de datos personales, elaboración de perfiles con fines publicitarios, venta de información confidencial y secretos de empresa, etc.). Al no suscribir un Contrato de Encargado del Tratamiento con Data&Coin, nada impide a esta última usar esos datos con fines comerciales y/o para finalidades sustancialmente distintas a las que los interesados consintieron al ceder sus datos a SPYNET como Responsable del Tratamiento.

Esta falta de diligencia, sin duda favorece la comisión de graves delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio como el descubrimiento y revelación de secretos de los arts. 197 a 197 ter del Código Penal. No se pretende ahora hacer un análisis exhaustivo de los requisitos del tipo, ni de si eventualmente concurrirían los elementos necesarios del art. 31 bis del Código Penal para derivar responsabilidad penal de la persona jurídica, sin embargo, se identifica como un riesgo muy alto que debe gestionarse inmediatamente.

- **Pornografía infantil (art. 189 CP):**

Las mismas circunstancias explicadas en el apartado anterior se agravan en áreas como IA Service dónde sus productos (específicamente analizados por el equipo de HLT) captan datos personales especialmente protegidos que afectan a lo más profundo de la intimidad de las personas (imágenes y voz de personas, menores, hábitos, gustos, aficiones, planos de la casa, correos electrónicos de tipo personal, etc.), o incluso imágenes de menores más comprometidas, como las que pueden ser captadas por P3CO en el desempeño de algunas de sus funciones (ayudar a los niños a cambiarse y ducharse) que utilizadas con fines sexuales podrían dar lugar a la de comisión de delitos de pornografía infantil del art. 189 del Código Penal, o en todo caso, a una altísima indemnización por responsabilidad civil subsidiaria, pues como se desprende de las Entrevistas de Evaluación, debido a los plazos de lanzamiento impuestos por Dirección general, y a la falta de implementación de medidas de seguridad suficientes (análisis estáticos, dinámicos, test de intrusión, listas de vulnerabilidades, cifrado de los datos, falta de diligencia en el almacenamiento, etc.), el nuevo producto de IA Service presenta graves vulnerabilidades que en cualquier momento podrían ser explotadas por los

atacantes, con alta probabilidad de causar una brecha de seguridad que comprometa la confidencialidad de la información almacenada. Por todo ello y, con carácter particular se recomienda suspender el lanzamiento de P3CO hasta que se subsanen las vulnerabilidades del producto.

- **Daños informáticos (arts. 264-264 ter CP):**

Guardian es el Responsable del Tratamiento de cientos de empresas, algunas de ellas competencia directa o indirecta de SPYNET, situación que podría ser aprovechada por la compañía para obtener un beneficio directo o indirecto. Por ejemplo, se identifica como riesgo la capacidad del personal de Guardian de destruir, alterar o hacer inaccesibles datos de la competencia o de terceros alojados en sus servidores con objeto de adelantar su posición respecto de los otros, o de obtener una recompensa por parte de otro, lo que supondría la comisión de un delito de daños informáticos del art. 264.1 del Código Penal.

Igualmente, existe un alto riesgo de provocar denegaciones de servicio en los programas de clientes gestionados por Guardian con objeto de adelantar su posición respecto de otros, o de obtener una recompensa de terceros, dando lugar a la comisión de un delito del art. 264 bis del Código Penal. Del mismo modo, podrían facilitarse las contraseñas de acceso a estas aplicaciones clientes a terceros a cambio de una recompensa (art. 264 ter CP), por lo que se recomienda abordar esta situación adoptando un Sistema de Gestión de Seguridad de la Información en SPYNET, que coordine todas las áreas y ofrezca unas normas de actuación y unos procedimientos que deban ser observados por todo el personal y garanticen la seguridad de la información.

- **Delitos contra derechos de Propiedad Intelectual (arts. 270-272 CP):**

Se ha advertido en todas las áreas de SPYNET la existencia de software ilegal por irregularidades en algunas de las licencias del paquete Office. Se trata de una situación relativamente corriente en muchas empresas, cuya resolución normalmente se encauza mediante la adquisición de las licencias correspondientes. Sin embargo, se ha observado que algunos programas especializados como Corel, Java y C entre otros, esenciales para el desarrollo de productos de SPYNET, no están licenciados o han sido reproducidos de forma fraudulenta. Esta situación de irregularidad supone un riesgo alto para la empresa, pues actualmente se está produciendo la comisión de delitos contra derechos de Propiedad Intelectual, agravados por la especial trascendencia económica del beneficio

obtenido que de conformidad con los art. 271. a) y 272 del Código Penal, darían lugar a una indemnización por daños y perjuicios bastante elevada[38]. Por lo que se recomienda regularizar esta situación inmediatamente, adquiriendo en primer lugar las licencias oportunas de aquellos programas que sean necesarios y, en segundo lugar, estableciendo las medidas adecuadas para impedir que se vuelva a producir esta situación.

- **Delitos contra derechos de Propiedad Industrial (arts. 274-277 CP):**

De la entrevista mantenida con el responsable de Impulsa, D. Eduardo Rolpán, se advierte que actualmente se están realizando campañas de marketing digital que potencialmente suponen un alto riesgo de comisión de infracciones de la marca en Internet, pudiendo llegar a constituir en casos excepcionales un delito contra los derechos de la Propiedad Industrial de los arts. 274 y siguientes del Código Penal.

El Derecho marcario en nuestro país se regula por la Ley 17/2001, de 7 de diciembre, de Marcas. En este sentido, se hace necesario aclarar que los criterios que en el plano *offline* determinan la extensión del derecho del titular de una marca a impedir a terceros utilizar su signo distintivo – el llamado *ius prohibendi* –, y que por tanto, determinan la infracción de la marca, aplican igualmente en el ámbito virtual.

De forma muy resumida, estos criterios son los siguientes[39]:

a) la existencia de un uso no consentido por parte de un tercero: lo que abarcaría el uso de i) cualquier signo idéntico a la marca anterior, para productos o servicios idénticos a los protegidos por la marca; ii) de cualquier signo que, por ser idéntico o similar a la marca anterior y ser los productos o servicios idénticos o afines a los de la marca anterior, implique un riesgo de confusión, iii) y de cualquier signo idéntico o similar a una marca anterior, para productos o servicios que no sean similares a aquéllos para los cuales esté registrada la marca anterior, si ésta fuera notoriamente conocida, y el uso se aprovechara indebidamente de su carácter distintivo.

b) que dicho uso afecte a una de las funciones marcarias: Las funciones marcarias son: i) indicación del origen empresarial; ii) función publicitaria; iii) función de inversión; iv) función de indicación de calidad; v) función condensadora del *goodwill*.

[38] Determinadas conforme a las previsiones del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

[39] LÓPEZ-TARRUELLA MARTÍNEZ A., (Direc.); GRACÍA MIRETE C.M. (Coord.), "*DERECHO TIC: Derecho de las tecnologías de la información y de la comunicación*" TIRANT LO BLANCH. Valencia, 2016. Pp. 103- 116.

c) que dicho uso se lleve a cabo en el tráfico económico: En síntesis, que el uso infractor no se limite a la esfera privada o particular, sino que trascienda al exterior, lo que se cumplirá en todo caso al hablar de usos online.

La jurisprudencia ha extendido el concepto de infracción marcaria en Internet a otros usos de marcas ajenas como keywords en un sistema de adwords, o como Meta tags, siempre y cuando estos usos cumplan con los tres criterios mencionados anteriormente y las particularidades interpretativas introducidas por los tribunales. En el caso de uso de la marca ajena como keywords en un sistema de adwords, se ha confirmado que el anunciante es el responsable de ese uso fraudulento, quedando el operador (Google) exento de responsabilidad[40]. Esta responsabilidad por el uso de la marca ajena como keywords en relación a "productos o servicios", se extiende tanto a los productos y servicios del propio anunciante que contrata y utiliza el sistema de adwords, como a los de terceros, que emplean los servicios de ese anunciante para promocionar sus productos y servicios[41]. Sin embargo, solo habrá infracción cuando el uso afecte a alguna de las funciones de la marca, cuestión que habrá de determinarse caso por caso atendiendo al texto del propio anuncio.

En cuanto al uso de signos distintivos ajenos como meta tags, por su naturaleza y funciones, tiene una gran equivalencia con los keywords, con la salvedad de que éstos operan sobre el posicionamiento orgánico y por tanto tienen capacidad intrínseca de afectar a la función publicitaria de la marca[42], y por tanto, suponen un mayor riesgo de comisión infractora. Se recomienda ofrecer formación a los trabajadores sobre los usos lícitos e ilícitos de la marca en Internet, así como establecer una guía de buenas prácticas en el SEO y SEM elaborada conjuntamente con asesoría jurídica especializada.

- **Descubrimiento y revelación de secretos de empresa (arts. 278-280 CP):**

Como ya se ha mencionado, los servicios de Hosting y Back up prestados por Guardian, de acuerdo con las previsiones de la normativa aplicable de Protección de Datos, otorgan a SPYNET la condición de Responsable del Tratamiento de sus clientes. En el marco de dicha prestación de servicios, se advierte la posibilidad técnica de que

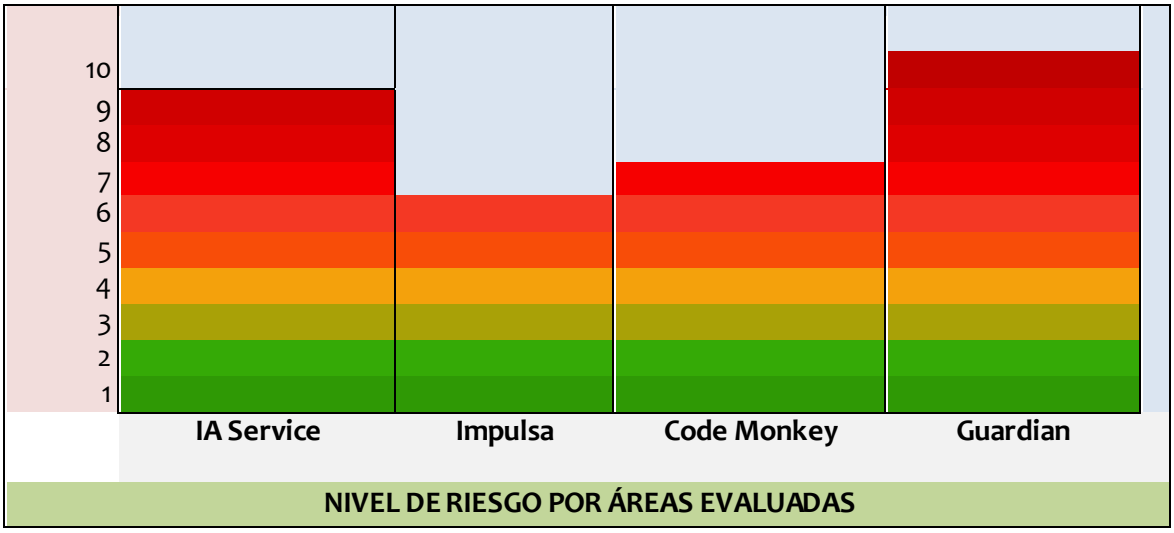
[40] STJUE de 23 de marzo de 2010, C-236/08, "*Google France*", apartados 52, 58 y 59.
[41] STJUE de 12 de julio de 2011, C-324/09, "*L´Oreal*", apartado 91.
[42] STJUE de 11 de julio de 2013, C-657/11, "*Belgian Electronic Sorting Technology*".

personas bajo la estructura organizativa de SPYNET tengan acceso a esos datos, encontrándose alojadas diversas tipologías de datos (datos personales, datos económicos, know how de empresas, secretos industriales, datos económicos, etc.), que sin duda alguna podrían ser de utilidad para SPYNET.

Esta situación, del mismo modo que se ha comentado al analizar el riesgo de comisión de delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, se agrava sustancialmente por la externalización de servicios de Back up a distintos proveedores sin suscribir con ellos contratos de encargado del tratamiento ni verificar siquiera la fiabilidad de los mismos.

B) Nivel de riesgo por áreas:

A continuación se presenta una gráfica representativa del nivel de riesgo existente en cada área de negocio:



1.3 Evaluación del riesgo:

Sobre el análisis de riesgos efectuado pueden realizarse las siguientes recomendaciones[43]:

- Adaptar la empresa al Reglamento Europeo de Protección de Datos (GDPR).
- Adaptar la web corporativa y todas sus intranets a las exigencias de la Ley de Servicios de la Sociedad de la Información (LSSI) y a las previsiones del GDPR, configurando desde el diseño mecanismos que permitan el ejercicio efectivo de

[43] Estas recomendaciones derivan exclusivamente de los delitos identificados y de la información que en el Supuesto de Hecho se ha facilitado, y se presenta únicamente con carácter ilustrativo. En una implementación real habría que tener en cuenta muchos otros aspectos.

los nuevos derechos como el de la limitación de los datos y el derecho a la portabilidad.

- Suscribir Contratos de Encargado del Tratamiento con todos aquellos proveedores a los que se les transfieran datos bajo el control y responsabilidad de SPYNET.
- Suspender el lanzamiento de P3CO hasta que se subsanen las vulnerabilidades de seguridad del producto.
- Contratar con un experto independiente la realización de test de intrusión y análisis dinámicos del código sobre cada nuevo producto previamente a su comercialización.
- Obtener la certificación ISO 27001, o implementar un Sistema de Seguridad de la Información apropiado que garantice la confidencialidad, integridad, autenticidad y disponibilidad de la información según el nivel requerido, mediante controles técnicos en sistemas y el establecimiento de diversas normas de actuación en políticas y procedimientos.
- Se recomienda también la suscripción de un contrato de confidencialidad (NDA) con todos los trabajadores en el momento de su incorporación, y guardar la evidencia de dichos compromisos.
- Regularizar la situación adquiriendo licencias para aquellos programas que sean necesarios y establecer la prohibición expresa de instalar software ilegal en el código Ético.
- Realizar auditorías periódicas de software para saber qué programas hay instalados en los equipos de los trabajadores y elaborar informes anuales sobre los riesgos potenciales de actuaciones ilícitas, o limitar los permisos de administrador estableciendo la prohibición a los trabajadores de instalar o ejecutar en los equipos de la empresa programas sin autorización expresa de su superior.
- Establecimiento de normas de uso adecuado de sistemas informáticos por parte de los usuarios, y normas de BYOD.
- Llevar un control de la adquisición de licencias y renovación de las mismas desde Administración.
- Ofrecer formación a los trabajadores sobre los usos lícitos e ilícitos de marcas en Internet, así como establecer una guía de buenas prácticas en el SEO y SEM elaborada conjuntamente con asesoría jurídica.

- Adopción y difusión del Código Ético o Código de Conducta que regule las normas de actuación que SPYNET quiere alcanzar en el seno de la compañía, poniendo todos los medios necesarios para garantizar su estricto cumplimiento.
- Adopción y difusión del Manual de Prevención de Delitos accesible a todos los empleados.
- Establecer un canal de denuncias internas que permita a cualquier persona comprendida en el alcance del Código de Conducta avisar de cualquier posible actividad delictiva o contraria a la normativa interna de SPYNET.
- Suscribir un seguro de responsabilidad civil frente a Ciberataques.

2. DISEÑO DEL SISTEMA

Una vez identificados los riesgos existentes y clasificados según el resultado de las evaluaciones de impacto, resulta necesario, en conformidad con el párrafo 2º del art. 31 bis. 5 del Código Penal, establecer «los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos». En otras palabras, los controles y las medidas apropiadas para prevenir o reducir la probabilidad de que estos riesgos se materialicen y todas aquellas normas de actuación interna que la empresa ha decidido adoptar, voluntariamente o por imposición de requerimientos legales, y que en adelante regirán el desempeño de su actividad.

Este proceso de formación de la voluntad se concretará en la siguiente evidencia documental:

- Código Ético o Código de Conducta;
- Manual de Prevención de Delitos; y
- Todos aquellos protocolos o procedimientos que desarrollan o concretan las previsiones del Manual de Prevención de Delitos.

La elaboración de esta documentación, independientemente de las ventajas organizativas que trae consigo, permite acreditar la diligencia exigida por nuestro legislador penal, lo que podría suponer la exención o atenuación de la responsabilidad penal, llegado el caso de imputación penal, y también permite acreditar la existencia de unas normas internas, que en caso de infracción pueden avalar consecuencias disciplinares o laborales[44].

[44] SÁIZ PEÑA, C.A.; (Coord.), *Compliance: Cómo gestionar los riesgos normativos en la empresa*. Thompson Reuters Aranzadi. Pamplona, 2015. Pp. 566.

A continuación, se expone de forma sucinta en qué consisten estos documentos, y con objeto de demostrar capacidad del alumno para «abordar el problema planteado desde una perspectiva práctica, que se traduzca en la propuesta de soluciones ante problemas concretos de interpretación o aplicación del Derecho, ajustando esas soluciones a los intereses de los clientes»[45], se proponen una serie de procedimientos que de acuerdo con el supuesto planteado serían «las estrategias más adecuadas» para gestionar los riesgos identificados y generar una cultura de cumplimiento eficaz.

2.1. Código Ético:

El Código Ético o también llamado Código de Conducta es una de las piezas clave que conforman la evidencia documental de un modelo de Compliance. Se trata de un documento interno de naturaleza esencialmente informativa que, sin embargo, es vinculante y debe ser observado por todas las personas que forman parte de la organización o incluso, por aquellas que por su relación con la misma, ha decidido obligarse a cumplirlo. El Código Ético refleja la identidad y los valores de la empresa, las actuaciones que repudia y las pautas de comportamiento profesional que han de seguirse en la operativa de la misma respecto a empleados, clientes, proveedores y cualquier parte interesada que pudiera interactuar con la empresa.

La *práxis* empresarial parece haber aceptado como necesaria la concurrencia de unos contenidos mínimos en todo Código Ético[46], pudiendo ser su estructura la siguiente:

- Introducción: Finalidad del Código y contextualización de la misión, visión y valores de la compañía.
- Objeto y alcance: Establecer a quien aplica el Código. Se trata de un requisito esencial en el caso de grupo de empresas, o en los casos en que se pretende que las empresas que quieran colaborar o ser proveedores se adecuen a los valores de la empresa.
- Principios generales: Máximo respeto a la legalidad, la igualdad, la integridad, la responsabilidad, etc.

  Compromisos de la empresa:

  - Respecto a los trabajadores

[45] Guía docente Trabajo de Fin de Máster. Máster Universitario Abogacía. Curso 2017/2018.
[46] SÁIZ PEÑA, C.A.; (Coord.), *Compliance: Cómo gestionar los riesgos normativos en la empresa.* Thompson Reuters Aranzadi. Pamplona, 2015. Pp. 568-571. Se recomienda su lectura para ampliar información.

- Respecto a los clientes
- Respecto a los proveedores
- Respecto al medio ambiente
- Respecto al Tratamiento de la información: esencial en este caso, reflejar las políticas de confidencialidad y de uso de la información.

- Ámbito relacional: Con clientes, accionistas e inversores, con proveedores, con instituciones públicas, etc.
- Imagen y reputación corporativa
- Cumplimiento y régimen disciplinario
- Denuncia de irregularidades: Se debe imponer la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención, y establecer un canal para ello.
- Identificación del *Compliance Officer* o Comité de Cumplimiento: Se trata de un requisito necesario.
- Fecha de la última actualización. Es recomendable realizar comunicaciones internas cada vez que se produzcan actualizaciones importantes del Código.

El Código Ético para poder cumplir con su finalidad informativa debe necesariamente ser comunicado a todas las personas incluidas en el alcance de forma directa y estar disponible en plataformas que permitan su correcta publicidad, como por ejemplo, pagina web corporativa, intranet, o cualquier otra que permita su acceso integro.

2.2. Manual de Prevención de Delitos:

El Manual de Prevención de Delitos es otro de los documentos clave de un modelo de Compliance. Se trata de un documento cuya finalidad principal es por un lado, reflejar las actividades potencialmente peligrosas que componen el mapa de riesgos de la organización, y por otro lado, integrar todos los documentos y normas internas de control y vigilancia que componen el modelo de Compliance.

La estructura mínima del Manual debería contener las siguientes partes[47] [48]:

Parte I: Descripción General que comprende:

[47] GONZÁLEZ RUISÁNCHEZ S., *Compliance: Sistemas de Cumplimiento y Gestión del Riesgo empresarial*. Universidad de Salamanca. Máster Compliance. Salamanca. Pp. 31 y ss.

[48] SÁIZ PEÑA, C.A.; (Coord.), *Compliance: Cómo gestionar los riesgos normativos en la empresa*. Thompson Reuters Aranzadi. Pamplona, 2015. Pg. 574.

(i) las características y componentes esenciales del Manual;

(ii) estructura general de la empresa, que incluye los deberes y facultades del Comité de Cumplimiento o del *Compliance Officer*; así como el procedimiento de información a éstos de los posibles riesgos e incumplimientos.

(iii) la referencia al Código de Conducta.

Parte II: Proceso de Gestión del Riesgo Penal:

(i) Descripción general de la Responsabilidad Penal de la Persona Jurídica, su regulación y alcance.

(ii) Implementación de Políticas y Procedimientos internos adecuados una vez,

a. identificadas las áreas de riesgo,
b. enumerados los delitos susceptibles de generar responsabilidad penal de la persona jurídica que sean relevantes para la empresa, y
c. la descripción de las conductas que potencialmente puedan ser delictivas.

(iii) Establecimiento de un sistema disciplinario.

(iv) Procedimiento de verificación periódica, ante infracciones relevantes, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

Parte III: Procedimientos o protocolos que integran el modelo de Compliance:

(i) Definición de los protocolos o procedimientos de toma de decisiones, de adopción y de ejecución de las mismas con relación a la gestión de los riesgos identificados.

2.3. Protocolos o procedimientos:

Dependientes del Manual de Prevención de delitos, se encuentran todos aquellos procedimientos o protocolos específicos para cada uno de los riesgos identificados. En el caso planteado, y de acuerdo a los hechos expuestos, sería recomendable la redacción de los siguientes procedimientos:

- Procedimiento de análisis de ciberseguridad del producto. Durante las fases de producción de los productos de IA Service introducir análisis dinámicos y estáticos para identificar posibles vulnerabilidades y fallos de seguridad, así como realizar test de intrusión con el modelo antes del lanzamiento al mercado.

- Welcome Pack: En el momento de incorporación de un trabajador hacer firmar un contrato de confidencialidad (NDA), dar formación sobre prevención de riesgos laborales, así como una clausula de Protección de Datos en la que los trabajadores consientan el tratamiento de sus datos personales.
- Política de Gestión de activos por parte de los empleados. Que regule las condiciones de uso de los activos de la empresa.
- Política de Auditorías de Software.
- Procedimiento de gestión de licencias de Software. Donde se relacionen las personas encargadas de renovar y actualizar las licencias en la empresa.
- Política de uso de dispositivos personales (BYOD).
- Guía de buenas prácticas en el SEO y SEM.
- Black List. Elaborar una lista que incluya los sitios web a los que, por su riesgo o por política de empresa, esté prohibido acceder a través de los activos de la empresa o de otros conectados a la red corporativa.
- Procedimiento de definición de los puestos de trabajo.
- Política de contratación de seguros corporativos.
- Política de Gestión de denuncias internas.
- Régimen disciplinario.
- Política de formación a empleados.
- Procedimiento de Gestión documental.
- Procedimiento de Inventario de Activos.
- Procedimiento de Gestión de soportes.
- Procedimiento de destrucción de la información.
- Procedimiento de homologación de proveedores.

Se hace recomendable estructurar estos procedimientos en razón de una metodología que siguiendo unas normas lógicas enumere y denomine los documentos de forma que sean fácilmente indetectables mediante la invocación de una siglas. Por ejemplo, "P001-Procedimiento de Gestión de Soportes".

3. IMPLANTACIÓN DEL SISTEMA

Una vez diseñadas las estrategias para hacer frente a los riesgos identificados, y aprobada su implantación, llega el momento de redactar toda esta documentación y

entregársela al cliente con objeto de que el Órgano de Gobierno de SPYNET, apruebe y adopte las medidas necesarias para la correcta implantación del modelo de Compliance.
Para ello, es necesario en primer lugar poner a disposición de todos los trabajadores y personas enmarcadas en el alcance el Código de Conducta, el Manual de Prevención de Delitos y todas las políticas y procedimientos elaborados para gestionar los riesgos identificados.

3.1. Comunicación del modelo de Compliance[49]:

A) Comunicación a trabajadores:

Para realizar la comunicación interna a los trabajadores, es recomendable establecer un repositorio documental o un apartado de la intranet donde todo trabajador pueda acudir y consultar estos procedimientos y sus actualizaciones de forma sencilla. Sin embargo, es importante guardar una evidencia de que todos los trabajadores han sido debidamente informados de la existencia del Código de Conducta y sus procedimientos relacionados, para ello, puede facilitarse físicamente a los trabajadores una copia de estos documentos y pedirles que tras leerlos firmen por duplicado una clausula en la que así lo declaren (una para ellos y otra para la empresa), o hacer lo propio mediante correo electrónico, intranet u otros medios digitales donde se guarde evidencia de que han leído y entienden el contenido, ya sea contestando haberlos recibido y leído, o mediante un *check* sin pre-marcar similar al de aceptación del aviso legal de una web, donde mediante la configuración técnica del sistema o bien mediante la conservación de *logs* de recepción quede constancia inequívoca de la identidad del usuario, así como de la fecha y hora de la aceptación.
En el caso de SPYNET todos los trabajadores en principio tienen acceso a la intranet y correo corporativo por lo que, la comunicación podría realizarse sin problema por estas vías, sin embargo, en el caso de una fábrica, por ejemplo, donde la mayor parte de la plantilla no tiene acceso a internet en el trabajo esta comunicación debería efectuarse mediante copias físicas.
Es importante apuntar que la evidencia recabada no es un requisito formal de cara a los trabajadores, sino que es un aspecto esencial para acreditar que la empresa ha actuado diligentemente, por ello todas estas evidencias deben almacenarse en un repositorio,

[49] SÁIZ PEÑA, C.A.; (Coord.), *Compliance: Cómo gestionar los riesgos normativos en la empresa*. Thompson Reuters Aranzadi. Pamplona, 2015. Pp. 579 – 584.

preferiblemente digital, donde se garantice la custodia, integridad y disponibilidad de estas evidencias.

B) Comunicación a proveedores:

En el caso de SPYNET, la comunicación a proveedores sería recomendable realizarla en el momento de contratación con el proveedor como parte integrante del procedimiento de homologación de proveedores propuesto, guardando igualmente evidencia de la aceptación del Código de Conducta de SPYNET y de sus protocolos y procedimientos. Sin perjuicio de la aceptación de estas clausulas por parte de los proveedores, es importante que la empresa efectúe todas las actuaciones necesarias establecidas en el procedimiento de homologación de proveedores para verificar que estos efectivamente cumplen con los valores de la empresa, y en caso de advertirse cualquier incumplimiento adoptar las medidas necesarias para subsanar o en el peor de los casos rescindir el contrato con aquellos.

En cuanto a la comunicación de actualizaciones de estos documentos, lo mejor sería enviar un correo electrónico a los interesados, poniendo a disposición de todas las partes el Código de Conducta y el Manual de Prevención de Delitos en la web corporativa.

C) Comunicación a clientes:

Lo importante respeto a los clientes, más que pretender que estos ajusten sus comportamientos a los principios de la empresa, es recabar la evidencia de que estos han sido informados, de forma preceptiva, de las condiciones de contratación del servicio o producto, así como de los valores y formas de actuación de la empresa.

La forma de comunicación más efectiva respecto de éstos es sin duda la publicación del Código Ético y del Manual de prevención de delitos, y la obtención del consentimiento mediante check sin pre-marcar de aceptación del Aviso Legal, de los Términos y Condiciones de Uso de la web conforme a los dispuesto en la LSSI, donde debe mencionarse la existencia de un modelo de Compliance, y en caso de recabar datos de carácter personal de la Política de Privacidad adaptada al GDPR y demás normativa en materia de protección de datos vigente en el momento de la cesión.

3.2. Canal de denuncias internas (*Whistleblowing*):

Como ya se ha mencionado, todo modelo de Compliance para ser considerado eficaz debe contener los requisitos establecidos en el art. 31 bis. 5 del Código Penal, entre estos se encuentra el deber la persona jurídica de imponer «la obligación de informar de

posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención». De la lectura de este precepto, la Fiscalía extrae la necesidad de que «un modelo de organización y gestión, además de tener eficacia preventiva debe posibilitar la detección de conductas criminales», propósito para el que entiende que «la existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas de la empresa es uno de los elementos clave de los modelos de prevención»[50].

Se trata de un mecanismo que posee una doble vertiente; por un lado es un sistema reactivo, ya que permite a la empresa reaccionar ante el conocimiento de determinados actos irregulares o ilícitos ya cometidos; y por otro lado preventivo, dado que la implantación de este canal puede ayudar a inhibir a una persona a realizar algún comportamiento irregular que, sin la existencia de este pudiera estar tentado a realizar[51].

Como requisitos esenciales, un canal de denuncias debe ser un sistema respaldado por Dirección, fácilmente accesible a cualquier persona integrada en el alcance del modelo de Compliance para que éstas puedan alertar o comunicar de forma confidencial todo comportamiento contrario al Código Ético a los procedimientos del modelo de Compliance o cualquier actuación potencialmente ilícita o delictiva, que de alguna forma pueda derivar responsabilidad penal, civil o administrativa de la empresa. Estas alertas pueden realizarse, por ejemplo, a través de un formulario online incluido en la web de la empresa o mediante el envío de un correo electrónico a una dirección corporativa específica (p.e. denuncialo@spynet.com). Sea el medio que sea, lo esencial es que haya sido previamente comunicado a todos los interesados. Asimismo, ligado a la confidencialidad de la denuncia, el sistema debe imprescindiblemente garantizar una regulación protectora específica del denunciante (*whistleblower*), garantista de que la empresa no efectuara ninguna represión contra el denunciante.

En este sentido, cabe preguntarse si el sistema debe ser anónimo o nominativo. En mi opinión, y en base a la interpretación de la Fiscalía, el sistema debe ser confidencial. Lo que se traduciría como la protección absoluta de la identidad del denunciante de cara toda persona ajena al Comité de Cumplimiento o en su caso al Comité de Denuncias Internas, en este sentido, no solo no veo problema en que el sistema sea nominativo, sino que lo considero recomendable de conformidad con la obligación que tienen las

[50] CIRCULAR 1/2016, de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015. Pp. 44 – 45.
[51] SÁIZ PEÑA, C.A.; (Coord.), *Compliance: Cómo gestionar los riesgos normativos en la empresa*. Thompson Reuters Aranzadi. Pamplona, 2015. Pp. 613 – 614.

personas implicadas de informar de posibles riesgos e incumplimientos (art. 31.bis.5.4º CP) de cara a generar una evidencia que podría ser útil en un eventual proceso penal o civil contra los denunciantes como personas responsables del cumplimiento en la empresa.

4. CONTROL Y SUPERVISIÓN:

Como ya se ha mencionado en la Introducción de este trabajo, los modelos de Compliance no son un repositorio de políticas y procedimientos estáticos que tras su implantación puedan guardarse en un armario. La Cultura Compliance, es casi un "ser vivo" y como tal, entiéndase figuradamente, necesita como toda criatura ser alimentada, cuidada y educada.

- Alimentada, pues requiere de actualizaciones continúas que favorecen su crecimiento y mejor funcionamiento. Especialmente cuando se produzcan cambios normativos que afecten a la organización, o cambios operativos que modifiquen sustancialmente el desempeño de su actividad.
- Cuidada, ya que es necesario supervisar y controlar su correcta aplicación mediante auditorias periódicas, o herramientas de gestión especificas que, independientemente de si se pretende o no obtener una certificación, sigan las directrices de la ISO 19600, o ISO 3100. En empresas como SPYNET se hace recomendable implementar controles técnicos en sistemas informáticos como mecanismos de prevención de fugas de información, sistemas de detección de intrusiones (IDS), medidas de control de acceso lógico, etc.
- Educada, en cuanto que alcanzar una Cultura de Cumplimiento es un proceso de formación y concienciación continua.

PARTE III: CONCLUSIÓN

«*Todos pertenecemos a todos*» escribió Aldous Huxley en 1932, al presentar su visión distópica del mundo futuro. Si analizamos el entorno actual, podemos observar que efectivamente todos pertenecemos a todos. No en el sentido carnal al que hacía referencia Huxley en un Mundo Feliz[52], pero sí en cuanto a la posibilidad de tener acceso a datos de carácter personal de casi cualquier persona, debido sustancialmente al fenómeno de monetización[53] que ha sufrido la privacidad con el pronunciado desarrollo de las TIC. Esta tendencia acusa una profunda banalización hacia lo que es nuestro, hacia lo privado, hacia lo íntimo. Hasta el punto de aceptar como común que se compren y vendan nuestros datos personales sin saber muy bien para qué.

Ante este escenario, el Derecho se ha visto en la necesidad avanzar alineándose con los progresos de la tecnología y la sociedad, para poder alcanzar verdaderamente una posición útil para la salvaguarda de los derechos y libertades de los ciudadanos, especialmente en los casos en los que éstos no son conscientes de los riesgos que les afectan. En este sentido, empresas, gobiernos y autoridades de control juegan un papel fundamental como garantes de la legalidad y de los principios éticos que rigen la sociedad.

Por ello, aunque parezca innecesario decirlo, es sumamente importante que la legislación esté estructurada de tal forma que aliente al cumplimiento real y efectivo de la Ley. La consagración de la responsabilidad penal de la persona jurídica y especialmente la aceptación de los modelos de Compliance como causa de exención, alientan al cumplimiento de la Ley. Entiéndase estas ideas bajo el concepto de Cultura Compliance que, ejecutado correctamente es, en definitiva una función social, pues además de la protección jurídica que brinda a la organización, el beneficio último de una actuación ética empresarial repercute en provecho de la sociedad. Asimismo, otras normas como las vigentes en materia de protección de datos y servicios de la Sociedad de la Información (entre tantas), deben complementar el proceso de formación de Compliance como eje motor de un cumplimiento efectivo, ya no sólo en el sector TIC

[52] En 1932 se publicó por primera vez *Brave New Word*, una novela de fantasía considerada actualmente como uno de los imprescindibles en la literatura clásica.

[53] Con este término se quiere hacer referencia al uso actual que estamos haciendo de la privacidad como moneda de cambio frente a determinados productos o servicios que consideramos como gratuitos. Por ejemplo, cedemos nuestros datos personales para poder usar una aplicación, obviando la lectura de la política de privacidad en la mayoría de los casos. O incluso, por presión de la sociedad, compramos nuestro grado de aceptación en la misma, mediante la exhibición de nuestra vida privada en redes sociales.

donde frecuentemente los datos personales son el *core* del negocio, sino cada vez más en cualquier tipo de empresa.

En el supuesto de hecho del presente trabajo se ha querido evidenciar la importancia de estas ideas, y conscientemente todos los riesgos que se han expuesto derivan de actividades estrechamente relacionadas con el entorno virtual. Estos riesgos deben ser gestionados pues implican ciertos derechos constitucionalmente reconocidos como[54] el derecho fundamental a la intimidad (18.1 CE), a la inviolabilidad del domicilio (18.2 CE), al secreto de las comunicaciones (18.3 CE), a la no intromisión en el entorno digital (18.4 CE), y el Habeas data o derecho al olvido. Adoptar un modelo de Compliance no es obligatorio, pero sí muy recomendable, pues como se ha puesto de manifiesto, puede ser de gran utilidad a las empresas para mejorar su capacidad organizativa, conocer sus verdaderas debilidades y ajustar toda su actividad, no sólo al más riguroso cumplimiento de la Ley, sino también a la visión y valores de la empresa, lo que repercute en beneficios económicos y reputacionales para propia empresa y en nuevas oportunidades de contratación tanto con el sector público como con grandes compañías, que cada vez más exigen a sus proveedores que hayan adoptado un modelo de organización y gestión.

[54] SÁIZ PEÑA, C.A. (Coord.); PÉREZ BES, F., (Coord.), *La Responsabilidad Legal de las Empresas Frente a un Ciberataque*. ISMS Forum Spain – ENATIC. Madrid. Pp. 85-86.

PARTE IV: REFERENCIAS

1. LEGISLACIÓN Y JURISPRUDENCIA

A continuación se enumeran todas aquellas referencias legislativas mencionadas o utilizadas a lo largo del presente trabajo para la redacción del mismo:

Reformas del Código Penal:

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 7/2012, de 27 de diciembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal en materia de transparencia y lucha contra el fraude fiscal y en la Seguridad Social.
- Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Normativa complementaria al Código Penal y otras normas de interpretación:

- Ley 37/2011, de 10 de octubre de medidas de agilización procesal.
- CIRCULAR 1/2016, de la Fiscalía General del Estado, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 17/2001, de 7 de diciembre, de Marcas.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Estándares genéricos y específicos:

- UNE-ISO 9001 de Calidad.
- UNE-ISO 19600 de Sistemas de Gestión de Compliance penal.
- UNE-ISO 27001 de Sistemas de Seguridad de la Información
- UNE-ISO 3100 de Gestión del Riesgo.

Jurisprudencia:

- Sentencia 514/2015, dictada el 2 de septiembre por la Sala de lo Penal del Tribunal Supremo.
- Sentencia 154/2016, dictada el 29 de febrero por la Sala de lo Penal del Tribunal Supremo.
- Sentencia 830/2014, dictada el 28 de diciembre por la Sala de lo Penal del Tribunal Supremo.
- STJUE de 23 de marzo de 2010, C-236/08, "*Google France*".
- STJUE de 12 de julio de 2011, C-324/09, "*L´Oreal*".
- STJUE de 11 de julio de 2013, C-657/11, "*Belgian Electronic Sorting Tecnology*".
- Sentencia JM Madrid de 22 de diciembre de 2011.
- Sentencia AP Barcelona de 23 de abril de 2001, "*Nexus*".

2. BIBLIOGRAFÍA:

- GONZÁLEZ RUISÁNCHEZ S., *Compliance: Sistemas de Cumplimiento y Gestión del Riesgo empresarial*. Universidad de Salamanca. Máster Compliance. Salamanca.
- GRACIA MARTIN, L., *Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica*, recpc 18-05 (2016).
- LÓPEZ-TARRUELLA MARTÍNEZ A., (Direc.); GRACÍA MIRETE C.M. (Coord.), "*DERECHO TIC: Derecho de las tecnologías de la información y de la comunicación*" TIRANT LO BLANCH. Valencia, 2016.
- MOOC: *Ciberseguridad entender los ataques para desplegar contramedidas.* Universidad Rey Juan Carlos. Madrid
- SÁIZ PEÑA, C.A.; (Coord.), *Compliance: Cómo gestionar los riesgos normativos en la empresa*. Thompson Reuters Aranzadi. Pamplona, 2015.
- SÁIZ PEÑA, C.A. (Coord.); PÉREZ BES, F., (Coord.), *La Responsabilidad Legal de las Empresas Frente a un Ciberataque*. ISMS Forum Spain – ENATIC. Madrid.
- ZUGALDIA ESPINAR, J.M., *Aproximación teórica y práctica al sistema de responsabilidad criminal de las personas jurídicas en el derecho penal español.*

Centro de investigación Interdisciplinaria en derecho Penal Económico (CIIPE). 2010.