RESUMEN EJECUTIVO

ESTUDIO AUTELSI

"GESTIÓN DEL COMPLIANCE EN EL ENTORNO TIC"

GRUPO DE REGULACIÓN DE AUTELSI

JULIO 2016

Los Departamentos TIC y la Función de COMPLIANCE

Informe de AUTELSI

Considerando el carácter transversal de la función de Compliance, su fuerte dependencia de los Sistemas de Información, y la ausencia de requisitos generalmente aceptados en este ámbito, el Grupo de Regulación de AUTELSI, en su labor de analizar las novedades normativas en el ámbito de las TIC, decidió centrarse en el estudio de la Gestión del Compliance en el entorno TIC.

Se trata de un estudio que viene a profundizar en un aspecto estratégico para las compañías que forman parte de la Asociación y que sigue la línea de anteriores trabajos de este Grupo, como el realizado en relación a la gestión de evidencias electrónicas (2013) o Privacidad por Diseño (2014)

Tras meses de estudio, el grupo ha elaborado el presente informe que persigue analizar y desgranar el concepto de Compliance y las funciones inherentes a la gestión del cumplimento, compromisos y comportamientos en la organizaciones, en especial, en relación con las funciones de los departamentos TIC (Sistemas de información, TI, …) y la responsabilidades inherentes a este área, de creciente relevancia en las estructuras organizativas, hoy en día.

Somos conscientes de la transformación que las Tecnologías de la Información y las Comunicaciones están operando en los negocios y de la creciente y alarmante dependencia que el uso de estas tecnologías esta generando en los mismos. Negocios que operan exclusivamente en la Sociedad de la Información, en Internet y negocios que se aventuran a ese mundo aprovechando las ventajas competitivas y la productividad que generan.

Se habla de transformación digital, de globalización, del valor de la información y el conocimiento (nuevo "petróleo" [1][2][3] del siglo XXI), de la innovación basada en tecnología, como motor de cambio. Miles de soluciones tecnológicas aparecen cada día respondiendo necesidades de PYMEs y grandes corporaciones de todo tipo de industria. Se habla de Big Data, de Cloud Computing, de Internet de las cosas, de Social Business, Open Source, Movilidad, … se habla de redefinir la Sociedad de la Información transformándola en la Sociedad Digital.

Se habla de esto y mucho mas, para los profanos de las TIC, desde una perspectiva técnica, pero es una realidad de la que no podemos apartarnos, que no podemos obviar cuando afecta a nuestros negocios de forma tan incisiva, como lo hacen las leyes y regulaciones.

En este estudio se tratan temas como la gestión de riesgos por el Departamento TIC y la identificación de medidas, controles y evidencias que den apoyo al *Compliance Global* de la organización. La doble perspectiva del *Compliance* del departamento TIC y del apoyo de este al *Compliance Global*, es el resultado en que se aterriza tras el estudio más general del concepto de *Compliance* y de los distintos aspectos que exige el establecimiento de un *Sistema de Gestión de Compliance (SGC)*.

[1] http://www.elmundo.es/economia/2014/05/29/5383855e268e3e13488b4576.html
[2] http://www.elpaisretina.com/el-petroleo-del-siglo-xxi-es-el-big-data/
[3] http://www.eleconomista.es/firmas/noticias/6576206/03/15/La-informacion-el-petroleo-del-siglo-XXI.html

El concepto de Compliance

Una primera aproximación al concepto de ***"compliance"*** lo podemos encontrar en la siguiente definición: *"Función que tiene por objeto garantizar y acreditar que empresas y organizaciones desarrollan sus actividades de forma responsable, ética y legal".* El término ***"compliance"*** proviene del verbo Inglés *"to comply",* lo que significa "actuar de acuerdo con una regla, requerimiento, una instrucción interna, una orden o petición",… en definitiva una obligación o compromiso.

La historia del compliance nos acerca a los escándalos de corrupción y financieros que afectaron a importantes compañías de los EEUU en los años 70, hasta la reciente reforma de nuestro Código Penal y la incorporación de la responsabilidad penal de las personas jurídicas, que viene a sumarse a las innumerables normas (Prevención de Blanqueo de Capitales, Protección de datos, Sociedades de Capital, Prevención de Riesgos Laborales, Gestión de Residuos, Buen Gobierno Corporativo, …) que exigen un control, una prevención y una gestión eficaz que permita acreditar el cumplimento y evitar responsabilidades y daños reputacionales.

El concepto práctico de ***"Gestión del compliance"*** como un *" Sistema de Gestión para controlar el cumplimiento de las leyes y reglamentos, políticas y directrices establecidas para el negocio y para las actividades de la Organización o empresa, y para prevenir, detectar y tratar cualquier desviación o no conformidad que pueda ocurrir",* nos invita a pensar que la implantación de un Sistema de Gestión del Compliance se antoja crucial, desde el punto de vista estratégico, para las organizaciones que quieren operar con eficacia en el Siglo XXI. Y la alineación del departamento de TIC con la estrategia de sus organizaciones ha de ser mayor que nunca, puesto que su papel tradicional está evolucionando desde el actual soporte al negocio hacia convertirse en un elemento fundamental de Transformación del Negocio. El papel de los CIO exige una implicación en el negocio, y por tanto, asumen un papel crucial en el apoyo al cumplimento normativo y al papel del *Compliance* en la organización.

En consecuencia, podemos definir el C*ompliance* como el conjunto de procedimientos y controles a través de los cuales una organización es capaz de evidenciar que ha puesto todas las medidas a su alcance para que todo el conjunto de la organización cumpla con

- La normativa legal y regulatoria
- Los compromisos contractuales y no contractuales
- La autorregulación y buenas prácticas
- Y demás principios de comportamiento ético

Es evidente necesidad de que los departamentos TIC se impliquen en la gestión de *compliance global*, en el control de cumplimento de las obligaciones y en el seguimiento de las medidas y controles preventivos para evitar incumplimientos, no solo de aquellas normas que afecten directamente al departamento de TIC, como pueda ser el estándar Payment Card Industry Data Security (PCI DSS) o la ley de medidas para la protección de infraestructuras críticas.

En general la función del compliance exige la búsqueda de implicación de las áreas de responsabilidad de las empresas en la toma de decisiones, teniendo en cuenta qué herramientas deben soportar su gestión, cómo se debe integrar en el Negocio sin obstaculizarlo.

Cultura y Liderazgo en la función del Compliance

Si la gestión del Compliance supone un manifiesto de la cultura de cumplimiento de obligaciones, una medición y la posibilidad de acreditar frente a terceros estos hechos, se puede afirmar que Compliance no es solo elaborar un código de conducta o código ético. Compliance, asumiendo las directrices recogidas en la Norma UNE-ISO 19600 supone la detección, análisis y gestión de los riesgos por incumplimientos de sus obligaciones legales, contractuales y compromisos, asumiendo la definición e implantación de medidas preventivas, proactivas y correctivas y de Controles personalizados, la planificación de Auditorias periódicas y la gestión de continua de incidencias. Compliance implica la definición de métricas e Indicadores, la gestión de evidencias y, en definitiva la medición del desempeño y la mejora continua.

Hablando exclusivamente de responsabilidad penal, un punto en el que coinciden las recientes Circular 1/2016 de la Fiscalía General del Estado y Sentencia del Tribunal Supremo de 29 de febrero de 2016 es el de la necesidad de que exista una cultura de cumplimiento en la empresa para que ésta pueda acceder a la exención de la responsabilidad penal. Los modelos de organización y gestión exigidos en el Art. 31 bis del código Penal no sólo tienen por objeto evitar la sanción penal de la empresa sino también promover una verdadera cultura ética empresarial.

Pero *Compliance* exige gestión y para ello se necesita un líder, un responsable, alguien que asuma la función y lidere el cambio, que lidere la transmisión de la cultura de cumplimento. Y ¿cómo se estructura en una organización la función de C*ompliance?. ¿A través de u*n órgano unipersonal? ¿Un órgano Colegiado? ¿Un comité de *Compliance*? ¿Interno en la Organización o Externo a la misma?

La decisión de cómo estructurar la función de Compliance en una organización dependerá fundamentalmente de sus dimensiones y del riesgo que tengan las actividades y áreas de negocio a las que se dedica. No se estructura de la misma manera en una empresa cotizada que en una PYME regida por un Administrador Único, al que la Ley le otorga la función de supervisión. También influirán la actividad, el número de empleados, la presencia internacional (si tiene delegaciones fuera o si es filial de una multinacional). En definitiva, todo dependerá de los elementos sometidos a vigilancia, control y elementos reguladores que le afecten.

Siguiendo con el Código Penal, la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado exige el nombramiento de 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

La ley está exigiendo un liderazgo al órgano de *compliance* y está marcando los requisitos de cómo deberá ejercerse ese liderazgo.

Habitualmente en las empresas, las funciones anteriormente descritas de las que ahora deba encargarse el órgano de *compliance* se encuentran divididas en el seno de la Organización. De esta forma existe:

- Recursos Humanos que suele encargarse de gestionar los asuntos relacionados con la prevención de riesgos, las denuncias relativas al acoso laboral, discriminación salarial, violaciones de intimidad, seguridad en el trabajo, etc., así como de la formación a los empleados en diferentes aspectos de la gestión de la compañía.

- Asesoría Jurídica, encargada de la identificación de la normativa aplicable en general y estar al día en los cambios legislativos que pueden afectar, cumplimiento de los compromisos adquiridos, relacionarse con los reguladores etc.
- Departamento Financiero, encargado de evaluar el estado financiero de la compañía.
- Auditoría interna, encargado de realizar las auditorías internas de los procedimientos y políticas internas implantadas en una organización.
- Departamento de Sistemas (TIC), encargado de dar soporte tecnológico a la organización, proveer de información así como de las herramientas necesarias para sus gestión, Supervisar, garantizar e implantar sistemas de información de todas las áreas de la empresa

Todos estos Departamentos, indudablemente, realizan tareas de supervisión, vigilancia y control de las actividades y, por tanto podremos decir que realizan funciones de *compliance*, pero como quiera que el legislador quiere integrar todo bajo la función de *compliance*, inmediatamente surge la pregunta "¿Es posible que exista una persona en la empresa capaz, con el poder y conocimientos suficientes para abarcar todas estas funciones de vigilancia?".

Por lo que siendo realistas y teniendo en cuenta los diferentes factores que se requieren, una opción buena puede ser que *la función del compliance* se estructure en un órgano colectivo integrado por varias personas con reporte directamente al Consejo de Administración y que actúe bajo la Dirección de una Persona ("Compliance Officer"). No obstante, reiterar que la legislación no dice nada al respecto y, por tanto, en principio, todas las opciones pueden ser válidas siempre y cuando cumplan de forma eficaz con las obligaciones de supervisión exigidas.

Lo que es importante recordar es que el Órgano de Administración, es el responsable frente a la sociedad, frente a los socios y frente a los acreedores sociales, del daño que causen por actos u omisiones contrarios a la ley o a los estatutos o por los realizados incumpliendo los deberes inherentes al desempeño del cargo, siempre y cuando haya intervenido dolo o culpa (Art. 236 de la Ley de Sociedades de Capital). De ahí que la cultura de compliance, la disposición de recursos y medios oportunos y la designación de responsables deba ser impulsada desde el Órgano de Administración. Deber ser tutelada (responsabilidad in vigilando) e impulsada designando el órgano responsable interno o externo, (responsabilidad in eligendo) según la modalidad que decida atendiendo a su contexto.

A su vez, y en relación con la posible comisión de delitos en el seno de una organización, el artículo 11 del Código Penal (comisión por omisión), parece que tiene la intención de colocar en situación de garante al órgano de administración del cumplimiento de ese deber de control. Es decir, como los administradores tienen a su cargo la vigilancia y el cuidado de los riesgos generados por la organización empresarial, es preciso establecer la responsabilidad penal en la que puedan incurrir los miembros del Consejo de Administración por los delitos que se pudieran cometer en el seno de la organización, precisamente por no haber puesto las medidas (substantivas y procedimentales) necesarias para evitarlo.

Identificación del marco de cumplimiento de aplicación a la función de TIC

Conforme a este estándar, la identificación del marco de cumplimiento implica revisar los siguientes aspectos dentro del ámbito de la responsabilidad la función de TI: Comprensión de la organización y de su contexto, Requisitos de las partes interesadas y Principios de Buen Gobierno.

Considerando los tres aspectos indicados, y teniendo asimismo en consideración las cuatro dimensiones a las que nos referíamos en la introducción (personas, infraestructuras, información, aplicaciones y servicios), la metodología propuesta para la determinación del marco de cumplimiento que afecta a la actividad del área de TI, se basa en la disponibilidad de un Catálogo de Servicios actualizado en el que se encuentren correctamente definidos y documentados dichos servicios y los requisitos y las partes interesadas en relación a cada uno de ellos.

En términos generales, los servicios pueden clasificarse en tres categorías conforme a la estructura propuesta en el marco de referencia ITIL (*Information Technology Infrastructure Library*), revisión de 2011:

- Servicios orientados a clientes externos, con valor directo para los clientes y cuya gestión puede implicar la consideración de obligaciones de cumplimiento asociadas a la prestación de servicios y al tratamiento de datos e información de usuarios y clientes finales.
- Servicios orientados a clientes internos, con valor directo para el funcionamiento interno de la organización, su gestión afecta a procesos internos necesarios para la comercialización de productos o prestación de servicios.
- Servicio de Soporte, relativos a la gestión de aplicaciones e infraestructuras.

La consideración de esta clasificación resulta relevante dado que los requisitos en materia de c*ompliance* varían en función del tipo de servicio.

Por otro lado, debe considerarse tanto los servicios operados directamente por la organización, como aquellos que se encuentran total o parcialmente externalizados. Cabe señalar que la externalización no suele eximir de responsabilidades al responsable último del servicio.

Asistencia del departamento TIC al “Compliance”

La función de Compliance ha de velar porque las políticas de uso de las TIC y los controles asociados estén principalmente orientados a frenar los posibles usos abusivos o ilícitos de los medios tecnológicos puestos a disposición de las Partes Interesadas, en especial de Administradores, Directivos y Empleados, pero también de Proveedores o Clientes, de acuerdo con las políticas de la Compañía y dentro del Marco Legal establecido, para la ejecución y operación de los Procesos y Servicios de Negocio.

En un departamento TIC, el sistema de control impacta a tres niveles:

- Al ***nivel de dirección ejecutiva*** donde se fijan los objetivos de negocio y se establecen políticas y recursos necesarios para ejecutar la estrategia de la compañía. En este caso, el ámbito de control TIC es guiado por este conjunto de objetivos y políticas de alto nivel.

- Al ***nivel de procesos de negocio***, en tanto éstos están automatizados e integrados con los servicios y/o sistemas de TIC, se aplican controles específicos que en algún caso se basan en procedimientos manuales como por ejemplo las autorizaciones relativas a la segregación de funciones y/o las conciliaciones contables. En este caso, el ámbito de control TIC da soporte a su diseño y desarrollo.
- Al ***nivel de controles generales TIC***, considerando que las soluciones y servicios ofrecidos pueden ser compartidos para diferentes procesos de negocio (tal como es la recolección y resguardo de evidencias y al análisis forense requerido sobre las mismas), una de las claves es la confiabilidad e integridad de la información de eventos que se custodia y del propio proceso de chequeo automático.

Análisis de Riesgos

Una vez definido el alcance de las obligaciones y compromisos de *compliance* que afectan a la función de TIC, resulta necesario disponer de un análisis de riesgos adecuado que permita a la organización conocer su nivel de exposición a los mismos y determinar las medidas de aplicación en cada caso.

La valoración de los riesgos es la base para la implementación de un Sistema de Gestión de *Compliance* adecuado a las necesidades de la organización

La identificación o definición de riesgos conlleva considerar las posibles causas de incumplimientos de *compliance* que pueden estar relacionadas con las personas, infraestructuras, información y aplicaciones objeto de los servicios prestados por el Departamento de TIC.

Se deben catalogar los riesgos en función de su probabilidad de ocurrencia e impacto y consecuencias, ya sea debida a factores externos al Departamento de TIC o asociados directamente al mismo.

Una vez identificados los riesgos y su probabilidad de concurrencia e impacto, deben describirse también las consecuencias de los mismos, incluyendo el coste asociado a la paralización de operaciones o a la necesidad de sustitución de determinados elementos o el coste reputacional.

Posteriormente, este nivel de riesgo deberá contrastarse con el que la organización puede y está dispuesta a asumir. No obstante, y tal y como nos recuerda la norma UNE-ISO 19600 apartado 4.6 (nota 2), un enfoque de gestion de compliance basado en el análisis de riesgos no significa que para situaciones de riesgo bajo, se deban aceptar incumplimentos. Este analisis solo sirve de ayuda para centrar la atencion primaria y los recursos en los riesgos mas elevados, para en última instancia, cubrir todos los riesgos de compliance.

Por último, debe indicarse la necesidad de establecer mecanismos adecuados para asegurar que los riesgos son reevaluados con una periodicidad suficiente y, en todo caso, siempre que se produzcan modificaciones significativas en los servicios o en los sistemas de información que les dan soporte.

Establecimiento de medidas y controles

El departamento TIC ofrecerá un conjunto de soluciones y servicios que constituyen en sí mismos medidas y controles de cumplimiento con sus respectivas evidencias, todo ello en relación con los riesgos identificados.

Estos servicios y soluciones deben integrarse en un Catálogo de Servicios en que se definan y documenten considerando los requisitos y las partes interesadas en cada uno de ellos. Entre otros se pueden destacar: Servicio de Análisis y Gestión de Riesgos, Servicio de Canal de Denuncias, Servicio de Detección, Control y Gestión del Fraude, Servicio de Protección de la Propiedad Intelectual, Servicio Seguridad Gestionada y Ciberseguridad, Servicio de Informática Forense, Herramientas de Segregación de Funciones, Herramientas DLP, Sistemas de Detección de Intrusiones (IDS/IPS), Soluciones de Control del Acceso a la Red (NAC),…

Los principales elementos de control interno se agrupan básicamente:

- El control del entorno,
- El análisis y gestión de riesgos,
- Los sistemas de acceso y difusión de información y comunicación, y
- Las actividades de control y monitorización.

Así, estas medidas y controles internos están soportados por políticas y procedimientos, establecidos por la organización con el objetivo de asegurar el cumplimiento normativo y legal, destacando los siguientes controles típicamente TI:

- Definición de las políticas de seguridad de la información y de uso de los medios tecnológicos en que se soportan los procesos de negocio, incluyendo supervisión y revisión periódica del cumplimiento.
- Control de acceso basado en la necesidad de conocer mediante los que se regule el acceso a la información que también permite en control de las fugas de información.
- Auditoría a nivel de sistemas, aplicaciones, redes y sistema operativo mediante los que se identifique el acceso, la modificación y el borrado de la información.
- Destrucción y borrado seguro de la información crítica para el negocio de los medios de almacenamiento, así como aquella que se encuentre en formato papel.
- Respaldo y recuperación de la información crítica para el negocio.
- Controles de integridad de la información para evitar su alteración (sirvan de ejemplo servicios y soluciones informáticas como cortafuegos, IDS/IPS, software de gestión de derechos, aplicaciones para filtrar la información, etc.).
- Clasificación de la información según su nivel de criticidad para los procesos de negocio de la organización, lo que constituirá la base de las medidas de seguridad a aplicar.
- Securización (o cifrado) de la información transmitida por medios electrónicos (principalmente el correo electrónico o la mensajería instantánea).
- Monitorización de la actividad en los sistemas, aplicaciones, redes, etc., para asegurar la emisión de alarmas al detectarse comportamientos anómalos.

Por ultimo, un buen Sistema de Gestión de Compliance exige la gestión de las evidencias de cumplimiento. Los principales elementos de control interno del Departamento TIC se agrupan básicamente en el control del entorno, el análisis y gestión de riesgos, los sistemas de acceso y difusión de información y comunicación, las actividades de control y monitorización, en el marco organizativo del aseguramiento del cumplimiento normativo y legal, destacan las siguientes evidencias generales:

- Registros de control de acceso de los usuarios a los diferentes sistemas y aplicaciones.
- Registros de auditoría a nivel de sistemas, aplicaciones, redes y sistema operativo mediante los que se identifique el acceso, la modificación y el borrado de la información.
- Registro de las tareas de destrucción y borrado seguro de la información crítica para el negocio.
- Registro del proceso de respaldo y recuperación de la información crítica para el negocio, incluyendo especialmente las evidencias relativas a las solicitudes de recuperación de información, con la debida autorización del responsable del dato o del proceso de negocio implicado.
- Registros de auditoría a nivel de elementos de seguridad como cortafuegos, IDS/IPS, software de gestión de derechos, etc.
- Registros de la información que es transmitida por medios electrónicos quera de la organización.
- Registros de auditoría de la actividad en los sistemas, aplicaciones, redes, etc., así como de las alarmas y eventos de seguridad recopilados mediante las herramientas y consolas de seguridad.

Las evidencias de cumplimiento de los controles definidos, y exigidos en base a los requisitos legales y normativos, deberán formar parte de un informe que esté a disposición del Compliance.

Agradecimientos

AUTELSI agradece a las siguientes personas, miembros del Grupo de Trabajo de Regulación de la Asociación, su esfuerzo y dedicación en la realización de este estudio sobre la Gestión del Compliance en el Entorno TIC

Presidente del Grupo Trabajo

Oscar López Rodríguez: Socio Director de Urbetec Abogados y de la consultora UBT Compliance.

Vocales del Grupo Trabajo

Carlos Bachmaier Johanning: Consultor en la Dirección TIC de SELAE.

Mariano J. Benito Gómez: Director de Seguridad / CISO de GMV Secure eSolutions.

Francisco Girón Guijarro: Responsable de Operaciones de UBT Compliance.

Pedro Pablo López Bernal: Gerente GRC & PIC (Gobierno, Riesgos, Compliance & Protección, Infraestructuras y Continuidad Global) de Rural Servicios Informáticos.

Antonio Simón Martínez García: Responsable de Seguridad Informática de Metro de Madrid.

Ramón Ortiz González: Responsable de Seguridad de Mediaset.

Emilio Pérez Mayuet: Jefe de Área de Planificación de Sistemas Informáticos de la IGAE (Ministerio de Hacienda y AAPP).

Susagna Pol Font: Information Compliance Director del Grupo Banco Sabadell.

Juan Carlos Ramiro Iglesias: Director de Accesibilidad en el Centro Nacional de Tecnologías de la Accesibilidad (CENTAC) y Vicepresidente de la Fundación de Tecnología Social.

José Antonio Rubio Blanco: Responsable de Seguridad TI y Protección de Datos de la Universidad Rey Juan Carlos.

Diego Soriano de Álvaro: Gerente de proyectos en CENTAC, (Centro Nacional de Tecnologías de la Accesibilidad).

María Suárez Pliego: Abogada y socia del despacho Suárez de la Dehesa Abogados.

Susana Zumel Vara: Responsable del área de Planificación e Innovación de Sistemas de Información de Cepsa.

También queremos manifestar nuestro agradecimiento a **Red.es** por la cesión de sus instalaciones para la celebración del desayuno en el que se presentó este informe el 7 de julio de 2016.