Modelos de diligencia debida y gestión de riesgos de terceros 2023

Guía completa para implantar un modelo de TPC (Third Party Compliance) en la cadena de suministro

28 de marzo de 2023

Introducción

En los últimos años las empresas están intentando implantar modelos de control de terceras partes con el doble objetivo de:

1. Cumplir los requisitos regulatorios que las normas van incorporando y
2. Mitigar los riesgos a los que se expone una organización cuando trabaja con una tercera entidad que forma parte de su cadena de suministro.

Todos hemos podido conocer casos (en prensa, hablando con colegas de profesión, o incluso dentro de nuestra compañía), donde queda patente que una compañía puede sufrir un impacto negativo derivado de las relaciones con proveedores, partners, o terceros en general.

Cuando un incidente ocurre en un partner o un proveedor estratégico de nuestra organización, nos vemos sometidos a muy diferentes impactos que pasan por reanudar un servicio lo antes posible, atender a los clientes afectados sus quejas o reclamaciones, gestionar los impactos legales y posibles sanciones, minimizar el daño reputacional a la imagen de la empresa, o manejar la falta de confianza por el mercado y accionistas en general.

Evolucionamos hacia una sociedad más digital e hiperconectada, y a su vez más descentralizada en cuanto a infraestructura, comunicaciones y datos, por lo que la protección de la información (y los derechos e intereses de una compañía) dependen también en gran medida de la protección que los agentes de su cadena de suministro ofrezcan, más allá del perímetro de esa compañía.

Las normativas como RGPD, ENS, NIS 2, DORA, Infraestructuras Críticas, Seguridad en redes 5G... establecen obligaciones por las cuales una organización debe implantar un sistema de diligencia debida (Third Party Compliance) con terceros, donde se realice algún tipo de comprobación sobre su sistema de seguridad, resiliencia, protección de datos ... que favorezca una toma de decisión informada y refleje las garantías suficientes, de forma previa a la contratación de esa entidad tercera que forma parte de la cadena de suministro (proveedores de servicios o productos, agentes, partners, etc.).

Implantar un sistema ágil y eficiente, que además cumpla con los diferentes requisitos normativos, no es fácil, ya que además la volumetría de “terceras partes” con las que las organizaciones se relacionan es muy grande y la casuística muy variada.

A su vez, las empresas proveedoras se someten de forma constante a la valoración de su estado de Compliance, Ciberseguridad, Protección de Datos, Resiliencia, Derechos Humanos, Sostenibilidad, etc. por parte de sus futuros clientes, normalmente en procesos de homologación. Las que están en un buen estado de cumplimiento desean que esos procesos sean ágiles, les aporte algún valor diferencial, y aligeran algunas tareas que posteriormente vendrán en la parte de negociación contractual. Por ello, trabajar en la creación de estándares y certificaciones comúnmente aceptadas por la industria puede ser interesante de cara a agilizar los procesos de diligencia debida, tanto para empresa cliente como para empresa proveedora.

Este será uno de los retos a los que nuestra comunidad de Compliance Officers, CISO´s y DPO´s se va a enfrentar en los próximos años. Por ello, hemos querido dedicar este monográfico a tratar el tema de la Diligencia Debida y los sistemas de Third Party Compliance, que esperamos os resulten útiles a todos.

Índice

1. ¿Qué es?

Con el concepto “Third Party Compliance” hacemos referencia a los procesos de gestión de riesgos con terceros, especialmente proveedores que forman parte de la cadena de suministro y el cumplimiento de las obligaciones de diligencia debida respecto ellos.

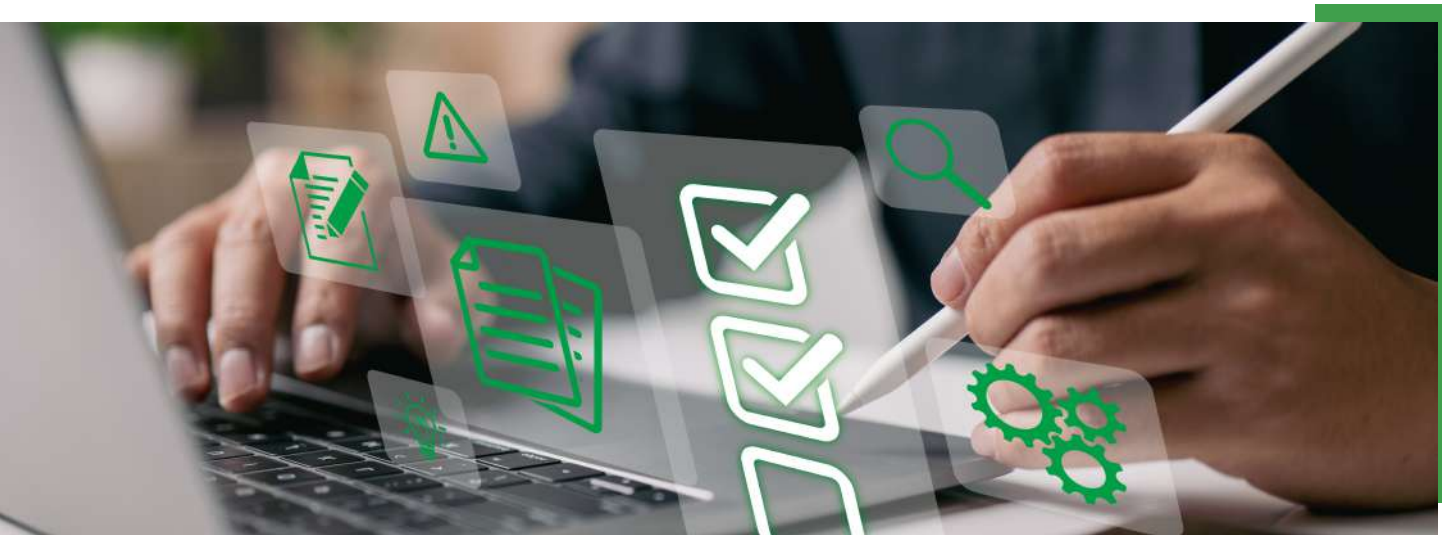
¿Por qué estamos obligados?

- Cada vez existen más normas (tanto Reglamentos y Directivas, como leyes nacionales) que requieren de un sistema de Diligencia Debida previa en la contratación con terceros, así como la monitorización de los riesgos durante dicha relación.
- Las exigencias derivan tanto de normativa sectorial como de normativa general de prevención de riesgos y cumplimiento.
- Existen diferentes regímenes sancionadores y Autoridades de Control que velan por el cumplimiento de estas obligaciones.

¿Cuál es la normativa y estándares que regulan la diligencia debida?

Existen diferentes normas que podríamos agrupar en 4 grupos y que regulan de alguna manera estas obligaciones de diligencia debida:

- Compliance (Riesgos penales, anticorrupción, blanqueo de capitales, sanciones internacionales, etc.).
- Privacidad y Protección de datos (RGPD y LOPDGDD).
- Ciberseguridad (Infraestructuras críticas, servicios esenciales, resiliencia digital, etc.).
- ESG (Sostenibilidad, derechos humanos, etc.).



Algunas de esas normas y estándares son:

- Código Penal
- ISO 37301 de Sistemas de Gestión de Compliance
- ISO 37001 de Sistemas de Gestión Antisoborno
- UNE 19601 de Sistemas de Gestión de Compliance Penal
- Ley de Prevención de Blanqueo de Capitales y Financiación del Terrorismo 10/2010, de 28 de abril
- RGPD Reglamento General Europeo de Protección de Datos
- LOPGDD Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
- Esquema Nacional de Seguridad
- Ley de Protección de Infraestructuras Críticas
- ISO 27001 Sistemas, de Gestión de la Seguridad de la Información
- Directiva NIS 2
- DORA Reglamento sobre la resiliencia operativa digital del sector financiero
- Ley de Ciberseguridad de las redes 5G
- Principios rectores de las Naciones Unidas sobre empresa y derechos humanos
- Directiva sobre la Diligencia Debida de las empresas en materia de sostenibilidad
- Etc.

¿Qué consecuencias puede conllevar el incumplimiento de la gestión de riesgos en la cadena de suministro?

- Sanciones económicas importantes impuestas por Autoridades de Control
- Impacto reputacional y sobre el valor accionarial.
- Impacto operacional (interrupción de servicio, asistencia a clientes, etc.)
- Responsabilidad civil, responsabilidad contractual, penalizaciones, resolución de contratos, etc.
- Posible responsabilidad penal de la persona jurídica.

2. Obstáculos y retos

2.1 ¿Por qué está costando en las empresas montar un sistema de diligencia debida en la cadena de suministro?

Desde **EcixTech** hemos podido ayudar a muchas organizaciones a implantar de forma eficaz este sistema de TPC. Son varios los retos complejos a los que se enfrentan los profesionales que tienen algún tipo de competencia en esta materia, como son los Responsables de Compras, Compliance Officers, Delegados de Protección de Datos, Chief Information Security Officers, etc. Entre ellos:

- Cada vez hay más normas que obligan a implantar un sistema de diligencia debida previa a la contratación con terceros en materias como Protección de Datos, Compliance, Ciberseguridad y Resiliencia, Sostenibilidad, Derechos Humanos, etc. La tendencia es que este tipo de obligaciones crecerá para las empresas, que además tendrán la obligación de acreditar que han implantado estos controles de manera efectiva.
- En algunos casos, la obligación no acaba solo con la fase de homologación previa a la contratación, sino que resulta necesario monitorizar dicha relación de manera continua.

- Existen normas, pero no hay desarrollo legislativo que contenga el detalle de cómo realizar esa labor de diligencia debida, hasta dónde hay que llegar para dar por cumplida esa obligación, qué umbrales de riesgo podrían ser aceptables, etc.
- El volumen de terceras partes en una entidad es algo que es necesario saber manejar de forma previa a implantar un modelo. La aplicación de procesos de diligencia debida muy ambiciosos, cuando se trabaja con miles de proveedores, implica dotarse de importantes recursos con los que es mejor contar de antemano para saber que podremos cumplir los objetivos que se persiguen.
- La velocidad y exigencia de los negocios muchas veces se enfrenta a la burocracia y/o lentitud que en ocasiones supone el seguimiento de estos procesos de diligencia debida, p.e. ante la necesidad de comenzar un proyecto con una tecnología concreta o contar con un servicio estratégico de un proveedor.
- No existe un modelo de Gobierno único y aplicable a todos los tipos de compañías en el que estén perfectamente fijadas las responsabilidades y competencias de las áreas involucradas: Compras, Compliance, Protección de Datos, Ciberseguridad, Riesgos, etc. Asimismo, al no existir un modelo único, muchas veces esas tareas están muy fragmentadas por lo que cada área avanza como puede y en muchos casos el resultado son procesos ineficientes que realmente no mitigan riesgos, la generación de molestias y burocracia a proveedores, el envío de comunicaciones contradictorias en los procesos de homologación, etc.
- Aunque se haya realizado un proceso de diligencia debida previo a la contratación de un tercero, después no se cuenta con los recursos para dar seguimiento al cumplimiento del SLA y la correspondiente monitorización continua que muchas de estas relaciones de negocio requieren.
- Falta de visibilidad por parte de la Dirección de la compañía de que haya un riesgo real, salvo que ya se hayan visto involucrados en algún escándalo o incidente grave con un proveedor. En algunos casos también existe una falsa sensación de seguridad basada en la mera existencia de contratos con proveedores que aceptan todo tipo de condiciones impuestas por la empresa compradora de sus servicios y productos, pero donde no se ha llevado a cabo ningún tipo de evaluación previa sobre su sistema de Compliance, Ciberseguridad, Protección de datos, Derechos Humanos, etc.

A todos estos aspectos, algunos de ellos vulnerabilidades endógenas de la empresa, hemos de sumarle los elementos exógenos, donde las noticias sobre los riesgos de terceros y el impacto que tienen en los negocios en algunos casos son alarmantes. Según el reciente informe publicado por ForgeRock sobre brechas de seguridad “ha aumentado un 297% en el número de infracciones relacionadas con ataques de terceros/supply chain, el acceso no autorizado representa el 50% de todas las violaciones, y el coste medio de un ataque en los Estados Unidos alcanza los 9,5 millones de dólares”.

Si hablamos de Corrupción y Cumplimiento, el Índice de Percepción de la Corrupción que publica anualmente Transparencia Internacional afirma que “dos años después del inicio de la catastrófica pandemia de covid-19, el Índice de Percepción de la Corrupción (CPI) advierte que el nivel de corrupción se encuentra estancado en todo el mundo. A pesar de sus compromisos sobre el papel, 131 países no han registrado ningún avance significativo en la última década, y este año 27 países se encuentran en el nivel más bajo de su trayectoria”

Todo ello hace que los aspectos relativos a las relaciones con terceros se hayan convertido en un punto importante en la agenda de las áreas de Gestión de Riesgos en las compañías y un ítem importante a desarrollar y/o mejorar en los próximos meses.

3. Claves prácticas para implantar un sistema de diligencia debida en la cadena de suministro

Para lograr diseñar e implantar un buen sistema de Third Party Compliance (TPC) con éxito en la cadena de suministro será necesario tener en cuenta varios aspectos. Aquí reflejamos algunos:

3.1 Análisis del contexto actual de la entidad

Es decir, conocer de dónde partimos:

- Si ya existe algún proceso de homologación y clasificación donde a los proveedores se les solicita información sobre estatutos, cuentas, seguros, solvencia técnica y económica, se les asigna un determinado nivel de riesgo, etc.
- Quién se encarga (si alguien lo hace) de solicitud de documentación, altas, interlocución con terceros, negociación de contratos, seguimiento de SLA´s, revisión de documentación, etc.
- Cuáles son las herramientas y procesos que se siguen actualmente: herramienta general de gestión de proveedores, herramientas de clasificación de proveedores, ofimática, work-flows de contratos, generación de pedidos, etc.
- Indicadores existentes: número de proveedores actuales, promedios anuales de nuevos proveedores, empresas solicitantes que finalmente no son homologados, renovaciones contractuales anuales, clasificación por categorías, etc.

3.2 Definición de un sistema de diligencia debida flexible

Es necesario un sistema que permita distinguir unos procedimientos más exigentes y otros menos robustos en base a diferentes criterios: la diferente tipología de terceros (proveedores), el nivel de riesgo/cumplimiento del tercero, los posibles impactos para la empresa y el confort con el contenido y alcance de la diligencia ejecutada.

De esta manera, pueden convivir diferentes estadios de profundidad, canalizando a cada proveedor en el que corresponda, por ejemplo, formulario básico de preguntas, formulario avanzado, solicitud de evidencias, petición de certificaciones y documentación, reunión con DPO, CISO, Compliance de la empresa proveedora, auditoría presencial, etc.

Incluir a todos los proveedores, de todo tipo, a través de un único mecanismo de diligencia debida podría derivar en situaciones ilógicas y desequilibradas, dedicando demasiado esfuerzo a proveedores y servicios que no lo requieren, y quizá menos esfuerzo a otros que requerirían mucho más para realizar una correcta gestión de ese riesgo.

3.3 Decisión de contar con herramientas que permitan automatizar gran parte de las tareas que implica operar un sistema de TPC, y le dote de la agilidad que el negocio necesita.

Una vez que se ha definido un modelo de gestión y se han aprobado los procedimientos adecuados es necesario contar con recursos personales y herramientas que operen el día a día de este sistema implantado, debiendo contar con las garantías suficientes para lograr los objetivos que se plantearon.

En este sentido, contamos con dos herramientas muy útiles para gestionar un sistema de diligencia debida:

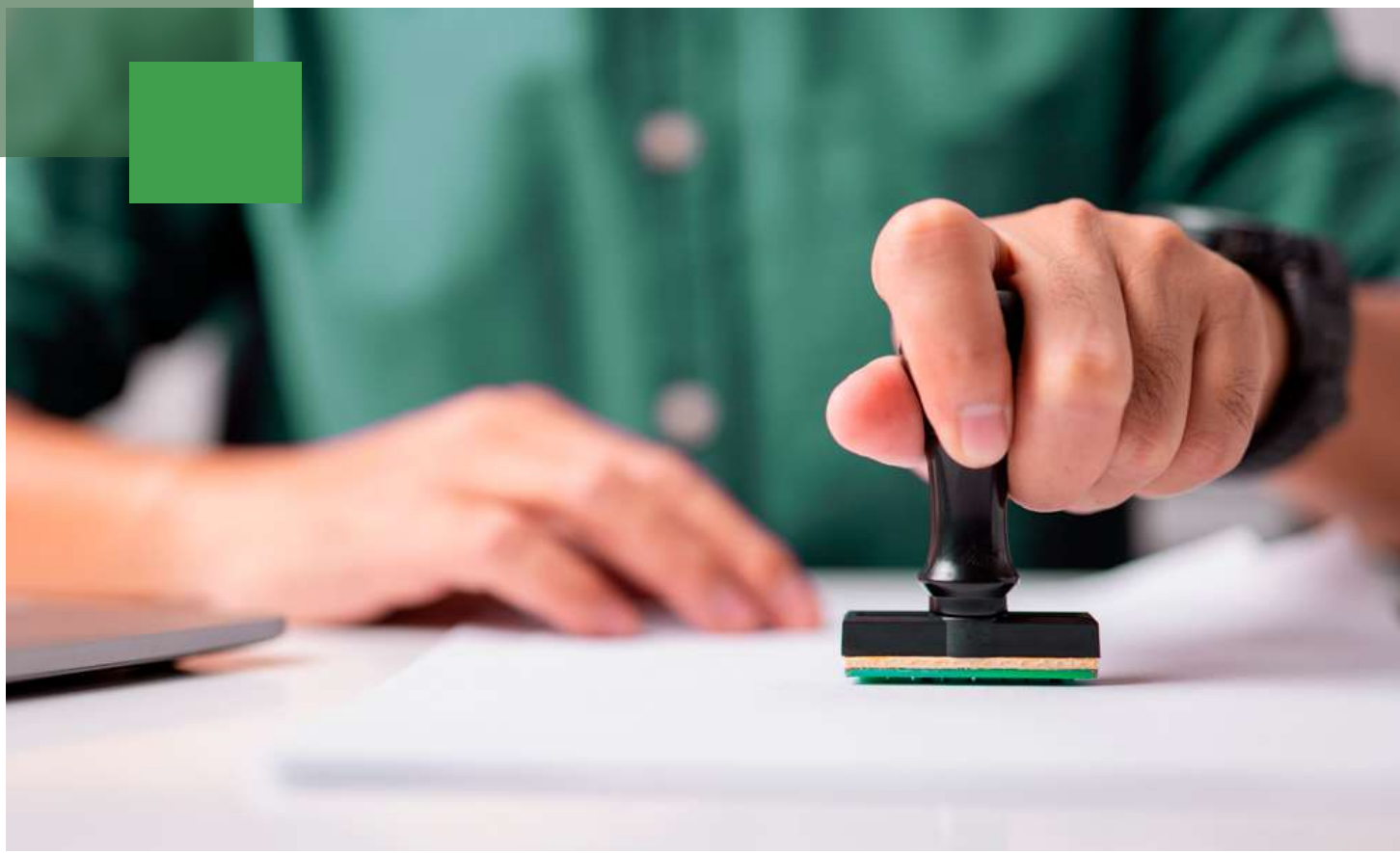
- **eTPC**: herramientas de gestión de formularios y proveedores, clasificación en base a riesgos e impactos, gestión de controles y monitorización de relaciones, etc.
- **MIA**: herramienta de revisión documental incorporando Inteligencia Artificial, que permite revisar en segundos las evidencias y documentos entregados por proveedores y tener una clasificación automática de sus niveles de cumplimiento/riesgo.

3.4 Conocimiento de estándares y buenas prácticas del mercado

El hecho de tener varias normas que regulan estas obligaciones, pero ningún detalle sobre su contenido y alcance hace que sea aconsejable considerar este tipo de documentos. Por ejemplo, el ISMS Forum ha desarrollado diversas iniciativas para facilitar estos sistemas:

- A través del Data Privacy Institute, desarrolló la "Guía Práctica para la gestión de terceros".
- Ofrece un curso a profesionales titulado "Gestión de Riesgo IT en la cadena de suministro".
- Está trabajando en una certificación acreditada para empresas que sean encargados de tratamiento.

Por último, existe una previsión optimista sobre la aparición de diferentes certificaciones que ayudarán a las empresas proveedoras a ganar confiabilidad y demostrar con mayor facilidad a sus clientes que son compañías comprometidas con el cumplimiento, sometidas a auditorías y revisiones periódicas para acreditarlo.



3.5 Establecimiento de un Modelo de Gobierno para TPC

Es fundamental trabajar en un modelo de Gobierno donde queden perfectamente fijadas las responsabilidades, tareas y objetivos de cada área y función que participe de alguna manera en ese proceso: Compras, Jurídico, DPO, Compliance, Ciberseguridad, etc.

3.6 Concienciación a la Dirección

Es necesario incluir en las acciones de concienciación a Dirección determinada información sobre lo que puede suponer el riesgo de terceros y crear una cultura de riesgo más allá del perímetro de nuestra empresa, haciendo visible los posibles impactos que podría tener un problema o escándalo por parte de un proveedor.

4. Retos para empresas proveedoras que deben acreditar su cumplimiento

Como venía diciendo en los artículos anteriores, los aspectos relativos a las relaciones con terceros se han convertido en un punto importante en la agenda de las áreas de Gestión de Riesgos en las compañías y un ítem importante a desarrollar y/o mejorar en los próximos meses.

Los “sufridores” que tienen que enfrentarse a esos procedimientos de diligencia debida son las empresas proveedoras que trabajan o tiene la expectativa de trabajar para una organización que tiene la obligación de realizar un examen de garantías de cumplimiento de manera previa a su contratación.

Desde este punto de vista, lo más habitual es que las entidades compradoras, los clientes, especialmente grandes compañías, invitan a empresas proveedoras a someterse al proceso de homologación de la compañía, donde se escrutan, entre otras cuestiones los aspectos referidos a Compliance, Protección de Datos, Ciberseguridad, Responsabilidad Social, etc.

Por otro lado, de manera poco habitual, existen grandes proveedores internacionales, especialmente en el mundo tecnológico, que tienen una posición de poder en la relación con sus clientes y donde existe poco margen de negociación de cualquier aspecto, adhiriéndose a unas condiciones generales y aceptando su estado de situación en cuanto a garantías de cumplimiento y ciberseguridad (normalmente muy altas y basadas en estándares internacionales).

Yendo a situaciones habituales, existen tantos procesos de diligencia debida diferentes como clientes, por lo que normalmente a los proveedores les llegarán formularios, peticiones de documentación, reunión de toma de datos, requerimientos de auditorías (en algunos casos), etc.

Desde el punto de vista de la empresa proveedora, para superar de la mejor manera tales procesos de diligencia debida y demostrar un alto nivel de confianza, considero que es importante:

4.1 Reforzar internamente las áreas relacionadas con Compliance, Protección de Datos, Ciberseguridad, etc.

Con profesionales que lideren esas áreas, que tengan los recursos, apoyo y herramientas necesarias, y tengan una visión muy clara de la protección de los activos propios de la compañía, así como la protección de los activos de los clientes con los que contratan.

A nivel de Compliance deberán demostrar que son una empresa sólida con una cultura de cumplimiento importante y que tiene mecanismos para gestionar sus riesgos. En materia de Ciberseguridad será necesario demostrar que sus productos, herramientas, infraestructuras, servicios... cuentas con las medidas de protección adecuadas y que tienen los mecanismos necesarios para gestionar cualquier ciberincidente. En materia de protección de datos, en muchos casos, serán considerados encargados de tratamiento, lo que conlleva unas responsabilidades establecidas en la Ley y también, de manera más concreta, en el contrato de encargo de tratamiento que deberán firmar con su cliente, el responsable de tratamiento. Si bien, existe esa obligación de diligencia debida previa a la contratación, donde la empresa cliente únicamente podrá contratar con un proveedor que acredite las garantías suficientes para cumplir la normativa y medidas de seguridad necesarias.

4.2 Dedicar tiempo y equipos a mejorar el nivel de acreditación de procedimientos y políticas para lograr más confianza en clientes.

Es fundamental apoyar desde estas áreas en las labores de pre-venta de la organización, ya que, con independencia de aspectos clave como la funcionalidad de un producto o su precio, las empresas clientes se interesarán muy pronto por los temas de Compliance, Privacidad y

Ciberseguridad.

Para ello, se puede trabajar en diferentes frentes:

a. Dotar a los cargos de DPO, Compliance Officer, CISO, etc. (o sus equipos) de capacidad de interlocución con clientes finales en procesos de homologación, negociación contractual, seguimiento y monitorización para trasladar una explicación del sistema de seguridad y cumplimiento que está implantado en la empresa proveedora.
b. "Paquetizar" un modelo documental que acredite todos estos aspectos. Será muy positivo cuanto más organizada esté, su orientación sea más empática con la figura del cliente y sus necesidades, más fácil de consultar sea, esté en los idiomas que normalmente se trabaje con clientes, contenga un sistema idóneo de actualización, esté muy vinculado al servicio o producto que se ofrece, etc.
c. Alinear esos programas a estándares internacionales, conocidos por todos los clientes, que permitan una interlocución más fácil, un alineamiento de sistemas de control entre diferentes normas y mayor facilidad para responder a las preguntas y solicitudes de documentación de cualquier cliente en sus procesos de diligencia debida.
d. Implantar un sistema de control que contemple el envío de actualizaciones y evidencias de cumplimiento durante el contrato. El seguimiento de los SLA por parte de muchas organizaciones es difícil de realizar y en ocasiones esa tarea queda huérfana. Cuando el proveedor se adelanta a ello y actualiza información de este tipo es bienvenida y da sensación de garantía y confort, aparte de cumplimiento normativo y/o contractual.

4.3 Diseñar y mantener un plan de Certificaciones actuales y futuras

Las certificaciones empresariales son un instrumento útil para acreditar ante clientes que se ha implantado y auditado por un tercero un sistema de cumplimiento en muy diversas materias.

En este sentido, son muy conocidas y aceptadas, entre otras:

a. En Compliance: ISO 37301 (sistema de gestión de cumplimiento), ISO 37001 (sistemas anticorrupción), UNE 19601 (sistema compliance penal) y UNE 19602 (sistema compliance fiscal)
b. En Ciberseguridad: ISO 27001 (sistema de gestión de seguridad), ENS (Esquema Nacional de Seguridad), CSA STAR CCM (servicios de Cloud), ISO 22301 (Continuidad de Negocio)
c. En Protección de Datos: ISO 27701 (sistema gestión de privacidad) y algunas nuevas que se están gestando.

El propio RGPD, en su artículo 42 regula la promoción por parte de los Estados, las Autoridades de Control, la Comisión y el Comité, de "la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados"

Desde ISMS Forum se está trabajando en el desarrollo de una nueva certificación que verá en unos meses la luz para prestadores de servicios que tienen la categoría de encargados de tratamiento, y cuyo objetivo es facilitar y agilizar la operativa de los procesos de diligencia debida entre responsables de tratamiento y sus proveedores (encargados de tratamiento).

4.4 Implantar a su vez un proceso de TPC para sus proveedores

Estos actúan como subcontrataciones (subencargados de tratamiento en el caso de protección de datos) de cara a los clientes. Es fundamental mantener el nivel de exigencia en la cadena de suministro, y cuando un proveedor da garantías a sus clientes, debe consolidar un modelo de control y diligencia debida con sus propios terceros.

5. Conclusiones

En un entorno empresarial cada vez más complejo y regulado, es fundamental que las empresas presten atención a la gestión de riesgos relacionados con terceros y proveedores. **La falta de diligencia debida en este ámbito puede llevar a multas, sanciones y dañar la reputación de la empresa.**

Además, es importante que **las empresas proveedoras preparen sus procedimientos y políticas para resultar "atractivas"** también en términos de cumplimiento y ciberseguridad de cara a sus clientes. Todo ello les ayudará a un mejor cumplimiento de las normas y también a dar las necesarias garantías ante los procesos de diligencia debida de dichas empresas.

5.1 Recomendaciones

Recomendamos a las empresas llevar a cabo estas acciones:

1. Revisar el estado actual de los procesos implantados, y contrastarlo con el marco normativo, nuevas exigencias, carencias, técnicas, necesidad de procedimientos y nombramientos, etc.
2. Decidir una tecnología adaptada a la norma y fiable, desde el punto de vista de seguridad y privacidad. Valorar la posibilidad de contar con apoyo externo para la recepción de información.
3. Adaptar internamente a la política y procedimientos del sistema a los requisitos de la norma.
4. Preparar una campaña de comunicación y formación a todas las partes implicadas sobre la necesidad de la diligencia debida y de cómo actualizarse.

5.2 Cómo implementar una solución para cumplir la normativa

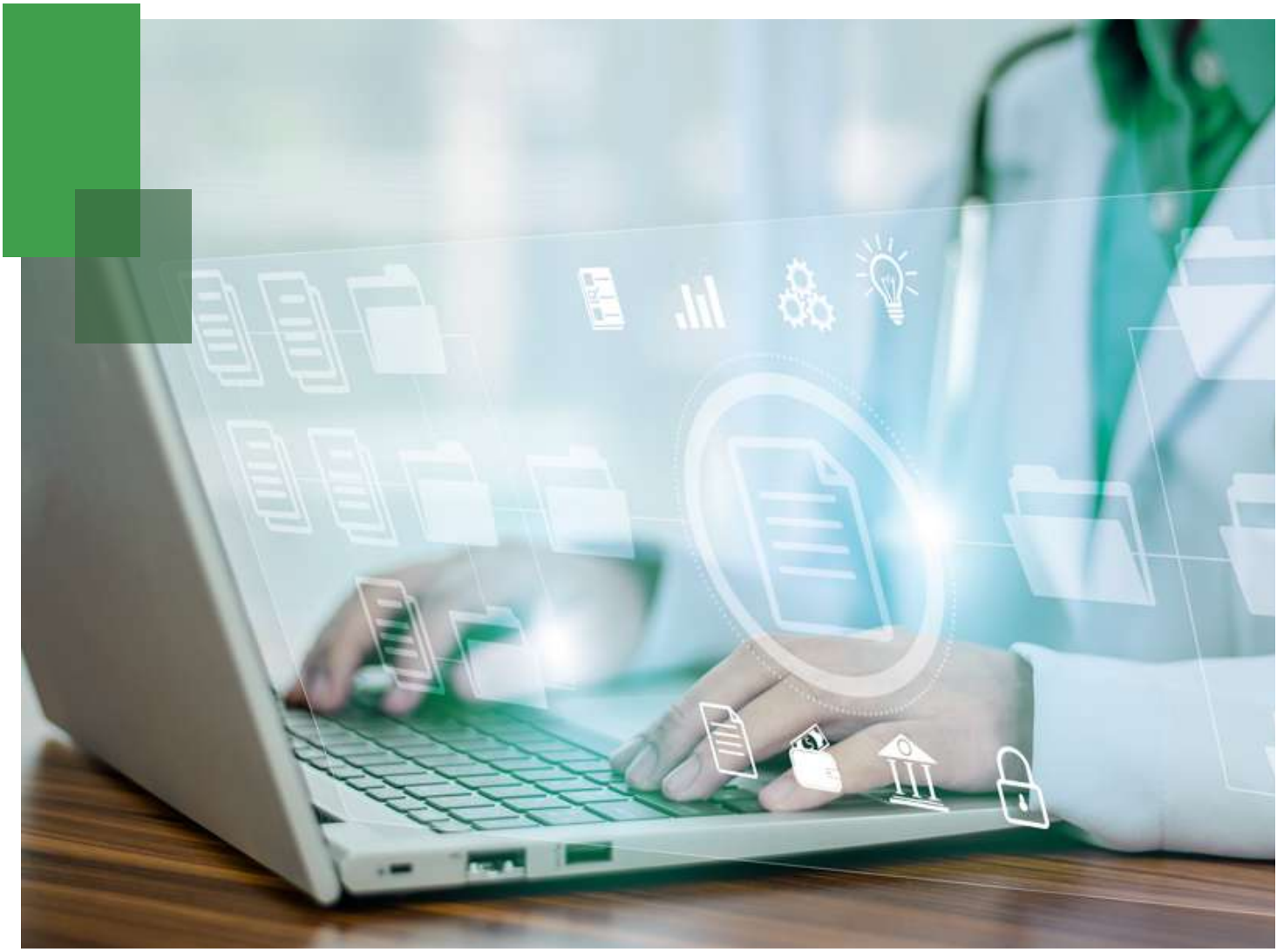
Existe una importante presión regulatoria para identificar y prevenir riesgos, previa a la contratación de terceros y durante su relación con ellos. Contar con una correcta estrategia es este punto, es fundamental para el éxito del cumplimiento normativo en 2023.

Dada la complejidad de este tipo de soluciones, nuestra recomendación es trabajar en dos tipos de actuación:

5.2.1 Utilizar tecnología que permite controlar de manera sencil la el nivel de cumplimiento y confiabilidad de terceras partes y proveedores

Existen varias herramientas tecnológicas en el mercado, pero no todas ofrecen una respuesta completa a las necesidades de una organización. Es importante contar con una que permita:

- Simplificar procesos y clasificar las relaciones según una matriz de riesgos que tenga en cuenta las limitaciones legales relevantes para cada empresa.
- Monitorizar los eventos críticos como la aparición de terceros en listas de sanciones, brechas de privacidad o procesos judiciales.
- Parametrizar la plataforma con su logo y ser accesible de forma independiente y clara.
- Mostrar una matriz que ofrezca la perspectiva óptima que las empresas necesitan para tomar las acciones oportunas.



5.2.2 Externalizar el diseño e implantación de programas globales de evaluación de terceras partes

Mitigar riesgos potenciales y certificar la diligencia debida es un proceso que muchas veces requiere de ayuda especializada.

El asesoramiento de un experto externo puede ayudar a mejorar la eficiencia y eficacia de la gestión empresarial al reducir los riesgos de incumplimiento normativo, evitar conflictos de interés, mejorar la productividad y reducir el tiempo y los recursos dedicados a la gestión de riesgos.

En caso de que la organización opte por contar con apoyo externo para la gestión del programa de Third Party Compliance, el tercero externo deberá garantizar el principio de independencia, el derecho de confidencialidad y la protección de los datos personales comunicados por las partes intervinientes.

Las empresas que deseen tener un control efectivo sobre el nivel de cumplimiento de terceras partes y proveedores deberían considerar una tecnología que les permitirá simplificar y centralizar sus procesos de gestión de relaciones con terceros, clasificar a sus proveedores según su nivel de riesgo, y mitigar posibles riesgos potenciales a través de la certificación de la diligencia debida.

6. EcixTech

Como especialistas en Derecho Digital y Cumplimiento Normativo, EcixTech puede ayudarte a afrontar los retos a los que las funciones de Ciberseguridad, Compliance, Riesgos y Privacidad se van a enfrentar en el nuevo escenario empresarial con nuestros servicios especializados y herramientas pioneras.

Asesoramos desde hace más de 20 años en las áreas de Ciberseguridad, Compliance y Protección de Datos a las principales empresas españolas. En EcixTech prestamos un servicio de primer nivel mediante un equipo de más de 150 profesionales especializados y una Metodología propia fruto del resultado de la investigación y la aplicación de Inteligencia Artificial, matemáticas y Big Data.

Desde 2002 desarrollamos herramientas que ayudan a nuestros clientes en la identificación y gestión de riesgos legales y empresariales. Desde soluciones de Protección de Datos, Cookies, Consentimientos, GRC, evaluación de terceras partes (TPC), Formación y Concienciación, etc.

Conoce nuestras soluciones Regtech que te ayudarán a ser más eficiente y evitar multas y sanciones evidenciando el cumplimiento de tu empresa en ***https://ecix.tech/***.

www.ecix.tech