RIESGOS NORMATIVOS EN EL PROCESO DE REACTIVACIÓN DE LA ACTIVIDAD EMPRESARIAL

ECIJA

Índice

Introducción

Con la llegada a Europa y más concretamente a España del COVID-19, el país vio interrumpida, en mayor o menor medida, su actividad en todos sus ámbitos, social, laboral y económico. Tras la declaración, el 11 de marzo, por parte de la OMS (Organización Mundial de la Salud), del COVID-19 como pandemia, hemos venido enfrentándonos a una situación absolutamente excepcional de la que no conocemos cual puede ser su duración, su impacto final o incluso si se perdurará en el tiempo al menos de forma parcial.

En este escenario el Gobierno, comunidades autónomas y ayuntamientos, entre otras administraciones, han tomado numerosas medidas para hacer frente a la pandemia, destacando las medidas de confinamiento, restringiendo la libertad de movimiento individual y el cierre temporal de varios sectores de actividad económicos, destacando aquellos relacionados con hostelería y servicios, todo ello con la finalidad última de evitar la extensión del contagio. Cuestiones que han puesto de manifiesto la necesidad de avanzar en nuevas formas de organización del trabajo, tales como la adopción efectiva de políticas de teletrabajo, intensamente recomendadas por las administraciones.

Durante la pandemia se han publicado un buen número de nuevas normas, y todo ello bajo el paraguas del Real Decreto 463/2020, publicado el 14 de marzo por el que se declaró el estado de alarma para la gestión de la situación de crisis sanitaria, por un plazo de 15 días el cual, a día de hoy, ha sido prorrogado hasta en cinco ocasiones.

Con un posible final del periodo del estado de alarma más cercano y ante la perspectiva de rebajar las medidas de confinamiento y reactivar la actividad económica, se aprobó el 3 de mayo desde el ejecutivo, de acuerdo con criterios sanitarios, un plan de desescalada, para permitir de forma gradual que las diferentes organizaciones pudieran ir retomando la normalidad de sus actividades.

Esto, no obstante, deberá realizarse cumpliendo con todas las medidas de seguridad y criterios del Ministerio de Sanidad, lo que ha generado incertidumbre y situaciones de duda sobre las obligaciones y medidas que deben implementarse a la hora de retomar y reactivar la actividad profesional. Ante la anterior situación de incertidumbre e inseguridad jurídica, conviene que, las organizaciones actúen en todo momento siguiendo criterios de diligencia debida y evaluación de los riesgos derivados de un potencial incumplimiento o la necesidad de reevaluar, de manera continua, las medidas que deben ser adoptadas.

Estas cuestiones se han manifestado en diferentes materias y bloques de cumplimiento, siendo algunas de éstas, que generan alta preocupación entre las diferentes organizaciones, las normas de ámbito laboral, penal o de protección de datos.

Por todo ello, antes de tomar una decisión, será recomendable para las empresas, contar con un análisis de riesgos normativo propio de los sistemas de Compliance en cualquiera de las tres áreas identificadas. De esta forma no sólo se conocerán los posibles impactos negativos de las mismas, sino que se dejará constancia de que las decisiones han sido tomadas con la diligencia debida, teniendo muy en cuenta los posibles riesgos existentes y en su caso adoptando las medidas tendentes a la evitación del mismo. Cuestiones que posibilitan, igualmente, la acreditación de las propias obligaciones legales, como es el caso de la normativa sobre protección de datos y la realización de análisis de riesgos y evaluaciones de impacto. Por todo lo anterior y, teniendo en cuenta las cuestiones comunes en las tres áreas analizadas, tener una visión completa, no sólo mitiga riesgos y por tanto posibles contingencias, si no que facilita una mayor eficacia y coordinación en los procesos de gestión.

Análisis y evaluación de riesgos normativos

Para el análisis y evaluación de riesgos normativos es muy recomendable seguir los estándares internacionales y hacer uso de las metodologías propias de gestión de Riesgos y de Compliance de las ISO 31000 y 19600 cada organización deberá seguir los siguientes pasos a la hora de realizar un plan de tratamiento de riesgos normativos asociados a esta situación excepcional:

1- Identificación de situaciones de hecho o actividades propias de la desescalada aplicables a su caso que podrían generar un riesgo normativo
2- Identificación de amenazas normativas asociadas
3- Definición de Indicadores para la evaluación del riesgo
4- Análisis de riesgos y sanciones aplicables
5- Establecimiento de medidas mitigadoras de los riesgos identificados.

En la presente nota, a modo de ejemplo seguiremos este proceso de forma general, sin tener en cuenta un tipo de actividad concreta o las situaciones de hecho y circunstancias particulares que se podrían dar en cada empresa. Esta nota no se puede tomar, por lo tanto, como una evaluación de riesgos que pueda seguirse de manera exhaustiva por las empresas, no obstante, lo cual, sí puede servir como punto de partida, para que el análisis se realice de una forma individualiza por cada organización, teniendo en cuenta por cada Comité de Compliance o Compliance Officer las especiales características de su empresa, para después poder facilitar el resultado de su análisis al órgano de Administración.

SITUACIONES DE HECHO HABITUALES ASOCIADAS A LA VUELTA AL TRABAJO TRAS EL ESTADO DE ALARMA

Desde ECIJA se han identificado y enumerado varios supuestos de hecho que, dada la situación actual, se entienden pueden darse dentro de las diferentes organizaciones y que pueden generar dudas, confusión, o incluso llevar a las mismas a incurrir o en algún tipo de infracción normativa, o al incumplimiento de los controles introducidos a raíz de Programas de Compliance implementados con anterioridad, debilitando así los sistemas normativos internos ya implementados, o exponiendo a las mismas indirectamente a posibles sanciones:

SITUACION DE HECHO	CATEGORÍA DE AMEZANA
1.- Control temperatura en el acceso al centro de trabajo	LABORAL
	PROTECCIÓN DE DATOS
2.- Realización test serológicos y pruebas PCR.	LABORAL
	PROTECCIÓN DE DATOS
3.- Cuestionarios a trabajadores de cara a identificar quien se puede incorporar o no al trabajo: estado de salud, enfermedades, datos de familiares, edad, cómo van al trabajo, etc.	LABORAL
	PROTECCIÓN DE DATOS
4.- Cuestionarios a personal externo que visita las instalaciones de la empresa: visitas a países de alta prevalencia del virus, sintomatología, etc.	LABORAL
	PROTECCIÓN DE DATOS
5.- Incumplimiento por parte de los trabajadores de las medidas establecidas por la entidad: no llevar mascarilla o guantes cuando se estipule su obligatoriedad, etc.	LABORAL
	PENAL

	PROTECCIÓN DE DATOS
6.- Obligatoriedad de que el personal comunique su situación de cuarentena preventiva o infección del COVID-19, contacto con positivos, etc.	LABORAL
	PENAL
7.- Comunicaciones a las autoridades sanitarias sobre personal infectado en su puesto de trabajo.	LABORAL
	PROTECCIÓN DE DATOS
8.- Posible comunicación de trabajadores que hayan dado positivo a las personas con las que tuvo contacto: proveedores, clientes, otros trabajadores.	LABORAL
	PROTECCIÓN DE DATOS
9.- Identificación del personal especialmente vulnerable	LABORAL
	PROTECCIÓN DE DATOS

10.- Teletrabajo: riesgos de pérdida de información.	PENAL
	PROTECCIÓN DE DATOS
11.- Teletrabajo: riesgos laborales (trabajador a distancia), política de uso de medios y riesgos en materia de PRL.	LABORAL
	PENAL
	PROTECCIÓN DE DATOS
12.- Incorporación a la oficina: coordinación de actividades con proveedores y clientes, riesgo grave e inminente, protección de los trabajadores y Servicio de Prevención de Riesgos Laborales.	LABORAL
13.- Desarrollo de planes de desescalada que conlleven la reincorporación de los trabajadores a las oficinas.	LABORAL
	PENAL
14.- Formación e información a los trabajadores.	LABORAL
	PROTECCIÓN DE DATOS

Identificación de amenazas normativas

RIESGOS EN MATERIA LABORAL Y DE PREVENCIÓN DE RIESGOS LABORALES

Con respecto a las posibles amenazas normativas en materia laboral habrá que tener en cuenta como regla general, la importancia de que cualquier actuación sea informada y realizada juntamente con el Servicio de Prevención de Riesgos, habitualmente externalizado a una empresa diferente de la empleadora, en la medida en que esta entidad adopta el rol preventivo y material de las actuaciones relacionadas con la salud y a la seguridad de la plantilla. Asimismo, será esencial, en todo momento, atender a los criterios definidos por las autoridades sanitarias, tanto en lo relativo a su utilidad como a su proporcionalidad.

Desde el punto de vista laboral, el riesgo principal está en la **falta de cumplimiento de los requisitos establecidos en el artículo 22 de la Ley 31/1995**, de 8 de noviembre, de prevención de Riesgos Laborales. El artículo 22 de la Ley de Prevención de Riesgos laborales exige la vigilancia de la salud (en adelante, "**LPRL**") de los empleados por parte de la empresa. Para ello, se requiere la correspondiente evaluación de riesgos, que ha de incluir los reconocimientos médicos. Este mismo artículo recoge la forma de actuar en los reconocimientos médicos, que, en resumen, requieren el respecto del carácter voluntario y confidencial principalmente por respeto a la intimidad frente al poder empresarial. Sin embargo, ningún derecho es absoluto y caben excepciones y matices recogidas en la propia ley.

RIESGOS EN MATERIA DE PRIVACIDAD Y PROTECCIÓN DE DATOS

Las situaciones de hecho identificadas, muchas de ellas tendentes a cumplir con las medidas y recomendaciones previstas por las autoridades competentes, conllevan la necesidad de que las empresas realicen tratamientos de datos personales que, como tal, deben ajustarse a las previsiones de la normativa de protección, lo que implica la necesidad de que el empleador aplique los principios y obligaciones recogidos en la normativa la protección de datos.

Estos aspectos, han puesto de manifiesto, junto con la utilización de las nuevas tecnologías, las diferentes tipologías de datos que pueden derivarse. En este sentido, los nuevos tratamientos implicarán el tratamiento de datos de salud o de determinada información derivada de la utilización de sistemas de reconocimiento facial (datos biométricos), geolocalización, entre otros, que pueden ser considerados como categorías especiales de datos, lo que conlleva la adopción de medidas adicionales al objeto de garantizar la protección de esta categoría de datos.

La AEPD insiste en que las nuevas actividades de tratamiento deben realizarse respetando en todo caso los **principios generales** recogidos en el artículo 5 del RGPD, tomando especial consideración en el: (i) **principio de limitación de la finalidad**, en la salvaguarda de la salud de los trabajadores y de terceros en riesgo de contagio; (ii) el **principio de minimización** de datos, limitando los datos tratados a los necesarios para tal finalidad y; (iii) el principio de **limitación del plazo de conservación**, bloqueando o suprimiendo los datos personales cuando dejen de ser necesarios para el cumplimiento de la finalidad descrita.

En el ámbito de protección de datos se ha tomado como referencia la siguiente normativa:

- 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 (en adelante, "**RGPD**");
- Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos de Datos Personales y garantía de los derechos digitales (en adelante, **"LOPDGDD");**
- Informe de la Agencia Española de Protección de Datos 0017/2020, sobre el tratamiento de datos de salud, en relación con la situación derivada del COVID-19 (en adelante, el "**Informe**").
- FAQS publicadas por la Agencia Española de Protección de Datos en relación con el COVID-19.
- Declaración del Comité Europeo de Protección de Datos sobre el tratamiento de datos personales en el marco del COVID-19.
- Nota en relación con los tratamientos de datos personales relacionados con las medidas para hacer frente al COVID-19, de la Agencia de Protección de Datos Catalana.

El inicio y desarrollo de las nuevas operaciones de tratamiento surgidas a partir del COVID-19 pueden generar riesgos que se materialicen en un daño o perjuicio a los interesados cuyos datos personales son objeto del tratamiento.

Desde el punto de vista de protección de datos, las principales amenazas que pueden traer consigo las mencionadas actividades de tratamiento sin adoptar las correspondientes medidas técnicas, organizativas y jurídicas al objeto de proteger a los interesados son las siguientes:

- Tratamiento ilícito por no contar con una base de legitimación acorde al RGPD.

- Realizar un tratamiento de datos perteneciente a la categoría especial de datos sin la concurrencia de alguna de las bases de legitimación del artículo 9 del RGPD.
- Omisión del deber de información del Empleador a los interesados conforme a los artículos 13 y 14 del RGPD.
- Comunicaciones de datos personales a terceros no autorizados o sin contar con una causa legitimadora.
- Falta del cumplimiento de los principios recogidos en el art.5 RGPD, entre ellos, principio de minimización y limitación del tratamiento, utilizando más datos de los necesarios para llevar a cabo la finalidad.
- Falta de limitación del plazo de conservación de los datos, bloqueando o suprimiéndolos cuando dejen de ser necesarios para el fin para el que fueron recabados.
- Omisión de la obligación de realizar una evaluación de impacto en materia de protección de datos, en caso de resultar una actividad de tratamiento con un nivel de riesgo alto.
- Incumplimiento de las obligaciones relativas a la detección y comunicación de brechas de seguridad de datos personales.
- Falta de atención y gestión de los derechos recogidos en los artículos 15 al 22 del RGPD.
- Vulneración del deber de confidencialidad.
- Falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño.
- Falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento.
- Falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento.
- Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido en el RGPD.

Con respecto a las sanciones aplicables, realizar el tratamiento de nuevas actividades en el entorno del COVID-19 sin adoptar las garantías y obligaciones previstas en la normativa en materia de protección de datos puede conllevar infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta **20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior**, optándose por la de mayor cuantía,**, atendiendo a los siguientes factores:**

- La naturaleza, gravedad y duración de la infracción;
- Las medidas tomadas por el Empleador para paliar los daños y perjuicios ocasionados;
- La intencionalidad o negligencia de la infracción;
- Historial, en su caso, de anteriores infracciones y el grado de colaboración prestado a la autoridad de control;

- La afectación o no datos pertenecientes a la categoría especial, y;
- La forma en la que la autoridad de control tuvo conocimiento de la infracción.

No debe olvidarse que las cuestiones referidas en el ámbito laboral, implican tratamientos de datos personales, que atañen a categorías especiales de datos, por lo que junto con la legitimación, existen determinados aspectos que han de considerar, como los plazos de conservación, la intervención de personal de seguridad en los procesos de tomas de temperaturas, la utilización de cámaras termométricas, o el establecimiento de nuevos sistemas de fichaje con la finalidad de evitar contagios (tales como sistema de identificación facial, por ejemplo). Igualmente, existen determinadas de comunicación de datos a las propias Administraciones, como las derivadas de la Orden SND/404/ de 11 de mayo del Ministerio de Sanidad.

Finalmente, debe recordarse que las cuestiones analizadas, no sólo afectan al personal de la propia empresa, si no también a la relación con los proveedores o en la desescalada a los propios cliente so usuarios, en tanto deben garantizarse las medidas de seguridad correspondientes de acuerdo con el sector de actividad, aspectos que afectan, de forma tangencial a otras cuestiones como la protección civil del derecho al honor, intimidad y propia imagen o el propio derecho de admisión. En todos estos casos, el análisis de los tratamientos de datos, deben ser entendidos como información que pueda posibilitar una identificación, en el momento o a posteriori, y la necesaria evaluación de los riesgos, derivados, no sólo de la tecnología a emplear, si no del propias finalidades y tratamientos posteriores que se puedan realizar.

RIESGOS EN EL ÁMBITO PENAL

Desde el punto de vista de Compliance Penal, y de los delitos que pueden ser atribuidos a la persona jurídica, cada supuesto, **está íntimamente ligado y deriva en mayor medida del incumplimiento por parte del empleador de las medidas en materia de prevención de riesgos laborales, y de los incumplimientos de dicha legislación.**

En este sentido, aclarar que el Código Penal regula una serie de delitos que son imputables a las personas jurídicas y por los que puede resultar penalmente responsable. En adición a este catálogo, deberán valorarse igualmente aquellos ilícitos respecto de los cuales, puedan resultar impuestas penas accesorias.

En este sentido, analizamos los delitos que podrían materializarse, o afectar a la persona jurídica en caso de incumplimiento de las obligaciones en materia de prevención de riesgos laborales:

Delito contra los derechos de los trabajadores

El artículo 318 del Código Penal, hace referencia a las penas atribuibles a las personas jurídicas en caso de cometerse actuaciones que den lugar a la comisión de delitos contra los trabajadores. Dentro de estas actuaciones el artículo 316 del Código Penal castiga a

"*Los que con infracción de las normas de prevención de riesgos laborales y estando legalmente obligados, no faciliten los medios necesarios para que los trabajadores desempeñen su actividad con las medidas de seguridad e higiene adecuadas, de forma que pongan así en peligro grave su vida, salud o integridad física*".

Respecto del tipo penal descrito, hay un destinatario claro de la obligación de respetar las obligaciones relativas a las medidas de seguridad e higiene legalmente impuestas, que es el empresario. A estos efectos corresponde precisar que esta obligación (y consecuente responsabilidad por incumplimiento) se extiende a las personas a las que el empresario delegue su deber de facilitación de medios para el adecuado cumplimiento de la norma.

La pena podrá ser impuesta tanto a administradores de la sociedad (no únicamente a los de derecho sino también a los de hecho, entendiéndose por aquellos quienes adopten e impongan las decisiones de la gestión de la sociedad), como a los encargados responsables de la infracción y a quienes, pudiendo remediarlo, no hubieran adoptado medidas para ello. La enumeración anterior incluiría por tanto a las **personas responsables de la toma de decisiones que pudiera suponer el incumplimiento de la normativa de Prevención de Riesgos Laborales** y a los componentes de los órganos internos o comités constituidos a tal efecto.

Se trata de un tipo penal de estructura omisiva o más bien una infracción de un deber que protege la seguridad en el trabajo. En este sentido, es una norma penal en blanco, lo que implica que, para constatar si hay un mínimo de trascendencia penal, la interpretación del incumplimiento se remite a la normativa laboral vigente en materia de Prevención de Riesgos Laborales.

Sin perjuicio, en su caso, de una posterior concreción exhaustiva de la normativa que en materia de seguridad y salud de los trabajadores pueda resultar de aplicación, con carácter general deberá estarse a lo previsto en la ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales y sus disposiciones de desarrollo o complementarias.

El artículo 3.1. de la citada norma refiere expresamente que sus disposiciones resultarán de aplicación a

"Esta Ley y sus normas de desarrollo serán de aplicación tanto en el ámbito ***de las relaciones laborales reguladas en el texto refundido de la Ley del Estatuto de los Trabajadores, como en el de las relaciones de carácter administrativo o estatutario del personal al servicio de las Administraciones Públicas****, con las peculiaridades que, en este caso, se contemplan en la presente Ley o en sus normas de desarrollo. Ello sin perjuicio del cumplimiento de las obligaciones específicas que se establecen para fabricantes, importadores y suministradores, y de los derechos y obligaciones que puedan derivarse para los trabajadores autónomos. Igualmente serán aplicables a las sociedades cooperativas, constituidas de acuerdo con la legislación que les sea de aplicación, en las que existan socios cuya actividad consista en la prestación de un trabajo personal, con las peculiaridades derivadas de su normativa específica. "*

A estos efectos resulta igualmente fundamental lo dispuesto en el Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, donde se recogen las sanciones administrativas cuyo incumplimiento podrían dar lugar a una posterior responsabilidad penal cuando con su omisión se pueda poner en riesgo grave la integridad o la salud de los trabajadores. En el anterior sentido habrá que establecer los **controles necesarios** para no incurrir en las sanciones previstas en los artículos 11 a 13 que reglan las infracciones, leves, graves y muy graves en materia de prevención de riesgos laborales.

La actividad de la empresa es un elemento esencial a tener en cuenta, ya que dependiendo de la misma y de si el contagio por el SARS-CoV-2 es o no un riesgo derivado de su actividad, aumentará o disminuirá el nivel de riesgo, de incurrir en sanciones derivadas del presente tipo penal. No obstante, el hecho de que el contagio no sea un riesgo derivado de la actividad, no exime a la empresa de evaluar el riesgo de exposición en que se pueden encontrar sus empleados en cada una de sus funciones y seguir las pautas y recomendaciones formuladas por las autoridades sanitarias con el fin de poder garantizar que su actividad se desarrolle en un entorno seguro.

- **Delito de lesiones imprudentes**

Desde un punto de vista penal, se entiende por lesión, el menoscabo en la integridad corporal, incluida la salud, física y mental de las personas.

Este menoscabo en la salud consecuencia del COVID-19, puede materializarse desarrollando una actividad laboral. En cuyo caso las lesiones provocadas por el contagio irían unidas al delito contra los derechos de los trabajadores.

No obstante, debemos tener en cuenta, el supuesto de que un tercero ajeno a la organización pueda contagiarse, por la imprudencia y negligencia del empresario, al no implementar las oportunas medidas de seguridad tanto para los empleados como para aquellas personas que no mantengan una relación laboral con la organización, pero que queden contagiadas.

Al no ser un delito atribuible a la persona jurídica, no se podría considerar responsable penalmente de la misma, por lo que no cabría una sanción penal sobre la misma, no obstante, si podría llegar a condenarse a la compañía a una **responsabilidad civil derivada del delito** sufrido por la víctima.

- **Delito de homicidio imprudente**

El Código penal recoge las características de este tipo en su artículo 142, concurriendo por el que por imprudencia grave causare la muerte de otro.

La materialización de este tipo penal, directamente relacionado con el contagio por COVID-19 en el ejercicio de la actividad laboral dependerá en todo caso, de poder probar el nexo causal entre el fallecimiento y el contagio por imprudencia y negligencia del empresario.

En relación con **estos dos últimos tipos penales** indicados, debemos señalar que ninguno es contemplado por el Código Penal como un delito susceptible de ser cometido por la persona jurídica, si bien, la persona jurídica si puede verse expuesta a una eventual responsabilidad civil subsidiaria, que le sea reconocida a la víctima.

Además del posible contagio por parte de los trabajadores, debemos tener en cuenta, el supuesto de que un tercero ajeno a la organización pueda contagiarse, por la imprudencia y negligencia del empresario, al no implementar las oportunas medidas de seguridad tanto para los empleados como para aquellas personas que no mantengan una relación laboral con la organización, pero que queden contagiadas.

Nuevamente, y tal como hemos expuesto, al no ser delitos atribuibles a la persona jurídica, no se podría considerar responsable penalmente de la misma, por lo que no cabría una sanción penal, pudiendo no obstante enfrentarse a una **responsabilidad civil con carácter subsidiario. Sí podrían enfrentarse como personas físicas, en concurso con el derecho del delito contra los derechos de los trabajadores (en caso de ser la victima un trabajador) los administradores de hecho o derecho de la empresa.**

Respecto a **las penas** que podrían llegar a imponerse en el orden penal, deberá diferenciarse entre:

Penas susceptibles de ser impuestas a administradores, encargados del servicio o quienes conociéndolo y pudiendo remediarlo no adoptaron medidas para ello: podrá imponerse una pena de prisión de seis meses a tres años y multa de seis a doce meses

Penas susceptibles de ser impuestas a la Persona Jurídica: Si bien sobre la misma no se determinará la responsabilidad penal, el órgano judicial podrá imponer a la organización, además de la obligación de satisfacer las responsabilidades civiles correspondientes, las siguientes medidas accesorias:

- Suspensión de sus actividades por un plazo que no podrá exceder de cinco años.
- Clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años.
- Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá ser temporal o definitiva.
- Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años.

- Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años.

De forma adicional la comisión de un delito de este tipo en una situación excepcional que afecta al interés general ocasionaría sin duda un **daño reputacional**, agravándose el mismo, si fuera conocido por la opinión pública a través de los medios de comunicación.

Por último, en caso de contar ya la empresa con un sistema de Compliance muy probablemente este tipo de situaciones **no harían sino manifestar una debilidad y falta de eficacia del sistema.**

Análisis de riesgo y sanciones aplicables

AMENAZAS Y SANCIONES EN EL AMBITO LABORAL

SUPUESTOS DE HECHO	LABORAL	
	AMENAZAS E INCUMPLIMIENTOS	SANCIÓN Y/O CONSECUENCIA
1. CONTROL TEMPERATURA: REQUISITOS PARA PODER IMPONER EL CONTROL.	**(i)** Vulnerar derecho a la intimidad	**(i)** Multa de hasta 187. 515 € (infracción muy grave)
	(i) Realizar pruebas sin haber recabado el informe previo de la representación de los trabajadores.	**(i)** Multa de hasta 6.250 € (Infracción grave)
	(i) Incumplimiento de los derechos de información, consulta y participación de los trabajadores	**(i)** Multa de entre 1.502,54 € y 30.050, 61€ (podría llegar a ser muy grave) **(ii)** Reclamación del trabajador por **daños y** perjuicios (pueden ir de entre 6010 € a 15.025,30 €)
2. REALIZACIÓN TEST SEROLÓGICOS Y PRUEBAS PCR.	**(i)** Vulneración de Derechos Fundamentales, al realizarlos masivamente y sin control de los datos que se recaban	**(i)** No cuantificada

3. CUESTIONARIOS A TRABAJADORES DE CARA A IDENTIFICAR QUIEN SE PUEDE INCORPORAR O NO AL TRABAJO: ESTADO DE SALUD, ENFERMEDADES, DATOS DE FAMILIARES, EDAD, CÓMO VAN AL TRABAJO, ETC.	**(i)** Vulneración de derechos, como el de intimidad personal, al exigir al trabajador información que no sea necesaria y no quiera facilitar de forma voluntaria	**(i)** Multa de entre 6.251€ hasta 187.515 €
4. CUESTIONARIOS A PERSONAL EXTERNO QUE VISITA LAS INSTALACIONES DE LA EMPRESA: VISITAS A PAÍSES DE ALTA PREVALENCIA DEL VIRUS, SINTOMATOLOGÍA, ETC.	Sin implicaciones en materia laboral, por no hacer referencia a trabajadores	Sin implicaciones en materia laboral, por no hacer referencia a trabajadores
5. INCUMPLIMIENTO POR PARTE DE LOS TRABAJADORES LAS MEDIDAS ESTABLECIDAS POR LA ENTIDAD	**(i)** Fallar en garantizar la seguridad y la salud de los trabajadores, ya sea por no interponer los medios de seguridad necesarios, o por no ejercer correctamente su deber de vigilancia del cumplimiento de las medidas establecidas.	**(i)** Multas **administrativas** **(ii) Multas de** la LISOS por infracciones graves en materia de PRL pueden alcanzar los 40.985€
6. OBLIGATORIEDAD DE QUE EL PERSONAL COMUNIQUE SU SITUACIÓN DE CUARENTENA PREVENTIVA O INFECCIÓN DEL COVID-19, CONTACTO CON POSITIVOS, ETC.	**(i)** Incumplir **la** obligación en materia de PRL de llevar a cabo evaluaciones de riesgos, así como sus actualizaciones y revisiones **(ii) Incumplimiento de** las nuevas	**(i)** Multa puede alcanzar los 40.985€. (Infracción grave)
7. COMUNICACIONES A LAS AUTORIDADES SANITARIAS SOBRE PERSONAL INFECTADO EN SU PUESTO DE TRABAJO.	**(i)** No dar cuenta, en tiempo y forma, a la autoridad competente en materia sanitario-laboral, de las enfermedades profesionales o accidentes	**(i)** Multa puede alcanzar los 40.985€. (Infracción grave)

8. POSIBLE COMUNICACIÓN DE TRABAJADORES QUE HAYAN DADO POSITIVO A LAS PERSONAS CON LAS QUE TUVO CONTACTO: PROVEEDORES, CLIENTES, OTROS TRABAJADORES.	**(i)** Que la a empresa no cumpla con determinadas obligaciones en materia de PRL aparejadas a la comunicación a los trabajadores y a la autoridad laboral	**(i)** multas de la LISOS por infracciones graves en materia de PRL pueden alcanzar los 40.985
9. IDENTIFICACIÓN DEL PERSONAL ESPECIALMENTE VULNERABLE	**(i) Incumplir** la obligación de realizar la correspondiente evaluación y actividad preventiva teniendo en cuenta todas las posibilidades vulnerabilidades y casos especiales **(ii) No comunicar** los casos vulnerables al Servicio de Prevención de Riesgos Laborales	**(i)** Multa **puede** alcanzar los 40.985€. (Infracción grave)
10. TELETRABAJO: RIESGOS DE PÉRDIDA DE INFORMACIÓN.	**Sin implicaciones** en materia laboral (los riesgos laborales asociados al teletrabajo se especifican en el siguiente punto)	**Sin implicaciones** en materia laboral, por no hacer referencia a trabajadores (los riesgos laborales asociados al teletrabajo se especifican en el siguiente punto)
11. TELETRABAJO: RIESGOS LABORALES (TRABAJADOR A DISTANCIA), POLÍTICA DE USO DE MEDIOS Y RIESGOS EN MATERIA DE PRL.	**(i)** No contar con el correspondiente acuerdo que permite el teletrabajo entre empresa y trabajador, y que establece las condiciones de esta modalidad contractual, especialmente la duración de esta modalidad.	**(i)** Acción de daños y perjuicios por parte del trabajador por no garantizar su derecho a la desconexión digital **(ii)** Conflicto posterior a la hora de reincorporarse al centro de trabajo al considerarse que el teletrabajo se pactó de manera indefinida

	(i) No contar con una política de uso de medios tecnológicos, y por ello, no poder realizar el correspondiente control sobre el empleado, o, en caso de realizarlo, que tal control sea ilícito.	**(i)** Daños y perjuicios a favor del empleado. **(ii)** Que la acción posterior sería declarada nula (por ejemplo, el despido), **con** las consecuencias legales que ello conlleva (en términos generales, obligación de reincorporar al trabajador y abono de los salarios de tramitación).
	(i) No adoptar las medidas necesarias **en materia preventiva** para esta nueva modalidad.	**(i)** Multa que puede alcanzar los 40.985€.
12. INCORPORACIÓN A LA OFICINA: COORDINACIÓN DE ACTIVIDADES CON PROVEEDORES Y CLIENTES, RIESGO GRAVE E INMINENTE, PROTECCIÓN DE LOS TRABAJADORES Y SERVICIO DE PREVENCIÓN DE RIESGOS LABORALES.	**(i)** No adoptar las medidas de cooperación y coordinación necesarias para la protección y prevención de riesgos laborales	**(i)** Multa puede alcanzar los 40.985€. (Infracción grave)
	(i) Informar lo antes posible a todos los trabajadores de la situación y las medidas a adoptar. **(ii)** Adoptar las medidas y dar las instrucciones necesarias para que, en caso de peligro grave, inminente e inevitable, los trabajadores puedan interrumpir su actividad y, si fuera necesario, abandonar de inmediato el lugar de trabajo	**(i)** Multa puede alcanzar los 40.985€. (Infracción grave) **(ii)** Reclamación del trabajador por daños y perjuicios

13. OBLIGAR A LOS TRABAJADORES A INCORPORARSE A LA OFICINA.	**(i)** Obligar a la incorporación, cuando la empresa no cumple con las medidas de prevención que garanticen su seguridad a los trabajadores	**(i)** Multa puede ascender hasta los 819.780 €,
14. FORMACIÓN E INFORMACIÓN A LOS TRABAJADORES.	**(i)** No proporcionar la formación o los medios adecuados para el desarrollo de sus funciones a los trabajadores designados para las actividades de prevención y a los delegados de prevención	**(i)** Multa puede alcanzar los 40.985€. (Infracción grave)
15. CONTAGIO-MUERTE DEL EMPLEADO	**(i)** Muerte o lesiones de un empleado, causado por el incumplimiento del empresario de sus obligaciones en materia de prevención de riesgos laborales.	**(i)** Multas administrativas previstas por los incumplimientos de la normativa de PRL **(ii)** Recargo de prestaciones de la Seguridad Social **(iii)** Responsabilidad civil **para resarcir** el daño generado cuando el accidente de trabajo (**probar el** nexo entre la relación laboral y el contagio

AMENAZAS Y SANCIONES EN MATERIA DE PRIVACIDAD Y PROTECCIÓN DE DATOS

SUPUESTOS DE HECHO	PROTECCIÓN DE DATOS	
	AMENAZAS E INCUMPLIMIENTOS	SANCIÓN Y/O CONSECUENCIA
1.CONTROL TEMPERATURA: REQUISITOS PARA PODER IMPONER EL CONTROL.	**(i)** No contar con una base legitimadora que permita realizar el tratamiento de datos **(ii)** No informar de forma adecuada a los interesados del tratamiento que se va a llevar a cabo **(iii)** No identificar quién y cómo va a llevar a cabo los controles, acceder a la información, etc. **(iv)** No identificar las comunicaciones o cesiones de datos que puedan producirse, tanto a administraciones como a terceras empresas, por ejemplo, en el caso de los proveedores **(v)** No guardar especial cautela a la hora de recabar, almacenar o incluso comunicar a terceros autorizados los resultados del control de temperatura. (vi) No haber realizado las evaluaciones impacto en relación con la tecnología utilizada o la regularización con los posibles proveedores, que pudieran entenderse como infracciones o incluso como transferencias internacionales de datos.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía Posible vulneración del derecho al honor intimidad y propia imagen de los afectados, pudiendo dar lugar a las correspondientes indemnizaciones.

2. REALIZACIÓN TEST SEROLÓGICOS Y PRUEBAS PCR.	**(i)** Incumplir el principio de limitación de la finalidad al obtener datos de salud que excedan de la obtención del dato de confirmación o no del contagio por COVID-19 **(ii)** Falta de consentimiento y legitimación de familiares o personas con las que convive el trabajador, si la realización de las pruebas se extiende a familiares o personas con las que convive **(iii)** Vulneración del principio de minimización y de limitación del tratamiento **(iv)** Falta de legitimación para realizar el tratamiento de información de salud, en relación con el servicio de PRL en caso de contar con el consentimiento del empleado legitimando dicha comunicación.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía Posible vulneración del derecho al honor intimidad y propia imagen de los afectados, pudiendo dar lugar a las correspondientes indemnizaciones. Posible incumplimiento de la normativa en materia de salud, en relación con el secreto profesional y confidencialidad, así el tratamiento de la información como parte de la historia clínica.
3. CUESTIONARIOS A TRABAJADORES DE CARA A IDENTIFICAR QUIEN SE PUEDE INCORPORAR O NO AL TRABAJO: ESTADO DE SALUD, ENFERMEDADES, DATOS DE FAMILIARES, EDAD, CÓMO VAN AL TRABAJO, ETC.	Vulneración de los principios de minimización y de limitación del tratamiento. Para ello, se deben evitar cuestionarios extensos y detallados sobre la salud de los interesados o de terceros con los que conviva, así como preguntas no relacionadas con el COVID-19	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía. Posible vulneración del derecho al honor intimidad y propia imagen de los afectados, pudiendo dar lugar a las correspondientes indemnizaciones.
4. CUESTIONARIOS A PERSONAL EXTERNO QUE VISITA LAS INSTALACIONES DE LA EMPRESA: VISITAS A PAÍSES DE ALTA PREVALENCIA DEL VIRUS, SINTOMATOLOGÍA, ETC.	Vulneración de los principios de minimización y de limitación del tratamiento si las preguntas no son limitadas. En este sentido, el objeto de los cuestionarios debe ser, únicamente, averiguar si el personal externo padece algún síntoma o se encuentra afectado por algún factor de	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía

	alto riesgo en relación con el COVID-19 y, así, impedir su acceso a las instalaciones.	Posible vulneración del derecho al honor intimidad y propia imagen de los afectados, pudiendo dar lugar a las correspondientes indemnizaciones.
5. INCUMPLIMIENTO POR PARTE DE LOS TRABAJADORES LAS MEDIDAS ESTABLECIDAS POR LA ENTIDAD	Incumplimiento de los principios de minimización y limitación del tratamiento, en el supuesto de que, por ejemplo, se pretendan utilizar las imágenes de las cámaras de videovigilancia instaladas con fines de seguridad para sancionar o amonestar al trabajador por incumplir las medidas impuestas por el empleador.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía
6. OBLIGATORIEDAD DE QUE EL PERSONAL COMUNIQUE SU SITUACIÓN DE CUARENTENA PREVENTIVA O INFECCIÓN DEL COVID-19, CONTACTO CON POSITIVOS, ETC.	**(i)** En aplicación de la normativa laboral el responsable del tratamiento, conforme al principio de calidad de los datos, deberá mantener la información actualidad, incluso de oficio o cancelarla igualmente. **(ii)** La comunicación de esta información a terceros, no salvaguardando la identidad del afectado como norma general, como base en la protección de los intereses vitales de los interesados o terceros. En este sentido, la posible comunicación, si no se realiza de una manera correcta podría implicar un incumplimiento del deber de secreto en materia de protección de datos o una vulneración del derecho a la intimidad de los empleados.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía Posible vulneración del derecho al honor intimidad y propia imagen de los afectados, pudiendo dar lugar a las correspondientes indemnizaciones.

7. COMUNICACIONES A LAS AUTORIDADES SANITARIAS SOBRE PERSONAL INFECTADO EN SU PUESTO DE TRABAJO.	**(i)** Comunicar datos personales, más allá de los estrictamente necesarios y fuera de los criterios y prevención y fuera de los criterios de las Autoridades Sanitarias. Teniendo en cuenta que la no comunicación de determinados datos podría implicar un incumplimiento o sanciones administrativas. **(ii)** Incumplimiento de los principios de minimización y limitación del tratamiento. El empleador optará por no identificar a la persona afectada siempre que ello permita proteger la salud del resto de trabajadores. En caso contrario, será necesaria la identificación de esta, aportando, en todo caso, los datos mínimos **(iii)** Incumplimiento del deber de confidencialidad	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía Posible vulneración del derecho al honor intimidad y propia imagen de los afectados, pudiendo dar lugar a las correspondientes indemnizaciones.
8. POSIBLE COMUNICACIÓN DE TRABAJADORES QUE HAYAN DADO POSITIVO A LAS PERSONAS CON LAS QUE TUVO CONTACTO: PROVEEDORES, CLIENTES, OTROS TRABAJADORES.	**(i)** Incumplimiento de los principios de minimización y limitación del tratamiento. El empleador optará por no identificar a la persona afectada siempre que ello permita proteger la salud del resto de trabajadores. En caso contrario, será necesaria la identificación de esta, aportando, en todo caso, los datos mínimos **(ii)** Incumplimiento del deber de confidencialidad **(iii)** Intromisión en el derecho a la intimidad.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía Posible vulneración del derecho al honor intimidad y propia imagen de los afectados, pudiendo dar lugar a las correspondientes indemnizaciones.

9. IDENTIFICACIÓN DEL PERSONAL ESPECIALMENTE VULNERABLE	**(i)** Incumplimiento de los principios de minimización y limitación del tratamiento. **(ii)** Intromisión en el derecho a la intimidad.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía Posible vulneración del derecho al honor intimidad y propia imagen de los afectados, pudiendo dar lugar a las correspondientes indemnizaciones.
10. TELETRABAJO: RIESGOS DE PÉRDIDA DE INFORMACIÓN.	Incumplir o no disponer de una política de medios tecnológicos que cumpla con todos los requisitos legales, haciendo especial mención al uso correcto de los recursos a través del acceso en remoto, los controles aplicables que permitan garantizar la confidencialidad, integridad y disponibilidad de la información, así como prohibir determinadas conductas que supondrían un riesgo para la seguridad de la información. Necesidad de adoptar políticas en relación con la identificación, comunicación y gestión de brechas de seguridad. Implementación de políticas de BYOD que eviten perdida de información, tanto datos personales como información sensible y confidencial de la empresa o sus clientes.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía
11. TELETRABAJO: RIESGOS LABORALES (TRABAJADOR A DISTANCIA), POLÍTICA DE USO DE MEDIOS Y RIESGOS EN MATERIA DE PRL.	No garantizar el derecho a la desconexión digital de los trabajadores. La no adopción de las medidas de seguridad corporativas o políticas BYOD Utilización de datos personales, no facilitados en el marco de la relación laboral	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía

	para el contacto o gestión de los empleados.	
12. INCORPORACIÓN A LA OFICINA: COORDINACIÓN DE ACTIVIDADES CON PROVEEDORES Y CLIENTES, RIESGO GRAVE E INMINENTE, PROTECCIÓN DE LOS TRABAJADORES Y SERVICIO DE PREVENCIÓN DE RIESGOS LABORALES.	No contar con una base de legitimación que habilite el tratamiento de categorías especiales de datos Flujos y cesiones de datos, así como tratamientos por parte de prestadores de servicios o terceros (e.g. arrendatario de las oficinas)	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía
13. OBLIGAR A LOS TRABAJADORES A INCORPORARSE A LA OFICINA.	Necesidad de aportar garantías suficientes en relación con el estado de salud. Medidas de seguridad en relación con los tratamientos de datos y garantías con respecto a la disponibilidad de los datos. Gestión de registros de accesos y autorizaciones. Tratamientos de datos de salud del empleado o terceros en caso de contingencia.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía
14.FORMACIÓN E INFORMACIÓN A LOS TRABAJADORES.	Incumplimiento de cualesquiera de los principios de la normativa de protección de datos por falta de formación y conocimiento de los procedimientos de actuación.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía

15. CONTAGIO-MUERTE DEL EMPLEADO	Acceso a información del fallecido par parte de terceros allegados atendiendo a lo establecido en la LOPDGDD y la voluntad del fallecido. En relación con las posibles vulneraciones de los derechos al honor, intimidad personal y familiar, si bien son derechos personalísimos que se extinguen tras el fallecimiento, pueden tener implicaciones para con terceras personas y por tanto riesgos en tanto no se traten de forma adecuada adoptando garantías adicionales.	Incurrir en infracciones en materia de protección de datos que podrían conllevar multas económicas, de hasta 20.000.000.-€ o de una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía

AMENZAS Y SANCIONES EN EL ÁMBITO PENAL

SUPUESTOS DE HECHO	COMPLIANCE PENAL	
	AMENAZAS E INCUMPLIMIENTOS	SANCIÓN Y/O CONSECUENCIA
1. CONTROL TEMPERATURA: REQUISITOS PARA PODER IMPONER EL CONTROL.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal
2. REALIZACIÓN TEST SEROLÓGICOS Y PRUEBAS PCR.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal
3.CUESTIONARIOS A TRABAJADORES DE CARA A IDENTIFICAR QUIEN SE PUEDE INCORPORAR O NO AL TRABAJO: ESTADO DE SALUD, ENFERMEDADES, DATOS DE FAMILIARES, EDAD, CÓMO VAN AL TRABAJO, ETC.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal

4.CUESTIONARIOS A PERSONAL EXTERNO QUE VISITA LAS INSTALACIONES DE LA EMPRESA: VISITAS A PAÍSES DE ALTA PREVALENCIA DEL VIRUS, SINTOMATOLOGÍA, ETC.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal
5. INCUMPLIMIENTO POR PARTE DE LOS TRABAJADORES LAS MEDIDAS ESTABLECIDAS POR LA ENTIDAD	Posible materialización por parte de los administradores de hecho o derecho de un delito contra los derechos de los trabajadores, con la consecuente imposición de penas accesorias a la persona jurídica	**(i)** Penas susceptibles de ser impuestas a **administradores, encargados del servicio**, podrá imponerse una pena de prisión de seis meses a tres años y multa de seis a doce meses **(ii)** Penas susceptibles de ser impuestas a la **Persona Jurídica ya definidos**

6.OBLIGATORIEDAD DE QUE EL PERSONAL COMUNIQUE SU SITUACIÓN DE CUARENTENA PREVENTIVA O INFECCIÓN DEL COVID-19, CONTACTO CON POSITIVOS, ETC.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal
7.COMUNICACIONES A LAS AUTORIDADES SANITARIAS SOBRE PERSONAL INFECTADO EN SU PUESTO DE TRABAJO.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal
8. POSIBLE COMUNICACIÓN DE TRABAJADORES QUE HAYAN DADO POSITIVO A LAS PERSONAS CON LAS QUE TUVO CONTACTO: PROVEEDORES, CLIENTES, OTROS TRABAJADORES.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal

9 IDENTIFICACIÓN DEL PERSONAL ESPECIALMENTE VULNERABLE	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal
10. TELETRABAJO: RIESGOS DE PÉRDIDA DE INFORMACIÓN.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal
11. TELETRABAJO: RIESGOS LABORALES (TRABAJADOR A DISTANCIA), POLÍTICA DE USO DE MEDIOS Y RIESGOS EN MATERIA DE PRL	Posible materialización por parte de los administradores de hecho o derecho de un delito contra los derechos de los trabajadores, con la consecuente imposición de penas accesorias a la persona jurídica	**(i)** Penas susceptibles de ser impuestas a **administradores, encargados del servicio**, podrá imponerse una pena de prisión de seis meses a tres años y multa de seis a doce meses **(ii)** Penas susceptibles de ser impuestas a la **Persona Jurídica ya definidos**
12. INCORPORACIÓN A LA OFICINA: COORDINACIÓN DE ACTIVIDADES CON PROVEEDORES Y CLIENTES, RIESGO GRAVE E INMINENTE, PROTECCIÓN DE LOS TRABAJADORES Y SERVICIO DE PREVENCIÓN DE RIESGOS LABORALES.	Posible materialización por parte de los administradores de hecho o derecho de un delito contra los derechos de los trabajadores, con la consecuente imposición de penas accesorias a la persona jurídica	**(i)** Penas susceptibles de ser impuestas a **administradores, encargados del servicio**, podrá imponerse una pena de prisión de seis meses a tres años y multa de seis a doce meses **(ii)** Penas susceptibles de ser impuestas a la **Persona Jurídica ya definidos**

13. OBLIGAR A LOS TRABAJADORES A INCORPORARSE A LA OFICINA.	Posible materialización por parte de los administradores de hecho o derecho de un delito contra los derechos de los trabajadores, con la consecuente imposición de penas accesorias a la persona jurídica	**(i)** Penas susceptibles de ser impuestas a **administradores, encargados del servicio**, podrá imponerse una pena de prisión de seis meses a tres años y multa de seis a doce meses **(ii)** Penas susceptibles de ser impuestas a la **Persona Jurídica ya definidos**
14. FORMACIÓN E INFORMACIÓN A LOS TRABAJADORES.	**Sin implicaciones** en materia penal	**Sin implicaciones** en materia penal
15. CONTAGIO DE UN EMPLEADO EN EL CENTRO DE TRABAJO CON RESULTADO DE MUERTE DEL EMPLEADO	Posible materialización por parte de los administradores de hecho o derecho de un delito contra los derechos de los trabajadores, con la consecuente imposición de penas accesorias a la persona jurídica Posible delito de lesiones u homicidio imprudente (no susceptible de ser cometido por la persona jurídica), contra terceros ajenos a nuestra organización, o no considerado como personal laboral. * Para que este supuesto concurra, deberá probarse la relación de causalidad y nexo entre la relación laboral y el contagio que ha ocasionado la lesión o fallecimiento.	**(i)** Penas susceptibles de ser impuestas a administradores, encargados del servicio, podrá imponerse una pena de prisión de seis meses a tres años y multa de seis a doce meses **(ii)** Penas susceptibles de ser impuestas a la **Persona Jurídica ya definidos** **(iii)** Responsabilidad civil con carácter subsidiario de la responsabilidad civil que se reconozca a favor de la víctima

Medidas para la mitigación del riesgo

SUPUESTOS DE HECHO	LABORAL	COMPLIANCE PENAL	PROTECCIÓN DE DATOS
	MEDIDAS DE MITIGACIÓN	MEDIDAS DE MITIGACIÓN	MEDIDAS DE MITIGACIÓN
1.CONTROL TEMPERATURA: REQUISITOS PARA PODER IMPONER EL CONTROL.	**(i)** Plan interno para la realización de pruebas (checklist-criterios Autoridades Sanitarias) **(ii)** No realizar sin pruebas sin el preceptivo informe de la representación de los trabajadores **(iii)** Dar participación a los trabajadores, en cualquier cuestión que afecte a la seguridad y salud en el trabajo, a través de una plataforma de la que quede constancia de las intervenciones (e-mail)	**Sin implicaciones** en materia penal	**(i)** Contar con una base legitimadora para el tratamiento **(ii)** Limitar los plazos de conservación estableciendo el bloqueo y la supresión de los datos cuando dejen de ser necesarios. **(iii)** Limitar los accesos a los datos personales a las personas estrictamente necesarias. **(iv)** Delimitar las finalidades del tratamiento. **(v)** Comunicar datos personales solamente en aquellos supuestos en los que se cuente con una base que lo legitime. **(vi)** Registrar el tratamiento y llevar a cabo un análisis de riesgos. **(vii)** Formación o información a los trabajadores efectos de que conozcan las medidas que deben adoptar en los nuevos tratamientos de datos **(viii)** Realizar una evaluación de impacto de privacidad si fuese necesario **(ix)** Cumplir con el deber de confidencialidad. **(x)** Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos. **(xi)** Cumplir con el deber de información

2. REALIZACIÓN TEST SEROLÓGICOS Y PRUEBAS PCR.	**(i)** Limitar la realización de pruebas diagnósticas para la detección de la COVID-19 a los ámbitos de actuación descritos, establecidos por el Ministerio de Sanidad	**Sin implicaciones** en materia penal	**(i)** Establecer qué datos son los necesarios para los fines perseguidos. **(ii)** Contar con una base legitimadora para el tratamiento **(iii)** Limitar los plazos de conservación estableciendo el bloqueo y la supresión de los datos cuando dejen de ser necesarios. **(iv)** Limitar los accesos a los datos personales a las personas estrictamente necesarias. **(v)** Delimitar las finalidades del tratamiento. **(vi)** Comunicar datos personales solamente en aquellos supuestos en los que se cuente con una base que lo legitime. **(vii)** Registrar el tratamiento y llevar a cabo un análisis de riesgos. **(viii)** Recabar y documentar los consentimientos de familiares o personas con las que convive el trabajador, si se van a someter a la prueba **(ix)** Realizar una evaluación de impacto de privacidad si fuese necesario **(x)** Cumplir con el deber de confidencialidad. **(xi)** Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos.

3. CUESTIONARIOS A TRABAJADORES DE CARA A IDENTIFICAR QUIEN SE PUEDE INCORPORAR O NO AL TRABAJO: ESTADO DE SALUD, ENFERMEDADES, DATOS DE FAMILIARES, EDAD, CÓMO VAN AL TRABAJO, ETC.	**(i)** Recabar cualquier información de esta tipología a través del Servicio de Prevención Ajeno, de acuerdo con la normativa de protección de datos	**Sin implicaciones** en materia penal	**(i)** Evitar cuestionarios extensos y detallados sobre la salud de los interesados o de terceros con los que conviva, así como preguntas no relacionadas con el COVID-19. **(ii)** Delimitar las finalidades del tratamiento **(iii)** Cumplir con el deber de información **(iv)** Limitar los plazos de conservación estableciendo el bloqueo y la supresión de los datos cuando dejen de ser necesarios. **(v)** Registrar el tratamiento y realizar un análisis de riesgos **(vi)** Cumplir con el deber de confidencialidad. **(vii)** Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos.
4. CUESTIONARIOS A PERSONAL EXTERNO QUE VISITA LAS INSTALACIONES DE LA EMPRESA: VISITAS A PAÍSES DE ALTA PREVALENCIA DEL VIRUS, SINTOMATOLOGÍA, ETC.	Sin implicaciones en materia laboral, por no hacer referencia a trabajadores	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**(i)** Evitar cuestionarios extensos y detallados sobre la salud de los interesados o de terceros con los que conviva, así como preguntas no relacionadas con el COVID-19. **(ii)** Limitar las preguntas, y no equiparar los cuestionarios, con los que se realizan a los trabajadores **(iii)** Delimitar las finalidades del tratamiento **(iv)** Cumplir con el deber de información **(v)** Limitar los plazos de conservación estableciendo el bloqueo y la supresión de los datos cuando dejen de ser necesarios. **(vi)** Registrar el tratamiento y realizar un análisis de riesgos **(vii)** Cumplir con el deber de confidencialidad.

			(viii) Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos.

5. INCUMPLIMIENTO POR PARTE DE LOS TRABAJADORES LAS MEDIDAS ESTABLECIDAS POR LA ENTIDAD: NO LLEVAR MASCARILLA O GUANTES CUANDO SE ESTIPULE SU OBLIGATORIEDAD, ETC.	**(i)** Diseñar y transmitir las necesarias instrucciones en materia de prevención a los trabajadores. **(ii)** Realizar comunicaciones periódicas a los empleados sobre la obligatoriedad de utilizar y hacerlo de manera correcta, de dichos equipos, herramientas y EPIs, así como requerir al Servicio de Prevención Ajeno para que realice los controles oportunos. **(iii)** Investigar cualquier posible incumplimiento de la obligación laboral del empleado que se niega a utilizar el equipo, sancionándolo en su caso si ello fuera necesario	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**(i)** Realizar análisis de ponderación de los intereses de los trabajadores e información a los mismos **(ii)** Establecer medidas de vigilancia y control, destinadas a verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. **(iii)** Dar formación a los trabajadores a efectos de que conozcan las medidas y finalidad. (iv) Cumplir con el deber de información (v) Contar con una base que legitime el tratamiento

6. OBLIGATORIEDAD DE QUE EL PERSONAL COMUNIQUE SU SITUACIÓN DE CUARENTENA PREVENTIVA O INFECCIÓN DEL COVID-19, CONTACTO CON POSITIVOS, ETC.	**(i)** Comunicación constante por el Servicio de Prevención Ajeno **(ii)** Establecer desde un inicio, un protocolo común en relación con todas las obligaciones normativas. **(iii)** Monitorización diaria de las obligaciones establecidas para las empresas (toda vez que se han aprobado varias a raíz del estado de alarma)	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**Sin implicaciones** en materia de protección de datos.
7. COMUNICACIONES A LAS AUTORIDADES SANITARIAS SOBRE PERSONAL INFECTADO EN SU PUESTO DE TRABAJO.	**(i)** Preestablecer un protocolo de actuación interno, definiendo el proceso de comunicación a la autoridad laboral **(ii)** el responsable de PRL (en principio, el Servicio de Prevención Ajeno), haga seguimiento de que todos los casos de los que se tenga conocimiento como positivos del COVID-19	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**(i)** Realizar la comunicación a través del servicio de prevención de riesgos laborales (propio o ajeno) y, debe limitarse a proporcionar aquellos datos estrictamente necesarios. **(ii)** Comunicar datos personales solamente en aquellos supuestos en los que se cuente con una base que lo legitime. **(iii)** Cumplir con el deber de confidencialidad **(iv)** Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos. **(v)** Cumplir con el deber de información a los interesados

8. POSIBLE COMUNICACIÓN DE TRABAJADORES QUE HAYAN DADO POSITIVO A LAS PERSONAS CON LAS QUE TUVO CONTACTO: PROVEEDORES, CLIENTES, OTROS TRABAJADORES.	**(i)** Preestablecer un protocolo de actuación interno COVID-19 recogiendo específicamente, los pasos a seguir ante el conocimiento de un positivo (plan de actuación en diferentes ámbitos, personas responsables, tiempos y herramientas) **(ii)** Informar de ello al Servicio de Prevención Ajeno para que, informando de los posibles trabajadores que han estado en contacto con dicho trabajador, pueda realizar la correspondiente evaluación de la situación y ordenar las medidas que correspondan	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**(i)** No identificar a la persona afectada siempre que ello permita proteger la salud del resto de trabajadores. En caso contrario, será necesaria la identificación de esta, aportando, en todo caso, los datos mínimos. **(ii)** Contar con una base legitimadora para el tratamiento **(iii)** Cumplir con el deber de información **(iv)** Limitar los accesos a los datos personales a las personas estrictamente necesarias. **(v)** Cumplir con el deber de confidencialidad. **(vi)** Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos.
9. IDENTIFICACIÓN DEL PERSONAL ESPECIALMENTE VULNERABLE	**(i)** Comunicar a la plantilla las obligaciones relacionadas con la salvaguarda de la salud de los trabajadores, se solicita que comuniquen a la empresa cualquier situación de salud especial que pueda requerir atención especializada en relación al COVID-19 dentro de la actividad preventiva	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**(iii)** Delimitar las finalidades del tratamiento **(iv)** Cumplir con el deber de información **(v)** Limitar los plazos de conservación estableciendo el bloqueo y la supresión de los datos cuando dejen de ser necesarios. **(vi)** Registrar el tratamiento y realizar un análisis de riesgos **(vii)** Cumplir con el deber de confidencialidad. **(viii)** Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos.

10. TELETRABAJO: RIESGOS DE PÉRDIDA DE INFORMACIÓN.	**Sin implicaciones** en materia laboral, por no hacer referencia a trabajadores	**(i)** Actualizar o implementar las políticas de uso de medios tecnológicos haciendo especial mención al uso correcto de los recursos a través del acceso en remoto, los controles aplicables que permitan garantizar la confidencialidad, integridad y disponibilidad de la información	**(i)** Actualizar las políticas de uso de medios tecnológicos haciendo especial mención al uso correcto de los recursos a través del acceso en remoto, los controles aplicables que permitan garantizar la confidencialidad, integridad y disponibilidad de la información **(ii)** Prohibir determinadas conductas que supondrían un riesgo para la seguridad de la información **(iii)** Adopción de políticas "*bring your own device*" en los casos en los que los empleados utilicen medios propios. **(iv)** Disponer de un procedimiento de detección de brechas de seguridad y un procedimiento para la comunicación de las mismas a la autoridad de control o interesados. **(v)** Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos. **(vi)** Cumplir con el deber de confidencialidad

11. TELETRABAJO: RIESGOS LABORALES (TRABAJADOR A DISTANCIA), POLÍTICA DE USO DE MEDIOS Y RIESGOS EN MATERIA DE PRL.	**(i)** Recomendable contar con un acuerdo completo, donde se recojan las nuevas condiciones de trabajo del empleado, incluidas aquellas en materia de prevención de riesgos laborales e incluso qué parte asume qué gastos (Internet, luz, etc.). **(ii)** Contar con la correspondiente política, debidamente aprobada previa participación de los representantes de los trabajadores. En caso de no existir RLT, habrá que crear la correspondiente comisión para, en todo caso, dar participación a la plantilla. **(iii)** Comunicarse inmediatamente al Servicio de Prevención Ajeno, solicitando que realice la correspondiente evaluación adaptada de los puestos, o en su caso remita la correspondiente autoevaluación **(iv)** Contar con un protocolo para aquellos casos en los que, o bien en atención a una solicitud del trabajador, o bien por decisión de la empresa puesta en común con el trabajador, se adopte esta modalidad de trabajo.	**(i)** Actualizar o implementar las políticas de uso de medios tecnológicos haciendo especial mención al uso correcto de los recursos a través del acceso en remoto, los controles aplicables que permitan garantizar la confidencialidad, integridad y disponibilidad de la información	**(i)** Incumplir en el marco de la implementación de las políticas de teletrabajo y nuevos modelos organizativos que se implementen en la empresa, deberá tenerse en cuenta, en relación con la gestión de jornada, el derecho a la desconexión digital, regulado en la normativa de protección de datos y garantías de derechos digitales. **(ii)** Disponer de un procedimiento de detección de brechas de seguridad y un procedimiento para la comunicación de las mismas a la autoridad de control o interesados. **(iii)** Adoptar medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los datos. **(iv)** Cumplir con el deber de confidencialidad

12. INCORPORACIÓN A LA OFICINA: COORDINACIÓN DE ACTIVIDADES CON PROVEEDORES Y CLIENTES, RIESGO GRAVE E INMINENTE, PROTECCIÓN DE LOS TRABAJADORES Y SERVICIO DE PREVENCIÓN DE RIESGOS LABORALES.	**(i)** Antes de reiniciar la actividad presencial, o si ésta ya está teniendo lugar, realizar un listado de aquellos clientes y proveedores en cuyos centros de trabajo (propios o ajenos) concurren empleados propios con los de estos terceros, y solicitar al Servicio de Prevención Ajeno que realice cuantas actuaciones sean necesarias para cumplir con tal fin de cooperación **(ii)** Control diario de la actividad de manera que se pueda detectar inmediatamente cualquier riesgo, asignando dicho rol a un perfil concreto	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**Sin implicaciones** en materia de protección de datos
13. OBLIGAR A LOS TRABAJADORES A INCORPORARSE A LA OFICINA.	**(i)** Ordenar la reincorporación presencial a la oficina solo cuando se cuenten con todas las medidas y actuaciones indicadas por el Servicio de Prevención Ajeno para iniciar la actividad de manera presencial.	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**Sin implicaciones** en materia de protección de datos

14. FORMACIÓN E INFORMACIÓN A LOS TRABAJADORES.	**(i)** Contactar con el Servicio de Prevención Ajeno, para que nos informe y ejecute las correspondientes actividades de formación e información actualizadas dada la nueva situación y el riesgo de contagio del COVID-19.	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	Dar formación a los trabajadores a efectos de que conozcan las medidas que deben adoptar en los nuevos tratamientos de datos en aras a cumplir con las disposiciones de la normativa de protección de datos.
15. CONTAGIO-MUERTE DEL EMPLEADO	**(i)** Con independencia de posibles pólizas de seguro y sus condiciones, resulta esencial solicitar al Servicio de Prevención Ajeno, un informe sobre las obligaciones específicas en materia de salud a adoptar por parte de la empresa en relación con el COVID-19, y cumplir todas aquellas medidas que este servicio informe **(ii)** Establecer un protocolo interno específico de actuación frente al COVID-19 en el que se regule por parte de la empresa todas las medidas implementadas por la empresa	**(i)** Definición de un plan de riesgos laborales, conforme a los riesgos de actividad de la organización **(ii)** Cumplimiento de las medidas recomendadas en materia laboral	**Sin implicaciones** en materia de protección de datos

	(iii) Establecer de manera periódica una evaluación de cumplimiento periódica: • Se ha enviado y recibido a los trabajadores la formación e información para la realización del trabajo encomendado. • Se han adoptado las medidas de seguridad previstas en el plan de evaluación de riesgos laborales actualizado por el Servicio de Prevención Ajeno. • Se han facilitado a todos los empleados y empleadas, los medios de seguridad adecuados. • Facilitados los medios de seguridad, generalmente EPIS, se vigila de manera rutinaria por parte del empresario la utilización efectiva de los mismos por parte de los trabajadores.		

Indicadores genéricos para la evaluación del riesgo de incumplimiento basados en probabilidad e impacto

Una vez identificados los supuestos de hecho concretos y los riesgos normativos a los que se encuentran expuestos cada uno de ellos, a fin de evaluar el grado o nivel de riesgo que pudiera darse en cada empresa habría que definir una serie de indicadores que pudieran en su conjunto conformar la probabilidad y el impacto de la forma más objetiva posible.

Si se hace este ejercicio se podrán identificar qué medidas concretas debemos aplicar a cada situación de hecho para mitigar los riesgos existentes en cada organización.

Factores Probabilidad:

- **Sector de actividad**: **La exposición y el hecho de que nuestra actividad pueda exponer en mayor o menor riesgo al contagio del COVID-19**, es un factor determinante a la hora de valorar el riesgo al que se enfrenta la organización, así como a la hora de definir las medidas a implementar. No es lo mismo una empresa u organización sin contacto con el público y con escasa movilidad de los trabajadores, que una empresa deslocalizada con un movimiento constante de sus trabajadores y con contacto directo con el público.

  Asimismo, el sector de actividad se define como **un factor esencial a analizar**, teniendo en cuenta que existen **guías específicas en algunos sectores**, como puede ser por ejemplo el del deporte profesional, en el que el ministerio de Sanidad ha establecido unos requisitos concretos que la organización en cuestión deberá implementar.

- **Tamaño de la organización**: Habida cuenta que la presente amenaza está directamente relacionada con la problemática que puede ocasionar el contacto social, debemos entender, que a mayor número de empleados y/o miembros que conforman la organización, mayor será el riesgo de materialización de las amenazas expuestas.

- **Infraestructura y medios de la Organización**: Al hilo del factor inmediatamente anterior, y teniendo en cuenta que el distanciamiento físico y social es una de las medidas esenciales de cara a la gestión de la crisis, el hecho de contar con una infraestructura adecuada y que permita las distancias recomendadas, así como con los medios adecuados, tanto a nivel técnico, para facilitar medidas de teletrabajo, como materiales, para poder facilitar a empleados y terceros, mascarillas, guantes, gel, etc. disminuirá o aumentará el riesgo de incurrir en las amenazas descritas.

- **Antecedentes Sancionadores**: Contar con alguna sanción previa en materia de prevención de riesgos laborales podría aumentar el riesgo inherente.
- **Estructura Organizativa**: El hecho de contar con una estructura dentro de la organización y un programa específico, tanto de cumplimiento como en materia de prevención de riesgos laborales, y con una figura o departamento visible que responda en última instancia del efectivo cumplimiento de los mismos (no siendo necesariamente la misma persona y/o departamento), disminuye significativamente el riesgo de materialización de las amenazas expuestas.

Factores de Impacto:

- **Sanciones**: Deberá tenerse en cuenta las sanciones, tanto a nivel económico, como administrativo, laboral, civil y de protección de datos a los que me enfrento.

- **Daño Reputacional:** Teniendo en cuenta que la crisis a la que nos enfrentamos es sanitaria, y que las consecuencias de no implementar las preceptivas medidas de seguridad afectan directamente a la salud de las personas, debemos asumir que el daño reputacional será alto, pudiendo variar en función de la gravedad de los perjuicios causados.

Conclusiones

El resultado de un trabajo de este tipo, elaborado de forma específica para una empresa concreta, tendrá como objetivo el servir de ayuda al Órgano de Administración en la toma de decisiones que pudieran entrañar un riesgo de incumplimiento de una o varias normas.

Los análisis de riesgos normativos deben cumplir la misión de facilitar información útil a los órganos de gobierno que adoptan las decisiones estratégicas de la compañía. No se puede seguir pensando en los análisis de riesgo únicamente como un requisito del artículo 31 bis del Código Penal.

Se trata por lo tanto de aportar una información adicional sin la cuál se podría haber adoptado una decisión que, aunque pareciera acertada desde el punto de vista de negocio estaría obviando las posibles consecuencias jurídicas de las mismas.

Un análisis de riesgos de este tipo no sólo servirá como apoyo en la toma de decisiones, sino que deberá ir acompañado del consecuente plan de acción en el que se deberán incluir al menos; las medidas tendentes a mitigar los riesgos, los plazos de ejecución de las mismas y los responsables de llevarlas a cabo.

www.ecija.com

ECIJA

España | Portugal | EEUU | Chile | Panamá | Costa Rica | Honduras | Nicaragua | República Dominicana | Guatemala | El Salvador | Puerto Rico | México | Brasil | Ecuador