Compliancers

Paso a paso

Guía de uso de la Plataforma Tecnológica Compliancers I

Versión 4.0

:

INDICE

1. INTRODUCCION

1.1 Le damos la bienvenida a Compliancers y confiamos que la presente Guía de Uso resulte de su interés.

1.2 Compliancers es una plataforma tecnológica de ayuda al profesional que ha sido concebida con el objetivo de optimizar los recursos de su despacho y de facilitarle el seguimiento en los distintos pasos que habrán de ser llevados a cabo en el asesoramiento en la implementación de un manual de compliance penal.

1.3 Compliancers está especialmente diseñada para el asesoramiento legal de las pymes españolas y desempeña su trabajo mediante un administrador de flujos que opera sobre los distintos departamentos de la empresa, teniendo en cuenta 33 tipos delictivos de los que cabe derivar responsabilidad penal a la persona jurídica.

1.4 El administrador de flujos genera de manera metódica y estructurada una serie de documentos que conforman la base y fundamento de un modelo de cumplimiento penal.

1.5 Sin embargo, ha de señalarse que Compliancers en modo alguno desarrolla por sí sola un programa de cumplimiento penal. Es de gran valor la intervención del profesional, quien habrá de aplicar sus conocimientos y detectar las actividades de riesgo de la empresa hasta obtener desde su singularidad, un programa de compliance penal personalizado e individualizado que cumpla con las exigencias de “eficacia” e “idoneidad” requeridas por el art. 31 bis del Código Penal.

1.6 Compliancers no pretende suplir o limitar el criterio del profesional. Por esta razón, todos los informes que se generan quedan abiertos en “word”, permitiendo que el profesional pueda trabajar sobre ellos, haciendo su aportación a la personalización, en aras de alinear su trabajo con las necesidades de su cliente.

1.7 Compliancers permite el asesoramiento en la implantación de un modelo de cumplimiento penal de conformidad con las directrices y recomendaciones de la UNE ISO 19600. Tomamos la referencia de dicha norma internacional a modo de guía para implementar un sistema de gestión de compliance eficaz, cuyo cronograma debe transitar por el principio de mejora continua*:* Planificar + Hacer + Verificar + Actuar.

1.8 Compliancers tiene su aparición en el mercado en el mes de octubre de 2015. La presente guía contempla la Versión 4.0, aprobada el día 01.06.2017 y constituye el resultado de las sucesivas mejoras incorporadas desde su origen.

1.9 Es nuestro propósito proseguir en el plan de mejora continua hasta consolidar una plataforma de trabajo que sea un referente en el ámbito del Corporate Compliance nacional de la pequeña y mediana empresa.

1.10 Nuestro compromiso es la implementación de constantes avances y nuevas versiones que serán inspiradas desde la praxis del día a día, desde el feedback que recibimos de los licenciatarios que la utilizan y desde la doctrina que viene desarrollando la jurisprudencia.

1.11 Además, queremos decirle que nuestro objetivo es aportar a su trabajo diario mucho más que un software. Nuestra resolución es aportarle valor añadido en contenidos complementarios: documentos de trabajo, hojas de encargo, actas sociales, acuerdos de colaboración, noticias relacionadas, reseñas jurisprudenciales, encuestas de evaluación de solvencia de un manual de compliance, pruebas de conocimiento y un largo etcétera que deberá ir alimentándose día a día con las sugerencias nacidas desde la experiencia práctica de nuestros licenciatarios.

1.12 Recomendamos que la presente Guía de Uso sea leída en su totalidad antes de iniciar la aplicación de Compliancers.

1.13 Agradecemos la confianza depositada en Compliancers, le rogamos nos dé traslado de su feedback ya que éste constituirá una valiosa aportación para mantener nuestro propósito de desarrollo continuo y le anunciamos nuestro compromiso de hacer evolucionar nuestra plataforma hasta consolidarla como una herramienta que aporte valor al posicionamiento de los despachos de abogados y consultores que cuentan con nosotros.

1.14 Nota final. Con independencia de la presente Guía de Uso, podrá el licenciatario acceder al “video demo” que se presenta en la web de Compliancers www.compliancesofficers.com.

2. PASOS DEL PROCESO Y RECOMENDACIONES BASICAS

2.1 Para una correcta utilización de Compliancers hemos de considerar los siguientes pasos y recomendaciones prácticas.

PASO 1 **Información General Datos de la empresa**	**PASO 2** **Fase de Consultas Check List**	**PASO 3** **Introducción al Manual de Compliance**
PASO 4 **Actividades de Riesgo**	**PASO 5** **Conductas de Riesgo**	**PASO 6** **Políticas Corporativas**
PASO 7 **Código de Etica y Conducta**	**PASO 8** **Procedimientos y Directrices.**	**PASO 9** **Plan de Vigilancia, Seguimiento y Control Tareas**
PASO 10 **Plan de Formación**	**PASO 11** **Régimen Disciplinario**	**PASO 12** **Canal de Denuncias**
PASO 13 **Acciones Post-delictivas**	**PASO 14** **Welcome Pack**	**PASO 15** **Imprimir documentos**
PASO 16 **Guardar Documentos Personalizados**	**PASO 17** **Prueba Documental**	**DOCUMENTOS DE APOYO**

3. Como gestiona la plataforma Compliancers.

3.1 Compliancers administra los flujos del proceso de compliance de manera metódica y estructurada a partir de la Fase de Consultas (check-list). Genera dos grandes bloques de informes: a) Informes particularizados y b) Informes generalistas.

Informes Particularizados.

3.2 En función de las respuestas registradas en el check-list de la Fase de Consultas, Compliancers presenta documentación personalizada y rigurosamente adaptada a las respuestas obtenidas. Cada empresa responde de manera diferente. Cada empresa se enfrenta a riesgos diferentes. Cada manual de compliance será, pues, diferente.

3.3 Son informes particularizados los siguientes:

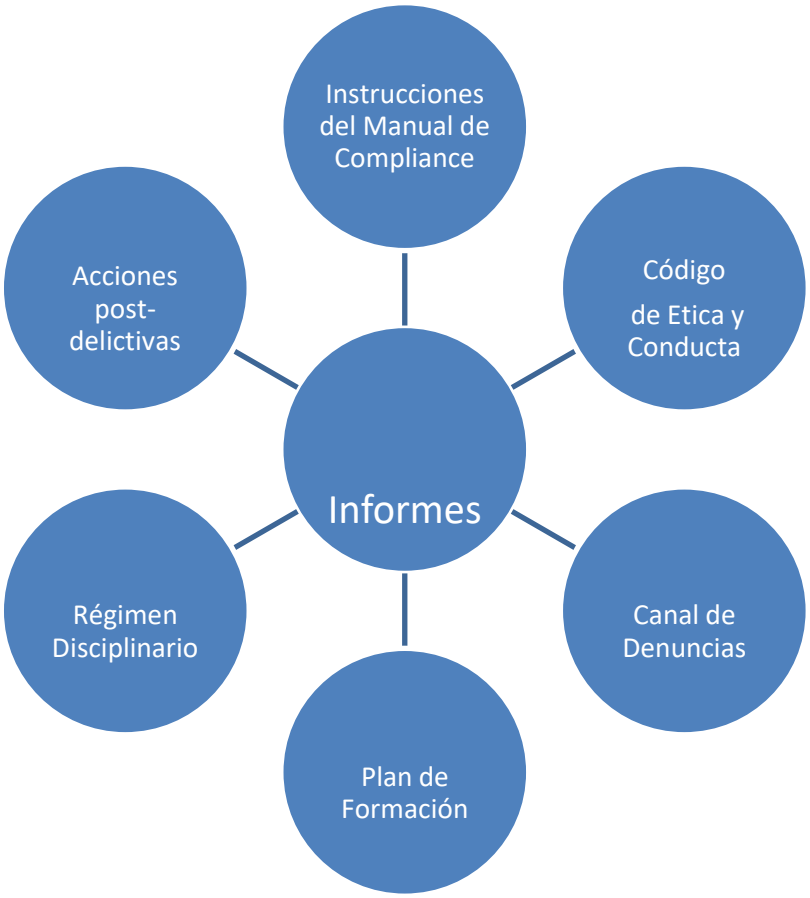
Informes Generalistas.

3.4 Compliancers presenta, además, una serie de informes que se exponen con carácter generalista y que, en consecuencia, son de igual contenido para todos los programas de compliance, si bien se presentan con referencia concreta a la denominación y logo de la empresa cliente.

3.5 Estos informes genéricos requieren, no obstante, una cierta intervención del profesional a fin de dotarlos de aquellas consideraciones que, a su criterio, precisen de la adecuada particularización.

3.6 Hemos de recordar la Circular nº 1/2016 de la Fiscalía General del Estado cuando sostiene que no serán admitidos programas estándar de "copia y pega" ni operaciones de "mero maquillaje". Es decir, que un programa de compliance penal ha de ser un trabajo hecho a la medida de las singularidades de cada empresa

3.7 Estos informes genéricos son los siguientes:



4. PASO 1. INFORMACION GENERAL

Acceso. Se accede a la plataforma mediante las claves de usuario y contraseña asignadas.

Crear. Nos permite acceder a la acción de alta un nuevo expediente: alta de una nueva empresa cliente.

Logo. Introducción de la imagen del logo de la empresa que acompañará a toda la documentación generada.

Editar. Nos permite la introducción de datos. Siempre que se desee introducir datos deberá activarse "editar".

Datos de empresa. Deben ser completados todos los requeridos.

Tipo de Estructura. Debe definirse con qué estructura empresarial vamos a trabajar para la implementación del compliance penal.

Para ello, solicitaremos de nuestro cliente que nos facilite el organigrama de su empresa, detallando las funciones de cada departamento y las personas responsables de los mismos.

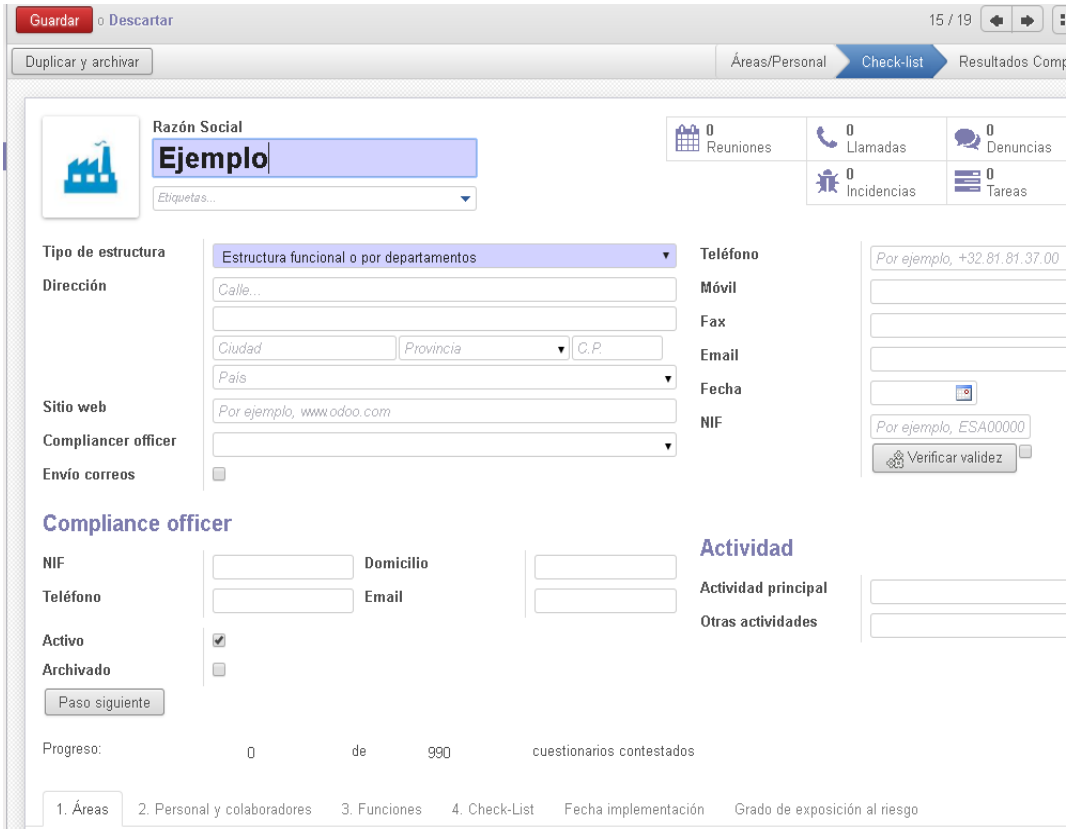
La Plataforma considera 2 tipos de estructura:

(a) Integral. Cuando estamos en presencia de una micro empresa que tiene concentradas sus áreas funcionales en una sola persona.

(b) Por departamentos o Areas Funcionales. En los demás casos.

Compliance Officer. Se identificará la persona que haya de ejercer las funciones de Compliance Officer y se cumplimentarán sus datos personales. En especial, le será asignada una dirección de correo electrónico ad hoc, independiente de la dirección habitual. Por ejemplo: complianceofficer@xxx.com. Será necesaria para gestionar el Plan de Vigilancia.

Fecha. Se hará costar la fecha de terminación del manual. Esta fecha aparecerá en toda la documentación como "fecha de implementación".



Areas. Selección de Departamentos - Areas Funcionales. Esta acción es de suma importancia, dado que, según los departamentos seleccionados, se comportará la plataforma y se desarrollarán los informes posteriores.

Son presentadas 27 áreas funcionales predefinidas y 3 opciones que permiten añadir hasta 3 áreas funcionales no predefinidas.

Corresponde al profesional seleccionar aquellas que se correspondan con el organigrama de la empresa. Las áreas predefinidas son:

	Departamentos – Áreas Funcionales	In	Ex
01	Organo de Administración.		
02	Financiero-Contabilidad.		
03	Facturación.		
04	Informática – Nuevas Tecnologías.		

05	Auditoría de Cuentas.
06	Asesoría Jurídica.
07	Asesoría Fiscal.
08	Asesoría Laboral. Nóminas. Seguridad Social.
09	Prevención Riesgos Laborales.
10	Recursos Humanos.
11	Aprovisionamiento – Compras.
12	Almacén – Depósitos.
13	Producción Industrial.
14	Producción Servicios.
15	Proyectos
16	Mantenimiento - Reparación
17	Logística
18	I+D+I
19	Calidad
20	Ventas Nacional
21	Ventas Exportación
22	Ventas on line
23	Atención a Cliente
24	Servicios postventa
25	Marketing y Comunicación
26	Transporte
27	Seguridad

Edición de departamentos. El profesional podrá autoeditar su propio organigrama, eliminando los departamentos predefinidos y sustituir el departamento que precise con uno definido por él mismo.

Recomendación. En las pymes, suele ocurrir que un mismo departamento gestione desde un mismo responsable varias áreas de trabajo. En tales casos, nuestra recomendación es que su tratamiento se lleve a cabo de manera unificada en un solo departamento que podrá llevar por título la conjunción de todas o de algunas de ellas.

Otros. Si el profesional precisa incorporar nuevas áreas funcionales podrá hacerlo usando el apartado de "otros" (hasta un total de 3).

Recomendación. Departamentos Externalizados. El profesional deberá tener en cuenta que un departamento concreto puede ser interno o externalizado. Por ejemplo, el área de asesoría fiscal, el área de auditoría, etc. En tales casos recomendamos que en el título del área se incluya mediante la autoedición el término "externalizado". Esto podrá ocurrir con otros servicios o proveedores, cuyas actividades puedan generar un riesgo para la empresa cliente.

Personal y colaboradores. Se introducirán todos los datos solicitados del personal y colaboradores afectos a cada departamento, cuidando de señalar en cada departamento quién es el "responsable". Será necesario en la Fase de Consultas, en los Procedimientos y Directrices y en el Plan de Vigilancia.

Recomendación. Debe tenerse presente que puede suceder que una misma persona realice trabajos en varios departamentos. En tal caso, procederá que sea incluida en aquel departamento en el que su presencia resulte más relevante. No hacerlo así conlleva a que, cuando se gestione el Plan de Seguimiento, Vigilancia y Control, este empleado recibirá un excesivo número de comunicaciones (muchas de las cuales serán repetitivas) y se correrá el riesgo de que le resulten bloqueantes hasta generar el conocido síndrome del "compliance fatigue".

Dirección de correo electrónico. Deberá incluirse en todo caso la dirección de correo electrónico de todo el personal. Será necesaria en el Plan de Vigilancia.

Comité de Vigilancia. Por defecto, se designa que este comité está formado por los responsables de cada departamento. Esta designación aparece en el Código de Etica y Conducta.

En todo caso, corresponderá al profesional, de conformidad con los criterios sugeridos desde la empresa cliente, quien deberá definir la composición del Comité de Vigilancia.

Funciones. Debe definirse las funciones de cada área funcional. Esta definición nos permitirá un mayor grado de conocimiento de la empresa y llevar a cabo el proceso de check-list teniendo en cuenta tales funciones.

5. PASO 2. FASE DE CONSULTAS. CHECK LIST

5.1 **Concepto**. El objetivo de esta acción es la identificación de las actividades de riesgo penal a las que pueda resultar expuesta la empresa en función de su negocio y, de manera muy especial, de las actividades de riesgo derivadas de las actuaciones de las personas con capacidad de decisión en el marco de la empresa.

Para la identificación de estas actividades de riesgo, deberá efectuarse una fase de consultas con los responsables de cada Area Funcional o Departamento de la empresa. Esta fase de consultas es definida como Check-list.

5.2 **Check-list.** El check-list cuenta con una serie de preguntas predefinidas que han sido configuradas en atención al ilícito penal previsto en capa tipo delictivo.

Su objetivo es identificar las actividades de riesgo por cada uno de los tipos delictivos (33) que han sido considerados relevantes, respecto de cada una de las Areas Funcionales ya seleccionadas.

El check list se realiza cerca del responsable de cada una de las Areas Funcionales con el fin de identificar los procesos en los que puede residir el riesgo penal.

Las respuestas al Check list son de “si” o “no”.

Recomendación. Se recomienda que, en esta acción, además del responsable del departamento a consultar, asista el órgano de administración. Su aportación es relevante.

5.3 **Aportación a la personalización**. Es el profesional quien, a la vista de la pregunta formulada, deberá profundizar e instruir suficientemente al responsable consultado, asegurándose de que comprende la pregunta y si en el marco de sus responsabilidades funcionales debe contestar con un “si” o con un “no”.

En esta fase de Consultas estamos analizando la exposición al riesgo. Por ello, ha de tenerse presente que lo que se contesta con un “sí” o con un “no” no es solamente que tal acción sea o no realizada por el entrevistado. Contestaremos con un “sí” siempre que, a juicio del profesional, pueda ser apreciada la posibilidad de incurrir en la exposición al riesgo objeto de pregunta.

Por ejemplo: Ante la pregunta: “¿extraes documentación de la empresa?” la respuesta puede ser “no”. Sin embargo, se anotará un “sí” cuando, dada la función del departamento consultado, exista, a criterio del profesional, el riesgo de que, teniendo acceso a documentación de la empresa, pueda ser extraída fuera de sus instalaciones. Se trata, en definitiva, de valorar la existen-

cia de exposición al riesgo para su posterior tratamiento en el modelo de cumplimiento.

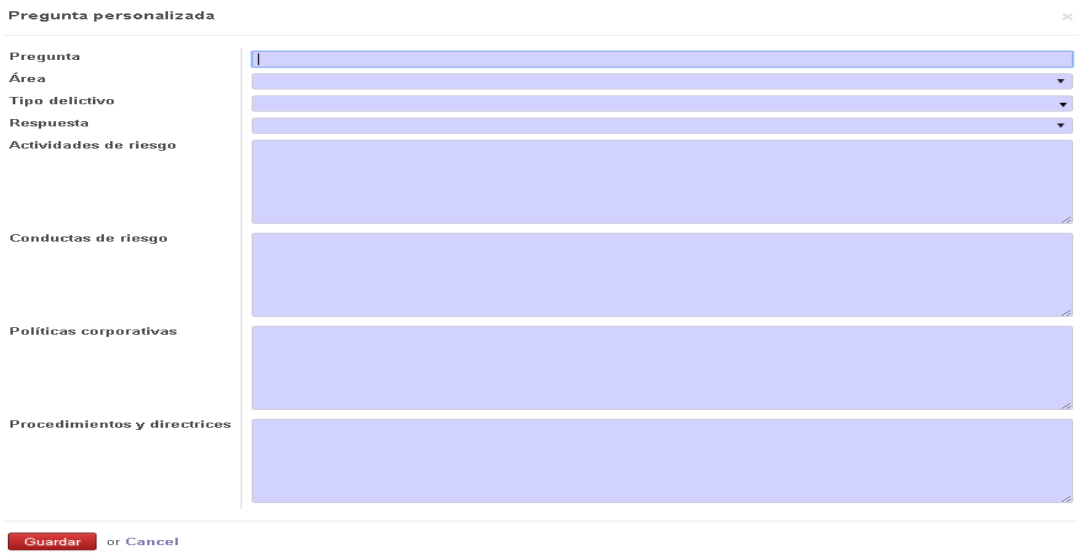
5.4 **Importancia**. La Fase de Consultas es absolutamente esencial en la medida que Compliancers tiene definida su administración de flujos a partir de las respuestas registradas en esta fase. Un error en esta acción reportará un error en los informes siguientes.

Recomendación. Para la realización de esta fase de consultas se hace necesario que el profesional disponga de conocimientos en el ámbito jurídico penal con el fin de llevar a cabo una correcta interpretación de los delitos vigentes identificados en el Código Penal, así como de un conocimiento del negocio de la empresa sobre el que está definiendo el inventario de actividades de riesgo.

Siendo así que el conocimiento del negocio no siempre estará a disposición del profesional, éste deberá dedicar el tiempo suficiente en recabar la necesaria instrucción del personal cualificado de la empresa y, de manera especial, del equipo directivo.

Hemos de reiterar nuestra llamada de atención acerca de la importancia de dedicar el tiempo necesario en el desarrollo de esta fase.

5.5 **Preguntas Personalizadas**. La plataforma tiene configuradas más de 400 preguntas que habrán de ser evacuadas a cada departamento de la empresa; lo que, en principio, podría ser considerado suficiente. Sin embargo, el profesional puede detectar la conveniencia de realizar alguna pregunta que no está comprendida en el check-list predefinido. En este caso, hará uso de un clic en **"preguntas personalizadas".**



Las respuestas a preguntas personalizadas no están contempladas en el sistema. Es por ello que, tras la respuesta, deberá tener presente el profesional la necesidad de definir cuál es la nueva actividad de riesgo y desarrollar personalmente y de forma manual el proceso completo en el Informe de Actividades de Riesgo, en el Informe de Conductas de Riesgo, en las Políticas Corporativas, en los Procedimientos y Directrices y, finalmente, en el Plan de Vigilancia, Seguimiento y Control.

5.6 Repetir Preguntas. Permite repetir un cuestionario.

5.7 Visualización. El Informe de Check list puede ser visualizado haciendo clic en la pestaña “imprimir”.

No será posible visualizar ni imprimir el resultado del check-list hasta haber activado “paso siguiente” y “guardar”.

5.8 Inventario de delitos. Los tipos delictivos que serán objeto de Check-list son los siguientes:

Artículo CP	Tipo Delictivo
156 bis	Tráfico ilegal y trasplante de órganos
177 bis	Trata de seres humanos
187	Prostitución – explotación sexual – corrupción de menores
197	Delitos contra la intimidad y el allanamiento informático
248	Estafa
257	Insolvencia punible. Alzamiento de bienes.
259	Insolvencia punible. Insolvencia actual o inminente.
262	Dopaje deportivo
264	Daños informáticos.
270	Delitos contra la propiedad intelectual.
273	Delitos contra la propiedad industrial.
278	Descubrimiento y revelación de secretos de empresa.
281	Desabastecimiento de materias primas
282	Publicidad engañosa.

283	Facturación fraudulenta.
286	Acceso ilegal al servicio de radiodifusión o televisión.
286 bis	Corrupción en los negocios.
286 bis	Corrupción deportiva.
301	Receptación y blanqueo de capitales.
304 bis	Financiación ilegal de partidos políticos.
305	Delitos contra la Hacienda Pública.
307	Delitos contra la Seguridad Social.
311	Delitos contra los derechos de los ciudadanos.
318 bis	Delitos contra los derechos de los ciudadanos extranjeros.
319	Delitos contra la ordenación del territorio.
325	Delitos contra los recursos naturales y el medio ambiente.
348	Delitos de riesgo provocado por explosivos.
359	Delitos con medicamentos contra la salud pública.
363	Delitos alimentarios contra la salud pública.
368	Delitos contra la salud. Drogas y estupefacientes.
386	Falsedad de medios de pago
424	Cohecho
429	Tráfico de influencias.

5.9 Ejemplo. A continuación, pasamos a ver un ejemplo de Check-list.

DELITOS CONTRA LA INTIMIDAD Y EL ALLANAMIENTO INFORMATICO **Art. C.P. 197 - 197 bis - ter - quater - quinquies - 198 - 199 - 200**	
01 – TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL. ¿Tienes o tiene tu departamento acceso o tratamiento de datos de carácter personal: socios, directivos, empleados, profesionales, clientes, proveedores y otros terceros?	

02 – ACCESO A SISTEMAS INFORMATICOS DE LA EMPRESA O DE TERCEROS. ¿Tienes o tiene tu departamento acceso a sistemas informáticos de la empresa o de terceros?	
03 – CORREO ELECTRONICO. ¿Tienes o tiene tu departamento acceso al correo electrónico del personal interno o externo (claves de usuario y contraseña)?	
04 – COPIA EN EQUIPOS O DISPOSITIVOS. ¿Copias y traspasas o copia y traspasa tu departamento información archivada en los equipos informáticos de la empresa a algún dispositivo portátil?	
05 – EXTRACCION DE INFORMACION ELECTRONICA. ¿Extraes o extrae tu departamento archivos contenidos en los sistemas informáticos de la empresa?	
06 – EXTRACCION DE DOCUMENTOS FISICOS. ¿Extraes o extrae tu departamento documentación en papel de trabajo fuera de la empresa?	
07 – ESCUCHA Y GRABACION. ¿Existen en tu departamento o en su personal alguna clase de dispositivos que permitan grabar conversaciones o videos?	

6. PASO 3. INTRODUCCION AL MANUAL DE COMPLIANCE

6.1 Concepto. El presente documento constituye la presentación de lo que es un programa de cumplimiento penal y forma parte de su documentación como primer documento.

El objetivo es explicar de manera sucinta por qué un programa de compliance, la metodología seguida, la definición de sus objetivos y el compromiso formalizado por la empresa.

6.2 Modelo Generalista. Este documento tiene el carácter de modelo general y es, en principio, aplicable a cualquier empresa cliente.

6.3 Aportación a la personalización. El profesional podrá aceptar el modelo o incorporar aquellas consideraciones que estime pertinentes.

Visualización. El contenido del Informe de Introducción al Manual de Compliance puede ser visualizado haciendo clic en la pestaña “imprimir”.

7. PASO 4. ACTIVIDADES DE RIESGO

7.1 Informe de Actividades de Riesgo. En función de las respuestas registradas en la Fase de Consultas (check-list), la plataforma genera un Informe de Actividades de Riesgo.

Este informe es generado sólo a partir de las respuestas contestadas con un "SI".

Cuando la respuesta de la Fase de Consultas es un "NO", la plataforma declina la existencia de tal actividad de riesgo y lo trata como "actividad de riesgo irrelevante".

7.2 Administración de flujos. Las actividades de riesgo emanan de la Fase de Consultas de cada una de las áreas funcionales.

7.3 Aportación a la personalización. Ha de tenerse presente que Compliancers configura el Informe de Actividades de Riesgo a tenor de las consultas predefinidas. De tal manera que, si el profesional ha añadido alguna pregunta personalizada, corresponderá a éste la definición de la actividad de riesgo pertinente.

En tal caso, procederá a añadir manualmente tal actividad de riesgo en el Informe de Actividades de Riesgo.

Cada departamento seleccionado dará lugar a información de riesgo por cada uno de los 33 tipos delictivos.

7.4 Grado de Exposición al Riesgo. El grado de exposición al riesgo mide la frecuencia de exposición de un departamento a la comisión de un tipo delictivo concreto y el nivel de probabilidad de incurrir en éste. Esta acción es generada de manera automática por la plataforma, de acuerdo con los criterios y matrices generalmente aceptados en la evaluación y auditoría de riesgos. El grado de exposición se evalúa de menos a más del 1 = Irrelevante; 2 = Muy bajo; 3 = Bajo; 4 = Medio; 5 = alto; 6 = Muy alto. Este mapa permite al Compliance Officer, administrador de las CACs, elegir qué riesgos merecen ser tratados a fin de establecer prioridades para su tratamiento y control.

%	GRADO DE RIESGO
81-100	MUY ALTO
61-80	ALTO
41-60	MEDIO
21-40	BAJO
1-20	MUY BAJO
0	IRRELEVANTE

7.5 **Visualización**. El Informe de Actividades de Riesgo puede ser visualizado haciendo clic en la pestaña “imprimir”.

No será posible visualizar ni imprimir el Informe de Actividades de Riesgo hasta haber activado “paso siguiente” y “guardar”.

7.6 **Ejemplo**. A continuación, se muestra un ejemplo del Informe de las Actividades de Riesgo respecto de delito contemplado en el art. 197 y siguientes del Código Penal.

DELITOS CONTRA LA INTIMIDAD Y EL ALLANAMIENTO INFORMATICO Art. C.P. 197 - 197 bis - ter - quater - quinquies - 198 - 199 - 200
Grado de exposición al riesgo: MUY ALTO
01 – TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL. Tratamiento de datos de carácter personal de socios, directivos, empleados, profesionales, colaboradores, clientes, proveedores y otros terceros.
02 – ACCESO A SISTEMAS INFORMATICOS DE LA EMPRESA O DE TERCEROS. Acceso a sistemas informáticos de la empresa o de terceros.
03 – CORREO ELECTRONICO. Acceso al correo electrónico del personal interno o externo (claves de usuario y contraseña).
04 – COPIA EN EQUIPOS O DISPOSITIVOS. Copia, traspaso o reproducción de información archivada en los equipos informáticos de la empresa a algún dispositivo portátil.
05 – EXTRACCION DE INFORMACION ELECTRONICA. Extracción fuera de la empresa de archivos e información contenidos en los sistemas informáticos de la empresa.
06 – EXTRACCION DE DOCUMENTOS FISICOS. Extracción de documentación de trabajo en papel fuera de la empresa.
07 – ESCUCHA Y GRABACION. Grabación de sonido o imagen.

7.7 **Ejemplo**. A continuación, se muestra un ejemplo del Informe resumen de las Actividades de Riesgo respecto de algunos de los delitos contemplados en el compliance program supuesto:

ANÁLISIS DE RIESGOS		Ver.1
AREA FUNCIONAL DE GERENCIA		
Nº	DELITO	GRADO DE SEVERIDAD
1	Art. C.P. 197 DELITOS CONTRA LA INTIMIDAD Y EL ALLANAMIENTO INFORMATICO	MUY ALTO
2	Art. C.P. 248 ESTAFAS	MUY ALTO
3	Art. C.P. 257 INSOLVENCIA PUNIBLE. FRUSTRACION DE LA EJECUCION	MUY ALTO
4	Art. C.P. 259 INSOLVENCIA PUNIBLE. INSOLVENCIA ACTUAL O INMINENTE	MUY ALTO
5	Art. C.P. 264 DAÑOS INFORMATICOS	MUY ALTO
6	Art. C.P. 270 DELITOS CONTRA LA PROPIEDAD INTELECTUAL	ALTO
7	Art. C.P. 273 DELITOS CONTRA LA PROPIEDAD INDUSTRIAL	IRRELEVANTE
8	Art. C.P. 278 DESCUBRIMIENTO Y REVELACION DE SECRETOS DE LA EMPRESA	MUY ALTO
9	Art. C.P. 282 PUBLICIDAD ENGAÑOSA	MUY ALTO
10	Art. C.P. 283 FACTURACION FRAUDULENTA	IRRELEVANTE
11	Art. C.P. 286 ACCESO A LA RADIODIFUSION SONORA O TELEVISIVA	MEDIO
12	Art. C.P. 286 bis CORRUPCION EN LOS NEGOCIOS	MUY ALTO
13	Art. C.P. 298 RECEPTACION Y BLANQUEO DE CAPITALES	MUY ALTO
14	Art. C.P. 304 bis FINANCIACION ILEGAL DE PARTIDOS POLITICOS	MUY ALTO
15	Art. C.P. 305 DELITOS CONTRA LA HACIENDA PUBLICA	MUY ALTO
16	Art. C.P. 307 DELITOS CONTRA LA SEGURIDAD SOCIAL	MUY ALTO
17	Art. C.P. 311 DELITOS CONTRA LOS DERECHOS DE LOS TRABAJADORES	MUY ALTO
18	Art. C.P. 318 bis DELITOS CONTRA LOS DERECHOS DE LOS CIUDADANOS EX-TRANJEROS	IRRELEVANTE
19	Art. C.P. 319 DELITOS CONTRA LA ORDENACION DEL TERRITORIO	IRRELEVANTE
20	Art. C.P. 325 DELITOS CONTRA LOS RECURSOS NATURALES Y EL MEDIO AM-BIENTE	IRRELEVANTE
21	Art. C.P. 348 DELITOS CON EXPLOSIVOS Y OTROS AGENTES	IRRELEVANTE
22	Art. C.P. 359 DELITOS CON MEDICAMENTOS CONTRA LA SALUD PUBLICA	IRRELEVANTE
23	Art. C.P. 363 DELITOS CON ALIMENTOS CONTRA LA SALUD PUBLICA	IRRELEVANTE
24	Art. C.P. 368 DELITOS CONTRA LA SALUD. DROGAS ESTUPEFACIENTES Y SUS-TANCIAS PSICOTROPICAS	IRRELEVANTE
25	Art. C.P. 424 COHECHO	ALTO
26	Art. C.P. 429 TRAFICO DE INFLUENCIAS	ALTO

8. PASO 5. CONDUCTAS DE RIESGO

8.1 **Informe de Conductas de Riesgo**. La Plataforma genera el Informe de las Conductas de Riesgo. Estas conductas de riesgo representan los supuestos de hecho contemplados en las actividades de riesgo generadas y su vinculación con los tipos delictivos analizados.

8.2 **Administración de flujos**. Las conductas de riesgo emanan del análisis previo de las actividades de riesgo de la empresa y, en especial, de cada una de las áreas funcionales.

8.3 **Aportación a la personalización**. Este informe individualizado puede ser definitivo en el contexto del programa de cumplimiento penal, en tanto que el administrador de flujos lo mantiene asociado a las actividades de riesgo.

Ello, no obstante, el profesional deberá proceder a su revisión por si, en atención a la singularidad de la empresa analizada, fuera el caso de añadir o matizar alguna conducta de riesgo que resulte aconsejable desde su opinión profesional.

En todo caso, ha de tenerse presente que Compliancers configura el Informe de Conductas de Riesgo a tenor de las consultas predefinidas. De tal manera que si el profesional ha añadido alguna pregunta personalizada, corresponderá a éste la definición de la conducta de riesgo oportuna.

En tal caso, procederá a añadir manualmente tal conducta en el Informe de Conductas de Riesgo.

Cada departamento seleccionado dará lugar a información de conductas de riesgo por cada uno de los 33 tipos delictivos analizados.

La identificación de estas conductas de riesgo facilitará la posterior elaboración de las Políticas Corporativas, la implantación de los Procedimientos y Directrices y el Plan de Vigilancia y Control.

8.4 **Grado de Severidad del Riesgo**. El grado de Severidad de la Conducta de Riesgo mide la severidad de las posibles consecuencias de una conducta delictiva determinada. Esta acción es generada de manera automática por la plataforma, de acuerdo con los criterios y matrices generalmente aceptados en la evaluación y auditoría de riesgos. El grado de exposición se evalúa de menos a más del 1 = Alto; 2 = Muy Alto; 3 = Crítico. Este mapa permite al Compliance Officer, administrador de las CACs, elegir qué riesgos merecen ser tratados a fin de establecer prioridades para su tratamiento y control.

AÑOS	GRADO DE SEVERIDAD
7-8 años	CRÍTICO
4-6 años	MUY ALTO
0-3 años	ALTO

8.5 **Visualización**. El Informe de Conductas de Riesgo puede ser visualizado haciendo clic en la pestaña “imprimir”.

No será posible visualizar ni imprimir el Informe de Conductas de Riesgo hasta haber activado “paso siguiente” y “guardar”.

8.6 **Ejemplo**. A continuación, presentamos un ejemplo:

DELITOS CONTRA LA INTIMIDAD Y EL ALLANAMIENTO INFORMATICO Art. C.P. 197 - 197 bis - ter - quater - quinquies - 198 - 199 - 200
Grado de severidad: ALTO
01 – TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL. Apoderarse, descubrir y/o revelar datos de carácter personal de socios, directivos, empleados, profesionales, colaboradores, clientes, proveedores, y otros terceros.
02 – ACCESO A SISTEMAS INFORMATICOS DE LA EMPRESA O DE TERCEROS. Apoderarse, descubrir y/o revelar información de carácter confidencial de socios, directivos, empleados, profesionales, colaboradores terceros.
03 – CORREO ELECTRONICO. Apoderarse, descubrir y/o revelar información de carácter personal o confidencial de la empresa o de terceros.
04 – COPIA EN EQUIPOS O DISPOSITIVOS. Apoderarse, descubrir y/o revelar información archivada en los equipos informáticos de la empresa.
05 – EXTRACCION DE INFORMACION ELECTRONICA. Apoderarse, descubrir y/o revelar información contenida en los archivos informáticos de la empresa.
06 – EXTRACCION DE DOCUMENTOS FISICOS. Apoderarse, descubrir y/o revelar información contenida en la documentación física de la empresa.
07 – ESCUCHA Y GRABACION. Efectuar grabaciones de sonido o imagen sin autorización.

9. PASO 6. POLITICAS CORPORATIVAS

9.1 **Concepto**. Políticas corporativas son los estándares de conducta necesarios para asegurar el cumplimiento de la ley.

Comprende las obligaciones y las conductas especialmente prohibidas en el seno de la empresa.

9.2 **Administración de flujos**. Las políticas de empresa emanan del análisis previo de las conductas de riesgo examinadas.

9.3 El objetivo de esta acción es la configuración de aquellos comportamientos que deberán ser seguidos por todos los integrantes de la organización.

La plataforma genera de manera metódica unas Políticas de Empresa, en función de los tipos delictivos que han quedado configurados en el Informe de Conductas de Riesgo.

9.4 Las Políticas de Empresa presentan:

- Obligaciones.
- Prohibiciones.

9.5 **Obligaciones.** Son aquellas actuaciones o comportamientos exigidos a todos los integrantes de la organización con carácter obligatorio en razón de que su incumplimiento puede dar lugar a la realización de conductas delictivas.

Las obligaciones se presentan con carácter genérico y común para todas las políticas corporativas.

9.6 **Prohibiciones.** Son aquellas actuaciones que quedan impedidas a todos los integrantes de la organización, en razón de que su incumplimiento puede dar lugar a la realización de conductas delictivas.

Las prohibiciones se presentan de manera individualizada y personalizada por cada departamento, en función de las respuestas registradas en la fase de consultas y del Informe de Conductas de Riesgo.

9.7 **Aportación a la personalización**. El profesional leerá con detenimiento estas políticas de empresa y podrá evaluar la conveniencia de incorporar o matizar las que considere oportunas y convenientes.

En todo caso, ha de tenerse presente que Compliancers configura el Informe de las Políticas Corporativas a tenor de las consultas predefinidas. De tal manera que, si el profesional ha añadido alguna pregunta personalizada, corresponderá a éste la definición de la política corporativa pertinente.

En este caso, procederá a añadir manualmente tal política de empresa en el Informe de Políticas Corporativas.

Cada departamento seleccionado dará lugar a información de políticas corporativas por cada uno de los 33 tipos delictivos

9.8 **Visualización**. El Informe de Políticas Corporativas puede ser visualizado haciendo clic en la pestaña “imprimir”.

No será posible visualizar ni imprimir el Informe de Políticas Corporativas hasta haber activado “paso siguiente” y “guardar”.

9.9 **Ejemplo**. A continuación, presentamos un ejemplo de cómo queda definida una Política de Empresa en el Area de Administración y Gerencia.

AREA FUNCIONAL DE ADMINISTRACION Y GERENCIA
INSOLVENCIA PUNIBLE. INSOLVENCIA ACTUAL O INMINENTE Art. C.P. 259, 259 bis, 260, 261 y 261 bis
OBLIGACIONES
01 – Estricto cumplimiento del Código de Ética y de las Políticas Corporativas de la empresa.
02 – Asistir a las formaciones que en materia de Compliance proporcione la empresa.
03 – Leer y comprender el “código de ética”, el documento de las “políticas corporativas”, el “canal de denuncias” y el “régimen disciplinario” y preguntar sobre las dudas a que hubiere lugar.
04 – Atender con diligencia los comunicados y requerimientos que en relación a políticas corporativas y procedimientos remita la empresa.
05 – Informar de posibles riesgos y de los incumplimientos observados de la presente política al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención, a través de los canales de denuncia establecidos.
06 – Si en el presente programa de cumplimiento penal ha sido designado como Responsable de un Área Funcional o Departamento de la empresa, ejecutar el Plan de Acción Anual que se le asigna desde los Procedimientos y Directrices aprobados.
CONDUCTAS PROHIBIDAS
01 – OPERACIONES VINCULADAS. En situación de insolvencia inminente o actual, dirigir o gestionar operaciones vinculadas de la empresa con otras empresas del grupo o con socios y administradores, ocultando bienes de la empresa o alterando significativamente la estructura y composición de los estados financieros de la empresa.
02 – OPERACIONES DE VENTA DE ACTIVOS. En situación de insolvencia inminente o actual, realizar actos de disposición de bienes y derechos que carezcan de justificación económica o por precio inferior al de mercado en perjuicio de acreedores. Realizar, sin justificación económica o empresarial, actos generadores de obligaciones, pagos de un crédito no exigible o la concesión de garantías no exigibles, favoreciendo a un acreedor en perjuicio de otros.
03 – OPERACIONES DE CREDITO. En situación de insolvencia inminente o actual, simular o reconocer créditos de terceros ficticios.
04 – LIQUIDEZ. En situación de insolvencia inminente o actual, ocultar o manipular la situación de liquidez de la empresa. Ocultar bienes y derechos de la empresa.
05 – OPERACIONES ESPECULATIVAS. En situación de insolvencia inminente o actual, participar en negocios especulativos que pongan en riesgo la solvencia de la empresa.
06 – PAGOS Y COBROS. En situación de insolvencia inminente o actual, ordenar o ejecutar pagos o cobros de la empresa con base a operaciones inexistentes.
07 – FONDOS PROPIOS. Ocultar o manipular el estado real de los fondos propios de la empresa.