BLOQUE 6: Mapa de riesgos y demás procedimientos y políticas

Sesión 10 (13 de noviembre de 2024)
Identificación de políticas, procedimientos y protocolos necesarios en un programa de compliance

- *Miguel Gadea (DLA Piper)*
- *Víctor Caballero (Centro de Estudios Garrigues)*

Fundación Pro Bono España

CENTRO DE ESTUDIOS GARRIGUES

Fundación Nemesio Diez

ÍNDICE

1.- INTRODUCCIÓN A LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

1. INTRODUCCIÓN

Responsabilidad criminal de las personas jurídicas

❖ **La Ley Orgánica 5/2010 de 22 de junio introdujo la responsabilidad penal de las personas jurídicas.**

- Es una responsabilidad **separada e independiente** de la persona física que comete el delito.
- Tiene su fundamento en " *el* ***defecto estructural en los mecanismos de prevención*** *exigibles a toda entidad, y que de haber funcionado correctamente* ***hubieran evitado la infracción delictiva*** *cometida por quién forma parte de dicha organización*".
- Sólo cabe la responsabilidad penal en los **casos expresamente previstos** en el Código Penal.

❖ **Las personas jurídicas son responsables penalmente (artículo 31 bis CP)**

a. De los delitos **cometidos en nombre o por cuenta de las mismas**, y en su **beneficio directo o indirecto.**

1. INTRODUCCIÓN

Responsabilidad criminal de las personas jurídicas

❖ **Las personas jurídicas son responsables penalmente (artículo 31 bis CP)**

b) Por:

- ❑ sus representantes legales
- ❑ por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están **autorizados para tomar decisiones** en nombre de la persona jurídica u **ostentan facultades de organización y control** dentro de la misma.
- ❑ estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por **haberse incumplido** gravemente por aquéllos los **deberes de supervisión, vigilancia y control** de su actividad atendidas las concretas circunstancias del caso

1. INTRODUCCIÓN

Responsabilidad criminal de las personas jurídicas

❖ **Penas imponibles a las personas jurídicas (art. 33. 7 CP)**

a) **Multa** por cuotas o proporcional.
b) **Disolución** de la persona jurídica.
c) **Suspensión** de sus actividades por un plazo que no podrá exceder de cinco años.
d) **Clausura** de sus locales y establecimientos por un plazo que no podrá exceder de cinco años.
e) **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. Si fuere temporal, el plazo no podrá exceder de quince años.
f) **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.
g) **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.

Art 31 bis. 5

1. ***Identificar*** *las* ***actividades*** *en cuyo ámbito puedan ser* ***cometidos los delitos*** *que deben ser prevenidos.*
2. ***Establecer*** *los protocolos o procedimientos que concreten el* ***proceso de formación de la voluntad*** *de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.*
3. ***Disponer*** *de* ***modelos de gestión*** *de los* ***recursos financieros*** *adecuados para impedir la comisión de los delitos que deben ser prevenidos.*
4. ***Imponer*** *la obligación de* ***informar de posibles riesgos*** *e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.*
5. ***Establecer*** *un sistema disciplinario que* ***sancione*** *adecuadamente* ***el incumplimiento de las medidas*** *que establezca el modelo.*
6. ***Realizar*** *una* ***verificación periódica del modelo*** *y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.*

→ **Mapa de riesgos**

Políticas y procedimientos

El juicio a las personas jurídicas es una realidad

Fundación Pro Bono España · CENTRO DE ESTUDIOS GARRIGUES · Fundación Nemesio Diez · DLA PIPER

2.- ANTECEDENTES Y DERECHO COMPARADO

2. ANTECEDENTES Y DERECHO COMPARADO

- **Normas ISO y normas UNE**
  - UNE-ISO 37301, Principios de políticas de compliance
- **Marcos integrados de COSO**
  - Control interno y gestión de riesgos
- **Derecho comparado (EEUU)**
  - *Foreign Corruption Practices Act* (1977) , *The Defense Industry Initiative* (1986)

ISO International Organization for Standardization (iso.org)

cen (cen.eu)

UNE (une.org)

Asociación privada, multisectorial y sin fines lucrativos, designada por el Mº Economía, Industria y Competitividad como organismo nacional de normalización. Miembros: asociaciones empresariales.

[otros países: BSI, DIN, AFNOR, UNI, ANSI…]

Normas ISO → Normas EN ISO → Normas UNE-EN ISO
Normas EN → Normas UNE-EN
Normas UNE-ISO
Normas UNE

[No todas son certificables]

[ESTÁNDARES O NORMAS]

ENAC Entidad Nacional de Acreditación

Entidad designada por el Gobierno (Mº Economía, Industria y Competitividad), para operar en España como el único Organismo Nacional de Acreditación, en aplicación del Reglamento (CE) nº 765/2008 que regula el funcionamiento de la acreditación en Europa. Asociación sin ánimo de lucro y declarada de utilidad pública. Miembros públicos (órganos de calidad y seguridad industrial, ambiental, alimentaria…) y privados.

→ AENOR, EQA, SGS, BV, DNV… →

Certificar de forma previa varios modelos (sin logo ENAC), supervisión por ENAC y, en su caso, certificar oficialmente (con logo ENAC).

1) Revisión documental
2) Revisión de la implantación
3) PAC (Plan de Acciones Correctivas)
4) Certificado válido 3 años
5) Auditorías externas anuales de seguimiento
6) Al tercer año auditoría de renovación del certificado

3.- Mapas de riesgos penales

- **¿Qué son los mapas de riesgos?**

Son documentos que sirven de compendio de los riesgos penales que pueden afectar a una organización.

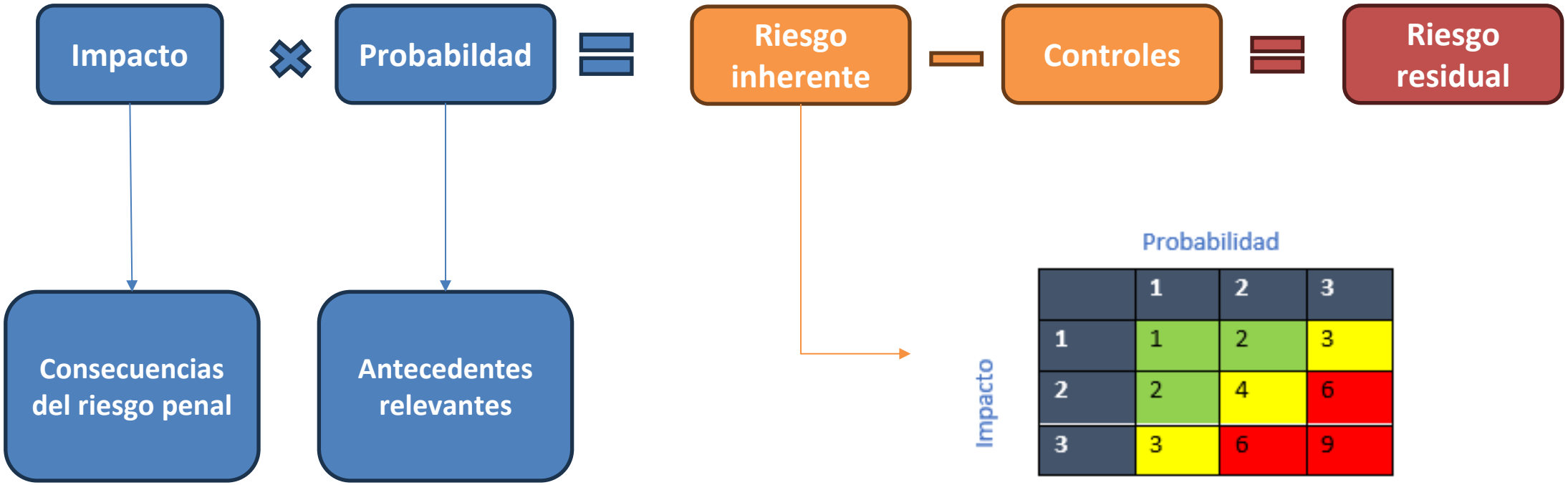
- **¿Qué contenido debe tener un mapa de riesgos?**

  - Riesgos
  - Valoración de los riesgos
  - Áreas afectadas
  - Controles aplicados

Control	Descripción	Alcance	Propietario	Riesgos	Documento	Entrada en vigor	Aprobado por
Nombre	Breve	Áreas, etc.	Responsable	Riesgo 1 Riesgo 2 Riesgo 3 Etc.	Documento, edición	Fecha	Aprobador

Riesgo	Control	Descripción	Alcance	Propietario	Documento	Entrada en vigor	Aprobado por
Riesgo 1	Control 1	Desc. 1	Áreas 1	Respons. 1	Doc., ed. 1	Fecha 1	Aprobador 1
Riesgo 1	Control 2	Desc. 2	Áreas 2	Respons. 2	Doc., ed. 2	Fecha 2	Aprobador 2
Riesgo 1	Etc.	Etc.	Etc.	Etc.	Etc.	Etc.	Etc.

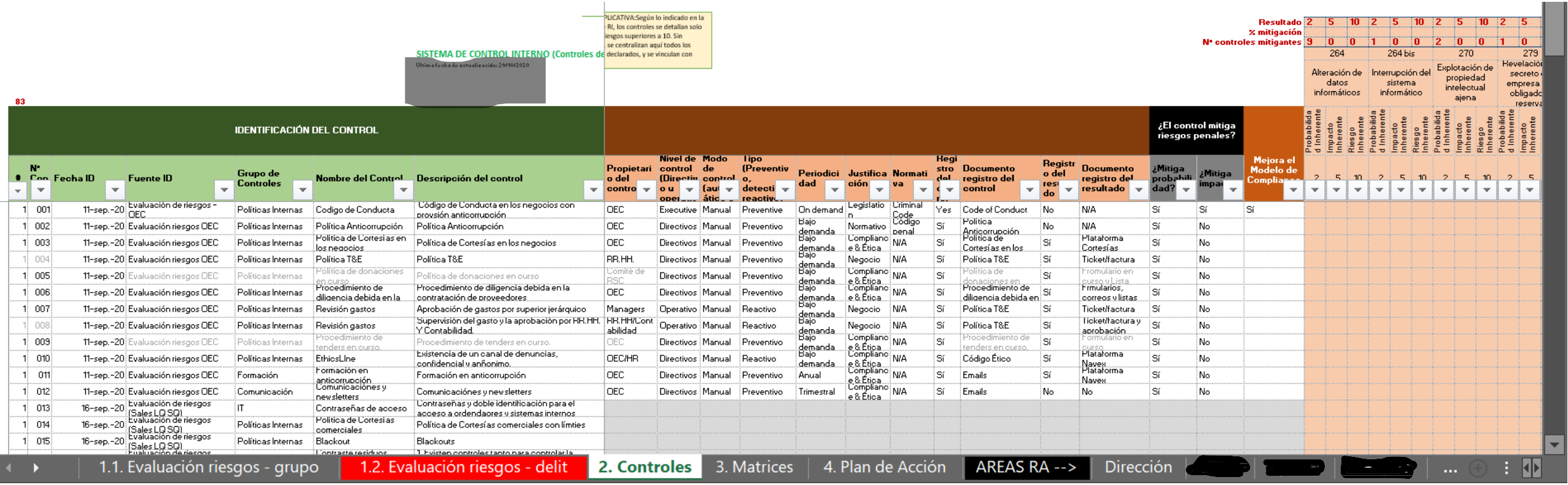
VALORACIÓN DEL RIESGO



Ejemplo de mapa de riesgos

Identificación del riesgo				Análisis y evaluación del riesgo				Tratamiento del ries	
Artículo del Código Pen	Tipo delictivo o riesgo legal	Conductas asociadas al tipo	Ejemplos de situaciones de riesgo	Departamento	Probabilidad	Impacto	Riesgo inherent	Tratamiento	Mitigador
173	Delito contra la integridad moral	Infligir a otra persona un trato degradante, menoscabando gravemente su integridad moral.	Faltas de respeto, burlas, bromas pesadas, comentarios en redes sociales	RR.HH.	1	1	1	Aceptar	• Código de Conducta • Política de Grupo contra la discriminación y el acc • Canal interno de denuncias *Speak up* • Monitorización por el Compliance Officer
173	Delito contra la integridad moral	En el ámbito de cualquier relación laboral o funcionarial y prevaliéndose de su relación de superioridad, realizar contra otro de forma reiterada actos hostiles o humillantes que, sin llegar a constituir trato degradante, supongan grave acoso contra la víctima.	Las conductas anteriores realizadas por superiores jerárquicos	RR.HH.	1	1	1	Aceptar	• Código de Conducta • Política de Grupo contra la discriminación y el acc • Canal interno de denuncias *Speak up* • Monitorización por el Compliance Officer
184	Acoso sexual	Solicitar favores de naturaleza sexual, para sí o para un tercero, en el ámbito de una relación laboral provocando a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante.	Un empleado hace comentarios y sugerencias de carácter sexual a otro empleado	RR.HH.	1	1	1	Aceptar	• Código de Conducta • Política de Grupo contra la discriminación y el acc • Plan de Igualdad entre Hombres y Mujeres • Protocolo de Prevención de acoso sexual y acos razón de género • Canal interno de denuncias *Speak up* • Monitorización por el Compliance Officer
184	Acoso sexual	La conducta anterior prevaliéndose de una situación de superioridad laboral, docente o jerárquica, o sobre persona sujeta a su guarda o custodia, o con el anuncio expreso o tácito de causar a la víctima un mal relacionado con las legítimas expectativas que aquella pueda tener en el ámbito de la indicada relación.	Un manager de Springer hace comentarios y sugerencias de carácter sexual a una subordinada.	RR.HH.	1	1	1	Aceptar	• Código de Conducta • Política de Grupo contra la discriminación y el acc • Canal interno de denuncias *Speak up* • Monitorización por el Compliance Officer
197 quinquies/197	Descubrimiento y revelación de secretos y allanamiento informático	Apoderarse de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento.	Sustracción de documentos o efectos personales accediendo al puesto de trabajo de un empleado Interceptación de correos electrónicos	IT RR.HH.	1	1	1	Reducir	• Código de Conducta • Group Privacy & Information Technology Policy • Levels of Authority IT • Política de obligaciones de personal en relación c tratamiento de datos de carácter personal y utiliza de sistemas informáticos de Macmillan • Medidas de control sobre los equipos y las redes carácter exhaustivo) • Empleo de VPN y firewalls, • Directrices generales de los servicios centrales s cómo plataformar los equipos informáticos, • Empleo de un sistema centralizado que gestiona l credenciales de acceso al sistema y su monitoriza periódica, • Enrutamiento de la red a efectos de asegurar que sean vulneradas las medidas de seguridad,
197 quinquies/197	Descubrimiento y revelación de secretos y allanamiento informático	Interceptar las telecomunicaciones o utilizar artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, para descubrir los secreto o vulnerar la intimidad de otro.	Intercepción de llamadas telefónicas o de micrófonos en dispositivos. Instalación de micrófonos, cámaras o grabadoras	IT RR.HH.	1	1	1	Reducir	
197 quinquies/197	Descubrimiento y revelación de secretos y allanamiento informático	Sin estar autorizado, apoderarse, utilizar o modificar, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, o acceder por cualquier medio a esa misma información y alterarla o utilizarla en perjuicio del titular de los datos o de un tercero.	Hackeo de bases de datos en las que se contengan datos personales, sean de terceros o de trabajadores.	IT RR.HH.	1	1	1	Reducir	

EJEMPLO DE MAPA DE RIESGOS



SISTEMA DE CONTROL INTERNO (Controles de

Última fecha de actualización: 29/10/2020

PLICATIVA:Según lo indicado en la RI, los controles se detallan solo iesgos superiores a 10. Sin se centralizan aquí todos los declarados, y se vinculan con

Resultado 2 5 10 2 5 10 2 5 10 2 5
% mitigación
Nº controles mitigantes 9 0 0 1 0 0 2 0 0 1 0

264 | 264 bis | 270 | 279

Alteración de datos informáticos | Interrupción del sistema informático | Explotación de propiedad intelectual ajena | Revelación secreto empresa obligado reserva

83

IDENTIFICACIÓN DEL CONTROL | ¿El control mitiga riesgos penales? | Mejora el Modelo de Compliance

#	Nº Con.	Fecha ID	Fuente ID	Grupo de Controles	Nombre del Control	Descripción del control	Propietario del control	Nivel de control (Directivo u operativo)	Modo de control (automático)	Tipo (Preventivo, detectivo reactivo)	Periodicidad	Justificación	Normativa	Registro del control	Documento registro del control	Registro del resultado	Documento registro del resultado	¿Mitiga probabilidad?	¿Mitiga impacto?	Mejora el Modelo de Compliance	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Probabilidad Inherente	Impacto Inherente	Riesgo Inherente	Probabilidad Inherente	Impacto Inherente
																					2	5	10	2	5	10	2	5	10	2	5
1	001	11-sep.-20	Evaluación de riesgos - OEC	Políticas Internas	Codigo de Conducta	Código de Conducta en los negocios con provisión anticorrupción	OEC	Executive	Manual	Preventive	On demand	Legislation	Criminal Code	Yes	Code of Conduct	No	N/A	Sí	Sí	Sí										
1	002	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	Política Anticorrupción	Política Anticorrupción	OEC	Directivos	Manual	Preventivo	Bajo demanda	Normativo	Código penal	Sí	Política Anticorrupción	No	N/A	Sí	No												
1	003	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	Política de Cortesías en los negocios	Política de Cortesías en los negocios	OEC	Directivos	Manual	Preventivo	Bajo demanda	Compliance & Ética	N/A	Sí	Política de Cortesías en los	Sí	Plataforma Cortesías	Sí	No												
1	004	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	Política T&E	Política T&E	RR.HH.	Directivos	Manual	Preventivo	Bajo demanda	Negocio	N/A	Sí	Política T&E	Sí	Ticket/factura	Sí	No												
1	005	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	Política de donaciones en curso	Política de donaciones en curso	Comité de RSC	Directivos	Manual	Preventivo	Bajo demanda	Compliance & Ética	N/A	Sí	Política de donaciones en	Sí	Formulario en curso y Lista	Sí	No												
1	006	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	Procedimiento de diligencia debida en la contratación de proveedores	Procedimiento de diligencia debida en la contratación de proveedores	OEC	Directivos	Manual	Preventivo	Bajo demanda	Compliance & Ética	N/A	Sí	Procedimiento de diligencia debida en	Sí	Formularios, correos y listas	Sí	No												
1	007	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	Revisión gastos	Aprobación de gastos por superior jerárquico	Managers	Operativo	Manual	Reactivo	Bajo demanda	Negocio	N/A	Sí	Política T&E	Sí	Ticket/factura	Sí	No												
1	008	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	Revisión gastos	Supervisión del gasto y la aprobación por RR.HH. Y Contabilidad.	RR.HH/Contabilidad	Operativo	Manual	Reactivo	Bajo demanda	Negocio	N/A	Sí	Política T&E	Sí	Ticket/factura y aprobación	Sí	No												
1	009	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	Procedimiento de tenders en curso.	Procedimiento de tenders en curso.	OEC	Directivos	Manual	Preventivo	Bajo demanda	Compliance & Ética	N/A	Sí	Procedimiento de tenders en curso.	Sí	Formulario en curso	Sí	No												
1	010	11-sep.-20	Evaluación riesgos OEC	Políticas Internas	EthicsLine	Existencia de un canal de denuncias, confidencial y anónimo.	OEC/HR	Directivos	Manual	Reactivo	Bajo demanda	Compliance & Ética	N/A	Sí	Código Ético	Sí	Plataforma Navex	Sí	No												
1	011	11-sep.-20	Evaluación riesgos OEC	Formación	Formación en anticorrupción	Formación en anticorrupción	OEC	Directivos	Manual	Preventivo	Anual	Compliance & Ética	N/A	Sí	Emails	Sí	Plataforma Navex	Sí	No												
1	012	11-sep.-20	Evaluación riesgos OEC	Comunicación	Comunicaciones y newsletters	Comunicaciones y newsletters	OEC	Directivos	Manual	Preventivo	Trimestral	Compliance & Ética	N/A	Sí	Emails	No	No	Sí	No												
1	013	16-sep.-20	Evaluación de riesgos (Sales LQ SQ)	IT	Contraseñas de acceso	Contraseñas y doble identificación para el acceso a ordenadores y sistemas internos																								
1	014	16-sep.-20	Evaluación de riesgos (Sales LQ SQ)	Políticas Internas	Política de Cortesías comerciales	Política de Cortesías comerciales con límties																								
1	015	16-sep.-20	Evaluación de riesgos (Sales LQ SQ)	Políticas Internas	Blackout	Blackouts																								
			Evaluación de riesgos		Contraste residuos	1 Existen controles tanto para controlar la																								

1.1. Evaluación riesgos - grupo | 1.2. Evaluación riesgos - delit | 2. Controles | 3. Matrices | 4. Plan de Acción | AREAS RA --> | Dirección

4.- Políticas y procedimientos

- **¿Qué son las políticas de empresa?**

➢ Son principios, pautas a seguir, formas de pensar y de actuar que emanan de la dirección de la empresa. Gracias a la política de empresa, los empleados disponen de una guía de normas que deben seguir en determinados ámbitos.

- **¿Por qué debemos tener políticas y/o procedimientos?**

➢ Las políticas y procedimientos sirven para mitigar la arbitrariedad y el desvío de poder dentro de las organizaciones.

- **¿Sobre qué áreas se deben realizar políticas y/o procedimientos?**

➢ Principalmente, en aquellos aspectos de la organización en que se produce una disposición de recursos.
➢ Igualmente, aspectos organizativos y de gestión que se consideran relevantes para la organización.
➢ Elementos éticos y signos de identidad de la organización.

- **¿Cómo deben ser las políticas?**

➢ Ser coherentes y claras.
➢ Ser aceptadas y cumplidas por todos los integrantes de la organización.
➢ Ser útiles para encaminar a la empresa hacia sus objetivos.
➢ Gozar del máximo consenso dentro de la empresa.
➢ Deben estar alineadas con la cultura y los valores de la empresa.

Ejemplos de políticas y procedimientos

Económicos

- Política de compras
- Política de homologación de proveedores
- Políticas de gestión de tesorería y de consolidación de la información financiera
- Política de donaciones

Organizativos

- Manual del empleado
- Política de seguridad e higiene en el trabajo
- Protección de datos
- Política de uso de equipos informáticos
- Política para la selección y contratación de empleados
- Otras políticas (bonus, compensaciones, etc.)

Éticos

- Código de Conducta
- Código de Conducta de proveedores
- Manual y procedimientos de PBC/FT
- Políticas anticorrupción
- Conflicto de intereses
- Canal de denuncias
- Procedimiento de investigaciones internas

DISEÑO DE POLÍTICAS Y/O PROCEDIMIENTOS

DISEÑO DE CONTROLES

Identificar

- Descubrir, reconocer y registrar posibles incumplimientos en función del contexto en cada actividad.
- Plus: Identificar situaciones, causas, fuentes de incumplimientos…

Analizar

- Análisis de controles: ¿tratan adecuadamente el riesgo? ¿funcionan de la manera prevista? ¿pueden demostrar que son eficaces?
- Plus: Estimar probabilidad y gravedad de las consecuencias (impacto), considerando escenarios, controles, etc.

Valorar

- Nivel riesgo vs. apetito riesgo.
- Estrategia de respuesta en cada riesgo.

¡Muchas gracias!

Fundación Pro Bono España

CENTRO DE ESTUDIOS GARRIGUES

Fundación Nemesio Diez

DLA PIPER