APUNTES 03

LEGISLACIÓN PARA EL CUMPLIMIENTO DE LA RESPONSABILIDAD PENAL

NORMATIVA DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

Legislación para el cumplimiento de la responsabilidad penal.

- A lo largo de esta unidad van a desarrollar competencias sobre el desarrollo y generación de sistemas de compliance penal y anti soborno, principalmente serán:
- Identificar riesgos penales para una organización.
- Implantación de medidas de eliminación o minimización de riesgos penales.
- Desarrollo de sistemas de gestión penal de acuerdo don la legislación y la normativa vigente.
- Desarrollo de los principios básicos de las organizaciones para compartir el soborno y promover una cultura empresarial ética.

En esta unidad se van a desarrollar los siguientes contenidos:

1. Riesgos penales que afectan a la organización.
2. Sistemas de gestión de Compliance penal.
3. Sistemas de gestión anticorrupción.

1.- CUMPLIMIENTO DE LA RESPONSABILIDAD PENAL.

Caso práctico

La organización está inmersa en un proceso de crecimiento exponencial, por este motivo, el nivel de control de la dirección en los distintos empleados y en el nivel medio de gestores de departamento ha disminuido. Ante esta situación, y teniendo en cuenta el riesgo asociado a las sanciones penales que pueda sufrir la empresa, han decidido llevar a cabo un análisis de los posibles delitos en los que puede incurrir la empresa, así como una manera de gestionarlos. Uno de los principales riesgos identificados esta relacionado con la corrupción y el soborno. Teniendo en cuenta esta situación, la organización está analizando el despliegue de un sistema de gestión de compliance penal, así como otro sistema de gestión complementario para los riesgos relacionados con el soborno y la corrupción.

- **Riesgos penales que afectan a una organización.**

Los riesgos penales en las organizaciones surgen como consecuencia del incumplimiento de las leyes aplicables. Una ley se define como una norma jurídica dictada por un legislador, en que se obliga o prohíbe algo en consonancia con la justicia y cuyo incumplimiento conlleva una sanción.

Las posibles sanciones que pueda recibir una organización en relación al cumplimiento legal, son riesgos que deben ser tenidos en cuenta para alimentar los sistemas de gestión de cumplimiento, y uno de los conceptos iniciales necesarios es el conocimiento de las leyes aplicables.

El Riesgo penal está relacionado con el desarrollo de conductas que pueden ser constitutivas de delito según el régimen de responsabilidad de las personas jurídicas definido en el Código Penal Español.

- **Principales leyes de afectación a las tecnologías de información en España.**

El Reglamento General de Protección de Datos (RGPD, o GDPR por sus siglas en inglés) y la Ley Orgánica de Protección de Datos (LOPD). Son las dos principales normas que velan por la privacidad de los datos personales. Todas las empresas deben tenerlas en cuenta y cumplirlas escrupulosamente. Serán explicadas detenidamente en los siguientes temas.

Ley de Propiedad Intelectual (LPI). Protege las creaciones originales, en cualquier formato y medio: grabaciones, emisiones de radio, etc. Debe tenerse en cuenta, no obstante, que no incluye ideas, procesos ni conceptos de matemáticas.

Leyes de Propiedad Industrial. Similares a la anterior, pero, en este caso, destinadas a la protección de diseños industriales, marcas, nombres comerciales, patentes, etc. Son varias normativas diferentes: de marcas, de patentes…

Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE). Regula todos los intercambios comerciales realizados a través de Internet, estableciendo los requisitos que debe cumplir cualquier comercio online.

Reglamento Europeo de Identificación Electrónica y Servicios de Confianza en el Mercado Interior (eIDAS). Tiene como objetivo reforzar la seguridad y la confianza de las transacciones electrónicas realizadas dentro del marco del Mercado Único Digital Europeo.

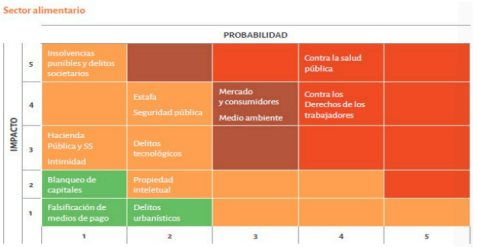
- **Identificación de riesgos penales.**

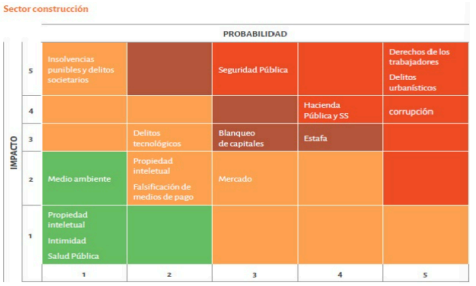
Los posibles delitos y sanciones que puede recibir una organización, están estipulados en el código penal, consultable en el BOE a través de su página web.

En el código penal, se enumeran los posibles delitos que pueden ser cometidos por una organización:

- ➢ Tráfico ilegal de órganos.
- ➢ Trata de seres humanos.
- ➢ Delitos relativos a la prostitución y corrupción de menores.
- ➢ Delitos contra la intimidad, allanamiento informático y otros delitos informáticos.
- ➢ Estafas y fraudes.
- ➢ Frustración a la ejecución.
- ➢ Insolvencias punibles.
- ➢ Daños informáticos.
- ➢ Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores.
- ➢ Blanqueo de capitales.
- ➢ Financiación ilegal de partidos políticos.
- ➢ Cohecho.

- ➢ Delitos contra la Hacienda Pública y la Seguridad Social.
- ➢ Delitos contra los derechos de ciudadanos extranjeros.
- ➢ Delitos de construcción, edificación o urbanización ilegal.
- ➢ Delitos contra el medio ambiente.
- ➢ Delitos relativos a la energía nuclear y a las radiaciones ionizantes.
- ➢ Delitos de riesgo provocado por explosivos.
- ➢ Delitos contra la salud pública.
- ➢ Falsedad de moneda.
- ➢ Falsedad en medios de pago.
- ➢ Tráfico de influencias.
- ➢ Corrupción de funcionario extranjero.
- ➢ Provocación a la discriminación, odio y la violencia.
- ➢ Financiación del terrorismo.
- ➢ Contrabando.
- ➢ Relativos a la manipulación genética.
- ➢ Alteración de precios en concursos y subastas públicas.
- ➢ Negativas a actuaciones inspectoras.
- ➢ Contra los derechos de los trabajadores.
- ➢ Asociación ilícita.
- ➢ Organización y grupos criminales.





Para la identificación de riesgos penales, se ha de tener en cuenta las actividades realizadas por cada área de la organización. Se debe realizar un análisis de riesgos relacionado con los delitos que pueden ser cometidos por cada una de ellas, evaluando los impactos posibles en la organización y teniendo en cuenta la probabilidad de su ocurrencia en función de su negocio.
Así pues, siguiendo los ejercicios realizados en las evaluaciones de riesgo, se pueden identificar por ejemplo los siguientes riesgos penales para una organización en el sector alimentario:
Para el sector de construcción, por ejemplo, se identificarán estos otros riesgos penales por consecución de la siguiente tipología de delitos:

Para saber más: la Confederación Canaria de Empresarios, ha construido dos documentos muy detallados acerca del compliance penal y los riesgos asociados al mismo, es muy recomendable echarle un vistazo a estos documentos ya que amplían la información proporcionada en la unidad con un sentido práctico. Guía de compliance para pymes y Pasos prácticos para la implementación de un sistema de gestión en cumplimiento penal para pymes

1.1.- SISTEMAS DE GESTIÓN DE COMPLIANCE PENAL.

- **Introducción a los sistemas de gestión de compliance penal.**

Un sistema de gestión de compliance penal se trata de un conjunto de elementos de una organización elaborados para concretar y medir el nivel de consecución de objetivos en materia de cumplimiento de la legislación vigente, así como las políticas, procesos y procedimientos para lograr dichos objetivos, reduciendo en consecuencia los riesgos penales de una organización.
Como en el caso del compliance, existe una norma similar para la construcción de un sistema de gestión de riesgos penales, sin embargo, esta es una norma específica para España. Se trata de la UNE 19601.
La norma UNE 19601 desarrolla las guías para la construcción de un sistema de gestión de riesgos penal. Es específica y adaptada al código penal español, sigue la misma estructura de sistemas de gestión que cualquier norma ISO y es certificable.
La certificación de un sistema de gestión implica una declaración pública de una entidad de certificación en la que se afirma que la organización ha implantado y está operando un sistema de gestión según lo definido en la norma ISO/UNE oportuna.
Su objetivo es definir unas directrices que permitan prevenir y reducir los riesgos penales en las organizaciones y generar una cultura ética y respetuosa con la ley, como respuesta a la Ley Orgánica 1/2015 que establece las reformas del código penal y limita en su artículo 31b, la responsabilidad penal de las personas jurídicas en determinadas ocasiones, siempre y cuando estas cuenten con un sistema de gestión de riesgos penales.
A diferencia de la ISO 37301, la UNE 19601 está enfocada en riesgos penales mientras que la ISO hace referencia al cumplimiento en general.
Son varios los beneficios de la existencia de un sistema de gestión de compliance penal en la organización, entre ellos destacan:

1. La demostración de los esfuerzos y compromiso de la dirección por el cumplimiento legal.
2. Mejorar la imagen de la organización ante todos los elementos con los cuales se relaciona.
3. Mejorar la valoración de la organización ante los reguladores y mitigar las posibles sanciones.
4. Establecer una cultura de cumplimiento normativo entre los integrantes de la organización.
5. Facilitar las relaciones comerciales con terceros que requieran de garantías de cumplimiento legal en sus clientes y proveedores.

- **Sistema de gestión de compliance penal (SGCP) según el estándar UNE 19601**

La elaboración de un sistema de gestión de compliance penal implican el despliegue de una serie de políticas, procedimientos y procesos. A continuación, se repasan los principales puntos requeridos, así como la documentación necesaria y ejemplos relacionados en la elaboración del sistema.
Los principales elementos con los que debe contar un SGCP son:

- ➢ Demostración de liderazgo y cultura de cumplimiento.
- ➢ Designación de recursos.
- ➢ Evaluación de riesgos.
- ➢ Implantación de mecanismos de control.
- ➢ Formación, concienciación y comunicación.
- ➢ Monitorización.
- ➢ Sistema de denuncias.
- ➢ Sistema disciplinario.

No obstante, como cualquier otro Sistema de Gestión, sigue la misma estructura de otros ya explicados, por lo que se van a especificar únicamente los elementos específicos de éste, emplazando a la unidad anterior, donde en los apartados 2.1 y 2.4 se explican detalladamente las implicaciones de cada epígrafe de la norma.

Contexto de la organización
El primer elemento necesario para desarrollar un SGCP es el conocer el contexto en el que funciona la organización, y obtener entendimiento de los objetivos que se buscan al desarrollar el sistema.
Para conocer el contexto de la organización, será necesario desarrollar un documento en el que se dé respuesta a elementos básicos tales como, descripción de la función de la misma, tamaño en empleados, clientes o volumen de negocio, estructura organizativa, ubicaciones físicas, actividades y complejidad de la organización, relación con funcionarios públicos y obligaciones legales, contractuales y profesionales.

Elementos de contexto interno a tener en cuenta:

- ➢ Cultura de la organización.
- ➢ Estructura organizativa y roles de cada función.
- ➢ Normas y objetivos, normas, directrices y modelos adoptados por la organización, misión, visión y valores de la organización.
- ➢ Recursos humanos.
- ➢ Recursos y conocimiento.
- ➢ Recursos financieros tecnológicos y redes.
- ➢ Gobernanza.
- ➢ Necesidades y/o expectativas de partes interesadas internas.

Elementos de contexto externo a tener en cuenta:

- ➢ Factores legales, reglamentarios, económicos, financieros, sociales, culturales, políticos, ambientales o tecnológicos.
- ➢ Niveles de corrupción.
- ➢ Cultura de cumplimiento.
- ➢ Entorno regulatorio.
- ➢ Internalización.
- ➢ Relaciones contractuales y compromisos.
- ➢ Necesidades y/o expectativas de partes interesadas externas.

Asimismo, la organización debe identificar a las partes interesadas o stakeholders de la organización, siendo estas definidas como las personas u organizaciones afectadas o que puedan sentirse afectadas por las actividades y decisiones de una organización. Pueden considerarse como stakeholders interno, por ejemplo, los trabajadores, sindicatos, accionistas, y socios de la empresa. Asimismo, como stakeholders externos, los clientes, proveedores, Administraciones, Organizaciones Gubernamentales, Organizaciones Ciudadanas.
Después, uno de los elementos fundamentales del proceso se basa en identificar los intereses de las partes interesadas con respecto al SGCP, es decir, entender que beneficio quieren obtener en el desarrollo del SGCP.
En este epígrafe también se establecerán elementos como la metodología de gestión de riesgos (habitualmente basada en ISO 31000), así como el establecimiento de los requisitos legales de la organización y su nivel de aversión al riesgo, es decir, que nivel de riesgo considera evitar.

Liderazgo de la organización y cultura de cumplimiento
La siguiente fase del SGCP consiste en demostrar el liderazgo de la organización en términos de gestión de compliance penal, así pues, la norma UNE define los deberes a asumir para demostrar ese liderazgo y compromiso en relación con el sistema de gestión de compliance, como son:

1. El deber de establecer y defender, como uno de los valores fundamentales de la empresa, que las actuaciones de todos los miembros de ésta sean siempre conformes al ordenamiento jurídico, promoviendo una cultura de Compliance adecuada en el seno de la misma.

2. El deber de aprobar la política de Compliance penal de la empresa; lo que exige establecer los objetivos de la misma con la finalidad de lograr resultados específicos de manera eficaz.

3. El deber de adoptar, implementar, mantener y mejorar continuamente un sistema de gestión de Compliance penal idóneo para prevenir y detectar delitos o para reducir de forma significativa el riesgo de su comisión; dotando al mismo de recursos financieros, materiales y humanos adecuados y suficientes para su funcionamiento eficaz.

El órgano de gobierno de la organización debe ser formalizado en un documento que recoja sus principales deberes y responsabilidades en términos de cumplimiento, tales como:

- Implementar y mantener un sistema de compliance penal.
- Dotar al sistema de los recursos necesarios.
- Apoyar y firmar la política de cumplimiento penal de la organización.
- Establecimiento de una cultura de cumplimiento.

Una de las maneras de generar una cultura de cumplimiento de la organización es el establecimiento de un código ético que sirva de directriz comportamental para los integrantes de la organización.
El código ético debe establecer la manera en la que se toman las decisiones en la organización como se relaciona la organización con empleados, accionistas, clientes y proveedores, además de los valores de la organización. El código ético no tiene consecuencias en sanciones para la organización, no obstante, si resulta obligatorio para la organización.
El código ético debe recoger los siguientes elementos:

- El mecanismo por el cual se aprueba y se actualiza el documento.
- La finalidad.
- En ámbito de aplicación.
- Los valores corporativos y los principios de comportamiento.
- Las pautas de conducta.
- El seguimiento, control y sanción.
- La comunicación, difusión, la formación y la evaluación.
- La actualización y aceptación.

Para saber más: a continuación, se presentan ejemplos de organizaciones que han publicado sus códigos éticos: Iberdrola, Elecnor, Deloitte

Designación de recursos
La designación de recursos consiste en determinar y proporcionar los recursos necesarios para la implementación y operación del sistema de gestión de compliance penal. Estos recursos no serán solo financieros, también se deben proporcionar recursos humanos con competencias específicas en compliance y recursos financieros y tecnológicos para la implementación de acciones en el sistema tales como planes de formación, acciones de comunicación y por lo general acciones de reducción de riesgos o consecución de objetivos del sistema.
Como parte de la dotación de los recursos necesarios, el órgano de gobierno debe designar un órgano de compliance penal, que se encargue principalmente de:

- Impulsar y supervisar la implementación y eficacia del sistema de gestión de compliance penal.
- Asegurar de que se proporciona la formación continua.
- Emitir un documento que recoja expresamente las actividades y delitos asociados, si no es recogido dentro de la política de compliance penal.
- Contribuir a la identificación de las obligaciones de compliance penal.
- Colaborar para que las obligaciones de compliance penal se traduzcan en políticas, procedimientos y procesos viables o que se integren en las políticas, procedimientos y procesos existentes.
- Promover la inclusión de las responsabilidades de compliance penal en las descripciones de los puestos de trabajo y en los procesos de gestión de desempeño.
- Poner en marcha un sistema de información y documentación de compliance penal.
- Adoptar e implementar procesos para gestionar la información.
- Establecer indicadores de desempeño de compliance penal, midiéndolo y analizándolo para identificar las acciones correctivas necesarias.
- Identificar y gestionar los riesgos penales, incluidos los relacionados con los socios de negocio.
- Asegurar que el sistema de compliance penal se revisa a intervalos planificados.
- Asegurar que se proporciona a los empleados acceso a los recursos de compliance.
- Proporcionar asesoramiento objetivo a la empresa en materias relacionadas con compliance.

Otro de los elementos requeridos para la evidencia del soporte y compromiso por parte de la dirección es la definición de una política de cumplimiento penal. Esta, será el elemento base del SGCP, en ella se deberán definir las funciones y responsabilidades de todos los integrantes de la organización para vigilar el cumplimiento, así como las medidas de control interno para detectar y prevenir posibles incumplimientos.

Los principales aspectos a incluir en este documento son los siguientes:

- Finalidad de la Política de Compliance Penal.
- Defensa de un sistema de gestión en Compliance Penal.
- Características del sistema de gestión en Compliance Penal.
- Ratificar el compromiso del cumplimiento.
- Situar el cumplimiento normativo penal como parte fundamental de la actividad empresarial.
- Asignar el rol de responsable del cumplimiento.
- Valorar los riesgos asociados a las actividades desarrolladas.
- Definir el plan de acción para mitigar los riesgos.
- Establecer planes de formación.
- Establecer un canal de denuncias dentro de la organización.
- Definir un sistema de auditoría interno.
- Establecer sanciones por incumplimientos.

La política de compliance penal de la organización debe estar publicada para todos los miembros de la misma, así como para todos los terceros relacionados.

Para saber más: no obstante, existen organizaciones que publican sus políticas de gestión de compliance, en las siguientes líneas, se proponen tres ejemplos de políticas publicadas por tres organizaciones de tres sectores distintos:

- Política de compliance penal de Alsa
- Política de compliance penal de Caixa Popular
- Política de cumplimiento penal de la mutualidad de la abogacía

Análisis de riesgo y planificación

El siguiente elemento del SGCP se basa en el análisis de riesgos penales que está soportando la organización. Para ello, se deben considerar los diferentes procesos de negocio de la organización e identificar los posibles riesgos por incumplimiento y los delitos tipificados en el código penal y detallados en la unidad 3.1 sobre riesgos penales.

A continuación, se presenta un ejemplo de posibles delitos sobre una organización que están recogidos en el código penal:

Los delitos han sido identificados en relación a su exposición a las diferentes áreas de negocio dentro de la organización.

Por cada uno de los delitos penales identificado, se ha de evaluar el riesgo asociado.

Para ello utilizaremos la misma metodología explicada en la unidad anterior, evaluando el impacto y la probabilidad de ocurrencia en la organización.

En relación a la medición, se presenta la tabla de impacto:

Y la tabla de probabilidad:

El riesgo esta definido por el producto del impacto por la probabilidad de ocurrencia, siendo en este caso un numero entre el 1 y el 16, si tomamos como ejemplo los valores de las dos tablas anteriores.

Así pues, podemos establecer una referencia automatizada para el tratamiento de riesgos, si asignamos valores a las siguientes opciones de tratamiento:

DELITO PENAL	DIRECCIÓN	GERENCIA	RRHH	FINANZAS	DESARROLLO	GESTIÓN PROYECTOS
Trata de Seres Humanos (177 bis 7 CP)	X	X	X		X	X
Prostitución, explotación de menores y corrupción (189 bis CP)	X	X	X		X	X
Descubrimiento y revelación de Secretos. Protección de Datos (197,197bis, 197ter CP)	X	X	X	X	X	X
Estafas y Defraudaciones. (251 CP)	X	X	X	X	X	X
Daños informáticos. (264 quater CP)	X	X				
Relativos a la Propiedad Intelectual, industrial, al mercado y a los consumidores. (270,271,273,274,275,276,283,285 286 CP)	X	X			X	X
Corrupción en los Negocios y financiación ilegal de los Partidos Políticos. (277,278,279,280,281 y 282 CP)	X	X		X	X	
Delitos Societarios. (290 a 297 CP)	X	X		X	X	
Receptación y Blanqueo de Capitales. Financiación al Terrorismo. (301 y 302 CP)	X	X		X	X	X
Contra la hacienda Pública y la Seguridad Social. (310 bis CP)	X	X	X	X	X	X
Contra los Derechos de los trabajadores. (318 CP)	X	X	X		X	X
Contra los Recursos naturales y el Medio Ambiente. (328 CP)	X	X			X	X
Contra el Ejercicio de los Derechos Fundamentales y Libertades Públicas. (510 bis CP)	X	X	X		X	X
Riesgos provocados por Explosivos y Otros agentes. (348.3 CP)	X	X			X	X
Cohecho. (427 bis CP)	X	X	X	X	X	X
Tráfico de Influencias. (430 CP)	X	X	X	X	X	X

CONSECUENCIAS	CRITERIO	VALOR (C)
INSIGNIFICANTES	La repercusión de la materialización del riesgo (sanciones, reputación de la organización, etc) no representa ningún impacto significativo (sanciones, reputación para la organización, etc) para la organización	1
BAJAS	Si bien la repercusión de la materialización del riesgo del incumplimiento representa un perjuicio para la organización, el impacto (sanciones, reputación, etc) es asumible por esta.	2
MODERADAS	La repercusión de la materialización del incumplimiento representa un perjuicio que pone en riesgo la supervivencia y/o continuidad de la organización	3
INTOLERABLES	La repercusión de la materialización de incumplimiento impediría la continuidad de la organización.	4

EXPOSICIÓN	DEFINICIÓN	VALOR (E
BALADI	La actividad que puede dar lugar al incumplimiento en principio no tiene porqué realizarse en su funcionamiento habitual	1
BAJAS	La actividad que puede dar lugar al incumplimiento se realiza de forma ocasional (por ejemplo: alguna vez al año)	2
MEDIA	La actividad que puede dar lugar al incumplimiento se realiza de forma irregular (por ejemplo: alguna vez al trimestre)	3
ALTA	La actividad que puede dar lugar al incumplimiento se realiza de forma frecuente (por ejemplo: alguna vez al mes)	4

TRIVIAL (T)	No se requiere acción específica
TOLERABLE (TO)	No se necesita mejorar los controles existentes salvo que el coste se reducido. Se requieren comprobaciones periódicas para asegurar que se mantiene la eficacia de las medidas de control
MODERADO (M)	Se deben hacer esfuerzos para reducir el riesgo, determinando los controles. Las medidas para reducir el riesgo deben implantarse en un periodo determinado
IMPORTANTE (I)	Se deben hace esfuerzos para reducir el riesgo, determinando los controles. Deben implantarse en un tiempo inferior al de los riesgos moderados.
INTOLERABLE (IN)	Debería paralizarse la actuación que genera el factor del riesgo hasta el establecimiento de los controles.

Tomando el ejemplo, podemos hacer una referencia estableciendo valores horquilla:

- Entre los valores 1 y 4 la opción referencia será trivial (T)
- Entre los valores 5 a 8 la opción de referencia será tolerable (TO)
- Entre los valores 9 a 11 la opción de referencia será moderado (M)
- Entre los valores 12 a 14 la opción de referencia será importante (I)
- Entre los valores 15 y 16 la opción de reverencia será intolerable (IN)

Y en función a esta clasificación se establecerá entonces la opción preferida de tratamiento, como hemos visto en la unidad anterior, consiste principalmente en Aceptar, Mitigar, Evitar/Eliminar o Transferir el riesgo.

Los planes de acción resultantes del SGCP darán respuesta a los riesgos identificados, no obstante, a la hora de diseñarlos, también se deben tener en cuenta los objetivos de la organización, que deben estar alineados con los requisitos establecidos por las partes interesadas en el epígrafe de contexto de la organización y ser medibles, seguibles y comunicados.

Medidas para reducir o mitigar el riesgo penal

La organización puede establecer controles para mitigar el riesgo penal, la norma UNE 19601 establece grupos de controles como pueden ser controles financieros y controles no financieros. A continuación, se presenta un listado de medidas preventivas que permiten reducir los riesgos penales:

- Construcción de un sistema de gestión de riesgo penal.
- Definición de políticas de cumplimiento penal.
- Establecimiento de procesos de diligencia debida con terceros.

- Incentivos y medidas disciplinarias con empleados.
- Proporcionar formación, comunicación y concienciación a los empleados.
- Despliegue de un canal de denuncias.
- Ejecución de auditorías internas y externas de cumplimiento.
- Delimitación de puestos de trabajo y funciones dentro de la organización.
- Existencia de políticas de segregación de funciones.
- Aprobación de transacciones por diferentes integrantes de la organización.

Formación y comunicación en compliance

Uno de los elementos principales del sistema de gestión es la formación y comunicación en compliance. La organización debe establecer un plan formativo para que todos los integrantes de la misma sean conscientes de sus funciones y obligaciones y riesgos existentes en la organización con respecto al compliance penal.

Ilustración que muestra una Profesora dando clases

Jerrykimbrel10. Formación (Dominio público)

La formación y comunicación puede ser un elemento más de demostración del liderazgo de los comités de dirección de la organización, dicha formación debiera estar respaldada y promovida por la dirección de la organización.

Con respecto a los contenidos de los planes de formación, existen algunos, que son de obligado cumplimiento como pueden ser el blanqueo de capitales o la financiación del terrorismo, no obstante, un buen programa de formación de compliance penal debe cubrir los siguientes aspectos:

- Obligaciones y riesgos de los integrantes de la organización en relación a la actividad que desempeñan en la organización y su nivel de responsabilidad.
- Cubrir las necesidades de formación de un empleado en su comienzo en la organización para luego realizar actividades formativas recurrentes.
- Establecer puntos de referencia de la organización sobre el cumplimiento penal, es decir, cual es la posición de la organización con respecto al cumplimiento legal.
- Ser relevantes para la función de los empleados, resultando más completos y extensos en aquellos empleados que desempeñen funciones con un mayor nivel de riesgo penal e incluyendo contenido tal como código de conducta ético, gobernanza y gestión del riesgo, responsabilidad económica y penal y prevención penal.
- Adaptarse a modalidades presencial y remota.
- Revisarse y actualizarse periódicamente para cubrir nuevos requisitos legales.
- Deben recoger la normativa legal y sectorial más relevante.
- Deben poner a prueba los conocimientos de los integrantes de la organización.
- Deben permitir establecer nuevas acciones formativas en función de los resultados de las pruebas de conocimiento a los integrantes de la organización.
- Deben permitir guardar el registro de las acciones formativas realizadas por cada empleado.

Además del plan de formación, se debe establecer una estrategia de comunicación para todos los elementos relacionados con el sistema de gestión del compliance penal. El plan de comunicación debe incluir elementos como:

- Contenido de la comunicación (que se debe comunicar).
- Cuando se debe comunicar (ante que eventos, o con qué frecuencia).
- Receptor del mensaje (a que personas, colectivos o entidades va destinado el mensaje).
- Canal (presencial, mail, teléfono, nota de prensa…).
- Origen de la comunicación (que persona, departamento o rol dentro de la organización debe enviar la comunicación).
- Registro lingüístico de la comunicación (formal, informal, técnico o no).

Monitorización del funcionamiento del sistema de gestión de compliance

El sistema de gestión de compliance penal debe ser revisado, supervisado y monitorizado durante su operación, para modificarlo y actualizarlo en caso de ser necesario.

En línea con la definición de sistema de gestión, la consecuencia del despliegue del mismo es el establecimiento de políticas, procedimientos y procesos en la organización.

Cualquier información sobre las iniciativas y procesos existentes son útiles para su seguimiento es utilizada para su monitorización. La supervisión de esta información es una de las funciones del órgano de supervisión de compliance.

Los procesos desplegados pueden ser monitorizados a través del establecimiento de métricas que permitan determinar su evolución y correcto funcionamiento. A continuación, se presentan una serie de ejemplos sobre posibles métricas de compliance penal a generar en una organización:

- Número y tipo de denuncias.
- Número y tipo de delitos confirmados.
- Modificaciones introducidas en los controles.
- Análisis de los factores internos y externos.Imagen de reglas
- Arielrobin (Dominio público)
- Acciones de información y formación.
- Análisis de los planes de acción.
- Objetivos cumplidos y los pendientes de cumplir.
- Número y tipo de denuncias.

- Número y tipo de delitos confirmados.
- Modificaciones introducidas en los controles.
- Análisis de los factores internos y externos.
- Acciones de información y formación.
- Análisis y creación de nuevos planes de acción para el año siguiente.
- Objetivos cumplidos y los pendientes de cumplir.
- Objetivos cumplidos.
- Evaluación del Manual de Compliance.
- Debilidades detectadas en el Manual de Compliance.
- Propuestas de acciones informativas y de formación en materia de cumplimiento normativo.
- Departamentos con más riesgo.
- Medidas disciplinarias aplicadas.
- Incumplimiento código ético

Con respecto a las iniciativas dentro del sistema de gestión de compliance, habrá que hacer un seguimiento de su estado, recursos financieros y tiempo invertido, y elementos pendientes. En función al estado de los mismos se tomarán decisiones, por ejemplo, sobre la apertura de nuevas iniciativas o bien sobre la priorización de las iniciativas en curso para su cierre, que influye en el estado del sistema de gestión.

Otro de los elementos específicos de la norma es la habilitación de un canal de denuncias para la comunicación de actividades sospechosas dentro de la organización, que puedan ser notificadas de manera anónima por los integrantes de la organización, y sean susceptibles de ser investigadas por el órgano de supervisión de compliance corporativo. Este canal de denuncias debe cumplir con los siguientes requisitos:

- Estar disponible tanto para los componentes internos de la organización como para entes externos a ella (personal subcontratado, proveedores, clientes…).
- Permitir la comunicación manteniendo el anonimato del denunciante.
- Evitar represalias de los individuos que utilicen el canal de denuncias.
- Facilitar el asesoramiento ante cualquier persona que utilice el canal de denuncias para dudas sobre el cumplimiento relacionadas con cualquier actividad.
- Se debe garantizar que los miembros de la organización conocen los canales de denuncias habilitados, además, se debe fomentar su uso.

Por último, como elemento diferenciador de los SGCP, se debe contar con un régimen sancionador informado a los integrantes de la organización en el que se puedan determinar las consecuencias que puede tener un incumplimiento del sistema cuyas consecuencias puedan suponer un riesgo penal para la organización. El régimen sancionador debe contar con los siguientes elementos:

- Clasificación de las sanciones, estableciendo niveles en función de las consecuencias puedan acarrear para la organización, por ejemplo, infracciones leves, graves o muy graves.
- Consecuencias de incurrir en las sanciones anteriores, como, por ejemplo, amonestación verbal para las sanciones breves hasta la suspensión de empleo y sueldo por periodos de tiempo para las sanciones más graves e incluso la rescisión de la relación laboral con el empleado.
- Procedimiento de actuación que incluya todos los pasos para su clasificación, sanción, comunicación y respuesta.

Los epígrafes 9 y 10 hacen referencia a las actividades de auditoria y mejora continua, y no se diferencian en mucho a otros sistemas de gestión como los ya explicados en el tema anterior.

1.2.- SISTEMA DE GESTIÓN ANTISOBORNO Y ANTICORRUPCIÓN.

- **Sistemas de gestión antisoborno y anticorrupción**

Sistemas de gestión antisoborno

El soborno consiste en una oferta, promesa, entrega, aceptación o solicitud de una ventaja indebida de cualquier valor, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o deje de actuar en relación las obligaciones de esa persona.

El soborno es uno de las formas de corrupción más habituales. Las organizaciones deben establecer medidas pasa la prevención del soborno a través de una cultura de integridad, transparencia, cumplimiento y lucha contra la corrupción.

La norma ISO 37001 se ha creado para el desarrollo de guías que permitan prevenir, detectar y gestionar conductas delictivas de soborno, cumpliendo con la legislación. Es una norma certificable.

La norma ISO 37001 vs la norma UNE 19601

La norma ISO 37001 es un sistema de gestión que se entiende como una guía en materia de prevención de la corrupción, siendo este un subconjunto de los posibles delitos en el alcance de la UNE 19601, siendo este un estándar nacional español. La implantación cualquiera de los dos sistemas de gestión no supone en sí mismo un eximente en caso de que la organización incurra en un delito ya sea de soborno, corrupción o cualquiera de los recogidos en el código penal, y que podrían estar ya registrados en el análisis de riesgos de la matriz del sistema de gestión de compliance penal, no obstante, si puede suponer un criterio para la limitación de la responsabilidad de la organización, siempre que se siga y se opere de manera diligente el sistema de gestión.

La ISO 37001 es algo más exigente en materia de corrupción y delitos anti soborno que la UNE 19601, no obstante, si la organización ya dispone de un sistema de gestión basado en la UNE, será suficiente con revisar las políticas, protocolos y controles establecidos para adaptarlos al delito de soborno.
Para ello, los principales pasos deberían ser:

1. Modificar el mapa de riesgos de la organización para incluir los riesgos de soborno y corrupción.
2. Revisar el alcance del sistema de gestión para verificar que se mantiene igual o se incluyen nuevas líneas de negocio expuestas a riesgos de soborno y corrupción.
3. Generación de la documentación que evidencie la gestión del riesgo de soborno y los objetivos para desarrollar e implementar un sistema anti soborno, siendo estos, por ejemplo, políticas antisoborno, (cuyo contenido puede ser añadido a la política de compliance penal), asignación de recursos específicos para las iniciativas anti corrupción y soborno.
4. Revisar las partes interesadas y evaluar si se mantienen con respecto al sistema de gestión de compliance penal o se incluyen nuevos actores tales como socios, proveedores, clientes o entes del sector público que permitan obtener licencias o participar en concursos.
5. Definir procesos de debida diligencia para los socios y entidades relacionadas que incluyan elementos de control anti corrupción y soborno tales como códigos éticos, controles financieros (aprobación de pagos, limitación de efectivo, mancomunidad, justificación de pagos...); control de pagos; control de regalos recibidos (crear bolsa común y reparto o sorteo entre los empleados).

Sistemas de gestión antisoborno con ISO 37001
Los requisitos documentales de la norma ISO 37001 son los siguientes:

- Existencia de una política antisoborno que prohíba el soborno.
- La expresión de liderazgo, compromiso y responsabilidad.
- Comunicación de la política a los empleados, los socios comerciales y otras partes interesadas.
- Nombramiento de un responsable para supervisar el programa.
- Controles de personal y formación.
- Evaluaciones periódicas del riesgo de soborno al que está expuesta la organización.
- Evaluaciones de debida diligencia en proyectos, socios comerciales y proveedores.
- Implementación de controles antisoborno.
- Implementación de controles financieros y no financieros apropiados para prevenir el riesgo de soborno.
- Informes, monitorización, investigación y auditoría.
- Acción correctiva y mejora continua.

Controles antisoborno:
Debida diligencia: proceso para evaluar con mayor detalle la naturaleza y alcance del riesgo de soborno y ayudar a las organizaciones a tomar decisiones en relación con transacciones, proyectos, actividades, socios de negocios y personal específicos.
Ejemplos: Análisis de conducta de terceros, análisis de reputación, antecedentes…
Control Financiero: para gestionar sus transacciones financieras correctamente y para registrar estas transacciones con precisión, de forma completa y de manera oportuna.
Ejemplos: Aprobaciones de transacciones en función de su volumen, segregación de funciones, rotación de personal.
Control No Financiero: para ayudar a asegurar que los aspectos comerciales, los relativos a las compras, operaciones y otros aspectos no financieros, relacionados con sus actividades, se gestionan de forma apropiada.
Ejemplos: Publicación de licitaciones, evaluación por varias personas, formación anticorrupción.
Control de Regalos, atenciones, donaciones y beneficios similares: Existencia de políticas de aceptación de regalos o similares. Registro de regalos recibidos, establecimiento de límites, cuantías… Control de regalos recibidos (crear bolsa común y reparto o sorteo entre los empleados).
Proceso de Contratación de personal: Investigación de antecedentes si fuera posible durante la contratación del personal, comunicación de las políticas de soborno, formación y concienciación.

A continuación, se proponen dos ejemplos de manuales de sistemas de gestión antisoborno:

- Política antisoborno de T-Systems México: T-Systems México
- Portal Antisoborno del Programa nacional de infraestructura educativa de Perú, con información detallada del sistema de gestión antisoborno: Acceso

Autoevaluación I

Acme cuenta con un total de 50 MHz de espectro de señal adquirida para las comunicaciones de los teléfonos móviles de sus clientes. Cuanto más baja sea la frecuencia de la señal, más penetración tiene en los edificios, por lo que están pensando utilizar 2 MHz no adquiridos por la franja inferior, que saben que hoy en día no están siendo utilizados. Las auditorías de radiofrecuencias no suelen ser muy habituales, pero si se hace al menos una vez al año.
Las sanciones que puede ocasionar esta situación pueden ser muy graves e incluso implicar la retirada de la licencia de operador de telecomunicaciones. Teniendo en cuenta esta situación ¿Qué decisión sería la más razonable?

a) Asumir. Solo son 2 MHz, apenas imperceptible y no causa molestia.
b) Eliminar. Se limitarán a emitir en las frecuencias adquiridas. Mitigar.
c) Se limitarán a emitir unicamente 1 MHz fuera de las frecuencias adquiridas.

TEST I:

1- La regulación que protege las creaciones originales, en cualquier formato y medio es:
a) LPI.
b) LSSI-CE.
c) RGPD.
d) Reglamento eIDAS.

2- ¿Cuál de los siguientes forma parte del contexto interno de una empresa?
a) Situación financiera de su área de actuación.
b) Legislación aplicable y el entorno regulatorio.
c) Relaciones contractuales.
d) Cultura de la organización.

3- La norma ISO 37001 es certificable. ¿Verdadero o falso?
a) Verdadero
b) Falso

4- El régimen sancionador debe...
a) Establecer a que finalidad se dedicará el dinero de las sanciones.
b) Ser utilizado al menos con carácter anual.
c) Publicar la información de los empleados sancionados.
d) Establecer las consecuencias de un incumplimiento.

5- Una de las maneras de generar una cultura de cumplimiento de la organización es el establecimiento de un código ético que sirva de directriz comportamental para los integrantes de la organización. ¿Verdadero o falso?
a) Verdadero
b) Falso

6- Los posibles delitos y sanciones que puede recibir una organización, están estipulados en la constitución, consultable en el BOE. ¿Verdadero o falso?
a) Verdadero
b) Falso

7- ¿Cuál de las siguientes normas ISO es relativa a la gestión antisoborno?
a) ISO 37301
b) UNE 19601
c) ISO 37001
d) ISO 19601

8- Un sistema de gestión de compliance penal basado en la UNE 19601 puede utilizar un análisis de riesgos basado en la ISO 31000. ¿Verdadero o falso?
a) Verdadero
b) Falso

9- La mejor manera de demostrar el liderazgo y la cultura de cumplimiento en una organización es:
a) Participando en las consultas públicas para la creación de leyes.
b) Invirtiendo en software de cumplimiento.
c) Teniendo una buena relación con las fuerzas y cuerpos de seguridad del estado.
d) Firmando, aprobando y promoviendo una política de compliance penal en la empresa.

10- El Riesgo penal está relacionado con el desarrollo de conductas que pueden ser constitutivas de delito según el régimen de responsabilidad de las personas jurídicas definido en el Código Penal Español.
a) Verdadero
b) Falso

Respuestas
Autoevaluación I: b)
TEST I 9/10: 1 a), 2 d), 3 a), 4 d), 5 a), 6 a), 7 c), 8 a), 9 d), 10 a)

Caso práctico

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.
ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.
ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.
Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO27001 en los servicios de comunicaciones.
La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.
Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.
La dirección de la organización es consciente de que es sujeto obligado para multitud de leyes y normativas. Tras el sistema de gestión de compliance desarrollado en semanas anteriores, ahora la preocupación esta enfocada en los riesgos penales, ya que uno de los principales competidores se ha visto envuelto en un escándalo de escuchas y ha sido objeto de sanciones penales considerables.
Teniendo en cuenta la compañía descrita en el escenario anterior, da respuesta a las siguientes preguntas:

Apartado 1: Cumplimiento de la responsabilidad penal.
¿Podrías identificar 10 delitos en los que pueda incurrir ACME?

1. Estafa y fraude, en caso de que la empresa prometa un servicio que no cumpla, engañando al cliente (por ejemplo, a través de publicidad engañosa).
2. Cohecho: ofrecer sobornos a funcionarios públicos para obtener contratos o ventajas.
3. Delitos contra la Hacienda Pública y la Seguridad Social: no pagar los impuestos correspondientes o falsificar cuentas.
4. Insolvencias punibles: ocultar activos o realizar operaciones fraudulentas para evitar pagar.
5. Blanqueo de capitales: participar en actividades para ocultar el origen ilegal de fondos.
6. Delitos contra los derechos de los trabajadores: no cumplir con las normativas laborales, como el pago de salarios o la seguridad en el trabajo.
7. Tráfico de influencias: utilizar la posición de la empresa para influir en decisiones de funcionarios públicos.
8. Delitos contra la intimidad, allanamiento y otros delitos informáticos: interceptar o escuchar comunicaciones privadas sin autorización (importante al trabajar con embajadas).
9. Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores: Utilizar tecnología o software sin licencia adecuada, podría considerarse una negligencia en la seguridad.
10. Delitos contra el medio ambiente: No gestionar adecuadamente los residuos o contaminar el entorno.

¿Podrías elaborar una matriz de riesgo penal de la organización?

Probabilidad / Impacto	1	2	3	4	5
5		Cohecho Blanqueo capitales		Delitos contra intimidad	
4		Delitos contra Hacienda Pública Insolvencias punibles	Delito contra trabajadores Tráfico de influencias	Estafa y fraude Delito contra propiedad intelectual	
3	Delito contra medio ambiente				
2					
1					

Dado el tipo de empresa que es ACME SA, es probable que ya tenga implantadas las medidas necesarias para que la probabilidad de estos delitos se mantenga en niveles moderados. Por eso, algunos de los delitos tienen una probabilidad moderada de ocurrir, su impacto en la empresa sería alto debido a las graves consecuencias legales y reputacionales.

- Estafa y fraude

Probabilidad: Alta (4) la empresa maneja una gran cantidad de clientes y servicios, lo que aumenta el riesgo de promesas incumplidas o publicidad engañosa.

Impacto: Alto (4) las consecuencias pueden incluir sanciones legales, pérdida de reputación y confianza del cliente pero no necesariamente devastadoras.

- Cohecho

Probabilidad: Media (2) aunque es menos probable, la obtención de contratos con embajadas y multinacionales puede llevar a intentos de soborno.

Impacto: Alto (5) las sanciones por cohecho son severas y pueden incluir multas significativas y penas de prisión, además de dañar gravemente la reputación de la empresa.

- Delitos contra la Hacienda Pública y la Seguridad Social

Probabilidad: Baja (2) la empresa debe cumplir con numerosas obligaciones fiscales y aunque es menos probable, cualquier incumplimiento podría ocurrir.

Impacto: Alto (4) las consecuencias de no pagar impuestos o falsificar cuentas pueden incluir multas, sanciones legales y daños en la reputación.

- Insolvencias punibles

Probabilidad: Baja (2) la ocultación de activos u operaciones fraudulentas para evitar pagos es un riesgo, aunque menos probable.

Impacto: Alto (4) las consecuencias son graves, suponiendo sanciones legales y pérdida de credibilidad ante los inversores y clientes.

- Blanqueo de capitales

Probabilidad: Bajo (2) aunque es poco probable, la empresa podría ser utilizada para ocultar fondos ilegales debido a su presencia internacional.

Impacto: Muy alto (5) las sanciones que corresponden al blanqueo de capitales son severas y pueden incluir multas significativas y penas de prisión.

- Delitos contra los derechos de los trabajadores

Probabilidad: Media (3) con una gran cantidad de empleados y posibles subcontratados, el riesgo de incumplimientos laborales es significativo.

Impacto: Alto (4) las consecuencias pueden incluir multas, sanciones y daños reputacionales, además afectar a la moral de los empleados.

- Tráfico de influencias

Probabilidad: Media (3) la empresa podría utilizar su posición para influir en decisiones de funcionarios públicos.

Impacto: Alto (4) las sanciones por este tipo de delito pueden ser severas y dañar la reputación de la empresa.

- Delitos contra la intimidad, allanamiento y otros delitos informáticos

Probabilidad: Alta (4) trabajando con embajadas y multinacionales, la interceptación de comunicaciones privadas sin autorización es un riesgo significativo.

Impacto: Muy alto (5) las consecuencias pueden ser devastadoras, incluyendo sanciones legales, pérdida de confianza y daños en la reputación de la empresa

- Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores

Probabilidad: Alto (4) el uso de tecnologías sin licencia adecuada o la seguridad necesaria, puede ocurrir, sobre todo en entornos tecnológicos avanzados.

Impacto: Alto (4) las consecuencias pueden incluir multas, sanciones y puede desembocar en posibles ciberataques y pérdida de datos, especialmente al trabajar con embajadas y organismos importantes.

- Delito contra el medio ambiente

Probabilidad: Media (1) la empresa tiene prácticas sostenibles, pero siempre existe el riesgo de incumplimientos ambientales.

Impacto: Medio (3) las consecuencias pueden incluir multas y sanciones, aunque el impacto será menor en comparación con otros delitos.

Aunque la probabilidad de que ocurran alguno de estos delitos sea moderada. ACME S.A. debe continuar fortaleciendo las medidas preventivas para mitigar los riesgos y proteger su reputación y estabilidad en el mercado.

Apartado 2: Sistema de gestión de compliance penal. Propón al menos una acción mitigante por cada riesgo identificado.

1. Estafa y fraude

Implementar controles internos rigurosos y auditorías periódicas para asegurar que los servicios prometidos se cumplan y que la publicidad sea acorde con lo que ofrece la empresa. Además, añadir un buzón de denuncias para que empleados y clientes reporten las irregularidades.

2. Cohecho

Desarrollar un código ético y de conducta que prohíba este tipo de acciones (sobornos). Realizar conferencias sobre ética y cumplimiento, para que los empleados se conciencien sobre el tema.

3. Delitos contra la Hacienda Pública y la Seguridad Social

Implementar un sistema de gestión fiscal que asegure el cumplimiento de las obligaciones tributarias y de seguridad social. Realizar auditorías fiscales internas y externas periódicamente.

4. Insolvencias punibles

Mantener una contabilidad transparente y precisa. realizar auditorías financieras regulares y establecer políticas claras para la gestión de ingresos (activos y pasivos).

5. Blanqueo de capitales

Implementar un programa de cumplimiento para evitar el lavado de dinero que incluya el debido cuidado del cliente (KYC: Know your customer), monitorear las transacciones y reportar las actividades sospechosas

6. Delitos contra los derechos de los trabajadores

Asegurar el cumplimiento de todas las normativas laborales mediante auditorías regulares y hacer a los empleados conscientes de sus derechos laborales. Establecer un buzón de denuncias para que puedan reportar violaciones de sus derechos.

7. Tráfico de influencias

Implementar políticas de transparencia en los procesos de contratación y toma de decisiones. Realizar capacitaciones sobre ética y conflictos de interés para los empleados.

8. Delitos contra la intimidad, allanamiento y otros delitos informáticos

Implementar medidas de seguridad cibernética, incluyendo encriptación de datos y monitoreo de redes. Enseñar a los usuarios sobre protección de datos y privacidad.

9. Delitos contra la propiedad intelectual e industrial, el mercado y los consumidores

Asegurar que todos los softwares y tecnologías utilizadas estén debidamente licenciados, realizar auditorías de cumplimiento y de seguridad, capacitar a los empleados sobre la importancia de respetar la propiedad intelectual para evitar este delito.

10. Delitos contra el medio ambiente

Implementar un sistema de gestión ambiental que incluya la evaluación del impacto ambiental de la empresa, la gestión adecuada de residuos. Realizar auditorías ambientales para hacer un seguimiento.

Apartado 3: Sistema de gestión antisoborno y anticorrupción.

Identifica al menos 3 riesgos en el entorno de ACME relacionados con el soborno y la corrupción.

- Sobornos para obtener contratos gubernamentales, ACME podría verse tentada a ofrecer sobornos a funcionarios públicos para asegurar contratos lucrativos, especialmente al trabajar con embajadas y organismos gubernamentales. Un ejemplo podría ser ofrecer pagos a funcionarios para ganar contratos de telecomunicaciones con embajadas.

La obtención de contratos gubernamentales es altamente competitiva y lucrativa, lo que puede incentivar prácticas corruptas para asegurar estos contratos.

- Corrupción a través de intermediarios, los intermediarios o agentes contratados por ACME podrían involucrarse en prácticas corruptas, como pagar sobornos en nombre de la empresa para obtener algún tipo de ventaja comercial.

El uso de intermediarios puede dificultar el control directo de las prácticas comerciales, aumentando el riesgo de corrupción.

- Fondos de soborno ocultos, la creación de fondos de soborno que no están registrados (cajas negras) para financiar sobornos y pagos indebidos a empleados de otras empresas o funcionarios.

La existencia de fondos no registrados facilita la realización de pagos corruptos sin ser detectados por los controles internos.

- Pagos o regalos para la facilitación, ofrecer favores, regalos, pagos u hospitalidad a clientes o funcionarios para acelerar o influir en sus decisiones y procesos administrativos.

Los pagos de facilitación son una forma común de corrupción que puede ser difícil de detectar pero que puede tener graves consecuencias legales y reputacionales.

Estos riesgos pueden tener graves consecuencias legales y reputacionales para la organización. Es crucial que la empresa implante un sistema de gestión antisoborno y anticorrupción robusto.