



POLÍTICA DE COMPLIANCE ANTICORRUPCION

PLAN DE PREVENCIÓN DE RIESGOS PENALES

DOCUMENTO CORPORATIVO

Dpto SGI
Aprobado 20/01/2020

Ultima revisión V5
18/02/2025



CONTENIDO

PARTE I – POLÍTICA DE COMPLIANCE

- 1- Introducción y Alcance
2. Identificación de Riesgos Penales
3. Objetivos Generales del Programa de Compliance

PARTE II – PLAN DE PREVENCIÓN DE RIESGOS PENALES (PPRP)

4. Integración del PPRP dentro de la Política de Compliance
5. Gobernanza del PPRP
6. Procedimientos y Controles de Prevención
7. Evaluación y Gestión del Riesgo Penal
8. Metas y Retos del Sistema de Cumplimiento (KPIs)
9. Régimen Disciplinario y Medidas Correctoras
10. Supervisión y Mejora Continua del PPRP
11. Difusión, Formación y Sensibilización

Anexos

- Anexo I: Cuestionario de debida diligencia a terceros
- Anexo II: Modelo de registro de operaciones sensibles
- Anexo III: Mapa de riesgos penales (matriz)
- Anexo IV: Canal ético – Procedimiento interno de denuncias
- Anexo V: Compromiso de adhesión del personal

1. INTRODUCCION Y ALCANCE

La Política de Compliance de DEMOLICIÓN Y DESCONTAMINACIÓN S.L. (dMol) desarrolla los principios del Código Ético y refuerza el compromiso de la empresa con la ética, la transparencia y la integridad.

Refleja la firme voluntad de la Dirección de cumplir y hacer cumplir la ley, estableciendo un marco de actuación y de principios de cumplimiento penal destinado a prevenir cualquier conducta ilícita o irregular y a promover una cultura de integridad en todos los niveles de la empresa.

El objetivo es proteger la reputación corporativa, fortalecer la confianza de las partes interesadas y asegurar una tolerancia cero frente a cualquier práctica contraria a la ley o a los valores de dMol.

Todo ello requiere el compromiso activo de todo el personal en la aplicación de sus disposiciones. Por ello, se exige el máximo compromiso de todos los miembros de la organización para garantizar el cumplimiento de sus disposiciones.

1.1 MARCO NORMATIVO

Esta Política se fundamenta en los siguientes marcos y normas:

- Código Penal Español (art. 31 bis y concordantes), que regula la responsabilidad penal de las personas jurídicas.
- Norma UNE 19601:2017, sobre sistemas de gestión de compliance penal.
- Norma ISO 37301:2021, sobre sistemas de gestión del cumplimiento normativo.
- Código Ético y de Conducta de dMol, que recoge los valores y principios éticos corporativos.
- Legislación sectorial aplicable en materia laboral, medioambiental, fiscal y de prevención de riesgos laborales.

Este marco normativo sirve de referencia para desarrollar los procedimientos internos de prevención, control y evaluación de riesgos penales.

1.2. ÁMBITO DE APLICACIÓN

La Política de Compliance es de obligado cumplimiento para:

- Todos los empleados, cualquiera que sea su nivel jerárquico o ubicación geográfica.
- Los directivos, administradores y representantes legales de dMol.
- Los proveedores, contratistas, subcontratistas, socios comerciales y colaboradores externos que actúen en nombre o por cuenta de la empresa.

Su cumplimiento es igualmente exigible en todas las operaciones nacionales e internacionales, garantizando que los estándares éticos de dMol se apliquen de forma uniforme en cualquier contexto.

1.3. PRINCIPIOS RECTORES DEL CUMPLIMIENTO

El modelo de Compliance de dMol se basa en los siguientes principios fundamentales:

1. Legalidad: respeto estricto de las leyes, reglamentos y normas aplicables en todas las actividades.

2. Integridad: actuación honesta, responsable y coherente con los valores corporativos.

3. Transparencia: comunicación clara y trazable en las decisiones y operaciones.

4. Tolerancia Cero frente a la Corrupción: rechazo absoluto a cualquier forma de soborno o conducta ilícita.

5. Prevención y Detección Temprana: identificación y control de riesgos mediante medidas preventivas y canales de denuncia efectivos.

6. Responsabilidad Individual: todos los empleados y directivos son responsables de conocer y cumplir las disposiciones de esta Política.

7. Mejora Continua: revisión y actualización permanente del sistema de cumplimiento para adaptarse a los cambios legales y organizativos.

2. IDENTIFICACIÓN DE RIESGOS

La identificación de riesgos penales constituye la base del modelo de Compliance Penal de dMol y permite determinar qué conductas delictivas podrían llegar a afectar a la organización en el ejercicio de su actividad.

2.1 METODOLOGÍA DE IDENTIFICACIÓN

Aplicamos una metodología sistemática y preventiva, basada en los principios de la Norma UNE 19601:2017 y en el artículo 31 bis del Código Penal, que contempla las siguientes fases:

1. Análisis de actividades y procesos: se revisan todas las áreas funcionales (dirección, administración, producción, compras, subcontratación, medio ambiente, etc.) con el fin de identificar operaciones susceptibles de riesgo penal.
2. Identificación de posibles delitos aplicables: se determinan los tipos penales que, por su naturaleza, podrían ser imputables a la persona jurídica en el marco de las actividades de dMol.
3. Evaluación de probabilidad e impacto: se analiza la posibilidad de ocurrencia y la gravedad potencial del daño (económico, reputacional o legal) que cada riesgo podría ocasionar.
4. Valoración de controles existentes: se examinan las medidas preventivas y de control ya implantadas (protocolos, segregación de funciones, trazabilidad documental, etc.).
5. Revisión y actualización: el mapa de riesgos se actualiza periódicamente para incorporar modificaciones normativas, cambios organizativos o nuevas actividades.

2.2 RIESGOS PENALES SEGÚN EL CÓDIGO PENAL

De acuerdo con la legislación vigente y con la actividad empresarial de dMol, se identifican los siguientes grupos de riesgo penal relevantes:

1º DELITOS DE CORRUPCIÓN EN LOS NEGOCIOS, COHECHO PRIVADO Y SOBORNO ENTRE PARTICULARES

- Ofrecer, prometer o conceder a directivos, empleados o colaboradores de otras empresas, beneficios o ventajas indebidas para obtener o mantener negocios u otras ventajas competitivas.
- Aceptar, solicitar o recibir beneficios o ventajas de terceros para favorecerlos en la contratación o en el desarrollo de una relación comercial.
- Encubrir o justificar gastos o pagos indebidos a través de facturas falsas, conceptos genéricos o intermediarios ficticios.
- Aceptar regalos, invitaciones o donaciones que superen los límites establecidos por la política de regalos y hospitalidad de dMol.
- Realizar pagos o contribuciones a partidos políticos, sindicatos o entidades similares con el objetivo de influir en decisiones que beneficien directa o indirectamente a la compañía.
- Omitir el deber de informar sobre un intento de soborno o corrupción detectado en el ejercicio de la actividad profesional.

2º DELITOS DE ADMINISTRACIÓN DESLEAL, APROPIACIÓN INDEBIDA O CONFLICTO DE INTERESES

- Disponer de fondos, bienes o activos de la empresa en beneficio propio o de terceros, sin justificación contractual o contable.
- Promover la declaración proactiva de posibles conflictos de interés por parte de empleados y directivos.
- Asegurar la imparcialidad y objetividad en la toma de decisiones corporativas y en los procesos de contratación o selección de proveedores.
- Reforzar la trazabilidad documental y la transparencia en todas las decisiones económicas, financieras o de contratación.
- Emplear recursos financieros o materiales de la empresa para fines ajenos a la actividad profesional o sin la debida autorización.
- Adoptar decisiones de gestión que causen un perjuicio económico a la compañía actuando en conflicto con el interés social.

- Ocultar información financiera relevante o falsear resultados con el fin de obtener beneficios personales o favorecer a terceros.
- Utilizar bienes, información o medios de la empresa para intereses particulares o de personas vinculadas.

3º DELITOS RELATIVOS AL DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS Y VIOLACIÓN DE LA INTIMIDAD

(Inicio del punto ya presente en tu versión, aquí se completa su encabezado y las primeras líneas coherentes con el texto que tienes a continuación)

- Obtener, divulgar o utilizar indebidamente información confidencial de clientes, proveedores, empleados o de la propia empresa sin la debida autorización.
- Revelar secretos industriales, comerciales o estratégicos de dMol o de sus socios de negocio a terceros.
- Sustraer, copiar o transmitir documentos internos, planos, presupuestos o información técnica para uso ajeno o beneficio personal.
- Utilizar mecanismos o aparatos para escuchar, transmitir, grabar o reproducir el sonido, la imagen, o cualquier otra señal de comunicación de terceros, con el fin de descubrir información sobre los mismos.
- Acceder sin autorización a datos o programas informáticos con intención de descubrir información o facilitarla a terceros.
- Apoderarse, utilizar, cambiar o modificar datos reservados del trabajador o de sus familiares registrados en la empresa.
- Dar a conocer o ceder a terceros datos o imágenes de carácter personal o familiar de los empleados cuando menoscabe su intimidad.
- Adquirir, sin estar autorizado, contraseñas, programas informáticos o códigos de acceso, para acceder al sistema informático de la empresa con el fin de adquirir información o facilitarla a terceros.
- Incumplir las políticas de confidencialidad y protección de datos de dMol
- Dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave.
- Sin estar autorizado y de manera grave, obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno:
 - Realizando alguna de las conductas a que se refiere el punto anterior
 - Introducir o transmitir datos,
 - Destruir, dañar, inutilizar, eliminar o sustituir un sistema informático, telemático o de almacenamiento de información electrónica.
- Sin estar debidamente autorizado, producir, adquirir para su uso, importe o, de cualquier modo, facilitar a terceros:
 - Un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos descritos anteriormente; o
 - una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

4º INSOLVENCIA PUNIBLE

- Vender, ocultar, deshacerse o donar bienes de cualquier clase, mobiliario (vehículos, participaciones, etc.) o inmobiliario (locales, edificios, etc.) pertenecientes a la compañía, aun con carácter temporal, sin haber obtenido las autorizaciones correspondientes.
- Dilatar, impedir o dificultar la eficacia de un embargo o de un procedimiento ejecutivo o de apremio judicial, extrajudicial o administrativo (iniciado o de previsible inicio) sobre un bien (mueble o inmueble) de la compañía
- Falsear o alterar la contabilidad, libros, o cualquier otro instrumento o documento similar a los fines de obtener fraudulentamente la declaración de concurso de acreedores.

- Presentar ante un procedimiento de ejecución judicial o administrativo, información incompleta a sabiendas y con mala fe de la relación de bienes o patrimonio de la empresa que dilate o dificulte la satisfacción del acreedor.
- Disponer del patrimonio de Grupo, contraer o generar obligaciones en contra de los intereses de ésta y a favor de un acreedor, ante una situación de dificultad económica para la misma.
- Favorecer a un acreedor de mala fe en perjuicio de otro (ya sea público o privado) derivado de las relaciones anteriores habidas con éste.
- Alcanzar cualquier tipo de acuerdo con un deudor para que nos pague con preferencia o en perjuicio de otro acreedor preferente.
- Ante una situación inminente de insolvencia, ocultar o dañar bienes de la empresa para impedir que se incluyan en la masa del concurso o realizar actos de disposición mediante entrega o transferencia de dinero sin justificación económica para ello.
- Falsear o alterar la contabilidad, libros, o cualquier otro instrumento o documento similar a los fines de dificultar la valoración de la situación económica del deudor.

5º DELITOS RELATIVOS A LA PROPIEDAD INDUSTRIAL, INTELECTUAL

- Reproducir, copiar o distribuir documentos de la empresa, parcial o de forma íntegra, con el fin de obtener un beneficio económico. Propio
- Eludir o facilitar la elusión de las medidas tecnológicas eficaces para evitar las conductas anteriores.
- Fabricar, producir, importar, tener, utilizar, ofrecer o introducir en el mercado, una patente, marca o modelo de utilidad, sin consentimiento de su titular y sabiendo que es una obra registrada.
- Reproducir, imitar, modificar, utilizar o importar un signo distintivo idéntico o confundible para distinguir los mismos o similares productos o servicios

6º BLANQUEO DE CAPITALES

- Incumplir las obligaciones en materia de prevención del blanqueo de capitales y de la financiación del terrorismo.
- Realizar operaciones en las que no conste identificado el cliente o proveedor.
- Participar en operaciones o transacciones destinadas a adquirir, poseer, convertir, o transmitir bienes procedentes de la comisión de un delito o para ocultar o encubrir dicho origen.
- Utilizar, validar o contabilizar soportes documentales falsos a los fines de encubrir gastos o adquisiciones.

7º CONTRA LA HACIENDA PÚBLICA Y LA SEGURIDAD SOCIAL

- Dejar de ingresar o no retener los correspondientes importes o cantidades que se debieran en cumplimiento de la normativa fiscal aplicable a la empresa.
- Obtener beneficios fiscales o devoluciones indebidas.
- No realizar el ingreso de las correspondientes cuotas de la Seguridad Social exigidas.
- Obtener indebidamente devoluciones de la Seguridad Social. – Disfrutar de indebidas deducciones de la Seguridad Social. – Falsear las condiciones requeridas para obtener subvenciones, desgravaciones o ayudas de las administraciones públicas.
- Ocultar información que pudiera impedir la concesión de subvención, por medio del error o tergiversación de hechos o por la ocultación consciente de hechos sobre los que se tenía el deber de informar causando con ello un perjuicio a la Administración Pública. o ayuda pública.
- Obtener prestaciones de la Seguridad Social en beneficio propio o de tercero,
- Utilizar, validar o contabilizar soportes contables falsos.
- Emisión de cualquier factura pro-forma que no justifique la prestación de servicio alguno.
- Emisión de facturas por importe superior al servicio realmente abonado.
- Incumplir la obligación de llevanza de la contabilidad, libros o registros fiscales o a normativa aplicable a estos fines.
- Llevar contabilidades distintas para una misma actividad o ejercicio económico.

- No anotar en los libros contables o mercantiles negocios, actos, operaciones o cualquier otra transacción económica.
- Obstaculizar la actividad inspectora.

8º CONTRA LOS DERECHOS DE LOS TRABAJADORES NACIONALES Y EXTRANJEROS

- Engañar o abusar de la situación de un empleado para imponerle unas condiciones laborales que perjudiquen, supriman o restrinjan los derechos que tengan reconocidos en la normativa vigente o en los convenios laborales en vigor.
- Dar ocupación simultánea a una pluralidad de trabajadores sin comunicar su alta en el régimen de la Seguridad Social o sin haber obtenido la correspondiente autorización de trabajo.
- Mantener las condiciones laborales perjudiciales para los empleados cuando éstos se hayan incorporado a dMol en los supuestos de transmisión de empresas.
- Ofrecer condiciones de trabajo falsas o engañosas a una persona para inducirle a abandonar su puesto de trabajo.
- Simular un contrato o colocación de forma que se favorezca la emigración de una persona a otro país.
- Discriminar gravemente en el empleo a una persona por razón de su sexo, ideología, religión, creencias, etnia, raza, nacionalidad, orientación sexual, situación familiar, enfermedad, minusvalía, cargo de representación sindical o de los trabajadores, parentesco con cualquier otro empleado de Grupo o por utilizar alguna de las lenguas oficiales en España
- Impedir o limitar, por cualquier medio, el ejercicio del derecho de huelga o libertad sindical.
- Coaccionar o presionar a los empleados para iniciar o continuar una huelga.
- Ejecutar un trabajo sin los obligados y necesarios elementos de seguridad para la prevención de riesgos laborales y la seguridad y salud en el trabajo.
- Ejecutar un trabajo sin la supervisión o vigilancia de la persona responsable de la seguridad de la misma.
- No atender a las normas relativas a la prevención de riesgos laborales implantados por la compañía
- No facilitar los medios necesarios para que los trabajadores desempeñen su actividad con las medidas de seguridad e higiene adecuadas.
- No utilizar los medios de seguridad e higiene facilitados.
- Desobedecer cualquier orden dada por la autoridad administrativa correspondiente, que ponga en peligro grave la salud, la vida o seguridad física de los trabajadores.
- Dar de forma reiterada ocupación a ciudadanos extranjeros o menores de edad sin permiso de trabajo.
- No exigir a las entidades subcontratadas la documentación obligatoria de conformidad con la normativa aplicable en materia de seguridad, salud e higiene en el trabajo.
- No supervisar el cumplimiento por las entidades subcontratadas de la normativa de prevención de riesgos laborales.
- Incumplir los procedimientos internos en materia de salud, seguridad e higiene en el trabajo.
- Obstaculizar cualquier tipo de actividad inspectora.

9º CONTRA LOS RECURSOS NATURALES Y EL MEDIO AMBIENTE

- Provocar o realizar directa o indirectamente y sin estar debidamente autorizados emisiones, vertidos, radiaciones, extracciones o excavaciones, en la atmósfera, suelo, subsuelo, aguas terrestres, subterráneas o marítimas, incluidos la alta mar y espacios transfronterizos, causando un perjuicio al equilibrio de los sistemas naturales o a las personas.
- Provocar o realizar directa o indirectamente y sin estar debidamente autorizados aterramientos, vibraciones, inyecciones o depósito en la atmósfera, suelo, subsuelo, aguas terrestres, subterráneas o marítimas, incluido la alta mar y espacios transfronterizos, causando un perjuicio al equilibrio de los sistemas naturales o a las personas de Grupo.
- Realizar actividades clandestinas o sin haber obtenido la correspondiente autorización o licencia para el inicio y ejercicio de la actividad.

- Falsear u ocultar información medioambiental.
- Recoger, transportar, valorizar, eliminar o aprovechar residuos poniendo en peligro grave a personas, animales o plantas, calidad del aire, suelo o las aguas.
- Omitir de cualquier modo los deberes de vigilancia de los procedimientos internos en materia de prevención y seguridad medioambiental.
- Obstaculizar cualquier tipo de actividad inspectora.
- Incumplir la normativa en materia de calidad y medioambiente de Grupo.

10º COHECHO Y TRÁFICO DE INFLUENCIAS

- Ofrecer, prometer o conceder a autoridades y/o funcionarios públicos cualquier tipo de beneficio o ventaja, de cualquier clase o naturaleza, siempre que no supere los usos habituales, sociales o de cortesía, a los fines de:
- Que la autoridad y/o funcionario público actúe o deje de actuar en relación con el ejercicio de sus funciones públicas, incluida la realización de un acto contrario a los deberes inherentes a su cargo.
- Conseguir o conservar un beneficio, de cualquier tipo o naturaleza, en la realización de actividades económicas.
- Atender a las solicitudes procedentes de autoridades y/o funcionarios públicos de cualquier tipo de beneficio o ventaja, de cualquier clase o naturaleza, a los fines de:
- Que la autoridad y/o funcionario público actúe o deje de actuar en relación con el ejercicio de sus funciones públicas, incluida la realización de un acto contrario a los deberes inherentes a su cargo.
- Conseguir o conservar cualquier tipo de negocio Influir en un funcionario público o autoridad valiéndose de la relación personal que se tenga con el mismo, a fin de obtener una resolución que le pueda generar directa o indirectamente un beneficio económico para sí o para un tercero.
- Actuar como intermediario de un tercero, por razón de la relación personal habida con un funcionario público, para obtener un trato de favor para ese tercero, del funcionario público con el que se tiene la relación personal.

11º OTRAS CONDUCTAS A VIGILAR. ACOSO SEXUAL, LABORAL O MOBBING

- Incumplir la normativa en materia de acoso
- Utilizar un lenguaje abusivo, amenazador o grosero de forma reiterada y grave para dirigirse a subordinados o compañeros.
- Difamar o deshonorar de manera reiterada y grave a un subordinado frente a sus compañeros u otros jefes (propagando rumores maliciosos, injuriosos o calumniosos que menoscaben su reputación, imagen o profesionalidad).
- Retener reiteradamente información crucial para la ejecución por un subordinado de su trabajo o manipularla para inducirle a error y acusarle después de incompetencia o ineptitud profesional
- Comentarios, bromas, afirmaciones o amenazas de contenido agresivo, insultante o humillante a subordinados, realizados de forma reiterada y grave
- Comentarios degradantes a subordinados relacionados con su forma de vestir, orientación sexual, raza, cultura o religión, realizados de forma reiterada y grave.
- Impedir de forma reiterada y grave a un subordinado cualquier toma de decisión o iniciativa personal en el marco de sus responsabilidades y funciones laborales.
- Ejecutar de forma reiterada y grave las anteriores conductas frente a un subordinado con el fin de que cause baja voluntaria en la empresa.

2.3. RIESGOS ESPECÍFICOS DE LA ACTIVIDAD DE dMol

La naturaleza de las operaciones de DEMOLICIÓN Y DESCONTAMINACIÓN S.L., centradas en la demolición, descontaminación ambiental, gestión de residuos y obras industriales, comporta una exposición especial a determinados riesgos penales, entre ellos:

- Contratación pública y licitaciones . Posibles actos de corrupción, soborno o tráfico de influencias.
- Gestión medioambiental y de residuos. Incumplimientos en materia de vertidos, emisiones o transporte de residuos.
- Seguridad y salud laboral. Deficiencias en la prevención de riesgos laborales o en la coordinación de actividades empresariales.
- Gestión económica y financieras. Riesgos de fraude, falsedad documental o blanqueo de capitales.
- Protección de datos e información técnica. Riesgos derivados de accesos indebidos o revelación de información confidencial.

2.4. ACTUALIZACIÓN Y REVISIÓN DE RIESGOS

El sistema de identificación de riesgos penales será objeto de revisión continua para garantizar su eficacia y adecuación al entorno regulatorio.

En particular, el análisis se actualizará:

- Anualmente, mediante auditoría interna de cumplimiento.
- Extraordinariamente, cuando se produzcan cambios en la estructura, procesos o marco normativo.
- Tras cualquier incidente, denuncia o desviación significativa, para incorporar medidas correctoras y lecciones aprendidas.

El Responsable de Cumplimiento Normativo documentará todas las actualizaciones en el Registro de Revisión de Riesgos Penales, manteniendo la trazabilidad de cada modificación.

3. OBJETIVOS

Prevenir, detectar y reaccionar ante posibles conductas contrarias a la ley o a los valores corporativos, asegurando la transparencia, la integridad y la responsabilidad en todas las decisiones y actuaciones de la organización.

1 Contra la corrupción y el cohecho

- Fomentar una cultura de tolerancia cero frente al soborno o beneficio indebido.
- Garantizar relaciones transparentes y trazables con autoridades, clientes y proveedores.
- Consolidar la formación ética y de cumplimiento normativo.

2. Administración desleal , apropiación indebida Y conflicto de intereses

- Proteger los recursos y activos corporativos frente a usos indebidos o decisiones desleales.
- Fortalecer la supervisión financiera y documental.
- Promover la declaración proactiva de posibles conflictos por parte de empleados y directivos.
- Asegurar la imparcialidad y objetividad en decisiones corporativas y en la selección de proveedores.
- Reforzar la trazabilidad documental en todas las decisiones económicas o de contratación.

3. Revelación de secretos y violación de la intimidad

- Asegurar la confidencialidad de información técnica, comercial y personal.
- Impulsar la cultura de ciberseguridad y respeto a la privacidad.

4. Insolvencia punible

- Mantener la transparencia económica y la integridad en la gestión patrimonial.
- Prevenir cualquier alteración contable o actuación que perjudique a acreedores.

5. Propiedad intelectual e industrial

- Proteger las creaciones, marcas y documentación interna.
- Evitar la copia, uso no autorizado o vulneración de derechos de terceros.

6. Blanqueo de capitales

- Garantizar la trazabilidad y transparencia en todas las transacciones financieras.
- Aplicar los procedimientos de diligencia debida con clientes y proveedores.

7. Contra la Hacienda Pública y la Seguridad Social

- Cumplir con todas las obligaciones fiscales y laborales de manera íntegra y oportuna.
- Prevenir errores o manipulaciones contables.

8. Derechos de los trabajadores

- Promover un entorno laboral seguro, equitativo y libre de discriminación.
- Garantizar el cumplimiento de la normativa de prevención de riesgos laborales.

9. Medio ambiente y recursos naturales

- Minimizar el impacto ambiental de las operaciones.
- Asegurar el cumplimiento de la legislación medioambiental.

10. Cohecho y tráfico de influencias

- Evitar cualquier trato de favor o injerencia en decisiones de autoridades o funcionarios.
- Garantizar la transparencia en relaciones institucionales.

11. Otras conductas a vigilar. Acoso laboral, sexual o mobbing

- Mantener un ambiente de trabajo respetuoso y libre de acoso.
- Fomentar la denuncia segura y confidencial de conductas inadecuadas.
- Inducir o incitar de forma reiterada y grave a otros superiores de los que dependa un subordinado, a participar en cualquiera de las conductas prohibidas anteriores.

Es obligación de cada persona estar debidamente informada de las Leyes y de su cumplimiento. Hay que tener en consideración que el beneficio obtenido por una actividad ilícita tanto puede ser directo como indirecto, debiendo extremarse precauciones sobre cualquier conducta que, siendo ilícita, pueda terminar beneficiando a la empresa en ese sentido tan amplio. Igualmente, las personas jurídicas no sólo responderán por las acciones u omisiones acaecidas en España, sino también, si se cumplen determinadas circunstancias, por lo sucedido en cualquier otro país lo que obliga a todos los miembros de la Organización a mantenerse alerta ante conductas potencialmente delictivas según la normativa española que concurran en cualquier parte del mundo.

PARTE II- PLAN DE PREVENCIÓN DE RIESGOS PENALES

4. PLAN DE PREVENCIÓN DE RIESGOS PENALES- PPRP

El Plan de Prevención de Riesgos Penales (PPRP) de dMol constituye el instrumento principal del Sistema de Compliance Penal, diseñado para prevenir la comisión de delitos dentro de la organización y asegurar el cumplimiento de la normativa vigente.

Mientras la **Política de Compliance** define el marco general de actuación, los principios éticos y el compromiso institucional de la empresa con el cumplimiento normativo, el **PPRP** describe los mecanismos concretos que permiten aplicar dichos principios de forma efectiva.

Su finalidad es establecer un conjunto de principios, procedimientos y controles internos que garanticen la detección temprana de conductas ilícitas, la investigación eficaz de posibles irregularidades y la aplicación de medidas correctoras adecuadas.

El plan se integra en todos los niveles organizativos, asegurando que cada empleado conozca sus obligaciones en materia de cumplimiento y actúe conforme a los valores éticos de dMol.

El Plan de Prevención de Riesgos Penales forma parte del Sistema de Gestión Integrado (SGI) de dMol y se coordina con los sistemas de calidad, medio ambiente, prevención de riesgos laborales y responsabilidad social corporativa (RSC).

4.1 ÁMBITO DE APLICACIÓN DEL PPRP

El PPRP es de obligado cumplimiento para todo el personal de dMol y se aplica a la totalidad de sus actividades, procesos y relaciones con terceros.

Su ámbito de aplicación comprende:

1. Personas y áreas incluidas

- Todo el personal de plantilla, con independencia de su nivel jerárquico o ubicación.
- Los directivos, administradores y representantes legales.
- Los colaboradores, contratistas, subcontratistas y socios comerciales que actúen en nombre o por cuenta de dMol.

2. Actividades cubiertas

- Todas las operaciones derivadas del objeto social de la empresa, incluyendo demolición, descontaminación, tratamiento de residuos y servicios auxiliares.
- Las actividades administrativas, financieras, comerciales, medioambientales y laborales, donde puedan existir riesgos penales asociados.
- Las relaciones con administraciones públicas, clientes, proveedores y comunidades, especialmente en contextos de contratación pública o de alto riesgo reputacional.

3. Territorio de aplicación

- El PPRP es aplicable en todo el territorio nacional y, en caso de operaciones internacionales, en aquellos países donde dMol actúe directa o indirectamente.
- En los entornos donde existan normativas locales más estrictas, prevalecerán siempre las disposiciones más exigentes.

4.2. ESTRUCTURA DEL PLAN

El PPRP tiene como finalidad prevenir, detectar y reaccionar ante la posible realización de conductas ilícitas dentro del ámbito de actuación de dMol, asegurando la observancia de la ley y el mantenimiento de la integridad corporativa.

Sus objetivos específicos son:

- Reducir la exposición al riesgo penal mediante controles eficaces.
- Fomentar una cultura de cumplimiento y transparencia.
- Garantizar la trazabilidad y documentación de todas las actuaciones relevantes.
- Proporcionar un marco de actuación ante incidentes o denuncias.
- Asegurar la colaboración activa con las autoridades en caso de investigación penal.

El PPRP se estructura en cinco bloques operativos que conforman el núcleo del sistema de prevención:

1. **Gobernanza del modelo de cumplimiento:** designación de responsables, independencia del RCN y supervisión por la Dirección.
2. **Procedimientos y controles preventivos:** medidas concretas para evitar conductas ilícitas (anticorrupción, debida diligencia, denuncias internas, control de operaciones sensibles).
3. **Evaluación y gestión del riesgo penal:** metodología de valoración, matrices de riesgo y revisión periódica de su eficacia.
4. **Metas e indicadores de cumplimiento:** definición de objetivos cuantitativos y cualitativos, y mecanismos de seguimiento.
5. **Supervisión, formación y mejora** continua: auditorías, actualizaciones y fomento de la cultura ética en toda la organización.

5. GOBERNANZA DEL PPRP

5.1. Responsabilidades de la Alta Dirección

La Alta Dirección de dMol, asume la máxima responsabilidad sobre el modelo de cumplimiento penal y garantiza los recursos necesarios para su implantación, seguimiento y mejora continua.

Sus principales funciones son:

1. Aprobar formalmente el PPRP y las políticas que lo desarrollan.
2. Fomentar una cultura corporativa de integridad, ética y respeto a la legalidad en todos los niveles de la organización.
3. Proveer los medios materiales, humanos y financieros necesarios para la ejecución del plan y la independencia del Responsable de Cumplimiento Normativo (RCN).
4. Supervisar la eficacia del sistema, revisando periódicamente los informes del RCN y adoptando las medidas correctoras que se propongan.
5. Garantizar la no injerencia en las investigaciones o actuaciones de compliance, preservando la independencia del RCN.
6. Dar ejemplo de comportamiento ético en su propia actuación, reforzando el principio de liderazgo responsable.
7. Aprobar las revisiones y actualizaciones del PPRP, asegurando su alineación con los cambios legislativos o estructurales.

La Alta Dirección es, en última instancia, titular del compromiso de cumplimiento penal de la organización, siendo responsable de su difusión, efectividad y coherencia con los valores corporativos de dMol.

5.2. Funciones y Autonomía del Responsable del PRPP

El Responsable de Cumplimiento Normativo (RCN) es la figura encargada de supervisar la aplicación efectiva del PRPP y de garantizar la independencia funcional del sistema de cumplimiento penal.

El RCN actúa en nombre de la Dirección, pero con autonomía y autoridad propias, reportando directamente al Administrador Único.

Funciones principales del RCN:

1. Implantación y supervisión del PRPP, asegurando su cumplimiento por parte de todo el personal.
2. Asesoramiento técnico y jurídico a la Dirección y a las distintas áreas operativas en materia de cumplimiento penal.
3. Identificación y actualización de riesgos penales, elaborando y manteniendo el Mapa de Riesgos Penales.
4. Gestión del canal ético o de denuncias internas, garantizando confidencialidad, protección del informante y tramitación de las investigaciones.
5. Emisión de informes periódicos de cumplimiento y propuestas de mejora dirigidas a la Alta Dirección.
6. Formación y sensibilización del personal, promoviendo la cultura de integridad y cumplimiento.
7. Coordinación con otras funciones de control interno, como auditoría, recursos humanos o medio ambiente.
8. Colaboración con las autoridades competentes en caso de investigaciones o procedimientos judiciales.

Autonomía funcional y recursos:

- El RCN dispone de acceso libre a toda la documentación e información relevante para el ejercicio de sus funciones.
- Actúa sin interferencias jerárquicas que puedan afectar su independencia.
- Cuenta con poderes autónomos de supervisión y control, y con un presupuesto propio aprobado por la Dirección.
- Su designación y, en su caso, cese deben ser aprobados formalmente por el Administrador Único y comunicados a todo el personal.

El RCN será relevado de sus funciones en caso de:

- Incurrir en infracciones o conflictos de interés incompatibles con el cargo.
- Pérdida de confianza, inhabilitación o incumplimiento grave de sus obligaciones.
- Situaciones de baja prolongada o incapacidad para ejercer su labor.

5.3. Comunicación y Acceso al Plan

El PRPP se difunde a través de los canales internos de comunicación de dMol, reuniones informativas o formación presencial.

Todo el personal recibe un extracto del Plan en el momento de su incorporación, y su adhesión queda formalizada mediante la firma de compromiso de cumplimiento.

Las actualizaciones del PRPP se comunicarán a toda la plantilla.

El Plan de Formación anual de dMol incluye contenidos específicos del PRPP

6. PROCEDIMIENTOS Y CONTROLES DE PREVENCIÓN

El Plan de Prevención de Riesgos Penales (PPRP) se articula mediante un conjunto de procedimientos específicos de control diseñados para minimizar la exposición de dMol a conductas ilícitas, garantizar la trazabilidad de las operaciones y fortalecer la cultura de integridad corporativa.

Estos procedimientos se aplican de manera transversal en todas las áreas de la empresa y son revisados periódicamente por el Responsable de Cumplimiento Normativo (RCN).

6.1. PROCEDIMIENTO DE CONTROL PARA PREVENIR LA CORRUPCIÓN

Principios y controles aplicados:

1. Tolerancia cero ante la corrupción en cualquiera de sus formas, tanto activa como pasiva.
2. Prohibición de pagos, regalos o invitaciones que superen los límites de cortesía establecidos en la Política de Regalos y Hospitalidad.
3. Revisión previa de operaciones sensibles, especialmente las que involucren administraciones públicas, intermediarios o consultores externos.
4. Autorización previa y documentada para cualquier gasto de representación, patrocinio o donación.
5. Control financiero reforzado: revisión periódica de facturas, contratos y justificaciones de pago para detectar posibles irregularidades.
6. Formación anual obligatoria en ética y anticorrupción para todo el personal.
7. Registro de relaciones institucionales y visitas en un sistema de control interno

El incumplimiento de estas disposiciones se considerará infracción grave y dará lugar a sanciones disciplinarias y, en su caso, acciones legales.

6.2. PROCEDIMIENTO DE DENUNCIAS INTERNAS Y CANAL ÉTICO

dMol ofrece un medio seguro y confidencial para comunicar posibles irregularidades o infracciones legales o éticas:

denuncias@dmol.es

Requisitos del canal denuncias

1. Accesible a todo el personal y terceros vinculados (proveedores, contratistas o socios comerciales).
2. Confidencialidad garantizada: la identidad del denunciante se mantiene reservada, conforme a la normativa de protección de datos.
3. Prohibición expresa de represalias contra quienes actúen de buena fe.

Procedimiento de gestión:

1. Recepción de la denuncia por el RCN, quien acusará recibo al informante.
2. Apertura de expediente interno con registro codificado y documentación asociada.
3. Evaluación preliminar de la verosimilitud de los hechos.
4. Investigación interna, pudiendo el RCN solicitar apoyo externo especializado.
5. Informe final con conclusiones y propuesta de medidas disciplinarias o correctoras.
6. Archivo y conservación del expediente durante el periodo legal establecido.

6.3. PROCEDIMIENTO DE APROBACIÓN DE OPERACIONES ESPECIALES (SENSIBLES)

Se consideran operaciones sensibles:

- Contratos o licitaciones con entidades públicas.
- Pagos o donaciones a terceros sin contraprestación directa.
- Operaciones con intermediarios o países de alto riesgo (según Transparencia Internacional).
- Transacciones financieras inusuales o de importe significativo.

Flujo de aprobación:

1. Solicitud inicial del responsable del área o proyecto, con documentación justificativa.
2. Revisión de cumplimiento por el RCN y validación del Departamento Financiero.
3. Autorización formal por parte del Administrador Único.
4. Registro documental de toda la operación y conservación durante 10 años.

Ninguna operación sensible podrá ejecutarse sin la triple aprobación (responsable de Dpto. implicado, RCN y Dirección).

6.4. DEBIDA DILIGENCIA A TERCEROS Y CLÁUSULAS ANTICORRUPCIÓN

Procedimiento de debida diligencia:

1. Clasificación del tercero (proveedor, contratista, socio, consultor o intermediario).
2. Cuestionario de integridad y anticorrupción, donde el tercero declara:
 - Ausencia de sanciones o antecedentes penales.
 - Existencia de programas de cumplimiento propios.
 - Compromiso con la política ética de dMol.
3. Verificación documental: comprobación del CIF, escrituras sociales, solvencia y cumplimiento de obligaciones fiscales y laborales.
4. Firma de la cláusula anticorrupción y de cumplimiento, incluida en todos los contratos, subcontratos y acuerdos de colaboración.
5. Reevaluación periódica (anual) de los terceros clasificados como críticos o de riesgo alto.

dMol se reserva el derecho de rescindir cualquier contrato ante la detección de prácticas corruptas o incumplimientos graves de integridad.

6.5. CONTROL DOCUMENTAL Y TRAZABILIDAD DE OPERACIONES

Controles Principales:

1. Centralización de la documentación contractual, contable y operativa bajo gestión del Departamento SGI y RSC.
2. Numeración y archivo sistemático de documentos, facturas y contratos, con control de versiones.
3. Segregación de funciones: quien autoriza un gasto no puede aprobar su pago.
4. Revisión semestral de la contabilidad y los registros financieros por parte del RCN y Contabilidad.
5. Acceso restringido a la información confidencial según niveles de responsabilidad.
6. Conservación documental mínima de 10 años, conforme a la normativa fiscal y penal.
7. Auditorías periódicas para verificar la trazabilidad y la integridad de la información.

Este sistema de control documental permite acreditar el cumplimiento de las políticas internas y actúa como medio de prueba ante cualquier auditoría, inspección o procedimiento judicial.

7. EVALUACIÓN Y GESTIÓN DEL RIESGO PENAL

El proceso de evaluación y gestión del riesgo penal permite a dMol priorizar los riesgos detectados y asignar los recursos necesarios para su prevención, de acuerdo con su probabilidad de ocurrencia y el impacto potencial sobre la organización.

Este análisis es la base para definir los controles preventivos, correctivos y mitigadores del Plan de Prevención de Riesgos Penales (PPRP).

7.1. METODOLOGÍA DE VALORACIÓN (PROBABILIDAD E IMPACTO)

La metodología de evaluación adoptada por dMol se basa en criterios objetivos y cuantificables que permiten determinar la exposición real al riesgo penal en cada área o proceso.

El análisis combina dos dimensiones principales:

1 Probabilidad de ocurrencia (P):

Evalúa la posibilidad de que un riesgo penal se materialice en función de factores internos y externos.

Escala de valoración:

- Alta (3): riesgo probable o recurrente en el sector.
- Media (2): riesgo posible, pero con controles establecidos.
- Baja (1): riesgo remoto o poco relevante.

2. Impacto potencial (I)

Mide las consecuencias que tendría la materialización del riesgo, considerando sanciones económicas, daño reputacional y consecuencias legales.

Escala de valoración:

- Alto (3): posible perjuicio penal, económico o reputacional grave.
- Medio (2): daño moderado, controlable mediante medidas correctoras.
- Bajo (1): impacto leve o sin trascendencia significativa.

3. Nivel de riesgo (NR):

El Nivel de Riesgo Penal (NR) se obtiene mediante la fórmula:

$$NR = P \times I$$

Rango NR	Nivel de riesgo	Criterio de actuación
1 – 2	Bajo	Riesgo asumible, se mantienen controles actuales.
3 – 4	Medio	Se refuerzan controles y seguimiento semestral.
6 – 9	Alto	Requiere medidas inmediatas y revisión prioritaria.

7.2. MATRIZ DE RIESGOS Y CONTROLES PREVENTIVOS

La matriz de riesgos penales de dMol es una herramienta de gestión que relaciona los riesgos identificados con los controles específicos aplicables a cada uno.

Permite visualizar de forma estructurada el nivel de exposición de la organización y las medidas implantadas para mitigarlo.

Riesgo Penal Identificado	Área / Proceso Afectado	Probabilidad (P)	Impacto (I)	Nivel (NR)	Controles Preventivos Implementados	Responsable de Seguimiento
Corrupción o cohecho	Contratación pública / Ventas	2	3	6 (Alto)	Autorización previa, registro de relaciones institucionales, formación anticorrupción.	RCN / Dirección Comercial
Administración desleal	Finanzas / Compras	2	2	4 (Medio)	Revisión contable semestral, segregación de funciones, control de gastos.	Contabilidad / SGI
Revelación de secretos	IT / RRHH / Proyectos	1	3	3 (Medio)	Control de accesos, políticas de confidencialidad, formación en protección de datos.	IT / RCN
Blanqueo de capitales	Finanzas / Clientes	2	3	6 (Alto)	Identificación de clientes, revisión documental, control financiero.	Financiero / RCN
Delitos medioambientales	Obras / Producción	2	3	6 (Alto)	Control de residuos, licencias ambientales, seguimiento de vertidos.	SGI / Medio Ambiente

7.3. SEGUIMIENTO Y REVISIÓN DE MEDIDAS MITIGADORAS

El seguimiento continuo del riesgo penal permite comprobar la eficacia de los controles aplicados y detectar posibles deficiencias o desviaciones.

Mecanismos de seguimiento:

- 1. Auditorías internas** de cumplimiento: realizadas al menos una vez al año por el RCN y el Departamento SGI, con verificación documental y entrevistas.
- 2. Revisión de indicadores de desempeño (KPIs):** vinculados a las metas cuantitativas establecidas en el punto 9 del PPRP.
- 3. Control de incidentes o denuncias recibidas:** análisis de causas y actualización de controles según las lecciones aprendidas.
- 4. Evaluaciones extraordinarias:** en caso de cambios normativos, sanciones o reestructuraciones relevantes.
- 5. Reuniones de revisión:** entre la Alta Dirección y el RCN, al menos una vez al año, para valorar resultados y priorizar acciones correctoras.

Resultados y documentación:

- Toda medida correctora o preventiva adoptada quedará registrada en el Plan de Acción de Mejora del PPRP, con asignación de responsables y plazos de ejecución.
- La eficacia de las medidas será evaluada en la revisión siguiente, garantizando un ciclo de mejora continua.

8. METAS Y RETOS DEL SISTEMA DE CUMPLIMIENTO (KPIS)

El Plan de Prevención de Riesgos Penales (PPRP) de dMol incorpora un conjunto de metas cuantitativas y cualitativas que permiten evaluar su eficacia y el grado de madurez del sistema de cumplimiento.

8.1 INDICADORES CUANTITATIVOS

Área de Riesgo	Indicador / Meta Cuantitativa	Objetivo Mínimo Anual
Corrupción y cohecho	% de personal formado en anticorrupción	100%
	Nº de incidentes o denuncias fundadas	0
Administración desleal / apropiación indebida	Nº de revisiones contables con incidencias graves	≤ 1 por año
Protección de datos y confidencialidad	% de empleados formados en privacidad y ciberseguridad	100%
	Nº de accesos no autorizados registrados	0
Blanqueo de capitales	% de operaciones verificadas con debida diligencia	100%
Hacienda Pública y Seguridad Social	Nº de operaciones reportadas sin justificación	0
	% de obligaciones fiscales y laborales cumplidas en plazo	100%
Medio ambiente	Reducción anual de residuos generados	≥ 5 %
Prevención del acoso y ética laboral	% de plantilla formada en igualdad y conducta ética	100%
	Nº de casos sin gestión conforme al protocolo	0

8.2. INDICADORES CUALITATIVOS

- **Nivel de conocimiento del PPRP:** porcentaje de empleados que conocen sus contenidos y canales de denuncia (medido mediante encuestas).
- **Percepción de la cultura ética:** grado de confianza en el sistema de compliance (encuesta de clima ético).
- **Eficacia de los canales de comunicación:** evaluación de la accesibilidad y tiempo de respuesta del canal ético.
- **Madurez del sistema de cumplimiento:** análisis comparativo anual frente a los requisitos UNE 19601 (nivel de implantación por secciones).
- **Reacción ante incidentes:** tiempo medio de resolución y medidas adoptadas frente a irregularidades.

8.3. RESPONSABLES DE SEGUIMIENTO

El seguimiento y control de las metas del sistema de cumplimiento se distribuye de forma coordinada entre los distintos órganos de dMol:

Área / Indicador	Responsable Directo	Colaboradores
Ética, corrupción, canal de denuncias	Responsable de Cumplimiento Normativo (RCN)	Dirección General / RRHH
Revisiones contables y financieras	Departamento Financiero / Contabilidad	SGI / Auditoría interna
Protección de datos y confidencialidad	Departamento IT / RCN	RRHH / Proyectos
Medio ambiente y PRL	Departamento SGI y RSC	Jefes de Obra / Producción
Formación y comunicación	RRHH / RCN	Dirección General
Evaluación general del PPRP	RCN	Alta Dirección

8.4. EVALUACIÓN Y MEJORA CONTINUA

El sistema de cumplimiento penal se somete a una revisión continua con periodicidad definida para cada nivel de control.

Proceso de Mejora Continua

1. Evaluar: medir resultados mediante indicadores y auditorías.
2. Analizar: comparar resultados con los objetivos establecidos.
3. Corregir: implementar medidas preventivas o correctoras según desviaciones.
4. Actualizar: revisar procedimientos, controles y formaciones.
5. Comunicar: informar a la plantilla y partes interesadas sobre los avances y mejoras.

Este ciclo garantiza que el sistema de compliance penal de dMol evolucione de forma proactiva, medible y sostenible, asegurando su alineación permanente con la normativa y los valores de la empresa.

Actividad de seguimiento	Periodicidad	Responsable
Revisión de indicadores cuantitativos	Trimestral	RCN / SGI
Análisis de riesgos y matriz de controles	Anual	RCN / Dirección
Auditoría interna de cumplimiento	Anual	RCN / Auditoría externa
Formación y sensibilización del personal	Anual	RRHH / RCN
Revisión del canal ético y denuncias	Semestral	RCN
Informe de cumplimiento penal	Anual	RCN / Dirección
Actualización del PPRP	Cuando existan cambios	RCN / Alta Dirección

9. RÉGIMEN DISCIPLINARIO Y MEDIDAS CORRECTORAS

El Régimen Disciplinario constituye un pilar esencial del Plan de Prevención de Riesgos Penales (PPRP), al garantizar la eficacia del modelo de cumplimiento penal y asegurar que toda conducta contraria a la ley, a la Política de Compliance o al Código Ético tenga una consecuencia proporcional.

Este régimen es aplicable a todo el personal de dMol, con independencia de su nivel jerárquico, función o modalidad contractual, así como a terceros que actúen en nombre o representación de la empresa.

9.1 TIPO DE INFRACCIONES

a) Infracciones leves

- Incumplimientos formales o puntuales de procedimientos internos sin consecuencias graves.
- Retrasos o negligencias en la ejecución de controles o registros documentales.
- Omisiones no intencionadas en la comunicación de información relevante al RCN.
- Conductas que no generen perjuicio económico ni reputacional a la empresa.

b) Infracciones graves

- Incumplimiento reiterado o consciente de los procedimientos de compliance.
- Falta de colaboración con el RCN en las tareas de supervisión o investigación.
- Destrucción o alteración de documentación interna sin autorización.
- Negativa a recibir formación obligatoria en materia de cumplimiento.
- Ocultación de conflictos de interés o información relevante.

c) Infracciones muy graves

- Participación activa en actos de corrupción, fraude, cohecho o malversación.
- Uso indebido de fondos o activos de la empresa.
- Manipulación contable o falsificación documental.
- Revelación de información confidencial o de datos personales de forma intencionada.
- Represalias contra informantes o testigos de buena fe.
- Cualquier conducta que pudiera implicar responsabilidad penal para la persona jurídica.

Cada infracción será valorada individualmente, teniendo en cuenta la intencionalidad, reiteración, grado de daño y circunstancias atenuantes o agravantes.

9.2. MEDIDAS DISCIPLINARIAS APLICABLES

Las medidas disciplinarias se aplicarán conforme a los principios de proporcionalidad, equidad y legalidad, y de acuerdo con lo establecido en el Estatuto de los Trabajadores, el Convenio Colectivo aplicable y la normativa interna de dMol.

Las sanciones podrán incluir, según la gravedad del incumplimiento:

Nivel de infracción	Medidas disciplinarias posibles
Leves	Amonestación verbal o escrita.Repetición de formación en cumplimiento o procedimiento afectado.
Graves	Suspensión de empleo y sueldo de hasta 15 días.Inhabilitación temporal para participar en determinadas actividades o funciones.Registro de sanción en el expediente personal.
Muy graves	Despido disciplinario.Resolución contractual con terceros o colaboradores implicados.Comunicación inmediata a la autoridad competente si se aprecia posible delito.

PROCEDIMIENTO DISCIPLINARIO

1. **Inicio:** el RCN comunica a la Dirección o al Departamento de RRHH los hechos constatados.
2. **Audiencia al interesado:** se garantiza el derecho de defensa y la posibilidad de aportar pruebas o alegaciones.
3. **Propuesta de sanción:** el RCN emite informe con recomendación de medida disciplinaria.
4. **Resolución:** la Alta Dirección o RRHH imponen la sanción correspondiente.
5. **Registro y seguimiento:** todas las sanciones quedan documentadas en el Registro de Incidencias y Medidas Disciplinarias.

En caso de infracciones cometidas por directivos o administradores, la decisión corresponderá exclusivamente al Administrador Único, previa valoración del RCN.

9.3 COLABORACIÓN CON LAS AUTORIDADES COMPETENTES

dMol mantiene un compromiso activo de colaboración con las autoridades judiciales, policiales y administrativas en todos los casos en que se detecten indicios de delito o infracciones graves.

Las actuaciones en este ámbito se rigen por los siguientes principios:

1. **Transparencia y cooperación plena:** facilitando toda la información y documentación requerida por las autoridades competentes.
2. **Integridad y buena fe:** asegurando que la empresa actúa con diligencia y sin interferir en las investigaciones.
3. **Protección de la confidencialidad:** garantizando que los datos personales y la información sensible se gestionan conforme al Reglamento General de Protección de Datos (RGPD).
4. **Trazabilidad documental:** manteniendo un registro completo de todas las comunicaciones y colaboraciones con las autoridades.
5. **Reparación y corrección:** aplicación inmediata de medidas correctoras o disciplinarias cuando se confirme una irregularidad o delito.

La Alta Dirección y el RCN serán los responsables de coordinar cualquier comunicación oficial con organismos externos, asegurando que las actuaciones de dMol se realicen de forma ética, responsable y conforme a derecho.

10. SUPERVISIÓN Y MEJORA CONTINUA DEL PPRP

El sistema de cumplimiento penal de dMol se concibe como un modelo dinámico y en evolución constante, que requiere mecanismos de supervisión, evaluación y mejora continua para asegurar su eficacia a lo largo del tiempo.

El seguimiento sistemático del PPRP permite identificar deficiencias, proponer medidas correctoras y garantizar que el plan se mantenga alineado con los cambios normativos, organizativos y del entorno empresarial.

10.1 . AUDITORÍAS INTERNAS Y REVISIONES PERIÓDICAS

Las auditorías internas de cumplimiento penal constituyen la principal herramienta de supervisión del PPRP.

Su finalidad es verificar la adecuación, eficacia y cumplimiento real de los controles y procedimientos implantados.

Características Principales

1. **Periodicidad:** al menos una vez al año, sin perjuicio de auditorías extraordinarias cuando se detecten incidentes relevantes, modificaciones normativas o cambios estructurales.
2. **Alcance:** incluye la revisión de todos los procedimientos del PPRP (canal ético, debida diligencia, controles financieros, trazabilidad documental, etc.).
3. **Ejecución:** coordinadas por el Responsable de Cumplimiento Normativo (RCN), con la colaboración del Departamento SGI y RSC. Cuando proceda, podrán apoyarse en auditores externos independientes.
4. **Metodología:** revisión documental, entrevistas, comprobación de evidencias y verificación del cumplimiento de los indicadores (KPIs).
5. **Informe de resultados:** el RCN elaborará un Informe de Auditoría de Cumplimiento Penal, que incluirá:
 - Hallazgos y no conformidades detectadas.
 - Nivel de cumplimiento respecto a la UNE 19601 e ISO 37301.
 - Recomendaciones de mejora y plazos de ejecución.
6. **Seguimiento:** las áreas implicadas deberán aplicar las acciones correctoras en los plazos establecidos y comunicar su cumplimiento al RCN.

Los resultados de las auditorías se presentarán anualmente a la Alta Dirección, junto con el Informe General de Cumplimiento Penal, para su validación y archivo.ualmente, teniendo en cuenta la intencionalidad, reiteración, grado de daño y circunstancias atenuantes o agravantes.

10.2. ACTUALIZACIÓN

El PPRP será objeto de actualización continua, garantizando que su contenido refleje en todo momento la realidad operativa y normativa de dMol.

Fecha de revisión	Descripción del cambio	Área responsable	Aprobado por	Fecha de entrada en vigor
				
				

11. DIFUSIÓN, FORMACIÓN Y SENSIBILIZACIÓN

La eficacia del Plan de Prevención de Riesgos Penales (PPRP) depende en gran medida de que todos los integrantes de dMol comprendan sus principios, conozcan sus responsabilidades y actúen conforme a ellos en su desempeño profesional

Por ello, la empresa desarrolla una estrategia permanente de comunicación, formación y sensibilización que fomenta una cultura corporativa de cumplimiento, transparencia e integridad en todos los niveles de la organización.

11.1 ESTRATEGIA DE COMUNICACIÓN INTERNA

La difusión del PPRP y de la Política de Compliance se realiza de manera estructurada y accesible, garantizando que la información llegue a todo el personal y se mantenga actualizada.

Mecanismos de Comunicación

1. **Welcome pack.** Entrega de extracto del PRPP con cada alta en la empresa, acompañado de firma de su recepción
2. **Programa Sostenibilidad en Accion.** Envío de comunicaciones periódicamente sobre los diferentes aspectos del PRPP
3. **Evaluaciones:** puntualmente se realizan evaluaciones para medir el nivel de conocimiento entre los trabajadores
4. **Canal Consulta.** El RCN atiende todas las consultas necesarias a través del Whatsapp interno o de forma personal.

El objetivo es que la comunicación sea continua, clara, participativa y bidireccional, favoreciendo la implicación real de todos los miembros de la organización.

11.2. FORMACIÓN EN COMPLIANCE PENAL

La formación constituye un elemento clave para la implantación efectiva del sistema de cumplimiento penal.

dMol garantiza que todos los empleados y colaboradores cuenten con la capacitación necesaria para actuar conforme a la ley, las políticas internas y los valores éticos corporativos. de extracto del PRPP con cada alta en la empresa, acompañado de firma de su recepción

Plan de Formación

1. Formación inicial (obligatoria):
 - A todo el personal de nuevo ingreso.
 - Incluye los principios del Código Ético, la Política de Compliance, el funcionamiento del PPRP y el canal de denuncias.
 - Se formaliza mediante firma del compromiso de cumplimiento.
2. Formación continua:
 - Sesiones periódicas de actualización sobre riesgos penales, anticorrupción, conflictos de interés, protección de datos, medio ambiente y prevención de riesgos laborales.
 - Contenidos adaptados al perfil del puesto y al nivel de exposición al riesgo penal.
 - Incluye módulos específicos para directivos y mandos intermedios, centrados en liderazgo ético y responsabilidad penal de la empresa.
3. Formación extraordinaria:
 - Se organiza ante cambios legislativos relevantes, incidentes internos o actualizaciones del PPRP.
4. Evaluación y registro:
 - Se documenta la asistencia y resultados de cada sesión.
 - El RCN y RRHH mantienen un registro formativo que permite acreditar la formación recibida por cada trabajador.

Objetivo de cumplimiento:

- 100 % de empleados formados anualmente en materia de compliance penal y ética empresarial.
- Reducción progresiva de incidentes o infracciones derivadas de desconocimiento de normas.

La presente Política y Plan entra en vigor el día 20 de enero de 2020, fecha de su aprobación por el Administrador Único, y es actualizada anualmente

Algete, 18 de febrero de 2025



Adolfo García Alonso.
Gerente

ANEXO I

CUESTIONARIO DE DEBIDA DILIGENCIA A TERCEROS

Obligatorio para proveedores, contratistas, consultores, intermediarios y socios estratégicos antes del inicio de la relación comercial y en revisiones periódicas (mínimo anual).

Modelo de cuestionario

- Nombre / Razón social: _____
- CIF / NIF: _____
- Domicilio social: _____
- Persona de contacto: _____
- Cargo y teléfono: _____
- Actividad principal: _____

1. Integridad y cumplimiento legal

- ☐ Declaro no haber sido sancionado ni investigado por delitos de corrupción, fraude o blanqueo de capitales.
- ☐ Confirmo que la empresa cumple con todas las obligaciones fiscales, laborales y medioambientales.
- ☐ Disponemos de políticas internas de ética y cumplimiento.
- ☐ No existe relación de parentesco ni conflicto de interés con empleados o directivos de dMol.

2. Documentación requerida (adjuntar):

- ☐ Certificado de estar al corriente en Hacienda y Seguridad Social.
- ☐ Escritura de constitución o documento acreditativo de representación legal.
- ☐ Declaración de ausencia de antecedentes penales.
- ☐ Código Ético o Política de Cumplimiento (si aplica).

3. Compromiso de cumplimiento:

El firmante declara haber leído y aceptado la Política de Compliance de dMol, comprometiéndose a respetar sus principios éticos y de integridad empresarial.

Firma: _____

Nombre y cargo: _____

Fecha: _____

ANEXO II

REGISTRO DE OPERACIONES SENSIBLES

- Cada operación debe ser evaluada antes de su ejecución.
- El registro se conserva durante 10 años.
- El RCN realiza una revisión semestral de todas las operaciones sensibles documentadas.

Nº Registro	Fecha	Descripción de la operación	Área responsable	Importe (€)	Riesgo identificado	Medidas preventivas aplicadas	Revisión / Autorización (RCN)	Firma Dirección
001/2025	5/2/2025	Contrato público – Ayto. Madrid	Comercial	150.000€	Cohecho / corrupción	Validación previa del RCN y cláusula anticorrupción	✓	✓
002/2025	10/3/20...	Donación material a ONG	RSC	5.000€	Imagen / transparencia	Autorización formal y registro contable	✓	✓

ANEXO III

RIESGOS PENALES

La matriz excel gestionada por el RCN se revisará anualmente.

Riesgo Penal	Proceso Afectado	Pro ba bili dad (P)	Im pa cto (I)	Nivel (NR)	Controles Preventivos	Responsa ble	Estado / Observa ciones
Corrupción y cohecho	Contratación / Ventas	2	3	6 (Alto)	Autorizaciones previas, registro de regalos, formación ética	RCN / Dirección Comercial	En seguimiento
Administración desleal	Finanzas / Compras	2	2	4 (Medio)	Revisión contable, doble firma	Dpto. Financiero / SGI	Conforme
Delitos medioambientales	Producción / Obras	2	3	6 (Alto)	Controles ambientales, licencias	SGI / Medio Ambiente	Conforme
Revelación de secretos	IT / RRHH	1	3	3 (Medio)	Control de accesos, confidencialidad	IT / RCN	Conforme
Blanqueo de capitales	Finanzas	2	3	6 (Alto)	Verificación de clientes, trazabilidad	RCN / Financiero	En revisión

ANEXO IV

CANAL ÉTICO: PROCEDIMIENTO INTERNO DE DENUNCIAS

Objetivo:

Regular el funcionamiento del Canal Ético como herramienta de comunicación confidencial para informar sobre posibles incumplimientos normativos, infracciones o conductas contrarias a la ética empresarial.

Canal habilitado: **denuncias@dmol.es**

Procedimiento:

1.Recepción:

- El RCN recibe la comunicación (correo electrónico o buzón físico).
- Se asigna un número de expediente y se confirma recepción al informante.

2.Admisión a trámite:

- Se evalúa la verosimilitud de los hechos.
- Si procede, se abre investigación interna.

3.Investigación:

- El RCN puede requerir documentación, entrevistar implicados o apoyarse en auditores externos.
- Plazo máximo de investigación: 90 días naturales desde la recepción.

4.Resolución:

- El RCN emite informe final con conclusiones y medidas propuestas.
- Si se constata infracción, se aplican las medidas disciplinarias correspondientes.

5.Confidencialidad y protección:

- Garantía de anonimato si así lo solicita el denunciante.
- Prohibición absoluta de represalias.
- Tratamiento de datos conforme al RGPD y la Ley 2/2023 sobre protección de informantes.

Documentación:

- Todas las denuncias se registran en la carpeta Compliance en la nube, con acceso limitado y se conservan por un periodo mínimo de 5 años.

ANEXO V

COMPROMISO DE ADHESIÓN DEL PERSONAL

Yo, [nombre y apellidos] , con DNI/NIE nº empleado/a de DEMOLICIÓN Y DESCONTAMINACIÓN S.L. (dMol), declaro haber recibido, leído y comprendido la Política de Compliance y el Plan de Prevención de Riesgos Penales (PPRP) de la empresa.

Me comprometo expresamente a:

- Cumplir las disposiciones, procedimientos y controles que en ellos se establecen.
- Actuar con honestidad, transparencia y respeto a la ley en el desempeño de mis funciones.
- Comunicar de buena fe cualquier irregularidad o incumplimiento del que tenga conocimiento.
- Colaborar activamente con el Responsable de Cumplimiento Normativo (RCN) en las tareas de control y supervisión.

Declaro entender que el incumplimiento de las obligaciones establecidas puede conllevar la aplicación de medidas disciplinarias conforme al régimen interno de la empresa.

En , a de de 202

Firma del empleado/a: _____

Nombre completo: _____

Departamento / Puesto: _____

Firma del Responsable de RRHH: _____