Política relativa al Sistema Interno de Información

Grupo IBM en España

Aprobada por el Órgano de Gobierno en Julio 2023

Información importante sobre este documento	
Identificación de la Norma	Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción
Ámbito territorial de aplicación de la Norma	Nacional
Apartado de las Normas de Conducta Profesional (NCP) que desarrolla	Apartado 1.3 de las NCP
Otras Normas que desarrolla	DIRECTIVA (UE) 2019/1937 relativa a la protección de las personas que informen sobre infracciones del Derecho de la UE.
Normas que sustituye	[Ninguna]
Normas que deroga	[Ninguna]
Normas relacionadas que conforman y se integran dentro de la Política	Canal de denuncias ya establecido a nivel corporativo “Employee concerns”
Unidad de negocio o función a la que afecta	Todas las unidades de negocio y funciones de IBM incluido su Perímetro de adhesión
Sujetos afectados por este documento	Todos los Miembros de la Organización así como los Socios de negocio y Terceros.
Responsable principal de su vigilancia	Responsable del Sistema Interno de Información
Fecha de aprobación	07 de julio de 2023

Conforme a lo dispuesto en la Ley 2/2023 (La Ley), de 20 de febrero, reguladora de la protección de las personas que denuncien infracciones de la normativa y de la lucha contra la corrupción.

Este documento tiene por objeto adaptar la Política que debe seguirse por parte de cada Canal de Denuncias en España y se estructura de la siguiente forma:

- Parte I: Finalidad y Ámbito de aplicación.
- Parte II: Procedimiento de gestión de informaciones. Presentación y Gestión de la Denuncia.
- Parte III: Esquema de interacción del Responsable con el canal corporativo existente "Employee Concerns"
- Parte IV: Reglas para la protección del *Informante* y del afectado.
- Parte V: Apéndice y Enlaces.

La presente Política que rige el Sistema Interno de Información y que se integra en el canal "Employees Concerns" preexistente en *IBM a nivel corporativo*, complementa e incorpora al mismo las formalidades legalmente previstas para el tratamiento de denuncias que entren dentro del ámbito de aplicación de la Ley en España.

Así pues, no anula ni sustituye el procedimiento específico que se encuentren en vigor en IBM a nivel corporativo que mantendrá su plena aplicación rigiéndose por su proceso específico.

<u>Definiciones principales:</u>

Se relacionan a continuación las definiciones de aquellos conceptos (citados en cursiva) que se utilizarán de manera frecuente en el presente documento:

- ***IBM a nivel corporativo:*** Las menciones hechas a IBM a nivel corporativos se entenderán hechas a IBM como grupo internacional.
- ***IBM:*** Las menciones hechas a IBM se entenderán hechas a las entidades del grupo mercantil IBM en España incluido su perímetro de aplicación.
- ***Miembros de la Organización/IBM:*** Órgano de Administración, empleados de IBM, trabajadores o empleados temporales o bajo convenio de colaboración, voluntarios de la Organización y el resto de las personas bajo subordinación jerárquica de cualquiera de los anteriores.
- ***Perímetro de aplicación:*** incluye a IBM y a las entidades que se relacionan en el Anexo I de esta política.
- ***Órgano de gobierno:*** Órgano de gestión social de IBM en la medida que tiene asignadas la responsabilidad y autoridad fundamental de las actividades, la gobernabilidad y las políticas. La anterior definición se entenderá "mutatis mutandi" referida al Órgano de gobierno de la correspondiente entidad del Perímetro de aplicación a los efectos de la correspondiente aplicación de la Política Sistema Interno de Información.
- ***Política Sistema Interno de Información:*** conjunto de disposiciones contenidas en este documento, en adelante, también mencionado como "Política".

- ***Canal de denuncias:*** plataforma que asegura la comunicación directa, confidencial y segura de las Denuncias presentadas.

- ***Denuncia:*** comunicación relativa a un posible *Incumplimiento* de la normativa aplicable a *IBM.*

- ***Responsable del Sistema*****:** Responsable de la gestión del Sistema Interno de información y de tramitación de expedientes de investigación.

- ***Incumplimiento:*** comportamiento, activo u omisivo, que suponga la infracción de la normativa aplicable a la Organización. Un Incumplimiento, en función de su gravedad, puede abarcar desde el mero Incumplimiento formal de un requisito incluido en una norma interna, hasta la comisión de hechos constitutivos de un delito potencialmente imputable a la Organización.

- ***Informante***: persona física o jurídica que interpone una *Consulta* o *Denuncia*. La figura del *Informante* incluye:
  - *Miembros de la Organización*: incluye trabajadores cuya relación laboral se encuentre vigente, haya finalizado o no haya comenzado, accionistas y personas pertenecientes al Órgano de Administración, voluntarios remunerados o no y trabajadores en prácticas.
  - *Socios de negocio*, así como cualquier persona que trabaje bajo la supervisión y la dirección de estos. Sujetos o personas jurídicas externas a la *Organización*, con la que esta tiene o plantea establecer una relación comercial, así como cualquier persona que trabaje bajo la supervisión y la dirección de estos.
  - *Terceros* y otros individuos como, por ejemplo, representantes sindicales.
  - Cualquier persona, con un encaje presente o futuro, en los contextos anteriores.
- ***Tercero:*** persona física o jurídica u órgano independiente de la *Organización*.
- ***Partes interesadas pertinentes:*** La figura de *Partes interesadas pertinentes* incluye:
  - Testigos, u otras personas que estén involucradas en la *Denuncia*.
  - Investigadores.
  - Familiares, representantes sindicales, y otras personas que apoyen al *Informante*.
  - Aquellos de los que se obtenga la información que motivó la interposición de una *Denuncia*.
- ***Sujetos de la Denuncia***: persona o personas físicas o jurídicas a las que se le imputa una *Denuncia* sobre un presunto incumplimiento.

Parte I: Finalidad y Ámbito de aplicación

1. Finalidad

En IBM existe la convicción de crear un entorno seguro y confidencial en la comunicación de irregularidades que afecten a IBM, para ello se informa a través de esta Política de la existencia de un entorno de equidad y garantías en la tramitación de este tipo de comunicaciones.

De esta forma, a través de la publicación de esta Política, IBM fomenta la cultura de la información y promueve la notificación de cualquier preocupación a través de su *Canal de denuncias Corporativa "Employee Concerns"* o a través de w3 (presentación en línea), Notas por correo electrónico a CSIRT, Ombudsman, Tell@IBM u otras fuentes.

2. Ámbito de aplicación:

2.1. Ámbito de aplicación objetivo:

La presente Política será aplicable a todas aquellas situaciones de *Denuncias* que tengan lugar a través del *Canal de denuncias* de *IBM a nivel corporativo*, mediante la que se informe de cualquier *Incumplimiento* de la normativa ética o cualquier otra normativa aplicable, europea o nacional, a la Organización en materia de infracciones penales, administrativas graves o muy graves y laborales.

Desde IBM se recuerda que antes de presentar una *Denuncia* deben existir la creencia razonable por el *Informante* de que la información presentada sobre presuntas infracciones o actos, omisiones o delitos al amparo de la legislación aplicable es veraz y atiende a datos fiables en el momento de la notificación. Las dudas frívolas, triviales, repetitivas o malintencionadas no se tratarán en el marco de este proceso, pudiendo tener consecuencias disciplinarias la presentación de *Denuncias* falsas intencionadamente.

2.2. Ámbito de aplicación subjetivo:

La presente Política será de obligado cumplimiento y aplicación a todos los Miembros de la Organización.

Los Miembros de la Organización deberán cumplir con su contenido, independientemente de la posición y de la función que desempeñan.

Además, a través de esta Política IBM recuerda que se brindará protección y apoyo tanto al *Informante* de buena fe como a las Partes interesadas pertinentes frente al eventual perjuicio que estos puedan sufrir por informar sobre posibles *Incumplimientos* de los que hayan tenido conocimiento.

3. Principios generales del Canal de denuncias

En todo caso, la gestión del *Canal de denuncias,* esta guiada en todo momento por los siguientes principios:

- Principio de objetividad: se deben investigar, no sólo los hechos y circunstancias que establecen y agravan la responsabilidad del sujeto de la *Denuncia*, sino también los que le eximan de ella o la extingan o atenúen.
- Principio de subsidiariedad o ultima ratio: en el caso de no proporcionar el *Informante* un medio preferente para proceder a la comunicación con el mismo, desde IBM se tendrá en cuenta el medio de comunicación menos lesivo tanto para el *Informante* como para posibles *Sujetos de la Denuncia.*

- Principio de proporcionalidad: este principio responde a la necesidad de que la sanción se ajuste a la gravedad de los hechos, evitando que ésta sea una medida desproporcionada. Nutriéndose también de los siguientes principios:
  - Principio de adecuación: las sanciones deben ser las adecuadas al fin que justifican.
  - Principio de suficiencia: las sanciones deben ser suficientes para el fin que persiguen.
  - Principio al "debido proceso": toda persona afectada tiene derecho a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento y a hacer valer sus pretensiones legítimas frente a los encargados de la investigación. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación.

  - Presunción de inocencia y al honor de las personas afectadas: la presunción de inocencia es el derecho de todo sujeto de la *Denuncia,* a ser tratado como si fuese inocente, hasta que, en su caso, se demuestre lo contrario tras la oportuna investigación, así como velar en todo momento por el respeto al derecho al honor durante la tramitación del procedimiento.

Parte II: Procedimiento de gestión de informaciones. Presentación y gestión de la Denuncia:

1. Presentación de la *Denuncia*:

Los Miembros de la Organización tienen el derecho, pero, sobre todo, la obligación de poner en conocimiento de IBM cualquier dato o indicio de que pueda haberse cometido o pueda cometerse un *Incumplimiento.*

En este sentido, existen tres opciones diferentes, tanto de forma nominativa como anónima, para presentar una *Denuncia* a través del canal interno corporativo habilitado específicamente para ello "Employee Concerns":

1.- **Nominativa:** El *Informante* puede escoger que su nombre y contacto sean compartidos con la persona que está tratando el problema.

Desde IBM recordamos la estricta confidencialidad en cualquier tipo de dato personal identificativo del *Informante* con motivo de la *Denuncia,* y por ello, animamos al *Informante* a su identificación con todas las garantías de estricta confidencialidad.

2.- **Correo electrónico:** El *Informante* puede proporcionar una dirección de correo electrónico corporativa o, si así lo prefiere su dirección personal que no permita su identificación. Si se selecciona esta última opción, la información personal no se relacionará con la solicitud ni se compartirá con IBM.

3.- **Correo postal y vía telefónica:** El *Informante* puede comunicar la *Denuncia* por correo postal o por teléfono (Talk it over).

4.- **Reunión presencial:** A solicitud del *Informante*, podrá mantenerse una reunión presencial para la presentación de la *Denuncia*. En este caso, el *Informante* puede ponerse en contacto con el administrador de "Employee Concerns" (appeals@us.ibm.com).

En este sentido, además de las vías de comunicación previstas, el *Informante* podrá designar un medio de comunicación preferente para poderle solicitar información adicional, si fuera necesario.

Según lo expuesto, cualquier comunicación verbal de las citadas anteriormente se grabarán o transcribirán en un formato accesible, duradero y seguro contando con el previo consentimiento del *Informante.*

En el caso de que el *Informante* decida usar la opción online de "Employee concerns" y facilita sus datos de contacto se le dará un numero de seguimiento.

Si por alguna razón el *Informante* no pudiera o no quisiera acceder al sistema online, podrá rellenar el formulario impreso que se facilita en el propio *Canal de denuncias.* Podrá enviarlo por correo electrónico o postal a la dirección que figura en el propio formulario.

Adionalmente, se puede presentar una denuncia a través de w3 (presentación en línea), Notas por correo electrónico a CSIRT, Ombudsman, Tell@IBM u otras fuentes.

Independientemente de la opción que elija el *Informante*, mantener la confidencialidad es el principal objetivo de IBM por ello (i) la información comunicada a IBM solo será compartida en caso de que sea estrictamente necesario, (ii) IBM prohíbe tajantemente las amenazas o actos de represalia por denunciar de buena fe posibles irregularidades o comportamientos inapropiadas.

En todo momento, se garantizará la confidencialidad de la identidad del *Informante* y de cualquier *Tercero* mencionado en la Comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo en todo caso el acceso de personal no autorizado.

En este sentido, se recuerda al personal de IBM que cuando la comunicación sea remitida por otros canales que no sean el *Canal de denuncias* o a miembros del personal no responsable de su tratamiento, deberá el receptor de esta información remitirla de inmediato al Órgano de Compliance penal de IBM, y, de no hacerlo, se considerara como una infracción muy grave y tendrá las oportunas medidas disciplinarias.

Además, IBM informa a los posibles *Informantes* que también disponen de canales externos de información ante las autoridades competentes, como la Autoridad Independiente de Protección al *Informante,* y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea, como son, entre otros, los citados en el Anexo de la presente Política.

Si bien, se recomienda el uso de los canales internos mencionados como canal preferente para la comunicación de este tipo de conductas.

2. Gestión de la *Denuncia*:

Como se indica en el siguiente esquema, lo primero es la fase de triaje en las que intervendrá un Focal Point en cada una de las áreas descritas a continuación y según la materia que se trate (a; b; y c):

a) Las *Denuncias* que le afecten personalmente o de las que haya sido testigo, como un comportamiento inadecuado o un trato injusto, serán tratadas por un Employee Concerns Partner. Algunas situaciones pueden resolverse rápidamente mediante una conversación facilitada, mientras que otras pueden requerir una investigación.

b) Denuncias sobre una infracción (o sospecha de infracción) de las Normas de Conducta Profesional de IBM que impliquen infracciones financieras o de cumplimiento, u otras conductas poco éticas o ilegales, se dirigirán a la función de Servicios de Garantía y Asesoramiento Corporativos para su tratamiento adecuado (formalmente conocida como Auditoría Interna).

c) Las denuncias relativas a una política, práctica o programa en IBM y/o a nivel corporativo se dirigirán al propietario funcional más adecuado (como el Ejecutivo de la Unidad de Negocio pertinente, RR.HH., RESO, Compras, CIO, etc.).

La *Denuncia* será analizada detenidamente y se realizará la comprobación de elegibilidad, esto es, si entra o no dentro del ámbito de aplicación de la presente Política.

1.- Si la *Denuncia* recibida no entra dentro del ámbito de aplicación seguirá el proceso habitual de denuncias implementado a nivel corporativo.

2.- Si la *Denuncia* recibida por el Focal Point de alguna de las áreas entra en el ámbito de aplicación de la presente Política (se confirma criterio de elegibilidad) este se pondrá en contacto inmediatamente con el Responsable del *Canal de Denuncias* para España (el Responsable) adjuntando la *Denuncia* en un correo electrónico con asunto "Confidencial" sin compartir la *Denuncia* con otras personas salvo, en caso de especial complejidad en los que sea estrictamente necesario y/o que se refieran a denuncias relativas a las Normas de Conducta Profesional de IBM, en cuyo caso:

- El Focal Point con el Responsable en copia en todo momento, remitirá la denuncia con asunto estrictamente “Confidencial” al “Allegation Review Board” (ARB) incluyendo al Coordinador Whistleblowing para Europa.

- El ARB revisará la denuncia remitida por el Focal Point y determinará qué área u organización es la apropiada para iniciar la investigación (Employee Concerns, Recursos Humanos, Auditoria Interna, Seguridad Corporativa, Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), IBM Corporate Legal).

- El ARB dará su opinión y consejo al Focal Point y Responsable sobre:

    (i) Proceder con la investigación.

    (ii) No seguir con la investigación.

    (iii) Dejar en suspenso hasta que se disponga de más información.

El Responsable junto con el Focal Point y el Coordinador Whistleblowing serán notificados de la posición que adopte el ARB.

Si la denuncia no revistiera especial complejidad o no fuera un incumplimiento de las Normas de Conducta Profesional el Focal Point del área podrá decidir no acudir al ARB y sólo mantener informado al Responsable todo con estrictas garantías de confidencialidad.

En cualquiera de los dos escenarios, el Focal Point del área y el Responsable trabajarán juntos durante el inicio y el proceso de investigación, en su caso, para garantizar una forma segura de operar que garantice la confidencialidad de la identidad del informante y de cualquier *Tercero* mencionado en el informe.

Concretamente, el Responsable guiará al Focal Point y le aconsejará sobre (i) el tratamiento especial que debe seguir la *Denuncia* conforme a los requisitos legales y (ii) la confidencialidad y la conservación del registro así como garantizar los derechos del afectado.

El Focal Point enviará un acuse de recibo de la *Denuncia* al *Informante*, manteniendo al Responsable en copia en todo momento, en el plazo de (7) siete días desde dicha recepción, tal y como marca la Ley.

En caso de que se solicite una *Denuncia* presencial la reunión se llevará a cabo en un plazo de (7) siete días.

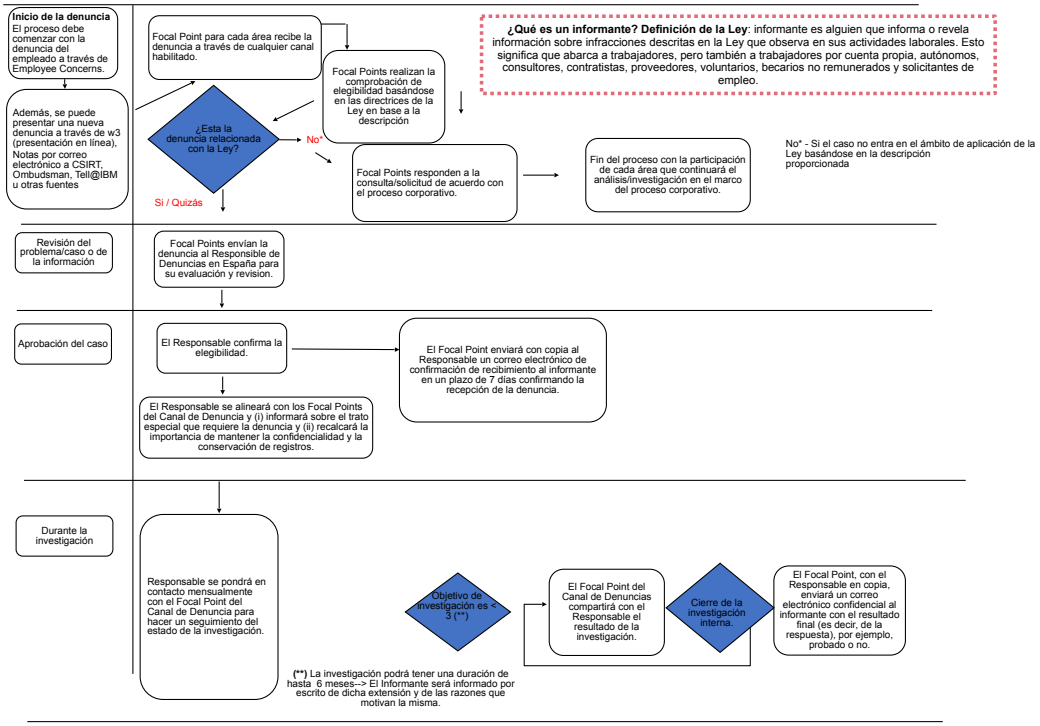
El Focal Point asignado actuará como instructor de la investigación manteniendo en todo momento al tanto al Responsable y será el encargado de mantener la comunicación con el *Informante* y, en caso necesario, solicitarle más información y proporcionarle feedback.

En un plazo máximo de (3) tres meses desde que se confirme el recibimiento de la *Denuncia*, el *Informante* recibirá un informe sobre el proceso de investigación llevado a cabo. El plazo podrá ampliarse hasta (6) seis meses si se tratará de un caso de especial complejidad. De ser este el caso, el *Informante* será informado de la extensión del plazo y de las razones que motivan dicha extensión.

Durante la tramitación del proceso de investigación, la persona afectada por la *Denuncia* tendrá derecho a ser informada debidamente de las acciones u omisiones que se le atribuyen, y a ser oída en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación y siempre garantizando la más estricta confidencialidad de cualquier dato identificativo del *Informante.*

En el caso que concluya, fuera de toda duda razonable, que la actuación de algún Miembro de IBM o *Tercero* pudiera ser, además, constitutiva de un ilícito penal, tal circunstancia será puesta de manifiesto a las Autoridades Públicas competentes para el conocimiento, como el Ministerio Fiscal o la Fiscalía Europea, la investigación de los hechos y persecución de sus autores. Tal comunicación se acompañará con todas aquellas pruebas y/o indicios recopilados y puestos de manifiesto durante el procedimiento de gestión de *Denuncias.*

Parte III: Esquema de interacción del Responsable con el canal corporativo existente



Parte IV: Reglas para la protección del *Informante* y Sujetos de la *Denuncia*:

La Ley exige que se proteja la identidad del *Informante.* Por consiguiente, la información relativa a las *Denuncias* que entran en el ámbito de aplicación de la Ley es totalmente confidencial y debe gestionarse en consecuencia. Compartir información confidencial sólo se hará entre las personas designadas al efecto, es decir, el Focal Point (instructor) y el Responsable y:

- Cuando haya comunicación con otras en funciones por la necesidad de conocimiento para la investigación, los datos confidenciales relativos al remitente cuando se conozcan se encriptarán para que no pueda identificarse al *Informante*: se suprimirán los nombres de los empleados, los títulos, los números de serie, los números de departamento, las ubicaciones o cualquier hecho, o combinación de hechos, o cualquier dato personal que pudieran revelar la identidad del *Informante.*

- Las comunicaciones sólo serán reeditadas por el Focal Point y el Responsable. Estas comunicaciones serán encriptadas.

- Se ejercerá el buen juicio y el principio de mínima intervención de otros departamentos para proteger las identidades: por ejemplo, al decidir a quién se incluye en la distribución cuando se requiera recabar información. Cuando se facilite información, debe llevar siempre la etiqueta de "IBM Confidencial", y encriptada.

- El Focal Point como instructor es responsable de garantizar que los destinatarios entienden y protegen la confidencialidad del procedimiento, y que no deben distribuirse copias indiscriminadamente entre el personal.

- El espacio de trabajo también estará protegido. Si el área de trabajo es compartida, el Focal y Point y el Responsable tomarán las medidas necesarias para garantizar que su pantalla no sea visible para los demás, que las conversaciones sean privadas y que la correspondencia y los archivos en copia impresa estén debidamente protegidos. Las copias impresas de la correspondencia y los archivos de las *Denuncias*/alegaciones se guardarán en un armario o escritorio cerrado con llave.

- Deberán seguirse las siguientes directrices de la empresa: HR113; LEG116, y 117, MKT115; Corporate Policy Letter 130 IBM Data Privacy Policy; Corp Inst 122, Security & use of Standards for IBM Emps ITCS300, IBM Worldwide Records Mgt, y IBM Guidelines for the Protection of Employee Information (URL http://w3.ibm.com/ibm/privacy/policies.html#leg), así como cualquier otra instrucción relativa al tratamiento de información personal de la empresa o información personal sensible de la empresa y la legislación de la Whistleblowing Directive.

- El nombre del remitente en copia impresa se mantendrá en un entorno separado y seguro. Salvo en ocasiones extremas y con las aprobaciones pertinentes, sólo el Responsable y el Focal Point o su reemplazo o el administrador técnico o sólo aquellos que tengan la necesidad de conocer a efectos de investigación tendrán acceso a cierta información.

- Si algún empleado, incluido el Focal Point o el Responsable, recibe presiones para revelar información confidencial o la identidad de un Informante, deberá comunicarlo inmediatamente a la dirección o al asesor jurídico de IBM en España.

- Se garantizará que las bases de datos en las que se almacenen las alegaciones y/o la identidad de los Informantes se limiten a las personas que tengan una estricta necesidad de conocerlas (es decir, el Responsable y Focal Point) y que el acceso se limite en consecuencia.

- Igualmente, IBM garantizará la presunción de inocencia y el honor del afectado durante la tramitación de toda Denuncia. El afectado tendrá derecho a ser informado de las acciones u omisiones que se le imputan y a ser oído en cualquier momento del proceso de investigación.

Parte V.- Apéndice – Enlaces:

- Ley española:
  https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513

- Whistleblower Directive:
  https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937

- Enlace para poder presentar denuncias externas:

  En materia de defensa a la competencia: Denuncia de conducta prohibida | CNMC

  En materia de infracciones tributarias: Agencia Tributaria: Denuncias
  En materia de fraudes e irregularidades vinculadas con fondos europeos: Buzón antifraude - Canal de denuncias del Mecanismo para la Recuperación y Resiliencia | Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (planderecuperacion.gob.es)

- P&R de la Comisión Europea:
  https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3442

- Whistleblower Monitor - asociación que supervisa y realiza aportaciones sobre la aplicación de la DMC: https://whistleblowingmonitor.eu/about.php

- Comentarios del grupo de trabajo de la WhistleBlower Directive: https://ec.europa.eu/transparency/expert-groups-register/screen/expertgroups/consult?lang=en&groupID=3709

- Actas de las reuniones: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3709

Anexo I

Entidades que forman parte del *Perímetro de aplicación:*

- **INTERNATIONAL BUSINES MACHINES, S.A.**

- **IBM GLOBAL SERVICES ESPAÑA, S.A.**

- **IBM GLOBAL SERVICES REDES DE ORDENADORES Y SERVICIOS, S.A.**

- **IBM INTERNATIONAL SERVICES CENTER, S.A.**