

Política y procedimiento de gestión de canal de denuncias

1 Propósito

Huawei Technologies España, S.L. (en adelante, la "Compañía" o "Huawei") desea fomentar un entorno de trabajo abierto y honesto. Como consecuencia, y conjuntamente con el compromiso permanente de Huawei de cumplir estrictamente con las correspondientes leyes locales específicas aplicables, todos y cada uno de sus empleados y directores, junto con una serie de terceros relevantes (en adelante, "Usted"), tendrán derecho a comunicar las cuestiones que aquí se definen (artículo 2), y siempre sin temor a represalias, perjuicio o trato menos favorable, siendo objeto de medidas de protección específicas.

Los propósitos de esta política son:

- Exponer el procedimiento adecuado aplicable para la recepción y tramitación, por parte de la Sociedad, de dicho tipo de comunicaciones emitidas por las personas mencionadas anteriormente ("Sistema Interno de Información");
- Proporcionar información sobre el Sistema Interno de Información de Huawei y dar publicidad al respecto.

Esta política no forma parte del contrato laboral de ningún empleado y puede ser modificada si es necesario.

Este procedimiento está sujeto a la legislación española.

2 Aplicación - Temas dentro del ámbito de aplicación del Sistema de Comunicaciones

2.1 De acuerdo con la 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, en adelante "Ley de Whistleblowing"). Esta política define el procedimiento aplicable para emitir y procesar comunicaciones sobre comportamientos o situaciones que, puedan:

- Constituir una infracción del Derecho de la Unión Europea si:
 - a. Afectan a cualquiera de los asuntos enumerados en el anexo de la Directiva de la UE 2019/1937 (la llamada Directiva Whistleblowing);
 - b. Afectan a los intereses financieros de la UE;
 - c. Tienen un impacto en el mercado interior de la UE, incluidas las infracciones de la competencia, las infracciones de las subvenciones estatales u otras de

conformidad con el artículo 26.2 del TFUE.

- Son infracciones administrativas graves o muy graves según la ley española (incluidos aquellos que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social).
- Constituyan actos delictivos según la ley española, incluyendo
 - acoso o discriminación;
 - incumplimiento de las obligaciones de confidencialidad;
 - daños a la salud y la seguridad personal.

2.2 Exclusiones: Cualquier asunto que no esté expresamente enumerado anteriormente no entra dentro del alcance del presente procedimiento de comunicaciones, en particular, pero no limitado a:

2.3.1 Temas:

La aplicabilidad de la presente regulación no se aplicará a:

- Información que afecta a información clasificada.
- Las obligaciones derivadas de la protección del secreto profesional de los profesionales del derecho
- Las infracciones en procedimientos de contratación que contengan información clasificada o que hayan sido declaradas secretas o reservadas, o aquellas cuya ejecución deba ir acompañada de medidas especiales de seguridad de conformidad con la legislación vigente, o cuando la protección de intereses esenciales para la seguridad del Estado así lo requiera.

2.3.2 Protección

La aplicabilidad del Sistema Interno de Información y la protección prevista en el presente Reglamento quedan expresamente excluidas de aquellas personas que comuniquen o divulguen:

- Información relativa a quejas sobre conflictos interpersonales o que conciernen solo al informante y las personas a las que se refiere la comunicación o divulgación.
- Información que ya está plenamente disponible para el público o que constituye meros rumores.
- Información relativa a acciones u omisiones no contempladas en los artículos 2.1 y

2.2 supra.

3 Procedimiento que debe seguirse para comunicar situaciones que entran en el ámbito de aplicación del Sistema Interno de Información

3.1 Individuos protegidos - ¿Quién puede ser un informante?

- Todos y cada uno de los directores, accionistas, miembros del consejo de administración de Huawei, miembros de cualquier órgano administrativo, directivo o supervisor, o empleados (sin importar el tipo de contrato que puedan tener);
- Cualquier persona que trabaje para o bajo la supervisión y dirección de socios, subcontratistas o proveedores;
- Consultores /autónomos;
- Cualquier persona que proporcione información obtenida en el marco de una relación laboral ya terminada, voluntarios, interns, empleados en período de formación, o incluso aquellos que aún no han iniciado una relación laboral si dicha información se obtuvo durante el proceso de contratación o durante la negociación precontractual.

Las medidas de protección, incluida la protección contra represalias, perjuicios o trato menos favorable, se aplicarán también a:

- Representantes legales de los trabajadores durante el ejercicio de sus funciones;
- Aquellos que mantengan una relación con el informante que puedan sufrir represalias, como compañeros de trabajo o familiares;
- Entidades jurídicas relacionadas en las que el informante pueda trabajar o en las que tenga alguna participación especial.

3.2. Sistema Interno de Información

Quien tenga una creencia razonable de la existencia de una infracción en los campos anteriores, en relación con Huawei o que surja de o esté relacionada con su negocio, gestión y operaciones, podría comunicar dicho asunto bien **de forma confidencial o bien de forma anónima** a través del Sistema Interno de Información que estará a disposición de todos los informantes protegidos por la ley.

El Sistema Interno de Información garantizará la **protección de datos** (cuando proceda) y la confidencialidad de:

- la **identidad de los informantes**,

- la identidad de cualquier **tercero** mencionado
- **Acciones llevadas a cabo** en el tratamiento de la comunicación

Permitir la presentación de comunicaciones:

- Por escrito (correo electrónico);
- Verbalmente (cara a cara) ante el Responsable del Sistema Interno de Información designado por Huawei (el "responsable de Huawei SII") que deberá documentarse, con el consentimiento previo del informante, a través de la grabación o transcripción de la conversación.

Una vez realizada la comunicación, se enviará un acuse de recibo al informante en un **plazo de siete días naturales**. Todas las comunicaciones serán registradas de forma privada y solo serán accesibles para la autoridad judicial previa resolución judicial.

El plazo máximo para las investigaciones y para dar respuesta al informante de la resolución será de **3 meses desde la recepción de la comunicación** (6 meses en los casos más complejos).

La **presunción de inocencia** será siempre base de la investigación realizada.

3.2.1 Responsable del Sistema Interno de Información y medios de contacto

El Sistema Interno de Información será gestionado por un Responsable (responsable de Huawei SII) designado por el consejo de administración y totalmente independiente y autónomo.

Para llevar a cabo las investigaciones específicas, el Responsable de SII de Huawei contará con la asistencia del equipo de investigación, que se constituirá de acuerdo con las disposiciones del apartado 4 a) a continuación.

El **Director de Recursos Humanos de Huawei España** ha sido nombrado "**Responsable de Huawei SII**";

Está disponible a través de:

1. Directamente concertando una reunión o
2. A través de la dirección de correo: Alertahuaweisp@huawei.com.

3.3. Canales externos y revelación pública

Con independencia del mencionado Sistema Interno de Información, Usted puede remitir el asunto a la "Autoridad Independiente de Protección del Informante" ("AAI"), o a las autoridades u organismos competentes de la comunidad autónoma bien directamente o bien

habiendo previamente comunicado dicho asunto a través del correspondiente Sistema Interno de Información de Huawei.

Además, Ud. puede hacer una revelación pública y poner a disposición del público en general la información sobre una posible infracción. En tal caso, el informador que realice una comunicación pública estará sujeto a esta norma si se cumple alguno de los siguientes requisitos:

- a) En caso de que el informante opte por realizar una comunicación pública a los organismos públicos mencionados anteriormente, ya sea previamente reportándola a través de canales internos, o directamente a través de los canales externos ya mencionados, y no se haya tomado ninguna medida adecuada dentro del plazo legal.
- b) En caso de que el informante tenga la creencia razonable de que la infracción puede constituir un peligro inminente para el interés público, en particular cuando exista una situación de emergencia o un riesgo de daños irreversibles; o haya realizado una comunicación a través de un canal externo y exista un riesgo efectivo de represalias, de destrucción de pruebas o colaboración y/o implicación inapropiadas de una autoridad con las acciones comunicadas.

3.4 Modalidades de presentación de comunicaciones

Como se expresa en el punto 3.2 supra, el Sistema Interno de Información permitirá la presentación y posterior tratamiento de comunicaciones anónimas y no anónimas. No obstante, todas las comunicaciones, ya sean anónimas o no, serán gestionadas con confidencialidad y respetando las disposiciones legales aplicables.

Al reportar comportamientos o situaciones en todo el Sistema Interno de Información, hay cierta información que Usted debe proporcionar:

1. Dependiendo de si es una comunicación anónima o no:
 - Comunicaciones no anónimas: deberá indicar su identidad (nombre y apellidos), posición e información de contacto (número de teléfono y/o dirección de correo electrónico);
 - Comunicaciones anónimas: cualquier dato de contacto anónimo para que sea posible enviarle un acuse de recibo y poder solicitarle más información durante la investigación si es necesario.
2. Aplicable a todas las comunicaciones: los hechos que desea informar (descripción de los hechos, fecha de los hechos comunicados, lugar, personas involucradas) con el respaldo de cualquier evidencia que considere relevante. Se le pedirá que proporcione todos los elementos que considere útiles para la investigación. Dichos elementos se

proporcionarán junto con su declaración, pero también se podrán comunicar posteriormente.

Además de lo anterior, también debe seguirse el procedimiento a continuación, dependiendo de si las comunicaciones se realizan oralmente o por escrito:

- **Comunicaciones orales**

Si decide informar oralmente, la declaración podrá hacerse en una reunión física organizada máximo 7 días después del acuse de recibo de su comunicación.

Las comunicaciones orales realizadas mediante reunión presencial deberán documentarse de una de las siguientes formas, con el consentimiento del informante:

(a) grabando la conversación en un formato seguro, duradero y accesible; o

b) mediante una transcripción completa y precisa de la conversación realizada por el personal responsable de tratarla.

Sin perjuicio de los derechos que corresponden a la normativa de protección de datos, se ofrecerá al comunicante la oportunidad de comprobar, rectificar y aceptar la transcripción mediante la firma de esta.

- **Escrito**

Por medios electrónicos habilitados a tal efecto conforme al artículo 3.2.1.

Ya sea que el informe se haga por escrito u oralmente, su identidad permanecerá confidencial dentro de Huawei, durante todo el procedimiento de denuncia de irregularidades y en la mayor medida posible. La Sociedad seguirá estando facultada para remitir directamente el informe a las autoridades competentes si los hechos comunicados son particularmente graves y si así lo exige la ley.

4 Procedimiento aplicable para el tratamiento de las comunicaciones realizadas a través del Sistema Interno de Información

El Sistema Interno de Información es un sistema puesto en práctica para permitir la comunicación de determinadas infracciones.

Independientemente del medio que haya utilizado, entre los enumerados anteriormente en el artículo 3.4, al recibir su comunicación se aplicará el siguiente proceso:

- a. Constituir la comisión de investigación.** Se creará una comisión para procesar la comunicación y proceder con la investigación. Este equipo gestionará el Sistema Interno de Información en el marco de la investigación específica y estará compuesto por los siguientes miembros: Responsable de SII de Huawei, una persona del Departamento de Compliance, una persona de Legal y una persona del Departamento de Recursos Humanos. Las personas específicas para componer este equipo serán elegidas directamente por el Responsable de SII de Huawei y siempre se asegurará de que ninguna persona afectada por los hechos informados forme parte de este equipo, y de que no haya conflicto de interés para ningún miembro de este. Alternativamente, para casos de acoso laboral o sexual, el equipo de investigación estará compuesto por los miembros definidos en los protocolos específicos.
- b. Acuse de recibo de su comunicación.** Se le informará, por escrito, de la recepción y del plazo previsible necesario para el examen de su admisibilidad en un plazo de 7 días a partir de la recepción de su comunicación. En cualquier caso, dicho acuse de recibo de su comunicación nunca se interpretará como una confirmación de su admisibilidad. Para ser admisible, la comunicación se ajustará a las modalidades de presentación de comunicación establecidas en los artículos 2 y 3 supra.
- c. Análisis preliminar de la información comunicada.** La comisión de investigación llevará a cabo una evaluación inicial para determinar el alcance de cualquier investigación. Dicha evaluación inicial tiene por objeto garantizar que la comunicación entre en el ámbito determinado en el artículo 2 supra.
- d. Comienzo de la investigación.** Cuando los hechos comunicados cumplan con los requisitos establecidos en el artículo 2 de esta política, el Responsable de SII iniciará una investigación para verificar los hechos comunicados. Si el Responsable de SII considera que el asunto comunicado no será objeto de ninguna otra verificación, cerrará el expediente. Si el asunto comunicado está relacionado con un asunto distinto al establecido en el artículo 2 de esta política, el Responsable de SII lo procesará de conformidad con la ley aplicable.
- e. Verificación.** Si es necesario, se le solicitará que proporcione cualquier elemento adicional, o prueba, para cumplimentar un procesamiento adecuado de la comunicación.
- f. Entrevistas.** Durante la investigación, según sea el caso, Usted y cualquier otro empleado o director pueden ser entrevistados por el equipo de investigación (el plazo promedio para una investigación es de aproximadamente 3 meses a partir de la fecha de acuse de recibo de su informe). Las entrevistas dirigidas por la Compañía son de carácter no coercitivo. Cuando sea apropiado, se redactará un informe al final

de la entrevista y tendrá la oportunidad de leerlo, y hacer cualquier comentario si es necesario antes de firmarlo.

- g. La Compañía le mantendrá informado regularmente** del progreso de cualquier investigación resultante por correo electrónico hasta el "cierre" de dicha investigación y hará una evaluación inicial de la comunicación.
- h. La persona afectada por la comunicación** también será informada de manera oportuna.
- i. Al final de la investigación**, se elaborará **un informe oficial** para registrar: i) todos los hechos y pruebas reunidos, tanto inculpativos como exculpativos, para establecer o eliminar la sospecha, ii) así como el método seguido. El informe concluirá sobre las medidas que deben adoptarse. Este informe se transmitirá al Director General de la Sociedad.
- j. Si se prueba que las alegaciones efectuadas son ciertas** en el informe de investigación y la persona afectada por la comunicación es susceptible de ser responsable de los hechos alegados:
 - Se podrán aplicar sanciones disciplinarias adecuadas si se cumplen las disposiciones del derecho laboral, y dependiendo de la gravedad de los hechos comunicados, de acuerdo con lo dispuesto en el Reglamento Interno y el Convenio Colectivo aplicable;
 - En su caso, se aplicarán sanciones comerciales o contractuales, adecuadas a la gravedad de los hechos comunicados, al tercero o terceros interesados;
 - Y/o se iniciarán acciones legales según lo exija la ley.

La decisión final con respecto a tales acciones será tomada por el Administration Team (AT). El Director General y la alta dirección de la Compañía se mantendrán informados durante todo el procedimiento de investigación, cuando proceda y en el respeto de las obligaciones de confidencialidad y la regulación de datos personales, especialmente en lo que respecta a cuestiones de alta sensibilidad, manteniendo siempre la confidencialidad legalmente prevista.

La Compañía también puede tomar otras acciones internas sobre la base del informe de investigación, cuando proceda, como una actualización de su mapa de riesgos de cumplimiento o de algunas normas y reglamentos internos y/o una comunicación de seguimiento sobre el asunto investigado y sus consecuencias.

A veces, la necesidad de confidencialidad puede impedir que Usted tenga detalles específicos con respecto a cualquier investigación o acción disciplinaria que pueda tomarse contra cualquier miembro del personal relevante como resultado. También debe tratar como confidencial cualquier información que pueda recibir sobre la investigación.

Cuando los hechos pudieran constituir un delito, la Empresa deberá remitir dicha información inmediatamente al Ministerio Fiscal. En caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirán a la Fiscalía Europea.

Finalmente, insistiendo en lo siguiente, cualquier divulgación bajo esta política:

- **debe hacerse de buena fe, con una creencia razonable de que las alegaciones son sustancialmente verdaderas:** incluso si los hechos son finalmente inexactos o no dan lugar a ninguna medida,
- **no expondrán al informante a ninguna sanción disciplinaria o legal;**
- **no se hará por razones despectivas indebidas o de mala fe;**
- **no se harán para obtener ganancias financieras directas.**

La Compañía tiene como objetivo fomentar la apertura y apoyará a cualquier miembro del personal de la Compañía o a terceros que presenten comunicaciones genuinas de acuerdo con esta política.

5 Alcance limitado y naturaleza específica del Sistema Interno de Información

Esta política debe utilizarse exclusivamente para reclamaciones relacionadas con el alcance detallado en el artículo 2. Si no está seguro de si algo está dentro del alcance de esta política, debe consultar a su Manager o al Compliance Officer de Huawei España.

Quedará a discreción del Responsable de SII determinar el curso de acción apropiado después de dicha divulgación.

Cualquier persona que utilice este canal de comunicación de irregularidades es responsable de la aplicación adecuada de esta política y debe asegurarse de que la utiliza para revelar cualquier verdadero peligro o infracción sospechada.

6 Datos personales tratados en el marco del sistema de denuncia de irregularidades

Huawei España cumple con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, 2016 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos ("RGPD") y también con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Como consecuencia de ello, las actividades de procesamiento de datos personales que se llevan a cabo en el curso del sistema de comunicación de irregularidades y el proceso de verificación se detallan en el registro de procesamiento de datos de la empresa correspondiente (Inventario de datos) y han sido objeto de una evaluación de impacto en la protección de datos (DPIA).

El propósito de las actividades de procesamiento es cumplir con las obligaciones de Huawei establecidas en la ley mencionada anteriormente, y también:

- acoso o discriminación moral;
- incumplimiento de las obligaciones de confidencialidad;
- violaciones graves de la salud y la seguridad personal.

El Titular de las actividades de tratamiento en el ámbito del Sistema Interno de Información es: Huawei Technologies España S.L., CIF número B84136464, Calle Isabel Colbrand 22, 28050 Madrid, España. También puede comunicarse con el controlador y el DPO en {<https://www.huawei.com/es/personal-data-request>}

Más detalles sobre las actividades de procesamiento y sus derechos están disponibles en el "Aviso de privacidad del sistema de denuncia de irregularidades" disponible en el sitio web de W3.

7 Derechos de la persona afectada por la comunicación

Además de la información mencionada anteriormente, la persona la persona afectada por la comunicación deberá ser informada oportunamente de la comunicación (i) por carta certificada enviada a su dirección postal personal y/o (ii) por correo electrónico protegido a su dirección de correo electrónico profesional.

En tal caso, se proporcionará la siguiente información a la persona objeto de la comunicación:

- La identidad del responsable de SII de Huawei
- Los hechos comunicados
- La existencia de sus derechos otorgados por la normativa española y europea de protección de datos (es decir, derecho de acceso, derecho de rectificación y derecho de oposición) y los datos de contacto del responsable del ejercicio de dichos derechos.

En caso necesario, la persona objeto de la comunicación sólo podrá ser informada después de un período razonable de tiempo necesario para obtener las pruebas del informe y adoptar las medidas de protección necesarias o apropiadas.

Durante el procedimiento de tramitación del informe (el expediente), la persona objeto de la comunicación tendrá derecho a:

- Presunción de inocencia
- Defender su interés por cualquier medio legal disponible para impugnar todo o parte de los hechos comunicados contra él
- Acceder al expediente según condiciones legales
- Salvaguardar su identidad de acuerdo con los términos legales
- La confidencialidad de los hechos y detalles del procedimiento

En caso de entrevista organizada por Huawei según el artículo 4 f), se aplicarán los siguientes derechos:

- derecho a ser asistido por un abogado y por un intérprete cuando proceda;
- derecho a permanecer en silencio y posibilidad de finalizar la entrevista si así lo desea y cuando lo desee (La empresa sigue estando facultada para deducir cualquier conclusión del ejercicio de tales derechos).

Las entrevistas dirigidas por la Compañía son de carácter no coercitivo. Al final de la entrevista se redactará un informe y la persona objeto de la comunicación tendrá la oportunidad de leerlo, y hacer los comentarios que estime necesarios, antes de firmarlo.

En cualquier caso, las personas objeto de la comunicación no tienen derecho a obtener la información relativa a la identidad de los autores de las comunicaciones.

8 Seguridad y confidencialidad

Huawei tratará las comunicaciones con el máximo grado de confidencialidad en cada etapa de su procesamiento y revisión.

En particular, se proporcionarán las siguientes garantías:

- Todo miembro del personal y/o referente dedicado al Sistema Interno de Información está sujeto a una obligación documentada y reforzada de confidencialidad por medio de compromiso de confidencialidad firmado al efecto. Cualquier violación de la confidencialidad puede llevar a una sanción disciplinaria.
- El acceso al informe está restringido a las personas autorizadas (exclusivamente el responsable de SII de Huawei y la comisión de investigación que se ocupa directamente del Sistema Interno de Información) que precisen por sus funciones tener un acceso de identificación, y:
 - o Las contraseñas se actualizarán periódicamente;
 - o El acceso al sistema se registrará, supervisará y actualizará periódicamente.

Se informa a toda persona que presente una alerta de que su identidad se mantendrá confidencial en todas las etapas del proceso y no se revelará al personal objeto de la comunicación.

Quedan expresamente prohibidos los actos de represalia, incluidas las amenazas de represalia y los intentos de represalia contra las personas que presentan una comunicación conforme a lo dispuesto en la presente ley.

En consecuencia, el autor de la comunicación realizada en cumplimiento de la política tiene la garantía de que no sufrirá la divulgación de la información en el marco del presente procedimiento.

8.1 Represalias

Represalia se refiere a cualquier acto u omisión prohibido por la ley, o que, directa o indirectamente, conlleve un trato desfavorable que coloca a las personas que las sufren en una situación de desventaja particular con respecto a otra persona en el contexto laboral o profesional por haber divulgado cualquier información en el ámbito del artículo 2 anterior y de conformidad con las disposiciones del presente documento o con las disposiciones de la Ley de Whistleblowing.

El período de protección contra las represalias será de dos años. Si alguien ha sufrido alguna represalia después de dicho plazo por las razones anteriores, tendrá derecho a solicitar una prórroga a las autoridades competentes, que podrán prorrogar o no este período de protección.

Ejemplos de represalias son:

- a) Suspensión del contrato de trabajo, despido o terminación de la relación laboral o estatutaria.
- b) Daño, incluyendo pérdida de reputación o económica, coerción, intimidación, acoso u ostracismo.
- c) Evaluación o referencias negativas sobre el trabajo o el desempeño profesional.
- d) Inclusión en listas negras o difusión de información en un ámbito sectorial específico, que dificulte o impida el acceso al empleo o la contratación de obras o servicios.
- e) Negación o cancelación de una licencia o permiso.
- f) Denegación de training.
- g) Discriminación, o trato desfavorable o injusto.

9 Tiempo de retención

9.1 Si el informe no está cubierto por el alcance del Sistema Interno de Información (véase el Artículo 2 de este documento) será destruido, o anonimizado cuando proceda, inmediatamente.

9.2 Si el informe está cubierto por el alcance del Sistema Interno de Información, los datos relacionados con el informe se conservarán durante el período de tiempo apropiado y limitado tal y como se detalla en el "Aviso de privacidad del sistema de denuncia" disponible en el sitio web de W3.

En particular, todos los datos personales recopilados por la Compañía en relación con su Sistema Interno de Información están sujetos a la siguiente duración de almacenamiento:

- (i) En caso de que no sea necesario investigar, los datos personales se eliminarán inmediatamente.
- (ii) En caso de que los datos personales se consideren personales de categorías especiales, también se eliminarán inmediatamente.
- (iii) En caso de que la información se considere no veraz, se eliminará inmediatamente.
- (iv) En caso de que no se inicie ninguna investigación, los datos personales se conservarán 3 meses después de la comunicación.
- (v) En cualquier caso, los datos personales solo se conservarán durante el tiempo esencialmente necesario.

10 Control y revisión de esta política

Huawei España es responsable de la interpretación de esta política, así como de supervisar su despliegue y su correcta aplicación.

La empresa se reserva el derecho de modificar este documento y procedimiento de vez en cuando o según sea necesario en virtud de las leyes y reglamentos de España. Esta Política se revisará cuando sea necesario.

11 Others

Los departamentos responsables de este fichero son Legal y Quality, Business Process & IT Dept, que se reservan el derecho de interpretar y actualizar esta política.

Esta política entra en vigor a partir de 13 de junio de 2023 y tiene una validez de 5 años.