

Índice

| | | |
|-------|---|---|
| 1 | Propósito y objetivo | 2 |
| 2 | Conectar con nosotros | 2 |
| 3 | Procedimiento y responsabilidades | 2 |
| 3.1 | Protección de datos, protección del informante y confidencialidad | 2 |
| 3.1.1 | Designación del equipo instructor | 3 |
| 3.2 | Protección de la persona investigada..... | 3 |
| 3.3 | Etapas del proceso | 3 |
| 3.3.1 | Acuse de recibo y análisis preliminar | 3 |
| 3.3.2 | Investigación con el equipo instructor | 4 |
| 3.3.3 | Informe de conclusiones | 4 |
| 3.4 | Situaciones con indicios de un delito penal | 4 |
| 3.5 | Plazos de gestión para casos de compliance..... | 4 |
| 4 | Documentos | 5 |
| 5 | Registros | 5 |
| 6 | Control de cambios..... | 5 |

1 Propósito y objetivo

El propósito de este documento es proporcionar una guía para aquellas personas que deseen informar sobre posibles irregularidades en nuestra empresa. Se detalla el procedimiento para llevar a cabo este proceso, los principios básicos y derechos del informante, cómo tratamos la información y cómo nos comunicamos en situaciones de este tipo.

2 Conectar con nosotros

Para reportar hechos o actos que los empleados directos o indirectos, así como otras partes interesadas¹, consideren o puedan considerar relevantes para la empresa, se han establecido unos canales de comunicación. Estos permiten transmitir esta información al/la Responsable del Sistema de Información local que en nuestra empresa es asumido por el/la Oficial de Cumplimiento local (Compliance Officer) y el equipo instructor designado para cada caso.

- Aplicación del informante (véase la website the Menshen: www.menshen.com)
- Dirección de correo electrónico del canal compliance (compliance@menshen.com)
- Teléfono (directo al Compliance Officer)
- Carta (a la atención del Compliance Officer)

Cabe destacar que, además de los canales de información internos mencionados anteriormente, existe la opción de ponerse en contacto directamente con las autoridades competentesⁱ (véase el listado de la nota al final de este documento).

3 Procedimiento y responsabilidades

Todos los posibles casos de cumplimiento reportados son gestionados por el/la Responsable del Sistema de Información de la planta correspondiente, quien también es responsable de asegurar que todos los casos queden registrados en un informe de incumplimiento y sean reportados al/la Compliance Officer del Grupo Menshen.

3.1 Protección de datos, protección del informante y confidencialidad

Nuestros canales de información aseguran que solo las personas autorizadas para recibir y procesar incidentes, tengan acceso a la información recibida a través de dichos canales.

El/La Responsable del Sistema de Información local asegura la confidencialidad² de la identidad de las siguientes personas:

- la persona que proporciona la información
- la(s) persona(s) que son objeto de un incidente
- otra(s) persona(s) mencionada(s) en el informe

¹ (i) trabajadores por cuenta ajena; (ii) autónomos; (iii) accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa; (iv) plantilla de contratistas, subcontratistas y proveedores; e incluso (vi) voluntarios, becarios y trabajadores en periodos de formación con o sin retribución.

² MENSHEN IBER S.L.U. será el responsable del tratamiento de los datos y tratará la información personal de conformidad con la normativa de protección de datos. Puede obtener más información sobre este tratamiento de datos en [www.menshen.com].

3.1.1 Designación del equipo instructor

El/La Responsable del Sistema de Información encargado/a de procesar un caso garantiza que la identidad de las personas mencionadas anteriormente solo sea conocida por ellos y por los gestores designados para dicho caso. Los gestores externos deben firmar, junto con el contrato pertinente, un acuerdo de confidencialidad como colaboradores autorizados para el tratamiento de los datos del Sistema Interno de Información. Por su parte, los gestores internos deben firmar la aceptación de su nombramiento como Gestores Internos del Sistema Interno de Información de Menshen Iber.

El requisito de confidencialidad de la identidad se aplica siempre, independientemente de si el/la Responsable del Sistema de Información es responsable o no de gestionar el caso denunciado.

3.2 Protección de la persona investigada

En principio, toda persona implicada y bajo investigación por un posible incidente de cumplimiento está sujeta a la presunción de inocencia. Al procesar un caso de incumplimiento, se debe garantizar la protección de los datos personales. Además, la persona investigada tiene el derecho de ser informada de las acciones u omisiones de las que se le acusa y de ser escuchada en cualquier momento.

3.3 Etapas del proceso

3.3.1 Acuse de recibo y análisis preliminar

Si la persona que proporciona la información se identifica con sus datos de contacto, recibirá confirmación de que el informe ha sido recibido. Tras el análisis preliminar, el/la Responsable del Sistema de Información le comunicará al informante si se archiva su denuncia y se cierra el caso, o si se abre una investigación, dándole la oportunidad de aclarar directamente cualquier consulta que pueda surgir durante el proceso.

Esto no es posible para los casos que lleguen de forma anónima, excepto de manera indirecta cuando se utiliza la aplicación para informantes de la web. Si el informante utiliza la aplicación, debe guardar el número de informe que el sistema le proporciona al reportar el caso. Este número puede ser introducido en la aplicación en cualquier momento para conocer el estado del caso o para proporcionar información adicional.

Si el/la Responsable del Sistema de Información tiene alguna pregunta mientras procesa un incidente que ha llegado a través de la aplicación, puede plantearla en la misma aplicación. Sin embargo, no es posible determinar si estas son leídas por la persona que informa, ya que la aplicación garantiza que las entradas realizadas no pueden ser rastreadas.

Si la información sobre un posible incidente de cumplimiento llega a la empresa a través de personas que no están oficialmente designadas para tramitar este tipo de incidencias, el procedimiento será el siguiente:

El/la Responsable del Sistema de Información notifica a la persona informante que está obligada a mantener un secreto absoluto acerca de esta información y le solicita la firma del protocolo redactado para tal caso. De esta forma, queda advertida de que el incumplimiento de la obligación de confidencialidad está tipificado como infracción muy grave, y se aplicarán medidas conforme a la legislación laboral.

3.3.2 Investigación con el equipo instructor

La investigación de un caso de denuncia consiste en un proceso estructurado y confidencial para examinar las alegaciones reportadas. Este proceso se inicia con la evaluación de la denuncia por el responsable junto con el equipo instructor designado para determinar su veracidad y gravedad. A continuación, se recopilan evidencias relevantes mediante entrevistas, revisión de documentos y otras técnicas de investigación. El objetivo es esclarecer los hechos, identificar posibles infracciones y determinar si se han violado políticas internas o leyes aplicables. Durante todo el proceso, se garantiza la protección del denunciante contra represalias y se mantiene la confidencialidad de la información.

3.3.3 Informe de conclusiones

Al finalizar la investigación, se elabora un informe detallado con los hallazgos y recomendaciones para la toma de decisiones y, si es necesario, la implementación de medidas correctivas o disciplinarias. Este informe de conclusiones se entrega al Responsable de Recursos Humanos y se eleva a la Dirección. El informe incluye un resumen de la denuncia, el análisis de las evidencias recopiladas, entrevistas realizadas y cualquier documentación relevante. También se detallan las conclusiones obtenidas y se sugieren acciones concretas para resolver las irregularidades identificadas. El Responsable de Recursos Humanos revisa el informe y coordina con el equipo directivo para decidir las acciones a seguir, asegurando que se cumplan todas las políticas internas y leyes aplicables. La Dirección evalúa las recomendaciones y, de ser necesario, ordena la ejecución de medidas correctivas o disciplinarias, así como la implementación de cambios en los procesos internos para prevenir futuras irregularidades. Todo el proceso se documenta meticulosamente para garantizar la transparencia y la responsabilidad en la gestión de la denuncia.

3.4 Situaciones con indicios de un delito penal

Si, durante el análisis de un caso de incumplimiento, surgen pruebas y se acumulan indicios que apuntan a un delito penal, la fiscalía correspondiente será informada por el/la Compliance Officer.

3.5 Plazos de gestión para casos de compliance

Se establecen los siguientes plazos para la tramitación de casos de compliance:

- El/la Responsable del Sistema de Información debe confirmar por escrito la recepción de la comunicación al Informante a más tardar 7 días naturales después de recibirla.
- La investigación de cada caso de cumplimiento debe comenzar no más tarde de 15 días naturales después de recibir la información. El/la Responsable del Sistema de Información local es responsable de documentar la recepción de la información y el inicio de la investigación con la fecha y, si es posible, la hora de la transacción.
- Cada incidente de cumplimiento debe ser resuelto en un plazo de tres meses. Se pueden hacer excepciones en casos complejos. Si fuese necesario, el tiempo de procesamiento se puede extender por tres meses adicionales.

El/la informante recibirá por escrito una respuesta sobre el caso en un plazo de tres meses. En esta respuesta se incluirá la notificación del estado de su denuncia o comunicación: si se ha archivado, si se ha abierto una investigación, si la investigación sigue en curso, o si la investigación se ha terminado, se han tomado medidas y se ha cerrado el caso.

4 Documentos

- M01_PI_03_Compliance-Management_INT

5 Registros

- Notas de Compliance
- NDA gestores externos del Sistema Interno de Información
- Contrato para Gestor Externo encargado del tratamiento de datos del Sistema Interno de Información
- Carta de aceptación Gestores Internos

6 Control de cambios

| Fecha | Índice | Descripción del cambio |
|-------|--------|------------------------|
| | | |
| | | |
| | | |
| | | |

ⁱ Listado de Canales externos de Información

- Oficina Europea de Lucha contra el Fraude Unión Europea (OLAF):

https://fns.olaf.europa.eu/main_es.htm

- Fiscalía Europea (EPPO):

<https://www.eppo.europa.eu/es/form/eppo-report-a-crime>

- Autoridad Independiente de Protección del Informante (AAI):

Pendiente de creación del canal

- Servicio Nacional de Coordinación Antifraude (SNCA):

consultasantifraude@igae.hacienda.gob.es

- Oficina Antifraude de Cataluña (OAC):

- Buzón antifraude - Canal de denuncias del Mecanismo para la Recuperación y Resiliencia

<https://planderecuperacion.gob.es/buzon-antifraude-canal-de-denuncias-del-mecanismo-para-la-recuperacion-y-resiliencia>