GRAN HOTEL ERCILLA SA

Política de Gestión del Sistema Interno de Información

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

Control de versiones

	NOMBRE	FUNCIÓN	FECHA
Redactado por:	GESPRODAT S.L.	Asesor externo	03/11/2023
Verificado por:			
Aprobado por:			

Control de modificaciones

VERSIÓN	FECHA	MODIFICADO POR	MODIFICACIÓN REALIZADA

Normas, Leyes y Reglamentos aplicables

NOMBRE DE LA NORMA, LEY O REGLAMENTO	ACCESO
REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS UE 2016/679	Link
Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales	Link
DIRECTIVA (UE) 2019/1937 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión	Link
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.	Link

Índice

Control de versiones 2
Control de modificaciones 2
Normas, Leyes y Reglamentos aplicables 2
Índice 3
Objeto 5
Sujetos obligados 5
Sector Público 5
Sector Privado 6
Representación legal de los trabajadores 7
Alcance 7
¿De qué se puede informar? 7
¿Cuál es el contenido de una información? 7
¿Qué se protege? 7
¿Quién puede utilizar el sistema de información? 8
¿A quién se protege? 8
Requisitos del sistema de información 9
Publicidad en la página web 10
Derechos de los informantes 10
Derechos de las personas afectadas 11
Responsable del sistema 11
Uso indebido del canal 12
Evaluación, revisión y aprobación de la política 12
PROCEDIMIENTO 13
Canales de información 13
Canal interno 13
Canal externo 13
Revelación Pública 14
Identificación del Responsable del sistema de información 15
Nombramiento, destitución o cese 15
Contenido de la información 16
Registro de informaciones 16
Medidas de protección 17
Prohibición de represalias 17

Medidas de apoyo 18
Fases del procedimiento 19
1. Recepción y análisis preliminar de la denuncia 19
2. Fase de Archivo o Admisión de la denuncia 19
3. Fase de Instrucción 20
4. Fase de Resolución y Medidas 21
Diagrama de Funcionamiento 23
Protección de datos de carácter personal 25
Licitud del tratamiento 25
Transparencia e Información 25
Derechos de los interesados 26
Acceso a los datos 26
Minimización de datos 27
Datos especialmente protegidos 27
Conservación de los datos 27
Confidencialidad 28
Registro de actividades de tratamiento 28
Análisis de riesgos 29
¿CÓMO IMPLEMENTAR ESTA POLÍTICA? 30
Anexos asociados 32
Anexo I: Designación del Responsable del Sistema. 32
Anexo II: Destitución o cese del Responsable del Sistema 33
Anexo III: Información web sección Sistema de Información Interno 34
Anexo IV: RGPD reunión presencial 36
Anexo V: Información a trabajadores (infografía) 37

Objeto

El objeto del presente protocolo es establecer un sistema eficaz de gestión, investigación y respuesta de las informaciones recibidas que sean interpuestas por las personas incluidas en el ámbito subjetivo del mismo ante la/s persona/s y órgano previamente designado/a/as a tales efectos, como consecuencia de la comisión de hechos contrarios a la legalidad.
Este sistema interno será un cauce preferente para informar y se tratará de manera efectiva y sin riesgo de represalias.
De esta manera, se instaura en GRAN HOTEL ERCILLA SA un proceso reglado de obligado seguimiento que comprenderá la actuación a llevar a cabo desde el momento que se recibe una información hasta que, en su caso, la infracción cometida sea sancionada, incluyendo, asimismo, la evaluación de la incidencia y la proposición de medidas a implantar en favor del informante o de aquellas personas que se vieran afectadas, en el supuesto en el que sea considerado necesario.
Este protocolo tiene por finalidad otorgar una protección adecuada al informante sobre las represalias que puedan sufrir y fomentar la cultura de la información o comunicación como mecanismo para la prevención y detección de amenazas de interés.

Sujetos obligados

SECTOR PÚBLICO

- La Administración General del Estado, las Administraciones de las comunidades autónomas y Ciudades con Estatuto de Autonomía y las Entidades que integran la Administración Local.
- Los Organismos y Entidades públicas vinculadas o dependientes de alguna Administración pública, así como aquellas otras asociaciones y corporaciones en las que participen las Administraciones y organismos públicos.
- Las Autoridades Administrativas Independientes, el Banco de España y las Entidades gestoras y Servicios comunes de la Seguridad Social.
- Las Universidades públicas.
- Las Corporaciones de Derecho público.
- Las fundaciones del sector público.

- Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de entidades mencionadas señaladas sea superior al 50 por 100 o en los casos en que, sin superar ese porcentaje se trate de un Grupo de Sociedades.
- Los órganos constitucionales, los de relevancia constitucional e instituciones autonómicas análogas a las anteriores.

SECTOR PRIVADO

- Personas físicas o jurídicas que tengan contratados **50 o más trabajadores.**
- Personas jurídicas que entren en el ámbito de aplicación de los actos de la Unión Europea en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente, con independencia del número de trabajadores.
- Personas jurídicas que desarrollen en España actividades a través de **sucursales o agentes**, o mediante prestación de servicios sin establecimiento permanente.
- Partidos políticos, sindicatos, organizaciones empresariales y fundaciones creadas por ellos siempre que reciban o gestionen fondos públicos

Grupos de Empresas

En el caso de **grupos empresariales** (según art. 42 del Código de Comercio), atenderá a lo siguiente:

- La sociedad dominante aprobará una política general relativa al Sistema interno de información.
- La sociedad dominante asegurará la aplicación de sus principios en todas las entidades que lo integran, con las modificaciones o adaptaciones que resulten necesarias en cada sociedad integrante para el cumplimiento de la normativa aplicable en cada caso.
- El Responsable del Sistema podrá ser uno para todo el grupo, o bien uno para cada sociedad integrante del mismo.
- El Sistema interno de información podrá ser uno para todo el grupo.
- Será admisible el intercambio de información entre los diferentes Responsables del Sistema del grupo, si los hubiera, para la adecuada coordinación y el mejor desempeño de sus funciones.

Representación legal de los trabajadores

Conforme al artículo 64 del Estatuto de los Trabajadores, el presente procedimiento deberá ser comunicado a la representación legal de las personas trabajadoras en cumplimiento de su derecho a ser informados y consultados por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores.

Alcance

¿DE QUÉ SE PUEDE INFORMAR?

El ámbito de aplicación objetivo no se limita a las infracciones del ordenamiento jurídico europeo, sino que se incluyen también los incumplimientos del derecho nacional.

A título enunciativo y no limitativo, se puede informar sobre infracciones en los siguientes ámbitos:

- Laboral (acoso, privacidad, igualdad, discriminación)
- Finanzas (robo, soborno, blanqueo, malversación)
- Medio ambiente (residuos, vertidos, contaminación)
- Etc.

¿CUÁL ES EL CONTENIDO DE UNA INFORMACIÓN?

Las personas que realicen comunicaciones sólo deberán proporcionar aquella información específica y objetiva que sea necesaria para determinar si el objeto de su comunicación es relevante a los efectos de la denuncia.

En este sentido, los interesados deberán evitar, salvo que sea indispensable para entender el alcance de su comunicación, facilitar datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como datos biométricos, datos relativos a la salud o datos relativos a la vida sexual u orientaciones sexuales del interesado o informante, las personas afectadas o terceros.

¿QUÉ SE PROTEGE?

Las informaciones y comunicaciones sobre infracciones de derecho comunitario, así como sobre infracciones penales y administrativas graves o muy graves. Además, garantiza la protección de todas las personas que informen/comuniquen sobre cualquier infracción o irregularidad de derecho comunitario detectada.

¿QUIÉN PUEDE UTILIZAR EL SISTEMA DE INFORMACIÓN?

En este sentido, se distinguirá el ámbito de aplicación plena, para las personas físicas que tengan la condición de informantes, y un ámbito de aplicación parcial para las personas que, sin ser informantes, por prestarle asistencia o formar parte de su entorno, pudieran ser objeto de represalias y por ello deban contar con algún régimen de protección.

Así, tendrán la consideración de "informantes", sólo las personas físicas, a título individual, que hayan obtenido informaciones sobre infracciones en un contexto laboral o profesional, en un sentido amplio.

De manera que se extiende la protección a todas aquellas personas que tienen vínculos profesionales o laborales con entidades tanto del sector público como del sector privado, y también a aquéllas que ya han finalizado su relación profesional, o sean becarias, voluntarias, desarrollen trabajo en prácticas o en período de formación, e incluso personas que participan en procesos de selección; o a personal de contratistas, entre otras.

¿A QUIÉN SE PROTEGE?

Las personas que mantengan un vínculo con la organización, en particular:

- Personas autónomas, accionistas, partícipes, miembros del órgano de administración, dirección o supervisión de una empresa; plantilla de contratistas, subcontratistas y proveedores; con relación finalizada o por comenzar, e incluso voluntarios, becarios y trabajadores en periodos de formación con o sin retribución.
- Personas físicas que, en el marco de la organización en la que preste servicios el informante, asistan al mismo en el proceso
- Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante.
- Personas jurídicas para las que el informante trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa

Requisitos del sistema de información

El sistema de información, cualquiera que sea su forma de gestión, deberá:

- Permitir a todas las personas comunicar información sobre las infracciones.
- Estar diseñado, establecido y gestionado de forma segura, de manera que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación.
- Permitir la presentación de comunicaciones por escrito o verbal, o de ambos modos.
- Integrar los distintos canales internos de información que pudieran establecerse dentro de la organización.
- Garantizar que las comunicaciones puedan tratarse de manera efectiva.
- Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos.
- Contar con un responsable del sistema.
- Contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno de información[1].
- Establecer las garantías para la protección de los informantes.

En caso de externalizar el sistema con terceros, se exigirá garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones. El tercero externo que gestione el Sistema tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales y se regirá según lo previsto en el artículo 28 del RGPD.

[1] A tal efecto, se propone en el Anexo 3 un modelo de política corporativa interna (junto con el resto de información exigida en esta Ley). La versión propuesta o la modificación final de esta política deberá ser aprobada por la Alta Dirección.

Publicidad en la página web

En caso de tener página web, la información sobre el Sistema de Información interno deberá estar disponible en la página de inicio, en una sección separada y fácilmente identificable. Además, deberá contener la siguiente información:

- el uso de todo canal interno de información que hayan implantado,
- los principios esenciales del procedimiento de gestión.

En el Anexo 3 se propone un diseño de esta información a mostrar en la sección web de whistlelink.

Derechos de los informantes

Las personas informantes tienen derecho a la confidencialidad, a no recibir represalias, al anonimato y a la información, de conformidad con lo dispuesto en la presente Política.
Se garantiza el derecho a la total confidencialidad respecto a la identidad de la persona informante y del contenido íntegro de la información de la misma, así como de todas aquellas personas intervinientes, directa o indirectamente afectadas, mediante lo establecido a tales efectos en el presente documento.
Se prohíbe la adopción, por parte de la organización, de cualquier tipo de represalia o tentativa de represalia contra la persona informante como consecuencia de la denuncia interpuesta.
Toda persona informante podrá comunicar su información directamente a la Autoridad Independiente de Protección del Informante[2] (A.A.I.) a través de su canal oficial (bien sea la autoridad nacional o autonómica). Y lo podrá hacer directamente o previo a hacerlo por el canal interno corporativo.

[2] La A.A.I. todavía no se ha constituido, ni a nivel nacional ni a nivel local, a la fecha de aprobación de esta política interna.

Derechos de las personas afectadas

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos regulados en esta ley, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

Las personas denunciadas ostentarán la totalidad de los derechos y de las garantías fundamentales reconocidas legalmente, siendo estos:

a) Derecho a la presunción de inocencia.
b) Derecho a su defensa durante el procedimiento.
c) Derecho de acceso al expediente, con las limitaciones que establece la Ley[3].

Responsable del sistema

El órgano de administración u órgano de gobierno de cada entidad, pública o privada, es el responsable de la implantación del Sistema interno de información, previa consulta con la representación legal de los trabajadores y tendrá la condición de responsable del tratamiento de los datos personales.

Asimismo, las entidades deben designar un responsable del sistema interno de información que puede ser una persona o un órgano colegiado y cuyo nombramiento, destitución o cese debe depender del órgano de administración o gobierno de la entidad. Este cargo puede recaer en el responsable de la función de cumplimiento normativo siempre que ostente un cargo directivo, en el sector privado, y, en todo caso, sea una persona con independencia y autonomía.

El nombramiento, y cese o destitución, se formalizará por escrito (Anexos 1 y 2 respectivamente).

[3] A fin de garantizar el derecho de defensa de la persona afectada, la misma tendrá acceso al expediente sin revelar información que pudiera identificar a la persona informante, pudiendo ser oída en cualquier momento, y se le advertirá de la posibilidad de comparecer asistida de abogado.

Uso indebido del canal

El uso del sistema interno de información se debe de hacer de forma responsable y con la finalidad que se le ha conferido. Por ello, no se tolerará el uso de este canal de comunicación con fines distintos a los establecidos en el presente documento. Además, se podrán adoptar medidas disciplinarias ante aquellos que hagan un uso indebido del mismo.

Evaluación, revisión y aprobación de la política

Al menos anualmente, el responsable del sistema evaluará la eficacia del protocolo, su conformidad con la normativa aplicable y revisará y actualizará el contenido cuando proceda, dejando constancia en el control de versiones del presente documento. La evaluación se podrá llevar a cabo, por ejemplo, a través de cuestionarios anónimos que midan el conocimiento, uso y satisfacción del canal.

La Dirección de la organización aprobará esta política y el Responsable del Sistema responderá de su tramitación diligente.

PROCEDIMIENTO

A continuación, se describe el procedimiento interno: notificación, análisis, investigación y resolución.

Canales de información

CANAL INTERNO

Se permitirá realizar las comunicaciones:

- Por medios electrónicos, a través de: www.ercilladebilbao.whistlelink.com
- A través de una reunión presencial, bajo solicitud del informante, informando al Responsable del Sistema.

En el caso de las **comunicaciones verbales o reuniones presenciales**[4], se documentarán de las siguientes formas, previo consentimiento del informante:

- Mediante una grabación de la conversación en un formato seguro, duradero y accesible, o
- A través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

En todo caso, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

CANAL EXTERNO

En todo caso, el informante podrá acudir al canal externo de la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas.

[4] Si el solicitante escoge la opción de **reunión presencial**, deberá celebrarse dentro del plazo máximo de siete días.

REVELACIÓN PÚBLICA

Se entiende por revelación pública la puesta a disposición del público de información sobre acciones u omisiones.

Cuando los cauces internos o externos no hayan funcionado (porque el informante los haya utilizado sin resultados), exista una amenaza inminente para el interés público, o exista un riesgo de represalias o de no tratamiento efectivo, el informante podrá utilizar la vía o canal de la revelación pública, esto es, usar plataformas web, redes sociales, medios de comunicación, o equivalentes para dar publicidad a su denuncia.

Si la organización tiene conocimiento de la información denunciada a través de una revelación pública, se someterá igualmente a las obligaciones y requisitos de esta política, así como a la ejecución de sus fases.

Identificación del Responsable del sistema de información

El responsable del Sistema, es decir, la persona física encargada de gestionar el sistema interno de información es: Mónica Menéndez, responsable del departamento de RRHH.

Este responsable ejercerá sus funciones bajo los principios de confidencialidad, exhaustividad, respeto y dignidad, durante todo el procedimiento.

Su designación, así como sus funciones y obligaciones, como figura garante de cumplimiento de este canal, se describen en el Anexo 1.

NOMBRAMIENTO, DESTITUCIÓN O CESE

Su nombramiento, destitución o cese debe depender del órgano de administración o gobierno de la organización.

Asimismo, tanto el nombramiento como el cese de la persona física individualmente designada, deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el ámbito de sus respectivas competencias, en el plazo de los diez días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo.

Contenido de la información

Las irregularidades deberán ser comunicadas con la máxima información disponible al respecto. Una lista mínima de información requerida al solicitante podría ser:

- Hecho sobre el que informar
- Persona(s) afectad(s)
- Fecha y lugar de los hechos cuando ocurrieron

Asimismo, a las denuncias deberán acompañarse todos los elementos probatorios de los que disponga el informante.

Registro de informaciones

Se deberá contar con un libro-registro de las **informaciones recibidas y de las investigaciones** internas que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad.

Este registro será privado y únicamente se podrá proporcionar, a petición razonada, a la Autoridad Judicial competente, en el marco de un procedimiento judicial podrá accederse total o parcialmente al contenido del registro.

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas de este registro solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con esta ley[5].

En ningún caso podrán conservarse los datos por un período superior a **diez años**.

[5] Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.
En todo caso, transcurridos **tres meses** desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada.

Medidas de protección

Las condiciones de protección a las personas informantes se producirán en las siguientes circunstancias:

- Tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de este sistema interno de denuncias.
- La revelación pública se ha realizado dentro de los parámetros que establece esta ley.

Por su parte, quedan **excluidos** de protección las personas informantes que comuniquen o revelen:

- Informaciones contenidas en comunicaciones que hayan sido inadmitidas.
- Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.
- Informaciones que ya estén completamente disponibles para el público o que constituyan meros rumores.

PROHIBICIÓN DE REPRESALIAS

Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación a través del sistema interno.

Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes, o por haber realizado una revelación pública. Algunos ejemplos, a título meramente enunciativo, serían:

- Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier

medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido.

- Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
- Evaluación o referencias negativas respecto al desempeño laboral o profesional.
- Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.
- Denegación o anulación de una licencia o permiso.
- Denegación de formación.
- Discriminación, o trato desfavorable o injusto.

Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la **presunción de inocencia, al derecho de defensa y al derecho de acceso** al expediente en los términos regulados en esta política, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.

MEDIDAS DE APOYO

Asimismo, se prevén determinadas medidas de apoyo a las que podrán acceder los informantes, tales como, asesoramiento público y gratuito sobre procedimientos y recursos disponibles, asistencia efectiva por parte de las autoridades en relación con la protección frente a represalias o, en su caso, apoyo financiero o psicológico.

Fases del procedimiento

1. RECEPCIÓN Y ANÁLISIS PRELIMINAR DE LA DENUNCIA

Una vez recibida la información, se procederá a su registro y en un plazo de **siete días naturales** se remitirá un acuse de la recepción de la misma al informante, salvo que éste haya indicado expresamente que no desea recibir comunicaciones relativas a la investigación.

A continuación, se procederá a su análisis pudiendo resultar del mismo su archivo o la apertura de un expediente, si de la denuncia resulta algún indicio de criminalidad, de incumplimiento de la normativa penal y/o administrativa, o de la normativa interna de la organización.

2. FASE DE ARCHIVO O ADMISIÓN DE LA DENUNCIA

La decisión de archivo o admisión no superará los **diez días hábiles**.

Si la denuncia resultara infundada o estuviera fuera del ámbito de aplicación del canal o no existen indicios suficientes para ser considerada una irregularidad o un acto contrario al Código Ético, a las normas y políticas internas de la organización o al incumplimiento de alguna ley, normativa o reglamento, el Responsable del Sistema procederá al archivo de la misma notificando al informante dentro de los **cinco días hábiles siguientes a la decisión**, salvo que el informante haya indicado expresamente que no desea recibir comunicaciones relativas a la investigación. Los datos personales que puedan aparecer en la denuncia serán eliminados o anonimizados del canal, en cumplimiento de la normativa de protección de datos.

Si de la denuncia se desprendieran indicios sobre su fundamento, ésta se admitirá y el Responsable del Sistema lo pondrá en conocimiento del informante dentro de los **cinco días hábiles siguientes a la decisión**, salvo que el informante haya indicado expresamente que no desea recibir comunicaciones relativas a la investigación. Por su parte, también se dará traslado las personas afectadas, dentro del mismo plazo, de:

- los hechos informados, de forma sucinta;
- su derecho a presentar alegaciones;
- su derecho a la protección de datos.

En ningún caso se comunicará a las personas afectadas la identidad del informante ni se le dará acceso a su comunicación sobre la denuncia realizada.

3. FASE DE INSTRUCCIÓN[6]

Tras la admisión de la información y durante la tramitación del procedimiento, la organización podrá adoptar, por iniciativa propia o, a solicitud del Responsable del Sistema, las medidas cautelares procedentes dirigidas al cese inmediato del incumplimiento normativo que se estuviese produciendo. La adopción de tales medidas deberá acordarse por escrito.

En el mismo, se expondrán detalladamente (a) las razones y necesidades que conducen a la adopción de las medidas cautelares, (b) la duración que tendrán las mismas, (c) la identificación de las medidas concretas que se adoptan, y (d) un juicio de proporcionalidad entre las medidas adoptadas y los fines perseguidos por aquéllas.

La adopción de medidas cautelares será excepcional y se optará siempre por la medida menos gravosa de entre las más eficaces, necesarias y útiles para lograr los fines perseguidos.

Con las debidas medidas de transparencia y confidencialidad, se iniciará el proceso de investigación cuya duración máxima será de 3 meses a contar desde la recepción de la comunicación (pero podría ampliarse a seis cuando sea necesario debido a circunstancias específicas del caso, en particular la naturaleza y la complejidad del objeto de la denuncia, que puedan justificar una investigación larga).

Durante dicho período, el Responsable del Sistema practicará las pruebas necesarias para una eficaz investigación de los hechos (entrevistas a implicados, solicitud de documentos, obtención de información a través de otras personas o de fuentes externas, etc.).

Durante la instrucción se dará noticia de la comunicación con sucinta relación de hechos al investigado, y tendrá acceso al expediente sin revelar información que pudiera identificar a la persona informante.

Como parte de la fase de instrucción y siempre que sea posible, se podrá realizar una entrevista con la persona afectada en la que, siempre con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes. A fin de garantizar el derecho de defensa de la persona afectada, la misma tendrá acceso al expediente sin revelar

[6] Esta fase podrá contar con asesores legales externos especializados, sujetos a acuerdos de confidencialidad y protección de datos.

información que pudiera identificar a la persona informante, pudiendo ser oída en cualquier momento.

El responsable del sistema interno tendrá las facultades suficientes para dirigirse a cualquier departamento o persona de la organización para solicitar su colaboración especializada, y obtener la información o documentación necesaria.

El proceso de investigación se llevará a cabo con el máximo rigor para comprobar la veracidad de los hechos, respetando la presunción de inocencia, derecho a su intimidad y los demás derechos que asisten a las personas denunciadas.

Todas las personas participantes en el proceso estarán obligadas a guardar secreto sobre las informaciones que conozcan con ocasión de dicha labor.

4. FASE DE RESOLUCIÓN Y MEDIDAS

Concluida la investigación, se emitirá un informe de instrucción debidamente justificado en el que se propondrá al órgano directivo de la organización alguna de las siguientes recomendaciones:

- El archivo de la denuncia si se comprueba que el incumplimiento normativo no se ha producido. Las partes deberán ser informadas de este extremo, y se cerrará el expediente.
- Las medidas correctoras o sancionadoras que procedan si resultase acreditado el incumplimiento normativo. Estas medidas, en función de resultado que haya arrojado la investigación y el expediente tramitado, pueden consistir en la imposición de alguna sanción de acuerdo con lo establecido en los manuales internos de la entidad (Código Ético, Manual de Compliance, normativa interna etc.) o en el traslado al juez o a la fiscalía de los hechos por su carácter penal, así como, en su caso, la adopción de las medidas preventivas que se estimen oportunas para evitar que incumplimientos similares se vuelvan a producir.

Además, el informe que se emita deberá contener, al menos, los siguientes puntos:

- Una exposición de los hechos relatados junto con la fecha de registro.
- La clasificación de la comunicación a efectos de conocer su prioridad o no en su tramitación.
- Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos.
- Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

En aquellos casos en que la organización proceda a comunicar a la Justicia los hechos denunciados e investigados, pondrá a disposición de las autoridades judiciales competentes el expediente íntegro resultante de la investigación, incluyendo la totalidad de las pruebas obtenidas en el marco de la misma.

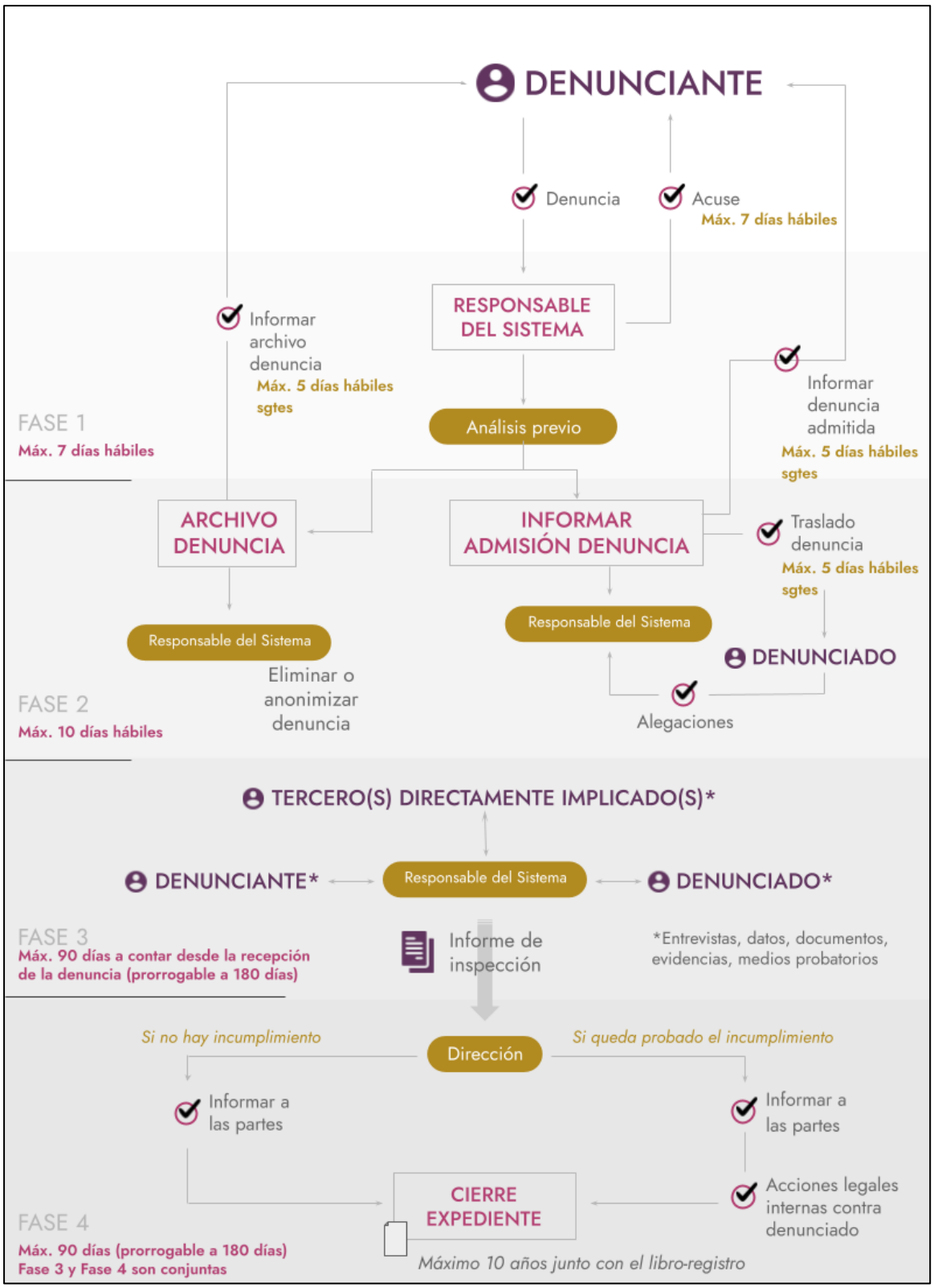
Asimismo, en caso de incoación del correspondiente procedimiento judicial, la organización prestará completa colaboración con la autoridad judicial competente para la debida y adecuada investigación y esclarecimiento de los hechos.

Con independencia de la decisión que se adopte en relación con la finalización de la investigación, dicha decisión deberá quedar documentada en el expediente correspondiente.

Esta fase, que se considera la finalización de la Fase 3 anterior, se incluirá dentro del plazo de los 3 meses (Fase 3 y 4 conjuntas).

Diagrama de Funcionamiento

Actores participantes en el proceso: informante, personas afectadas, tercero(s) directamente implicado(s), Responsable del Sistema, asesores legales especializados (si procede) y Dirección.


DENUNCIANTE
Denuncia
Acuse
Máx. 7 días hábiles
RESPONSABLE DEL SISTEMA
Informar archivo denuncia
Máx. 5 días hábiles sgtes
Informar denuncia admitida
Máx. 5 días hábiles sgtes
FASE 1
Máx. 7 días hábiles
Análisis previo
ARCHIVO DENUNCIA
INFORMAR ADMISIÓN DENUNCIA
Traslado denuncia
Máx. 5 días hábiles sgtes
Responsable del Sistema
Responsable del Sistema
DENUNCIADO
Eliminar o anonimizar denuncia
Alegaciones
FASE 2
Máx. 10 días hábiles
TERCERO(S) DIRECTAMENTE IMPLICADO(S)*
DENUNCIANTE*
Responsable del Sistema
DENUNCIADO*
FASE 3
Máx. 90 días a contar desde la recepción de la denuncia (prorrogable a 180 días)
Informe de inspección
*Entrevistas, datos, documentos, evidencias, medios probatorios
Si no hay incumplimiento
Dirección
Si queda probado el incumplimiento
Informar a las partes
Informar a las partes
Acciones legales internas contra denunciado
CIERRE EXPEDIENTE
FASE 4
Máx. 90 días (prorrogable a 180 días)
Fase 3 y Fase 4 son conjuntas
Máximo 10 años junto con el libro-registro

Protección de datos de carácter personal

A continuación, se describen las consideraciones en materia de protección de datos según las disposiciones legales siguientes:

- Reglamento (UE) 2016/679 General de Protección de Datos (RGPD),
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD),
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

LICITUD DEL TRATAMIENTO

Cuando es la implantación del Sistema de Información sea obligatorio, se presumirá lícito en cumplimiento de una obligación legal aplicable[7]. De no establecerse como obligatorio o mediante una revelación pública, el tratamiento de datos, estará amparado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable[8].

Del mismo modo, en los casos de **comunicación de datos dentro de la organización** (siempre de forma confidencial y a las personas autorizadas), se entenderá lícita esta comunicación en base a criterios normativos

Cuando se produzcan tratamientos de datos de **categoría especial por razones de un interés público esencial**, será lícito este tratamiento en virtud del artículo 9.2.g) RGPD.

TRANSPARENCIA E INFORMACIÓN

Los informantes que utilicen el canal, deberán ser informados de acuerdo con el artículo 13 RGPD y el artículo 11 LOPDGDD.

A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

[7] Artículos 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, cuando, de acuerdo a lo establecido en los artículos 10 y 13 de la presente ley, sea obligatorio disponer de un sistema interno de información.

[8] Artículo 6.1 e) RGPD.

La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante.

Asimismo, los **empleados y terceros** deberán ser informados acerca del tratamiento de datos personales en el marco de los sistemas de información.

En el caso de los empleados, deberán haber sido informados previamente de la existencia de estos sistemas y del tratamiento de los datos que conlleva la formulación de una denuncia.

La información puede proporcionarse por varios cauces:

- Directamente en el contrato de trabajo.
- Individual o colectivamente al implementar o modificar el sistema.
- Mediante circulares informativas al personal y a su representación informando de la existencia y finalidad de un tratamiento de datos relacionado con estos buzones o sistemas de denuncias.

DERECHOS DE LOS INTERESADOS

Los interesados podrán ejercitar sus derechos en materia de protección de datos. Sin embargo, en caso de que la persona a la que se refieran los hechos relatados ejerciese el **derecho de oposición**, se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales.

ACCESO A LOS DATOS

El acceso a los datos contenidos en el sistema interno de información quedará limitado exclusivamente a:

- El Responsable del Sistema y a quien lo gestione directamente,
- El responsable de recursos humanos o el órgano competente debidamente designado, **sólo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador**,
- El responsable de los servicios jurídicos de la entidad u organismo, **si procediera la adopción de medidas legales** en relación con los hechos relatados en la comunicación,
- Los encargados del tratamiento (si existen para este procedimiento),
- El delegado de protección de datos (si se ha designado internamente).

El acceso a los datos por parte de personas distintas a las anteriores será válido sólo cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

MINIMIZACIÓN DE DATOS

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida. En ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones, procediéndose, en su caso, a su inmediata supresión. Asimismo, se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.

DATOS ESPECIALMENTE PROTEGIDOS

Si la información recibida contuviera datos personales incluidos dentro de las **categorías especiales de datos**, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

CONSERVACIÓN DE LOS DATOS

Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados.

Si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

En todo caso, transcurridos **tres meses** desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema.

Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma **anonimizada**, sin que sea de aplicación la obligación de bloqueo de la normativa de protección de datos.

CONFIDENCIALIDAD

La identidad de las personas que denuncien no será revelada a terceras personas.

Los sistemas de información, tanto internos como externos, no deberán obtener datos que permitan la identificación del informante.

Además, estos sistemas deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

La identidad del informante sólo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora. En estos casos, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El tratamiento de datos personales realizado mediante el sistema interno de información requiere la creación de un registro de actividades de tratamiento. Éste deberá contener, al menos:

- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluidas las garantías adecuadas;
- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

ANÁLISIS DE RIESGOS

El tratamiento de datos personales realizado mediante el sistema interno de información requiere que se analicen las amenazas a las que puede verse expuesto en materia de protección de datos, a través de un análisis de riesgos.

¿CÓMO IMPLEMENTAR ESTA POLÍTICA?

A partir de todo lo expuesto en esta política, a continuación se describen los diferentes puntos de verificación para implementar las obligaciones de esta Ley.

SOBRE EL RESPONSABLE DEL SISTEMA:

- Debe designarse formalmente, conocer sus funciones y obligaciones, y gestionar el sistema interno de información de forma diligente y responsable.
    - Ver Anexo 1
- Del mismo modo, su destitución o cese también deberá ser formalizado.
    - Ver Anexo 2

SOBRE EL DISEÑO DEL SISTEMA EN LA WEB[9]:

- Debe crearse una sección específica. Por ejemplo "Sistema de Información Interno".
- Esta nueva sección web debe contener los siguientes requisitos informativos (***Ver Anexo 3***):
    - Contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno de información;
    - El uso de todo canal interno de información que hayan implantado,
    - Los principios esenciales del procedimiento de gestión.
- El sistema diseñado en la página web debe cumplir con determinados **requisitos técnicos** que permitan proteger los intereses del informante, de las personas afectadas, así como de la propia organización para afrontar posibles responsabilidades. Esto es:
    - Opción a presentar denuncias anónimas, y que las posteriores comunicaciones sigan siendo anónimas.
    - Cifrado de datos en tránsito, que garantice la confidencialidad de la información que se transmite a través de internet.
    - Control de acceso, dotando acceso al sistema interno de información sólo a las personas autorizadas en base a la Ley.
    - Registro de actividad, que permita saber en todo momento y sin lugar a dudas todas las acciones que se realizan sobre la denuncia, desde que llega al sistema interno de información, hasta que se cierra el expediente. Esto es: qué

[9] En ausencia de un aplicativo específico para gestionar el sistema interno de información.

usuario (autorizado) consulta, modifica o borra una denuncia en el sistema, y en qué momento exacto realiza cada acción.

- Debe permitir al informante conocer el estado o tramitación de su denuncia.

SOBRE LA INCLUSIÓN DE LA PROTECCIÓN DE DATOS EN EL DISEÑO DEL SISTEMA EN LA WEB:

- Solicitar/aceptar una reunión presencial, deberá utilizarse un formulario en soporte papel en la reunión física que se celebre con el Responsable del Sistema, que contendrá un aviso sobre información básica y completa sobre protección de datos.
  - Ver Anexo 4
- La política de privacidad deberá actualizarse, infromando sobre el tratamiento de los datos personales recogidos en el sistema interno de información.

SOBRE LA TRANSPARENCIA AL COMITÉ O REPRESENTANTES DE LOS TRABAJADORES:

- De conformidad con los deberes de responsabilidad y transparencia, se pondrá en conocimiento la presente política al comité de empresa o a la representación de los trabajadores, según corresponda.

SOBRE LA TRANSPARENCIA A LOS TRABAJADORES:

- De conformidad con los deberes de responsabilidad y transparencia, se pondrá en conocimiento de los trabajadores, previa comunicación al comité de empresa o a la representación de los trabajadores, la existencia del canal y su objeto.
  - Ver Anexo 5 (infografía)

SOBRE OTROS REQUISITOS DE PROTECCIÓN DE DATOS:

- Crear el registro de actividades de tratamiento para este canal.
- Realizar en análisis de riesgos para este canal.

Anexos asociados

ANEXO I: DESIGNACIÓN DEL RESPONSABLE DEL SISTEMA.

Don/Doña _____, en su calidad de Director/a de la entidad GRAN HOTEL ERCILLA SA, con CIF A48060149, acuerda el nombramiento de Don/Doña _____, como Responsable del Sistema interno de información, de conformidad con el artículo 8 de 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.

De este modo, mientras ostente este cargo tendrá las siguientes funciones:

- Desarrollar y mantener la cultura de cumplimiento adecuada acerca del Sistema interno de Información.
- Asesorar sobre cuestiones relativas al Sistema interno de Información.
- Supervisar el cumplimiento efectivo del Sistema interno de Información.
- Proponer medidas a Dirección, sólo o conjuntamente con personal especializado, en el caso de denuncias donde queda probado el incumplimiento.
- Informar y capacitar a los usuarios acerca del Sistema interno de Información.

Como prueba de aceptación del nombramiento y para que conste a los efectos oportunos, se firma la presente acta en _____ a _____ de _____ de 202__.

Firma

Firma

ANEXO II: DESTITUCIÓN O CESE DEL RESPONSABLE DEL SISTEMA[10]

Don/Doña _____, en su calidad de Director/a de la entidad GRAN HOTEL ERCILLA SA, con CIF A48060149, acuerdael cese de Don/Doña _____, como Responsable del Sistema interno de información, de conformidad con el artículo 8 de 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.

Como prueba de aceptación del cese y para que conste a los efectos oportunos, se firma la presente acta en _____ a _____ de _____ de 202__.

Firma

_____

Firma

_____

[10] Tanto el nombramiento como el cese de la persona física individualmente designada deberán ser notificados a la Autoridad Independiente de Protección del Informante, A.A.I., o, en su caso, a las autoridades u órganos competentes de las comunidades autónomas, en el plazo de los diez días hábiles siguientes, **especificando, en el caso de su cese**, las razones que han justificado el mismo.

ANEXO III: INFORMACIÓN WEB SECCIÓN SISTEMA DE INFORMACIÓN INTERNO (WHISTLELINK)

Bienvenido a nuestro canal de información

Puedes utilizar nuestro canal interno de información para denunciar sospechas de mala conducta e irregularidades en nuestra organización. El objetivo de nuestro canal de información es ofrecer una vía segura para informar acerca de cualquier conducta indebida, así como brindar mayor protección al informante.

¿Sobre qué puedes informar?

Al enviar un caso, debes tener motivos válidos para creer que la información enviada es correcta en el momento del envío del caso. El canal de información tiene como objetivo prevenir y detectar el fraude, la corrupción, las actividades ilícitas y el incumplimiento de las normas en diversos ámbitos. También puede tratarse de actividades ilegales, poco éticas o dañinas que pueden afectar negativamente a otros.

Por ejemplo:

• Delitos financieros y fraude

• Corrupción y soborno

• Delitos ambientales o riesgos para la salud y la seguridad

• Violaciones deliberadas de la ley La mala conducta no tiene que ser actual o continua, también se puede informar sobre conductas anteriores. El propósito de este servicio no es expresar insatisfacción con las condiciones de trabajo, organización o gestión, o conflictos en el lugar de trabajo. Las denuncias de conductas indebidas que afectan exclusivamente al denunciante oa su situación laboral, por lo general, no se consideran denuncias.

tu caso
El caso que envías debe contener la siguiente información • El tipo de falta que deseas denunciar. • Donde ha tenido lugar. • Cuando ocurrió. Menciona la hora y la fecha y si es algo recurrente. • Documentación en cualquier formato, si tienes acceso a ella. Si no tienes acceso pero sabes que existe dicha documentación, incluye qué tipo de documentación es y dónde se puede encontrar. • Detalles de cualquier otra acción que hayas tomado en relación con la mala conducta. ¡Atención! Es importante que leas y comprendas el contenido del enlace Privacidad de datos antes de enviar tu caso. No se deben enviar datos personales que no sean claramente relevantes para el caso. Si aún así envías dicha información, podríamos eliminarla sin informarte.

Denuncias externas

También es posible denunciar una mala conducta de forma externa a un organismo competente que pueda recibir y proporcionar información, así como realizar el

seguimiento de los casos de denuncias de irregularidades y, cuando proceda, a instituciones, organismos o agencias de la UE. Puede encontrar información de contacto para cada país en el enlace de Denuncias externas.

Anónimo

Mantendrá su anonimato completamente al enviar una denuncia, a menos que proporcione información personal voluntariamente. No es obligatorio proporcionar ninguna información personal.

ANEXO IV: RGPD FORMULARIO DE REUNIÓN PRESENCIAL

Información sobre protección de datos

¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO?
Identidad del responsable: GRAN HOTEL ERCILLA SA (en adelante, la Organización)
CIF: A48060149
Dirección física: C/ ERCILLA 37-39
Correo electrónico: ercilla@ercilladebilbao.com
Teléfono: 94 470 57 00

FINALIDAD EN EL TRATAMIENTO DE LOS DATOS
Tratamiento de los datos personales con la finalidad de gestionar el sistema interno de información o canal ético, investigar los hechos y proponer medidas resolutorias, prevenir incumplimientos normativos y corregir los ya detectados, así como contribuir a la eficacia de funcionamiento de la Organización con la mejora continua de los procesos internos para la gestión y control de conductas ilegales o contrarias a la cultura ética de la Organización.

LEGITIMACIÓN EN EL TRATAMIENTO DE LOS DATOS
La finalidad en el tratamiento está legitimada por un obligación legal: 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.

PLAZOS DE CONSERVACIÓN
Se conservarán los datos mientras sean necesarios para cumplir con la finalidad para la cual fueron recabados. En todo caso, transcurridos tres meses desde la introducción de los datos, se procederá a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Transcurrido el plazo mencionado, los datos podrán seguir siendo tratados, por el órgano al que corresponda la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas.

DESTINATARIOS DE SUS DATOS
Los datos personales recabados podrán ser comunicados a la administración pública con competencia en la materia y a terceros cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.

EJERCICIO DE DERECHOS
El interesado podrá ejercitar sus derechos sobre protección de datos (acceso, rectificación, oposición, supresión, limitación, portabilidad y no ser objeto de decisiones individuales automatizadas) por correo electrónico en ercilla@ercilladebilbao.com. En cualquier caso, puede solicitar la tutela de la Agencia Española de Protección de Datos a través de su página web www.aepd.es

ANEXO IV: INFORMACIÓN A TRABAJADORES (INFOGRAFÍA)