SISTEMA INTERNO DE INFORMACIÓN

CANAL DE DENUNCIAS Y PROTECCIÓN DE LA IDENTIDAD DEL INFORMANTE

BIENVENIDO FERNÁNDEZ ARIAS S.L.

1.- CONCEPTO Y CARACTERISTICAS

Es el soporte para la recopilación de información, a través de éste se recibirán aquellos sucesos relativos a riesgos materializados o aquellos hechos sobre los que puedan recaer sospechas de comisión de delito, o que supongan un incumplimiento del Código Ético, con el fin de cumplir 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.
El órgano de administración de la empresa, será el responsable de la implantación del Sistema interno de información, previa consulta con la representación legal de las personas trabajadoras, si las hubiera, y tendrá la condición de responsable del tratamiento de los datos personales:

Nombre: BIENVENIDO FERNÁNDEZ ARIAS S.L.
CIF/NIF: B21016027
Dirección: FERNANDO EL CATÓLICO, 11-1ºE - 21003 - HUELVA

El canal de denuncias estará habilitado para todos los empleados de la organización o cualquier tercero que mantenga una relación mercantil con la Sociedad, actuando de buena fe, y contarán con la confidencialidad derivada de la aplicación de este Ley. Y más concretamente:
- Trabajadores por cuenta ajena y propia (autónomos);
- Accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;
- Cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.
- Informantes que comuniquen información tras una relación laboral ya finalizada;
- voluntarios, becarios, trabajadores en periodos de formación;- aquellos cuya relación laboral todavía no haya comenzado, y estén en el proceso de selección o de negociación precontractual.
- Los representantes legales de las personas trabajadoras (RLPT) en el ejercicio de sus funciones o si actúan como informantes, estarán protegidas.
- toda persona física relacionada con el informante inicial y que pueda sufrir represalias. Y personas jurídicas para las que trabaje o con las que tenga una vinculación.

La comunicación se llevará a cabo de forma confidencial. El informante que use está herramienta no podrá ser represaliado, discriminado o perjudicado por el mero hecho de denunciar una conducta ilícita, siempre y cuando actué de buena fe.
El canal de denuncias sustenta su funcionamiento sobre los siguientes principios:
- Confidencialidad.
- Integración en todos los procedimientos de la empresa.
- Sencillez para el comunicante.
- Diversidad de vías de acceso, primando siempre la comunicación efectuada por correo electrónico o a través de otro canal, si existiera, especificado en esta política.
- Divulgación máxima de su existencia.
- Fiabilidad de la información.

La identidad del denunciante, así como los datos de carácter personal que comunique en referencia a una actuación irregular a través de este canal, tendrán la consideración de información confidencial, y, por tanto, no podrá ser comunicada sin su consentimiento expreso al denunciado.
Es importante resaltar que la confidencialidad del denunciante no implica necesariamente el anonimato a todos los efectos, ya que la realización de una comunicación o denuncia no implica más que un mecanismo de inicio de una actividad instructora o indagatoria por parte del RESPONSABLE DE LA

GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN en aras a averiguar cuanta información pudiera recabar para verificar los hechos comunicados/denunciados, siendo que de ese modo resultaría importante, por no decir imprescindible, que tanto para el comunicante como para el órgano encargado de la gestión fuese posible ponerse en contacto con el denunciante, para ampliar o matizar las informaciones enviadas o recibidas, en función de las necesidades de la investigación a realizar.
El canal de denuncias puede ser gestionado internamente, en cuyo caso las denuncias serán recibidas, investigadas y resueltas por departamentos internos de la empresa, o puede externalizarse su gestión en un tercero que será quién realice las tareas de investigación, si así se estableciera en esta política. Inicialmente se establece que su gestión será interna.
En todos los casos, la decisión sobre la resolución de la denuncia y las medidas a adoptar deberá ser tomada por el RESPONSABLE DE LA GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN, lo que no significa que pueda ser asesorado por profesionales y/o especialistas de cada materia investigada en cuestión.
Todas las denuncias que se reciban deben ser registradas, seriadas, e investigadas adecuadamente y resueltas por el órgano designado por la empresa. Finalizada la investigación y resuelta la incidencia, la persona que realizó la denuncia deberá ser informada del resultado y se le comunicarán los términos de la resolución adoptada.
Toda denuncia o comunicación recibida con trascendencia penal implicará necesariamente el inicio de un expediente por parte del órgano de investigador.

2.- COMUNICACIÓN DE INFRACCIONES, CONTENIDO MÍNIMO EXIGIBLE A CADA DENUNCIA Y CLAVES PARA SU FUNCIONAMIENTO

Podrá comunicarse cualesquier acción u omisión que pueda constituir:
- infracciones penales o administrativas graves o muy graves
- infracciones del Derecho de la Unión Europea

Para su admisión y adecuada tramitación, las comunicaciones o denuncias deberán contener necesariamente los siguientes datos:

- Denunciante identificado con nombre y apellidos de forma opcional. Podrá ser de forma anónima.
- Exposición sucinta de los hechos o argumentos que sustenten la comunicación/denuncia.
- Persona o colectividad contra la que se dirige la denuncia.

La carga de la prueba corresponderá siempre al denunciante, quien deberá aportar los documentos en que se fundamente la misma y el denunciado podrá aportar los documentos que estime sean adecuados para contraponer los del denunciante.
Las claves para que el canal de denuncias funcione de forma efectiva y de esta manera sirva para identificar conductas irregulares dentro de la organización son fundamentalmente dos aspectos:
- Que todos los empleados tengan total confianza en que en ningún caso habrá represalias por el hecho de efectuar denuncias siempre que se realicen de buena fe.
- Que todas las denuncias, sin excepciones, se investiguen hasta el final y que, en caso de que efectivamente se estuvieran produciendo comportamientos irregulares, éstos tengan consecuencias para el infractor. En todo momento se mantendrá la confidencialidad del denunciante, salvo que dicha información sea requerida por autoridad competente judicial o administrativa, en cuyo caso la empresa se verá obligada a ceder dicha información al órgano requirente.

Existiendo la posibilidad de que en el canal de denuncias se reciban, por alguno de los medios que lo permitan, algún tipo de comunicación donde no consten datos del denunciante, y a pesar de que el espíritu del canal es dar cumplimiento a lo expuesto por el gabinete jurídico de la A.E.P.D. de 2007, Informe para la Creación de sistemas de denuncias internas en las empresas (mecanismos de □whistleblowing□), de forma que en la medida de lo posible se eviten las comunicaciones anónimas, las mismas no serán automáticamente rechazadas, aunque nunca podrán servir como única prueba de la comisión de una irregularidad o un delito.

CANAL DE COMUNICACIÓN

- La comunicación/denuncia se remitirá al RESPONSABLE DE LA GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN, preferentemente por correo electrónico, en la dirección: **administracion@bifesa.com**

- Opcionalmente la comunicación de denuncia podrá remitirse también por correo certificado, dirigida al RESPONSABLE DE LA GESTIÓN DEL SISTEMA INTERNO DE INFORMACIÓN a la dirección de su domicilio social, indicada al comienzo de este documento.

- Recibida la comunicación/denuncia la persona encargada de la gestión del canal acusará recibo de la misma al denunciante en un plazo de 7 días naturales e iniciará las oportunas verificaciones y comprobaciones necesarias. En caso de que entre las personas afectadas por la comunicación/denuncia se encuentre alguna de las que formen parte del ÓRGANO DE GESTIÓN, esta/s deberá/n ser substituida/s por otra en las tareas de investigación relacionadas directamente con la comunicación/denuncia en cuestión.
- El plazo máximo para dar respuesta a las actuaciones de investigación será inferior a 3 meses (ampliables a otros 3 por casos de especial complejidad).
- La persona afectada deberá ser informada de las acciones u omisiones que se le atribuyen, garantizando siempre la presunción de inocencia y su honor. En todo caso, se garantizará en todo momento la confidencialidad de la comunicación/denuncia.
- Las comunicaciones realizadas generarán un expediente que se registrará e identificará por un número de referencia, garantizándose el cumplimiento de lo previsto en la normativa de protección de datos.
- Todas las personas que intervengan en los posibles procesos de investigación tienen la obligación de mantener la debida confidencialidad y el secreto de los datos e informaciones a las que hayan tenido acceso, pudiendo en caso contrario ser sancionados.

3.- PERSONA-ORGANO DE GESTIÓN E INSTRUCCIÓN DE DENUNCIAS

- Funciones:
  - Velar por el debido cumplimiento del modelo de prevención establecido, realizando las periódicas actualizaciones que puedan resultar necesarias.
  - Realización de labores de instrucción y gestión del canal de denuncias, intentando mantener en la medida de lo posible el carácter colegiado del mismo, si lo hubiere.

- Composición:
  - Según lo dispuesto en la normativa vigente, BIENVENIDO FERNÁNDEZ ARIAS S.L. ha decidido designar como responsable de la gestión de este sistema a:

Nombre: **PEDRO-GUILLERMO GARCÍA MONTERO**
Dirección: **FERNANDO EL CATÓLICO, 11-1ºE - 21003 - HUELVA**
Email: **administracion@bifesa.com**

La entidad podrá nombrar como responsable de este sistema de gestión a un órgano interno cuyos componentes deberán estar identificados en este documento o externalizar esta función, identificando igualmente en este documento al tercero en cuestión. En caso de externalización del servicio dicho encargado de tratamiento tendrá las funciones asignadas descritas en el Contrato de Prestación de Servicios firmado entre ambas Sociedades, en el que se delimitará de forma precisa el alcance y contenido del mandato. De igual forma, se establecerá un contrato de acceso a datos de terceros según la normativa europea y nacional en materia de protección de datos de carácter personal.

Podrán incorporarse al mismo puntualmente, y, para cada caso concreto, la/s persona/s de la organización que así se decidan en cada momento según la naturaleza del hecho denunciado.

- Procedimientos relacionados con la gestión del Canal de Denuncias y la gestión de las Denuncias Recibidas.

- EL RESPONSABLE DEL SISTEMA realizará entre otras, las siguientes funciones:
  a) Gestión del canal de denuncias:
    1.- Recepción de denuncias
    2.- Clasificación de denuncias
  b) Gestión de las denuncias recibidas
    1.- Instrucción de la denuncia
    2.- Redacción de informe dirigido al órgano de decisión

Para realizar dichas funciones se detallan a continuación unas líneas básicas de carácter meramente orientativo, pudiendo el RESPONSABLE DEL SISTEMA estimar en cada caso concreto la realización de cuantas modificaciones considere procedentes en aras a una mejor consecución de sus objetivos.

Este último párrafo no será de aplicación para aquellos expedientes que tengan trascendencia penal.

A) Gestión del canal de denuncias

En relación con la gestión de las denuncias recibidas, corresponderá al RESPONSABLE DEL SISTEMA tomar las decisiones, debidamente justificadas, correspondientes a permisos de acceso, escritura, impresión, eliminación o bloqueo de datos almacenados, los plazos para su cancelación definitiva o las razones por las que se podría acceder a datos bloqueados, previa consulta al DPO (Delegado de protección de datos) designado por la entidad, si existiera esta figura.

De conformidad con la normativa en protección de datos, el acceso a los datos almacenados por parte de un tercero interesado quedará limitado a los propios datos de carácter personal objeto de tratamiento, no pudiendo considerarse los datos de terceras personas como incluidos dentro de este derecho, de modo que tanto los datos del/los denunciante/s deberán mantenerse en todo caso bajo estricta situación de confidencialidad, así que como cualesquiera otros datos relativos a terceros que consten en la comunicación recibida o en el expediente que se incoe.

Sobre la clasificación de las denuncias, esta función se corresponde con el análisis de las denuncias recibidas y la materialización de los riesgos que se den en la compañía, correspondiendo al responsable del sistema separar aquellas que realmente se corresponden a riesgos penales, y que por tanto deberán ser tramitadas por este órgano, de aquellas que responden a una casuística diferente, y que deberán ser dirigidas a los departamentos correspondientes si pudiesen ser de interés, o incluso desechadas directamente si no tuvieran trascendencia alguna.

Para facilitar las tareas, tanto de clasificación como de instrucción, cada denuncia tendrá asignado un código de identificación que se facilitará a la persona que la presentó, de forma que permita al acceso a dicho expediente y la comunicación entre el órgano investigador y el denunciante, en caso de requerir nuevas comunicaciones entre las partes.

B) Gestión de las denuncias recibidas

Iniciado el oportuno expediente, se analizará el alcance de la información recibida, determinando si la misma afecta a alguna o algunas personas concretas. En caso de ser necesaria la recusación o abstención de alguno de los miembros que conforman el responsable del sistema, por verse afectados de forma directa por la información recibida, esta se producirá en este primer momento.

Para la instrucción de las denuncias el responsable del sistema podrá funcionar de forma colegiada y este podrá, mediante designación expresa, encomendar a uno de sus miembros la instrucción del procedimiento.

Iniciada la instrucción, el encargado de la misma podrá adoptar medidas de carácter urgente, siempre y cuando estén debidamente motivadas. Las medidas de carácter urgente deben tener como finalidad:

- Paliar los efectos del riesgo materializado o por materializar
- Evitar destrucción de pruebas
- Comunicación urgente, en su caso, de la información a los órganos de gobierno de la empresa.

A título de ejemplo, dentro de las medidas urgentes que podrán acordarse por el instructor, siempre y cuando estén suficientemente motivadas, serán entre otras: la incautación o precinto de medios informáticos, la comunicación a proveedores de servicios para la conservación de determinada información, o incluso el mantenimiento de información recibida en secreto por el tiempo estricta y prudencialmente necesario para el aseguramiento de las finalidades descritas anteriormente.

Igualmente, si fuese necesario, podrá comunicarse con el denunciante a los efectos de ampliar la información recibida, garantizando siempre la confidencialidad de identidad e información.

Una vez realizada la primera fase de la investigación, por el órgano de investigación se aprobará una propuesta de resolución definitiva que deberá ser presentada al órgano de decisión de la entidad con un informe que contendrá:

- Información descriptiva de la denuncia, fechas de interposición y principales hitos.
- Medidas de urgencia llevadas a cabo, motivación de las mismas y efectos.
- Objetivación de la denuncia, análisis de la fiabilidad del denunciante y veracidad de la información.
- Valoración de si resulta necesario cualquier tipo de apoyo o asesoría externa.
- Propuesta de actuación y resolución, con proposición de las medidas ya adoptadas y que se deban mantener.
- La investigación del denunciante por deslealtad o por faltar dolosamente a la verdad;
- El envío de la información a los tribunales o agentes de la autoridad por ser delitos que no estén dentro del ámbito de la persona jurídica, etc.

C) Procedimientos relacionados con la revisión del sistema.

Los procedimientos y controles previstos en este sistema serán válidos en tanto en cuanto se mantengan las idénticas condiciones empresariales sobre las que el mismo se diseñó, y mientras no se detecten fallos.

Anualmente se realizará una revisión ordinaria del plan. En dicha revisión se valorarán, como mínimo, los siguientes aspectos:

- La existencia de cambios o modificaciones sustanciales de normas legales que rijan el funcionamiento de la empresa o del sector o actividad de negocio, siempre que tenga entidad suficiente para afectar al plan de cumplimiento normativo.
- La existencia de cambios en las condiciones económicas, empresariales o laborales de la empresa, especialmente aquellas que fundamentaron la evaluación de los riesgos de este plan.

Si se detectara alguna de estas modificaciones con antelación a la revisión anual, podrá esta adelantarse a los efectos de verificar la adecuación del plan a la nueva situación. En todo caso, deberá instarse la revisión inmediata del plan en el momento en que por el órgano investigador o el DPO se detecte un incumplimiento de las conductas descritas en él.

4.- PROTECCIÓN DEL INFORMANTE

Se prohíbe expresamente todo acto constitutivo de represalia, incluso amenazas de represalia y las tentativas de represalia, contra las personas que presenten una comunicación. 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. En el ámbito laboral pueden considerarse represalias, si no están debidamente justificadas, a título enunciativo:

- la suspensión del contrato de trabajo, despido o extinción de la relación laboral, por cualquier motivo o modificación sustancial de las condiciones de trabajo, falta de conversiones contractuales, etc.
- 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 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.

5.- PROTECCIÓN DE DATOS

La base legitimadora de este tratamiento es por obligación legal y se verá sometida a la normativa en vigor en materia de protección de datos. Respecto del periodo de conservación de esta tipología de datos

personales objeto de tratamiento, la Ley 2/2023 en su artículo 32 apartado tercero, establece que los datos personales podrán conservarse en el sistema de información el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. Además, este artículo en su apartado cuarto, establece que, 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 prevista en el artículo 32 de la LOPDGDG.
El informante tiene la posibilidad de ejercer los siguientes derechos sobre sus datos personales: derecho de acceso, rectificación, supresión u olvido, limitación, oposición, portabilidad y a retirar el consentimiento prestado. Para ello podrá enviar un email al RESPONSABLE DEL SISTEMA INTERNO DE INFORMACIÓN, al RESPONSABLE DEL TRATAMIENTO o al DELEGADO DE PROTECCIÓN DE DATOS (DPO).
Además, el interesado puede dirigirse a la Autoridad de Control en materia de Protección de Datos competente para obtener información adicional o presentar una reclamación.