POLÍTICA SOBRE EL SISTEMA INTERNO DE INFORMACIÓN

SQUIRE PATTON BOGGS

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

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 (comúnmente denominada ley "*whistleblowing*" y, en adelante, la "**Ley de Protección al Informante**") establece la obligación de implantar un **sistema interno de información** mediante el que sea posible -a través de uno o varios canales- informar sobre vulneraciones del ordenamiento jurídico en el marco de una relación laboral o profesional, de forma que los informantes estén adecuadamente protegidos frente a las represalias que pudieran sufrir por razón de haber facilitado dicha información.

Squire Patton Boggs UK LLP Sucursal en España ("**SPB**") cuenta con un sistema interno de información que posibilita la comunicación de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial aplicable, así como la tramitación de dichas comunicaciones.

SPB unifica la gestión de las notificaciones relacionadas con las mencionadas infracciones en un único **sistema integrado de información** (el "**Sistema Interno de Información**"), dotándose de este modo de una vía común a través de la cual todos sus empleados, directivos y restantes grupos de interés puedan comunicar información de la que por cualquier medio tengan conocimiento sobre acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea en los ámbitos que más adelante se exponen o que puedan ser constitutivas de infracción penal o administrativa grave o muy grave según la normativa española.

El Sistema Interno de Información abarca tanto el canal de denuncias, entendido como buzón o cauce para la recepción de la información, como la figura del responsable del sistema y el procedimiento de tramitación de denuncias. El Sistema Interno de Información debe ser el medio preferente para canalizar la información, pues la compañía es quien está en mejor posición para paralizar las consecuencias perjudiciales de las actuaciones investigadas.

Por ello, invitamos a todos los empleados y directivos de SPB a comunicar cualquier presunta infracción de la legalidad citada de la que tengan conocimiento. Sólo así será posible que cualquier sospecha o duda de irregularidad sea comprobada y, en su caso, se puedan adoptar las medidas adecuadas para reparar sus consecuencias y evitar que esa irregularidad se repita en el futuro, mejorando de esta manera el entorno profesional, social, ético y de compromiso con el cumplimiento de leyes y normas de SPB.

2. ÁMBITO DE APLICACIÓN Y DISPOSICIONES GENERALES

La presente Política sobre el Sistema Interno de Formación (la "**Política**") es de aplicación a SPB.

Es función del **órgano de gobierno de SPB** (*Office Managing Partner*) establecer las bases, fijar los instrumentos y diseñar los mecanismos necesarios para una adecuada y eficiente coordinación en las actividades relacionadas con la gestión de denuncias. Para ello, corresponde al órgano de gobierno de SPB **aprobar esta Política y asegurar tanto la aplicación de sus principios como la implantación del Sistema Interno de Información,**

previa consulta con la representación legal de las personas trabajadoras, en el caso de que las hubiera.

Además, el órgano de gobierno de SPB designará a la persona **Responsable del Sistema Interno de Información** -quien debe tener la condición de directivo- encargada de la tramitación diligente de las comunicaciones. El Responsable del Sistema Interno de Información desarrollará sus funciones de forma independiente y autónoma respecto del resto de los órganos de organización de la entidad, no podrá recibir instrucciones de ningún tipo en su ejercicio, y dispondrá de todos los medios personales y materiales necesarios para llevarlas a cabo. *Las funciones del Responsable del Sistema Interno de Información pueden asumirse por el responsable de la función de cumplimiento normativo, recursos humanos ("**RRHH**") o de políticas de integridad.*

El Responsable del Sistema Interno de Información puede ser una persona física (directivo) o un órgano colegiado. En este caso, la gestión del Sistema Interno de Información y el tratamiento de expedientes de investigación deberán estar delegados en uno de los miembros del órgano colegiado, quien debe tener la condición de directivo.

Son funciones del Responsable del Sistema de Información: (i) garantizar el más amplio acceso al Canal de Denuncias; (ii) recibir las denuncias y encargarse de su registro, admisión a trámite e instrucción; (iii) formalizar las conclusiones alcanzadas en la investigación en un informe final; (iv) adoptar las medidas oportunas para evitar los daños derivados de las infracciones que se hubieran podido cometer, o derivarlo a quienes, según el caso, tengan competencia para ello (v) informar periódicamente al órgano de gobierno de SPB sobre la actividad desarrollada en el Canal de Denuncias.

El órgano de gobierno de SPB también será quien acuerde la destitución o cese del **Responsable del Sistema Interno de Información.**

Tanto el nombramiento como el cese del Responsable del Sistema de Información deberán comunicarse a la Autoridad Independiente de Protección del Informante o a las autoridades y organismos de las comunidades autónomas, en el ámbito de sus respectivas competencias, en los diez (10) días hábiles siguientes, especificando, en el caso del cese, las razones que lo justifiquen.

En la gestión del Sistema Interno de Información rigen los principios de **confidencialidad** de los datos aportados y de las declaraciones realizadas y de **respeto y de protección a las personas.** Cualquier decisión que se adopte a partir de la recepción de la información, se tomará de forma razonada, proporcionada y considerando las circunstancias de los hechos denunciados, con pleno respeto a los derechos y con las debidas garantías para el informante y para las personas afectadas.

En particular, **el Sistema Interno de Información garantiza la confidencialidad de la identidad de los informantes y personas afectadas**, así como de las comunicaciones. Igualmente, se garantiza la **presunción de inocencia** a todas las personas afectadas. Toda persona que denuncie gozará de la debida protección, por lo que cualquier acción respecto a ella que pueda entenderse como amenaza, discriminación o represalia, será sancionable.

Cualquier comunicación podrá realizarse a través de los canales habilitados en el Sistema Interno de Información, pudiéndose realizar tanto de forma verbal como escrita. No obstante, se incorpora como Anexo un formulario para la realización de las denuncias. La denuncia puede ser, además, anónima.

2.1. Ámbito subjetivo

Podrán denunciar irregularidades a través de los canales que se integran en el Sistema Interno de Información:

i. Empleados, exempleados, trabajadores en periodos de formación -remunerados o no-, voluntarios, becarios y candidatos en un proceso de selección cuando la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.
ii. Directivos, entendiendo por tales quienes presten servicios de dirección para la compañía y ostenten en ella facultades de representación, organización o control, con independencia de que su relación contractual con la Sociedad sea mercantil o laboral.
iii. Los Administradores y/o socios.
iv. Colaboradores externos, tales como agentes o personas que tengan la condición de autónomos y cualquier persona que trabaje bajo la supervisión y dirección de contratistas, subcontratistas o proveedores.

Por otra parte, pueden ser **objeto de denuncia** todos los empleados, directivos, socios o colaboradores externos de SPB que hayan cometido alguna irregularidad o conducta que puedan constituir infracciones del Derecho de la Unión Europea o que puedan ser constitutivas de infracción penal o administrativa grave o muy grave.

2.2. Ámbito objetivo

Las **conductas** que pueden ser objeto de denuncia a través del Sistema Interno de Información son:

- **Acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea** en los siguientes ámbitos:

  i. Contratación pública
  ii. Servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo
  iii. Seguridad y conformidad de los productos comercializados en el mercado de la Unión
  iv. Seguridad del transporte
  v. Protección del medio ambiente
  vi. Protección frente a las radiaciones y seguridad nuclear
  vii. Seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales
  viii. Salud pública
  ix. Protección de los consumidores
  x. Protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información

- **Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave**.

En todo caso, se entenderán como tales las infracciones que impliquen un quebranto para la Hacienda Pública y/o la Seguridad Social.

Asimismo, se incluyen las eventuales infracciones en materia de seguridad y salud en el trabajo

3. OPERATIVA DEL SISTEMA INTERNO DE INFORMACIÓN

3.1. Acceso y funcionamiento del Sistema Interno de Información

El Sistema Interno de Información es único para SPB. El Sistema Interno de Información está diseñado de forma que garantiza la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado.

El Sistema Interno de Información es el cauce preferente para informar de las infracciones contenidas en el apartado 2.2 de esta Política, siempre que se pueda tratar de manera efectiva la infracción y que no haya riesgo de represalias. El Canal Interno de Información destinado a la presentación de información respecto de las infracciones mencionadas en el apartado 2.2 de esta Política estará integrado dentro del Sistema Interno de Información.

El Canal Interno de Información será accesible a través de los siguientes medios:

- Grabación por **Voz**. A través del Sistema Interno de Información. En dicho caso, se advertirá al informante que la comunicación será grabada y se conservará como grabación de audio, con arreglo a la legislación que resulte de aplicación.
- Dirección de **correo electrónico** especifica del Sistema Interno de Información.
- A través de la **web corporativa**.
- Mediante una comunicación remitida por **vía postal** a las oficinas de Squire Patton Boggs, Plaza Marqués de Salamanca 3 y 4, 7ª Planta.
- A solicitud del informante, también podrá presentarse mediante una reunión presencial en el plazo máximo de siete (7) días.

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las comunicaciones.

El informante que desee mantenerse en el anonimato podrá hacerlo con las garantías suficientes establecidas en esta Política.

El Sistema Interno de Información se complementa con un canal externo, gestionado por una autoridad pública, denominada **Autoridad Independiente de Protección del Informante**. A quienes realicen la comunicación a través del Canal Interno de Información se les informará, de forma clara y accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la UE.

Cualquier acción encaminada a impedir que un empleado realice una comunicación a través del Sistema Interno de Información será sancionada de acuerdo con el régimen laboral y disciplinario aplicable.

3.2. Registro y clasificación de las denuncias

Todas las denuncias recibidas se analizarán por el **Responsable del Sistema Interno de Información**.

Están permitidas las comunicaciones por escrito (vía electrónica), verbalmente (por mensajería de voz) o de las dos formas. En cualquier caso, las comunicaciones verbales deberán documentarse previo consentimiento del informante:

a) mediante una grabación de la conversación en un formato seguro, duradero y accesible, o
b) a través de una transcripción completa y exacta de la conversación realizada por el responsable de tratarla. El informante tendrá derecho a comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

Por otro lado, está permitida la presentación y tramitación de comunicaciones anónimas. Ello significa que el Sistema Interno de Información habilita mecanismos que permiten la presentación de denuncias sin que sea preciso para el informante revelar su identidad. La identidad del informante sólo podrá ser comunicada a la autoridad judicial, al Ministerio Fiscal o la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

Una vez recibida la comunicación, se deberá enviar **acuse de recibo** de la comunicación en un plazo máximo de 7 días, salvo que el informante prefiera no recibirlo o pudiera suponer un riesgo para la confidencialidad de la comunicación.

La denuncia deberá constar de una descripción completa del hecho denunciado, además de identificar a las personas presuntamente afectadas o implicadas en el mismo – en el caso de que las hubiera – y aportar datos concretos, fechas, empresas o terceros relacionados con el hecho o actuación descrita; todo ello con objeto de favorecer, en su caso, la posterior comprobación de los hechos objeto de la comunicación.

La información recibida se deberá clasificar por orden de importancia del 1 al 5, siendo 1 aquellas consideradas más relevantes y 5 aquellas consideradas menos relevantes. Se consideran como aspectos de mayor relevancia los siguientes:

- Situaciones que puedan dar lugar a eventuales responsabilidades penales de la compañía o sus directivos, incluyendo, pero sin limitarse, a aquellas que puedan involucrar actos que, de confirmarse, pudieran llegar a ser clasificadas como corrupción en el ámbito público, en alguna de sus formas.
- Situaciones en las cuales exista el riesgo de vulnerar alguna legislación vigente.
- Situaciones que, de conocerse fuera de la compañía, pudieran causar un daño a la imagen de la Sucursal, la Compañía o al Grupo mercantil.
- Situaciones que supongan un riesgo para la “continuidad del negocio”.
- Situaciones de denuncia fundada asociada a un importe elevado.

- Número de personas o áreas afectadas por los hechos denunciados.
- Hechos que pudieran ser constitutivos de actos de corrupción.

La valoración indicada en este apartado determinará con carácter provisional la prioridad a la hora de comenzar la revisión de la denuncia y la asignación de los recursos.

En el caso de que, con posterioridad, se obtengan nuevos datos o indicios que aconsejen variar el rating asignado inicialmente, se modificará justificadamente el cambio de prioridad, documentándose debidamente.

Las denuncias que se reciban a través del Sistema Interno de Información y que guarden relación con situaciones de discriminación, acoso moral (*mobbing*) y acoso sexual o por razón de género, se tramitarán, en su caso, de conformidad con los procedimientos específicos que puedan existir para estas materias concretas en la sociedad empleadora del informante.

Las denuncias presentadas a sabiendas de su falsedad serán consideradas infracciones muy graves de acuerdo con lo dispuesto en el artículo 63 f) de la Ley de Protección del Informante y serán objeto de las acciones disciplinarias aplicables a las faltas muy graves en el ámbito laboral.

3.3. Análisis preliminar de los hechos denunciados

Recibida una comunicación, se determinará si procede o no darle trámite, considerando si reúne los requisitos mínimos para ello. Para ello, se comprobará en primer lugar si la denuncia expone hechos o conductas incluidos en el apartado 2.2 de esta Política.

El Responsable del Sistema Interno de Información podrá inadmitir la comunicación a trámite cuando (i) los hechos relatados carezcan de toda verosimilitud o sean manifiestamente infundados; (ii) los hechos no sean constitutivos de alguna de las infracciones a que se refiere el apartado 2.2 de esta Política; y (iii) cuando, siendo anónima, no aporte información suficiente para la comprobación de los hechos denunciados.

En el caso de que el Responsable del Sistema Interno de Información aprecie que los hechos pueden ser indiciariamente constitutivos de delito, remitirá inmediatamente la información al Ministerio Fiscal, o a la Fiscalía Europea en el caso de que los hechos afecten a los intereses financieros de la UE.

Esta decisión deberá ser documentada.

3.4. Comprobación de los hechos denunciados

Admitida a trámite la comunicación, el Responsable del Sistema Interno de Información procederá a la comprobación y análisis de los hechos denunciados. Si fuera necesario se podrá requerir la colaboración de otras áreas de la compañía o de terceros.

El Responsable del Sistema Interno de Información garantizará que la persona afectada por la información tenga noticia de: (i) la presentación de la denuncia y un relato sucinto de los

contenidos en la misma; (ii) el derecho que tiene a presentar alegaciones por escrito; y (iii) del tratamiento de sus datos personales.

Esta información podrá efectuarse en el trámite de audiencia si se considerara que su aportación con anterioridad pudiera facilitar la ocultación, destrucción o alteración de las pruebas.

La investigación de los hechos comprenderá, siempre que sea posible, 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. La persona afectada también tendrá derecho a formular alegaciones por escrito, así como a ser oída en cualquier momento de la investigación.

Para 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.

En ningún caso se comunicará a los sujetos afectados la identidad del informante ni se dará acceso a la comunicación.

Adicionalmente, se deberá asegurar un adecuado cumplimiento de la Legislación de protección de datos aplicable y en particular, respecto a los derechos de los titulares de dichos datos.

3.5. Resolución de la denuncia

Concluida la investigación sobre los hechos denunciados, el Responsable del Sistema Interno de Información alcanzará las conclusiones que procedan y las trasladará a las áreas competentes para adoptar los planes de acción y medidas correspondientes. De acuerdo con las disposiciones que desarrolla esta Política, dichas conclusiones se formalizarán en un informe cuyo contenido contendrá:

- La fecha de presentación de la denuncia y una exposición de los hechos contenidos en la misma;
- La clasificación de la comunicación a efectos de conocer su prioridad en la tramitación;
- Las actuaciones realizadas para comprobar la verosimilitud de los hechos; y
- Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

La respuesta a las actuaciones de investigación no podrá tardar más de 3 meses desde la recepción de la comunicación[1], aunque se puede extender por otro período de hasta 3 meses más en casos que revistan mayor complejidad.

Emitido el informe, el Responsable del Sistema de Información tomará alguna de las siguientes decisiones:

[1] Para el caso de que no se hubiera remitido acuse de recibo, el plazo de los tres meses comenzará a contar a partir del vencimiento del plazo de siete días después de efectuarse la comunicación.

a) Si se considera no acreditada la existencia de infracción: Archivo del expediente

Si se determina que no ha quedado acreditada la comisión de ninguna irregularidad, acto contrario a la legalidad o a las normas internas, se acordará dar por concluido el expediente sin necesidad de adoptar ninguna medida, procediéndose a su archivo y documentándose tal decisión.

El archivo del expediente será notificado al informante y a la persona afectada.

b) Si se considera acreditada la existencia de infracción

Si se determina que ha quedado acreditada la comisión de alguna irregularidad, acto contrario a la ley o a las normas internas, se dará traslado al responsable del área afectada y al área de RRHH para los efectos disciplinarios oportunos.

En aquellos casos en que por su relevancia se considere necesario, a instancia de cualquiera de las áreas anteriormente citadas, se podrá dar traslado:

- A la autoridad judicial
- Al Ministerio Fiscal
- A la Autoridad Administrativa

SPB cuenta con un **libro-registro** en el que se recogen todas las comunicaciones recibidas, así como las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, la confidencialidad del informante y de la persona afectada.

El libro-registro no será público y únicamente a petición razonada de la autoridad judicial competente, mediante auto, en el marco de un procedimiento judicial podrá accederse total o parcialmente al contenido del libro-registro.

4. PROTECCIÓN DE DATOS PERSONALES

En la gestión del Sistema Interno de Información, se dará cumplimiento a lo establecido en el Reglamento (UE) 2016/679, de Protección de Datos (RGPD) y por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). En particular, se tendrán en cuenta los siguientes aspectos:

- **Se deberán implantar las medidas de seguridad de los datos personales** que resulten de aplicación según el nivel de riesgo que se establezca para el Sistema Interno de Información o, en su caso, las medidas que resulten obligatorias en virtud de la normativa legal aplicable y la normativa interna de SPB al respecto, al objeto de protegerlos de divulgaciones o accesos no autorizados. El nivel de seguridad deberá ser, como mínimo, el equivalente al previsto en el sistema de cumplimiento de protección de datos para los datos sensibles o de categoría especial, de acuerdo con la normativa de protección de datos aplicable.

- **Se deberá garantizar un adecuado cumplimiento del tratamiento de datos de carácter personal**, y en particular respecto a los derechos de los titulares de dichos datos a ser informados sobre el tratamiento de los mismos.

El responsable de la implantación del Sistema Interno de Información es el órgano de administración u órgano de gobierno (Office Managing Partner).

Los datos personales recabados en el marco del Sistema Interno de Información:

- Se limitarán a los estricta y objetivamente necesarios para tramitar las denuncias y, si procede, comprobar la realidad de los hechos denunciados;

- Serán tratados en todo momento de conformidad con la normativa de protección de datos aplicable, para fines legítimos y específicos en relación con la investigación que pueda surgir como consecuencia de la denuncia;

- No se utilizarán para fines incompatibles;

- Serán adecuados y no excesivos en relación con las citadas finalidades.

SPB se asegurará de que se adopten todas las medidas técnicas y organizativas necesarias para preservar la seguridad de los datos recabados al objeto de protegerlos de divulgaciones o accesos no autorizados.

A estos efectos, SPB ha adoptado medidas apropiadas para garantizar la confidencialidad de todos los datos y se asegurará de que los datos relativos a la identidad del informante no sean transmitidos al denunciado durante la investigación, respetando en todo caso los derechos fundamentales de la persona, sin perjuicio de las acciones que, en su caso, puedan adoptar las autoridades judiciales competentes.

Además, se llevará a cabo una evaluación de impacto en la privacidad de los tratamientos necesarios para dar cumplimiento a las obligaciones establecidas en la misma y una evaluación del riesgo de dichos tratamientos con la finalidad de garantizar el funcionamiento respetuoso del Sistema Interno de Información.

Asimismo, para dar cumplimiento a las obligaciones en materia de transparencia e información establecidas en la citada normativa de protección de datos personales, se informa al denunciante y a la persona o personas denunciadas (el interesado), en su caso, de que sus datos serán incorporados a un sistema de tratamiento bajo la responsabilidad de SPB, con domicilio social en Plaza del Marqués de Salamanca, 3-4, 28006, Madrid, con las siguientes finalidades:

- **Gestionar la comunicación de cualesquiera hechos denunciables, adoptar las medidas correctivas correspondientes y, si fuera necesario, informar al denunciante** sobre el resultado del procedimiento (en el marco de dichas investigaciones se podrá realizar un análisis de correos electrónicos, sistemas informáticos o documentos y discos duros relevantes, verificación de pagos, declaraciones presentadas y recibos; también se podrán realizar entrevistas a los empleados de SPB o a terceras personas -físicas o jurídicas- y obtener información de terceras personas externas a SPB así como analizar los sistemas de videovigilancia o realizar inspecciones in situ en sus instalaciones).

- **Proteger a los empleados de SPB**, en particular, a aquellos que pudieran haber sufrido cualquier tipo de daño o perjuicio por razón de las conductas investigadas, pero, también, a aquellos sobre los que pudieran haber recibido denuncias infundadas.

- **Prevenir la comisión de conductas indebidas,** poniendo los medios necesarios para evitar que se incumplan obligaciones legales, contractuales o recogidas en los reglamentos internos de SPB en el futuro.

- **Ejercitar acciones (judiciales y extrajudiciales)** dirigidas a compensar y/o evitar daños o pérdidas económicas o de otro tipo para SPB para, de este modo, defender, ejercer y hacer valer sus derechos e intereses y los de sus empleados y clientes de forma efectiva.

- **Mejorar las estructuras de cumplimiento de SPB**, mediante la identificación y remoción de posibles puntos débiles en su organización interna de cumplimiento.

- **Proteger los valores corporativos de SPB**.

La LOPDGDD, así como la Ley de Protección al Informante, presumen lícitos los tratamientos realizados en el marco de la creación y mantenimiento de sistemas de información de denuncias internas. La Ley de Protección al Informante establece que dichos **tratamientos** se consideran **necesarios para el cumplimiento de una obligación legal** aplicable al responsable del tratamiento.

La **base legitimadora del resto de los tratamientos** anteriormente indicados es la protección de **intereses legítimos de SPB**, dirigida a evitar o minimizar el alcance para SPB (incluidos sus empleados, colaboradores y clientes) de los potenciales daños económicos y reputacionales derivados de las conductas denunciables o de una gestión deficiente de las denuncias realizadas a través del sistema. SPB dispone de los instrumentos y realizará los tratamientos necesarios para la defensa y ejercicio de acciones legales frente a los propios empleados y/o frente a terceros en el marco de procedimientos judiciales y extrajudiciales y ante las autoridades.

El acceso a los datos contenidos en el Sistema Interno de Información se limitará exclusivamente a quienes desempeñen funciones de control interno y cumplimiento de conformidad con lo establecido en la Política del Sistema de Información de SPB, incluidos las personas encargadas del tratamiento de datos designados eventualmente a tal efecto. Sólo cuando pudiera proceder la adopción de medidas disciplinarias contra algún empleado o socio, dicho acceso se permitirá al personal al equipo de RRHH.

Adicionalmente, sólo cuando sea necesario para la adopción de medidas correctivas o para la tramitación de procedimientos legales, **los datos serán cedidos a**:

- **Otras entidades del grupo al que pertenece SPB.** La base legitimadora del tratamiento es nuestro interés legítimo en llevar a cabo de forma adecuada y eficaz el proceso de denuncia de irregularidades. Dicha transferencia de datos intragrupo puede ser necesaria en particular si los hechos denunciados afectan a varias entidades del grupo dentro del E.E.E.

- **Tribunales, autoridades y otros organismos públicos.** Cuando sea aconsejable para proteger a nuestras compañías, empleados, colaboradores y clientes y/o lo exija la normativa aplicable. Esto puede implicar una transferencia a las autoridades fiscales, tribunales u otras autoridades españolas o extranjeras. La base legitimadora de estas cesiones será el interés legítimo de SPB en proteger los derechos y libertades de sus empleados, colaboradores y clientes y sus propios intereses económicos y, cuando la revelación sea obligatoria, el cumplimiento de las correspondientes obligaciones legales.

- **Proveedores de servicios.** Podemos recurrir al apoyo de empresas proveedoras de servicios externos, por ejemplo, asesores jurídicos, empresas auditoras, investigadore/as privados, personas especialistas en tecnologías de la información o asesores fiscales. La base legitimadora de esta cesión es nuestro interés legítimo en asegurarnos una correcta defensa y el ejercicio de reclamaciones legales, así como obtener asesoramiento adecuado sobre cómo gestionar una situación determinada para evitar daños y perjuicios para SPB.

Los datos introducidos en el Sistema Interno de Información **se conservarán durante el plazo estrictamente necesario para esclarecer los hechos denunciados**, quedando posteriormente bloqueados por los plazos de prescripción de las acciones e infracciones que pudieran derivarse de las actuaciones de SPB.

Transcurridos tres (3) meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, se procederá a su supresión, salvo que se decida su conservación para dejar evidencia del funcionamiento del Sistema Interno de Información.

El interesado podrá ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición al tratamiento de sus datos de carácter personal, dirigiendo su petición a la dirección postal indicada más arriba o al correo electrónico: DataProtectionOfficer@squirepb.com.

También podrá dirigirse a la Autoridad de Control, en este caso la Agencia Española de Protección de Datos, para presentar una reclamación, si lo considera oportuno.

Asimismo, si lo estima oportuno, el interesado puede realizar cualquier consulta respecto al tratamiento de sus datos personales a nuestro Delegado de Protección de Datos, dirigiendo su petición a la dirección de correo electrónico: DataProtectionOfficer@squirepb.com.

5. DERECHOS Y GARANTÍAS DEL INFORMANTE

Son derechos y garantías del informante, entre otros, los siguientes:

- Decidir si formula la comunicación de forma anónima o no.
- Formular la comunicación verbalmente o por escrito.
- Indicar un lugar seguro donde recibir las comunicaciones.
- Renunciar a recibir comunicaciones.

- Comparecer ante la Autoridad Independiente.
- Solicitar que la comparecencia sea realizada por videoconferencia.
- Ejercer los derechos de protección de datos personales.
- Conocer el estado y resultado de la denuncia.

5.1 Medidas de protección

El Sistema Interno de Información se rige por los principios de **confidencialidad, respeto y fundamentación**. Toda persona que denuncie de buena fe la comisión de alguna de las infracciones recogidas en el apartado 2.2 de esta Política gozará de la debida protección conforme a lo establecido en la normativa aplicable.

Las medidas de protección al informante también se aplicarán a:

a) Las personas físicas que, dentro de SPB, asistan al mismo proceso.

b) Las personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo y familiares del informante.

c) Las personas jurídicas para las que trabaje o con las que mantenga cualquier tipo de relación en un contexto laboral, o en las que ostente una participación significativa.

d) Los representantes legales de los informantes en el ejercicio de sus funciones de asesoramiento y apoyo.

El Sistema Interno de Información se ha diseñado para que el informante que desee mantenerse en el anonimato pueda hacerlo con las garantías suficientes. En este sentido, si el informante opta libremente por ocultar su identidad, el informe de resolución de la denuncia no hará referencia a la identidad del informante ni de las partes implicadas, en aras de garantizar la debida confidencialidad. Aun cuando el informante opte libremente por no ocultar su identidad, el informe de resolución de la denuncia se abstendrá de hacer referencia a la identidad del informante o de las partes implicadas, en aras de garantizar la debida confidencialidad.

Las medidas de protección también aplican a las personas afectadas, manteniendo todos sus derechos de tutela judicial y defensa, de acceso al expediente, de confidencialidad y reserva de identidad, de presunción de inocencia y al honor.

5.2 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. Se entiende por represalia cualquier conducta que esté prohibida por la ley, o que, de forma directa o indirecta, suponga un trato desfavorable que sitúe a los informantes, por tal condición, en desventaja particular con respecto a otra en el contexto laboral o profesional[2].

[2] A título enunciativo, se consideran represalias las que se adopten en forma de (i) 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,

Cualquier acción contra el empleado informante que pueda entenderse como amenaza, discriminación o represalia por efectuar una denuncia tendrá, en su caso, la consideración de infracción laboral en los términos establecidos en la legislación vigente que resulte de aplicación.

La prohibición de represalias no impedirá la adopción de las medidas disciplinarias que procedan cuando la investigación interna determine que la denuncia es falsa y que la persona que la ha realizado era consciente de su falsedad, habiendo actuado así con mala fe.

5.3 Medidas de protección frente a represalias

Los informantes no incurrirán en responsabilidad por la adquisición o acceso a la información objeto de comunicación, siempre que dicha adquisición o acceso no constituya un delito.

En los procedimientos ante un órgano jurisdiccional u otra autoridad relativos a los perjuicios sufridos por los informantes, si el informante demuestra razonablemente que la comunicación se hizo de conformidad con la Ley de Protección del Informante y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar. En tales casos, corresponderá a la persona que adoptó la medida perjudicial demostrar que obedecía a motivos debidamente justificados no vinculados a la comunicación realizada por el informante.

5.4. Exención y atenuación de sanciones

Si el propio informante hubiera participado en la comisión de una infracción administrativa objeto de la comunicación, y siempre que el informante lo comunique con anterioridad a la incoación del procedimiento, el órgano competente podrá eximirle de la sanción administrativa si (i) ha cesado en la comisión de la infracción, (ii) ha cooperado a lo largo del procedimiento de investigación, (iii) facilita información veraz y relevante y (iv) procede a la reparación del daño causado. Si no se cumplieran todos los requisitos en su totalidad, la posibilidad de atenuar la sanción al informante quedará a criterio de la autoridad correspondiente.

La atenuación de la sanción podrá extenderse al resto de los participantes en la comisión de la infracción, en función del grado de colaboración activa en el esclarecimiento de los hechos, identificación de otros participantes y reparación o minoración del daño causado.

---

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; (ii) daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo; (iii) evaluación o referencias negativas respecto al desempeño laboral o profesional; (iv) 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; (v) Denegación o anulación de una licencia o permiso; (vi) denegación de formación; y (vii) discriminación o trato desfavorable o injusto

6. PUBLICIDAD

Sin perjuicio de la obligación que tienen los empleados de conocer y actuar de conformidad con lo dispuesto en la normativa interna en el desempeño de sus funciones, se promoverá y velará por la debida difusión de esta Política y de la existencia del Sistema Interno de Información.

7. ENTRADA EN VIGOR

Esta Política entrará en vigor a partir del día 1 de diciembre de 2023 y su duración se presume indefinida.

ANEXO: Formulario del Sistema Interno de Información

SISTEMA INTERNO DE INFORMACIÓN	
Nombre y Apellidos	
DNI/NIE	
CP	
Población	
Correo electrónico	
Relación con la empresa*	
Hecho o conducta denunciada y lugar*	
Adjuntar documentación	
Nota: *Todos los campos marcados con asterisco (*) son obligatorios*	

A tenor de lo dispuesto en la normativa vigente y aplicable en materia de protección de datos personales, le informamos de que sus datos serán incorporados a un sistema de tratamiento bajo la responsabilidad de Squire Patton Boggs (UK) LLP, con la finalidad primordial de gestionar la comunicación de cualesquiera hechos denunciables, adoptar las medidas correctivas correspondientes y, si fuera necesario, informar al denunciante sobre el resultado del procedimiento. Puede ejercitar sus derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición al tratamiento de sus datos de carácter personal, dirigiendo su petición a la dirección postal de la compañía o al correo electrónico: sonia.zunzunegui@squirepb.comTambién podrá dirigirse a la Autoridad de Control, en este caso la Agencia Española de Protección de Datos, para presentar una reclamación, si lo considera oportuno.

Puede acceder a información completa acerca de cómo tratamos sus datos personales accediendo a la Política de sobre el Canal Interno de Información de Squire Patton Boggs UK LLP disponible en [Incluir URL o enlace a la Política].