# POLÍTICA PARA LA PREVENCIÓN DEL FRAUDE Y VIOLACIÓN DEL CÓDIGO ÉTICO

## Y PARA LA GESTIÓN DE COMUNICACIÓN DE INFRACCIONES EN MATERIA

## *"WHISTLEBLOWING"*

Sociedades:
**Esprinet Ibérica, V-Valley Advanced Solutions España, Esprinet Portugal**

Sede:
**Todas las sedes**

Subsistema:
**Código Penal, Reglamento UE 2016/679**

Nombre del fichero:
**ESDIS01001 Política para la prevención del fraude y violación del Código Ético y para la gestión de las denuncias en materia de *"Whistleblowing"***

Responsabilidad para el documento:

| Rev. | Fecha | Nota de Revisión | Redactado | Controlado | Aprobado |
|---|---|---|---|---|---|
| 00 | 01/03/16 | Actualización Whistleblowing | P. Aglianò<br>CRO | G. Monina<br>RIA | A.Cattani<br>AD |
| 01 | 15/10/18 | Actualización Whistleblowing | P. Aglianò<br>CRO | G. Monina<br>RIA | A.Cattani<br>AD |
| 02 | 29/06/21 | Actualización | P. Aglianò<br>CRO | G. Monina<br>RIA | A.Cattani<br>AD |
| 03 | 16/03/22 | Extensión a V-Valley Advanced Solutions España | P. Aglianò<br>CRO | G. Monina<br>RIA | A.Cattani<br>AD |
| 04 | 08/06/22 | Extensión a Dacom Spa | P. Aglianò<br>CRO | G. Monina<br>RIA | A.Cattani<br>AD |
| 05 | 13/11/23 | Adaptación a normativa portuguesa y Ley 02/2023 | A. Biffi<br>Risk Manager | G. Monina<br>RIA | A.Cattani<br>AD |

# INDICE

## 1. ALCANCE Y ÁMBITO DE APLICACIÓN

La presente política resume los principios establecidos por la Sociedad con el propósito de gestionar eficazmente la comunicación de comportamientos fraudulentos e ilegítimos y, en cualquier caso, en contra del Código Ético y del Modelo Organizativo de las Sociedades, y de cualesquiera de las normas vigentes que resulten de aplicación, por parte de todos los empleados (a partir de ahora simplemente Grupo Esprinet) y colaboradores del Grupo Esprinet.

La rigurosa aplicación de tales principios, no pueden prescindir de la participación de todos y a todos los niveles, bajo el supuesto de que el control interno solo puede ser efectivo a través de la contribución de todos los departamentos de la compañía, todos los empleados y colaboradores, así como las funciones de control y soporte.

Su contenido está inspirado en las principales mejores prácticas internacionales en el campo del control interno, en primer lugar, el sistema CoSo-ERM.

Este procedimiento controla el comportamiento de los receptores, como se define a continuación, con el fin de prevenir la comisión de uno o más delitos contemplados por los distintos Códigos Penales y dar cumplimiento a la normativa sobre protección de datos de carácter personal. En particular, este procedimiento tiene el propósito de:

- identificar las tareas y responsabilidades de la dirección/departamentos/unidades organizativas involucradas;
- regular e identificar la trazabilidad de los controles realizados;
- reducir al mínimo el riesgo de comisión de los delitos de conformidad con los distintos Códigos Penales;
- asegurarse de que cumplen con la normativa vigente y el sistema de procedimientos empresarial;
- cumplir con el principio de privacidad por defecto y desde el diseño previsto en el Reglamento (UE) 2016/679, de 17 de abril relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y la libre circulación de éstos;
- garantizar el cumplimiento del principio de confidencialidad, integridad, disponibilidad y trazabilidad de la información.

## 2. DESTINATARIOS

La presente política se aplica a todos los empleados, colaboradores[1] y clientes del Grupo Esprinet y a la parte relativa a las comunicaciones de infracción en materia de *Whistleblowing* de todos los Destinatarios del Código Ético y del Modelo Organizativo.

Será responsabilidad y deber de cada responsable de departamento, difundir los principios también entre los proveedores, consultores y colaboradores ocasionales.

[1] Se entienden por colaboradores, los empleados de los proveedores, los colaboradores de proyectos, los agentes y cualquier persona que trabaje permanentemente con el Grupo Esprinet.

## 3. TERMINOS Y DEFINICIONES

| | |
|---|---|
| **ABUSO** | Cualquier conducta que produzca o pueda producir un daño a la empresa, con la ventaja o beneficio directo o indirecto de otros, caracterizado por el uso distorsionado de la confianza y la elusión de las normas de la empresa. |
| **COSO ERM** | COSO ERM se define como un proceso puesto en marcha por la Alta Dirección, dirigido para identificar factores potenciales que pueden ejercer una influencia significativa en la organización y a proporcionar una seguridad razonable respecto a la consecución de los objetivos de la organización. |
| **FACTOR DE RIESGO** | Elemento que puede llevar a un aumento de la probabilidad de propagación de comportamientos fraudulentos e infieles que actúan sobre uno de los componentes del triángulo del fraude. |
| **EVALUACIÓN DEL RIESGO DE FRAUDE** | Es la evaluación del riesgo del fraude la que permite no sólo determinar "qué" podría causar un fraude y su impacto en la Sociedad, sino también comprender la eficacia de las medidas. |
| **FRAUDE** | Cualquier hecho que resulte de una conducta humana, caracterizada por el fraude, es decir, por una falsa representación de la realidad, o por el uso distorsionado de la confianza otorgada o por la elusión de las normas de la empresa que causen o puedan causar daño a la empresa, con el fin de obtener una ventaja o beneficio directo o indirecto para el autor o para otros. |
| **FRAUDE EXTERNO** | Fraude contra las sociedades del Grupo Esprinet, cometido por personas ajenas a la organización (clientes, proveedores, terceros) |
| **FRAUDE INTERNO** | Fraude contra las sociedades del Grupo Esprinet, cometido por sujetos de dentro de la organización (empleados) |
| **FRAUDE MIXTO** | Fraude contra una empresa, hecho gracias a la complicidad entre sujetos externos e internos de las sociedades del Grupo Esprinet (por ejemplo, acuerdo entre la Oficina de Compras y los proveedores) |
| **CONDUCTA IRREGULAR EMPRESARIAL** | Cualquier evento de naturaleza humana (conducta o elemento subjetivo) que causa o pueda causar un daño en la empresa |
| **INFRACCIÓN NORMATIVA** | Se entiende la comisión – o posible comisión – de un delito que sea aplicable la responsabilidad de las entidades de conformidad con el Código Penal español (Ley Orgánica 10/1995, de 23 de noviembre) y el Código Penal portugués (Decreto-Lei n.º 48/95). Estos delitos se enumeran en los distintos Códigos Penales y la restante legislación aplicable. |

| | |
|---|---|
| **IRREGULARIDAD** | Se consideran como tales infracciones de los procedimientos y normas previstos en el Código Ético y/o al Modelo Organizativo, Gestión y Control de las sociedades del Grupo Esprinet. |
| **INDICADOR DE RIESGO** | Elemento cuya variación es sintomática de un aumento del nivel de riesgo (ej. aumento de las operaciones «fuera de procedimientos») |
| **INDICADOR DE ANOMALÍA** | Señal de fraude potencial que requiere mayor investigación. (por ejemplo, reembolso de gastos anormales, consumo anormal de combustible, etc…) |
| **KPI ANTIFRAUDE** | Indicador de *performance* referido a uno o más controles antifraudes (ejemplo disminución de las diferencias inventaríales) |
| **RED FLAG** | Indicadores relevantes de fraude o abuso potencial como punto de partida para una auditoría. |
| ***WHISTLEBLOWING o SISTEMA INTERNO DE INFORMACIÓN*** | Un sistema de información mediante el cual una parte interesada que, mientras desarrolla su actividad laboral o mantiene una relación comercial con el Grupo Esprinet, detecta un posible fraude, agravio, infracción normativa, irregularidad, peligro u otro riesgo grave llevado a cabo por un empelado del Grupo Esprinet y/o un colaborador que puede perjudicar a clientes, colegas, accionistas, el público o la integridad y reputación de la empresa/entidad pública/fundación y decide realizar la comunicación al Grupo Esprinet. |
| Para las siguientes definiciones, véase también la "relazione sul governo societario e gli assetti proprietari" de conformidad con el artículo 123-bis TUF disponible para su consulta sobre el sitio institucional Esprinet – area investor relations | |
| **CCR** | Comité Control y Riesgo |
| **CdA** | Consejo de Administración |
| **AD** | Consejero Delegado |
| **AI** | Administrador Encargado del sistema de control interno |
| **RIA** | Responsable Internal Audit |
| **CdS** | Collegio Sindicale |
| **CRO** | Risk Manager |
| **SCIGR** | Acrónimo de Sistema de Control Interno y Gestión de Riesgos. Se define como el conjunto de normas, comportamientos, políticas, procedimientos y estructuras organizativas destinadas a permitir la identificación, medición, gestión y seguimiento de los principales riesgos de gestión, contribuyendo a asegurar la salvaguarda de los activos de la empresa, la eficiencia y eficacia de los procesos de la empresa, la fiabilidad de la información financiera, el cumplimiento de las leyes y reglamentos, así como los estatutos y procedimientos internos de la empresa. |

## 4. ACCIONES CONSTITUTIVAS DE FRAUDE

Por conductas fraudulentas y/o conductas contrarias al Código Ético, se entenderán todas aquellas acciones llevadas a cabo en contra de las reglas corporativas o a través del abuso de la confianza conferida por la Sociedad, con el objetivo de obtener una ventaja injusta. El fraude se define como la representación falsa de un hecho material (o del uso distorsionado de la confianza otorgada) para obtener, directa o indirectamente, una ventaja para el sujeto o para un tercero.

A modo meramente indicativo, a continuación, se indican algunas de las actividades ilegales que se consideran, a estos efectos, incluidas en el concepto de fraude:

- robo de activos del Grupo Esprinet;
- falsificación o alteración de documentos;
- falsificación o manipulación de cuentas y omisión intencional de registros, eventos o datos;
- destrucción, ocultación o uso inapropiado de documentos, archivos, muebles, instalaciones y equipos;
- malversación de dinero, objetos de valor, suministros u otros activos pertenecientes al Grupo Esprinet;
- dar una suma de dinero u otorgar otros beneficios a un funcionario público como contraprestación a sus posibles actuaciones, gestiones u omisiones en lo que respecta a las obligaciones o procedimientos a seguir (por ejemplo, simplificación de los procedimientos de aduana);
- aceptación de dinero, bienes, servicios u otros beneficios como incentivos para favorecer a los proveedores / empresas;
- informes de falsificación de gastos (por ejemplo, reembolsos "inflados" o transferencias falsas);
- falsificación de asistencia al trabajo;
- divulgación de información confidencial y de propiedad del Grupo Esprinet a partes externas (por ejemplo, competidores);
- uso de recursos y activos de la organización para uso personal sin autorización.

## 5. REFERENCIAS

| | |
|---|---|
| **LEYES Y REGLAMENTOS** | Código Penal español (Ley Orgánica 10/1995, de 23 de noviembre) |
| | Código Penal portugués (Decreto-Lei n.º 48/95) |
| | Lei n.º 34/87, de 16 de Julho |
| | Lei n.º 20/2008, de 21 de Abril |
| | 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 |
| | Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. |
| | Lei n.º 58/2019, de 08 de Agosto (Lei da Proteção de Dados Pessoais) |
| | RGPD (Reglamento 2016/679, de 17 de abril, del Consejo Europeo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos y la libre circulación de éstos) |
| | Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores |
| **PROCEDIMIENTOS Y DOCUMENTOS INTERNOS** | Código Ético |
| | Sistema disciplinario interno |
| | Modelo de organización, gestión y control de riesgos penales adoptado para España y Portugal |
| | Reglas para la correcta utilización de los Medios Informáticos |
| | Procedimiento Regalos de Mercancía |
| | Política Anticorrupción |
| | Política Conflictos de interés del Grupo Esprinet en España |
| | Procedimiento para la Gestión Partes Relacionadas |
| | Gestión Regalos, Donaciones y Patrocinio |
| | Gestión de las Visitas de Inspección |
| | Procedimiento de Gestión de Sistemas de Reconocimiento de Imágenes del Grupo Esprinet |
| | Procedimiento nota de gastos |
| | Linea de dirección para el Sistema de Control Interno y de Gestión del Riesgo |
| | Procedimiento en tema de Compras y Operaciones de Patrimonio |
| | Función encargada Privacy Grupo Esprinet |
| | Reglamento Interno Información Privilegiada |

## 6. ROLES Y RESPONSABILIDADES

### 6.1. Consejeros Delegados

Los Consejeros Delegados (o los departamentos correspondientes en las diferentes sociedades del Grupo Esprinet) asignan un amplio compromiso a los departamentos operativos delegados en la gestión del sistema de prevención del fraude y en la verificación de las comunicaciones de infracción de casos sospechosos y toman nota de las actividades realizadas, de las medidas aplicadas y de los casos detectados en los informes elaborados por el RIA.

Asimismo:

- serán informados sin demora por el Organismo de Vigilancia en los casos más graves que afecten a los altos directivos, a los miembros del Órgano de Control o a los otros componentes del Organismo de Vigilancia o que, en cualquier caso, puedan tener un impacto grave o afectar a la correcta gestión de la empresa;
- asumiendo medidas en los casos mencionados en el punto anterior.
- asumen la responsabilidad de implantar un Sistema Interno de Información en el Grupo Esprinet en España, nombrar el Responsable del Sistema de Información en el Grupo Esprinet en España y de adoptar el procedimiento de gestión de informaciones.

### 6.2. Los Organismos de Vigilancia del Grupo Esprinet en España como Responsable del Sistema Interno de Información

El Organismo de Vigilancia de la Sociedad de cada una de las sociedades del Grupo Esprinet en España ha sido designado como Responsable del Sistema Interno de Información, estando organizado de manera colegiada y siendo los miembros del mismo a quienes se les reconoce la suficiente competencia para la gestión de las comunicaciones reportadas a través de los canales habilitados. En este sentido, el órgano designado como responsable del Sistema Interno de Información ejercerá su cargo garantizando la ausencia de conflictos de intereses, así como de manera independiente y autónoma respecto del resto de órganos de la Sociedad, incluyendo al Consejo de Administración. La principal función del Responsable del Sistema Interno de Información será la gestión diligente del procedimiento de gestión de informaciones implementado por el Grupo Esprinet en España.

### 6.3. Chief Risk Officer

El CRO define las líneas guiadas de la presente *política*, identificando los riesgos de fraude en la fase de evaluación del riesgo de fraude, con otros riesgos operativos, de cumplimiento y de información financiera, y presenta al Comité de Control y Riesgos las mismas y sus actualizaciones o modificaciones.

Deberá prestarse especial atención a la evaluación del impacto fiscal de los actos fraudulentos.

Además, verifica la coherencia de los criterios específicos para evaluar los riesgos de fraude con respecto a las metodologías de análisis de riesgos más generales y la propensión al riesgo de la empresa (RAF – *Risk Appetite Framework*).

### 6.4. Comité de Control y Riesgo

El CCR examina la política presentada del CRO y propone posibles modificaciones e integraciones de la misma. También toma nota de las actividades desarrolladas, de las medidas implantadas y de los casos aplicados en el curso de las reuniones del comité a los cuales es llamado a participar el RIA.

Por lo que se refiere a los casos de comunicación de infracciones de Whistleblowing, el Organismo de Vigilancia de Esprinet S.p.A. es informado por el Organismo de Vigilancia de España o Portugal en la hipótesis de mayor gravedad que estén involucrados altos directivos, miembros del Órgano de Control u otros componentes del Organismo de Vigilancia o que, en cualquier caso, puedan tener un impacto grave o afectar a la correcta gestión de la empresa.

### 6.5. Internal Audit

*Internal Audit*:

- realiza análisis en profundidad sobre los informes del Organismo de Vigilancia;
- si durante la realización de las actividades de auditoría tiene conocimiento de presuntos fraudes o infracciones de normativa o del Código Ético, realizará una evaluación preliminar de los mismos y lo notificará al Organismo de Vigilancia;
- complementa su informe periódico al Consejo de Administración con la evolución del sistema de prevención fraude y con las eventuales medidas adoptadas.

### 6.6. Recursos Humanos

El Responsable de los Recursos Humanos:

- Será informado de los hechos objeto de comunicación por parte del informante e intervendrá prestando soporte al Organismo de Vigilancia sólo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador o interviniera como instructor del proceso de investigación. En el caso de hechos de relevancia penal, seguidos de la presentación de una denuncia o querella, y no se hayan producido infracciones disciplinarias independientes, procede a la contestación inmediata, valorando caso por caso si suspender o no el procedimiento disciplinario hasta la definición del procedimiento penal.

### 6.7. Oficina Legal

El Abogado interno:

- Podrá ser informado de los hechos objeto de comunicación por parte del informante, así como intervenir prestando soporte al Organismo de Vigilancia, evaluando el carácter delictivo de los hechos presuntamente ocurridos y verificando, con la ayuda de abogados externos, si el delito es punible de oficio o mediante denuncia de una de las partes.

### 6.8. Responsables de Departamento

Los Responsables de Departamento representan el control de primer nivel y deben constantemente recordar que con su ejemplo pueden contribuir eficazmente a la difusión de comportamientos virtuosos y respetuosos de los valores y normas de la empresa, en relación con los cuales no dejarán de sensibilizar a sus colaboradores en cada ocasión favorable.

Estos están obligados:

- a comunicar al OdV cualquier sospecha de violación del Modelo Organizativo o del Código Ético, de las normas y procedimientos de la empresa o de conductas que puedan constituir fraude o infracción normativa, interviniendo con prontitud para evitar la continuación de conductas perjudiciales para la empresa;
- a mantener confidencial la identidad del empleado o quién le informe de cualquiera de los hechos a los que se refiere el punto anterior;
- a evitar comportamientos discriminatorios o vejatorios y en general represalias hacia quienes comuniquen los hechos mencionados en los puntos anteriores;
- a comunicar con prontitud las situaciones de conflicto de intereses para sí mismos o para sus colaboradores, incluidas las relativas a los miembros de su familia, absteniéndose de tomar decisiones o de intervenir en cualquier caso en los procesos de toma de decisiones que puedan integrar dichas situaciones;
- a no utilizar información empresarial para fines privados;
- a asumir comportamientos de forma justa e imparcial;
- a repartir equitativamente la carga de trabajo entre sus empleados, en función de sus competencias, actitudes, profesionalidad y respeto de sus deberes;
- a hacer evaluaciones imparciales del personal;
- a difundir las buenas prácticas y los buenos ejemplos, fortaleciendo el sentido de confianza y perteneciente a la empresa.

## 7. VALORACIÓN DEL RIESGO DE FRAUDE Y CONDUCTAS CONTRARIAS AL CÓDIGO ÉTICO

El riesgo de fraude y conducta contraria al Código Ético es de carácter transversal, ya que puede tener un impacto no sólo en las pérdidas económicas sino también en la imagen corporativa y en el comportamiento fisiológico de las operaciones.

Por lo tanto, para que la evaluación del riesgo sea eficaz, habrá que tenerla en cuenta:

- daños directos (valor material del activo de la empresa afectada y/o sanción en caso de implicación legal de la empresa), daños indirectos (coste de las medidas necesarias para restablecer la normalidad de las operaciones – sin cambios) y daños consecuentes (daños a la imagen o a la reputación con posibles repercusiones en la pérdida de cuotas de mercado);
- del análisis de los casos que se han producido en otras empresas (*fraud business case*) y que se han dado a conocer a través de los medios de comunicación.

Los Responsables de Departamento contribuirán a un análisis y evaluación de riesgos eficaz mediante una cooperación abierta y leal con el *Chief Risk Officer* y el RIA, proporcionando los datos e información necesarios y su profundo conocimiento de los procesos de negocio.

## 8. CANALES INTERNOS DE INFORMACIÓN

La detección de posibles casos de fraude puede beneficiarse de la contribución leal de todos los empleados y destinatarios de esta política.

La totalidad de los empleados del Grupo Esprinet tienen la obligación de informar, a través de los canales indicados en el siguiente apartado y habilitados por la Sociedad, de cualquier fraude, violación o incumplimiento del Código Ético y del Modelo Organizativo e infracciones normativas que se hayan producido o se tenga mera sospecha de ello.

### 8.1. Whistleblowing

Por *whistleblowing* se entiende la posibilidad de comunicar casos de posibles delitos, infracciones normativas, sospechas de fraude y/o violaciones del Código Ético y del Modelo Organizativo, de los cuales los empleados y los colaboradores hayan tenido conocimiento por motivos laborales, con la garantía de una protección absoluta de la identidad del informante, con el objetivo de evitar cualquier tipo de discriminación contra el mismo.

En cada caso, es deber primordial de los empleados y/o colaboradores la comunicación al Organismo de Vigilancia competente y la adopción por parte de este de todas las medidas destinadas a garantizar la confidencialidad de la identidad del denunciante.

Con tal fin, la empresa pone a disposición los siguientes canales de denuncia:

- por carta al ORGANISMO DE VIGILANCIA en función del país de la Sociedad a la que se traslade la denuncia:
    - España:
        - Esprinet Ibérica. Calle Osca 2 -Campus 3·84 - Pol. PLAZA (Plataforma Logística de Zaragoza), 50197, Zaragoza, España

- V-Valley Advanced Solutions España, S.A.U. Calle Osca 2 -Campus 3·84 - Pol. PLAZA (Plataforma Logística de Zaragoza), 50197, Zaragoza, España

- Portugal:

  - Edificio AVIZ Trade-Center Rua Eng. Ferreira Dias, 924, 1º - Escritório E19 4100-246, Porto, Portugal

- plataforma de *Whistleblowing* accesible desde cualquier navegador (incluso en dispositivos móviles) con la siguiente dirección https://esprinet.eticainsieme.it. Este último instrumento ofrece las más amplias garantías de confidencialidad para el informante y la posibilidad de realizar comunicaciones anónimas.

- Correo electrónico remitido al Organismo de Vigilancia de:
  - Esprinet Ibérica, SLU: odveib@esprinet.com
  - V-Valley Advanced Solutions España, SAU: odv@v-valley.es
  - Esprinet Portugal, LdA: odvep@esprinet.com

- Por medio de una reunión presencial entre el informante y los miembros del Organismo de Vigilancia de competencia. Dicha reunión deberá ser celebrada dentro de un plazo máximo de siete (7) días desde la solicitud del informante.

  La reunión presencial deberá ser documentada, previo consentimiento por parte del informante, mediante:
  - Grabación de la conversación en formato seguro, duradero y accesible, informando sobre los derechos en materia de protección de datos; o
  - Transcripción completa y exacta de la conversación, permitiendo la comprobación, rectificación y aceptación mediante firma del informante.

  En caso de que el informante no preste el consentimiento mencionado, el Organismo de Vigilancia levantará acta de la reunión mantenida.

Adicionalmente, las personas que tengan conocimiento de una información que pueda entrañar la comisión de una infracción normativa o de un delito, también podrán notificar los hechos objeto de comunicación a través de los canales habilitados por las autoridades públicas nacionales competentes o, en su defecto, por las autoridades competentes de las comunidades autónomas que hayan designado a un organismo a tal efecto.

El Grupo Esprinet en España y Portugal ha adoptado un procedimiento de gestión de comunicación de infracciones normativas.

### 8.2. Contenido de la infracción

El informante debe proporcionar todos los elementos que conozca para verificar, con la debida diligencia, los hechos reportados. En particular, el informe debe ser detallado y completo para que se pueda establecer el hecho comunicado y debe contener los siguientes elementos esenciales:

- los datos de la persona que realiza la comunicación de infracción, indicando su rol actual o anterior en la empresa, excepto cuando el informante decida realizar la comunicación de forma anónima. De hecho, el informante tiene derecho a realizar la comunicación de forma anónima;
- una descripción clara y completa de los hechos objeto de la denuncia;
- las circunstancias del momento y lugar en que se cometieron los actos comunicados;
- los detalles de la persona que ha implementado los hechos comunicados;
- las indicaciones de los beneficiarios y de las personas afectadas por el acto ilícito o de la infracción;
- las indicaciones de otras personas que puedan informar sobre los hechos objetos de la infracción;
- el archivo adjunto de los documentos que puedan confirmar la validez los hechos denunciados; y
- cualquier otra información que pueda proporcionar información útil sobre la existencia de los hechos comunicados.

La comunicación deberá prever asimismo la necesidad de que el informante declare su compromiso de comunicar lo que sabe a su leal saber y entender.

### 8.3. Plataforma de comunicación de infracción

La plataforma de comunicación adoptada, alojada en el servidor de un tercero, prevé el registro confidencial, el uso de técnicas de cifrado y una ruta guiada para que el informante pueda introducir la información necesaria enumerada en el apartado 8.2. Así mismo, dicha plataforma permite la realización de comunicaciones anónimas.

El informante deberá rellenar una serie de preguntas abiertas y cerradas, lo que permitirá al receptor de la comunicación profundizar en el tema de este en primera instancia, incluso sin crear un contacto directo con el propio informante.

Al final del proceso de comunicación, la plataforma acusará recibo de la misma y proporcionará al informante un código que le permitirá acceder al sistema y, por lo tanto, a su comunicación para:

- control del progreso del proyecto;
- integrar su conocimiento con elementos de hechos adicionales u otra documentación;
- tener un contacto directo con los destinatarios de la comunicación, iniciando también eventuales intercambios de solicitudes e información.

### 8.4. Gestión de las comunicaciones de infracción

El destinatario notificará al informante la recepción de la comunicación en un plazo máximo de 7 días a partir de su recepción, y la analizará en un plazo de 15 días, con la posibilidad de involucrar a las otras figuras y departamentos identificados en los párrafos anteriores sobre la base de una evaluación preliminar de la gravedad del objeto del informe y de los posibles sujetos y departamentos implicados en los hechos denunciados.

A través del uso de la plataforma, existe la posibilidad de intercambiar solicitudes entre el informante y los destinatarios de la infracción al fin de profundizar los temas objeto de comunicación.

Se llevarán a cabo los controles apropiados, incluidas las posibles audiencias con el informante si da el consentimiento, en el caso en el que la comunicación de infracción resultase fundada serán informadas los departamentos empresariales de la empresa donde se emprenden las acciones disciplinarias que involucran a los órganos de gestión y el control de la Sociedad.

En un plazo máximo de 90 días (3 meses) desde que se interpuso la comunicación por parte del informante, el órgano competente debe completar la investigación preliminar e informar a la parte informante del resultado. Adicionalmente y para casos de especial complejidad, el plazo podrá ser ampliado hasta un máximo de otros tres (3 meses), sumando un total de seis (6) y debiendo el Organismo de Vigilancia aportar motivos que justifiquen dicha extensión temporal.

En cualquier momento después de recibir la comunicación, los destinatarios pueden archivarla si lo consideran irrelevante según esta Política.

Al final de la investigación, los destinatarios redactarán un informe tomando una o más de las siguientes medidas:

- archivo de la comunicación por irrelevancia;
- propuesta para modificar el Modelo de Organización, Gestión y Control, políticas y procedimientos internos y/o al Código Ético;
- propuesta para iniciar procedimientos disciplinarios o sancionadores – de conformidad a lo previsto en el Modelo de Organización, Gestión y Control – en relación con los hechos comunicados y por los cuales se ha reconocido la comisión de un delito o irregularidad;
- propuesta para iniciar procedimientos disciplinarios o sancionadores – de acuerdo con las disposiciones del Modelo de Organización, Gestión y Control y de este procedimiento, con respecto a los denunciantes que hayan presentado denuncias infundadas, basadas en circunstancias falsas y realizadas con dolo o negligencia grave.

### 8.5. Registro de información

La Plataforma utilizada por la empresa permite el almacenamiento de las informaciones recibidas y de la documentación adjunta de forma informatizada y encriptada y de conformidad con la normativa aplicable en materia de protección de datos.

Dicho registro se gestiona de forma informatizada y encriptada y de acuerdo con la legislación aplicable en materia de protección de datos de carácter personal. Asimismo se informa que el registro no será público y únicamente podrá acceder al mismo la Autoridad judicial competente que presente una solicitud razonada mediante auto dictado en el marco de un procedimiento judicial.

Cualquier otra documentación producida por los destinatarios de las comunicaciones será archivada y se conservará manteniendo la confidencialidad.

## 9. PROTECCIÓN DE DATOS PERSONALES Y ACCESO A LOS DATOS

El Grupo Esprinet se compromete a cumplir con la normativa en materia de protección de datos y a adoptar las medidas organizativas y técnicas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos tratados en el marco del proceso de gestión de comunicación de infracciones.

En cualquier caso, se limitará el acceso a los datos personales contenidos en el expediente y/o de los hechos objeto de comunicación a las siguientes personas:

- El Organismo de Vigilancia competente y a quien lo gestione directamente;
- Responsable de Recursos Humanos, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo;
- El responsable de los servicios jurídicos de la entidad, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación;
- Encargados de tratamiento que eventualmente se designen;
- Delegado de Protección de datos

Los informantes, las personas afectadas y los demás sujetos involucrados podrán ampliar la información relativa al tratamiento de los datos personales informados a través de privacy@esprinet.com (para Esprinet Ibérica, S.L.U. y Esprinet Portugal, LdA) o mediante privacy@v-valley.com (para V-Valley Advanced Solutions España). Asimismo, también podrá contactar con el Data Protection Officer del grupo Esprinet en España por medio de la siguiente dirección de correo electrónico: dpo@esprinet.com.

## 10. OTROS SISTEMAS DE DETECCIÓN

### 10.1. Actividad ordinaria de Auditoria

Internal Audit, durante el desarrollo de verificaciones ordinarias previstas en el Plan de Auditoría, podría detectar signos de comportamiento fraudulento o violaciones graves del Código Ético (por ejemplo, *red flag*).

También en estos casos se lleva a cabo una evaluación preliminar según lo establecido en la presente política.

### 10.2. Reclamaciones de clientes

Las reclamaciones de clientes, además de requerir una intervención rápida por motivos de satisfacción de cliente, puede implicar aspectos fraudulentos o conductas contrarias al Código Ético.

Por esta razón, cualquiera que reciba tales quejas debe evaluarlas cuidadosamente e informar al Organismo de vigilancia solo en los casos más graves.

En tal caso, cuando la reclamación del cliente consista en la potencial comisión de una infracción de la normativa interna y/o externa al Grupo Esprinet, esta deberá ser comunicada a través de los canales de información habilitados por la Sociedad y referenciados en el apartado 8.1 de la presente Política.

Asimismo, tal y como se ha informado anteriormente, las infracciones también podrán ser comunicadas a través de los canales de información adoptados por las autoridades públicas competentes, ya sea a nivel nacional o autonómico

## 11. TUTELA DEL INFORMANTE

El Grupo Esprinet reconoce unos determinados derechos a las personas que adoptan la posición de informante, ello desde el momento en que la Sociedad recibe las informaciones comunicadas por el mismo. De este modo, se garantiza el respeto a la confidencialidad de cualquier dato proporcionado y a la reserva de la identidad del informante y/o el anonimato del mismo cuando así lo hubiera decidido el mismo. Dichos derechos son garantizados a lo largo de la tramitación del expediente en cuestión.

Excepto en los casos en que exista responsabilidad penal por calumnia o difamación (en estos casos, la Sociedad informará al informante antes de proceder a la revelación de su identidad, salvo que dicha revelación pudiera perjudicar la investigación o el procedimiento judicial en curso), la identidad del informante está protegida en cada una de las fases del proceso de gestión de infracciones. Por tanto, la identidad del informante no puede revelarse sin su consentimiento expreso y todos los que reciben o participan en la gestión de las comunicaciones están obligados a proteger su confidencialidad.

La violación de la obligación de confidencialidad representa una violación grave disciplinaria.

Asimismo, cualquier forma de represalia o discriminación contra el informante y las personas afectadas constituye una infracción disciplinaria grave.

En cualquier caso, el despido por represalia o discriminatorio de la persona que comunica los hechos objeto de la comunicación de infracción es nulo y sin efecto. La modificación de los derechos laborales también es nula y sin efecto.

Por último, en caso de litigios relacionados con la imposición de sanciones disciplinarias o la degradación, el despido, el traslado o la sumisión del informante a otra medida organizativa que tenga efectos negativos directos o indirectos sobre las condiciones de trabajo, es responsabilidad de la empresa demostrar que tales medidas no son en modo alguno consecuencia del propio informe.

### 11.1. Comunicaciones No permitidas

Las comunicaciones de infracción deben tener siempre un contenido del que surge un leal espíritu de participación en el control.

También está prohibido:

- El uso de expresiones injuriosas;
- La transmisión de denuncias con fines puramente difamatorios o calumniosos;
- La emisión de denuncias que se refieran exclusivamente a aspectos de la vida privada, sin ninguna relación directa o indirecta con las actividades empresariales. Estos informes se considerarán aún más serios cuando se refieran a hábitos, orientación sexual, religiosa y política.

## 12. TUTELA DE LA PERSONA AFECTADA

Del mismo modo que el Grupo Esprinet garantiza el respeto de los derechos de las personas informantes, también reconoce una serie de derechos a favor de las personas afectadas, es decir, aquellas que han sido acusadas de cometer una infracción de la normativa interna y/o externa con carácter presunto.

En este sentido, la Sociedad dirige esta Política considerando el derecho de tutela judicial y de defensa, de acceso al expediente bajo los términos de las leyes aplicables, de confidencialidad y, especialmente, el de presunción de inocencia.

La persona afectada tiene derecho a que no se revele su identidad sin su consentimiento expreso, salvo cuando constituya una obligación necesaria y proporcionada impuesta por la legislación vigente o en el curso de una investigación en el marco de un proceso judicial. La persona afectada tiene derecho a un proceso sin dilaciones indebidas y con todas las garantías.

La persona afectada tiene derecho a conocer que existe una comunicación de infracción en su contra y será informada al respecto en el plazo más breve posible, siempre y cuando no comprometa la investigación, y antes de su declaración.

## 13. FLUJOS DE INFORMACIÓN HACIA EL ORGANISMO DE VIGILANCIA

Toda persona que tenga conocimiento de violaciones de la presente Política por parte de los Destinatarios debe notificar inmediatamente al Organismo de Vigilancia de la Sociedad específica o, de acuerdo con la Política DIS01001 Política para la prevención del fraude y violación del Código Ético y para la gestión de las denuncias en materia de "Whistleblowing", hacer una denuncia a través de la plataforma de denuncias.

## 14. CUMPLIMIENTO

El incumplimiento de las normas y estándares éticos compromete al Grupo Esprinet. Por ello, todos los Colaboradores deberán conocer y respetar el contenido de la presente Política.

El incumplimiento de los contenidos de esta Política y del Modelo de Organización y Gestión, del Código Ético y de la normativa interna de la empresa podrá generar la interposición de las sanciones, proporcionales a la gravedad de los hechos, previstas por la normativa laboral aplicable o las consecuencias indicadas por las cláusulas contractuales.

## 15. ARCHIVO

La copia original en papel de esta política se encuentra archivada en el Departamento de Internal Audit, con evidencia de firmas de redacción, control y aprobación.

Una copia se archiva en el sistema de documentación de la empresa.