POLÍTICA PARA LA PREVENCIÓN DEL FRAUDE Y VIOLACIÓN DEL CÓDIGO ÉTICO Y PARA LA GESTIÓN DE LAS DENUNCIAS EN MATERIA *"WHISTLEBLOWING"*

Sociedades:
Esprinet Spa, V-Valley Srl, Esprinet Ibérica, Vinzeo Technologies, V-Valley Advanced Solutions España, Esprinet Portugal, Dacom Spa

Sede:
Todas las sedes

Subsistema:
D.Lgs. 231/01, Código Penal, L. 179/2017, Reglamento UE 2016/679, Código penal portugués

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 CRO	G. Monina RIA	A.Cattani AD
01	15/10/18	Actualización Whistleblowing	P. Aglianò CRO	G. Monina RIA	A.Cattani AD
02	29/06/21	Actualización	P. Aglianò CRO	G. Monina RIA	A.Cattani AD
03	16/03/22	Extensión a V-Valley Advanced Solutions España	P. Aglianò CRO	G. Monina RIA	A.Cattani AD
04	08/06/22	Extensión a Dacom Spa	P. Aglianò CRO	G. Monina RIA	A.Cattani AD

INDICE

1. ALCANCE Y ÁMBITO DE APLICACIÓN

La presente política resume los principios establecidos por la Sociedad con el propósito de prevenir y contrastar eficazmente comportamientos fraudulentos e ilegítimos y, en cualquier caso, en contra del Código Ético, del Modelo Organizativo ex D.Lgs. 231/01, y de cualesquiera de las normas vigentes que resulten de aplicación, por parte de todos los empleados del Grupo Esprinet (a partir de ahora simplemente 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 mas delitos contemplados por D. Lgs. 231/01 y 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 minimo el riesgo de comisión de los delitos de conformidad con D. Lgs. 231/01 y 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 y colaboradores[1] del Grupo Esprinet y a la parte relativa a las denuncias 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
ILÍCITO (relevante también a las denuncias Whistleblowing)	Se entiende la comisión – o posible comisión – de un delito que sea aplicable la responsabilidad de las entidades de conformidad con el D. Lgs 231/01 para Italia y el Código Penal español (Ley Orgánica 10/1995, de 23 de noviembre), el Código Penal portugués (Decreto-Lei n.º 48/95). Estos delitos se enumeran en el mismo de D. Lgs 231/01 y en los distintos Códigos Penales.

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	Un sistema de información mediante el cual un trabajador que, mientras trabaja en una empresa, detecta un posible fraude, agravio, irregularidad, peligro u otro riesgo grave que pueda perjudicar a clientes, colegas, accionistas, el público o la integridad y reputación de la empresa/entidad pública/fundación y decide realizar la denuncia
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 UN 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	D.lgs. n. 231/01
	D.Lgs. n. 196/2003
	D.Lgs. n. 151/2015
	CCNL Commercio
	Legge n. 300/1970 (Statuto dei Lavoratori)
	Código Penal español (Ley Orgánica 10/1995, de 23 de noviembre)
	Código Penal portugués (Decreto-Lei n.º 48/95)
	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales
	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
	Modello "231" adoptado para el Grupo Esprinet Italia / 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
	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
	Encargado Privacy Grupo Esprinet
	Reglamento Interno di *Internal Dealing*
	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) asignan un amplio compromiso a los departamentos operativos delegados en la gestión del sistema de prevención del fraude y en la verificación de las denuncias 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.

6.2. 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*).

6.3. 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 REALIZADAS, DE LAS MEDIDAS IMPLEMENTADAS 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 denuncias de Whsitleblowing, el CCR es informado por el Organismo de Vigilancia 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.

6.4. 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 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.

6.5. Recursos Humanos

El Responsable de los Recursos Humanos:

- procede sin demora a la elaboración de la denuncia y a la investigación del procedimiento relativo en caso de que el Organismo de Vigilancia y los Administradores Delegados reciban pruebas de hechos significativos que afecten disciplinariamente a un empleado. 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.

6.6. Oficina Legal

El Abogado interno:

- evalúa el carácter delictivo de lo que ha surgido durante el examen y el análisis en profundidad de las denuncias de presuntos fraudes o violaciones del Modelo Organizativo o del Código Ético, verificando, con la ayuda de abogados externos, si el delito es punible de oficio o mediante denuncia de una de las partes. En este último caso, presenta las denuncias oficiales al Consejero Delegado para que las firme y las presenta a la Policía Judicial o a las Oficinas Judiciales competentes por medio de abogados externos.

6.7. 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 conducta ilícita, interviniendo con prontitud para evitar la continuación de conductas perjudiciales para la empresa;
- a mantener confidencial la identidad del empleado que le informe de cualquiera de los hechos a los que se refiere el punto anterior;

- a evitar comportamientos discriminatorios o vejatorios hacia quienes denuncien 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

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. CANAL DE DENUNCIAS Y TUTELA DEL DENUNCIANTE

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

Todo el mundo está obligado a informar al Organismo de Vigilancia de cualquier caso de sospecha de fraude o violación del Código Ético y del Modelo Organizativo del que tenga conocimiento, de acuerdo con las siguientes disposiciones.

8.1. Whistleblowing

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

En cada caso, es deber primordial del destinatario de la denuncia (Organismo de Vigilancia 231, o en alternativa RIA y CRO, en el caso de denuncias Whistleblowing) adoptar 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:
    - Italia:
        - Esprinet S.p.A. c/o Energy Park 20871 Vimercate (MB)
        - Dacom S.p.A. c/o Via Pregnana 32-20010 Cornaredo (MI)
    - España o Portugal: Esprinet Ibérica. Calle Osca 2 -Campus 3·84 - Pol. PLAZA (Plataforma Logística de Zaragoza), 50197, Zaragoza, España
- 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 denunciante.

8.2. Contenido de las denuncias

El denunciante 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 denunciado y debe contener los siguientes elementos esenciales:

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

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

8.3. Plataforma de denuncia

La plataforma de denuncia adoptada, alojada en el servidor de un tercero, prevé el registro confidencial, el uso cifrado y una ruta guiada para el denunciante que le permitirá introducir la información necesaria enumerada en el apartado 8.2.

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

Al final del proceso de denuncia, la plataforma proporcionará al denunciante un código que le permitirá acceder al sistema y, por lo tanto, a su denuncia para:

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

8.4. Gestión de las denuncias

Una vez recibida la denuncia, el destinatario de esta, tras haber evidenciado al denunciante – lo analizará en un plazo de 15 días, con la posibilidad de involucrar a las demás 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 denunciante y los destinatarios de la denuncia al fin de profundizar los temas objeto de comunicación.

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

Dentro de los 60 días, los destinatarios de la denuncia deben completar la investigación preliminar e informar a la parte del denunciante del resultado.

En cualquier momento después de recibir la denuncia, los destinatarios pueden archivarlo si lo consideran irrelevante según este procedimiento.

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

- archivo del informe por irrelevancia;
- propuesta para modificar el Modelo de Organización, Gestión y Control 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 temas denunciados 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. Archivo

La Plataforma utilizada por la empresa permite el almacenamiento de los informes y documentación adjunta de forma informatizada y encriptada y de acuerdo con la legislación aplicable en materia de protección de datos de carácter personal.

Cualquier otra documentación producida por los destinatarios de los informes se archivará y mantendrá confidencial.

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

8.6. Información sobre el tratamiento de datos derivados de la gestión de denuncias

De acuerdo con la normativa vigente en materia de Protección de Datos, informamos a los interesados que sus datos personales serán tratados por la empresa del Grupo Esprinet que reciba la denuncia con la finalidad de tramitar esta denuncia.

Los datos personales y demás información manifestada en la denuncia podrán ser puestos en conocimiento de las figuras y departamentos identificados en los párrafos anteriores para la correcta investigación y tramitación de la misma.

La base que nos legitima para el tratamiento de sus datos es el propio interés legítimo del *Data Controller*, quien en cumplimiento de su Sistema de Compliance Penal, ha previsto gestionar las denuncias presentadas por los interesados ante cualquier incumplimiento de esta Política, del Código Ético o demás normativa interna.

<u>Calidad de los datos</u>

Los hechos o conductas contenidos en una denuncia deberán tener una implicación real en la relación contractual que vincula al denunciado con el Grupo Esprinet.

Los denunciantes deben garantizar que los datos personales contenidos en la denuncia son verdaderos, exactos y actualizados.

En este sentido, los datos personales proporcionados como parte de la denuncia serán tratados de acuerdo con la normativa aplicable en materia de protección de datos para los fines legítimos relativos a la investigación que, en su caso, derive de la denuncia, no pudiendo ser usados para finalidades incompatibles con dicho propósito y deberán ser adecuados y no excesivos a tales efectos.

Derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento de datos o revocación del consentimiento

Cada una de las empresas que integran el Grupo Esprinet será considerada *Data Controller* de denuncias efectuadas siguiendo el procedimiento regulado en la presente Política cuando éstas afecten a su personal.

Los titulares de los datos podrán ejercitar sus derechos de acceso, rectificación, cancelación, oposición, solicitar la limitación del tratamiento de sus datos o revocar su consentimiento en cualquier momento, de acuerdo con los procedimientos y con los límites establecidos por la legislación vigente en cada momento, para lo cual deberán enviar un correo electrónico a privacy@esprinet.com (Dacom Spa: privacy@dacomaidc.com; Vinzeo Technologies: privacy@vinzeo.com; V-Valley y V-Valley Advanced Solutions España: privacy@v-valley.com), indicando el derecho concreto que desean ejercitar.

En caso de ejercitar el derecho de acceso, el interesado debe saber que el ejercicio del derecho de acceso estará limitado a sus propios datos personales, no quedando comprendidos por el ejercicio de tal derecho a los datos del denunciante.

Comunicación y transferencia de datos

Además, los datos relacionados con las denuncias podrán ser comunicados a las restantes empresas del Grupo, cuyas denominaciones y domicilios figuran en la página web www.esprinet.com cuando el Órgano interno encargado de la denuncia considere que su intervención resulte necesaria para la investigación y esclarecimiento de los hechos. En estas circunstancias, las empresas del Grupo a las que se comuniquen los datos actuarán como *Data Controller*. La empresa que les comunique dichos datos se asegurará de que se obligan a cumplir escrupulosamente las obligaciones de protección de datos que sean aplicables, de acuerdo con los estándares de privacidad vigentes tanto en España como en la Unión Europea.

Además, los datos recibidos a través del sistema de denuncias internas descrito en esta Política podrán ser facilitados a otras entidades que presten servicios de asesoramiento necesarios para la correcta gestión de las denuncias, que actuarán como encargados del tratamiento.

Retención de registros y plazo de conservación

Los datos que sean objeto de tratamiento en el marco de las investigaciones serán cancelados tan pronto como éstas hayan finalizado, salvo que de las medidas adoptadas se deriven procedimientos disciplinarios, administrativos o judiciales, en cuyo caso se cancelarán el día de la finalización de los mismos siempre que no cupiese recurso alguno frente a la resolución disciplinaria o judicial o una vez transcurrido el plazo

legalmente previsto para ello.

Los datos personales relativos a denuncias que no den lugar a investigación deberán ser cancelados de forma inmediata o en un plazo máximo de 15 días.

La cancelación consistirá en el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de Administraciones Públicas, Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido este plazo, ser procederá a la supresión de los datos.

Se adoptarán las medidas que garanticen la adecuada seguridad y confidencialidad de la información, pudiendo establecerse medidas reforzadas de seguridad y extremando las cautelas que garanticen el cumplimiento del deber de confidencialidad teniendo en cuenta la naturaleza de los datos recabados. Igualmente se implantará una estricta política de control de acceso restringido al personal autorizado para acceder al buzón de denuncias.

9. OTROS SISTEMAS DE DETECCIÓN

9.1. Denuncias al Organismo de Vigilancia

El Organismo de Vigilancia (OdV), además de los flujos ordinarios de información, debe recibir informes de presuntas violaciones del Modelo Organizativo que puedan constituir un riesgo "231" o riesgo penal directo o indirecto.

Esta información es necesaria para que el Organismo pueda adoptar medidas oportunas para prevenir la comisión de delitos previstos en el D.Lgs. n. 231/2001, el Código Penal español (Ley Orgánica 10/1995, de 23 de noviembre) y el Código Penal portugués (Decreto-Lei n.º 48/95 y vigilar el cumplimiento de las normas que forman parte integrante del propio Modelo.

9.2. 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 el capítulo 13.

9.3. 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.

10. PROTECCIÓN DEL DENUNCIANTE

Excepto en los casos en que exista responsabilidad penal por calumnia o difamación según las disposiciones o el artículo 2043 c.c. o la normativa correspondiente a los distintos países de las Sociedades del Grupo Esprinet, la identidad del denunciante está protegida en cada una de las etapas posteriores al propio informe.

Por tanto, la identidad del denunciante no puede revelarse sin su consentimiento expreso y todos los que reciben o participan en la gestión de los informes 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 denunciante, que está obligado a denunciar dicha conducta a su superior directo o directamente al Organismo de Vigilancia, constituye una infracción disciplinaria grave.

En cualquier caso, el despido por represalia o discriminatorio de la persona que denuncia los hechos en materia de *Whistleblowing* es nulo. La modificación de los derechos también es nula de acuerdo con el artículo 2103 c.c. o la normativa correspondiente a los distintos países de las Sociedades del Grupo Esprinet.

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

Durante el procedimiento disciplinario, la identidad del denunciante sólo puede ser revelada al departamento de Recursos Humanos y al acusado en los siguientes casos:

- cuando el denunciante haya dado su consentimiento expreso;
- cuando la respuesta disciplinaria resulta fundada, en todo o en parte, en la denuncia y el conocimiento de la identidad del denunciante es absolutamente esencial para la defensa del acusado. En cualquier caso, la actividad de verificación debe tender a adquirir pruebas independientes que no requieran el uso de esta última necesidad.

10.1. Denuncias No permitidas

Las denuncias 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.

11. CONTROLES PERMITIDOS Y CONTROLES PROHIBIDOS

11.1. Controles indirectos sobre las herramientas de trabajo y la videovigilancia

En relación con el derecho a la intimidad de los trabajadores (D.Lgs. n. 151/2015 o la normativa aplicable a los distintos países de las sociedades del Grupo Esprinet), cualquier control indirecto sobre la actividad de los trabajadores realizado a través de los instrumentos de trabajo (email, tarjeta, pc, teléfono móvil, etc. ...) por razones organizativas, de seguridad en el lugar de trabajo y protección del patrimonio de la empresa, podrá ser realizado para la finalidad de verificar si existen presuntos comportamientos fraudulentos o contrarios al Código Ético (por ejemplo, utilización no autorizada de credenciales de acceso de otra persona).

En cualquier caso, deberán ser respetados los principios *privacy* de proporcionalidad, de relevancia y sin excesos.

Se prohíben cualquier control que tenga carácter vejatorio.

Tales instrumentos, en ningún caso, podrán ser utilizado como forma de control continuo de la actividad de trabajo del empleado, incluso cuando tal control tenga por objeto la detección de posibles infracciones.

Solo posteriormente en caso de denuncia u otros elementos fundados, podrán ser extraídos datos para ser utilizados como prueba de conductas disciplinarias o penalmente atribuibles.

11.2. Otras actividades de control prohibidas

Está totalmente prohibido:

- instalar sistemas de videovigilancia que incluyan también registros de audio;
- instalar sistemas de videovigilancia en lugares recreativos tales como, comedor, aseos, vestuarios, etc.…);
- activar sistemas que permitan desde remoto las escuchas telefónicas o de cualquier otra forma de comunicación;
- activar el sistema de altavoz, en el curso de una conversación telefónica, permitiendo la escucha de terceros presentes, sin la autorización del interlocutor;
- cualquier otra forma de control oculto, remoto o no autorizado.

11.3. Controles directos

Por control directo se entiende cualquier intervención por parte de un superior directo o de los departamentos de control con respecto al trabajador. No solo está permitido, sino que también es un deber.

Tal forma de control representa la expresión la expresión del deber y el poder de gestión de quienes tienen la responsabilidad de alcanzar los objetivos de la empresa y de velar por el cumplimiento de las normas a

tal fin.

El control directo debe estar orientado a difundir comportamientos virtuosos de acuerdo con el Código Ético y los procedimientos de la empresa.

En el caso de sospechas de comportamientos fraudulentos o contrarios al Código Ético, el responsable directo y el departamento de *Internal Audit* están autorizados a:

- el control del puesto de trabajo
- el control directo sobre el contenido del ordenador de la empresa que se proporciona a cada empleado.

Estos controles sólo deben tener lugar en presencia de la persona interesada y, sólo en casos excepcionales, urgentes y graves, se permite el control incluso en su ausencia, pero en presencia de un colega indicado por ella o de un representante sindical.

12. POLITICA DE SEGURIDAD INFORMÁTICA

Todos los empleados están obligados a cumplir lo indicado en la *LIG01001 Política empresarial sobre el uso de las herramientas informáticas y la seguridad de la información*.

Las disposiciones del párrafo 11 de esta política se aplicarán con respecto a la utilización de los resultados de vigilancia requerida para la verificación de cualquier conducta ilícita.

También se hace referencia a lo previsto en la Política mencionada.

13. MÉTODO DE EJECUCIÓN Y DOCUMENTACIÓN DE LAS ENTREVISTAS

Durante las verificaciones realizadas por el departamento de Internal Audit y/o por el ODV con respecto a las denuncias en materia de Whistleblowing, con el fin de determinar una presunta conducta fraudulenta o una violación del Código Ético, pueden llevarse a cabo entrevistas a empleados y colaboradores que puedan indicar algún aspecto útil.

Cualquiera que sea llamado a una audiencia por el RIA o por el Organismo de Vigilancia, está obligado a:

- acudir;
- cooperar de forma justa y con la máxima transparencia, informando de las circunstancias que conozca en relación con los hechos y preguntas que se le planteen;
- a proporcionar cualquier documentación que le sea requerida, para apoyar la información proporcionada;
- a firmar el informe de la entrevista que se redactará.

El Departamento de *Internal Audit* y el Organismo de Vigilancia se encargarán de:

- evitar el acoso o las actitudes inquisitivas hacia el empleado/colaborador entrevistado, incluso cuando el empleado/colaborador sea el presunto autor de la violación;
- no permitir que ninguna otra persona que no sea el demandado asista a la audiencia;
- no entregar una copia del informe de la entrevista;

La entrevista no constituye de ninguna manera una denuncia disciplinaria, incluso si se refiere al presunto autor de la violación que es objeto de la investigación.

14. MÉTODO Y CRITERIOS PARA LA TRAZABILIDAD, EL ARCHIVO, CONTROL Y LA PRESENTACIÓN DE INFORMES SOBRE LAS ACTIVIDADES REALIZADAS

Las actividades de verificación responden a los principios generales de SCIGR y los estándares profesionales de los auditores, incluido el tema de la trazabilidad, archivo y presentación de informes en las actividades de verificación.

Sin embargo, dada la naturaleza particular, también con finalidad de privacidad, de los datos recogidos durante una actividad de verificación, esta documentación deberá ser objeto de medidas de seguridad reforzadas.

Se prohíbe la eliminación o destrucción de correos electrónicos, archivos o documentos que deban conservarse en cumplimiento de una obligación legal, por razones fiscales y por lo dispuesto en las políticas de la empresa. Además, todos los documentos electrónicos (correo electrónico, archivo, etc…) deben ser trazables y archivado como resultado de las operaciones, a excepción de aquellos supuestos indicados en las políticas de la empresa

15. GESTIÓN DE LAS RELACIONES CON LAS AUTORIDADES POLICIALES Y JUDICIALES

En el caso de que sea necesario, por hechos graves, solicitar la intervención de la policía, el Organismo de Vigilancia deberá informar al Responsable de Seguridad, quien se ocupará de ello en función de las responsabilidades territoriales y funcionales. Cualquier queja/consulta es procesada y archivada por el Departamento Legal.

Toda persona convocada por la policía judicial o por la autoridad judicial o por el juez de lo penal, como persona informada sobre los hechos o como testigo de hechos relacionados con la actividad de la empresa o de fraudes o delitos comprobados de los que la empresa haya presentado una denuncia/informe, está obligada a informar al Órgano de Vigilancia, quien podrá autorizar el visionado de los actos o declaraciones internas que se hayan realizado con anterioridad en el transcurso de la entrevista, como ayuda para la memoria y para permitir una colaboración efectiva y transparente con los órganos de la policía y de la autoridad judicial.

Fuera de estos casos, la persona convocada mantendrá absoluto secreto sobre los detalles y las razones de la citación recibida.

16. RÉGIMEN SANCIONADOR

El régimen sancionador aplicado por la empresa y prescrito por el CCNL Convenio colectivo nacional prevé el pago de las siguientes sanciones disciplinarias:

- reprimenda verbal por mala conducta menor;
- reprimenda por escrito en caso de reincidencia, tal como se indica en el punto anterior;
- multa que no exceda la cantidad de 4 horas de pago normal;
- suspensión de pago y servicio por un máximo de 10 días;
- despido disciplinario sin previo aviso y con las demás consecuencias de la razón y la ley

La elección de la sanción que debe aplicarse debe ser proporcionada, de acuerdo con el principio de proporcionalidad, una vez comprobada la gravedad de la infracción cometida, teniendo en cuenta, en particular, lo siguiente:

- las pruebas recogidas en el procedimiento disciplinario;
- la naturaleza voluntaria o culposa de la infracción cometida;
- la reincidencia del comportamiento ilegal;
- el daño, incluso potencial, causado a la empresa, entendido tanto como una estructura física como a los empleados/colaboradores.

En relación con la siguiente política, aunque no es una lista completa, las siguientes infracciones siempre conllevarán responsabilidad disciplinaria:

- incumplimiento de la obligación de proteger la confidencialidad de la identidad del denunciante;
- represalias o discriminación contra el denunciante;
- denuncias falsas o injuriosas;
- destrucción/cancelación de email, ficheros o documentos inherentes a la actividad de trabajo, sin la correspondiente autorización;
- negarse a comparecer en la audiencia tras la convocatoria por parte de Internal Audit o del Organismo de Vigilancia;
- negativa a cooperar con las funciones mencionadas en el punto anterior, al no responder a las preguntas planteadas o a proporcionar información falsa.

Finalmente, cualquier otra violación de las reglas de actuación establecidas en esta política constituye una ofensa disciplinaria.

17. 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.