P.01.
Política del Sistema Interno de Información y Defensa del Informante

IDENTIFICACIÓN: **P.01. POLÍTICA DE CANAL ÉTICO**		
REVISIONES		
Rev. nº	**Fecha**	**Comentarios**
01	31/03/2025	Primera versión procedimiento de Política de Canal Ético.

Aprobado por el Administrador Único de SUITELE S.L.

Fecha: 28/04/2025

Elaborado por ADEPLUS CONSULTORES, S.L.U.
Fecha: 31 de Marzo de 2025

ÍNDICE

PREÁMBULO

0. OBJETO

1. ÁMBITO SUBJETIVO DE APLICACIÓN

2. ÁMBITO OBJETIVO DE APLICACIÓN

3. PRINCIPIOS DE ACTUACIÓN

3.1. Principio de Independencia

3.2. Principio de Autonomía

3.3. Principio *de confidencialidad*

3.4. Protección legal y defensa del informante

3.5. Protección de los afectados y de los terceros en el procedimiento

4. COMUNICACIÓN, DIFUSIÓN Y COMPROMISO

5. CONTROL Y EVALUACIÓN

PREÁMBULO

La aprobación de la Política, y sus eventuales modificaciones corresponde al Administrador Único de SUITELEC S.L.

De igual modo, le corresponde al Administrador Único la designación de la persona física responsable de la gestión del Sistema de Información (en adelante indistintamente "Sistema de Información" o "Canal Ético")..

La Política de SUITELEC S.L. (la "Entidad") en materia de Sistema Interno de Información y Defensa del Informante resulta de la conjunción de tres elementos:

a) El compromiso de la Entidad con la promoción de una verdadera cultura ética empresarial

b) La identificación de las personas de SUITELEC S.L. con valores, principios y pautas éticas y de conducta establecidos en el Código de Conducta.

c) El alineamiento de la actividad de la Entidad con un cumplimiento legal responsable, visible en el diseño y la organización de los procesos, y en los procedimientos de *compliance*.

Como reflejo de lo anterior la presente Política se aprueba al más alto nivel de Gobierno, a propuesta del Administrador Único.

0. OBJETO

El objetivo de la Política es enunciar los principios generales para su implantación en materia de Sistema interno de información y defensa del informante, y su fin último fomentar un entorno de Cumplimiento basado en los principios y valores de SUITELEC S.L.

A partir de la aprobación y entrada en vigor de la Política se refuerza la obligación de informar de posibles riesgos de infracciones administrativas y/o penales graves o muy graves como elemento esencial de la cultura de cumplimiento de la Entidad, protegiendo a las personas que en este contexto laboral o profesional lo comuniquen mediante los mecanismos regulados en el Procedimiento de Gestión de Comunicaciones, que se aprueba conjuntamente con esta Política.

1. ÁMBITO SUBJETIVO DE APLICACIÓN

Esta Política se aplica a cualquier persona que haya obtenido información sobre infracciones en un contexto laboral o profesional, con independencia de cuál sea la modalidad jurídica que determine su relación laboral o de servicios con la Entidad, e incluso de si la citada relación jurídica se encuentra en vigor, extinguida o no iniciada.

Por su parte, tienen la capacidad de ser afectadas, todas aquellas personas que estén sujetas o vinculadas a la autoridad y control de la Entidad, sobre la base de una relación de índole laboral o mercantil. En este sentido, a modo de ejemplo, pueden ser afectados: las personas trabajadoras, incluyendo el personal directivo, entidades colaboradores y los proveedores, y cualquier otra persona vinculada al Modelo de Cumplimiento Normativo de la Entidad.

2. ÁMBITO OBJETIVO DE APLICACIÓN

El ámbito objetivo de aplicación del Canal de Comunicaciones abarca todas aquellas conductas que vulneren la normativa interna de la Entidad, sus políticas, y especialmente aquellas que se tengan al menos alguna de las siguientes características:

a) Que se encuentren tipificadas como constitutivas de delito en el Código Penal.
b) Que supongan una infracción de carácter administrativo.
c) Que puedan atribuir responsabilidad o cualquier clase de perjuicio, o descrédito a la Entidad.
d) Cualquier información, conocimiento, experiencia, o cualquier otra circunstancia que la persona sujeta o vinculada, considere oportuno o conveniente poner en conocimiento de la Entidad por tener relación directa con asuntos éticos de la gestión interna de la Entidad, con relevancia en el cumplimiento normativo y/o en cualquiera de los puntos anteriores.

Como requisito adicional para su tratamiento en el Sistema de Información, estas acciones o conductas tienen que ser atribuibles a cualquier persona, o entidad vinculada a la Entidad..

3. PRINCIPIOS DE ACTUACIÓN

Como principio general, la Entidad cumplirá escrupulosamente en la gestión del Canal ético con la legislación actual (artículo 31 bis y concordantes de la L.O. 1/2015 y 1/2019 de modificación del Código Penal) , la Directiva UE 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión Europea, y 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, así como con la Normativa vigente en materia de Protección de Datos de Carácter Personal.

En relación a lo expuesto el SUITELEC S.L. velará por el cumplimiento de los Principios relacionados a continuación.

3.1. Principio de Independencia

El Responsable del Sistema persona ejercerá su cargo con independencia del órgano de administración de la Entidad, aunque con acceso a éste y a la alta dirección. Tiene una posición jerárquica adecuada que le legitima suficientemente para acceder a los documentos, informaciones y personas que precise para el desarrollo de sus cometidos, sin que ello pueda verse obstaculizado por motivos jerárquicos, y reduciendo a su vez la posibilidad de que la función vea conculcada la neutralidad en su análisis.

En todo momento se asegurará la gestión del conflicto de intereses por parte del órgano de cumplimiento normativo de SUITELEC S.L. para que en ningún caso la persona vinculada con la comunicación participe o pueda tener voz o voto en dicho expediente durante la tramitación del mismo.

La designación, destitución o cese, del Responsable del Sistema se comunicará a la Autoridad de Protección del Informante.

3.2. Principio de Autonomía

El Responsable del sistema tendrá libertad operativa, con capacidad para actuar por iniciativa propia, sin perjuicio del establecimiento de Planes directores anuales.

3.3. Principio de Confidencialidad

En cualquier caso se preservará la identidad del informante y de las personas afectadas, con medidas técnicas y organizativas adecuadas, permitiendo asimismo la posibilidad de presentación y tramitación de comunicaciones anónimas.

Asimismo, todos los datos personales derivados de la formulación de cualquier comunicación están especialmente protegidos por la normativa vigente en cada momento sobre protección de datos de carácter personal. Excepcionalmente, como medida para garantizar dicha confidencialidad se hace constar expresamente que el ejercicio del derecho de acceso por parte del afectado no supone, en ningún caso, el acceso a los datos relativos a la identidad del informante.

Las personas que excepcionalmente, por necesidades imperativas para la investigación y decisión, tengan conocimiento de las comunicaciones que se realicen a través del Sistema de información están obligadas a guardar secreto profesional sobre los datos de la persona informante, en

particular los relativos a su identidad. No obstante lo anterior, la protección de la confidencialidad del informante o de terceros no se aplicará cuando se haya revelado por los mismos de manera intencionada su identidad en el contexto de una revelación pública.

La comunicación a terceros de la identidad del informante sólo podrá realizarse a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora, de lo que se dará traslado al informante antes de revelar su identidad salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial.

3.4. Protección legal y Defensa del informante

La buena fe, esto es, la conciencia honesta de que se han producido o pueden producirse hechos graves perjudiciales constituye un requisito indispensable para la protección del informante. Esa buena fe es la expresión de un comportamiento cívico y se contrapone a otras actuaciones que por el contrario, resulta indispensable excluir de la protección, tales como la remisión de informaciones falsas o tergiversadas, así como aquellas que se han obtenido de manera ilícita.

Al mismo tiempo, dicha protección no se perderá cuando el informante comunique información inexacta por error cometido de buena fe. En cualquiera de los casos, los motivos del informante para llevar a cabo su comunicación son irrelevantes con relación al buen funcionamiento del Canal. Se concede también protección a las personas que no aporten pruebas concluyentes pero que planteen dudas o sospechas razonables sobre los hechos.

La Entidad velará activamente por la aplicación de las medidas de apoyo y de protección al informante, de acuerdo con las circunstancias concurrentes en cada momento, Esta protección se instrumentaliza en las siguientes medidas:

- Garantía de confidencialidad y aplicabilidad de la Normativa de protección de datos de carácter personal.

- Prohibición de represalias y medidas de apoyo y protección al informante.

Por el término «represalia» se expresa la estrecha relación (de causa y efecto) que debe existir entre la comunicación y el trato desfavorable sufrido, directa o indirectamente, por el informante, de modo que dicha persona pueda gozar de protección jurídica, frente a cualquier tipo de represalia, discriminación y penalización por motivo de las comunicaciones realizadas de buena fe.

La prohibición de represalias prevista en el párrafo anterior no impedirá la adopción de las correspondientes medidas disciplinarias que sean procedentes, cuando la investigación interna determine que la comunicación realizada es falsa, y, que la persona que la ha realizado es consciente de su falsedad.

- El asesoramiento al informante

El Responsable del sistema será el encargado de prestar y proporcionar el asesoramiento individualizado y la información precisa al informante, con relación al ejercicio responsable de su facultad de llevar a cabo una comunicación

- Inmunidad del informante

Cuando el informante hubiera obtenido de manera legal acceso a la información comunicada o los documentos que la contienen, tendrá inmunidad con relación a la responsabilidad civil, administrativa o laboral derivada de la comunicación presentada.

Esto se aplica tanto a los casos en los que el informante revele el contenido de documentos a los que tenga acceso legalmente como a aquellos en los que realice copias de los mismos o los retire de los locales de la organización de la cual es empleado en contravención de cláusulas contractuales o de otro tipo que estipulen que dichos documentos son propiedad de la organización.

Cuando el informante haya obtenido la información o documentos mediante la comisión de una infracción penal como la intromisión física o informática, su responsabilidad penal ha de regirse por la legislación que en cada caso sea aplicable. No obstante, lo anterior, el informante será responsable de las acciones y omisiones que no guarden relación con la comunicación o no resulten necesarias para revelar una infracción.

Por otra parte, las obligaciones legales o contractuales de las personas, como las cláusulas de fidelidad o los acuerdos de confidencialidad y no publicidad, no podrán ser invocadas para impedir las comunicaciones, para denegar la protección o para penalizar a los informantes por haberlas presentado cuando la transmisión de información que esté contemplada en dichas cláusulas o acuerdos sea necesaria para revelar la infracción. Cuando se cumplan estas condiciones, no se podrá imputar a los informantes responsabilidad alguna, ya sea civil, penal, administrativa o laboral. Dicha exención no debe hacerse extensiva a la información superflua o desconectada causalmente con los hechos objeto de la comunicación, que el interesado hubiera revelado sin basarse en motivos fundados

3.5. La protección de los afectados y de los terceros en el procedimiento

La protección de la identidad de las personas afectadas y/o de los terceros a que se refiera la comunicación (por ejemplo, testigos, etc.) en todas las fases del procedimiento, en la mejor garantía de protección.

Asimismo, estas personas mantienen todos sus derechos de tutela judicial y defensa, de acceso al expediente, de confidencialidad y reserva de identidad y la presunción de inocencia; en fin, de los mismos derechos que goza el informante.

4. COMUNICACIÓN, DIFUSIÓN Y COMPROMISO

Las personas trabajadoras dispondrán de una copia de esta política a su disposición a través del canal interno de comunicación disponible de SUITELEC S.L.

Asimismo la Entidad proporciona información adecuada de formar clara y fácilmente accesible sobre el uso del Sistema interno de información implantado, así como sobre los principios esenciales del procedimiento de gestión a todos sus *stakeholders* a través de la página web, en una sección separada y fácilmente identificable sin perjuicio de otras acciones de difusión y compromiso con la política entre todas las partes interesadas: proveedores, Administraciones Públicas, etc.

Las personas trabajadoras de SUITELEC S.L. se encuentran vinculadas por el Código de Conducta y esta Política y asumen su cumplimiento, estando obligados a informar de los posibles riesgos e incumplimientos al Órgano de control interno a través del Canal Ético habilitado en www.suitelec.com

5. CONTROL Y EVALUACIÓN

El Responsable del sistema reportará periódicamente al Administrador Único de SUITELEC S.L. sobre la aplicación de la presente Política y de su cumplimiento efectivo, y al menos lo hará una vez al año.

La aprobación de esta Política se documenta en Acta del Administrador Único de SUITELEC S.L. de fecha 28/04/2025 estableciéndose su entrada en vigor a partir del día siguiente de su comunicación a la plantilla.