

## CANAL ÉTICO de "VIGUESA DE CALDERERÍA, S.A."

### SOLICITUDES DE INFORMACIÓN Y PRESENTACIÓN Y GESTIÓN DE DENUNCIAS

El Administrador aprueba y documenta por escrito este procedimiento que regula el CANAL ÉTICO, detallando el funcionamiento del sistema en todos los extremos que se relacionan a continuación.

#### OBJETO

- **Ámbito de aplicación**

El canal ético se aplicará a los empleados, directivos, comerciales, y a todo el personal que mantenga con la empresa un vínculo contractual (del carácter que fuere), tales como colaboradores proveedores, empresas subcontratadas, etc.

Estará además abierto a terceros, que podrán utilizarlo para comunicar posibles incumplimientos observados en el desarrollo de la actividad empresarial.

Este canal tiene un doble objetivo: por un lado la solución de dudas relativas al cumplimiento del modelo de organización y gestión, y por otro la presentación de denuncias en caso de que se detecten posibles incumplimientos.

- **Carácter obligatorio**

El administrador de "VIGUESA DE CALDERERÍA, S.A." establece el carácter obligatorio del canal ético, basado en lo dispuesto en el **artículo 31 bis 5 del Código Penal**, según el cual los Modelos de organización y gestión implantados en las empresas para la prevención de delitos "impondrán la OBLIGACIÓN de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención".

- **Divulgación**

El canal ético será divulgado entre todos los empleados, socios y y cuantas personas estén vinculadas a la empresa. La información sobre su existencia debe figurar en todos los contratos que la empresa suscribe (empleados, proveedores, clientes, colaboradores externos, etc.) así como en la página web de la empresa.

En caso de denuncia tanto los denunciantes como los denunciados deben ser informados previamente de la existencia del canal ético y del tratamiento de los datos que conlleva la formulación de una denuncia, así como de las consecuencias que para el denunciado puede ocasionar dicha denuncia.

## CARACTERÍSTICAS

- **Consentimiento**

Para implantar el canal ético no es necesario contar con el consentimiento de los trabajadores de la empresa. Tampoco es necesario el consentimiento de dichos trabajadores para la comunicación a terceras partes de los datos de la denuncia, con el fin de que investiguen los hechos denunciados.

Así pues, la implantación de un canal de denuncias no requiere el consentimiento de los interesados siempre que exista con ellos un vínculo contractual y se les informe de la existencia de dicho sistema, quedando esa información incorporada a la relación contractual establecida.

- **Solicitudes de información en materia de cumplimiento legal**

El canal ético está a disposición de cualquier interesado que tenga relación con la empresa para resolver cuestiones relativas a posibles incumplimientos del modelo de prevención y control de delitos, utilizando para ello un vínculo incluido en el correo electrónico que se le remite a dicho interesado.

Estas solicitudes podrán ser realizadas directamente al Compliance Officer designado D. Pablo Benavides Barreiro, mediante remisión de correo electrónico a la dirección: [pablo@vicalsa.es](mailto:pablo@vicalsa.es)

- **Interposición de DENUNCIAS**

El canal ético está también a disposición de cualquier interesado que tenga relación con la empresa, para la presentación de denuncias de casos de posibles incumplimientos del modelo de prevención y control, utilizando también para ello un vínculo incluido en el correo electrónico que se le remite a dicho interesado. Dicho vínculo le dará acceso al formulario de denuncia.

Es importante tener en cuenta que los hechos denunciados deben tener una implicación directa en la relación que exista entre el denunciante y el denunciado. Es decir no puede ser objeto de denuncia cualquier tipo de comportamiento, sino aquellos hechos que estén relacionados con su vinculación contractual a la empresa.

- **Comportamientos**

Deberán ser objeto de denuncia todos aquellos comportamientos o decisiones adoptadas por personas vinculadas a la empresa que puedan ser contrarias a las normas aprobadas por ésta como parte del Modelo de gestión y prevención de delitos, tales como: respeto a los valores

éticos, respeto a la dignidad de las personas, manipulación de la información, corrupción y soborno, lealtad a la empresa, neutralidad política, relaciones con clientes, contratistas y proveedores, etc.

- **Sanciones**

Tanto los denunciantes como los denunciados deberán haber sido avisados previamente de las consecuencias que para ambos puede comportar este hecho, es decir las sanciones que conlleva con arreglo al régimen disciplinario de la entidad, sin perjuicio de posibles responsabilidades de otra índole que puedan corresponder según la sentencia de jueces, tribunales y órganos competentes.

- **Doble investigación**

La denuncia realizada puede tener una doble vertiente:

- Por una parte se debe verificar si el comportamiento del denunciado es realmente irregular.
- Y por otro lado se debe comprobar si el denunciante ha comunicado una denuncia falsa, y en este caso se debe aclarar si se trata de un simple error o por el contrario ha actuado de mala fe y con ánimo de perjudicar al denunciado.

- **Confidencialidad**

Es determinante garantizar al denunciante la confidencialidad de la información durante todo el proceso. En este sentido, el término confidencialidad hace referencia a todos los extremos de la denuncia, tales como datos del denunciante, hechos, y personas cuya conducta o actuación pueda ser constitutiva de delito. Dicha confidencialidad podrá ser suspendida cuando el conocimiento de los hechos sea requerido por los jueces, tribunales o autoridad competente.

- **Denuncias anónimas**

La Agencia Española de Protección de Datos "NO permite" a las empresas aceptar denuncias anónimas, garantizando de esta forma la exactitud e integridad de la información que predica la normativa de protección de datos, pues en caso contrario se vulneraría el "deber de calidad" establecido en su artículo 4º.

- **Represalias**

El denunciante debe tener claro que además de la confidencialidad de sus datos identificativos, también se le garantiza que no puede ser objeto de ningún tipo de represalia por el hecho de denunciar. En este sentido se le debe informar al denunciante que en el caso de estar relacionado con los hechos denunciados, la denuncia realizada tendrá un carácter atenuante para él, como consecuencia de la confesión anterior al descubrimiento al delito y por disminución de sus efectos.

## **COMITÉ DE DENUNCIAS**

- **Independencia**

El comité de denuncias debe hacer cumplir el procedimiento de denuncias y garantizar una eficaz gestión del sistema.

Es un órgano totalmente independiente dentro de la empresa, integrado por el compliance officer y dos responsables de departamento.

En el caso de que un miembro del comité esté implicado en una denuncia, este deberá abstenerse de participar en el tratamiento de la denuncia y comunicar inmediatamente al comité de esta circunstancia.

- **Funciones**

Las funciones del comité de denuncias son las siguientes:

- Recepcionar la denuncia.
- Decidir si la denuncia se inadmite, o se da trámite a la misma.
- Designar por cada denuncia el responsable de instrucción.
- Aprobar y motivar las excepciones al procedimiento.
- Velar por el cumplimiento de las obligaciones establecidas por la Ley de Protección de Datos.
- Informar al Administrador de la empresa.
- Nombrar un secretario para que levante acta de las reuniones.

- **Responsable de instrucción**

El responsable de instrucción debe ser un responsable de departamento, y sus principales funciones son:

- Designar al instructor que llevara a cabo la investigación de cada denuncia.
- Marcar actuaciones, prioridades y plazos de ejecución.

- Aprobar el informe emitido por el instructor con el resultado de la investigación.
- Comprobar el cumplimiento de la implantación de las medidas de seguridad establecidas por la Ley de Protección de Datos.

- **Instructor**

El instructor será designado entre los miembros del Comité de denuncias, y sus principales funciones son:

- Documentar y registrar las denuncias recibidas.
- Investigar los hechos y recopilar evidencias.
- Documentar y registrar todas las acciones realizadas.
- Elaborar el informe bajo la supervisión del responsable de instrucción.
- Cumplir con las exigencias de la normativa de la protección de datos.

#### CONSERVACIÓN DE LOS DATOS

- **Plazos**

- Desde el inicio de la investigación hasta su finalización el plazo no podrá superar los 6 meses.
- Desde la finalización de la investigación:
  - - Si los hechos no se prueban, el plazo no podrá superar los 1 mes.
  - - Si los hechos se prueban, el plazo no podrá superar los 2 meses a partir de finalizar el procedimiento.

- **Bloqueo**

A partir de los plazos mencionados, la cancelación de la información implica el bloqueo de la misma, por si pudieran derivarse responsabilidades posteriores, algo que resulta factible en este ámbito. Se recomienda que dicho bloqueo se realice durante un plazo prudencial de un año.

El término "Bloquear" significa conservar la documentación de forma separada, sin realizar ningún tipo de tratamiento y de manera totalmente confidencial. Dicha información solo podrá utilizarse a expensas de una reclamación judicial u otra administración pública con autoridad en la materia.

#### INFORMACION A INTERESADOS

- **Deber de información al denunciante**

El canal de denuncias debe de prever facilitarle al denunciante la siguiente información:

- - Razón social y dirección del responsable del fichero que realiza el tratamiento.
- - Finalidad del tratamiento de los datos.
- - Estricta confidencialidad de los datos, excepto posibles comunicaciones a terceros implicados (testigos) en la investigación o jueces y tribunales.
- - Consecuencias de realizar una denuncia falsa o con mala fe.
- - No tomar represalias por parte de la empresa.
- - Informar sobre la manera de ejercer los derechos ARCO.
- - Comunicar que no se tramitarán denuncias anónimas (Art. 4º de la LOPD).

- **Deber de información al denunciado y terceros implicados**

La empresa deberá informar dentro de los 3 meses siguientes, contados desde el día en que se recibe la denuncia, tanto a la persona denunciada como a las terceras partes implicadas (afectados, testigos, etc.).

Este deber de información no implica revelar la identidad del denunciante o datos que permitan deducir su identidad, si no la siguiente información:

- - Que ha sido denunciado a través del canal de denuncias.
- - Los hechos denunciados.
- - Razón social y dirección del responsable del fichero que realiza el tratamiento.
- - Finalidad del tratamiento de los datos.
- - Estricta confidencialidad de los datos, excepto posibles comunicaciones a terceros implicados en la investigación o jueces y tribunales.
- - Informar sobre la manera de ejercer los derechos ARCO.

Se debe celebrar una reunión individual con cada interesado (denunciado, afectados y testigos) dentro del plazo máximo de 3 meses con el fin de redactar un acta en la que figuren las preguntas sobre los hechos denunciados y se incluya la cláusula de información, de forma que se pueda aprobar su cumplimiento ante cualquier requerimiento que pudiera hacer la Agencia Española de protección de datos.

## DERECHOS ARCO

- **Acceso**

El derecho de acceso del denunciado solo le permite obtener información de sus datos personales, y nunca sobre los datos identificativos del denunciante u otros terceros, pues de lo contrario estaríamos ante un supuesto de cesión de datos sin consentimiento.

- **Rectificación**
- El derecho de rectificación podrá ser ejercitado durante la tramitación de la denuncia por denunciante, denunciado y terceros.
- **Cancelación**

El derecho de cancelación no podrá ser ejecutado durante la tramitación de la denuncia.

- **Oposición**

El denunciado no puede interponer el derecho de oposición, es decir no puede oponerse a que sus datos sean tratados en el sistema de denuncias.

- **Obligación a contestar**

Con independencia de cualquier derecho solicitado por el denunciado, la empresa está obligada a contestar al interesado siempre que la petición se haya realizado en tiempo y forma.

#### MEDIDAS DE SEGURIDAD

- **Sobre seguridades de acceso**
  - El permiso de acceso a las denuncias debe concederse a un grupo reducido de personas que lo necesiten.
  - Debe existir una relación actualizada de usuarios con acceso.
  - Las claves de usuario y contraseña deben cambiarse como mínimo una vez al año.
  - De cada intento de acceso el sistema guardara durante 2 años como mínimo la siguiente información:
    - - La identificación del usuario que accede.
    - - La fecha y hora en la que realizo el acceso.
    - - El fichero al que accede y si ha sido autorizado.
    - El compromiso de confidencialidad debe estar firmado por las personas encargadas de la gestión del canal de denuncias y permiso de acceso.

- **Sobre información**

- El comité de denuncias debe estar informado de cualquier anomalía o no conformidad que aparezca.
- Se debe llevar un registro de entrada y salida de la información enviada a jueces, tribunales, etc.
- Se debe realizar la auditoria que exige la Ley de Protección de Datos sobre el fichero de denuncias internas al menos cada 2 años, informado del resultado a la dirección de la empresa.
- Toda la información relativa a denuncias internas debe estar en el sistema de información, incluyendo también los correos electrónicos.
- Las copias de seguridad deben realizarse al menos una vez a la semana
- La información no puede encontrarse en dispositivos portátiles, USB, y/o pendrive.
- El responsable de seguridad o persona en la que delegue, se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe relativo a dichas revisiones y los problemas detectados.

#### SANCIONES POR INCUMPLIMIENTO

- **Ley de Protección de Datos**

La implantación de un canal de denuncias sin cumplir los requisitos establecidos por la Ley de Protección de Datos puede dar lugar a las siguientes sanciones:

- - Admitir y gestionar denuncias anónimas: Supone una infracción Grave que va de 40.001€ a 300.000€
- - No eliminar (bloquear) los datos de la denuncia en su plazo: Supone una infracción Grave que va de 40.001€ a 300.000€
- - No informar al denunciante: Supone una infracción Leve que va de 600€ a 40.000€
- - No informar al denunciado o terceros afectados: Supone una infracción Grave que va de 40.001€ a 300.000€
- - No cumplir las medidas de seguridad exigidas: Supone una infracción Grave que va de 40.001€ a 300.000€ o bien, Muy Grave que va de 300.001€ a 600.000€
- - No obtener autorización para TID: Supone una infracción Muy Grave que va de 300.001€ a 600.000€

- **Régimen disciplinario interno**

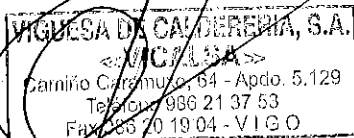


Con independencia de las sanciones anteriores, la empresa puede aplicar las sanciones establecidas en el régimen disciplinario interno como consecuencia de faltas cometidas por empleados o colaboradores. Las cuantías establecidas en dichas sanciones, se aplicarán en función de diversos criterios, tales como el carácter continuado de la infracción, reincidencia y grado de intencionalidad.

- **Procedimiento**

Puede presentar una denuncia ante el Compliance Officer siguiendo el siguiente enlace: [Página de denuncias](#)

Vigo, a 3 de Marzo de 2017.



Fdo.: D. Julio Gómez Rodríguez

Administrador Único de "VIGUESA DE CALDERERÍA, S.A."