PROCEDIMIENTO DE

GESTIÓN DE COMUNICACIONES

THE SUSTAINABLE TUNA COMPANY

FRIME

ÍNDICE

1. Introducción

Grupo FRIME tiene implementado una plataforma de canal de denuncias a la que se accede a través de su página web: https://frime.canaldenunciasanonimas.com, como cauce preferente a disposición de todos los directivos, empleados, colaboradores, proveedores y clientes, así como de cualquier otro tercero, para comunicar cualquier inquietud acerca de un posible incumplimiento o violación a lo dispuesto en el Código de Conducta o en cualquier otra Política interna de la organización, o reportar una irregularidad que ellos detecten en el desempeño de sus funciones, así como cualquier infracción u omisión de la que tenga conocimiento y que pueda suponer una infracción del derecho de la Unión Europea o sus intereses financieros o, incluso, infracciones penales o administrativas en el marco jurídico español, tal como se explica en la Política del Sistema Interno de Información de FRIME.

A través de este documento se desarrolla el Procedimiento de Gestión de Comunicaciones, el cual establece las previsiones necesarias para que el Sistema Interno de Información y el canal interno de comunicación cumplan con los requisitos establecidos en 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.

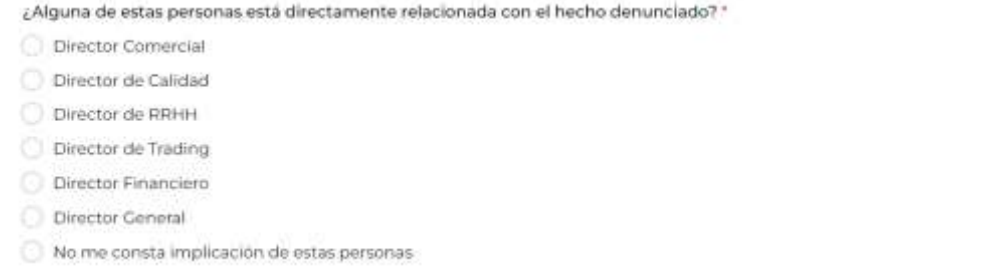
Si bien el canal de comunicaciones interno es el cauce preferente, alternativamente toda persona física puede informar ante la Autoridad Independiente de Protección del Informante (en adelante, "A. A. I.") o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualquier acción u omisión, ya sea directamente o previa comunicación a través del referido canal interno y de acuerdo con los términos establecidos en la precitada Ley 2/2023.

2. Etapas del Procedimiento de Gestión de las comunicaciones

2.1. Recepción de comunicaciones

En FRIME, la recepción de toda comunicación que se haga a través del Sistema Interno de Información es gestionada por la Compliance Officer, quien tiene acceso en principio exclusivo al canal interno de la organización.

Sin embargo, en los casos en los que ella se encuentra directamente relacionada con la situación a comunicar, la denuncia será derivada al Director Financiero quien llevará adelante la investigación. Para conocer tal circunstancia, la plataforma del canal de denuncias lo pregunta directamente al denunciante:



Dicha comunicación puede realizarse a través de la plataforma por escrito o verbalmente, pudiendo ser de forma anónima o nominal, siendo en cualquier caso confidencial e incluyendo la descripción de los hechos, la identificación de las personas involucradas y, en caso de ser posible, aportando pruebas que acrediten el incumplimiento referido, explicando las circunstancias en las que ha tenido acceso a dicha información.

Si se recibe una comunicación de forma verbal a través de la plataforma, ésta quedará registrada en grabación de audio, que puede ser con distorsión de voz a petición del informante, a efectos de garantizar el anonimato.

Asimismo, si excepcionalmente la comunicación se recibe a través de canales internos distintos a los establecidos por Grupo o es dirigida a miembros del personal no responsable de su tratamiento, la organización igualmente garantiza la conservación de la confidencialidad, advirtiendo que su incumplimiento implicaría una infracción muy grave de la Ley y que, inmediatamente, la comunicación es remitida al Responsable del Sistema.

Una vez recibida una comunicación o información, automáticamente se notifica al Compliance Officer quien, como Responsable del Sistema, es el órgano encargado de iniciar el proceso de investigación correspondiente, en su caso, para la aclaración de los hechos objeto de comunicación.

La propia plataforma pregunta al denunciante si la Compliance Officer se encuentra relacionada directamente con la comunicación porque, en caso afirmativo, esta será remitida automáticamente al Director Financiero, quien llevará adelante la investigación sin que la Compliance Officer tome conocimiento.

El Compliance Officer como Responsable del Sistema Interno de Información garantiza en todo momento el respeto a la independencia, la confidencialidad, la

protección de datos y el secreto de las comunicaciones.

En el plazo de siete (7) días naturales siguientes a la recepción de la comunicación se envía un acuse de recibo al informante. Este acuse de recibo se incorpora al expediente incluyendo, en todo caso, información clara y accesible sobre los canales externos de información ante las autoridades competentes.

En los casos en los que realizar un acuse de recibo pudiese poner en peligro la confidencialidad de la comunicación, para garantizarla, no se realizará hasta que haya trascurrido un plazo que se considere prudencial.

Tal como se mencionó en párrafos anteriores, alternativamente a este canal interno preferente, se puede informar ante la Autoridad Independiente de Protección del Informante, A.A.I., o ante las autoridades u órganos autonómicos correspondientes (en el caso de Cataluña, será la Oficina Antifraude de Cataluña), de la comisión de cualquier acción u omisión que pueda ser constitutiva de alguna de las infracciones susceptibles de ser comunicadas por medio del Sistema Interno de Información[1], ya sea directamente o previa comunicación a través del referido canal interno, siguiendo lo dispuesto en el Anexo 1, sobre los canales externos de información.

2.2. Trámite de admisión

Tras recibir la comunicación, se le asigna un NÚMERO DE REGISTRO que corresponde con su EXPEDIENTE y una serie de CÓDIGOS para anonimizar tanto al informante como al investigado, los hechos, y a cualquier otro tercero que se pueda ver afectado por la comunicación.

Si el Compliance Officer advierte que los hechos informados pudieran ser indiciariamente constitutivos de delito, remite la información de forma inmediata al órgano de administración, quien deberá decidir su remisión inmediata al Ministerio Fiscal.

[1] Al respecto ver lo indicado en el Apartado 3, "Del contenido de las comunicaciones", de la Política del Sistema Interno de Información.

Se comprueba que el Compliance Officer no se encuentre implicado en dicha comunicación. Si ese fuera el caso, la comunicación se remitirá automáticamente al Director Financiero, quien llevará adelante la investigación y abrirá el expediente.

Finalmente, tras la recepción de la comunicación, el Compliance Officer deja constancia de la siguiente información, la cual queda registrada en la propia plataforma:

- Los datos objetivos de la comunicación: hechos, fechas, nombres, cantidades, lugares, contactos, etc., que aporte quien efectúe la comunicación.
- Los datos subjetivos: opiniones, rumores, ideas, y apreciaciones que el informante considere necesarios en la narración de la comunicación.
- Valoración del Compliance Officer acerca de si la comunicación está asociada a una posible o supuesta infracción o si es una mera reclamación o sugerencia relativa a mejorar un área del negocio, la situación laboral, etc.

2.3. Trámite de investigación

En el supuesto de que se admitiera a trámite la comunicación, la investigación es dirigida por la persona física seleccionada por el Compliance Officer y desarrollada por éste.

En primer lugar y previo acuerdo con la persona informante, se toman las medidas cautelares preventivas que se estimen pertinentes.

En caso de que sea posible, se podrá solicitar a la persona informante que aporte información adicional necesaria para el transcurso de la investigación a la que haya dado lugar su comunicación.

En esta etapa se notifica y se ENTREVISTARÁ al INVESTIGADO, comunicándosele su derecho a ser informado sobre las acciones u omisiones que se le atribuyen, pudiendo igualmente ejercer su derecho a ser oído, sin que en ningún caso se le comunique la identidad del informante.

También se cita y entrevista a los terceros implicados (si los hubiere) a efectos de que expliquen e indiquen las alegaciones que consideren. Se realizarán cuantas diligencias de investigación sean necesarias para las partes y se dejará constancia documental de todo lo actuado en el expediente.

Las diligencias que se practiquen hacia terceros u otros órganos, áreas o departamentos de Grupo FRIME deberán realizarse manteniendo el anonimato del INFORMADOR y del INVESTIGADO, así como los motivos de la comunicación.

En todo momento se garantiza la confidencialidad de la información, así como la presunción de inocencia y el respeto al honor de todas las personas que se vean afectadas.

Durante esta etapa el Compliance Officer:

1º.- Investiga los hechos comunicados y, concretamente:

- Los elementos objetivos y subjetivos aportados por el informante, priorizando los elementos objetivos respaldados con documentación que acredite, todo o en parte, los hechos informados.
- La reputación, seriedad y fiabilidad del informante.
- Las alegaciones y pruebas de descargo aportadas por el investigado.
- La prueba practicada con terceros, o con otros órganos, áreas o departamentos relacionados.

2º.- Analiza y valora las eventuales consecuencias que los hechos comunicados puedan producir:

En primer lugar, el Compliance Officer comprueba si estos hechos se produjeron por una importante falta de controles internos en FRIME. En su caso, propondrá medidas paliativas y preventivas urgentes para evitar nuevos riesgos.

En segundo lugar, si la gravedad, especialidad o complejidad de los hechos lo aconseja, el Compliance Officer podrá nombrar a otro profesional directivo o a una tercera persona especializada para colaborar en la investigación. Asimismo, si como consecuencia de los hechos comunicados se pudieran producir pérdidas de activos, el Compliance Officer adopta las medidas tendentes a detener o mitigar dichas pérdidas. Si se puede producir una fuga o destrucción de pruebas relevantes para la comunicación, de forma previa al inicio de la investigación, el Compliance Officer se encarga de asegurarse evidencias. El Compliance Officer también valora la pertinencia de informar a los órganos de gobierno sobre esta comunicación. Por último, comprueba si existe la posibilidad de que se hayan causado perjuicios a terceros en cuyo caso, valora la entidad del perjuicio y la necesidad de informar al tercero perjudicado.

El plazo para desarrollar la investigación y dar una respuesta al informante sobre las actuaciones que se hayan llevado a cabo, así como el resultado de las mismas, depende de la gravedad de los hechos comunicados y sus potenciales consecuencias, quedando a criterio y riesgo del Compliance Officer la duración de esta etapa. No obstante, de acuerdo con lo establecido por el artículo 9.2. d) de 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, este plazo no puede ser superior a tres (3) meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, tres (3) meses a partir del vencimiento del plazo de siete (7) días después de efectuarse la comunicación. Esto, salvo en los casos de especial complejidad, cuyo plazo podrá extenderse hasta un máximo de otros tres (3) meses adicionales[2].

Si la comunicación contiene datos personales de terceros distintos al investigado (por ejemplo, testigos, proveedores, clientes, etc.), el Compliance Officer dejará constancia por escrito de que se deberá suprimir toda aquella información personal

[2] Estos plazos se cumplirán, en todo caso, sin perjuicio de lo dispuesto en la normativa laboral o convenio colectivo aplicable a cada supuesto, cuyos plazos prevalecerán en caso de contradicción.

facilitada que no sea necesaria para la investigación, y proceder a informar a los terceros cuyos datos vayan a ser tratados. La información cumplirá con los requisitos informativos de la normativa de protección de datos, omitiendo de esta información la identidad del informante, que deberá mantenerse confidencial.

Todas estas notificaciones se deciden por el Compliance Officer en su función de Responsable del Sistema, constan por escrito en el expediente y son ejecutadas a través del Canal de Denuncias al que se puede acceder a través de la página web de FRIME en la siguiente dirección: https://frime.canaldenunciasanonimas.com.

2.4. Terminación de las actuaciones

Tras la investigación de la comunicación y con la documentación acreditativa que sirviera para esclarecer los hechos, se elabora un VEREDICTO o RESOLUCIÓN que es aprobado mediante Acta extraordinaria del Compliance Officer con el siguiente contenido:

- Descripción de los hechos: nº de registro de la comunicación; fecha de la comunicación; hechos informados; partes intervinientes; documentación aportada a lo largo de la investigación por ambas partes (informante e investigado), por otros órganos, áreas o departamentos o por terceros; entrevista con el investigado y/o con terceros, etc.
- Análisis y valoración de las pruebas obtenidas.
- En caso de que efectivamente se compruebe la irregularidad comunicada, el Compliance Officer dedicará un apartado del veredicto para efectuar las recomendaciones que considere necesario implementar para mejorar los controles y protocolos internos que hayan sido deficientes en esta ocasión.
- Resolución: previa aprobación de los órganos de gobierno, dicha resolución está fundamentada y contiene los motivos por los cuales ARCHIVA SIN SANCIÓN o ARCHIVA CON SANCIÓN.

I. ARCHIVO SIN SANCIÓN: Tras la investigación, si se concluye que la infracción denunciada es manifiestamente menor y no requiere más seguimiento, se procede a su ARCHIVO. También corresponde el archivo en los supuestos de denuncias reiteradas que no contengan información nueva y significativa sobre infracciones ya denunciadas con anterioridad y cuyo procedimiento de investigación ya haya concluido, a menos que se den nuevas circunstancias de hecho o de derecho que justifiquen un seguimiento distinto. En estos casos, debe comunicarse al denunciante la resolución y ésta debe estar motivada.

II. ARCHIVO CON SANCIÓN: el Compliance Officer puede proponer la aplicación de una sanción, pero la decisión recae en el órgano de gobierno en coordinación con el área de recursos humanos, de conformidad con los procedimientos indicados para la aplicación de sanciones laborales en la organización.

III. COMUNICACIÓN A LAS AUTORIDADES: Si la comunicación recibida a priori pareciera tener relación con la comisión de un delito, el Compliance Officer la pondrá en inmediato conocimiento del órgano de administración a efectos de la valoración de su denuncia ante el Ministerio Fiscal.

En este sentido, la Ley de Enjuiciamiento Criminal española contempla en su art. 259 que quien presenciare la perpetración de cualquier delito público[3] está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal,

[3] La clasificación de un delito como público tiene relación con quién impulse su persecución (de oficio o por la parte perjudicada), siendo los delitos **públicos** perseguibles de oficio sin necesidad de la previa denuncia por el perjudicado. Además de los delitos contra la vida y la libertad, en el catálogo de delitos que generan responsabilidad penal de la persona jurídica encontramos, a título ejemplificativo los siguientes delitos públicos: la estafa, cohecho, tráfico de influencias, blanqueo de capitales, financiación del terrorismo, delitos contra la Hacienda Pública y la Seguridad Social, delitos contra el medioambiente y los recursos naturales, delitos contra la ordenación del territorio, contra los derechos fundamentales y libertades públicas, contrabando, entre otros). Por el contrario, son delitos **privados** las calumnias e injurias entre particulares (la justicia sólo podrá actuar cuando la persona perjudicada presente una denuncia o querella) y los delitos **semipúblicos** son perseguibles de oficio una vez que inicialmente el perjudicado haya hecho la denuncia (delitos de descubrimiento y revelación de secretos, delitos contra la propiedad intelectual, agresiones, acosos y abusos sexuales, entre otros).

> o funcionario fiscal más próximo al sitio en que se hallare, bajo una multa de 25 a 250 pesetas[4].
>
> Sin embargo, el deber de denunciar a las autoridades competentes se incrementa respecto a determinados delitos que distingue la norma penal. A este respecto, el Código Penal español, en su art. 450[5], contempla la "omisión de los deberes de impedir delitos o de promover su persecución", sancionando a quien no impidiere la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual, pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, y a quien, pudiendo hacerlo, no acuda a la autoridad o a sus agentes para que impidan unos de estos delitos y de cuya próxima o actual comisión tenga noticia.

Por lo tanto, si una vez finalizada la investigación de los hechos, se confirmara la veracidad de los mismos, Grupo FRIME tomará todas las medidas necesarias para poner fin al hecho denunciado y, si procede y teniendo en cuenta las características del hecho, aplicará las acciones que considere oportunas recogidas en el régimen disciplinario, la legislación laboral vigente y, en su caso, de acuerdo a la legislación penal precitada.

Las medidas que puedan imponerse internamente no limitarán, en ningún momento, el ejercicio de las acciones legales que pueda llevar a cabo FRIME.

[4] Según redacción literal actual del art. 259 de la Ley de Enjuiciamiento Criminal española.

[5] Art. 450 del Código Penal español: "1. El que, pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, no impidiere la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual, será castigado con la **pena de prisión de seis meses a dos años si el delito fuera contra la vida, y la de multa de seis a veinticuatro meses en los demás casos**, salvo que al delito no impedido le correspondiera igual o menor pena, en cuyo caso se impondrá la pena inferior en grado a la de aquél. 2. En las mismas penas incurrirá quien, pudiendo hacerlo, no acuda a la autoridad o a sus agentes para que impidan un delito de los previstos en el apartado anterior y de cuya próxima o actual comisión tenga noticia.

En todos los casos, se NOTIFICA la RESOLUCIÓN tanto al informante como al investigado, teniendo en cuenta el plazo máximo de tres (3) meses desde la recepción de la comunicación, no se notificará al informante cuando este haya renunciado a ello, no se disponga de datos de contacto o se trate de un informante anónimo.

Tras esto, el Compliance Officer ordena el ARCHIVO de la misma, respetando en todo caso, la legislación vigente en materia de protección de datos.

En caso de ARCHIVO CON SANCIÓN, la notificación al investigado contendrá la adopción de las medidas contractuales, disciplinarias o judiciales que se vayan a adoptar.

FRIME garantiza, tal como expone en su Política del Sistema Interno de Información, que nunca se tomarán represalias contra cualquier persona que de buena fe ponga en su conocimiento la comisión de un hecho ilícito, colabore en su investigación o ayude a resolverla. Esta garantía no alcanza a quienes actúen de mala fe con ánimo de difundir información falsa o de perjudicar a las personas. Contra estas conductas ilícitas, FRIME adoptará las medidas legales o disciplinarias que proceda.

3. Registro de las comunicaciones

El Responsable del Sistema cuenta con un registro de las informaciones recibidas y las investigaciones internas a que hayan dado lugar que proporciona la propia plataforma, de forma que le sirve para almacenar y/o recuperar información clave sobre cada incidencia, incluyendo la fecha y fuente de la comunicación original, el plan de la investigación, resultados de entrevistas o cualquier otro procedimiento de investigación, tareas pendientes, resolución final, así como la cadena de custodia de cualquier evidencia o información clave.

4. Protección de Datos Personales

Tal como se expone en la Política del Sistema Interno de Información de FRIME, los tratamientos de datos personales que deriven de la aplicación de dicha Política y del presente Procedimiento de Gestión de Comunicaciones, se rigen por lo dispuesto en el Título VI de Ley 2/2023, por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Considerando el principio de minimización de los datos del Reglamento General de Protección de Datos recogido en la Ley 2/2023, Grupo FRIME únicamente trata los datos personales necesarios para el conocimiento e investigación de las acciones u omisiones objeto de investigación a través del Sistema Interno. En consecuencia, en la medida en que los datos personales recabados no se consideren de necesario conocimiento o que se acreditase que no se trata de información veraz FRIME procederá a su supresión en los términos establecidos en el artículo 32 de la Ley 3/2018[6].

Asimismo, FRIME únicamente puede tratar datos de categoría especial[7] cuando los mismos resulten necesarios para la adopción de las correspondientes medidas correctoras o los procedimientos sancionadores que eventualmente deban cursarse, debiendo, en caso contrario, proceder a su inmediata supresión en los

[6] Cuando proceda la supresión, FRIME bloqueará los datos adoptando cuantas medidas resulten necesarias para impedir el tratamiento de la información bloqueado (salvo su puesta a disposición a las autoridades judiciales, Ministerio fiscal o administraciones públicas competentes para la exigencia de posibles responsabilidades) durante el tiempo necesario para guardar evidencia del funcionamiento del sistema que, considerando los plazos de prescripción indicados en la Ley 2/2023, se fija en 3 años. Es preciso destacar que la obligación de bloqueo y conservación no procede al respecto de datos personales contenidos en comunicaciones no investigadas, únicamente pudiendo ser conservadas de forma anonimizada.

[7] Datos personales que revelen el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, biométricos, datos relativos a la salud, a la vida sexual o las orientaciones sexuales de una persona.

términos mencionados anteriormente.

En último lugar, FRIME debe garantizar que los sujetos afectados por el tratamiento de datos personales llevados a cabo como consecuencia de la investigación puedan ejercer los derechos de acceso, rectificación de datos inexactos, supresión, limitación, portabilidad, oposición y a no ser objeto de una decisión basada únicamente en el tratamiento automatizado. Teniendo en cuenta para el ejercicio de derechos que, el derecho de acceso no podrá incluir información sobre el informante y que el derecho de oposición de las personas investigadas podrá denegarse por motivos legítimos.

5. Aprobación

El Procedimiento de Gestión de Comunicaciones ha sido aprobado por el Consejo de Administración y puede ser modificado con la finalidad de mejorar la confidencialidad y la efectividad en la gestión de las comunicaciones cursadas.

Asimismo, este Procedimiento se revisa y/o modifica por parte del COMPLIANCE OFFICER, quien puede externalizar el servicio a profesionales especialistas:

- Siempre que se produzcan cambios relevantes en la organización, en la estructura de control o en la actividad desarrollada por la entidad que así lo aconsejen.
- Siempre que haya modificaciones legales que así lo aconsejen.
- Siempre que se pongan de manifiesto infracciones relevantes de sus disposiciones que, igualmente, lo aconsejen.

Igualmente se revisa, aun cuando no se produzca ninguna de las circunstancias anteriormente descritas, al menos una vez al año.

6. Historial de versiones

Versión	Fecha	Aprobado por	Motivo del cambio
V. Original	2021	Compliance Officer y Consejo de Administración	
V.1.0	07/06/2023	Consejo de Administración	Adaptación a la Ley 2/2023

7. Anexo 1. Canales externos de información

7.1. Canal externo de información de la Autoridad Independiente de Protección del Denunciante, A.A.I.

Todas las personas físicas pueden informar ante la Autoridad Independiente de Protección del Informante (A.A.I.), o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualesquiera acciones u omisiones a las que se refiere el Sistema Interno de Información de FRIME, ya sea directamente o bien previa comunicación a través del canal de denuncias de la organización

Concretamente, en la Comunidad Autónoma de Cataluña el órgano competente en esta materia es la Oficina Antifrau de Catalunya[8], que ha habilitado un buzón de denuncias anónimas, garantizando en todo momento tanto la confidencialidad de las comunicaciones como en anonimato del denunciante, disponible a través del siguiente enlace:

https://www.antifrau.cat/es/comunicaciones-anonimas

[8] https://www.antifrau.cat/es/es

Oficina Antifrau de Catalunya

Qui som · Què fem · Recursos · Premsa · Transparència · Tràmits · Corrupció · Denuncia · Preguntes · Seu electrònica

Denuncia / Buzón de denuncias anónimas

Buzón de denuncias anónimas

El **buzón de denuncias anónimas** garantiza en todo momento la confidencialidad de las comunicaciones y el anonimato del denunciante.

Usted tiene dos opciones para realizar la denuncia de forma anónima mediante este canal:

—Utilizando su navegador. En este caso, queda rastro de la dirección IP desde la cual se realiza la comunicación.

—Utilizando **una red de anonimización, que garantiza plenamente el anonimato** de la comunicación en el entorno digital (también de la dirección IP, que puede identificar a quien navega por Internet). **La herramienta más utilizada para ello es la red TOR**. Como cualquier otro navegador, para hacer uso de la herramienta TOR es necesario descargar el navegador desde la **página de descarga**. Este **enlace** muestra un **video tutorial** sobre cómo descargar TOR.

7.2. Infofraude

El Servicio Nacional de Coordinación Antifraude[9] (SNCS), como órgano nacional encargado de coordinar las acciones destinadas a proteger los intereses financieros de la Unión Europea, y en dependencia de la Intervención General de la Administración del Estado, posibilita que la ciudadanía ponga en su conocimiento aquellos hechos de los que tengan conocimiento y que puedan ser constitutivos de fraude o cualquier otra irregularidad en relación con proyectos u operaciones financiados con fondos procedentes de la Unión Europea.

De este modo, desde su página web se puede acceder al formulario para la comunicación de fraudes e irregularidades (también conocido como infofraude) y que puede ser utilizado con garantía de confidencialidad:

[9] https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/paginas/inicio.aspx

https://www.igae.pap.hacienda.gob.es/sitios/igae/es-ES/snca/Paginas/ComunicacionSNCA.aspx