SISTEMA INTERNO DE INFORMACIÓN DE CORPORACIÓN DE RESERVAS ESTRATÉGICAS DE PRODUCTOS PETROLÍFEROS

PROCEDIMIENTO DE GESTIÓN DE INFORMACIONES

De acuerdo con lo establecido 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, CORES cuenta con un sistema interno de información (el "S.I.I").

Para la gestión de dicho sistema, la Junta Directiva de CORES designará al Responsable del Sistema Interno de Información ("RSI"), que ejercerá sus responsabilidades de forma completamente independiente y autónoma.

Para el trámite de cualquier comunicación recibida a través del canal interno, el RSI procederá de acuerdo con el siguiente procedimiento.

1. ACCESO AL CANAL INTERNO

CORES ha implantado un Canal Interno de Información, seguro y que garantiza la confidencialidad, para la recepción y gestión de las comunicaciones que los informantes deseen presentar, que permite proteger la identidad y derechos del informante y afectado, accesible mediante un enlace en la página web de la Corporación, en el apartado Canal Interno de Información, en el que también se informará de la existencia del canal externo que establece la Ley y la posibilidad de presentar la información a través de esa vía.

El Canal Interno de Información de CORES unifica todos los canales de información hasta ahora existentes en la Corporación, en las materias propias del Código de Conducta de CORES, el Modelo de Prevención de Riesgos Penales de CORES y el Protocolo Anti-Acoso de la Corporación.

Si se recibiese una información por un canal distinto al Canal Interno de Información, o por persona distinta del Responsable, se deberá guardar estricta confidencialidad y remitirla inmediatamente a dicho Responsable.

El Canal Interno de Información de CORES será inicialmente gestionado a través de la

plataforma informática contratada con la empresa Whistleblower Software ApS (en lo sucesivo, la “Plataforma de Gestión del S.I.I.”), adaptada a los requerimientos de la Ley 2/2023.

Los datos del proveedor de servicios para la Plataforma de Gestión del S.I.I. son: Whistleblower Software ApS, Nº de registro 42045136, Domiciliada en Kannikegade 4, 1., DK-8000 Aarhus C, Denmark. Esta empresa está certificada bajo la norma ISO/IEC 27001 la norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información.

Se adjunta, como **Anexo 1** a este Procedimiento, la Guía de la Plataforma de Gestión del S.I.I., en la que se explica detalladamente y paso a paso el funcionamiento de la misma y cómo presentar una información.

Se habilita a la Presidenta de CORES para modificar la plataforma sobre la que se establece el Canal Interno de Información de la Corporación a cualquier otra, interna o externa, que considere conveniente, o a cualquier medio de gestión del Canal Interno de Información que considere oportuno, siempre y cuando permita cumplir con los requerimientos que establece la Ley 2/2023.

Las características del Canal Interno y los principios que rigen su funcionamiento son:

- Garantía de confidencialidad de la identidad del informante en las comunicaciones a través del canal interno y durante todo el proceso de gestión de la información.
- Previsión de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitarle información adicional.
- Posibilidad de presentar comunicaciones anónimas.
- Establecimiento del derecho de la persona afectada a que se le informe de las acciones u omisiones que se le atribuyen y a ser oída en cualquier momento.
- Exigencia del respeto a la presunción de inocencia y al honor de las personas afectadas.
- Respeto de las disposiciones sobre protección de datos personales de acuerdo con lo previsto en la Ley.
- Remisión de la información al Ministerio fiscal con carácter inmediato cuando los

hechos pudieran ser indiciariamente constitutivos de delito.

2. ACUSE DE RECIBO

Toda información recibida se registrará con un identificador único por caso. Este registro permitirá llevar un seguimiento adecuado de las informaciones recibidas y facilitará el análisis y evaluación posterior.

La Plataforma de Gestión del S.I.I. acusará recibo de la comunicación automáticamente en el momento de su remisión, en el que también se proporcionará al informante una contraseña o código de acceso, mediante la cual podrá tener conocimiento puntual y detallado del estado de las gestiones en relación con la información proporcionada.

Es responsabilidad del informante conservar y custodiar la contraseña o código de acceso puesto que le será requerido por la Plataforma de Gestión del S.I.I. para acceder a información sobre el proceso.

Además, si el informante hubiese proporcionado su correo electrónico, recibirá en el mismo actualizaciones sobre el estado del caso.

3. ANÁLISIS INICIAL

Una vez recibida la comunicación del informante mediante la Plataforma de Gestión del S.I.I. el RSI procederá a la valoración de la virtualidad de su contenido para evaluar si la información se ajusta al ámbito de aplicación previsto en el artículo 2 de la Ley 2/2023, que incluye:

- Infracciones del Derecho de la UE.
- Infracciones administrativas graves o muy graves o penales.

Como resultado de este análisis inicial el RSI resolverá inadmitir la comunicación, si no se ajusta al ámbito previsto en la Ley antes mencionando, o admitirla a trámite.

4. INFORMACIONES AMPLIATORIAS

El informante podrá aportar nueva información a lo largo de la gestión de la información

por la misma vía por la que presentó su comunicación.

Por su parte, tras el estudio de la comunicación recibida, el RSI puede estimar necesario ampliar la información recibida para poder sustentar de forma adecuada su valoración y análisis y, en su caso, su traslado a los órganos competentes en el ámbito penal o disciplinario.

En caso de que la información sea considerada relevante y creíble en el análisis inicial, y revele indicios de una infracción de las incluidas en el ámbito de este Procedimiento, se llevará a cabo una investigación interna para recopilar pruebas adicionales y determinar la veracidad de la información.

El RSI informará al afectado, de manera sucinta, sobre la existencia de la comunicación así como sobre los hechos informados y sus derechos, en los términos y con los límites que establece la Ley.

La Investigación Interna puede involucrar la recopilación de pruebas adicionales y cualquier otra actuación necesaria. Las entrevistas personales podrán ser documentadas o registradas en soporte adecuado a este fin, informando de ello al compareciente.

La Investigación Interna comprenderá, siempre que sea posible y el buen fin de la investigación no pueda verse perjudicado por ello, una entrevista con la persona afectada en la que, con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes, pudiendo comparecer asistida de abogado. La entrevista podrá ser documentada o registrada en soporte adecuado a este fin, informando de ello al compareciente.

5. FINALIZACIÓN DEL PROCESO INTERNO

Una vez concluida la investigación, el RSI elaborará un Informe de Conclusiones que recoja las diligencias practicadas, las medidas adoptadas, los hechos considerados probados, las posibles infracciones cometidas y sus presuntos responsables, y las recomendaciones para prevenir futuras infracciones, que será remitido a la Dirección de la Corporación, a los efectos oportunos, y se mantendrá un registro adecuado de los informes finales generados.

Las informaciones serán remitidas al Ministerio Fiscal, en cualquier fase del presente Procedimiento, con carácter inmediato a disponer de indicios de que los hechos pudiesen ser constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea.

6. PLAZO PARA LAS ACTUACIONES

El plazo máximo para dar respuesta a las actuaciones de investigación no podrá ser superior a **tres meses** a contar desde la recepción de la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo a criterio del RSI, en cuyo caso, este podrá extenderse hasta un máximo de otros **tres meses adicionales**.

7. REGISTRO Y CONTROL INTERNO DE LA INFORMACIÓN

El S.I.I. de CORES garantiza desde el principio del proceso la confidencialidad del informante y la protección de sus datos de carácter personal.

El sistema no almacenará datos personales que no sean imprescindibles para el conocimiento y tratamiento de la información recibida. La Plataforma de Gestión del S.I.I., mediante el diseño del formulario establecido, mitiga la comunicación y registro de este tipo de datos.

El S.I.I. contará con un Libro de Registro de las informaciones recibidas que, en todo caso, garantizará los requisitos de confidencialidad previstos en esta ley. Este registro no será público y solo se podrá acceder a él mediante petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella.

Los datos personales relativos a las informaciones recibidas y a las gestiones del RSI solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la Ley 2/2023.

La Plataforma de Gestión del S.I.I. eliminará los registros de forma automática tras un plazo establecido, tras lo cual sólo quedará la información de carácter no personal en el Libro de Registro a efectos de control de actuaciones y estadísticos.

8. INFRACCIONES

La Autoridad Independiente de Protección del Informante es el órgano competente para el conocimiento de las infracciones contempladas en el título IX de la Ley cometidas en el ámbito del sector público estatal.

Entre dichas infracciones se tipifican, entre otras, la adopción de cualquier represalia derivada de la comunicación frente a los informantes, la vulneración de las garantías de confidencialidad y anonimato previstas en la Ley o del deber de mantener secreto sobre cualquier aspecto relacionado con la información, y comunicar o revelar públicamente información a sabiendas de su falsedad.