

CANAL ÉTICO

Política del Sistema
Interno de Información

BRUC

CONTENIDO

1.	EL CANAL ÉTICO DE BRUC	3
2.	FORMAS DE ENVIAR COMUNICACIONES.....	4
3.	PRINCIPIOS GENERALES	4
3.1	CONFIDENCIALIDAD	4
3.2	ANONIMIDAD.....	5
3.3	PROHIBICIÓN DE REPRESALIAS.....	5
3.4	DERECHOS DE LA PARTE INVESTIGADA.....	6
3.5	TRAMITACIÓN DE LAS COMUNICACIONES	6
3.6	INVESTIGACIÓN Y CONCLUSIONES	7
4.	PROTECCIÓN DE DATOS PERSONALES.....	8
4.1	RESPONSABLE DE LOS DATOS	8
4.2	CATEGORÍAS DE DATOS PERSONALES Y FUENTES DE DATOS	8
4.3	TRATAMIENTO DE DATOS PERSONALES (FINES, BASE JURÍDICA Y PLAZOS DE CONSERVACION).....	9
5.	FORMACIÓN Y DIFUSIÓN.....	11
6.	LEGISLACIÓN APLICABLE.....	11
7.	RÉGIMEN DISCIPLINARIO	11
8.	APROBACIÓN Y MODIFICACIONES.....	12

1. EL CANAL ÉTICO DE BRUC

Bruc Energy, SL y sus filiales¹ ("Bruc" o el "Grupo") tienen un firme compromiso con el cumplimiento de la legislación nacional e internacional y la ética empresarial durante su actividad, tal y como se recoge en el Código de Conducta del Grupo (el "Código de Conducta"), que puede consultarse en la página web de Bruc (www.brucmanagementprojects.com).

Como parte de este compromiso, Bruc ha puesto en marcha un sistema de información interno, articulado en torno al Canal Ético de Bruc, a través del cual los profesionales del Grupo (tal y como se define más adelante) o cualquier tercero deben denunciar posibles infracciones penales o administrativas o cualquier otra conducta ilícita, comportamiento contrario al Código de Conducta o conducta no ética cometida en el contexto de los negocios de Bruc.

El término "Profesionales de Bruc" incluye a todas las personas que integran el Grupo, incluidos sus administradores o directivos, ejecutivos, empleados, becarios, así como aquellas personas físicas que actúen en su nombre o representación. En todo caso, como se ha indicado anteriormente, cualquier otra persona física que disponga de información sobre posibles conductas irregulares en el marco de una relación profesional con el Grupo deberá utilizar el Canal Ético previsto en esta Política. Todas las personas mencionadas en este párrafo serán denominadas "Informante" o "Informantes".

La presente política sobre el sistema de información interno (la "Política") establece los principios fundamentales del procedimiento de gestión de comunicaciones de conformidad con lo dispuesto 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 (la "Ley de Protección de los Informantes").

Tal y como establece el artículo 4 de la Ley de Protección de los Informantes, el sistema de información interno regulado en esta Política es el canal preferente para la comunicación de las acciones u omisiones previstas en el artículo 2 de la Ley de Protección de los Informantes², así como cualquier otra conducta ilícita, comportamiento contrario al Código de Conducta o conducta no ética cometida en el contexto de los negocios de Bruc. No obstante, la Ley de Protección de los Informantes también establece un canal externo de denuncia ante la Autoridad Independiente de Protección del Informante, A.A.I. ("AIPI")³, o las correspondientes autoridades competentes que puedan crearse a nivel autonómico, sin perjuicio de que también puedan dirigirse a las demás autoridades competentes, en función de la naturaleza de la infracción de que se trate⁴.

¹ Grupo se refiere conjuntamente a Bruc Energy, S.L. y sus filiales en los términos del artículo 42 del Código de Comercio.

² Las infracciones susceptibles de ser denunciadas son (i) las infracciones del Derecho de la UE cuando entren en el ámbito de aplicación del Anexo I de la Directiva (UE) 2019/1937 del Parlamento y del Consejo, de 23 de octubre de 2019, afecten a los intereses financieros de la Unión o afecten al mercado interior; (ii) las infracciones administrativas graves o muy graves de acuerdo con la legislación española; y (iii) las infracciones penales.

³ La Ley de Protección de los Informantes autoriza la creación de la AIPI, aunque esta autoridad aún no ha sido creada a la fecha de aprobación de esta Política.

⁴ Dependiendo de la información de que se trate, las comunicaciones podrán dirigirse a distintas autoridades, entre ellas la Comisión Nacional de los Mercados y la Competencia, la Agencia Estatal de Administración Tributaria, la Comisión Nacional del Mercado de Valores, la Agencia Española de Protección de Datos, etc. o, en su caso, a las autoridades penales competentes (Juzgado de Instrucción o de Paz, Fuerzas o Cuerpos de Seguridad del Estado, las Comunidades Autónomas o las Corporaciones Locales, y el Ministerio Fiscal o, cuando los hechos puedan suponer un ilícito penal que afecte a los intereses financieros de la Unión Europea, la Fiscalía Europea).

2. FORMAS DE ENVIAR COMUNICACIONES

El sistema de información interno de Bruc incluye los siguientes canales para la presentación de comunicaciones:

(i). Por escrito:

- a) A través del Canal Ético que Bruc tiene habilitado. Se puede acceder al canal [aquí](#).
- b) Por correo postal dirigido al Responsable del Sistema⁵, que deberá remitirlo a la siguiente dirección: Arturo Soria 336, 7 izquierda, 28033, Madrid.

(ii). Verbalmente:

- a) A través del Canal Ético que Bruc tiene habilitado, grabando un mensaje de voz o realizando una llamada telefónica. Se puede acceder al canal [aquí](#).
- b) Llamando al Responsable del Sistema al +34 910492775.
- c) A petición del Informante, mediante una reunión presencial con el Responsable del Sistema en el plazo de siete días desde la recepción de la solicitud.

Si los hechos revelados en la comunicación implican al Responsable del Sistema, el Informante podrá remitir la comunicación directamente al Director General de Bruc. El Informante podrá enviar su comunicación al CEO (i) en persona, (ii) por llamada telefónica, +34 910492775; (iii) por correo postal, Arturo Soria 336, 7 izquierda, 28033, Madrid.

Cuando las comunicaciones se reciban a través de otros canales internos específicos del Grupo (incluidos, entre otros, protocolos en materia de acoso, igualdad o cumplimiento normativo), dichas comunicaciones serán igualmente integradas en el Sistema Interno de Información, mediante su traslado al Responsable del Sistema, garantizando la aplicación de los principios y garantías establecidos en la presente Política.

3. PRINCIPIOS GENERALES

3.1 CONFIDENCIALIDAD

El acceso al contenido del Sistema Interno de Información quedará estrictamente limitado al Responsable del Sistema y, en su caso, a las personas expresamente autorizadas para la gestión y tramitación de las comunicaciones, dentro del ámbito de sus competencias. Dicho acceso estará sujeto a medidas técnicas y organizativas que garanticen la seguridad, integridad y confidencialidad de la información, de conformidad con la normativa aplicable.

Cualquier persona que participe directa o indirectamente en el tratamiento de las comunicaciones y en las correspondientes investigaciones internas deberá respetar la confidencialidad tanto de la comunicación recibida como de la investigación realizada, de acuerdo con la legislación aplicable. En el caso de que una comunicación se realice a través de un canal distinto a los mencionados en esta Política y se dirija a cualquier Profesional de Bruc, el Profesional del Grupo que reciba la comunicación

⁵ Según se define en la sección 3.5 de la Política.

deberá remitirla inmediatamente al Responsable del Sistema, quedando igualmente sujeto a la obligación de confidencialidad antes mencionada.

La garantía de confidencialidad de la identidad del Informante es uno de los principios rectores del sistema interno de información. Por ello, los datos del Informante no serán revelados a personas distintas de las implicadas en la recepción y tramitación de las comunicaciones o, en su caso, en la evaluación y aplicación de las medidas correctoras, legales o disciplinarias que se consideren necesarias. No se revelará la identidad del Informante al investigado, ni se divulgará ningún dato personal que permita indirectamente su identificación.

3.2 ANONIMIDAD

El Canal Ético regulado en esta Política permite comunicaciones anónimas, independientemente del medio por el que se realicen (verbal o escrito). No obstante, Bruc anima a los Informantes a revelar su identidad, en la medida en que ello facilite los respectivos procedimientos de investigación.

3.3 PROHIBICIÓN DE REPRESALIAS

El Informante que actúe de buena fe no podrá ser sancionado ni sufrir consecuencias negativas o represalias⁶ (incluidas amenazas o intentos de las mismas) por haber presentado una denuncia o comunicación. Esta garantía de no represalia se extiende a las personas físicas y jurídicas vinculadas al Informante⁷, a las personas que, dentro de la organización en la que presta servicios el Informante, le asistan en el proceso y a los representantes legales de los empleados en el ejercicio de sus funciones de asesoramiento y apoyo al Informante. La mera colaboración con la investigación nunca debe ser motivo de sanción, represalia o cualquier otra consecuencia negativa.

Quedan estrictamente prohibidas las comunicaciones con información que se sepa falsa o sin motivos razonables para creer que es cierta en el momento en que se realiza la comunicación. La protección de los informantes no será aplicable en estos casos y el Informante estará sujeto a sanción disciplinaria (incluido el despido disciplinario) y, en su caso, a las responsabilidades administrativas, penales y/o civiles previstas en la normativa aplicable.

⁶ De conformidad con el apartado 2 del artículo 36 de la Ley de protección de los Informantes, el concepto general de represalia incluye "cualesquiera acciones u omisiones prohibidas por la ley o que, directa o indirectamente, supongan un trato desfavorable que coloque a las personas que las sufran en una situación de desventaja particular con respecto a otras en el contexto laboral o profesional, debido exclusivamente a su condición de Informantes, o por haber realizado una revelación pública". Además, de conformidad con el artículo 36(1) de la Ley de Protección de los Informantes, se prohíben todos los actos que equivalgan a represalias, incluidas las amenazas y los intentos de represalias.

⁷ En concreto: (a) personas físicas relacionadas con el Informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del Informante; y (b) personas jurídicas, para las que el Informante trabaje o con las que tenga cualquier otra relación en un contexto laboral o en las que tenga una participación accionarial significativa. A estos efectos, se considera que una participación en el capital o en los derechos de voto sobre acciones o participaciones es significativa cuando, por su cuantía, permite a la persona que la ostenta tener capacidad de influir en la persona jurídica participada.

3.4 DERECHOS DE LA PARTE INVESTIGADA

El investigado tiene derecho a ser informado de las acciones u omisiones que se le atribuyan y a ser oído por el investigador interno cuantas veces lo solicite. No obstante, las comunicaciones con el investigado se llevarán a cabo en el momento y forma que se consideren oportunos para asegurar el buen fin de la investigación y deberán realizarse respetando la garantía de confidencialidad. Durante la investigación interna, se respetará el derecho del investigado a la defensa de sus intereses, el derecho de defensa, al honor y demás derechos previstos en la normativa aplicable.

3.5 TRAMITACIÓN DE LAS COMUNICACIONES

El Responsable de ESG de Bruc es la persona encargada de gestionar el sistema de información interno regulado en esta Política, de conformidad con lo establecido en el artículo 8 de la Ley de Protección de los Informantes (el "**Responsable del Sistema**" o el "**Responsable**").

De conformidad con lo dispuesto en la Ley 2/2023, de 20 de febrero, el nombramiento, cese o modificación del Responsable del Sistema Interno de Información será comunicado a la Autoridad Independiente de Protección del Informante (AIPI) o, en su caso, a la autoridad autonómica competente, en los plazos legalmente establecidos. El Responsable del Sistema velará por el cumplimiento de esta obligación y por la adecuada actualización de la información comunicada a las autoridades competentes.

El Responsable del Sistema será el encargado de velar por la efectiva implantación del Canal Ético y de este Sistema de Información Interno, así como por el tratamiento diligente de las comunicaciones, actuando con la máxima confidencialidad y de forma independiente, autónoma del resto de órganos internos y en ausencia de conflictos de interés, disponiendo para ello de todos los medios humanos, técnicos y económicos necesarios, garantizando en todo momento la objetividad e imparcialidad en la gestión de las comunicaciones.

El Responsable del Sistema admitirá a trámite las comunicaciones recibidas salvo que concurra alguna de las circunstancias siguientes

- (i) cuando los hechos comunicados sean completamente inverosímiles;
- (ii) cuando los hechos no se refieran a la posible comisión de un ilícito penal o infracción administrativa o cualquier otra conducta ilícita o contraria al Código de Conducta del Grupo cometida en el ámbito de la actividad del mismo;
- (iii) cuando la comunicación carezca manifiestamente de fundamento (por ejemplo, cuando se base en una mera opinión personal sin indicios de veracidad) o existan motivos razonables para creer que la información que sustenta la comunicación ha sido obtenida como resultado de un delito penal; y
- (iv) cuando la comunicación se refiera a hechos cubiertos por una comunicación anterior y no contenga nuevos datos significativos que justifiquen su tratamiento.

Sin perjuicio de la decisión sobre la admisibilidad de la comunicación, se enviará al Informante un acuse de recibo de la misma en el plazo de siete días naturales a partir de su recepción, salvo que ello pudiera poner en peligro la confidencialidad de la información.

Se permite la comunicación con el Informante y, si se considera necesario, se le podrá solicitar información adicional sobre los hechos comunicados. Para ello, el Informante podrá facilitar una dirección, correo electrónico o lugar seguro para recibir las correspondientes comunicaciones.

Las comunicaciones admitidas a trámite serán tratadas eficazmente y estudiadas con detalle para adoptar las medidas que, en su caso, se consideren pertinentes.

El Responsable del Sistema velará por la inexistencia de conflictos de intereses, actuales o potenciales, en la tramitación de las comunicaciones, a fin de garantizar que las mismas sean tratadas con la máxima imparcialidad y objetividad.

En el caso de que la comunicación se refiera al Responsable del Sistema o implique al Responsable del Sistema, éste se abstendrá de participar en su investigación e informará inmediatamente al Consejero Delegado de la Compañía, quien procederá a su investigación.

El plazo máximo para dar respuesta al Informante sobre la investigación se establece en tres meses desde la recepción de la comunicación correspondiente, salvo casos de especial complejidad que requieran una prórroga, en cuyo caso el plazo podrá ampliarse hasta en tres meses adicionales.

3.6 INVESTIGACIÓN Y CONCLUSIONES

En caso de que la comunicación sea admitida a trámite, el Responsable del Sistema será el instructor y, por tanto, el encargado de llevar a cabo una investigación adaptada a la complejidad y a las circunstancias del caso para comprobar la veracidad de los hechos comunicados.

En el supuesto de que el investigado sea el Responsable del Sistema o este pudiera tener algún conflicto de interés en relación con los hechos objeto de investigación, el CEO de Bruc nombrará a un instructor sustituto para la realización de la investigación sin que el Responsable del Sistema pueda intervenir en ella.

El instructor gestionará la práctica de todas las diligencias de investigación que resulten oportunas para el esclarecimiento de los hechos. Estas diligencias podrán consistir en:

- i. realizar entrevistas con el investigado o con otras personas;
- ii. solicitar información y documentación a terceros;
- iii. recabar toda la información o documentación que estime necesaria de cualquier persona que forme parte de Bruc;
- iv. solicitar el apoyo de expertos externos para el análisis de determinada información o documentación; y
- v. cualquier otra diligencia que el instructor estime oportuna para la averiguación de los hechos y se ajuste a la normativa aplicable y a lo dispuestos en esta Política.

En caso de que los hechos objeto de investigación ya estén siendo investigados por la autoridad competente, el instructor tendrá en cuenta esta circunstancia a la hora de valorar la procedencia de practicar las diligencias de investigación indicadas en el presente apartado.

Realizada la investigación que correspondiere en cada caso, el instructor emitirá un informe en el que se indicarán las actuaciones realizadas, así como las conclusiones alcanzadas. Este informe será remitido a la Comisión de Auditoría de Bruc.

Sin perjuicio de lo anterior, el Responsable del Sistema podrá informar de forma periódica a la Comisión de Auditoría y/o al Consejo de Administración de la recepción de la comunicación y de los avances que se vayan realizando en su tramitación, así como sobre el funcionamiento del Sistema Interno de Información, incluyendo información agregada y anonimizada sobre las comunicaciones recibidas, su estado de tramitación y las medidas adoptadas, garantizando en todo caso la confidencialidad de las personas afectadas..

4. PROTECCIÓN DE DATOS PERSONALES

4.1 RESPONSABLE DE LOS DATOS

Bruc, como matriz del Grupo Bruc, será considerada responsable del tratamiento de los datos personales derivados del uso del sistema de información interno y del tratamiento de las investigaciones internas (los "Datos Personales") de acuerdo con esta Política y con lo dispuesto en la legislación sobre protección de datos personales. Cada entidad del Grupo Bruc, o cualquier persona implicada en la investigación interna o implicada en el tratamiento de datos personales derivados del uso del sistema de información interno y del tratamiento de investigaciones internas será considerada corresponsable de los Datos Personales.

El Delegado de Protección de Datos es el punto de contacto con Bruc y con las distintas empresas del Grupo Bruc como entidades corresponsables del tratamiento de los Datos Personales. Si lo desean, los interesados pueden ponerse en contacto con el Responsable de Protección de Datos en la siguiente dirección de correo electrónico protecciondedatos@brucenergy.com.

4.2 CATEGORÍAS DE DATOS PERSONALES Y FUENTES DE DATOS

Los Datos Personales que serán objeto de tratamiento en el ámbito del sistema interno de información serán los datos identificativos, de contacto, económicos, profesionales y laborales y los relativos a los hechos comunicados, y en ocasiones excepcionales cuando sea necesario en el contexto y de acuerdo con la naturaleza de la investigación, los datos de categoría especial (incluidos los relativos a infracciones penales o administrativas, salud, sexualidad u origen étnico o racial), así como cualesquiera otros datos derivados del uso y funcionamiento del canal de comunicación regulado en esta Política.

Los Datos Personales tratados en el ámbito del sistema de información interno serán los facilitados directamente por los interesados o, en su caso, por los Informantes, así como por los Profesionales de Bruc y terceros a los que se solicite información en el curso de la investigación, si los hubiere, y que en todo caso estarán relacionados con los hechos investigados.

4.3 TRATAMIENTO DE DATOS PERSONALES (FINES, BASE JURÍDICA Y PLAZOS DE CONSERVACION)

4.3.1 Finalidad del tratamiento

Los Datos Personales serán tratados con la finalidad de gestionar las comunicaciones y decidir sobre su admisión o no, y, en caso de admisión, realizar la correspondiente investigación y adoptar las medidas correctoras y disciplinarias que procedan.

El tratamiento de datos se realizará en base al cumplimiento de las obligaciones legales del Grupo - artículo 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 ("GDPR")- o, en su caso, al cumplimiento de una misión realizada en interés público -artículo 6.1.e) del GDPR- de conformidad con la Ley de Protección de los Informantes.

Del mismo modo, y sólo cuando sea estrictamente necesario para estos fines, podrán tratarse categorías especiales de datos por razones de interés público importantes, de conformidad con el artículo 9, apartado 2, letra g), del RGPD.

4.3.2 Almacenamiento de los datos

Los Datos Personales sólo serán tratados en el CANAL ÉTICO durante el tiempo necesario para tomar una decisión sobre su admisibilidad y no serán revelados a terceros, salvo que sea necesario para el correcto funcionamiento del sistema o para decidir sobre la admisibilidad de una comunicación.

En particular, cuando las comunicaciones se presenten verbalmente, el Informante reconoce que la comunicación se documentará (i) mediante la grabación de la conversación en un formato seguro, duradero y accesible; o (ii) mediante una transcripción completa y exacta de la conversación realizada por el personal responsable de su tratamiento, en cuyo caso se ofrecerá al Informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción de la conversación.

Una vez resuelta la admisibilidad o inadmisibilidad, los Datos Personales serán borrados del CANAL ÉTICO y, en todo caso, si no se ha adoptado una decisión al respecto, transcurridos tres meses desde su registro. No obstante, una cantidad limitada de información podrá ser almacenada durante un periodo de tiempo superior para acreditar el funcionamiento del sistema.

4.3.3 Procesamiento de los datos personales durante una investigación

Si la comunicación es admitida a trámite, los Datos Personales podrán ser tratados fuera del CANAL ÉTICO por el equipo de investigación para llevar a cabo la correspondiente investigación interna. Este tratamiento se realizará en cumplimiento de las obligaciones legales del Grupo -art. 6(1)(c) GDPR- o, en su caso, en cumplimiento de una misión de interés público -art. 6(1)(e) GDPR- de conformidad con la Ley de Protección de los Informantes.

Los Datos Personales serán tratados durante el tiempo necesario para completar la investigación y cumplir con las obligaciones legales.

Si se descubre que la información facilitada o parte de ella es falsa, deberá suprimirse inmediatamente en cuanto se tenga conocimiento de ello, a menos que la falsedad pueda constituir un delito, en cuyo caso la información se conservará durante el tiempo necesario para el procedimiento judicial.

Una vez finalizada la investigación, los Datos Personales se conservarán durante el tiempo necesario para adoptar y aplicar las medidas oportunas y, posteriormente, durante el plazo máximo de prescripción de las posibles acciones legales o contractuales. En ningún caso se almacenarán los datos durante más de diez años.

4.3.4 Destinatarios de los datos y transferencias internacionales

Los datos personales serán gestionados por el Responsable del Sistema y las personas del Grupo. Los datos personales serán gestionados por el Responsable del Sistema y las personas del Grupo que, en el ámbito de su autoridad y funciones y de conformidad con la Ley de Protección de los Informantes, estén obligadas a ello. Sólo se revelará a terceros cuando resulte oportuno para la investigación (por ejemplo, proveedores de servicios o consultores externos) o para la posterior adopción de medidas correctoras (por ejemplo, al responsable de recursos humanos -cuando se vayan a adoptar medidas disciplinarias contra un empleado- o al responsable de los servicios jurídicos -cuando proceda emprender acciones legales en relación con los hechos comunicados- del Grupo).

La identidad del Informante podrá ser revelada a las autoridades judiciales, al Ministerio Fiscal o a las autoridades administrativas competentes en el marco de una investigación penal, disciplinaria o sancionadora. Las divulgaciones realizadas con estos fines estarán sujetas a las garantías establecidas en la legislación aplicable. En particular, se informará de ello al Informante antes de revelar su identidad, salvo que dicha información pudiera poner en peligro la investigación o el procedimiento judicial.

Si los hechos comunicados o posteriormente investigados implican circunstancias que requieran una transferencia internacional de Datos Personales, se adoptarán las medidas oportunas de acuerdo con la legislación aplicable. Asimismo, si el tratamiento de los datos por alguno de los proveedores de servicios que colaboran en la gestión del CANAL ÉTICO o en la investigación implicara transferencias internacionales, éstas se realizarán de acuerdo con la legislación aplicable. Por ejemplo, se adoptarán cláusulas contractuales tipo aprobadas por la Comisión Europea o se transferirán Datos Personales a países para los que la Comisión Europea haya reconocido que ofrecen un nivel adecuado de protección de Datos Personales (por ejemplo, Reino Unido o Japón). Puede solicitar información sobre las medidas de protección adoptadas por el Grupo Bruc poniéndose en contacto con el Responsable de Protección de Datos.

4.3.5 Ejercicio de los derechos de protección de datos

Los interesados podrán dirigirse al Responsable del Sistema o al Delegado de Protección de Datos con el fin de ejercitar sus derechos de acceso, rectificación, oposición, supresión, portabilidad, limitación o cualesquiera otros reconocidos en la ley en relación con los datos que figuren en el correspondiente fichero, de conformidad con la legislación aplicable. No obstante, cuando la persona a la que se

atribuyan los hechos o cualquier tercero ejercite su derecho de acceso, no se le comunicarán los datos identificativos del Informante.

Los interesados también podrán presentar una reclamación o solicitud relacionada con la protección de sus Datos Personales ante la Autoridad de Protección de Datos correspondiente, en España, la Agencia Española de Protección de Datos (www.aepd.es).

4.3.6 Obligaciones del Responsable del Sistema

El Responsable del Sistema velará por que se mantenga un registro de todas las comunicaciones recibidas y de las correspondientes investigaciones internas, garantizando el cumplimiento de los requisitos de confidencialidad y de las obligaciones en materia de protección de datos previstas en esta Política y en la normativa aplicable. El acceso a dicho registro quedará estrictamente limitado al Responsable del Sistema y, en su caso, a las personas debidamente autorizadas en el ámbito de sus funciones. Asimismo, podrá darse acceso a todo o parte del contenido de este registro a las autoridades judiciales, al Ministerio Fiscal o a las autoridades administrativas competentes, cuando así se requiera en el marco de un procedimiento judicial o administrativo.

5. FORMACIÓN Y DIFUSIÓN

El contenido de la Política, así como el funcionamiento del Canal Ético, serán objeto de cuantas acciones de comunicación y formación sea necesario para su correcto conocimiento y entendimiento.

Asimismo, una copia de la Política será puesta a disposición de todos los empleados de Bruc cuando se unan a la Compañía. La Política será puesta a disposición del público, a través de una sección específica relativa al Canal Ético de la página web del Grupo.

6. LEGISLACIÓN APLICABLE

Esta Política ha sido creada en base a la legislación española aplicable (en particular, la Ley de Protección de los Informantes), así como a los principios y obligaciones establecidos en 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 denuncian infracciones del Derecho de la Unión. En caso de que la comunicación esté sujeta a la legislación de cualquier otro país, la Política será aplicable sin perjuicio del cumplimiento de legislación distinta a la española (dentro de su ámbito de aplicación) en la medida en que dicha legislación establezca protecciones o garantías adicionales a las previstas en la misma.

7. RÉGIMEN DISCIPLINARIO

El incumplimiento de las disposiciones de esta Política puede dar lugar a sanciones disciplinarias u otras acciones apropiadas dependiendo de la relación que el infractor tenga con el Grupo Bruc.

8. APROBACIÓN Y MODIFICACIONES

El Consejo de Administración de Bruc es el encargado de la aprobación de la Política y las posteriores revisiones.

La Política aplica al Grupo Bruc, en virtud del artículo 11 de la Ley de Protección de los Informantes.

Fecha de actualización: 18 de junio de 2024.