PROGRAMA DE CUMPLIMIENTO GLOBAL SOBRE RESPONSABILIDAD PENAL CORPORATIVA

Noviembre 2025

INTRODUCCIÓN

ENEL S.p.A. ("**ENEL**") es el holding de un grupo multinacional que opera en un sector empresarial complejo y estrictamente reglamentado, así como en varios contextos de tipo económico, político, social y cultural.

En dicho contexto, la integridad se entiende como un valor fundamental para desempeñar actividades comerciales. Supone que todo el personal del Grupo actúe con lealtad, rectitud, transparencia y el cumplimiento estricto de la legislación y de las normativas nacionales e internacionales, así como de los estándares y directrices internacionales.

El "Programa de Cumplimiento Global sobre Responsabilidad Penal Corporativa", "**Enel Global Compliance Program**" o "**EGCP**" se ha concebido como una herramienta que permite reforzar el compromiso de ENEL sobre los mejores estándares éticos, jurídicos y profesionales con objeto de aumentar y defender la reputación del Grupo. A este efecto, define una serie de medidas preventivas orientadas a la responsabilidad penal en el ámbito empresarial.

En estos últimos años, han ido aumentando constantemente los países que han establecido un régimen de responsabilidad corporativa penal o cuasi penal, permitiendo que los tribunales sancionen a los Destinatarios Corporativos por la conducta delictiva de sus representantes, empleados o terceros que actúan en su nombre.

En algunas jurisdicciones, la legislación y las normativas vigentes exhortan a las empresas a adoptar estructuras de gobernanza corporativa y sistemas de prevención del riesgo para llegar a prevenir cualquier conducta delictiva por parte de gerentes, ejecutivos, empleados, así como de asesores externos, incluso contemplando una exención o reducción de sanciones en caso de adoptar las medidas preventivas oportunas.

En función de la normativa internacional más pertinente, el EGCP pretende definir **normas generales** de conducta para los empleados, componentes del órgano de administración y cualquier otro miembro de los organismos de gestión y control ("**Destinatarios Corporativos**") así como para los asesores y otros contratistas y, en general, terceros ("**Terceros**" u "**Otros Destinatarios**") (a partir de ahora los Destinatarios Corporativos y los Otros Destinatarios se denominarán de forma conjunta como los "**Destinatarios**") que han sido contratados o designados respectivamente o que tratan con o actúan en nombre de las filiales no italianas (las "**Filiales No Italianas**" o "**NIS**").

El EGCP ha de aplicarse a nivel global a todas las NIS en conformidad con su estructura de gobierno corporativo y el contexto jurídico local, así como con las diferencias culturales, sociales y económicas en los países donde operan las NIS.

Cuando existan contradicciones entre el ECGP y otras normas privadas o técnicas, prevalecerán las normas del EGCP.

Cuando la legislación y las normativas locales contengan requisitos específicos que difieran de las provisiones del EGCP, prevalecerán dichos requisitos.

1 MISIÓN

El EGCP representa una oportunidad para aumentar una prevención proactiva de la responsabilidad penal corporativa reforzando el gobierno corporativo y el sistema de control interno y su objetivo es apoyar una conducta apropiada y legítima en el marco del Grupo.

El EGCP identifica las principales normas de conducta que se esperan de todos los Destinatarios Corporativos y (de especificarse) de los Otros Destinatarios con objeto de:

(i) proporcionar a las NIS un sistema de normas principales encaminadas a prevenir una responsabilidad penal corporativa en sus respectivos países;
(ii) integrar todos los programas de cumplimiento normativo o "compliance" a nivel local adoptados por las NIS de conformidad con la legislación vigente en materia de responsabilidad penal corporativa.

Las normas que figuran en el EGCP se integran con las siguientes:

(i) las disposiciones establecidas en el código ético, que representa los principios éticos del Grupo que todos los Destinatarios están obligados a cumplir;
(ii) las disposiciones establecidas en el Plan de Tolerancia Cero con la Corrupción adoptado por el Grupo ENEL;
(iii) las disposiciones de gobierno corporativo adoptadas por las NIS, que reflejan la legislación vigente y las buenas prácticas internacionales;
(iv) el sistema de control interno que adoptan las NIS;
(v) las disposiciones establecidas en todos los programas de compliance a nivel local que adoptan las NIS para cumplir la legislación local en materia de responsabilidad penal corporativa y en todas las directrices, políticas o documentos organizativos internos correspondientes.

2 ESTRUCTURA

El EGCP identifica:

a) las modalidades de su adopción por parte de las NIS y el proceso de actualización correspondiente;
b) su divulgación a los Destinatarios y actividades de formación;
c) el régimen sancionador vigente en caso de violación de cualquier disposición que contenga;
d) las normas generales de control;
e) las áreas de actividad que se supervisarán en relación a ciertos tipos de conducta ilícita (las "**Áreas de Supervisión**" o "**ABM**") – que figuran en la Sección 7 – que en general se consideren delictivos y pueden ser cometidos potencialmente por las NIS, así como la prevención de lo que ENEL considera como prioridad para llevar su negocio con honradez e integridad (los "**Delitos**");
f) las principales normas de conducta relacionadas con las Áreas de Supervisión.

El EGCP queda integrado por el Anexo 1 referido a "Ejemplos de conducta ilícita adoptada en las ABM".

3 ADOPCIÓN, IMPLEMENTACIÓN, RESPONSABILIDAD Y ENMIENDAS CORRESPONDIENTES

El EGCP ha sido aprobado por el Consejo de Administración de ENEL y será objeto de la preceptiva aprobación del Consejo de Administración, u otro órgano de administración que corresponda de cada NIS.

El consejo de administración u otro órgano directivo de cada NIS, de conformidad con su autonomía e independencia:

(i) adopta las medidas más adecuadas para la implementación y supervisión del EGCP, teniendo en cuenta la dimensión, la complejidad de las actividades que se llevan a cabo, el sistema de control interno, así como el perfil de riesgo específico concerniente a la NIS y a su marco normativo;

(ii) es responsable de la implementación correcta de las Áreas de Supervisión y de las principales normas de conducta, tal como se establecen en la sección 10.2 del EGCP, así como del control proporcionado por el Enel Global Compliance Program.

Las NIS aplicarán el EGCP con arreglo a la legislación vigente, al tipo de actividad que desempeñan, así como a las características específicas de la estructura de su organización.

Los comités internos de la junta directiva de Enel S.p.A. evalúan las enmiendas o ampliación del Programa de Cumplimiento Global de Enel y las someten a la aprobación del Consejo de Administración. Las modificaciones o integraciones del EGCP serán posteriormente presentadas al consejo de administración u órgano de gobierno correspondiente de NIS.

Cada NIS deberá informar sobre cualquier cambio o interpretación específica realizada conforme a la legislación o prácticas locales. Asimismo, el Consejo de Administración u órgano de administración que corresponda de las NIS designará la estructura (persona u organismo) responsable de dar apoyo en la implementación y supervisión del EGCP, así como de ejecutar los controles pertinentes, en cumplimiento de la normativa aplicable.

4 DIVULGACIÓN DEL EGCP Y ACTIVIDADES DE FORMACIÓN

El EGCP estará disponible y se podrá descargar de la Intranet del Grupo ENEL.

A nivel de País se llevarán a cabo actividades de formación específica para todo el personal (incluso a través del e-learning) para garantizar la divulgación y la comprensión correcta del EGCP, de las ABM, así como de los tipos de conducta pertinentes para prevenir que se cometan dichos Delitos. Dichas actividades de formación también pueden organizarse en el ámbito de cualquier programa de formación que adopte una NIS en relación con el cumplimiento del derecho penal local y de los programas de compliance locales.

5 COMUNICACIÓN A TERCEROS

Los Terceros recibirán información sobre los principios y el contenido del EGCP a través de adecuada documentación contractual oportuna que proporcionará cláusulas estándares que, en función de las actividades reguladas por el contrato, serán obligatorias para la contraparte.

6 REPORTE DE DENUNCIAS POR PARTE DE EMPLEADOS O TERCEROS (NOTIFICACIÓN DE DENUNCIAS)

Los Destinatarios Corporativos del EGCP están obligados a informar sobre cualquier posible conducta indebida, irregularidad e incumplimiento del Programa de Cumplimiento Global de Enel.

En cumplimiento de la normativa vigente y de su "Política de Notificación de Denuncias", ENEL ha establecido un Canal de Notificación específico, gestionado por la Dirección General de Auditoría,

diseñado para para garantizar la confidencialidad de la identidad del informante, de las personas mencionadas en el informe, así como del contenido y la documentación relacionada. Los informes pueden presentarse de la siguiente manera:

i. por escrito, es decir, a través de la web, o a través del sistema de notificación en línea disponible en el sitio web del Grupo;

ii. de forma oral, a través de los números telefónicos indicados en la misma página web;

iii. o bien, mediante una reunión presencial, a petición del denunciante, dentro de un plazo razonable y utilizando los canales mencionados anteriormente.

De acuerdo con lo ya definido en el presente documento, ENEL tramita las denuncias recibidas en los plazos previstos por la normativa vigente, prohíbe cualquier forma de represalia y garantiza que no se realice ningún acto de represalia a raíz de una denuncia.

ENEL aplica sanciones disciplinarias contra:

(i) aquellos que violen las medidas de protección del denunciante u otras personas protegidas por la ley pertinente, o (ii) que oculten o intenten ocultar el informe; o (iii) quien viole las obligaciones de confidencialidad previstas en la legislación vigente en materia de notificación de denuncias; o (iv) quien sea responsable del no establecimiento o gestión indebida de los canales de notificación de acuerdo con los requisitos establecidos en las normativas vigentes sobre notificación de denuncias; o (v) quien sea responsable de la falta de verificación y análisis de los informes; o (vi) aquellos que tomen medidas de represalia contra el denunciante u otras personas protegidas por la ley pertinente, a causa del mismo informe; así como (vii) el informante o denunciante cuando se establezca, incluso mediante sentencia de primera instancia, la responsabilidad penal del mismo por los delitos de difamación o calumnia, o su responsabilidad civil por el mismo título en casos de dolo o negligencia grave.

7 SISTEMA DISCIPLINARIO

Las funciones competentes de las NIS aplicarán las medidas disciplinarias oportunas en caso de violación de cualquier norma de conducta establecida en el EGCP, con arreglo al régimen sancionador vigente, en virtud de las normas aplicables o de los programas de compliance locales y sin perjuicio de la protección proporcionada a los empleados prevista por la legislación local (ej. el derecho a la defensa o el principio del contradictorio). Las medidas disciplinarias se aplicarán a pesar de los resultados de cualquier posible procedimiento penal efectuado por la autoridad judicial competente.

La documentación contractual establecerá las sanciones oportunas, incluyendo, pero no limitado a la rescisión del contrato, en conformidad con la legislación vigente en caso de violación por parte de Terceros de cualquiera de las disposiciones contenidas en el EGCP.

8 DELITOS

El EGCP abarca los tipos de Delitos siguientes (a partir de ahora, "los Delitos", según se describen a continuación):

A. Delitos de soborno/corrupción

B. Otros delitos contra la administración pública

C. Fraude contable

D. Abuso del mercado

E. Financiación del terrorismo y delitos de blanqueo de capitales

F. Delitos contra los particulares

G. Delitos contra la seguridad y la salud

H. Delitos contra el medio ambiente

I. Delitos cibernéticos

J. Delitos contra los derechos de autor

K. Delitos tributarios

La sección 10.2 siguiente del EGCP identifica las áreas de actividad que las NIS han de supervisar y la principal norma de conducta aplicable.

La lista que figura en el apartado 10.2. no exonera a las NIS de que efectúen su propia evaluación del riesgo y definición de las principales normas de conducta, de estimarse oportuno.

Por lo tanto, las NIS pueden identificar:

(i) las actividades empresariales que puedan suponer un riesgo específico de cometer un Delito efectuando un análisis de los procesos de empresa, así como de las formas posibles de delinquir atribuibles a los tipos de delitos;

(ii) las normas de conducta adicionales que han de cumplir todos los Destinatarios Corporativos y (cuando se especifique expresamente) los Otros Destinatarios con objeto de:

- abstenerse de todo tipo de comportamiento que dé lugar a cualquiera de los Delitos anteriormente citados; y
- abstenerse de cualquier tipo de comportamiento que, aunque no constituya en sí ninguno de los Delitos anteriormente citados, potencialmente pudiera convertirse en uno de ellos.

9 SISTEMA DE CONTROL DEL EGCP

El EGCP proporciona los dos niveles de control siguientes en relación a las Áreas de Supervisión:

- normas generales de control;
- principales normas de conducta aplicables a cada ABM.

10.1 NORMAS GENERALES DE CONTROL

Las NIS adoptarán las normas generales de control siguientes:

1. **separación de funciones**: la asignación de funciones, tareas y responsabilidades dentro de una NIS se lleva a cabo respetando la separación de funciones en virtud de la cual ningún individuo puede ejecutar un proceso completo por sí solo (ej. según este principio, ningún individuo puede encargarse automáticamente de llevar a cabo una acción, autorizándola y comprobándola posteriormente); también puede garantizarse una separación oportuna de

las funciones utilizando sistemas IT que habiliten exclusivamente a Destinatarios identificados y autorizados para efectuar ciertas operaciones;

2. **poderes de firma y autorización**: han de crearse unas normas formales sobre el ejercicio de los poderes internos y de los poderes de firma. Los poderes de firma serán coherentes con las responsabilidades organizativas y ejecutivas asignadas a cada representante de la NIS;
3. **transparencia y trazabilidad de los procesos**: siempre tendrá que garantizarse la identificación y trazabilidad de las fuentes, la información y los controles efectuados para respaldar la formación e implementación de las decisiones de las NIS, así como de la administración de los recursos financieros; tendrá que garantizarse el almacenamiento adecuado de los datos y de la información pertinentes, a través de sistemas de información y/o de soporte de papel.
4. **gestión oportuna de las relaciones con Terceros**:

(i) revisión (due diligence) adecuada de los requisitos de honorabilidad antes de entablar cualquier tipo de relación. El alcance da cada evaluación de due diligence (que puede suponer hacer preguntas a través de contactos empresariales, cámaras de comercio locales, asociaciones empresariales o búsqueda en Internet, así como verificando las referencias comerciales y los estados de cuentas anuales) será proporcional al riesgo efectivo o percibido de que cada socio, asesor o proveedor potencial, no poseyera los requisitos anteriormente citados; a este respecto, las circunstancias siguientes pueden considerarse una "alerta roja".

- el tercero se encuentra en un país en el que, con relación a los índices internacionales, como el Índice de Percepción de Corrupción de Transparencia Internacional, es conocido por su corrupción generalizada, o en un país considerado como "país no cooperador" según la "lista negra" del GAFI u otras listas internacionales preparadas por instituciones internacionales por lo que concierne a la lucha global contra la financiación del terrorismo y el blanqueo de capitales;
- al tercero se le prohíbe o se le ha prohibido participar en licitaciones o ponerse en contacto con empresas estatales/organismos públicos/ agencias gubernamentales debido a investigaciones de compliance realizadas por autoridades públicas;
- el tercero ya está sometido a un procesamiento penal;
- el tercero se niega a cumplir el programa de compliance adoptado por la empresa y no adopta ningún código de conducta ni normas similares;
- el tercero tiene una relación familiar con un funcionario clave de la agencia gubernamental o con un funcionario extranjero;
- un funcionario público es el dueño, gerente ejecutivo o accionista principal del tercero;
- la dirección de la empresa del tercero es una oficina virtual;
- el tercero tiene un beneficiario efectivo secreto.

(ii) controles suplementarios en caso de que durante la fase de due diligence surgiera cualquier tipo de "alerta roja";

(iii) supervisión periódica durante la relación para garantizar que la contraparte siga cumpliendo los requisitos aprobados por la NIS, y

(iv) adopción de medidas apropiadas en caso de que el Tercero no mantenga dichos requisitos o de que surgiera cualquier tipo de "alerta roja" durante la relación contractual como, por ejemplo:

- el tercero insiste en tratar directamente con los funcionarios, sin permitir la participación de la empresa;
- el tercero solicita pagos anticipados inusuales;

- el tercero propone la entrega o bien entrega facturas inexactas o facturas por servicios que no se le han asignado o que no tenían que realizarse;
- el tercero solicita pagos en efectivo o instrumentos al portador;
- el tercero solicita que se le efectúen pagos fuera de su propio país, en una jurisdicción que no tiene ninguna relación con los organismos involucrados en la transacción o para la transacción;
- el tercero solicita que los pagos se efectúen a un intermediario o a otro organismo o solicita que los pagos se realicen a dos o varias cuentas corrientes;
- el tercero solicita que se donen fondos a una institución o fundación sin ánimo de lucro.

10.2 ÁMBITOS DE SUPERVISIÓN Y PRINCIPALES NORMAS DE CONDUCTA

A. DELITOS DE SOBORNO/CORRUPCIÓN

Este tipo de Delitos se refiere al hecho de ofrecer, dar, solicitar o recibir dinero (o cualquier otro beneficio, ganancia o ventaja) con el objetivo o la intención de influir en el destinatario (que puede ser un individuo perteneciente a una empresa privada o un funcionario público) de forma favorable para el tercero que paga el soborno o corrupción.

Los sobornos consisten en regalos o el pago de dinero (otras formas de soborno pueden incluir varios bienes, privilegios, entretenimientos y favores) a cambio de un trato favorable.

El trato favorable que efectúa el sobornador podría consistir en:

- la participación del sobornador en un contrato importante (con una administración pública o con una empresa privada);
- la adjudicación de una licitación pública;
- una falsa deposición, favorable para el sobornador, en un juicio por parte de un testigo;
- un informe indulgente por parte de un funcionario público.

Para más detalles, véanse los ejemplos citados en el Anexo 1.

ÁMBITOS DE SUPERVISIÓN

En relación a este tipo de Delitos, habrá que supervisar las áreas siguientes:

(i) negociación, ejecución y gestión de contratos relevantes con todas las Partes (administraciones públicas, empresas, asociaciones, fundaciones, etc.);
(ii) participación en licitaciones públicas o privadas;
(iii) gestión de relaciones (que no sean relaciones contractuales) con organizaciones comunitarias y administraciones públicas (ej. con referencia a los requisitos sobre salud, seguridad y medio ambiente, gestión del personal y pago de impuestos);
(iv) gestión de litigios (pleitos, arbitrajes y procedimientos extrajudiciales);
(v) selección de socios, intermediarios y asesores, así como negociación, ejecución y gestión de los contratos correspondientes;
(vi) gestión de efectivo y de recursos financieros;
(vii) gestión de iniciativas sin ánimo de lucro;
(viii) gestión de regalos, entretenimientos y gastos de hospitalidad;
(ix) reembolso de gastos de los empleados;

(x) contratación de personal;
(xi) definición de incentivos (ej. Gestión por objetivos – MBOs) destinados a los ejecutivos de las NIS.

PRINCIPALES NORMAS DE CONDUCTA

Al hacer negocios con empresas privadas, así como con administraciones públicas, gobiernos internacionales, nacionales, regionales y locales (las "**Autoridades Públicas**"), las NIS y sus representantes están comprometidos a actuar con integridad y honradez, y a cumplir con la legislación y la normativa vigente.

A los Destinatarios Corporativos y a los Terceros (en virtud de cláusulas contractuales específicas) les está específicamente prohibido:

a) ofrecer dinero o conceder otras ventajas de cualquier clase (promesas de empleo, etc.) a los representantes de las Autoridades Públicas así como a los individuos que pertenecen a una empresa privada, o a miembros de su familia, con quienes las NIS tienen intención de entablar o ya han entablado una relación comercial o, cuando se trata con los representantes de las Autoridades Públicas, o cualquier otra relación que incluye la solicitud de fondos públicos, la presentación de una autorización o permiso público, etc.;
b) ofrecer regalos, hospitalidades u otros beneficios a las personas mencionadas en el punto anterior, salvo que se trate de prácticas aceptadas conforme a los estándares empresariales habituales. No se consideran admisibles, entre otros: (i) viajes; (ii) regalos o entretenimiento ofrecidos a personas vinculadas a procesos de licitación en los que participe un NIS o cualquier empresa del grupo ENEL. Sólo se permiten aquellos beneficios que constituyan una cortesía comercial razonable, tales como: (i) comidas ocasionales de bajo valor; (ii) asistencia ocasional a eventos deportivos locales, teatros u otros eventos culturales; y (iii) regalos promocionales de escaso valor, como bolígrafos, calendarios u objetos similares. Los regalos ofrecidos - excepto aquellos de bajo valor – deberá ser documentado para permitir su inspección conforme a los controles internos establecidos;
c) utilizar efectivo como medio de pago excepto en los casos en que la normativa lo permita (ej. gastos menores);
d) incurrir en gastos promocionales o de patrocinio, a no ser que los gastos hayan sido aprobados con antelación y por escrito por la función competente;
e) hacer cualquier tipo de donación a instituciones sin ánimo de lucro, proyectos de servicio a la comunidad y asociaciones profesionales a no ser que dichos gastos hayan sido aprobados con antelación y por escrito por parte de la función competente;
f) adjudicar servicios a Terceros que no estén suficientemente justificados en relación a las necesidades de la NIS;
g) pagar dinero a Terceros que no esté suficientemente justificado en relación al tipo de tarea a realizar y a las costumbres locales del momento;

Las NIS evaluarán la posibilidad de adoptar las medidas organizativas oportunas para prevenir que los Destinatarios efectúen cualquiera de las actividades anteriormente citadas. Asimismo, las NIS evaluarán la posibilidad de adoptar procedimientos adecuados para asegurar que:

h) se tengan las pruebas oportunas con respecto a las relaciones importantes (ej. procedimientos administrativos encaminados a obtener una autorización, una licencia o acto similar, empresas mixtas con entidades públicas, tramitación de documentos para obtener una cierta autorización pública) con las Autoridades Públicas y cualquier relación comercial importante;

i) las relaciones con las Autoridades Públicas, cuando las cuestiones concernientes a los intereses de la NIS estén bloqueadas, las llevarán como mínimo dos Destinatarios autorizados;
j) cualquier procedimiento de contratación de personal se efectuará exclusivamente por una necesidad empresarial efectiva demostrable; en el proceso de selección participarán como mínimo dos funciones y se basará en criterios de objetividad, competencia y profesionalidad para evitar favoritismos o nepotismo y conflictos de intereses;
k) los planes de incentivos para los gerentes se adoptarán para garantizar que los objetivos establecidos no den lugar a conductas abusivas y, por el contrario, se basen en un resultado posible, determinado, conmensurable y relacionado con el tiempo necesario para lograrlos;
l) en relación a la planificación de proyectos se establecerá un calendario realista;
m) en relación al reembolso de los gastos, se presentará la documentación oportuna, incluyendo los recibos originales del pago de los gastos o costes incurridos, al departamento de contabilidad antes del pago y se describirá con exactitud el pago o gasto subsiguiente (o recibo del mismo), quedando reflejado en los registros contables de la NIS en cuestión.

B. OTROS DELITOS CONTRA LA ADMINISTRACIÓN PÚBLICA

Este tipo de Delitos principalmente está relacionado con el fraude contra las instituciones públicas y ocurre cuando una empresa usa un artificio u otro engaño para defraudar a la entidad pública o para conseguir una ventaja económica a través de representaciones falsas o fraudulentas, promesas o pretextos.

Dicho tipo de Delitos suele estar relacionado con el uso de la financiación pública y de las subvenciones de forma diferente a la prevista en el acuerdo de subvención.

Este tipo de Delito puede darse por una amplia serie de razones, que suelen estar relacionadas con la obtención de una ventaja económica.

Para más detalles, véanse los ejemplos citados en el Anexo 1.

ÁREAS DE SUPERVISIÓN

En relación a este tipo de Delitos, habrá que supervisar las áreas siguientes:

(i) participación en licitaciones públicas y procedimientos públicos en general;
(ii) gestión de relaciones con Autoridades Públicas (ej. con referencia a los requisitos sobre salud, seguridad y medio ambiente, gestión del personal y pago de impuestos);
(iii) petición de financiación pública, subvenciones, subsidios o garantías concedidas por la Administración Pública;
(iv) gestión de la financiación pública recibida, subvenciones, subsidios o garantías obtenidas.

PRINCIPALES NORMAS DE CONDUCTA

Además de las principales normas de conducta establecidas en el apartado 10.2.A) anteriormente citado, los Destinatarios Corporativos y los Terceros (según condiciones contractuales específicas), se abstendrán de:

a) presentar documentos falsos o alterados, de forma parcial o total, durante la participación en ofertas públicas;
b) inducir de alguna forma a las Autoridades Públicas a efectuar una evaluación incorrecta durante el examen de la solicitud de autorizaciones, licencias, permisos, concesiones, etc.;

c) omitir información debida con objeto de dirigir en favor de la NIS decisiones de las Autoridades Públicas en relación a todas las circunstancias descritas en la letra a) y b) anteriormente citadas;
d) todo tipo de conducta encaminada a obtener de la Administración Pública cualquier tipo de subvención, financiación, préstamo bonificado o cualquier otro tipo de desembolso similar, presentando estados de cuentas y documentos falsificados, u omitiendo información pertinente o, en general, mediante artificio o engaño tratando de inducir a error a la institución otorgante;
e) utilizar el dinero recibido de las Autoridades Públicas como financiaciones, contribuciones o préstamos para fines que no tengan nada que ver con los fines para los que se hubieran concedido.

Asimismo, para aplicar las normas de conducta anteriormente citadas, las NIS evaluarán la posibilidad de adoptar las medidas organizativas oportunas para asegurar que:

f) las declaraciones presentadas a las Autoridades Públicas nacionales o internacionales a efectos de obtener financiaciones, subvenciones o préstamos incluyan exclusivamente información verdadera y estén firmadas por firmantes autorizados y cuando se obtengan dichas financiaciones, subvenciones o préstamos, se contabilicen correctamente;
g) exista una separación oportuna de los controles de las tareas, garantizando que las fases de solicitud, gestión y presentación de informes con respecto a los trámites administrativos a efectos de la obtención de financiaciones, subvenciones o préstamos sean efectuados por Destinatarios Corporativos diferentes dentro de la organización;
h) las actividades de recopilación y análisis de la información que son necesarias para la presentación de informes se lleven a cabo con el apoyo de las funciones competentes;
i) la documentación y la subsiguiente presentación de informes que se efectúe a efectos de la solicitud de financiaciones, subvenciones, préstamos y garantías tendrán que ser aprobados por los niveles jerárquicos oportunos.

C. FRAUDE CONTABLE

El Fraude Contable es un tipo de Delito que consiste principalmente en manipular intencionalmente los estados financieros para crear una representación falsa de la salud financiera de una empresa frente a los inversores, acreedores, accionistas y otras partes interesadas.

El Fraude Contable puede darse por varias razones, que incluyen, pero no se limitan a las siguientes:

(i) seguir obteniendo financiación de un banco (con este propósito, se podría alterar el estado de cuentas para crear una representación de salud financiera);
(ii) registrar beneficios no realistas u ocultar pérdidas;
(iii) ocultar circunstancias que podrían afectar negativamente a la empresa;
(iv) provocar la inflación del precio de las acciones;
(v) disimular la creación de fondos secretos;
(vi) encubrir actos indebidos (como robo, efectuados por gerentes de la empresa);
(vii) omitir hechos materiales que pueden inducir a error a cualquier interlocutor (ej. partes interesadas, acreedores, autoridades bursátiles, etc.).

Para más detalles, véanse los ejemplos citados en el Anexo 1.

ÁREAS DE SUPERVISIÓN

En relación a este tipo de Delitos, habrá que supervisar las áreas siguientes:

(i) redacción de documentos destinados a los inversionistas o al público (ej. estados de cuentas e informes financieros periódicos) concernientes a los activos y pasivos, ingresos, gastos y flujos de efectivo de las NIS, aunque dichos documentos no sean los documentos contables periódicos;
(ii) gestión de relaciones con auditores externos y órganos de supervisión.

PRINCIPALES NORMAS DE CONDUCTA

Las Filiales No italianas han de mantener los libros, registros y cuentas que reflejen con precisión y exactitud y con un grado de detalle razonable toda transacción y disposición de bienes de las empresas.

Las Filiales No italianas considerarán la posibilidad de adoptar las medidas oportunas, y el personal asignado para mantener los libros, registros y cuentas tendrá que actuar oportunamente para asegurar que:

a) los datos y la información que se utilice para preparar los informes financieros periódicos sean exactos y comprobados diligentemente;
b) todos los elementos de balance, cuya determinación y cuantificación supongan una evaluación discrecional, sean objetivos y estén respaldados por la documentación oportuna;
c) las operaciones se lleven a cabo según las autorizaciones generales o específicas de la dirección;
d) las facturas, así como otros documentos pertinentes relacionados con las transacciones sean examinadas, registradas y archivadas correctamente;
e) las operaciones se registren según es necesario para poder preparar los estados financieros, conforme con los principios de contabilidad generalmente aceptados o aplicables o cualquier otro criterio aplicable a dichos estados financieros;
f) el acceso a dichos registros de operaciones esté permitido sólo en virtud de las autorizaciones generales o específicas de la dirección.

Asimismo, para garantizar que se facilite al mercado una información completa y justa, las Filiales No italianas no pueden adoptar ningún tipo de conducta que impida y, en cualquier caso, obstaculice las actividades de control y auditoría por parte de auditores externos, ocultando documentación o utilizando otros medios fraudulentos.

Por último, es necesario que las Filiales No italianas efectúen todo tipo de comunicaciones hacia cualquier autoridad financiera pública (tal como requiere la legislación local vigente) de forma correcta, completa, adecuada y rápida, sin impedirse en modo alguno el desempeño de sus obligaciones, incluso en caso de inspecciones (ej. denegación expresa, rechazo irrazonable, conducta obstruccionista o falta de colaboración).

D. ABUSO DEL MERCADO

Esta categoría de Delitos se refiere principalmente a tres tipos diferentes de conducta: (1) comprar o vender instrumentos financieros utilizando información que no está a disposición del público ("Información interna" – Inside Information) o que se haya comunicado ilegalmente a terceros; (2) alterar el mecanismo de fijación de precios de los instrumentos financieros dando a sabiendas información falsa o engañosa para influir en el precio de un instrumento financiero; (3) efectuar órdenes de venta y de compra que proporcionan o pretenden (i) proporcionar indicaciones falsas o engañosas con respecto a la oferta, a la demanda o al precio de los instrumentos financieros, (ii) determinar el precio de mercado de uno o varios instrumentos financieros a un nivel anómalo o artificial.

Estos tipos de conducta pueden tener lugar para beneficiar a la empresa, por una serie de razones, que incluyen, pero no se limitan a las siguientes:

- deflactar el precio de las acciones de una empresa determinada antes de comprarlas;
- debilitar la reputación de una empresa rival;
- alterar el precio de un cierto instrumento financiero en cartera antes de efectuar cualquier actividad relacionada con el mismo.

Para más detalles, véanse los ejemplos citados en el Anexo 1.

ÁREAS DE SUPERVISIÓN

En relación a este tipo de Delitos, habrá que supervisar las áreas siguientes:

(i) gestión de la información pública (ej. con respecto a los inversores, analistas y periodistas financieros y otros representantes de los medios de comunicación) y organización y participación en reuniones de cualquier tipo con los Destinatarios anteriormente citados;
(ii) gestión de la Información Interna relacionada con las sociedades cotizadas del Grupo y los instrumentos financieros pertinentes (por ejemplo, nuevos productos, servicios y mercados, datos contables periódicos, datos de previsión y objetivos cuantitativos que conciernan a los resultados de la empresa, fusiones y escisiones, así como nuevos compromisos particularmente significativos, como, por ejemplo, conversaciones y acuerdos concernientes a la adquisición o a la venta de activos importantes);
(iii) gestión de la Información Interna relacionada con derivados energéticos (por ejemplo, información sobre la falta de disponibilidad de las instalaciones);
(iv) cualquier tipo de operación relacionada con los instrumentos financieros en cartera.

PRINCIPALES NORMAS DE CONDUCTA

Se prohíbe expresamente a todos los Destinatarios:

a) utilizar la Información Interna para negociar, directa o indirectamente, instrumentos financieros para obtener ventajas personales o para favorecer a Terceros o a las NIS o a cualquier otra empresa del Grupo;
b) revelar Información Interna a Terceros, salvo cuando lo requiera la ley u otras disposiciones normativas o contratos específicos en los que las contrapartes estén obligadas a utilizar la información sólo para la finalidad a la que estaba destinada en principio y manteniendo su confidencialidad;
c) aconsejar o inducir a una persona, en función de cierta Información Interna, a efectuar cualquier tipo de operaciones en instrumentos financieros.
d) divulgar información falsa o engañosa a través de los medios de comunicación (sobre la empresa o sobre otras empresas), incluyendo Internet, o por cualquier otro medio, para alterar el proceso de las acciones, derivados o cualquier actividad subyacente que respalden operaciones que ya han sido planificadas por el sujeto que divulga la información en cuestión;
e) realizar operaciones con instrumentos financieros (ej. compra o venta) contra las normas sobre el abuso del mercado.

E. FINANCIACIÓN DEL TERRORISMO Y DELITOS DE BLANQUEO DE CAPITALES

La financiación del terrorismo supone la solicitud, captación o suministro de fondos con la intención de utilizarlos para apoyar actos u organizaciones terroristas. El objetivo principal de los

individuos o entidades involucradas en la financiación del terrorismo es ocultar la financiación, así como la naturaleza de la actividad financiada.

El blanqueo de capitales es el proceso por el cual los ingresos derivados de actividades delictivas están encubiertos para ocultar su origen ilícito. Más concretamente, puede incluir tres conductas diferentes y alternativas: (i) la conversión o transferencia de fondos, a sabiendas de que se trata de ingresos derivados de actividades delictivas (ii) la ocultación o encubrimiento de la verdadera naturaleza, fuente, ubicación, disposición, movimiento o propiedad de o derechos con respecto a la propiedad, sabiendo que dicha propiedad representa ingresos derivados de actividades delictivas; y (iii) la adquisición, posesión o uso, sabiendo, en el momento de su recepción, que dicha propiedad representa ingresos derivados de actividades delictivas.

Cuando los ingresos de una conducta delictiva son creados por la misma persona que oculta su origen ilícito, en ciertos países dicha conducta se sanciona como autoblanqueo de capitales.

El blanqueo de capitales y la financiación del terrorismo suelen mostrar características similares, principalmente relacionadas con la ocultación del dinero. Los blanqueadores de capitales envían fondos ilícitos a través de canales legales para ocultar su origen ilícito, mientras quienes financian el terrorismo transfieren fondos que pueden ser legales o ilícitos en un principio ocultando su fuente y uso final, que es el apoyo al terrorismo.

Estos tipos de conducta pueden tener lugar para beneficiar a la empresa, por una serie de razones, que incluyen, pero no se limitan a las siguientes:

- obtener ingresos o cualquier otra ventaja que derive de las actividades ilegales efectuadas por las organizaciones terroristas que han sido financiadas (las otras ventajas pueden consistir en protección de la empresa, en los países donde dichas organizaciones tienen una gran influencia);
- encubrir el origen ilegal de los ingresos derivados de actividades delictivas.

Para más detalles, véanse los ejemplos citados en el Anexo 1.

ÁREAS DE SUPERVISIÓN

En relación a este tipo de Delitos, habrá que supervisar las áreas siguientes:

(i) transacciones financieras o comerciales realizadas con individuos o corporaciones (y entidades legales controladas directa o indirectamente por los sujetos mencionados anteriormente) que tienen su residencia o una oficina registrada en un país que representa una jurisdicción de alto riesgo y no cooperadora (ej. con deficiencias estratégicas en su estructura para combatir el blanqueo de capitales y la proliferación de la financiación del terrorismo) de conformidad con la evaluación efectuada por las autoridades internacionales (ej. FATF).

PRINCIPALES NORMAS DE CONDUCTA

Las NIS condenarán el uso de sus recursos para financiar o efectuar cualquier actividad encaminada a lograr objetivos relacionados con la financiación del terrorismo, así como todo uso indebido de instrumentos y operaciones financieros que pretendan encubrir el origen de los fondos de la empresa.

De manera más general, las NIS condenarán cualquier conducta posible encaminada, aunque fuera indirectamente, a facilitar delitos de receptación, blanqueo o uso de capitales, bienes o cualquier otra utilidad de origen ilícito; a este respecto la NIS se compromete a efectuar todos los controles necesarios previos y subsiguientes para lograr dicho objetivo, reglamentando asimismo las

relaciones con terceros mediante disposiciones contractuales que exijan el cumplimiento de la legislación vigente sobre la materia.

En especial, queda prohibido lo siguiente:

a) usar documentos de pago en blanco o efectivo para cualquier operación de cobro, pago, transferencia de fondos, etc.;
b) hacer o recibir pagos en cuentas corrientes anónimas o en cuentas corrientes de bancos ubicados en jurisdicciones de alto riesgo;
c) emitir o recibir facturas o emitir documentos con referencia a operaciones inexistentes.

Asimismo, para aplicar las normas de conducta anteriormente citadas, las NIS tienen que:

d) efectuar controles analíticos de los flujos de efectivo;
e) comprobar la validez de los pagos, controlando que su beneficiario sea efectivamente la contraparte con la que se ha contratado;
f) efectuar un control de los procedimientos, especialmente por lo que concierne a posibles operaciones que tengan lugar fuera de los procesos normales de la Empresa;
g) disponer de pruebas de todas las transacciones efectuadas;
h) garantizar la trazabilidad de todas las operaciones financieras, así como de acuerdos o cualquier otra inversión o proyecto de la empresa;
i) comprobar la coherencia económica de dichas operaciones e inversiones;
j) comprobar la lista negra internacional concerniente al terrorismo y jurisdicciones de alto riesgo.

F. DELITOS CONTRA LOS PARTICULARES

La expresión "delitos contra los Particulares" se refiere a varios tipos de delitos que a menudo suponen lesiones personales, la amenaza de agresión física u otras acciones cometidas contra la voluntad de una persona.

De cualquier forma, a efectos de este EGCP, los Delitos contra los Particulares se refieren principalmente a los delitos que pueden ocurrir con más frecuencia en la administración de una empresa como los que se refieren a prácticas de trabajos forzosos, que consisten principalmente en obligar a los empleados a trabajar utilizando la violencia o la intimidación, o por otros medios como la retención de los documentos de identidad.

Este tipo de Delito puede tener lugar por varias razones, que incluyen, pero no se limitan a lo siguiente:

- emplear mano de obra con un gasto mínimo;
- emplear mano de obra totalmente supeditada, que no podría negarse a cumplir con cualquier petición.

Para más información, consúltense los ejemplos que figuran en el Anexo 1.

ÁREAS DE SUPERVISIÓN

En relación a este tipo de Delitos, habrá que supervisar las áreas siguientes:

(i) celebrar contratos con proveedores que no utilizan personal especializado o trabajar en países donde los derechos humanos no están totalmente protegidos por la legislación internacional o local.

PRINCIPALES NORMAS DE CONDUCTA

Las Filiales No italianas deberán efectuar lo siguiente:

a) seleccionar Terceros externos (ej. socios, proveedores), especialmente los que suministren servicios que no sean técnicos, solo después de constatar atentamente su fiabilidad;
b) preparar una documentación contractual correcta con los contratistas externos exigiéndoles que cumplan, y exigiéndoles que sus subcontratistas cumplan, la legislación local e internacional vigente (ej. convenios de la OIT sobre la edad laboral mínima y sobre las peores formas de trabajo infantil) sobre el trabajo forzoso, protección del trabajo infantil y de las mujeres y cumplimiento de las condiciones higiénico-sanitarias;
c) contemplar y aplicar sanciones contractuales en el contrato en cuestión si un contratista o cualquiera de sus subcontratistas violara cualquiera de las leyes locales e internacionales vigentes.

G. DELITOS CONTRA LA SEGURIDAD Y LA SALUD

Los delitos contra la seguridad y la salud suelen relacionarse con el incumplimiento de la legislación local y de las normas laborales en los lugares de trabajo para evitar accidentes y enfermedades laborales.

Estos tipos de conducta pueden darse para beneficiar a la empresa, por una serie de razones, que incluyen, pero no se limitan a las siguientes:

(i) reducir costes, ya que adoptar las medidas necesarias supone costes adicionales para una empresa;
(ii) aumentar la productividad, ya que trabajar sin considerar procedimientos y políticas cautelares podría acelerar el proceso de producción.

Para más información, consúltense los ejemplos que figuran en el Anexo 1.

ÁREAS DE SUPERVISIÓN

Con respecto a los tipos de Delitos, habrá que supervisar las áreas siguientes:

(i) cumplir la normativa vigente sobre la seguridad y la salud.

PRINCIPALES NORMAS DE CONDUCTA

Al margen de la dimensión de la legislación local sobre la seguridad y la salud en el puesto de trabajo, la NIS fomentará y promoverá la protección de la seguridad en el puesto de trabajo, aumentando la toma de conciencia en relación a los riesgos y responsabilidades de la conducta individual.

A este efecto, no obstante, el cumplimiento de la legislación local vigente en materia de seguridad y salud en el puesto de trabajo, la NIS se compromete a adoptar las medidas necesarias, para proteger la integridad física y moral de sus trabajadores.

Especialmente, la NIS garantizará:

a) el respeto de las disposiciones legislativas que rigen la seguridad y la salud de los trabajadores en el puesto de trabajo como prioridad;
b) la evaluación de los riesgos de los trabajadores, en lo posible y gracias a la evolución de las técnicas más modernas, con el objetivo de protección de los mismos, eligiendo los materiales y equipos de seguridad más adecuados para eliminar o, cuando esto no sea posible, reducir el riesgo en su origen;

c) la información y capacitación de los trabajadores habrá de ser amplia, actualizada y específica con referencia a la actividad desempeñada;
d) la consulta periódica de los trabajadores sobre temas que conciernan a la seguridad y la salud de los trabajadores en el puesto de trabajo;
e) se aplique un sistema de supervisión eficaz para garantizar la correcta implementación de las medidas preventivas. Cualquier incumplimiento o área de mejora detectada durante la actividad laboral o en el marco de inspecciones periódicas será abordada de forma oportuna y eficaz;
f) la organización de las tareas laborales estará estructurada para proteger la integridad de los trabajadores, de Terceros y de la comunidad en la que opera la NIS.

Para lograr lo anteriormente expuesto, la NIS asignará recursos organizativos, instrumentales y económicos para garantizar el pleno cumplimiento de las disposiciones actuales sobre la prevención de accidentes laborales y para mejorar constantemente la seguridad y la salud de los trabajadores en el puesto de trabajo y las medidas preventivas oportunas.

Los Destinatarios Corporativos, cada cual en función del rol que desempeñe en la organización, deberán garantizar el pleno respeto de las disposiciones legislativas, de los procedimientos empresariales y de cualquier otra normativa interna que tenga por objeto proteger la seguridad y la salud de los trabajadores en el puesto de trabajo.

H. DELITOS CONTRA EL MEDIO AMBIENTE

Los Delitos contra el medio ambiente se refieren a una amplia lista de actividades ilícitas, que incluyen el comercio ilegal de flora y fauna silvestre, delitos relacionados con la gestión de las aguas, comercio ilícito y eliminación de residuos peligrosos y contrabando de substancias que afectan a la capa de ozono.

Los Delitos contra el medio ambiente afectan normalmente a la calidad del aire, del agua y del suelo, amenazan la supervivencia de las especies, pueden ocasionar desastres incontrolables y constituir una amenaza para la seguridad de un gran número de Destinatarios.

Viéndose estimuladas por las ganancias enormes y facilitadas por un bajo índice de detección y un bajo número de condenas, las redes criminales y las organizaciones de delincuencia organizada se están interesando cada vez más en estas actividades transnacionales ilícitas.

Estos tipos de conducta pueden darse para beneficiar a la empresa, por una serie de razones, que incluyen, pero no se limitan a las siguientes:

- reducir costes ya que la adopción de las medidas necesarias para proteger el medio ambiente a menudo implica costes extra;
- aumentar la productividad, ya que trabajar sin considerar las cuestiones ambientales podría acelerar el proceso de producción.

Para más información, consúltense los ejemplos que figuran en el Anexo 1.

ÁREAS DE SUPERVISIÓN

Con respecto a los tipos de Delitos, habrá que supervisar las áreas siguientes:

(i) cumplir la legislación vigente en materia de medio ambiente en lo referente al diseño, construcción, gestión mantenimiento, desactivación/desmantelamiento de las plantas, interconexiones e infraestructuras de redes de distribución
(ii) cumplimiento de la normativa ambiental aplicables en la prestación de productos y servicios relacionados con la energía, la eficiencia energética y la movilidad eléctrica,

tanto a clientes residenciales, como a pequeñas, medianas y grandes empresas, así como entidades del sector público; incluyendo el diseño, prueba y desarrollo de productos de movilidad eléctrica e innovación tecnológica.

PRINCIPALES NORMAS DE CONDUCTA

En sus actividades, la NIS seguirá el principio de proteger el medio ambiente. Especialmente, la NIS:

a) contribuye a la divulgación y a la toma de conciencia sobre la protección del medio ambiente y gestiona las actividades que se le encomiendan, en conformidad con la legislación vigente;
b) promueve el desarrollo científico y tecnológico encaminado a proteger el medio ambiente y a salvaguardar los recursos adoptando modernos sistemas de protección del medio ambiente y de eficiencia energética durante sus operaciones;
c) trabaja para cumplir las expectativas de sus clientes y accionistas por lo que concierne a las cuestiones del medio ambiente y adopta todos los medios oportunos para su protección y preservación, condenando toda forma de daños y perjuicios al ecosistema.

En los contratos que se celebren con Terceros donde puede plantearse la responsabilidad de la Empresa con respecto a las normas ambientales, en especial, a la gestión y eliminación de residuos, la Empresa incluirá disposiciones que impongan a dichos Terceros el cumplimiento de la normativa vigente y contemplará sanciones contractuales en caso de violación.

I. DELITOS CIBERNÉTICOS

Los Delitos cibernéticos pueden ser de dos tipos: uno en el que el objetivo es la red o un ordenador y otro en el que los delitos son ejecutados o enviados por un ordenador.

A efectos del EGCP, los Delitos cibernéticos no incluyen los delitos que pueden ser facilitados por un delito informático como fraude, robo, chantaje, falsificación e intimidación (ej. intimidación o acecho por Internet).

Por lo tanto, los Delitos cibernéticos considerados por el EGCP por ejemplo consisten en:

(i) intrusión no autorizada en un red protegida;
(ii) introducción de virus informáticos en un sistema informático;
(iii) interceptación de datos de una red informática.

Los Delitos cibernéticos pueden darse por varias razones, que incluyen, pero no se limitan a las siguientes:

- robar secretos comerciales a una empresa rival;
- poner en peligro o dañar el sistema informático de una empresa rival;
- conseguir información confidencial acerca de las estrategias de mercado de las empresas rivales.

Para más información, consúltense los ejemplos que figuran en el Anexo 1.

ÁREAS DE SUPERVISIÓN

Con respecto a los tipos de Delitos, habrá que supervisar las áreas siguientes:

(i) actividades digitales realizadas por los Destinatarios, tanto en entornos de Tecnologías de Información como de Tecnología Operativa, incluyendo el uso de recursos como la intranet, internet, correo electrónico corporativo, aplicaciones empresariales,

plataformas de colaboración e intercambio de datos, redes sociales, herramientas de mensajería instantánea;

(ii) gestión y protección de los dispositivos corporativos (por ejemplo, estaciones de trabajo, teléfonos inteligentes, dispositivos extraíbles) y de las infraestructuras tecnológicas (como servidores, switches, routers, cortafuegos y sistemas de almacenamiento)

(iii) planificación e implementación de medidas preventivas para mitigar el riesgo de pérdida de datos e información, así como para garantizar la confidencialidad, integridad y disponibilidad de los activas digitales gestión de perfiles de usuarios privilegiados;

PRINCIPALES NORMAS DE CONDUCTA

Las filiales no italianas considerarán la posibilidad de aplicar las medidas técnicas, físicas y organizativas oportunas para evitar y, todos los Destinatarios están obligados a, no incurrir, por ejemplo, en:

a) uso inadecuado de las credenciales personales para acceder a dispositivos, sistemas o infraestructuras de Tecnologías de la Información y Tecnología Operativa;
b) permitir el acceso ilícito de Terceros a dichos sistemas o infraestructuras;
c) el intercambio y divulgación de información empresarial y data no autorizado fuera de la empresa;
d) el acceso, extracción y modificación no autorizados de información y datos;
e) el uso de dispositivos personales o no autorizados para transmitir o almacenar información o datos de la empresa;
f) Entregar a otras personas los dispositivos proporcionados por la empresa;
g) la manipulación o alteración de los parámetros de configuración de los dispositivos o infraestructuras de la empresa. estructuras);
h) la manipulación de los sistemas de la empresa, el robo o destrucción de archivos, datos y programas;
i) el acceso a los sistemas de información corporativos sin la debida autorización;
j) envío de comunicaciones no solicitadas (spam);
k) conexión de dispositivos externos (ordenador personal, periféricos, discos duros externos, etc.) a los sistemas o infraestructuras de la empresa e instalación de programas informáticos y bases de datos sin autorización previa;
l) la instalación de software dañino (por ejemplo, gusanos y virus) en sistemas o infraestructuras de Tecnologías de la Información y Tecnología Operativa;
m) el uso de software y/o hardware no autorizado que pueda utilizarse para evaluar o comprometer la seguridad de los dispositivos, sistemas e infraestructuras de la empresa (por ejemplo, sistemas para identificar las credenciales, descifrar archivos cifrados, etc.).

Las filiales no italianas, con objeto de identificar una conducta poco habitual, la vulnerabilidad y deficiencia potencial en los sistemas empresariales y dispositivos, garantizarán una supervisión periódica de las actividades efectuadas por el personal de la NIS en el sistema informático de la empresa, en conformidad con la legislación local vigente.

Asimismo, la NIS recordará periódicamente a los Destinatarios Corporativos el uso correcto de los dispositivos, sistemas e infraestructuras de la empresa de las que disponen, incluso impartiendo sesiones específicas de capacitación si fuera necesario.

J. DELITOS CONTRA LOS DERECHOS DE AUTOR

La infracción de los Derechos de Autor en el entorno corporativo pueden manifestarse a través del uso no autorizado, reproducción, distribución o adaptación de obras protegidas por la legislación

de propiedad intelectual, tales como software, bases de datos, vídeos, imágenes, obras literarias y musicales.

A los efectos del EGCP, los delitos contra los derechos de autor comprenden principalmente aquellas conductas que pueden producirse con mayor probabilidad en el contexto de la gestión empresarial, como el uso ilícito de bases de datos o software, la reproducción no autorizada o la distribución de materiales protegidos, entre otros.

Este tipo de Delito puede darse por varias razones, que incluyen, pero no se limitan a lo siguiente:

a) Desconocimiento: los empleados pueden infringir derechos de autor de forma involuntaria debido a una formación insuficiente sobre la normativa aplicables y las políticas internas de la empresa;
b) Presión competitiva: en mercados altamente competitivos, los NIS podrían incurrir en el uso no autorizado de obras protegidas por derechos de autor con el fin de reducir costes de desarrollo y obtener ventajas comerciales.

Mala fe: empleados que, de forma deliberada, infringen derechos de autor con el objetivo de perjudicar a un competidor de las NIS. Para más información, consúltense los ejemplos que figuran en el Anexo 1.

ÁREAS DE SUPERVISIÓN

Con respecto a los tipos de Delitos, habrá que supervisar las áreas siguientes:

- uso o divulgación no autorizados de obras protegidas por derechos de autor, materiales de investigación o contenido de propiedad de terceros;
- uso de imágenes, vídeos o música con derechos de autor en campañas promocionales sin la debida autorización;
- uso no autorizado de software, piratería digital o extracción no autorizada de datos de dominios privados y bases de datos protegidas;
- infracciones derivadas de procesos de externalización, acuerdos de empresas conjuntas o deficiente supervisión de contratos de licencia, derechos de distribución de contenidos o gestión de activos digitales en el marco de acuerdos comerciales.

PRINCIPALES NORMAS DE CONDUCTA

Además de las principales normas de conducta establecidas en el apartado 9.2 sección I) anteriormente citado, las Filiales No italianas considerarán la posibilidad de adoptar las medidas técnicas, físicas y organizativas oportunas para evitar:

1. todo uso ilegal o divulgación pública, a través de redes informáticas o a través de conexiones de cualquier tipo, de obras originales protegidas o partes de las mismas;
2. el uso, la distribución, la extracción, la venta o el alquiler del contenido de bases de datos infringiendo los derechos exclusivos de ejecución y autorización del titular del copyright;
3. la descarga ilegal de cualquier software sin rellenar la documentación contractual oportuna;
4. la descarga de software peer-to-peer o cualquier otro software que no esté relacionado directamente con la actividad de la empresa.

Si la NIS ha celebrado un contrato con contratistas externos para la realización de actividades que se vean afectadas potencialmente por el riesgo de infringir los derechos de autor, dicho contrato habrá de contener disposiciones que requieran el cumplimiento de la legislación y la normativa vigentes.

Dichas medidas deberán cumplir con los siguientes pilares:

- respeto por los derechos de autor de terceros: obtener las autorizaciones necesarias antes de utilizar materiales protegidos, incluidos imágenes, videos, software y contenidos escritos;
- cumplimiento de políticas internas y formación continua: respetar las políticas internas relativas al uso, licenciamiento y protección de derechos de autor, difundirlas dentro de la organización y promover programas de formación actualizados conforme a la evolución normativa;
- supervisión interna y reporte de infracciones: fomentar una cultura de vigilancia interna y alentar a los empleados a reportar cualquier sospecha de infracción de derechos de autor o uso no autorizado de contenidos protegidos.

Asimismo, se deberá mantener una actitud proactiva en el respeto de todas las formas de propiedad intelectual, incluidas las marcas registradas, patentes y secretos comerciales. Esto implica.

- cumplir con las políticas internas destinadas a proteger los activos intangibles;
- fomentar una cultura organizacional basada en el cumplimiento normativo;
- realizar un seguimiento continuo de la evolución de la normativa en materia de propiedad intelectual, con el fin de adaptar las prácticas empresariales en consecuencia.

K. DELITOS TRIBUTARIOS

Los delitos tributarios comprenden conductas realizadas por el contribuyente que infringen disposiciones a proteger el interés de la administración fiscal en el ejercicio de sus funciones de evaluación, control y recaudación de impuestos.

Desde el punto de vista penal, los delitos fiscales se clasifican principalmente en tres categorías: declarativos, falsedad documental y relacionados con la evasión de impuestos:

- Los delitos declarativos incluyen: i) La presentación de declaraciones fraudulentas mediante el uso de facturas u otros documentos relativos a operaciones inexistentes; ii) Declaraciones fraudulentas mediante otros artificios, como operaciones simuladas (objetiva o subjetivamente) o el uso de documentación falsa distinta de la mencionada anteriormente; iii) Cualquier otra forma de engaño que pueda inducir a error a la administración tributaria;
- los delitos de falsedad documental consisten en la emisión de facturas u otros documentos por operaciones inexistentes, con el fin de facilitar la evasión fiscal;
- los delitos relacionados con la evasión de impuestos se refieren al incumplimiento de las obligaciones tributarias que correspondan.

Tanto los delitos declarativos como los documentales se consideran delitos de intención específica, es decir, requieren que el elemento subjetivo del delito esté orientado a la evasión del impuesto sobre la renta o del impuesto al valor añadido.

Asimismo, puede configurarse como delito fiscal el incumplimiento de los requisitos establecidos para acceder a incentivos o beneficios fiscales concedidos conforme a la legislación vigente.

ÁREAS DE SUPERVISIÓN

En relación con este tipo de delitos, deben supervisarse especialmente las siguientes áreas:

(i) gestión tributaria (incluida la preparación de declaraciones fiscales y el cumplimiento de obligaciones conexas);

(ii) elaboración, conservación y archivo de registros contables y demás documentos con relevancia fiscal;

(iii) facturación corporativa;

(iv) contabilidad y facturación entre empresas del Grupo;

(v) cesión de activos y operaciones societarias extraordinarias;

(vi) gestión de las relaciones con las autoridades fiscales;

(vii) gestión de compensaciones fiscales.

PRINCIPALES NORMAS DE CONDUCTA

Con el objetivo de garantizar una fiscalidad justa, responsable y transparente, los NIS se comprometen a actuar con integridad y honestidad, adoptando un enfoque plenamente orientado al cumplimiento de la normativa fiscal aplicable en los países en los que operan. Asimismo, se comprometen a interpretar dicha normativa de manera responsable, con el fin de mitigar el riesgo fiscal y atender adecuadamente los intereses de todas las partes interesadas.

Para aplicar estos estándares de comportamiento, las NIS deben:

a. garantizar una conducta íntegra y transparente, en cumplimiento con la legislación y reglamentación, así como de los procedimientos internos, en todas las actividades relacionadas con la gestión contable, la facturación, el mantenimiento de registros fiscales y la gestión tributaria (incluida la preparación de declaraciones y el cumplimiento de obligaciones conexas);

b. verificar la fiabilidad de los formularios de declaración y pago del impuesto sobre la renta y del impuesto sobre el valor añadido (IVA), contrastándolos con los registros contables, así como la exactitud de los datos consignados;

c. comprobar la corrección de los cálculos relativos a impuestos directos e indirectos;

d. asegurar la implementación oportuna de novedades legislativas en materia fiscal y, en consecuencia, actualizar los procedimientos y políticas internas;

e. verificar que los importes correspondientes al impuesto sobre la renta, al IVA y a las retenciones en origen certificadas por la empresa como agente de retención hayan sido correctamente calculados y pagados;

f. confirmar que los hechos económicos y financieros con relevancia fiscal se correspondan con eventos empresariales reales y debidamente documentados;

g. garantizar el registro contable completo, preciso y oportuno de facturas y demás documentos relevantes para fines fiscales;

h. asegurar la conservación de registros y documentos obligatorios mediante medios digitales que garanticen su disponibilidad e integridad;

i. verificar la integridad y exactitud de los datos consignados en las facturas, conforme a lo acordado contractualmente con proveedores o clientes, y en relación con los servicios efectivamente prestados;

j. asegurar la máxima integridad, transparencia y corrección sustantiva y procedimental en las transacciones con otras empresas del Grupo, garantizando que los servicios interempresariales estén debidamente regulados por contrato y se presten en condiciones de mercado;

k. definir criterios para la, determinación de precios de transferencia, en conformidad con la normativa aplicable;

l. establecer funciones, deberes y responsabilidades claras en relación con la verificación del cumplimiento de los criterios adoptados para los precios de transferencia;

m. garantizar la participación de las funciones fiscales pertinentes en la evaluación de impactos tributarios y en el cumplimiento normativo en el contexto de operaciones societarias extraordinarias;

n. verificar el cumplimiento de los procedimientos relativos a la cesión y eliminación de activos, asegurando su adecuado tratamiento fiscal;

o. promover la transparencia, equidad y cooperación en las relaciones con las autoridades fiscales, incluso durante procesos de fiscalización. Asimismo, fomentar la adhesión a regímenes de cumplimiento cooperativo para aquellas entidades que cumplan con los requisitos normativos locales, con el objetivo de fortalecer las relaciones institucionales;

p. verificar el cumplimiento de los requisitos normativos aplicables a la compensación de impuestos directos e indirectos, así como la veracidad y exactitud de las certificaciones que respaldan los créditos fiscales.

10.3 DISPOSICIONES FINALES

Para garantizar el cumplimiento de las disposiciones legales mencionadas, ENEL ha establecido un sistema de políticas y procedimientos internos que asigna de manera clara funciones y responsabilidades específicas dentro del grupo.

ANEXO 1 EJEMPLOS DE COMPORTAMIENTO ILÍCITO EN LAS ABM

A. DELITOS DE SOBORNO/CORRUPCIÓN

Alguien de la NIS:

- hace un obsequio a un funcionario público para obtener la adjudicación de una licitación;
- ofrece dinero a un funcionario durante una inspección en una planta para persuadirle de que "haga la vista gorda" con algunas irregularidades;
- promete contratar a un empleado de la empresa rival a cambio de obtener acceso a documentos secretos de dicho rival;
- ofrece dinero a un testigo para persuadirle de que haga una declaración falsa en un juicio en el que está involucrada la NIS.

B. OTROS DELITOS CONTRA LA ADMINISTRACIÓN PÚBLICA

Alguien de la NIS:

- durante el proceso de presentación de documentos o datos para participar en una licitación, facilita información falsa a un Organismo del Gobierno con objeto de garantizar la adjudicación de la misma;
- da una falsa representación de la situación financiera y empresarial de la NIS para obtener financiaciones públicas;

- no cumpliendo con el contrato de subvención, malversa los fondos recibidos de la entidad pública.

C. FRAUDE CONTABLE

Alguien de la NIS:

- omite indicar en los estados financieros pérdidas importantes sufridas por la NIS;
- oculta la creación de fondos secretos sobrestimando el costo de los servicios de asesoramiento recibidos por la NIS.

D. ABUSO DEL MERCADO

Alguien de la NIS (suponiendo que la NIS es una sociedad cotizada con respecto a los dos primeros ejemplos):

- divulga Información Interna a un pariente acerca de una próxima adquisición induciéndole a comprar acciones de la empresa;
- revela información falsa acerca de la situación financiera de la NIS con objeto de influir en el precio de sus acciones;
- difunde información falsa o engañosa acerca de una empresa rival para perjudicar su reputación en el mercado.

E. FINANCIACIÓN DEL TERRORISMO Y DELITOS DE BLANQUEO DE CAPITALES

Alguien de la NIS:

- recibe dinero de (o transfiere dinero a) una empresa ubicada en un paraíso fiscal o cuya cuenta corriente se encuentra en un banco situado en un paraíso fiscal con objeto de ocultar el origen delictuoso de dicho dinero;
- hacer ver que se paga a una empresa por servicios de asesoramiento, transfiere dinero a cuentas corrientes poseídas secretamente por una organización ilegal que financia ataques terroristas;
- utiliza los fondos secretos, cuya creación se ha encubierto manipulando los estados financieros de la empresa, para financiar partidos políticos que están vinculados a organizaciones terroristas.

F. DELITOS CONTRA LOS PARTICULARES

Alguien de la NIS:

- aprovechando la situación de un trabajador en estado de necesidad físico o psicológico, lo/a explota;
- obliga a trabajar a las personas, utilizando amenazas, abuso de autoridad o violencia;
- obliga a las personas inmigrantes a trabajar bajo amenaza de denunciarlas a las autoridades de inmigración.

G. DELITOS CONTRA LA SEGURIDAD Y LA SALUD

Alguien de la NIS, que actúa sin cumplir con la legislación vigente en materia de seguridad y salud:

- omite proporcionar Equipo de Protección Personal (EPP) de acuerdo a la evaluación de riesgos;
- omite implementar medidas de emergencia en el lugar de trabajo (organizativas, de capacitación y medidas técnicas) ;
- no proporciona el equipo de seguridad necesario y maquinaria a los trabajadores;

- permite que los empleados trabajen con máquinas sin instruirles sobre cómo utilizarlas en condiciones de seguridad;
- no somete periódicamente a los trabajadores a una visita médica especializada de conformidad con la ley para controlar su salud, evaluando si la labor que desempeñan les es perjudicial.

H. DELITOS CONTRA EL MEDIO AMBIENTE

Alguien de la NIS:

- se abstiene de considerar el impacto sobre la biodiversidad cuando se planea una expansión de la planta, perjudica el hábitat de especies animales protegidas, poniendo en peligro su existencia;
- administra una central térmica sin considerar los umbrales legales para las emisiones de gases, contaminando el área de los alrededores;
- no efectúa correctamente la eliminación de residuos de la empresa y, por el contrario, organiza un emplazamiento ilícito de eliminación de residuos;
- provoca contaminación del agua por uso inadecuado del recurso o por uso no adecuado de los sistemas de tratamiento del agua;
- se abstiene de gestionar adecuadamente las emisiones atmosféricas, al no adoptar sistemas adecuados de prevención y control, provocando contaminación atmosférica.

I. DELITOS CIBERNÉTICOS Y DELITOS CONTRA LOS DERECHOS DE AUTOR

Dentro del ámbito de las NIS, se considerará la comisión de delitos cibernéticos o relacionados con la propiedad intelectual cuando una persona:

- instala un software copiado ilegalmente en los dispositivos de trabajo;
- entra en el sistema informático de una empresa rival usando técnicas de piratería informática maliciosa para robar información y secretos comerciales y distribuir malware para dañarlo.

K. DELITOS TRIBUTARIOS

Dentro del ámbito de los NIS, se considerará la comisión de delitos fiscales cuando una persona:

-con el fin de evadir impuestos sobre la renta o el impuesto al valor añadido (IVA):

• utilice facturas u otros documentos relativos a operaciones inexistentes, o declare en su declaración fiscal elementos pasivos ficticios;

• oculte o destruya documentación que deba conservarse legalmente, impidiendo así la reconstrucción de los ingresos o del volumen de negocios;

- emita o expida facturas u otros documentos por operaciones inexistentes, con el propósito de permitir a terceros la evasión de impuestos sobre la renta o el IVA.

- no pague los impuestos debidos, utilizando para ello créditos fiscales inexistentes o indebidos como mecanismo de compensación.