PROGRAMA DE CUMPLIMIENTO GLOBAL SOBRE RESPONSABILIDAD PENAL CORPORATIVA

Mayo 2025

INTRODUCCIÓN

Enel S.p.A. ("**ENEL**") es la sociedad matriz de un grupo multinacional ("**Grupo**") que opera en un sector empresarial complejo y altamente regulado, y en diferentes entornos económicos, políticos, sociales y culturales. En este contexto, la integridad se concibe como un valor fundamental para la realización de la actividad empresarial. Requiere que todo el personal del Grupo actúe con lealtad, integridad, transparencia y estricto cumplimiento de las leyes y normativas nacionales e internacionales , así como de los estándares y directrices aplicables.

El "**Programa de Cumplimiento Global de Enel**" o "**EGCP**" está concebido como una herramienta para reforzar el compromiso de ENEL con los más altos estándares éticos, legales y profesionales, con el objetivo de mejorar y preservar la reputación del Grupo. Para ello, establece una serie de medidas preventivas orientadas a evitar la responsabilidad penal corporativa.

En los últimos años, ha aumentado de forma constante el número de países que en sus legislaciones han tipificado regimenes de responsabilidad penal corporativa, lo que viene a permitir que los tribunales de justicia puedan llegar a sancionar a las entidades corporativas por conductas delictivas de sus representantes, empleados o terceros que actúen en su nombre.

En determinadas jurisdicciones, las leyes y reglamentos aplicables fomentan que las empresas adopten estructuras de gobierno corporativo y sistemas de prevención de riesgos, con el fin de evitar que sus directivos, empleados, consultores o contratistas externos incurran en conductas delictivas. Asimismo, dichas normativas prevén la posibilidad de eximir o atenuar las sanciones aplicables cuando por las compañías se hayan implementado medidas preventivas adecuadas para prevenir la comisión de acciones que puedan derivar en responsabilidad penal de las personas jurídicas.

El EGCP, inspirado en los reglamentos internacionales más relevantes, tiene como objetivo definir **estándares generales** de conducta aplicables a empleados, personal directivo y demás miembros de los órganos de gestión y control ("**Destinatarios Corporativos**"), así como a consultores u otros contratistas y, en general, a terceros ("**Terceros**" u "**Otros Destinatarios**") (en lo sucesivo, los Destinatarios Corporativos y los Otros Destinatarios se denominarán conjuntamente los "**Destinatarios**") de las sociedades del Grupo de nacionalidad no italiana (en adelante "**NIS**") debiéndose respetar en todo momento la legislación local e idiosincracia cultural, social y económica de los diferentes países en los que operan los NIS que en caso de contradicción con el EGCP, siempre prevalecerán.

1 MISIÓN

El EGCP representa una oportunidad para reforzar la prevención proactiva de la responsabilidad penal corporativa mediante el fortalecimiento de la gobernanza y del sistema de control interno. stando diseñado para fomentar el desarrollo de conductas adecuadas y conformes a la a la legalidad vigentes y aplicable a todo el Grupo.

El EGCP establece los estándares clave de conducta esperados de todos los Destinatarios Corporativos y, cuando se especifique, de los demás Destinatarios, con el fin de:

i. proporcionar a las NIS un conjunto uniforme de normas orientadas a prevenir la responsabilidad penal corporativa en sus respectivos países;
ii. integrar cualquier programa de cumplimiento local adoptado por una NIS conforme a la legislación aplicable en materia de responsabilidad penal corporativa.

Las normas contenidas en el EGCP están alineadas con:

i. las disposiciones contenidas en el Código Ético, que recoge los principios éticos del Grupo ENEL y que todos los Destinatarios están obligados a respetar;
ii. las disposiciones del Plan de Tolerancia Cero contra la Corrupción, del Grupo ENEL;
iii. las normas en materia de gobernanza corporativa adoptadas por lss NIS, de conformidad con las legislación locales aplicables en cada caso y las mejores prácticas internacionales;
iv. los sistemas de control interno implementados por cada una de las NIS.
v. Las disposiciones contenidas en cualquier programa de cumplimiento local adoptado por la NIS para dar cumplimiento a sus respectivas legislaciones locales sobre responsabilidad penal corporativa, así como a las y en cualesquiera directrices, políticas o documentos organizativos internos relacionados.

2 ESTRUCTURA

El EGCP establece:

a. los procesos de implementación del EGCP adopción por parte de los NIS, así como los processo correspondiente de actualización del mismo que corresponda;
b. los mecanismos de difusión del EGCP dirigidos a los Destinatarios, junto con las actividades de formación asociadas;
c. el sistema disciplinario aplicable en caso de incumplimiento de cualquiera de las disposiciones contenidas en el EGCP;
d. los estándares generales de control;
e. las áreas de actividad sujetas a supervisión en relación con determinados tipos de comportamientos ilícitos (las "**Áreas a Supervisar**" o "**ABM**"), enumeradas en la Sección 8ª. cuya prevención constituye una prioridad para ENEL en su compromiso de dirigir sus operaciones con honestidad e integridad (los "**Delitos**");
f. los estándares clave de comportamiento aplicables a las "Áreas a Supervisar".

El EGCP se complementa con el **Anexo 1**, titulado"Ejemplos de comportamientos ilícitos cometidos en las ABM".

3 ADOPCIÓN, APLICACIÓN, RESPONSABILIDAD Y MODIFICACIONES POSTERIORES

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 de administración que corresponsa de cada NIS, en el marco de su autonomía e independencia:

i. adoptará las medidas más adecuadas para la implementación y la supervisión del EGCP, teniendo en cuenta el tamaño, la complejidad de las actividades realizadas, el sistema de control interno y el perfil de riesgo específico relativo del NIS y su marco regulatorio;
ii. será responsable de la correcta aplicación de las "Áreas a Supervisar" y los "Estándares Clave de Comportamiento", según lo dispuesto por la sección 10.2 del EGCP, así como de los controles establecidos en el Programa de Cumplimiento Global de Enel.

Los NIS aplicarán el EGCP de conformidad con la legislación local vigente, la naturaleza de las actividades que desarrollan y las características específicas de su estructura organizativa.

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 los 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 DIFUSIÓN DEL EGCP Y ACTIVIDADES DE FORMACIÓN

El EGCP estará disponible para su consulta y descarga a través de la Intranet del Grupo ENEL.

A nivel local , se desarrollarán actividades de formación específicas a todo el personal, incluyendo herramientas de formación digitales , con el objetivo de garantizar una adecuada difusión y comprensión del EGCP, las Áreas a Supervisar (ABM), así como de los comportamientos pertinentes para prevenir la comisión de los Delitos. Estas actividades de formación podrán integrarse en los programas de formación que cada NIS adopte en el marco del cumplimiento del derecho penal local y de sus respectivos programas de cumplimiento normativo.

5 COMUNICACIÓN A TERCEROS

Los Terceros serán informados sobre los principios y contenidos del EGCP, adhiriéndose al mismo mediante la suscripción de la documentación correspondiente.

6 INFORMES POR PARTE DE DESTINATARIOS CORPORATIVOS O DE 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 utilizandolos canales mencionados anteriormente.

In accordance with what is already defined in the current document, ENEL handles reports received within the timeframe provided for by the regulations in force, prohibits any form of retaliation and ensures that no act of retaliation is carried out by reason of a report.

ENEL aplicará sanciones disciplinarias en los siguientes casos:

(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 los NIS aplicarán las medidas disciplinarias correspondientes en caso de incumplimiento de cualquiera de losestándares de comportamiento establecidos en el EGCP, conforme al sistema disciplinario vigente; a la normativa aplicable y a los programas de cumplimiento locales. Todo ello sin perjuicio de las garantías legales reconocidas a los empleados por la legislación local, tales como el derecho a la defensa y el principio del debido proceso.

Las medidas disciplinarias serán aplicables independientemente del resultado de cualquier procedimiento penal que pueda ser iniciado por la autoridad judicial competente.

Asimismo, la documentación contractual deberá prever sanciones adecuadas en caso de incumplimiento del EGCP por parte de Terceros, incluyendo – aunque no limitándose a – la posibilidad de resolución contractual, de conformidad con la legislación aplicable.

8 DELITOS

El EGCP se aplica a los siguientes tipos de Delitos (en adelante, "los Delitos", tal como se describen a continuación):

A. Delitos de Soborno
B. Otros Delitos contra Entidades Públicas
C. Fraude Contable
D. Abuso del Mercado
E. Financiación del Terrorismo y Blanqueo de Capitales
F. Delitos contra Particulares
G. Delitos contra la Salud y Seguridad
H. Delitos Medioambientales
I. Delitos Cibernéticos
J. Delitos contra la Propiedad Intelectual
K. Delitos Fiscales

En la sección 10.2 del EGCP se identifican los ámbitos de actividad que deben ser objeto de supervisión por parte de los NIS, así como los estándares clave de comportamiento aplicables.

La lista incluida en el apartado 10.2 no exime a las Subsidiarias No Italianas de llevar a cabo su propia evaluación del riesgo y definición de estándares clave de comportamiento adicionales, cuando así se considere apropiado.

Por consiguiente, las NIS podran identificar:

i. las actividades empresariales que puedan entrañar un riesgo específico de comisión de delitos, mediante un análisis de los procesos operativos y de las posibles modalidades de comisión asociadas a los distintos tipos de delitos;
ii. estándares adicionales de comportamiento que deben cumplir todos los Destinatarios Corporativos y, cuando así se especifique expresamente, por otros Destinatarios para: abstenerse de cualquier conducta que pueda dar lugar a la comisión de alguno de los Delitos descritos anteriormente; y abstenerse de cualquier conducta que, sin constituir directamente uno de dichos delitos, pudiera razonablemente derivar en su comisión.

9 SISTEMA DE CONTROL DEL EGCP

El EGCP establece dos niveles principales de control en relación con las Áreas a Supervisar:

- estándares generales de control;
- estándares clave de comportamiento, específicos a cada ABM.

10.1 ESTÁNDARES GENERALES DE CONTROL

Las NIS deberán cumplir con los siguientes estándares generales de control:

1) **separación de funciones**: la asignación de funciones, tareas y responsabilidades dentro de un NIS se realiza de conformidad con la separación de funciones según la cual ninguna persona puede realizar de forma autónoma la totalidad de un proceso (es decir, de conformidad con este principio, ninguna persona puede encargarse autónomamente de realizar una acción, autorizarla y posteriormente verificarla); también se puede conceder una separación de funciones adecuada utilizando sistemas informáticos que permitan realizar determinadas transacciones únicamente a personas identificadas y autorizadas;
2) **delegación de firma y autorización**: debe haber normas formales sobre el ejercicio de poderes internos y delegaciones de firma. Las delegaciones de firma serán coherentes con las responsabilidades organizativas y de gestión asignadas a cada titular del poder en los NIS;
3) **transparencia y trazabilidad de los procesos**: siempre debe garantizarse la identificación y trazabilidad de las fuentes, la información y los controles realizados para respaldar la toma de decisiones y la ejecución de acciones por parte de las NIS, así como la gestión de los recursos financieros. Asimismo, deberá garantizarse el almacenamiento adecuado de los datos e información relevante, ya sea mediante sistemas de información electrónicos y/o soportes en papel;
4) **gestión adecuada de las relaciones con Terceros**:
   (i) antes de formalizar cualquier relación con un Tercero, deberá realizarse una evaluación de debida diligencia adecuada respeto a los requisitos de honorabilidad.. El alcance de dicha evaluación será proporcional al riesgo real o percibido de que el posible socio, consultor, o proveedor no cumpla con los estándares requeridos. Esta evaluación podrá incluir, entre otros, consultas a contactos empresariales, cámaras de comercio locales, asociaciones empresariales, búsquedas en Internet y revisión de referencias empresariales y estados financieros:
      - se considerarán señales de alerta las siguientes circunstancias:el Tercero está constituido en un país con altos niveles de corrupción según índices internacionales, como el Índice de Percepción de la Corrupción de Transparencia Internacional, o en un país clasificado como "país no cooperador" según la lista negra del GAFI u otra lista internacional relacionadas con la lucha contra el blanqueo de capitales y la financiación del terrorismo;
      - el Tercero ha sido suspendido o excluido de participar en licitaciones o contratos

con entidades estatales, organismos públicos o agencias gubernamentales debido a investigaciones de cumplimiento realizadas por las autoridades públicas;
- el Tercero ha sido objeto de procedimientos penales;
- el Tercero se niega a adherirse al programa de cumplimiento der la empresa y carece de un código de conducta o normativa equivalente en materia ética;
- el Tercero mantiene vínculos familiares con funcionarios clave de agencias gubernamentales nacionales o extranjeras;
- un funcionario público figura como propietario, directivo o accionista principal del Tercero;
- la dirección de la actividad empresarial del Tercero es una oficina virtual;
- el Tercero tiene un beneficiario final no revelado;

(ii) comprobaciones adicionales, en caso de que, durante la fase de debida diligencia, surjan señales de alerta,

(iii) supervisión continua durante toda la relación contractual para garantizar que la contraparte siga cumpliendo los requisitos establecidos por los NIS, y

(iv) medidas correctivas, si durante la relación contractual eltercero deja de cumplir con los requisitos establecidos o surgen nuevas señales de alerta, deberán adoptarse medidas adecuadas. Entre las situaciones que podrían activar estas medidas se incluyen:
- el Tercero insiste en interactuar directamente con funcionarios públicos, excluyendo a la empresa;
- el Tercero solicita pagos anticipados inusuales;
- el Terceropresenta facturas inexactas o por servicios no prestados;
- el Tercero solicita que los pagos se realicen en efectivo, o en instrumento al portador;
- el Tercero solicita que los pagos se realicen fuera de su país de origen, en jurisdicciones no relacionadas con la transacción;
- el Tercero solicita que el pago se realice a un intermediario o a otra entidad o solicita que se realicen pagos a dos o más cuentas bancarias;
- el Tercero solicita fondos para que sean donados a una institución o fundación sin ánimo de lucro.

10.2 ÁREAS A SUPERVISAR Y ESTÁNDARES CLAVE DE COMPORTAMIENTO

A. Delitos de soborno

Este tipo de Delitos se refieren a la oferta, entrega, solicitud o recepción de dinero (o cualquier otro tipo de beneficio, ganancia o ventaja) con el propósito o con la intención de influir en el destinatario (que puede ser una persona perteneciente a una empresa privada o un funcionario público) de manera que actúe en favor de quien proporciona el soborno.

A menudo, los sobornos consisten en regalos o pagos de dinero (otras formas de sobornos pueden incluir diversos bienes, privilegios, entretenimientos y favores) a cambio de un trato favorable. Dichos tratos favorables, que desencadenan el soborno, pueden consistir, por ejemplo, en:

- la contratación del sobornador en un contrato pertinente (ya sea con una administración pública o una empresa privada);o la adjudicación de una licitación pública;
- una declaración falsa, favorable al sobornador, por un testigo en un proceso judicial;
- la elaboración de un informe indulgente por parte de un funcionario público.

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

ÁREAS A SUPERVISAR

En relación con este tipo de Delitos, es necesario supervisar las siguientes áreas de actividad:

(i) negociación, ejecución y gestión de contratos relevantes con cualquier Parte (Autoridades Públicas, empresas, asociaciones, fundaciones, entre otras);
(ii) participación en licitaciones, tantopúblicas como privadas;
(iii) gestión de las relaciones no contractuales con organizaciones comunitarias y Autoridades Públicas (por ejemplo, en relación con los requisitos de salud, seguridad, medio ambiente, gestión del personal y cumplimiento tributario);
(iv) gestión de controversias, incluyendolitigios, arbitraje, procedimientos extrajudiciales;
(v) selección de socios, intermediarios y consultores, así como la negociación, ejecución y gestión de los contratos correspondientes;
(vi) gestión de efectivo y recursos financieros;
(vii) gestión de iniciativas sin ánimo de lucro;

(viii) gestión de regalos, entretenimiento y gastos de hospitalidad;
(ix) reembolso de gastos incurridos por los empleados;
(x) contratación de personal;
(xi) definición de incentivos de compensación, como los planes de objetivos por resultados (por ejemplo, MBO) dirigidos a los ejecutivos de los NIS.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Al realizar negocios con empresas privadas, así como con administraciones públicas y gobiernos internacionales, nacionales, estatales y locales (en adelante, las "**Autoridades Públicas**"), los NIS y sus representantes se comprometen a actuar con integridad y honestidad y deben cumplir con todas las leyes y normativas aplicables. Asimismo, los Destinatarios Corporativos y Terceros (conforme a los términos contractuales específicos), tienen expresamente prohibido:

a) ofrecer dinero u otorgar cualquier otro tipo de ventaja de cualquier tipo (incluidas promesas de empleo entre otras) a representantes de Autoridades Públicas, así como a las personas físicas pertenecientes a una empresa privada -o a sus familiares (en adelante, los "**Particulares**")- con quienes los NIS mantengan o pretendan establecer una relación comercial, o en el marco de cualquier otra interacción, como solicitudes de fondos públicos, tramitación de autorizaciones o licencias, entre otros;
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 documentadopara permitir su inspección conforme a los controles internos establecidos;
c) utilizar efectivo como medio de pago, salvo en los casos permitidos por la normativa vigente (por ejemplo, dinero para gastos menores);
d) incurrir en cualquier gasto de promoción o patrocinio, a menos que los gastos hayan sido aprobados, previamente, por escrito por el área competente;
e) efectuar cualquier contribución a instituciones sin fines de lucro, proyectos comunitarios o asociaciones profesionales, a menos que los gastos hayan sido aprobados, previamente, por escrito por el área competente;

f) asignar servicios a Terceros sin una justificación adecuada en relación con las necesidades de los NIS;

g) realizar pagos a Terceros que no estén suficientemente justificados con respecto al tipo de servicio prestado y de las prácticas locales vigentes.

Las subsidiarias no Italianas evaluarán la conveniencia de adoptar medidas organizativas adecuadas para prevenir que cualquier Destinatario incurra en las conductas descritas anteriormente. Además, los NIS considerarán la adopción de procedimientos específicos destinados a garantizar que:

h) exista documentación adecuada que respalde toda la relación material establecida con Autoridades Públicas (por ejemplo, procedimientos administrativos para la obtención de autorizaciones, licencias o actos similares, empresas conjuntas con entidades públicas, solicitudes de autorizaciones públicas) y cualquier relación comercial relevante;

i) las relaciones con Autoridades Públicas, cuando están en juego cuestiones relativas a los intereses de los NIS, sean gestionadas por al menos dos personas autorizadas, a fin de asegurar transparencia y control;

j) los procedimientos de contratación se realicen exclusivamente sobre la base de una necesidad empresarial real y demostrable, que el proceso de selección involucre al menos dos áreas distintas y se base en criterios de objetividad, competencia y profesionalismo, con el fin de evitar el favoritismo, el nepotismo y los conflicto de interés;

k) los planes de incentivos dirigidos a la gestión se diseñen de manera que los objetivos contingentes no fomenten conductas abusivas, sino que se enfoquen enresultados, específicos, medibles y alcanzables de un plazo determinado;

l) en relación con la planificación de proyectos, se establezcan plazos realistas, acordes con la naturaleza y complejidad de las actividades previstas;

m) en relación con el reembolso de los gastos, debe presentarse al departamento de contabilidad correspondiente, antes del pago, la documentación pertinente, incluidos los recibos originales que respalden el gasto realizado. Además, el pago o gasto correspondiente (o el recibo del mismo) se describa con precisión y se refleje en los registros contables pertinentes de los NIS.

B. Otros delitos contra autoridades públicas

Este tipo de delitos se refiere, principalmente, al fraude contra entidades públicas, y se produce cuando una empresa emplea artificios o esquemas ilícitos con el fin de defraudar a una entidad

pública u obtener una ventaja económica mediante declaraciones, promesas o pretensiones falsas o fraudulentas.

A menudo, este tipo de delitos están relacionados con financiación pública y subvenciones y ocurren cuando una empresa solicita financiación pública o subvenciones sin tener derecho a ellos, o hace un uso indebido de los mismos, distinto al previsto en el acuerdo de subvención.

Este tipo de delito puede producirse por múltiples motivaciones, que, normalmente, están relacionadas con la obtención de cualquier ventaja económica indebida.

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

ÁREAS A SUPERVISAR

En relación con estos delitos, es necesario prestar especial atención a las siguientes áreas:

(i) participación en licitaciones públicas y en procedimientos administrativos de carácter público en general;
(ii) gestión de relaciones con Autoridades Públicas, especialmente en lo relativo a requisitos de salud, seguridad, medio ambiente, gestión de personal y cumplimiento tributario;
(iii) solicitud de financiación pública, subvenciones, subsidios o garantías emitidas por Autoridades Públicas;
(iv) gestión de los fondos públicos recibidos, incluyendo subvenciones, subsidios o garantías obtenidas.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Además de los estándares establecidos en el apartado 10.2. A), los Destinatarios Corporativos y Terceros (conforme a los términos contractuales específicos), se abstendrán de incurrir en las siguientes conductas:

a) presentar documentos falsos o alterados, total o parcialmente, durante la participación en ofertas de licitación pública;
b) inducir a error a las Autoridades Públicas, por cualquier medio, durante la evaluación de solicitudes de autorizaciones, licencias, habilitaciones, concesiones u otros actos administrativos;

c) omitir información relevante en poder de los NIS que pueda influir en las decisiones de las Autoridades Públicas, en relación con las circunstancias descritas en el apartado a) y b) descritos anteriormente, a favor de los NSI;

d) toda conducta encaminada a obtener de una Autoridad Pública cualquier tipo de subvención, financiación, préstamos u otros desembolsos públicos, mediante declaraciones o documentos alterados o falsificados, la omisión de información pertinente o, mediante cualquier otro artificio o fraude, con la intención de inducir a error a la entidad pública correspondiente;

e) utilizar dinero recibido de las Autoridades Públicas como fondos, contribuciones o préstamos para fines distintos de aquellos para los que fueron concedidos.

Además, para implementar los estándares de comportamiento descritos anteriormente; las Subsidiarias no Italianas evaluarán la conveniencia de adoptar medidas organizativas apropiadas para garantizar que:

f) todas las declaraciones presentadas ante autoridades públicas, tanto nacionales como internacionales, con el propósito de obtener fondos, subvenciones o préstamos sólo contengan información veraz y estén firmadas por personas debidamente autorizadas y, en caso de obtención de dichos fondos, subvenciones o préstamos, éstos se contabilicen debidamente;

g) se establezcan controles adecuados de separación de funciones, garantizando que las fases de solicitud, gestión y notificación relacionadas con procedimientos públicos para la obtención de fondos, subvenciones o préstamos sean gestionadas por diferentes Destinatarios Corporativos dentro de la organización;

h) las actividades de recopilación y análisis de la información, necesarias para fines de notificación, se realicen con el apoyo de las funciones competentes, asegurando la calidad y veracidad de los datos;

i) la documentación y notificaciones posteriores relacionadas con solicitudes de subsidios, subvenciones o garantías sean aprobadas por niveles jerárquicos adecuados, conforme a los procedimientos internos de control y supervisión.

C. Fraudes contables

El fraude contable es un tipo de delito que consiste, principalmente, en la manipulación intencionada de los estados financieros con el objetivo de presentar una imagen falsa de la situación económica yfinanciera de una empresa ante inversores, acreedores, accionistas y otras partes interesadas.

El fraude contable puede producirse por varias razones, entre las que se incluyen, sin limitarse a:

i. obtener financiación bancaria, mediante la alteración de los estados financieros epara aparentar una solidez económica inexistente;
ii. reportar beneficios irreales u ocultar pérdidas;
iii. omitir información relevante, que pudiera afectar negativamente la valoración o reputación de la empresa;
iv. causar la inflación del precio de la acción;
v. ocultar la creación de fondos destinados a fines ilícitos;
vi. encubrir conductas indebidas, como el robo o malversación cometidos por directivos o empleados;
vii. omitir hechos materiales que puedan inducir a error a cualquier parte interesada, incluyendo autoridades bursátiles, entidades reguladores, acreedore e inversores.

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

ÁREAS A SUPERVISAR

En relación con este tipo de delitos, es necesario supervisar las siguientes áreas:

(i) la elaboración de documentos dirigidos a inversores o al público, incluidos, entre otros, estados financieros e informes financieros periódicos, que contengan información sobre activos, pasivos, ingresos, gastos o flujos de caja de las subsidiarias no italianas, incluso cuando dichos documentos no constituyan informes contables periódicos formales.

(ii) gestión de las relaciones con los auditores externos y órganos de supervisión.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Las Subsidiarias no Italianas evaluarán la conveniencia de aplicar las medidas apropiadas, y se requiere que el personal encargado de la contabilidad, los registros y las cuentas actúe de manera adecuada para garantizar que:

a) los datos y la información utilizados en la preparación de los informes financieros periódicos sean precisos y verificados con diligencia;
b) todas las partidas del balance, cuya determinación y cuantificación impliquen juicios discrecionales sean objetivas y estén debidamente respaldadas por la documentación correspondiente;

c) las transacciones se ejecuten conforme a las autorizaciones generales o específicas otorgadas por la dirección;

d) las facturas y demás documentación pertinente relacionada con las transacciones sean controladas, registradas y archivadas adecuadamente;

e) las transacciones se registren según sea necesario para permitir la elaboración de estados financieros de conformidad con los principios contables aplicables, o generalmente aceptados, o cualquier otro criterio aplicable a dichos estados;

f) el acceso a dichos registros de transacciones sólo se permita conforme a las autorizaciones generales o específicas de la dirección.

Además, para garantizar que se facilite al mercado una información completa y veraz, se impide a las Subsidiarias no Italianas incurrir en cualquier conducta que obstaculice o, en cualquier caso, obstruya la verificación de los auditores externos, ya sea mediante la ocultación de documentación o el uso de otros medios fraudulentos.

Por último, las Subsidiarias no Italianas están obligadas a realizar todas las comunicaciones con cualquier autoridad financiera pública (según lo dispuesto por la legislación local aplicable) de una manera correcta, completa, adecuada y rápida, sin impedirles, en modo alguno, la realización de sus funciones, incluso en el contexto de cualquier inspección (por ejemplo, mediante oposición expresa, negativa injustificada, conducta obstructiva o falta de cooperación).

D. Abuso del mercado

Esta categoría de delitos se refiere principalmente a tres tipos diferentes de conductas: (1) vender o comprar instrumentos financieros utilizando información que no esté disponible públicamente ("Información Privilegiada"), o comunicarla de manera ilegítima a terceros; (2) alterar el mecanismo de fijación de precios de instrumentos financieros mediante la difusión deliberada de información falsa o engañosa con el fin de influir en el precio de dichos instrumentos ; (3) ejecutar órdenes de compra y venta que tengan por objeto o efecto: (i) proporcionar indicaciones falsas o engañosas con respecto a la oferta, demanda o precio de instrumentos financieros, (ii) fijar el precio de mercado de uno o más instrumentos financieros a un nivel anómalo o artificial.

Este tipo de conductas pueden tener lugar para el beneficio de una empresa por múltiples razones, entre ellas, aunque no limitadas a:

- reducir artificialmente el precio de las acciones de una empresa objetivo antes de una adquisición;

- perjudicar la reputación de una empresa competidora;
- alterar el precio de un determinado instrumento financiero en cartera antes de realizar operaciones comerciales relacionadas con el mismo.

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

ÁREAS A SUPERVISAR

En relación con este tipo de delitos, es necesario supervisar las siguientes áreas:

(i) gestión de la información pública: incluye las interacciones con inversores, analistas financieros, periodistas y otros representantes de los medios de comunicación, así como la organización y participación en reuniones de cualquier tipo con dichas personas;
(ii) gestión de la información privilegiada relacionada con las sociedades cotizadas del Grupo y los instrumentos financieros pertinentes. Esto abarca, entre otros aspectos, información sobre nuevos productos, servicios y mercados; datos contables del período; previsiones y objetivos cuantitativos sobre el desempeño empresarial; fusiones/escisiones; y, en particular, nuevos compromisos relevantes como negociaciones y/o acuerdos relacionados con la adquisición y/o venta de activos significativos;
(iii) gestión de la Información Privilegiada vinculada a los derivados de energía, comopor ejemplo, información sobre la indisponibilidad de plantas o instalaciones;
(iv) cualquier tipo de transacción relacionada con instrumentos financieros en cartera.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Cada Destinatario tiene expresamente prohibido:

a) utilizar Información Privilegiada para negociar, directa o indirectamente, instrumentos financieros en aras de obtener ventajas personales o en favor de Terceros o de un NIS o de cualquier otra empresa del Grupo;
b) revelar Información Privilegiada a Terceros, excepto cuando así lo requiera la ley, u otras disposiciones reglamentarias o contratos específicos en los que las contrapartes estén obligadas a utilizar la información sólo para el propósito originalmente previsto y mantener su confidencialidad;
c) recomendar o inducir a una persona, basándose en cierta Información Privilegiada, a realizar cualquier tipo de transacción sobre instrumentos financieros.

Además, cada Destinatario tiene expresamente prohibido:

d) difundir información falsa o engañosa a través de los medios de comunicación (ya sea sobre la propia empresa o sobre cualquier otra empresa), incluyendo Internet, o por cualquier otro medio, sólo para alterar el proceso de acciones, derivados o actividades subyacentes que apoyen la transacción previamente planificado por el sujeto que difunde la información aquí contenida;

e) realizar cualquier transacción sobre un instrumento financiero (por ejemplo, compra o venta) contra las normativas de abuso del mercado.

E. Financiación del terrorismo y delitos de blanqueo de capitales

La financiación del terrorismo entraña la solicitud, recaudación o provisión de fondos con la intención de utilizarlos para apoyar actos u organizaciones terroristas.

El objetivo principal de las personas o entidades involucradas que participan en la financiación del terrorismo es ocultar tanto la financiación como la naturaleza de la actividad financiada.

El blanqueo de capitales es el proceso por el cual se encubre el origen ilícito de los fondos provenientes de actividades delictivas. Este proceso puede manifestarse a través de tres conductas diferentes y alternativas: (i) la conversión o transferencia de fondos, a sabiendas de que son productos del delito, (ii) la ocultación o el encubrimiento de la verdadera naturaleza, origen, ubicación, disposición, movimiento o titularidad de bienes o derechos respecto de ellos, a sabiendas de que esos bienes son producto de un delito; y (iii) la adquisición, posesión o uso de bienes, a sabiendas, en el momento de la recepción, que dichos bienes proceden de una actividad delictiva.

Cuando los productos de un delito son generados por la misma persona que oculta su origen ilícito, dicha conducta se castiga en algunos países como blanqueo de capitales por cuenta propia.

El blanqueo de dinero y la financiación del terrorismo comparten a menudo características transaccionales similares, principalmente relacionadas con el ocultamiento. Los blanqueadores de dinero envían fondos ilícitos por canales legales para ocultar sus orígenes delictivos, mientras que los que financian el terrorismo transfieren fondos que pueden ser de origen legal o ilícito de tal manera que ocultan su origen y uso final, que es el apoyo al terrorismo.

Este tipo de conductas pueden tener lugar en beneficio de una empresa por múltiples razones, incluyendo, pero sin limitarse a:

- obtener productos o cualquier otra ventaja derivada de las actividades ilegales realizadas por organizaciones terroristas que hayan sido financiadas (las otras ventajas pueden consistir en la protección de la actividad empresarial, en países donde dichas organizaciones tengan una influencia significativa);
- encubrir el origen ilegal de los productos del delito.

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

ÁREAS A SUPERVISAR

En relación con este tipo de Delitos, es necesario supervisar las siguientes áreas:

- transacciones financieras o comerciales realizadas con personas físicas, corporaciones, o entidades jurídicas controladas directa o indirectamente por los sujetos anteriormente mencionados, que tengan su residencia o domicilio social en un país que represente una jurisdicción de alto riesgo y no cooperativa (es decir, con deficiencias estratégicas en sus marcos legales y regulatorios para combatir el blanqueo de capitales y la financiación del terrorismo) según la evaluación realizada por las autoridades internacionales competentes, como el Grupo de Acción Financiera Internacional (GAFI).

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Los NIS condenan expresamente el uso de sus recursos para la financiación o ejecución de cualquier actividad encaminada a alcanzar objetivos asociados con la financiación del terrorismo, así como cualquier uso indebido de instrumentos financieros y/u operaciones encaminadas a ocultar el origen de los fondos de la empresa.

De manera más general, los NIS rechazan cualquier posible conducta encaminada, incluso indirectamente, a facilitar delitos como la recepción, el blanqueo y el uso de dinero, bienes o cualquier activo de origen ilícito; en este sentido, los NIS se comprometen a ejecutar todas las medidas preventivas y de control posteriores requeridas para alcanzar ese objetivo, regulando también las relaciones con terceros mediante disposiciones contractuales que requieran la observancia de las leyes aplicables en la materia.

Está expresamente prohibido:

a) utilizar pagos en blanco o en efectivo para cualquier operación de recaudación, pagos, transferencia de fondos, etc;
b) realizar o recibir pagos en cuentas bancarias anónimas o en cuentas bancarias ubicadas en jurisdicciones de alto riesgo;
c) emitir o recibir facturas o expedir documentos en relación con transacciones inexistentes.

Además, para aplicar los estándares de comportamiento anteriormente descritos, los NIS deben:

d) realizar controles analíticos de los flujos de caja;
e) verificar la validez de los pagos, controlando que su beneficiario sea efectivamente la contraparte involucrada en la transacción;
f) realizar controles de procedimiento, en particular en lo que respecta a las posibles transacciones que se produzcan fuera de los procesos normales de la empresa;
g) conservar evidencia documental de todas las transacciones realizadas;
h) garantizar la trazabilidad de cada operación financiera, así como de los acuerdos o cualquier otra inversión o proyecto empresarial;
i) verificar la coherencia económica de dichas operaciones e inversiones;
j) revisar la lista negra internacional sobre terrorismo y jurisdicciones de alto riesgo.

F. Delitos contra particulares

El término "delitos contra particulares" se refiere a varios tipos de delitos penales que suelen implicar lesiones personales, amenazas de daño físico u otras acciones cometidas en contra de la voluntad de una persona.

Sin embargo, a efectos de este EGCP, los delitos contra particulares se refieren principalmente a los delitos que pueden ocurrir con mayor probabilidad en la gestión de una empresa, como los referidos a prácticas de trabajo forzoso, consistentes principalmente en obligar a los empleados a trabajar mediante el uso de violencia, intimidación o por otros medios coercitivos, como la retención de documentos de identidad.

Este tipo de delito puede producirse por varias razones, incluyendo, pero sin limitarse a:

- emplear mano de obra a un coste mínimo.
- emplear mano de obra totalmente sumisa, que no cuestione órdenes ni rechace solicitudes.

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

ÁREAS A SUPERVISAR

En relación con este tipo de delitos, es necesario supervisar las siguientes áreas:

(i) la celebración de contratos con proveedores que empleen personal no especializado y/o que operen en países donde los derechos individuales no estén plenamente protegidos por la legislación local o internacional.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Non-Italian Subsidiaries are required to:

a) seleccionar Terceros externos (por ejemplo, socios, proveedores), especialmente aquellos que prestan servicios no técnicos, sólo después de haber verificado de forma rigurosa su fiabilidad;
b) formalizar la documentación contractual adecuada con contratistas externos que les requieran cumplir, y que sus subcontratistas cumplan, con cualquier legislación internacional y local aplicable. Esto incluye, entre otras, las convenciones de la Organización Internacional de Trabajo (OIT) relativas a la edad mínima para el empleo, las peores formas de trabajo infantil, el trabajo forzoso, la protección del trabajo infantil y de la mujer, así como el cumplimiento de las condiciones higiénicas y sanitarias adecuadas;
c) aplicar y hacer cumplir las sanciones contractuales previstas en los acuerdos correspondientes en caso de incumplimiento, por parte de un contratista o de cualquiera de sus subcontratistas, de cualquier legislación internacional o local aplicable.

G. Delitos de salud y seguridad

Los delitos de salud y la seguridad están relacionados principalmente con el incumplimiento de las legislaciones locales y los estándares laborales que deben llevarse a cabo en el lugar de trabajo para prevenir accidentes y enfermedades de los empleados.

Este tipo de conductas pueden tener producirse en beneficio de una empresa por múltiples razones, incluyendo, pero sin limitarse a:

i. reducir costes, ya que la implementación de las medidas requeridas conlleva, a menudo, gastos adicionales para una empresaM
ii. aumentar la productividad, dado que trabajar sin considerar procedimientos y políticas preventivas podría acelerar el proceso de producción.

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

ÁREAS A SUPERVISAR

En relación con este tipo de Delitos, es necesario supervisar las siguientes áreas:

(i) cumplimiento de las leyes de salud y seguridad aplicables.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Con independencia del alcance de la legislación local en materia de salud y seguridad laboral, los NIS promoverán y consolidarán una sólida cultura de protección en el lugar de trabajo, fomentando la concienciación sobre los riesgos y la responsabilidad individual en el comportamiento seguro.

En este sentido y más allá del cumplimiento estricto de la normativa local aplicable, los NIS se comprometen a adoptar todas las medidas necesarias para salvaguardar la integridad física y moral de sus trabajadores.

Los NIS garantizarán que:

a) El cumplimiento de las disposiciones legales en materia desalud y seguridad laboral constituya una prioridad;
b) los riesgos laborales sean evaluados y gestionados, en la medida de lo posible y conforme al desarrollo de las mejores técnicas disponibles, mediante la selección de los materiales y equipos adecuados y seguros, con el objetivo de eliminar o, cuando no sea posible, reducir el riesgo en su origen;
c) la información y formación de los trabajadores sea amplia, actualizada y específica en función de las actividades desempeñadas;

d) se escuche periódicamente a los trabajadores sobre cuestiones relacionadas con la salud y la seguridad en el entorno laboral;

e) se aplique un 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 del trabajo esté estructurada de manera que proteja la integridad de los trabajadores, de terceros y de la comunidad en la que operan los NIS.

Para alcanzar estos objetivos, los NIS asignarán recursos organizativos, técnicos y económicos necesarios para asegurar el pleno cumplimiento de la normativa vigente en materia de prevención de riesgos laborales, así comopara mejorar de forma continua las condiciones de salud y seguridad de los trabajadores.

Los Destinatarios Corporativos, en función del rol que desempeñen dentro de la organización, deberán garantizar el estricto cumplimiento de la legislación aplicable, de los procedimientos internos y de cualquier otra normativa corporativa destinada a proteger la salud y la seguridad de los trabajadores.

H. Delitos medioambientales

Los delitos medioambientales comprenden una amplia gama de actividades ilícitas, entre las que se incluyen el comercio ilegal de especies silvestres, la gestión indebida de los recursos hídricos, el tráfico y eliminación no autorizada de residuos peligrosos y el contrabando de sustancias que agotan la capa de ozono.

Este tipo de delitos suelen tener un impacto directo en la calidad del aire, el agua y el suelo, pone en riesgo la biodiversidad y puede desencadenar desastres ambientales de gran magnitud, representando una amenaza para la salud,la seguridad y el bienestar de amplios sectores de población.

Impulsadas por elevados beneficios económicos y facilitadas por un bajo riesgo de detección y escasas tasas de condena, estas actividades ilícitas atraen cada vez a más redes delictivas yorganizaciones criminales, especialmente en contextos transnacionales.

Estas conductas pueden producirse en beneficio de una empresa por diversas razones, entre ellas:

- reducción de costes:evitar la implementación de medidas de protección ambiental puede representar un ahorro económico inmediato;
- incremento de la productividad: operar sin considerar los impactos medioambientales puede acelerar procesos productivos, aunque a costa del cumplimiento normativo y la sostenibilidad.

Para ejemplosespecíficos, véase el Anexo 1.

ÁREAS A SUPERVISAR

En relación con este tipo de Delitos, es necesario supervisar especialmente las siguientes áreas:

(i) cumplimiento de la normativa ambiental aplicable en el diseño, construcción, operación, mantenimiento y desmantelamiento de plantas, interconexiones e infraestructuras de redes de distribución;
(ii) cumplimiento de lanormativa 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 apequeñas, medianas y grandes empresas, así como entidades del sector público; incluyendo el diseño, prueba y desarrollo de productos de movilidad eléctrica e innovación tecnológica.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

En el desarrollo de sus actividades empresariales, los NIS se comprometen a actuar conforme al principio de protección y preservación del medio ambiente.

En particular, los NIS:

a) contribuyen activamente a la concienciación y difusión de buenas prácticas en materia de protección ambiental, gestionando sus actividades en cumplimiento de la legislación aplicable;
b) promueven el desarrollo científico y tecnológico orientado a la protección del medio ambiente y a la conservación de los recursos naturales, mediante la adopción de sistemas avanzados que favorezcan la sostenibilidad y la eficiencia energética;

c) se esfuerzan por satisfacer las expectativas de sus clientes y demás partes interesadas en relación con cuestiones medioambientales, adoptando todas las medidas necesarias para la protección y preservación del entorno y condenando cualquier forma de daño al ecosistema.

En los acuerdos celebrados con Terceros que puedan implicar responsabilidad ambiental parala Empresa --especialmente en lo relativoc a la gestión y eliminación de residuos-- se incluirán clausulas específicas que impongan el cumplimiento de la norma ambiental aplicable, así como sanciones contractuales en caso de incumplimiento.

I. Delitos cibernéticos

Los delitos cibernéticos son infracciones penales que se dividen en dos categorías principales.

(i) aquellos en los que el objetivo es una red o un sistema informático;
(ii) aquellos en los que el delito es ejecutado o facilitado mediante el uso de un sistema informático.

A los efectos del EGCP, los Delitos Cibernéticos no incluyen aquellos ilícitos que, si bien pueden ser facilitados por medios informáticos, constituyen categorías penales distintas, como el fraude, el robo, la extorsión, la falsificación o el acoso (por ejemplo, ciberacoso) Por tanto, los Delitos Cibernéticos considerados en el marco del EGCP comprender, entre otros, los siguientes ejemplos:

(i) intrusión no autorizada en una red o sistemas informáticos protegidos;
(ii) introducción de virus u otros programas maliciosos en sistemas informáticos;
(iii) interceptación no autorizada de datos transmitidos a través de redes informáticas.

Estos delitos pueden tener diversas motivaciones, entre las que se incluyen:

- robo de secretos comerciales de empresas competidoras;
- sabotaje o daño intencionado a los sistemas informáticos de un competidor;
- obtención ilícita de información confidencial sobre estrategias de mercado de otras empresas.

Para ejemplos adicionales, veáse el Anexo 1.

ÁREAS A SUPERVISAR

En relación con este tipo de delitos, es necesario supervisar las siguientes áreas clave:

(i) actividades digitales realizadas por los Destinatarios, tanto en entornos de Tecnologias 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;
(iv) gestión de perfiles de usuarios con privilegios.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Deberán evaluarse la conveniencia de aplicar medidas técnicas, físicas y organizativas adecuadas para prevenir conductas indebidas,y cada Destinatario está obligado a abstenerse de incurriren las siguientes prácticas:

a) uso indebido de credenciales personales para acceder a dispositivos, sistemas o infraestructuras de Tecnologías de la Información y Tecnología Operativa;
b) permitir o facilitar el acceso no autorizado de terceros a dichos sistemas o infraestructuras;
c) divulgación o intercambio no autorizado de información o datos empresariales fuera del entorno corporativo;
d) acceso, extracción o modificación no autorizados de información o datos;
e) uso de dispositivos personales o no autorizados para transmitir o almacenar información o datos de la empresa;
f) compartir dispositivoscorporativos con personas no autorizadas;
g) manipulación o alteración de configuraciones en dispositivos o infraestructuras corporativas;
h) manipulación de sistemas ,robo o destrucción de archivos, datos o programas de la empresa;
i) acceso a sistemas de información corporativos sin la debida autorización;
j) envío de comunicaciones no solicitadas (spam);

k) conexión de dispositivos externos (ordenadores personales, periféricos, discos duros , etc.) a sistemas corporativos o instalación de software y bases de datos sin autorización previa;

l) instalación de software maliciosos(por ejemplo, virus o gusanos) en sistemas o infraestructuras de Tecnologías de la Información y Tecnología Operativa;

m) uso de software o hardware no autorizado que pueda emplearse para evaluar o comprometer la seguridad de los dispositivos, sistemas e infraestructuras corporativos (por ejemplo, herramientas para identificar credenciales o descifrar archivos cifrados).

Deberá garantizarse un monitoreo periódico de las actividades realizadas por el personal de los NIS en los sistemas informáticos corporativos con el fin de identificar comportamientos inusuales, posibles vulnerabilidades o deficiencias, siempre en conformidad con la legislación local aplicable.
Asimismo, será preciso que serecuerde periódicamente a los Destinatarios Corporativos la obligación de utilizar de forma adecuada los dispositivos, sistemas e infraestructuras puestos a su disposición, incluyendo la realización de sesiones de formación específicas cuando sea necesario.

J. Delitos de 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 originarse por diversas causas, entre las que se incluyen, sin limitarse a:

a) Desconocimiento: los empleados pueden infringir derechos de autor deforma involuntaria debido a una formación insuficiente sobre la normativaaplicables 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;

c) Mala fe: empleados que, de forma deliberada, infringeni derechos de autor con el objetivo de perjudicar a un competidor de los NIS.

Para ejemplos específicos, véase el Anexo 1.

ÁREAS A SUPERVISAR

En relación con este tipo de delitos, deben supervisarse especialmente los siguientes comportamientos o situaciones:

- uso o divulgación no autorizados de obras protegidas por derechos de autor, materiales de investigación o contenido de propiedad de terceros;
- uso de imágenes, videos 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 bases de datos protegidas;
- infracciones derivadas de procesos deexternalización, 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.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

Además de los estándares clave de comportamiento establecidos en el apartado 10.2 sección I) , deberá evaluarse la conveniencia de adoptar medidas técnicas, físicas y organizativas adecuadas para prevenir:

1. el uso o difusión ilícita al público, a través de redes informáticas o cualquier otro tipo de conexióna, de obras originales protegidas por derechos de autor, total o parcialmente;
2. el uso, distribución, extracción, venta o arrendamiento de contenidos de bases de datos en violación de los derechos exclusivos de explotación y autorización del titular de los derechos;
3. la descarga no autorizada de software sin la correspondiente documentación contractual;
4. la descarga de software de peer-to-peer u otros programas no vinculados directamente con la actividad corporativa.

En caso de que los NIS celebren contratos con terceros para la ejecución de actividades que puedan implicar riesgos de infracción de derechos de autor, dichos contratos deberán incluir cláusulas específicas que exigan el cumplimiento de lalegislación y reglamentación aplicables en la materia.

Las medidas adoptadas deberán basarse en los siguientes principios fundamentales:

- 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 fiscales

Los delitos fiscales 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 documentaly 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 A SUPERVISAR

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.

ESTÁNDARES CLAVE DE COMPORTAMIENTO

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 , los 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 yla 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 exactitudde los datosconsignados;

c. comprobar la corrección de los cálculos relativos aimpuestos 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 empresarialesreales y debidamente documentados;

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

h. asegurar la pconservación de registros y documentos obligatorios mediante medios digitales 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, garantizandoque 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. Asímismo, 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 COMPORTAMIENTOS ILÍCITOS COMETIDOS EN LAS ABM

A. Delitos de soborno

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

- entregue un obsequio a un funcionario con el fin de obtener la adjudicación de una licitación;
- ofrezca dinero a un funcionario durante una inspección en una planta para persuadirlo de ignorar determinadas irregularidades;
- prometa contratar a un empleado de una empresa competidora a cambio de obtener acceso a documentos confidenciales de dicha empresa;
- ofrezca dinero a un testigo con el propósito de inducirlo a realizar una declaración falsa en un proceso judicial en el que los NIS están involucrados.

B. Otros delitos contra autoridades públicas

Dentro del ámbito de los NIS, se considerará la comisión de otros delitos contra autoridades públicas cuando una persona:

- presente información falsa ante una agencia gubernamental durante el proceso de participación en una licitación, con el objetivo de asegurar su adjudicación;
- proporcione una representación falsa de la situación financiera o empresarial de los NIS con el fin de obtener financiación pública;
- incumpla las condiciones de un acuerdo de subvención, utilizando de forma indebida los fondos recibidos de una entidad pública.

C. Fraude contable

Dentro del ámbito de los NIS, se considerará la comisión de fraude contable cuando una persona:

- omita registrar en los estados financieros las pérdidas relevantes sufridas por los NIS;
- oculte la creación de fondos destinados a fines ilícitos, mediante la sobreestimación del coste de servicios de consultoría contratados por los NIS.

D. Abuso del mercado

En el supuesto de que los NIS sean una sociedad cotizada, se considerará abuso de mercado cuando una persona:

- divulgue información privilegiada a un familiar sobre una próxima adquisición, induciéndolo a comprar acciones de la empresa;
- difunda información falsa sobre la situación financiera de los NIS con el objetivo de influir en el precio de sus acciones;
- propague información falsa o engañosa sobre una empresa competidora con el fin de perjudicar su reputación en el mercado.

E. Financiación del terrorismo y delitos de blanqueo de dinero

Dentro del ámbito de los NIS, se considerará la comisión de delitos relacionados con la financiación del terrorismo o blanqueo de capitales cuando una persona:

- reciba o transfiera fondos desde o hacia una empresa ubicada en un paraíso fiscal, o con cuentas bancarias en dichas jurisdicciones, con el fin de ocultar el origen ilícito del dinero;
- simule el pago de servicios de consultoría a una empresa, transfieriendo en realidad fondos a cuentas bancarias secretamente controladas por una organización ilegal que financia actividades terroristas;
- utilice fondos destinados a fines ilícitos--cuya creación ha sido encubierta mediante la manipulación de los estados financieros de la empresa-- para financiar partidos políticos vinculados aorganizaciones terroristas.

F. Delitos contra particulares

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

- se aproveche de la situación de vulnerabilidad física o psicológica de un trabajadorpara explotarlo laboralmente;
- obligue a una persona a trabajarmediante amenazas, abuso de autoridad y/o violencia;
- coaccione a los personas migrantes para que trabajen bajo amenaza de ser denunciada ante las autoridadesmigratorias.

G. Delitos de salud y seguridad

Dentro del ámbito de los NIS, se considerará la comisión de delitos en materia de salud y seguridad cuando una persona actúe en incumpliento de la legislación aplicable, incluyendo, entre otros los siguientes supuestos:

- no proporcione el Equipo de Protección Personal (EPP) conforme a lo establecido en la evaluación de riesgos;
- omita la implementación de medidas de emergencia en el lugar de trabajo, incluyendo las medidas organizativas, formativas y técnicas;

- no suministre a los trabajadores el equipo de seguridad ni la maquinaria necesaria para el desempeño seguro de sus funciones;
- permita que los empleados operen maquinaria sin haber recibido la formación adecuada sobre su uso seguro;
- omita realizar los exámenes médicos periódicos exigidos por la normativa, necesarios para evaluar el estado de salud de los trabajadores y detectar posibles afectaciones derivadas de su actividad laboral.

H. Delitos medioambientales

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

- omita considerar el impacto sobre la Biodiversidad al planificar la expansión de una planta,o cause daños al hábitat de especies animales protegidas, poniendo en riesgosu existencia;
- opere una central térmica sin respetar los umbrales legales de emisión de gases, provocando la contaminación del aire en la zona circundante;
- no gestione adecuadamente la eliminación de residuos de la empresa y, en su lugar, establezca un sitio de disposición ilícita de residuos;
- contamine cuerpos de agua debido al uso inadecuado del recurso o de los sistemas de tratamiento de agua;
- no implemente sistemas adecuados de prevención y control de emisiones atmosféricas, generando la contaminación del aire.

I. Delitos cibernéticos y delitos relacionados con la propiedad intelectual

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

- istale software ilegalmente copiado en dispositivos de trabajo;
- acceda sin autorización a sistemas informáticos de empresas competidoras mediante técnicas maliciosas de piratería informática, con el fin de sustraer información confidencial, secretos comerciales o difundir malware con intención de causar daño.

K. Delitos fiscales

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.