Política contra el blanqueo de capitales y de financiación del terrorismo

CONTROL DE MODIFICACIONES		
Edición	**Fecha**	**Objeto de la Edición**
0	01-10-2024	Creación de la política
1	14-08-2026	Actualización prudencial: se acota el alcance de las medidas de diligencia debida de clientela a la condición de sujeto obligado de cada sociedad conforme a la Ley 10/2010, se incorpora un apartado sobre los riesgos reales de la actividad del Grupo (efectivo, fondos públicos y proveedores), se referencia el nuevo marco europeo (Reglamento UE 2024/1624, Directiva UE 2024/1640 y AMLA) y se unifica el canal de comunicación de indicios con el Sistema Interno de Información (Ley 2/2023).

1 | Fundamento y objetivos

En el Grupo **neo** (en adelante, indistintamente, el "Grupo" o "Grupo **neo**") estamos profundamente comprometidos con la prevención del blanqueo de capitales, la financiación de actividades terroristas y el cumplimiento de los Programas de Sanciones y Contramedidas Financieras Internacionales (en adelante "Sanciones"). Promovemos la aplicación de los más altos estándares internacionales en esta materia.

La criminalidad financiera es un fenómeno global que se aprovecha de la desaparición de barreras comerciales y la internacionalización de la economía. La lucha contra este fenómeno requiere una respuesta coordinada de la comunidad internacional y del sector financiero para evitar su uso con fines ilícitos de forma inadvertida e involuntaria.

El objetivo de esta Política Corporativa de Prevención del Blanqueo de Capitales, Financiación del Terrorismo y Gestión de Sanciones y Contramedidas Financieras Internacionales (en adelante la "Política") es (i) establecer un marco de cumplimiento a nivel de Grupo aplicable en todas las actividades, negocios y relaciones, tanto nacionales como internacionales; (ii) definir roles y responsabilidades en esta área; (iii) establecer las bases para la definición y aplicación de políticas y procedimientos en las filiales del Grupo; y (iv) proporcionar un marco de gobernanza.

La implementación de las medidas de esta Política debe garantizar el cumplimiento de la normativa aplicable en todas las jurisdicciones donde el Grupo **neo** opera.

En España, esta normativa está constituida principalmente por la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, cuya autoridad de supervisión competente es el SEPBLAC (Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias). El Grupo neo sigue asimismo la evolución del nuevo marco europeo constituido por el Reglamento (UE) 2024/1624, la Directiva (UE) 2024/1640 y la nueva Autoridad Europea de Lucha contra el Blanqueo de Capitales (AMLA), de aplicación plena a partir del 10 de julio de 2027, y adaptará esta Política conforme dicho marco se vaya desarrollando.

2 | Ámbito de Aplicación

La Política se aplica a todas las sociedades del Grupo **neo** obligadas a cumplir con la normativa de prevención de blanqueo o los programas de Sanciones. Debe ser adoptada en todas las jurisdicciones donde **neo** y sus filiales operan.

Las unidades encargadas de la prevención y supervisión desarrollarán normas y procedimientos para su correcta implementación, ejecución y cumplimiento. Las sociedades del Grupo adaptarán sus normas y procedimientos según los requerimientos legales específicos de cada jurisdicción, previa aprobación del departamento de Cumplimiento de **neo**, para asegurar que las adaptaciones son consistentes y no contradicen la Política. Tras la validación del departamento de Cumplimiento, las normas deben ser presentadas al Órgano de Control Interno del Grupo para su aprobación definitiva.

3 | Concepto de Blanqueo de Capitales y de Financiación del Terrorismo

Para los fines de esta Política, se entiende por Blanqueo de Capitales las siguientes actividades:

a. La conversión o transferencia de bienes sabiendo que proceden de una actividad delictiva, con el propósito de ocultar o encubrir su origen ilícito o ayudar a personas implicadas a eludir las consecuencias legales de sus actos.

b. La ocultación o encubrimiento de la naturaleza, origen, localización, disposición, movimiento o propiedad real de bienes o derechos sobre bienes, sabiendo que proceden de una actividad delictiva.

c. La adquisición, posesión o utilización de bienes sabiendo, en el momento de recibirlos, que proceden de una actividad delictiva.

d. La participación en las actividades mencionadas anteriormente, la asociación para cometer estos actos, la tentativa de perpetrarlos y la ayuda, instigación o consejo para realizarlos o facilitar su ejecución.

Asimismo, se entiende por Financiación del Terrorismo el suministro, depósito, distribución o recogida de fondos o bienes, directa o indirectamente, con la intención de utilizarlos o con el conocimiento de que serán utilizados, total o parcialmente, para la comisión de delitos de terrorismo.

4 | principios y estándares aplicables

Los principales principios y estándares que constituyen el marco de prevención que esta Política regula son:

1. Evaluación de Riesgos.
2. Diligencia Debida.
3. Detección, control y examen de operaciones.
4. Comunicación de operativa sospechosa.
5. Control de listas de Sanciones y Comunicación de detecciones.
6. Retención de la documentación.
7. Formación.
8. Roles y responsabilidades.
9. Gestión consolidada del riesgo.

4.1 | Evaluación de Riesgos

La exposición del Grupo **neo** a los riesgos de Blanqueo de Capitales, Financiación del Terrorismo y Sanciones está directamente relacionada con el tipo de negocio, productos, servicios, canales de comercialización, características de los clientes y/o las jurisdicciones en las que opera.

En el caso de las sociedades del Grupo **neo** dedicadas a la gestión de instalaciones deportivas y prestación de servicios deportivos, esta evaluación debe prestar especial atención a los riesgos vinculados al manejo de efectivo en taquillas, abonos y actividades similares; a la gestión de fondos y subvenciones públicas derivados de las concesiones administrativas que el Grupo opera, en línea con el compromiso con las Administraciones Públicas recogido en la ***Política de Derechos Humanos del Grupo***; y a los pagos realizados a personas proveedoras y colaboradoras externas, conforme a los criterios de diligencia debida de terceros recogidos en la ***Política contra la Corrupción y el Fraude*** del Grupo. La aplicación de las medidas de diligencia debida de clientela previstas en el apartado siguiente se ajustará, en cada sociedad del Grupo, a su condición de sujeto obligado conforme a la Ley 10/2010 y a la normativa que en cada jurisdicción resulte

aplicable, aplicándose en todo caso los principios generales de esta Política de forma proporcionada al perfil de riesgo real de cada actividad.

4.2 Diligencia Debida

La política de admisión de clientes y las medidas de diligencia debida no podrán vulnerar los derechos en las jurisdicciones donde la Sociedad del Grupo opere.

La política de admisión de clientes es dinámica y establece un marco de cumplimiento a nivel de Grupo que varía según el nivel de riesgo de segmentos o actividades específicos. La política de admisión debe cumplir los estándares internacionales y el principio de "Conoce a tu Cliente" (KYC, por sus siglas en inglés), garantizando un buen conocimiento del cliente y sus actividades en todo momento.

El principio de KYC y las políticas de diligencia debida aplicarán siempre con un enfoque basado en el riesgo, asegurando que las medidas aplicadas son adecuadas al riesgo subyacente de blanqueo de capitales, financiación del terrorismo o Sanciones.

1. **Clasificación de clientes**. Los clientes del Grupo deben ser segmentados y clasificados según el riesgo para diseñar medidas preventivas y de control adecuadas.

   Los controles y procedimientos deben garantizar un seguimiento continuo de la relación de negocio para adaptar el nivel de riesgo y las medidas a aplicar según las circunstancias del cliente.

   La valoración del nivel de riesgo se documentará en las sociedades del Grupo **neo** según su actividad y operativa, considerando diversos factores de exposición al riesgo, incluyendo:

   Características del cliente:

   - Actividad.
   - Zona geográfica.
   - Persona de Responsabilidad Pública (PRP).
   - Identidad del Titular Real.
   - Estructura de propiedad o Control.

   Características de productos o servicios:

- Tipo de producto.
- Segmento de negocio.
- Canal de relación.

Características de la operativa:

- Origen de los fondos.
- Transacciones.

Las Sociedades del Grupo utilizarán la siguiente clasificación de clientes según el grado de riesgo identificado:

- **Personas cuya admisión no está permitida**: No se admitirán relaciones de negocio con personas físicas o jurídicas en las siguientes situaciones:
    - Personas a las que no se les hayan podido aplicar las medidas de diligencia debida previstas en esta Política.
    - Personas incluidas en listas nacionales o internacionales de Sanciones.
    - Personas con negocios que hagan imposible verificar la legitimidad de las operaciones o la procedencia de los fondos.
    - Personas que rehúsen facilitar la documentación necesaria para una plena identificación formal del titular y/o beneficiario real.
    - Personas que presenten documentos falsos o dudosos.
    - Personas que rehúsen facilitar información sobre la verificación de actividades declaradas o la procedencia de los fondos.
    - Personas e instrumentos jurídicos cuya estructura de propiedad o control no pueda determinarse.
    - Bancos pantalla y entidades financieras que operen con este tipo de entidades.
    - Personas o entidades que pretendan realizar actividades financieras sin la correspondiente autorización oficial.
    - Cualquier otra categoría no contemplada que deba ser rechazada según una norma jurídica o política interna.
    - Personas físicas o jurídicas que, habiendo sido clientes del Grupo, hayan dejado de serlo por aplicación de esta Política.

- **Personas de riesgo superior al promedio**: Su aceptación como clientes requiere medidas de diligencia reforzada y aprobación centralizada. Incluye:

- Personas con responsabilidad pública (PRP).
- Personas con residencia o nacionalidad en una jurisdicción de riesgo.
- Clientes relacionados con la producción, comercialización, distribución y venta de armas.
- Entidades de pago, servicios de envío de dinero y cambio de moneda, casinos y sociedades de juegos recreativos con la correspondiente autorización oficial.
- Sociedades con títulos al portador, una vez determinada su estructura de propiedad o control.

- **El resto de personas o entidades** estarán sujetas a medidas de diligencia normales o simplificadas según la normativa aplicable o las normas y procedimientos internos.

2. **Identificación formal de clientes**: Las normas y procedimientos deben garantizar la adecuada identificación de todos los clientes de acuerdo con la legislación aplicable, incluyendo la verificación de la identidad mediante documentos válidos y vigentes.

   No se mantendrán relaciones de negocio con personas no identificadas. Se prohíbe la contratación de productos o servicios anónimos, cifrados o ficticios. Antes de establecer relaciones de negocio o ejecutar operaciones, se deberá identificar al titular real. Ante indicios o certeza de que los clientes no actúan por cuenta propia, se recabará información precisa sobre la identidad de las personas por cuenta de las cuales actúan, así como documentación que acredite los poderes con los que actúa.

3. **Conocimiento de la actividad y patrimonio del cliente**: Antes de establecer una relación de negocio, las sociedades del Grupo recabarán información sobre la actividad profesional o empresarial del cliente y el origen de los fondos o patrimonio.

   Según el nivel de riesgo asignado, podrán adoptar medidas adicionales para verificar documentalmente la información proporcionada por el cliente, especialmente en relación con su actividad profesional, el origen de los fondos y cualquier otra información relevante según las normas y procedimientos internos.

4.3 | Detección, control y examen de operaciones

Las sociedades del Grupo deben disponer de medios para la detección, control y examen de operaciones según el riesgo, incluyendo:

a. Comunicación interna por indicios realizada por el personal del Grupo, a través del Sistema Interno de Información previsto en la Ley 2/2023, de 20 de febrero.
b. Detección de operaciones sospechosas a través de sistemas de alertas establecidos.
c. Comunicaciones de organismos supervisores o autoridades policiales o judiciales.

La detección de operaciones sospechosas conlleva un análisis detallado para determinar la existencia de indicios de blanqueo de capitales y financiación del terrorismo. La metodología para este análisis se recogerá en un procedimiento específico denominado Procedimiento de Examen Especial, centralizado en una misma unidad para todas las sociedades del Grupo en la misma jurisdicción.

La monitorización será automatizada y revisará la actividad según los patrones identificados por la ley y las mejores prácticas en cada momento.

4.4 | Comunicación de operativa sospechosa

Las sociedades del Grupo comunicarán a los organismos supervisores y/o de Inteligencia Financiera cualquier hecho u operación sospechosa, incluso la tentativa, tras un examen especial que determine indicios de blanqueo de capitales o financiación del terrorismo.

En particular, se comunicarán las operaciones que no correspondan con la naturaleza, volumen de actividad o antecedentes operativos de los clientes.

La decisión de comunicar se adoptará centralizadamente en cada jurisdicción y se realizará a través del representante habilitado ante las autoridades competentes, incluyendo información sobre la decisión respecto a la continuación de la relación de negocio y su justificación.

El personal del Grupo deberá abstenerse de ejecutar operaciones con indicios de relación con el blanqueo de capitales o financiación del terrorismo. No se revelará al cliente ni a terceros que se ha comunicado información a los órganos de control interno o al organismo supervisor, o que se está examinando alguna operación.

4.5 | Control de listas de Sanciones y comunicación de detecciones

Para cumplir con las restricciones de los programas de Sanciones, las sociedades del Grupo deberán:

- Identificar y seguir los programas de Sanciones de la ONU, la UE, OFAC y programas locales aplicables.
- Evaluar los riesgos asociados a actividades restringidas o prohibidas por las Sanciones.
- Abstenerse de ejecutar operaciones con personas sancionadas.
- Cumplir con las prohibiciones y restricciones en la ejecución de transacciones, absteniéndose de realizarlas cuando supongan un incumplimiento de los programas de Sanciones.
- Bloquear activos y fondos según requieran los programas de Sanciones, comunicando tal circunstancia a las autoridades correspondientes.
- Implantar procedimientos de control interno y mecanismos de prevención adecuados, incluyendo herramientas de filtrado automatizado.

4.6 | Retención de la documentación

Las sociedades del Grupo **neo** establecerán políticas de conservación de la documentación que cumplan con los requerimientos legales aplicables en cada jurisdicción, siendo el mínimo periodo de conservación el que en cada momento determine la legislación en la materia, y nunca inferior a 10 años. La documentación que debe conservarse de acuerdo a las leyes de prevención incluye como mínimo, los siguientes aspectos.

En particular conservará para su uso en toda investigación o análisis en materia de posibles casos de prevención, por parte de los supervisores o de cualquier otra autoridad competente:

- Copia de los documentos exigibles en aplicación de las medidas de diligencia debida, con inclusión, en particular, de las copias de los documentos fehacientes de identificación, las declaraciones del cliente, la documentación e información aportada por el cliente u obtenida de fuentes fiables independientes.
- Original o copia con fuerza probatoria de los documentos o registros que acrediten adecuadamente las operaciones, los intervinientes en las mismas y las relaciones de negocio.
- Toda aquella documentación en la que se formalice el cumplimiento de sus obligaciones de comunicación y de control interno:
    - Comunicaciones a los organismos supervisores.
    - Comunicación del nombramiento de representantes ante las autoridades de Inteligencia Financiera.
    - Expedientes de examen especial.

- Comunicaciones de operativa sospechosa enviadas a los organismos supervisores y documentación relacionada con éstas.
- Requerimientos de información y solicitudes de rastreo recibidos de los organismos supervisores.
- Informes anuales del examen de experto externo y documentos relacionados.
- Actas de las reuniones de los órganos de control interno, conservándose también las actas y documentos de otros órganos respecto a aquellos aspectos con impacto en materia de prevención.

4.7 | Formación

La sensibilización sobre los riesgos asociados a estos delitos es clave en la lucha contra el blanqueo y terrorismo. Las sociedades del Grupo **neo** definirán, mantendrán y aplicarán programas de formación para garantizar un adecuado nivel de sensibilización de todo el personal, incluyendo la alta dirección y los órganos de administración, de forma periódica y adecuada al nivel de riesgo de su actividad.

4.8 | Roles y responsabilidades

Las entidades del Grupo **neo** deberán contar con una estructura de gobierno y organización interna que permita cumplir las obligaciones de identificación y prevención del blanqueo de capitales, financiación del terrorismo y Sanciones, garantizando la comunicación adecuada en cada jurisdicción a las Autoridades competentes y el bloqueo y congelación de fondos o recursos económicos según los marcos de sanciones internacionales y contramedidas.

4.9 | Gestión consolidada del riesgo

neo considera que la mejor forma de combatir los riesgos asociados a esta Política es la gestión consolidada y uniforme de la información relacionada con estos riesgos a nivel del Grupo, independientemente de la jurisdicción en la que operen las sociedades.

El principio de gestión agregada se constituye en un pilar fundamental del modelo de prevención, permitiendo coordinar los esfuerzos de todas las sociedades del Grupo y gestionar los riesgos de forma agregada. Todas las entidades del Grupo mantendrán informada a **neo** sobre relaciones de alto riesgo, actividades sensibles y sus riesgos asociados, atendiendo rápidamente

cualquier solicitud de información que **neo** formule en la gestión del riesgo regulatorio y reputacional.

Estas obligaciones se entienden sin perjuicio del estricto cumplimiento de la normativa aplicable, especialmente en protección de datos y privacidad. **neo** y las sociedades del Grupo adoptarán las medidas necesarias para preservar la confidencialidad y privacidad de los datos comunicados entre entidades del Grupo.

5 | Revisión

El desarrollo de las funciones de prevención, gestión, control y decisión requiere de una estructura de gobierno sólida que garantice la involucración de los órganos de decisión, gestión y administración de **neo**, así como una estrecha coordinación entre las sociedades del Grupo.

El Comité de Dirección revisará periódicamente el contenido de la Política, asegurando que recoge las recomendaciones y mejores prácticas internacionales vigentes, y propondrá al Consejo de Administración las modificaciones y actualizaciones que contribuyan a su desarrollo y mejora continua, atendiendo a las sugerencias y propuestas de los profesionales del Grupo.