

ROX PAY S.R.L.

POLÍTICA DE PREVENCIÓN Y CONTRA EL LAVADO DE ACTIVOS Y LA FINANCIACIÓN DEL TERRORISMO

1 - RESUMEN

1.1 – REGULACIONES Y ORIENTACIONES CLAVE

Este documento establece la Política de Rox Pay S.r.l. en materia de lucha contra el blanqueo de capitales, la financiación del terrorismo y la violación de medidas restrictivas.¹ y se aplica a Rox Pay S.r.l. y sus operaciones.

Las normas deben considerarse complementarias y aplicables siempre que no entren en conflicto con las disposiciones emitidas por las Autoridades locales.

1.2 – DESTINATARIOS Y MÉTODOS DE IMPLEMENTACIÓN

La Política se aplica a Rox Pay S.r.l.

2 – PRINCIPIOS GENERALES

2.1 MARCO REGULATORIO ALA-CFT

El lavado del producto de actividades ilegales y delictivas es una de las formas más graves de delito en los mercados financieros y es un área de interés específico para las actividades delictivas organizadas.

El lavado de dinero tiene un impacto negativo significativo en toda la economía: la reinversión de ganancias ilegales en actividades legales y la colusión entre individuos o instituciones financieras y organizaciones criminales afectan profundamente los mecanismos del mercado, socavan la eficiencia y la equidad de las actividades financieras y tienen un efecto debilitante en la economía. La financiación de actividades terroristas puede implicar el uso de ingresos derivados de la ley y/o del delito.

La naturaleza cambiante del blanqueo de capitales y la financiación del terrorismo, facilitada también por la continua evolución de la tecnología, requiere una adaptación constante de las medidas de prevención y contraste.

El marco regulatorio contra el lavado de dinero (AML) y la lucha contra la financiación del terrorismo (CFT) se basa en un conjunto integral de fuentes regulatorias nacionales, de la UE e internacionales.

A nivel internacional, una contribución clave a la armonización regulatoria provino del Grupo de Acción Financiera Internacional (GAFI), el principal organismo internacional activo en la lucha contra el lavado de dinero, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva.

¹ Tal como se define en las Directrices de la ABE (EBA/GL/2024/14): "Las medidas restrictivas de la Unión a que se refiere el artículo 2, punto (1) de la Directiva (UE) 2024/1226 y las medidas restrictivas nacionales adoptadas por los Estados miembros de conformidad con su ordenamiento jurídico nacional (en la medida en que se apliquen a instituciones financieras).

En el cumplimiento de sus responsabilidades, el GAFI estableció un conjunto de normas internacionales, las "40 recomendaciones", a las que se añadieron otras nueve recomendaciones especiales en 2001 para combatir la financiación internacional del terrorismo. El tema fue revisado completamente en febrero de 2012 con la adopción de las Normas Internacionales para la Lucha contra el Lavado de Dinero y la Financiación del Terrorismo y la Proliferación, que luego se resumieron en las "40 Recomendaciones" antes mencionadas.

Como parte de la lucha contra la proliferación de armas de destrucción masiva, las Naciones Unidas prepararon un conjunto de medidas para combatir la financiación de programas de proliferación, incluida la prohibición de ayudar o financiar a cualquier persona involucrada en tales actividades.

En implementación de las Resoluciones adoptadas en el marco de las Naciones Unidas, la Unión Europea emitió un conjunto de disposiciones con el fin de implementar medidas restrictivas como el congelamiento de fondos y recursos económicos de personas o entidades involucradas en el desarrollo de actividades sensibles a la proliferación de armas de destrucción masiva.

El GAFI ha desarrollado directrices para implementar las sanciones financieras adoptadas por las Naciones Unidas.

Recientemente se han incluido en las Recomendaciones medidas específicas que abordan la proliferación de armas de destrucción masiva, de conformidad con las resoluciones del Consejo de Seguridad de las Naciones Unidas.

Las directrices de la UE para prevenir el uso del sistema financiero para el blanqueo de dinero y la financiación del terrorismo están contenidas en la Directiva 2015/849 de la UE.²del Parlamento Europeo y del Consejo de 20 de mayo de 2015 (Cuarta Directiva contra el Lavado de Dinero), modificada por la Directiva UE 2018/843 (Quinta Directiva contra el Lavado de Dinero), así como en los Reglamentos y Directrices emitidas periódicamente respectivamente por la UE – Unión Europea y por la EBA – Autoridad Bancaria Europea.

A nivel nacional, la prevención y lucha contra el lavado de dinero y el financiamiento del terrorismo se encuentra regulada por las siguientes leyes primarias:

- **Decreto legislativo italiano n. 109 de 22 de junio de 2007 y modificaciones y complementos posteriores que establece "Disposiciones para prevenir, contrarrestar y reprimir la financiación del terrorismo y las actividades de los países que amenazan la paz y la seguridad internacional", implementando la Directiva 2015/849 modificada por la Directiva de la UE 2018/843;**
- **Decreto legislativo italiano n. 231, de 21 de noviembre de 2007, y posteriores modificaciones y complementos de desarrollo de la Directiva 2015/849/UE, por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, modificada por la Directiva 2018/843/UE, sobre prevención de la utilización del sistema financiero con fines de blanqueo de capitales y financiación del terrorismo (en adelante, también el Decreto).**

2 La Directiva UE 2024/1640 del Parlamento Europeo y del Consejo, de 31/05/2024, sobre los procedimientos que deben establecer los Estados miembros para impedir la utilización del sistema financiero con fines de blanqueo de capitales o financiación del terrorismo, que deberá transponerse antes del 10 de julio de 2027, modifica la Directiva UE 2019/1937 y deroga la Directiva UE 2015/849.

Por último, también existe legislación secundaria a nivel nacional emitida por el Banco de Italia. y la Unidad de Información Financiera ("UIF"), y está contenido en las siguientes fuentes regulatorias:

- **Disposición de 26 de marzo de 2019 que establece las disposiciones de aplicación sobre organización, procedimientos y controles internos destinados a prevenir el uso de intermediarios financieros y otras entidades con fines de blanqueo de capitales y financiación del terrorismo, modificada por la Disposición del Banco de Italia de 1 de agosto de 2023;**
- **Disposición de 28 de marzo de 2019 por la que se establecen instrucciones sobre comunicaciones objetivas;**
- **Disposición de 30 de julio de 2019 por la que se establecen disposiciones de aplicación sobre la diligencia debida del cliente, modificada por la Disposición del Banco de Italia de 13 de junio de 2023;**
- **Disposición de 24 de marzo de 2020 por la que se establecen disposiciones de aplicación para el almacenamiento y la disponibilidad de documentos, datos e información en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo;**
- **Disposición de 25 de agosto de 2020 que establece disposiciones para la presentación de informes ALD agregados;**
- **Disposición de 12 de mayo de 2023 sobre indicadores de anomalías para intermediarios para facilitar la identificación de transacciones sospechosas, con efectos a partir del 1 de enero de 2024.**

Rox Pay S.r.l. (en adelante "la Compañía") implementa las normas anteriores en sus documentos normativos internos.

A nivel general, la Sociedad ha adoptado esta "Política de lucha contra el blanqueo de capitales y la financiación del terrorismo" (en adelante la "Política") como expresión de su compromiso de combatir a nivel internacional los citados fenómenos delictivos, prestando especial atención al contraste, consciente de que la búsqueda de la rentabilidad y la eficiencia debe combinarse con el seguimiento continuo y eficaz de la integridad de las estructuras corporativas.

La Política aplicada dentro de la Empresa describe la política adoptada por Rox Pay S.r.l. de conformidad con las normas y principios dictados por las disposiciones reglamentarias nacionales y de la UE, de conformidad con los estándares internacionales pertinentes y se implementa conjuntamente con los procedimientos internos sobre Lucha contra el Lavado de Dinero y la Financiación del Terrorismo, el Código de Ética y los procedimientos internos que implementan la legislación local primaria y secundaria vigente que especifica procesos, roles y responsabilidades.

La presente Política fue aprobada por el Directorio de la Compañía.

Rox Pay S.r.l aplica las directrices AML y CFT. en coherencia con las leyes aplicables.

La Compañía se compromete a cumplir con este marco regulatorio, así como con las disposiciones de implementación emitidas por el Banco de Italia sobre diligencia debida del cliente, retención de datos e información, organización, procedimientos, controles y controles mejorados contra la financiación de programas destinados a la proliferación de armas de destrucción masiva.

La Compañía está completamente comprometida a garantizar que la organización operativa y el sistema de control sean completos, adecuados, funcionales y confiables para la supervisión estratégica, a proteger a la Compañía de la tolerancia o mezcla de formas de ilegalidad que puedan dañar su reputación y afectar su estabilidad.

Por estos motivos, Rox Pay S.r.l. ha adoptado normas organizativas y de comportamiento y sistemas de seguimiento y control encaminados a garantizar el cumplimiento de la legislación vigente por parte de los órganos de administración y control, el personal, los colaboradores y consultores de la Sociedad. Estos controles también son consistentes con las reglas y procedimientos establecidos por el código de protección de datos personales.

La Compañía también se apoya en indicadores de anomalías y patrones de comportamientos irregulares en el entorno económico y financiero, que son emitidos en el tiempo por la Unidad de Inteligencia Financiera (UIF) respecto de potenciales actividades de lavado de dinero y financiamiento del terrorismo.

2.2 - EL MARCO REGULATORIO EN MATERIA DE MEDIDAS RESTRICTIVAS Y EMBARGOS

Todas las medidas restrictivas establecidas para contrarrestar la financiación del terrorismo y todas las actividades ilícitas o sospechosas que amenazan la paz y la seguridad internacionales pueden ser comerciales, como restricciones a las importaciones/exportaciones desde/hacia un país, o financieras, como el bloqueo parcial o total de la transferencia de fondos, pero también limitaciones operativas y congelación de fondos.

Las medidas restrictivas incluyen sanciones financieras internacionales, también denominadas embargos, implementadas por el Estado italiano, agencias extranjeras (por ejemplo, OFAC, UKSL) y organizaciones supranacionales (ONU, UE) a través de una serie de obligaciones que la Compañía debe cumplir. El Consejo impone ciertas medidas restrictivas (sanciones) a todos los Estados miembros de las Naciones Unidas para implementar las Resoluciones adoptadas por el Consejo de Seguridad de las Naciones Unidas en virtud del Capítulo VII de la Carta de las Naciones Unidas. Además, la Unión Europea puede adoptar o decidir de forma autónoma sanciones mediante reglamentos del Consejo, que son inmediatamente ejecutables en cada Estado miembro para garantizar su aplicación oportuna y simultánea.

A nivel internacional, existen regulaciones que establecen prohibiciones o restricciones específicas a invertir en determinados sectores industriales o importar/exportar desde/hacia "Países de alto o significativo riesgo". En particular, se refiere a las resoluciones del Consejo de Seguridad de las Naciones Unidas (CSNU) en virtud del Artículo 41 del Capítulo VII de la Carta de las Naciones Unidas, a través de las cuales se imponen medidas restrictivas con respecto a personas y/o países.

En cuanto a la legislación comunitaria, las principales disposiciones son:

- el Reglamento 2021/821 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021³ y modificaciones posteriores, por las que se establece un régimen de la UE para controlar las exportaciones, la transferencia, el correteaje y el tránsito de artículos de doble uso;

³ que sustituyó al Reglamento 428/2009/CE del Consejo, de 5 de mayo de 2009

- el Reglamento (UE) 2023/1113 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, sobre la información que acompaña a las transferencias de fondos y determinados criptoactivos y por el que se modifica la Directiva (UE) 2015/849 (refundida);
- el Reglamento (UE) 2024/886 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, por el que se modifican los Reglamentos (UE) n.º 260/2012 y (UE) 2021/1230 y las Directivas 98/26/CE y (UE) 2015/2366 en lo que respecta a las transferencias instantáneas en euros;
- la Directiva (UE) 2024/1226 del Parlamento Europeo y del Consejo, de 24 de abril de 2024, sobre la definición de infracciones penales y sanciones por la infracción de medidas restrictivas de la Unión y por la que se modifica la Directiva (UE) 2018/1673 transpuesta al derecho italiano mediante el Decreto Legislativo 211/2025.
- **Directrices de la Autoridad Bancaria Europea sobre políticas, procedimientos y controles internos para garantizar la aplicación de medidas restrictivas nacionales y de la Unión (EBA/GL/2024/14)⁴;**
- **Directrices de la Autoridad Bancaria Europea sobre políticas, procedimientos y controles internos para garantizar la aplicación de medidas restrictivas nacionales y de la Unión, de conformidad con el Reglamento (UE) 2023/1113 (EBA/GL/2024/15) sobre la información que acompaña a las transferencias de fondos y determinados criptoactivos, y por el que se modifica la Directiva (UE) 2015/849⁵.**

Finalmente, a nivel nacional los embargos se regulan de la siguiente manera:

- **Legislación primaria:**
 - **Decreto Legislativo N° 221/2017, que modificó y simplificó los procedimientos de autorización para exportar artículos y tecnologías de doble uso y sanciones a embargos comerciales, así como todo tipo de operaciones de exportación de materiales proliferantes.**
- **Legislación Secundaria:**
 - **Disposición del Banco de Italia del 12 de mayo de 2023 que contiene indicadores de anomalías para los intermediarios con el fin de facilitar la identificación de transacciones sospechosas.**

Finalmente, todas las normas emitidas por las autoridades estadounidenses son relevantes para la actividad de la Compañía en vista de los aspectos reputacionales y la referencia a estas regulaciones en compromisos contractuales que implican la posible aplicación de sanciones con efecto extraterritorial (las llamadas "sanciones secundarias" estadounidenses). Dichas disposiciones regulatorias están contenidas en la USA Patriot Act⁶ y en las medidas relativas a las sanciones económicas y comerciales emitidas por el Gobierno de los Estados Unidos a través de la Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro.⁶

⁴ que el Banco de Italia declaró su intención de cumplir en la Nota no. 48 de 8 de abril de 2025 y aplicable a partir del 30 de diciembre de 2025.

⁵ que el Banco de Italia declaró su intención de cumplir en la Nota no. 52 de 19 de mayo de 2025 y aplicable a partir del 30 de diciembre de 2025.

⁶ Ley federal estadounidense del 26 de octubre de 2001, titulada oficialmente "Ley para unir y fortalecer a Estados Unidos proporcionando las herramientas apropiadas necesarias para interceptar y obstruir el terrorismo de 2001".

3 – MODELOS Y METODOLOGÍAS DE GRUPO

3.1 – ASPECTOS GENERALES

El marco regulatorio nacional establecido para la acción preventiva contra el lavado de dinero, el financiamiento del terrorismo y las violaciones a las Medidas Restrictivas se basa en una serie de obligaciones

que los destinatarios están obligados a respetar:

- obligación de adoptar estructuras organizativas, procedimientos y medidas de control interno adecuadas;
- obligación de adoptar procedimientos consistentes y coherentes para el análisis y evaluación de los riesgos relacionados con el lavado de dinero, el financiamiento del terrorismo y la violación de las Medidas Restrictivas, así como de establecer supervisión, controles y procedimientos necesarios para mitigar y gestionar esos riesgos;
- obligación de diligencia debida con el cliente, a través de la cual la Compañía adquiere y verifica información sobre la identidad de un cliente y cualquier beneficiario final, así como el propósito y la naturaleza prevista de la relación o de la transacción, al tiempo que garantiza el monitoreo constante de todas las transacciones realizadas por el cliente;
- un enfoque basado en el riesgo, mediante el cual las obligaciones de diligencia debida del cliente se dividen en diferentes grados de diligencia debida proporcionales al perfil de riesgo del cliente;
- obligación de conservar los documentos, datos e información con el fin de permitir su adquisición oportuna, su transparencia, exhaustividad, inalterabilidad e integridad, y su rápida y general accesibilidad;
- obligación de informar sobre transacciones sospechosas;
- obligación de abstenerse de entablar nuevas relaciones con clientes, realizar transacciones ocasionales o mantener una relación con clientes existentes cuando no se haya llevado a cabo la debida diligencia o se sospeche que puede haber un vínculo con el lavado de dinero o la financiación del terrorismo;
- obligación de notificar al Ministerio de Economía y Finanzas las infracciones a que se refieren los artículos 49 y 50 del Decreto Legislativo 231/07, y de cumplir con las limitaciones al uso de efectivo y valores al portador;
- monitorear todas las transacciones con personas físicas y jurídicas y/o con países incluidos en las Listas del Consejo de la Unión Europea (UE), en la Lista de Control de Activos Extranjeros (OFAC), en la Lista de Sanciones del Reino Unido (UKSL)⁷, en la Lista Consolidada de Sanciones del Consejo de Seguridad de las Naciones Unidas (ONU) en las Disposiciones emitidas por las Autoridades Nacionales que contienen medidas restrictivas específicas para la lucha contra el terrorismo;
- monitorear las transacciones celebradas con países considerados no cooperadores en materia fiscal, de supervisión financiera y de lucha contra el blanqueo de capitales, generalmente denominados “paraísos fiscales” o “centros financieros extraterritoriales”;
- adoptar programas apropiados de capacitación del personal para garantizar la implementación y aplicación adecuada de las leyes y reglamentos;
- obligación de proporcionar a la UIF “comunicaciones objetivas” de acuerdo con normas instrucciones sobre métodos y frecuencia de las comunicaciones;

7 La lista OFSI (Oficina de Implementación de Sanciones Financieras HMT) se cerró el 28 de enero de 2026; A partir de esa fecha, la Lista de Sanciones del Reino Unido es la única fuente oficial para todas las designaciones de sanciones del Reino Unido.

- obligación de informar de los incumplimientos o infracciones que puedan llegar a conocimiento de los Órganos de Control en el desempeño de sus funciones;
- obligación de adoptar procedimientos para gestionar las denuncias internas de infracciones presentadas por los empleados (Whistleblowing).

En lo que respecta a las actividades de lucha contra la financiación del terrorismo, la legislación italiana exige que las partes obligadas hagan lo siguiente:

- congelación de fondos y recursos económicos de determinadas personas incluidas en listas de la UE;
- informar a la Unidad de Inteligencia Financiera (UIF) de las medidas aplicadas para el congelamiento de fondos, o a la Unidad Especial de Policía Monetaria de la Guardia di Finanza (Policía Financiera) en caso de recursos económicos;
- informar a la UIF sobre transacciones sospechosas, relaciones comerciales y cualquier otra información disponible sobre partes incluidas en las listas negras publicadas por la propia UIF;
- informar transacciones sospechosas que, sobre la base de la información disponible, estén directa o indirectamente relacionadas con actividades de financiación del terrorismo.

Con respecto a las sanciones internacionales (los llamados embargos) y la exposición a medidas restrictivas, la legislación exige que se tomen ciertas medidas, que incluyen, entre otras:

- datos personales y controles transaccionales sobre operaciones relacionadas con importaciones y/o exportaciones realizadas por clientes, destinados a bloquear importaciones/exportaciones desde o hacia un país, y regulaciones correspondientes. La prohibición puede ser general, afectando a todo tipo de productos a menos que esté específicamente autorizada, o restringida a ciertos tipos de productos, p. armamentos (consulte el código aduanero);
- restricciones totales o parciales a las transferencias financieras desde/hacia un País;
- requisito de autorización previa para realizar traslados;
- obligación de notificar transferencias (salientes o entrantes);
- prohibición de financiar, proporcionar asistencia financiera o poner préstamos subsidiados a disposición del Gobierno (directa o, en algunos casos, indirectamente a través de empresas afiliadas o participación en instituciones financieras internacionales);
- prohibición de financiar a clientes que operan con países sancionados;
- implementación de medidas restrictivas contra súbditos rusos y bielorrusos;
- la trazabilidad de los controles realizados sobre operaciones provenientes o dirigidas a países, personas y entidades sujetas a restricciones.

3.2 - DEBIDA DILIGENCIA DEL CLIENTE

3.2.1 – Aspectos generales

La Compañía adopta todas las medidas de debida diligencia con el cliente cuando:

- establecer relaciones comerciales;

- realizar transacciones ocasionales, concertadas por los clientes, tales como transferencias electrónicas u otras transacciones iguales o superiores al umbral designado aplicable, independientemente de que la transacción se realice en una sola operación o en varias operaciones relacionadas o que consista en una transferencia de fondos, excediendo los límites legales;

- existe una sospecha de lavado de dinero o financiamiento del terrorismo, independientemente de cualquier excepción, exención o umbral designado que pueda aplicarse;
- existen dudas sobre la integridad, confiabilidad y veracidad de la información o documentación previamente adquirida con el fin de identificar a un Cliente.

Obligaciones de diligencia debida:

- se cumplen:
 - hacia nuevos clientes antes del establecimiento de una relación continua o de la ejecución de una transacción ocasional;
 - hacia clientes existentes, siempre que la debida diligencia sea apropiada a la luz de un cambio en el nivel de riesgo de lavado de dinero o financiamiento del terrorismo asociado con el cliente o cuando existan sospechas o dudas en cuanto a la exactitud o adecuación de la información obtenida previamente del cliente;
- y constan de las siguientes actividades:
 - identificar al Cliente, al beneficiario final y al ejecutor y verificar su identidad sobre la base de documentos, datos o información obtenidos de una fuente confiable e independiente;
 - obtener y evaluar información sobre el propósito y la naturaleza prevista de la relación comercial;
 - realizando un seguimiento continuo durante toda la duración de la relación con el cliente.

Para este fin, la Compañía - a través de sus empleados y/o a través de agentes/asesores financieros autorizados para realizar ofertas fuera de las instalaciones y que entran en contacto directo con el Cliente- obtiene la información requerida por la normativa y recopila cualquier otra documentación relevante según lo especificado en esta Política y en los documentos procesales de la Compañía.

La Sociedad aplica medidas de debida diligencia con el cliente ordinarias, simplificadas o mejoradas según el enfoque basado en el riesgo aplicado a los clientes.

3.2.2 - Incorporación remota de clientes

En los casos en que la Compañía utilice métodos de identificación remota según lo permitido por el Decreto Legislativo n. 231/07, artículo 19(1)(a)(2) y (5), adopta procedimientos especiales para el cumplimiento de sus obligaciones de diligencia debida, también en vista del riesgo de fraude asociado con el robo de identidad. En este caso, la identificación se basa en la adquisición del certificado cualificado de firma electrónica, que se genera tras un proceso de identificación realizado a través de:

- el uso del Sistema Público de Identidad Digital (SPID) o Cédula de Identidad Electrónica;
- mediante técnicas y procedimientos de identificación electrónica seguros y regulados, autorizados o reconocidos por la Agencia para la Italia Digital.

En todos los casos, el proceso de identificación a distancia implica la recopilación de los datos de identificación del cliente y de su posible ejecutor en formato electrónico, así como la

realización de verificaciones y controles de autenticidad de los datos, además de los previstos para la identificación presencial, según un enfoque basado en el riesgo, incluso mediante contacto telefónico en un número certificado (llamada de bienvenida) o una transferencia de dinero realizada por el cliente a través de un intermediario bancario y financiero con sede en Italia.

Con el fin de limitar la exposición a posibles riesgos de blanqueo de capitales y/o fraude, no está permitido establecer relaciones bancarias a distancia con personas jurídicas o personas físicas que actúen en nombre de una entidad jurídica, a menos que hayan sido identificadas personalmente (cara a cara).

No se permite el establecimiento de relaciones bancarias a distancia con clientes que no sean residentes en Italia.

3.2.3 – Evaluación Pre-Implementación y seguimiento continuo de los procesos de apertura de relaciones remotas.

Los procesos de identificación e incorporación remota de clientes están formalizados y detallados en la normativa interna. El modelo para supervisar estos procesos incluye:

- I. la evaluación preliminar de la solución de incorporación remota (la llamada evaluación previa a la implementación)⁸) dirigido a:
 - (i) evaluar la idoneidad de la solución en términos de integridad y exactitud de los datos y documentos a recopilar, así como la confiabilidad e independencia de las fuentes de información utilizadas;
 - (ii) evaluar el impacto del uso de la solución en los riesgos comerciales, incluidos los riesgos operativos, reputacionales y legales, mediante la participación de las funciones técnicas y especializadas pertinentes;
 - (iii) identificar medidas de mitigación y acciones correctivas para cada riesgo identificado;
 - (iv) definir pruebas ex ante para evaluar los riesgos de fraude y TIC y pruebas finales sobre el funcionamiento de la solución.
- II. seguimiento continuo de la solución de incorporación adoptada a través de controles periódicos y basados en eventos para garantizar su correcto funcionamiento en el tiempo (el llamado seguimiento continuo).
- III. la revisión de la evaluación preliminar en la solución de onboarding remoto (la llamada Evaluación Pre-Implementación) cuando se producen cambios estructurales en la solución adoptada o se producen ciertos eventos tales como:
 - (i) cambios en la exposición a riesgos en las áreas de lucha contra el blanqueo de capitales y la financiación del terrorismo, así como embargos;
 - ii) deficiencias detectadas para que nuestra solución funcione;
 - iii) un aumento de los intentos de fraude;
 - (iv) cambios en la legislación.

3.2.4 – Obligaciones de diligencia debida simplificadas

Generalmente, la Compañía utiliza un enfoque basado en el riesgo para identificar los tipos de clientes a quienes se pueden aplicar medidas simplificadas de diligencia debida. Esto incluye los casos en los que están presentes "indicadores de bajo riesgo", como se indica en el Anexo 1 de la Disposición del Banco de Italia sobre la diligencia debida del cliente del 30 de julio de 2019 (en adelante, "La Disposición").

⁸ Nota n.º 32 de 13 de junio de 2023, mediante la cual el Banco de Italia declaró su intención de cumplir las Directrices de la EBA (EBA/GL/2022/15) sobre el uso de soluciones remotas de incorporación de clientes.

Los "indicadores de bajo riesgo" relevantes para aplicar un procedimiento de diligencia debida simplificada se basan en el tipo de cliente, ejecutor o beneficiario real, el área geográfica de residencia o en la que está establecida la oficina central, el producto, servicio o canal de distribución específico.

En detalle, los tipos de clientes considerados con bajo riesgo de lavado de dinero, a los que se les puede aplicar la debida diligencia simplificada, incluyen:

- Administraciones públicas, Instituciones u Organismos que desempeñen funciones públicas, de conformidad con el Derecho de la Unión Europea;
- Empresas que cotizan en un mercado regulado y están sujetas a requisitos de divulgación, incluida la garantía de una transparencia adecuada del beneficiario final;
- las instituciones financieras y de crédito de la Comunidad Europea enumeradas en el artículo 3 (2) del Decreto contra el blanqueo de capitales, excepto las que figuran en las letras i), o), s), v)⁹— y las entidades financieras y de crédito residentes en Estados miembros o terceros países que dispongan de sistemas eficaces de blanqueo de capitales y financiación del terrorismo;
- Clientes, ejecutores o beneficiarios reales residentes o establecidos en zonas geográficas con bajo riesgo de blanqueo de capitales.

La Sociedad no aplica medidas simplificadas de debida diligencia con el cliente cuando:

- surgen dudas, incertidumbres o inconsistencias con respecto a los datos de identificación y la información recopilada durante la identificación del cliente, albacea o beneficiario final;
- ya no se cumplen las condiciones para la debida diligencia simplificada con el cliente sobre la base de los indicadores de riesgo previstos por el decreto contra el blanqueo de capitales y la normativa secundaria pertinente;
- el seguimiento de las operaciones globales realizadas por el cliente y la información recopilada a lo largo de la relación excluyen un tipo de riesgo bajo;
- sigue surgiendo la sospecha de blanqueo de capitales o financiación del terrorismo.

La Función Antilavado de Dinero tiene la responsabilidad exclusiva de la evaluación y autorización de medidas simplificadas de diligencia debida del cliente, llevadas a cabo siguiendo todos los pasos requeridos para el proceso ordinario de diligencia debida del cliente, incluida la obligación de identificar y verificar la identidad del cliente, el albacea y el beneficiario final, y adquirir todos los datos y documentos necesarios para su registro completo (por ejemplo, nombre, estatus legal, domicilio social y, cuando corresponda, código tributario), aunque reduciendo su nivel de profundidad, alcance y frecuencia.

3.2.5 – Obligaciones de debida diligencia mejoradas

La Compañía aplica medidas reforzadas de debida diligencia con el cliente en presencia de clientes o situaciones con mayor riesgo de lavado de dinero o financiamiento del terrorismo y en todos los casos a que se refiere el artículo 24 del Decreto. Estas medidas reforzadas incluyen, entre otras cosas, la participación de roles de responsabilidad proporcionales al nivel de riesgo identificado en relación con el cliente.

9 i) los corredores de bolsa a que se refiere el artículo 201 del TUF; o) los intermediarios de seguros a que se refiere el artículo 109, apartado 2, letras a), b) y d), de la PAC, que operen en las ramas de actividad a que se refiere el artículo 2, apartado 1, de la PAC; s) sociedades fiduciarias inscritas en el registro establecido conforme al artículo 106 del TUB; v) los asesores financieros a que se refiere el artículo 18-bis del TUF y las empresas de consultoría financiera a que se refiere el artículo 18-ter del TUF.

Respecto a los clientes de banca privada, la Sociedad evalúa los factores de riesgo específicos inherentes a la naturaleza de su negocio y aplica medidas reforzadas de debida diligencia basadas en la información global disponible y las evaluaciones realizadas.

Se requiere la intervención de la Función de Prevención de Blanqueo de Capitales en los siguientes casos:

- las personas físicas y jurídicas incluidas en las listas de personas o entidades sujetas a medidas de congelación de fondos en virtud de reglamentos o decretos europeos en virtud del Decreto Legislativo 109/07, así como las personas estrechamente asociadas a ellas;
- una relación de banca corresponsal transfronteriza establecida con un banco o una institución ubicada en un tercer país, basada en factores geográficos de alto riesgo (como se indica en el Anexo 2 de las disposiciones del Banco de Italia sobre debida diligencia del cliente);
- relaciones o transacciones en las que el cliente o el beneficiario final es una persona políticamente expuesta¹⁰;
- situaciones que involucren elementos de riesgo que requieran la aplicación de medidas específicas de confidencialidad;
- situación de mayor riesgo de lavado de dinero o financiamiento del terrorismo por contingencias objetivas, ambientales o subjetivas;
- clientes clasificados como "Fiduciarios", servicios de Transferencia de Dinero y Casas de Cambio Virtuales;
- Sociedades Fiduciarias, salvo lo dispuesto en el numeral 3.4;

Asimismo, antes de iniciar, continuar o mantener una relación en curso con Personas Expuestas Políticamente o Entidades Correspondientes de terceros países, es necesario obtener la autorización correspondiente del Gerente General o su delegado, previa opinión de la Función Antilavado de Dinero. En el caso de los delegados conforme al artículo 25 del Decreto Legislativo 231/07 pertenecientes a la Función Antilavado de Dinero, esta autorización se incluye en el proceso de debida diligencia reforzada.

En todos los demás casos, la aplicación de medidas reforzadas será proporcional al nivel de riesgo atribuido al cliente. Si el riesgo se considera medio/alto, o si determinados factores de riesgo están presentes independientemente de la puntuación asignada, se requiere la implicación del Responsable de la unidad de negocio responsable de la gestión comercial del cliente.

Ejemplos de tales casos son:

- clientes personas jurídicas con un Ejecutor identificado como PEP o PEP indirecta, independientemente del perfil de riesgo;
- servicios ofrecidos a través de redes de agentes financieros, asesores financieros, contratistas y agentes;
- clientes clasificados como Fundación/Organizaciones sin fines de lucro;
- clientes personas jurídicas durante la fase de incorporación;
- clientes con noticias negativas durante la fase de onboarding ("Noticias adversas");

¹⁰ Personas Políticamente Expuestas (PEP): según lo enumerado por el art. 1, párrafo 2, letra dd) Decreto Legislativo 231/07.

- clientes que residen o están basados en terceros países de alto riesgo o en el caso de relaciones continuas, servicios profesionales y operaciones que involucran países de alto riesgo;
- empresas que hayan emitido acciones al portador o que tengan dentro de su estructura de cadena de control una empresa emisora de acciones al portador;
- relaciones o transacciones en las que el cliente y el beneficiario final desempeñan un cargo público distinto de los enumerados para personas políticamente expuestas¹¹;
- empresas propiedad de Fideicomisos, Sociedades Fiduciarias, Fundaciones, sociedades anónimas a través de múltiples niveles de participación o tenencias cruzadas;
- Clientes que participan en un tipo de actividad económica particularmente expuesta al riesgo de blanqueo de capitales o en sectores de actividad "controvertidos".¹²
actividades comerciales que requieren un uso intensivo de efectivo, como dinero por oro, cambio de moneda, juegos de azar/apuestas, incluso en línea, industria armamentística, minería, recogida y eliminación de residuos, producción de energía renovable, empresas que operan en el sector de criptoactivos, construcción, adquisición de instrumentos farmacéuticos;
- clientes que participan en contratos públicos o reciben financiación pública (atención sanitaria, construcción, recogida y eliminación de residuos, producción de energía renovable, minería, suministro de instrumentos farmacéuticos);
- en los casos de clientes que hayan adquirido la ciudadanía de un Estado miembro u obtenido derechos de residencia en un Estado miembro (UE) a través de un programa de ciudadanía por inversión o un programa de residencia por inversión;
- en los casos de clientes entidades jurídicas residentes en un país de la UE, donde los derechos de propiedad de la empresa pertenecen, directa o indirectamente, en más del 40% a una entidad jurídica, organización u organismo establecido en Rusia, o a una persona física con residencia o ciudadanía rusa.

También se requiere la implicación del Responsable de la unidad de negocio responsable de la gestión comercial del cliente en caso de que se produzcan errores informáticos que puedan impedir el cálculo en tiempo real del riesgo de blanqueo del cliente.

Las medidas mejoradas de debida diligencia incluyen adquirir información adicional sobre el cliente, el ejecutor y el beneficiario final, investigar el propósito y la naturaleza de la relación y aumentar la frecuencia de los procedimientos destinados a garantizar un seguimiento continuo durante la relación en curso.

En pleno cumplimiento de la legislación vigente y de las disposiciones de los procedimientos internos en materia de Lucha contra el Lavado de Dinero y la Financiación del Terrorismo y en línea con el Código de Ética de la Compañía, la Compañía no apoya transacciones con clientes que operan en sectores controvertidos que

(i) no cumplen con la legislación nacional vigente y (ii) no están, cuando corresponda, autorizados previamente por las autoridades nacionales italianas competentes, en particular:

- la producción, tránsito y/o comercialización de materiales de armamento;
- la producción y venta de marihuana light, lugares de entretenimiento para adultos;

¹¹ Cargos públicos distintos de los desempeñados por Personas Expuestas Políticamente (PEP) a que se refiere la nota 1), aplicándose a todos aquellos que desempeñen cargos en, entre otros, organismos públicos, consorcios, asociaciones de carácter público enumerados en el apartado A 8) del Anexo 2 de la Disposición.

¹² un sector económico es "controvertido" si los bienes/servicios fabricados/ofrecidos y/o las formas en que se producen/ofrecen contrastan con los valores ampliamente compartidos de ética y sostenibilidad, incluso cuando los servicios o actividades son legales y, por lo tanto, no contrastan con las obligaciones legales.

- actividades comerciales que requieren un uso intensivo de efectivo distintas de las enumeradas anteriormente, como organizaciones benéficas y ONG no reguladas, la producción de metales y piedras preciosas, y remesas de dinero.

Además, la Compañía presta especial atención al cumplimiento de las medidas restrictivas implementadas por el Estado italiano, organismos extranjeros (por ejemplo, OFAC, UKSL) y/o organismos supranacionales (ONU, UE). Estas medidas pueden ser de naturaleza comercial (por ejemplo, bloqueo de importaciones/exportaciones) o de naturaleza financiera, como bloqueo parcial/total de transferencias de dinero desde o hacia un país específico o limitaciones a las operaciones y/o congelación de fondos mantenidos en intermediarios financieros.

Para cumplir con las obligaciones establecidas en el Decreto Legislativo italiano 109/07 - destinado a prevenir y combatir la financiación del terrorismo y las actividades de los Países que amenazan la paz y la seguridad internacionales, mediante la aplicación de medidas restrictivas para "congelar" fondos y recursos económicos en poder de personas físicas y jurídicas, grupos y entidades específicamente identificados por las Naciones Unidas y la Unión Europea ("sujetos designados") - y las obligaciones de diligencia debida reforzada establecidas en el Decreto Legislativo italiano 231/07, la Compañía ha adoptado medidas automáticas procedimientos de control. Estos procedimientos son capaces de verificar la coherencia entre los datos de identificación del cliente obtenidos a través del proceso de diligencia debida y los contenidos en las listas elaboradas por la UE y otras instituciones y organismos internacionales, tales como:

- las personas que tengan encomendado un cargo público destacado o que hayan cesado en su cargo por menos de un año (PEP), sus familiares y quienes tengan con ellos estrechos vínculos según la definición del art. 1 c. 2 letra dd del Decreto Legislativo 231/07 (PEP residentes y no residentes);
- personas residentes en Italia que ocupan cargos públicos, que no entran dentro de la definición de PEP, pero que, sin embargo, están expuestas a un riesgo significativo de corrupción y lavado de dinero;
- personas físicas y jurídicas que operan, incluso parcialmente, en Estados que no imponen medidas y reglamentaciones equivalentes, según las directrices del Banco de Italia u otras instituciones nacionales o supranacionales dedicadas a la prevención del delito;
- personas físicas y jurídicas sujetas a medidas de embargo o congelación de fondos/recursos económicos y activos financieros (Listas de Sanciones ONU, UE, UKSL, OFAC).

3.3 - PERFIL DEL CLIENTE

La Sociedad adopta procedimientos adecuados destinados a definir el perfil de riesgo (PR) de blanqueo de capitales y financiación del terrorismo atribuible a cada cliente, basándose en la información adquirida y los análisis realizados, con referencia tanto a los elementos de evaluación indicados en la Disposición como a otros elementos que la propia Sociedad pueda adoptar a lo largo del tiempo (el llamado perfil).

Sobre la base de la elaboración de perfiles de clientes, que también se realiza periódicamente, la Compañía aplica medidas estándar o mejoradas, que incluyen la participación de roles de responsabilidad proporcionales al nivel de riesgo identificado del cliente. Se requiere la opinión

previa de la Función Antilavado de Dinero de conformidad con las responsabilidades establecidas en el documento interno "Procedimientos Internos Antilavado de Dinero y Financiamiento del Terrorismo".

La clasificación de clientes para debida diligencia simplificada es autorizada por la Función Antilavado de Dinero, a solicitud del Jefe de la Unidad Operativa de Negocio.

En tal caso, el alcance y la frecuencia de los requisitos se reducen, y la verificación expira después de ocho años, independientemente de la puntuación de riesgo, a menos que ya no se cumplan las condiciones para aplicar la diligencia debida simplificada.

Además, la Compañía ha implementado un procedimiento de TI para evaluar el perfil de riesgo del cliente y definir consistentemente un marco de tiempo de reevaluación apropiado al nivel de riesgo calculado; la frecuencia de la reevaluación depende del proceso identificado en la última evaluación realizada o, en ausencia de un cuestionario KYC, del perfil de riesgo del cliente, como se especifica a continuación:

Clase de riesgo (RP)	Puntuación	Proceso de diligencia debida	Función de validación	Frecuencia de reevaluación
Cientes clasificados como sujetos a debida diligencia simplificada	NA	simplificado	Aceptación automática/Gerente de Unidad de Negocio (*)	8 años
Inmaterial	<=5	Estándar	Aceptación automática	8 años
Bajo	>=6 y <=12			6 años
Medio	>=13 y <=24	Mejorado	Gerente de Unidad de Negocio (**)	2 años
Alto	>=25			1 año
En el caso de elementos de riesgo específicos (***)		Mejorado	Función de validación AML	1 año

(*) proporcionado si la puntuación de riesgo calculada o resultante del KYC realizado es al menos media. (**) proporcionado incluso en presencia de elementos de riesgo definidos que mantengan el perfil de riesgo por debajo del medio.

(***) proporcionados incluso en presencia de Personas Jurídicas con RP >39, si realizan actividades comerciales relacionadas con la compra de oro, juegos y apuestas y recolección y eliminación de desechos (códigos ATECO de alto riesgo) y/o si están sujetos a auditorías/investigaciones.

3.4 - HERRAMIENTAS PARA APOYAR LA DILIGENCIA DEBIDA

La Compañía ha implementado herramientas tecnológicamente avanzadas para apoyar los procesos contra el lavado de dinero, además de las aplicaciones tradicionales ya en uso:

- Automatización Robótica de Procesos (RPA) aplicada a actividades de recopilación de datos en las áreas de debida diligencia del cliente y reporte de transacciones sospechosas;
- Motor de Inteligencia Artificial, basado en componentes estadísticos e indicadores predictivos (Predict Index AML, Reputational Index e Criminal Infiltración Index) construidos con técnicas de Data Analytics, aplicados al proceso regular de revisión de clientes;
- Plataforma de inteligencia Cogito, aplicación utilizada para recopilar noticias, documentos e información textual para buscar noticias adversas sobre clientes sujetos a due diligence;
- Rozes, una herramienta de inteligencia de datos que, a partir del análisis de estados

financieros en tiempo real, permite identificar empresas cuyo balance e indicadores financieros son similares a los de empresas sometidas a infiltración criminal.

Además, en el ámbito de las herramientas avanzadas mencionadas anteriormente, se han identificado ciertos "eventos desencadenantes", destinados a interceptar eventos relacionados con el cliente y/o relaciones relacionadas, determinando una variación en la fecha de vencimiento de la "Evaluación del Cliente - KYC", por ejemplo:

- en caso de cambios en los datos registrales del beneficiario real y del representante legal;
- en caso de cambio en el Perfil de Riesgo debido a la presencia de ciertos factores de alto riesgo entre los previstos por la Disposición;
- en caso de que un beneficiario efectivo asuma el rol de PEP, o el registro de un nuevo beneficiario efectivo de PEP;
- en caso de delegación a una persona física de la relación de cliente otorgada a una persona calificada como PEP;
- en caso de discrepancia entre el beneficiario efectivo inscrito en el registro y las pruebas recabadas de los extractos de la Cámara de Comercio;
- en caso de controles de segundo nivel por parte de la Función AML.

La responsabilidad del proceso de diligencia debida de un cliente recae en la unidad de gestión de relaciones del cliente, que normalmente se encarga del establecimiento de nuevas relaciones continuas, ejecuta transacciones ocasionales, reevalúa periódicamente a los clientes existentes y garantiza un seguimiento continuo de la relación con el cliente.

3.5 - OBLIGACIONES DE ABSTENERSE

La Compañía se abstiene de establecer, ejecutar o continuar la relación, operaciones y servicios profesionales (la llamada obligación de abstención) en caso de imposibilidad objetiva de realizar la debida diligencia con el cliente, evaluando si debe reportar una transacción sospechosa a la UIF.

En aquellos casos en los que no sea posible la abstención, por existir una obligación legal de ejecutar la operación inaplazable o si su negativa pudiera entorpecer la investigación, la Sociedad está igualmente obligada a informar inmediatamente de la operación sospechosa.

Además, si después de una evaluación adicional o del proceso de debida diligencia mejorada, surgen elementos de alto riesgo que podrían afectar el perfil legal y/o reputacional de la Compañía, la Compañía se reserva el derecho de limitar o terminar la relación comercial con el cliente. Estas limitaciones pueden referirse, por ejemplo, al acceso del cliente a ciertos tipos de productos o resultar en la interrupción de los servicios ofrecidos por la Compañía en relación con la cuenta/relación.

Sin embargo, las medidas de debida diligencia con los clientes adoptadas por la Sociedad no excluyen/niegan el acceso a los servicios financieros a clientes o a categorías enteras de clientes de alto riesgo que tendrían derecho a ellos según la legislación vigente, salvo en los casos expresamente previstos por el Decreto Legislativo 231/07, sobre prohibición de mantener relaciones con determinados tipos de entidades.

La Compañía no establece una relación de corresponsalía con un banco pantalla y se abstiene de establecer relaciones con entidades que permitan el acceso a relaciones de corresponsalía con un banco pantalla. No entablará una relación comercial con entidades cuya estructura de propiedad (corporativa, fiscal y financiera) se caracterice por un alto grado de opacidad que impida la identificación clara del beneficiario final o de la naturaleza y propósito de la estructura.

Con este fin, la Compañía toma todas las medidas para garantizar que no colabora deliberada y conscientemente con instituciones financieras que a su vez operan con bancos pantalla.

Además, la Compañía se abstiene de entablar o continuar una relación comercial con personas particularmente expuestas al riesgo de lavado de dinero/financiación del terrorismo, tales como:

- Sociedades fiduciarias que tengan su domicilio social en un país indicado por el GAFI como de mayor riesgo de lavado de dinero o que no adopten medidas consistentes con las obligaciones impuestas por el Decreto Legislativo 231/07 o las Directivas Europeas;
- Fideicomisos para los cuales no se dispone de información adecuada, precisa y actualizada sobre el beneficiario final del fideicomiso y su naturaleza y propósito;
- Sociedades de apuestas, incluidos los juegos de azar en línea, los casinos y los operadores de bingo, para los que no se hayan expedido y/o verificado las autorizaciones y/o licencias exigidas por la legislación italiana e internacional;
- Entidades afiliadas y agentes de proveedores de servicios de pago (referidos en la definición del art.1 c. 2 letra nn) y entidades de dinero electrónico que no cumplan con lo dispuesto en el Capítulo V del Decreto Legislativo 231/07 en los artículos 43 y siguientes;
- Sociedades de responsabilidad limitada o sociedades controladas mediante acciones al portador, con sede en Países de alto riesgo;
- Clientes que operen en la producción y venta de marihuana light o lugares de entretenimiento para adultos, si no puede verificar las autorizaciones requeridas por la ley.

La Compañía utiliza toda la información adquirida durante el proceso de debida diligencia sobre sus clientes y sus transacciones para determinar si una transacción o relación comercial está, directa o indirectamente, vinculada con personas o entidades involucradas en el lavado de dinero, financiamiento del terrorismo o en el desarrollo de armas de destrucción masiva, y de ninguna manera apoya transacciones que involucren armas controvertidas y/o prohibidas por tratados internacionales.

por ej. armas nucleares, biológicas y químicas, bombas de racimo, armas que contienen uranio empobrecido, minas terrestres antipersonal.

Respecto a la producción, tránsito y/o comercialización de materiales de armamento distintos a los mencionados anteriormente, la Compañía podrá respaldar transacciones que hayan sido debidamente autorizadas por las autoridades competentes y cumplan con la legislación aplicable y vigente.

3.6 – INFORME DE OPERACIONES SOSPECHOSAS

Cuando la Compañía sospeche o tenga motivos razonables para sospechar que se ha realizado o se está realizando o intentando una operación de lavado de dinero o financiamiento del terrorismo:

- presenta un informe de transacción sospechosa a la Unidad de Inteligencia Financiera (UIF), si la transacción tiene su sede en Italia;

- si la transacción tiene su sede en otro País, cumple con las disposiciones de la legislación local y, cuando ésta prevea la aplicación de medidas equivalentes a las establecidas por la legislación de la UE, informa inmediatamente al Responsable de Lucha contra el Blanqueo de Capitales, tomando todas las precauciones necesarias para proteger la identidad de las personas que informan de la transacción sospechosa.

La Compañía ha implementado procedimientos y procesos para monitorear, identificar y reportar actividades sospechosas de acuerdo con los tiempos y métodos requeridos por la ley aplicable.

Los empleados informan oportunamente cualquier conocimiento o sospecha de lavado de dinero, financiamiento del terrorismo u otras actividades delictivas, o producto de actividades delictivas, independientemente de su tamaño, de acuerdo con el modelo organizacional actualizado y los modos de operación previstos en la normativa interna de referencia. Hasta que se complete el proceso de información, la Compañía se abstiene de ejecutar la transacción, a menos que sea imposible por existir una obligación legal de aceptar la escritura o la ejecución de la operación no pueda posponerse por el normal desarrollo de los negocios o cuando pueda obstruir las investigaciones. En estos casos, el informe se presenta inmediatamente después de que se haya ejecutado la transacción.

Los motivos de sospecha incluyen las características, escala y naturaleza de la transacción, el intento de dividir la transacción y cualquier otra circunstancia que llegue a conocimiento de los empleados como resultado de sus funciones, teniendo también en cuenta el alcance financiero y la naturaleza del negocio realizado por el sujeto de la transacción sospechosa, basándose en los elementos adquiridos de conformidad con la legislación contra el lavado de dinero (por ejemplo, durante la diligencia debida).

Para limitar el riesgo de participación de la Compañía, incluso si no es intencional, en las actividades ilegales mencionadas anteriormente, se activa un proceso de debida diligencia mejorada en los acuerdos de transferencia de fondos donde los actores involucrados en este tipo de transacción (originador, beneficiario, los bancos involucrados en la transferencia de fondos) pueden dar lugar a sospechas de lavado de dinero, financiamiento del terrorismo o violaciones de las restricciones internacionales aplicables a ciertos bienes, personas o entidades.

Después del proceso de información, la Compañía puede limitar y/o interrumpir la relación comercial con los clientes, en particular cuando dicha relación pueda constituir un riesgo legal o reputacional significativo para Rox Pay S.r.l.

3.7 – CONSERVACIÓN DE DATOS

La Compañía conserva todos los documentos y registra todos los datos obtenidos a través del proceso de debida diligencia del cliente, asegurando la trazabilidad de las transacciones de los clientes para facilitar las funciones de control del Banco de Italia y la UIF, incluidas las inspecciones.

Para ello, Rox Pay S.r.l., como intermediario financiero con sede en Italia, creó un Archivo Electrónico Único (Archivo Unico Informatico o AUI) que le permite proporcionar información al Banco de Italia y a la UIF de acuerdo con las normas técnicas especificadas en el Anexo 2 de las Disposiciones sobre retención de datos. Este archivo almacena electrónicamente todos los datos de identificación y otra información relacionada con las relaciones comerciales en curso y

las transacciones de los clientes según lo exige la ley aplicable.

En este sentido, en respuesta a las recientes actualizaciones introducidas por las "Disposiciones sobre Retención de Datos y Acceso a Documentos, Datos e Información" y las "Disposiciones sobre Transmisión de Datos Agregados", la Compañía ha decidido adoptar ciertos principios para la exención de las obligaciones de registro según lo expresamente previsto. En particular, los datos y la información sobre operaciones realizadas por intermediarios bancarios y financieros, que se encuentren en los casos previstos en el artículo

8 de las Disposiciones sobre Conservación de Datos y el artículo 3 de las Disposiciones sobre Datos Agregados no quedan registrados en el Archivo Único Electrónico.

En cuanto a los requisitos de diligencia debida del cliente, la Compañía conserva copias o registros de todos los documentos requeridos durante un período de diez años después de que finalice la relación comercial.

En cuanto a las transacciones y relaciones comerciales en curso, todas las pruebas y registros de respaldo, por ejemplo, documentos originales o copias admisibles en procedimientos judiciales, se conservan durante un período de diez años después de la ejecución de la transacción o después de que haya terminado la relación comercial.

3.8 – PREVENCIÓN REGARGINA MEDIDAS RESTRICTIVAS

Dada la naturaleza, tamaño y complejidad de su negocio, así como la gama y tipo de servicios prestados, la Compañía está expuesta al riesgo de violar medidas restrictivas.

Con el fin de mantener un sistema organizativo y procesal destinado a garantizar el cumplimiento de las medidas restrictivas internacionales nacionales y de la UE, la Función Antiblanqueo evalúa el riesgo de incumplimiento de las medidas restrictivas en función de factores geográficos, de clientes, de productos/servicios y del canal de distribución, garantizando un seguimiento constante de la eficacia del sistema, garantizado también mediante la realización periódica de un ejercicio de autoevaluación, que permite identificar posibles acciones correctivas en respuesta a la detección de problemas críticos existentes y/o la adopción de medidas adecuadas de prevención de riesgos y medidas de mitigación.

La Compañía ha establecido procedimientos y procesos para monitorear, identificar y reportar actividades que violen las medidas restrictivas, con tiempos y métodos consistentes con los requisitos legales.

Los controles existentes sobre personas/entidades y transacciones se llevan a cabo a través de un proceso de selección automatizado, que se realiza tanto diariamente como durante la fase de incorporación, mediante el uso de listas específicas, actualizadas dos veces al día, sobre clientes, contrapartes, países y transacciones.

Existen procesos para monitorear los flujos entrantes o salientes con países y/o entidades sujetos a sanciones financieras internacionales, con responsabilidades definidas entre los departamentos competentes.

Se garantiza que el personal esté adecuadamente capacitado y sea consciente de las políticas, procedimientos y controles para cumplir con las medidas restrictivas.

4 – LISTA DE PROCESOS CLAVE

4.1 – GESTIÓN DE RIESGOS DE LAVADO DE DINERO Y FINANCIACIÓN DEL TERRORISMO

El proceso de “Gestión del Riesgo de Lavado de Activos y Financiamiento del Terrorismo” es el proceso mediante el cual se llevan a cabo las siguientes actividades dentro de la Compañía con el fin de mitigar el riesgo de incumplimiento de los requisitos contra el lavado de activos y el

financiamiento del terrorismo:

- Identificar el riesgo de incumplimiento de los requisitos ALD-CFT a través de la supervisión continua de los cambios en la legislación y la evaluación de los impactos en los procesos y procedimientos comerciales, así como la identificación y evaluación de riesgos ALD-CFT utilizando un enfoque basado en riesgos;

- Gestión y mitigación del riesgo de lavado de dinero y financiamiento del terrorismo mediante la implementación y monitoreo de acciones de mitigación del riesgo de incumplimiento establecidas en el Plan Anual (Plan AML) o identificadas por el Gobierno de la Compañía según las aplican todas las funciones comerciales relevantes en la implementación de procedimientos (regulaciones internas, aplicaciones de TI, procesos operativos, controles);
- Controles de cumplimiento (ex-ante y ex-post) en las áreas regulatorias asignadas por la titularidad mediante la definición y seguimiento de indicadores de riesgo y su evolución en el tiempo. El objetivo es encontrar posibles situaciones de incumplimiento así como realizar las actividades de control ex ante y ex post;
- Brindar asesoría y apoyo en temas ALA/CFT, participando en equipos de trabajo multifuncionales y brindando apoyo ya sea a las estructuras empresariales o a los Órganos de Alta Dirección en temas y procesos de negocios donde el riesgo de lavado de dinero y financiamiento del terrorismo sea relevante, realizando los cumplimientos previstos por las normas de supervisión y realizando una evaluación de conformidad preliminar en esta área al ofrecer nuevos productos/servicios;
- Monitoreo y control de riesgos ALD/CFT mediante el análisis de los flujos de información recibidos del Nivel I y otras funciones de control relacionadas con los requisitos operativos contra el lavado de dinero y mediante la implementación de controles de monitoreo de riesgos y la verificación constante de su idoneidad;
- Realizar una autoevaluación ALD mediante la realización de las actividades preliminares necesarias para completar los Cuestionarios denominados "Sistemáticos" y "Operativos", así como para determinar el riesgo residual;
- Informar a los órganos corporativos superiores y a las autoridades de control, más específicamente prepararse para informar anualmente a los órganos corporativos y al consejo de supervisión, así como prepararse para informar periódicamente sobre las actividades realizadas y cualquier solicitud específica de las autoridades de control;
- Proporcionar cursos de formación específicos ALD/CFT mediante la organización de un plan de formación adecuado junto con las demás funciones corporativas responsables de la formación. El objetivo es conseguir una formación continua de los empleados y colaboradores.

Las reglas y responsabilidades específicas de la Compañía respecto de este proceso se detallan en el reglamento interno.

documento "Procedimientos Internos contra el Lavado de Activos y la Financiación del Terrorismo".

4.2 – GESTIÓN DE LAS RELACIONES CON LAS AUTORIDADES DE SUPERVISIÓN PARA COMBATIR EL LAVADO DE ACTIVOS Y LA FINANCIACIÓN DEL TERRORISMO

El proceso de Gestión de Relaciones Regulatorias ALD/CFT es el proceso mediante el cual se llevan a cabo actividades dentro de la Compañía para gestionar, analizar, dirigir y monitorear todas las comunicaciones con los reguladores sobre asuntos relacionados con la lucha contra el lavado de dinero y el financiamiento del terrorismo. El objetivo es supervisar estas actividades, incluido el archivo de documentos en un repositorio único.

Como parte de este proceso se llevan a cabo las siguientes actividades:

- Gestión de las relaciones con las Autoridades de Control (Anti-Lavado de Dinero), gestionando, analizando y atendiendo las comunicaciones y solicitudes de las

Autoridades de Control en materia de conformidad en la materia;

- Gestión de informes de Supervisión contra el blanqueo de capitales, mediante la preparación del flujo y envío de informes de Supervisión contra el blanqueo de capitales;

- Tramitación de procedimientos administrativos relacionados con la lucha contra el lavado de dinero a través del examen de reconvenções relativas a procedimientos administrativos notificados a la Compañía por las autoridades competentes (GdF y UIF), así como representar a la Compañía ante el MEF, siendo responsable del censo de procedimientos en la solicitud correspondiente y de su imputación a la Provisión para Riesgos y Cargos y pago de posibles sanciones, en coordinación con la Función de Presupuesto.

Las normas y responsabilidades específicas de la Compañía respecto de este proceso se detallan en el documento interno "Procedimientos Internos Antilavado de Dinero y Financiamiento del Terrorismo".

4.3 – GESTIÓN DE REQUISITOS OPERACIONALES PARA COMBATIR EL LAVADO DE ACTIVOS Y LA FINANCIACIÓN DEL TERRORISMO

El proceso de Gestión de Requisitos Operativos ALA/CFT es el proceso mediante el cual se llevan a cabo las siguientes actividades dentro de la Compañía con el fin de cumplir con los requisitos regulatorios:

- limitar el uso de efectivo y valores al portador, mediante la aplicación de requisitos reglamentarios relativos a las limitaciones al uso de efectivo y bonos/valores al portador;
- gestionar las obligaciones adecuadas de diligencia debida del cliente, ejecutando las actividades de diligencia debida del cliente (o diligencia debida mejorada) en los casos establecidos por la ley italiana (Decreto Legislativo 231/07 y modificaciones posteriores) dependiendo del perfil de riesgo de los clientes, apoyando a la Red de la Compañía en el cumplimiento de las obligaciones requeridas por las leyes y regulaciones vigentes, y brindando soporte a las estructuras de la Compañía que gestionan las relaciones con los clientes y contrapartes bancarias y financieras para permitir el establecimiento y mantenimiento de relaciones;
- gestionar las obligaciones de notificación de operaciones sospechosas, realizando las actividades de notificación de operaciones sospechosas mediante la ejecución de las delegaciones de autoridad del Consejo de Administración (ex art. 36 Decreto Legislativo 231/07) y el seguimiento de las solicitudes recibidas de la UIF;
- gestionar las obligaciones relativas a la financiación del terrorismo, definiendo la metodología de control destinada a garantizar la aplicación de las medidas restrictivas nacionales y de la Unión, verificando la transposición de las actualizaciones de la Lista de Sanciones, así como informando a las autoridades competentes (nacionales y de supervisión) sobre las medidas restrictivas (UIF, MAECI y MEF) sobre las medidas de congelación de capital (ex Decreto Legislativo 109/07) y cumpliendo los requisitos operativos necesarios;
- gestionar las obligaciones de retención de datos, verificando la confiabilidad del Sistema de Información actualizando el Archivo Único Informático (AUI), realizando revisiones, enviando periódicamente datos agregados a la UIF y transmitiendo a la UIF y al Banco de Italia las notificaciones requeridas por la reglamentación;
- monitorear la implementación adecuada de las sanciones financieras internacionales (embargos financieros);
- monitoreo continuo de los clientes con mayor riesgo de lavado de dinero y financiamiento del terrorismo, monitoreando las solicitudes de investigación adicional de los clientes que potencialmente exponen a la Compañía a altos riesgos de lavado

de dinero, activando, cuando sea necesario, el proceso de evaluación de transacciones sospechosas y el proceso de selección de clientes que potencialmente exponen a la Compañía a altos riesgos de lavado de dinero.

Las reglas y responsabilidades específicas de la Compañía respecto de este proceso se detallan en el reglamento interno.

documento "Procedimientos Internos contra el Lavado de Activos y la Financiación del Terrorismo".

5 - MARCOS ORGANIZATIVOS Y ÓRGANOS DE CONTROL

Para gestionar eficazmente el riesgo de lavado de dinero y financiamiento del terrorismo, así como la violación de las Medidas Restrictivas, la Compañía ha identificado las funciones, recursos y procedimientos organizacionales que son consistentes y proporcionados con el tipo y tamaño de la actividad realizada, la complejidad organizacional así como las características operativas.

El seguimiento de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo está garantizado:

- por la Función Anti-Lavado de Dinero de Rox Pay S.r.l., cuya responsabilidad está asignada al Responsable de la Función ALD que reporta directamente al Consejero Delegado.
- Por el Miembro del órgano de administración responsable de la Lucha contra el Blanqueo de Capitales, con responsabilidad confiada al Director General, que es el principal punto de contacto entre el Responsable de la Función de Lucha contra el Blanqueo de Capitales y el Consejo de Administración y garantiza que el Consejo tenga la información necesaria para comprender plenamente la relevancia de los riesgos de blanqueo de dinero a los que Rox Pay S.r.l. está expuesto.

El seguimiento de los riesgos relacionados con la violación de Medidas Restrictivas:

- está asegurada por el Miembro Superior del Personal responsable de Medidas Restrictivas, cuya responsabilidad está asignada al Jefe del Departamento ALD, que supervisa la adecuación y eficacia de las políticas, procedimientos internos y controles relacionados con la gestión de Medidas Restrictivas, sanciones y embargos. El miembro superior del personal propone, en colaboración con las funciones pertinentes de la empresa, cambios organizativos y de procedimiento necesarios y/o apropiados para garantizar un seguimiento adecuado del riesgo de violación de medidas restrictivas, sanciones y embargos.

De acuerdo con la normativa vigente, la Sociedad ha establecido su estructura organizativa y su gobierno corporativo de manera que proteja los intereses de la Sociedad y, al mismo tiempo, garantice una gestión sana y prudente y evite el riesgo, incluso si no es intencionado.
- de cualquier implicación directa en actos de blanqueo de capitales y/o financiación del terrorismo.

Para ello, de acuerdo con el Sistema de Control Interno adoptado por la Sociedad, el Directorio y los Revisores Fiscales se involucran en la mitigación de los riesgos antes mencionados a través de tareas y responsabilidades claramente definidas.

Además, la Compañía ha establecido una unidad centralizada para la gestión del sistema interno de denuncia de infracciones, con la responsabilidad de supervisar las actividades de recepción, análisis y evaluación de las alertas enviadas por los empleados a través del procedimiento de Whistleblowing.

6 – REVISIÓN Y ACTUALIZACIÓN DE LA POLÍTICA

La Función Ant blanqueo revisa la política al menos una vez al año, la actualiza cuando sea necesario y prepara el texto para su aprobación por el Consejo de Administración a propuesta del Consejero Delegado.

Cualquier modificación de la Política aprobada por el Consejo de Administración de Rox Pay S.r.l. posteriormente se implementan en toda la Compañía por resolución de la alta dirección, alineando responsabilidades, procesos y normas internas.