DIRECTRICES DE CUMPLIMIENTO CONTRA EL BLANQUEO DE CAPITALES Y LA FINANCIACIÓN DEL TERRORISMO

INTRODUCCIÓN

El objetivo de estas Directrices para la lucha contra el blanqueo de capitales (AML), la financiación del terrorismo (CFT) y las medidas sancionadoras es garantizar que **UAB Criptomy** (Empresa) disponga de directrices internas para evitar el uso de su negocio para el blanqueo de capitales y la financiación del terrorismo y de directrices internas para la aplicación de sanciones internacionales.

Estas Directrices se han adoptado para garantizar que la Empresa cumpla con las normas y reglamentos establecidos en la Ley de la República de Lituania sobre la Prevención del Blanqueo de Dinero y la Financiación del Terrorismo (Ley) y demás legislación aplicable, incluida la siguiente:

- Requisitos Técnicos para el Proceso de Identificación del Cliente para la Autenticación de Identificación Remota a través de Dispositivos Electrónicos para la Transmisión Directa de Vídeo aprobados por el Director del Servicio de Investigación de Delitos Financieros dependiente del Ministerio del Interior de la República de Lituania el 30 de noviembre de 2016 mediante la Resolución nº V-314 "Para los Requisitos Técnicos para el Proceso de Identificación del Cliente para la Autenticación de Identificación Remota a través de Dispositivos Electrónicos para la Transmisión Directa de Vídeo" (en adelante - Requisitos Técnicos).[1]

- Resolución nº V-240 del 5 de diciembre de 2014 del Director del Servicio de Investigación de Delitos Financieros dependiente del Ministerio del Interior de la República de Lituania "Sobre la aprobación de la lista de criterios para la identificación del blanqueo de capitales y de operaciones o transacciones monetarias sospechosas o inusuales".[2]

- Resolución No. V-5 del 5 de enero 10 de 2020 del Director del Servicio de Investigación de Delitos Financieros dependiente del Ministerio del Interior de la República de Lituania "Sobre la aprobación de directrices para los operadores de monederos de moneda virtual depositarios y los operadores de cambio de moneda virtual para prevenir el blanqueo de dinero y/o la financiación del terrorismo."[3]

- Resolución nº V-273 del 20 de octubre de 2016 del Director del Servicio de Investigación de Delitos Financieros dependiente del Ministerio del Interior de la República de Lituania "Sobre la aprobación de las Directrices de Supervisión de Delitos Financieros para la Aplicación de Sanciones Financieras Internacionales en el Ámbito de la Normativa del Ministerio del Interior de la República de Lituania."[4]

- el Ministro del Interior de la República de Lituania el 16 de octubre de 2017 mediante la orden no. 1V- 701 "Sobre la suspensión de operaciones o transacciones monetarias sospechosas y la presentación de información sobre operaciones o transacciones monetarias sospechosas al Servicio de Investigación de Delitos Financieros en virtud de la descripción del procedimiento del Ministerio del Interior de la República de Lituania y la información sobre operaciones o transacciones en efectivo iguales o superiores a 15.000 euros o la presentación de la cantidad correspondiente en moneda extranjera".

[1] https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr
[2] https://www.e-tar.lt/portal/lt/legalAct/a664b2107ecd11e4bc68a1493830b8b9
[3] https://www.e-tar.lt/portal/lt/legalAct/570a231035e011ea829bc2bea81c1194
[4] https://www.e-tar.lt/portal/lt/legalAct/01d5d4e0974411e69ad4c8713b612d0f

moneda al Servicio de Investigación de Delitos Financieros bajo la aprobación de la descripción del procedimiento del Ministerio del Interior de la República de Lituania "[5]

- Director del Servicio de Investigación de Delitos Financieros 2015 21 de mayo por orden no. V-129 "Sobre la aprobación de los formularios de información, los esquemas de presentación y las recomendaciones para cumplimentar la información facilitada de conformidad con los requisitos de la Ley de prevención del blanqueo de capitales y de la financiación del terrorismo de la República de Lituania"[6]

Estas Directrices están sujetas a una revisión por parte del Consejo de Administración al menos una vez al año. La propuesta de revisión y la revisión de estas Directrices pueden programarse con mayor frecuencia por decisión del Responsable de Información sobre Blanqueo de Capitales (MLRO) de la empresa o del Responsable de Control Interno.

Estas Directrices serán aceptadas y aprobadas por resolución del Consejo de Administración de la empresa.

DEFINICIONES

Propietario efectivo es una persona física que, aprovechando su influencia, realiza una transacción, acto, acción, operación o paso o ejerce control de otra manera sobre una transacción, acto, acción, operación o paso o sobre otra persona y en cuyos intereses o en cuyo beneficio o por cuya cuenta se realiza una transacción o acto, acción, operación o paso. En el caso de una persona jurídica, el Propietario Beneficiario es una persona física cuya participación directa o indirecta, o la suma de todas las participaciones directas e indirectas en la persona jurídica, supere el 25 por ciento, incluidas las participaciones en forma de acciones u otras formas al portador.

Por **relación comercial** se entiende una relación que se establece tras la celebración de un contrato a largo plazo por parte de la empresa en actividades económicas o profesionales con el fin de prestar un servicio o distribuirlo de otra manera o que no se basa en un contrato a largo plazo, pero de la que se podía esperar razonablemente una cierta duración en el momento del establecimiento del contacto y durante la cual la empresa realiza repetidamente transacciones separadas en el curso de actividades económicas o profesionales mientras presta un servicio.

Empresa significa persona jurídica con los siguientes datos:

- Nombre de la empresa: UAB Criptomy;
- país de registro: Lituania;
- número de registro: 306127858;
- Dirección: Vilna, Eišiškių Sodų 18-oji g. 11;
- correo electrónico: info@criptomy.exchange, contact@criptomy.exchange

Monedero Virtual Custodio significa Dirección(es) de Moneda Virtual generada(s) con la clave pública[7] para almacenar y gestionar Monedas Virtuales confiadas a la Empresa pero que siguen siendo de su propiedad.

[5] https://e-tar.lt/portal/lt/legalAct/143ad320b24011e7afdadfc0e4460de4
[6] https://www.e-tar.lt/portal/lt/legalAct/e1f42fa0006d11e588da8908dfa91cac

Monedero Virtual Custodio significa Dirección(es) de Moneda Virtual generada(s) con la clave pública[7] para almacenar y gestionar Monedas Virtuales confiadas a la Empresa pero que siguen siendo de su propiedad.

Cliente significa una persona física o jurídica que mantiene la Relación Comercial con la Empresa.

Empleado se refiere al empleado de la Empresa y a cualquier otra persona que participe en la aplicación de estas Directrices en la Empresa.

Directrices: el presente documento, incluidos todos los anexos mencionados anteriormente. Las Directrices incluyen, entre otras cosas, el procedimiento de control interno de la empresa en relación con las Directrices y la política de evaluación de riesgos de la empresa en relación con el enfoque basado en el riesgo para los riesgos de BC/FT.

Por Consejo de Administración se entiende el consejo de dirección de la Empresa. Si la Empresa no tiene consejo de administración - el gerente de la Empresa será considerado como miembro del Consejo de Administración y será responsable de las funciones del Consejo de Administración en el contexto de las Directrices.

MLRO significa Oficial de Información sobre Blanqueo de Dinero, que es designado en la Empresa como persona responsable de recibir las revelaciones internas y de realizar los informes al Servicio de Investigación de Delitos Financieros (FCIS) y otras funciones descritas anteriormente.

Operación monetaria significa cualquier pago, transferencia o recepción de dinero.

Por **blanqueo de capitales (**LD) se entiende la ocultación del origen de fondos ilícitos mediante su introducción en el sistema económico legal y transacciones que parecen legítimas. Existen tres etapas reconocidas en el proceso de blanqueo de capitales:

- colocación, que consiste en colocar el producto del delito en el sistema financiero;
- La estratificación, que consiste en convertir el producto del delito en otra forma y crear complejas capas de transacciones financieras para disfrazar la pista de auditoría y el origen y la propiedad de los fondos;
- integración, que consiste en volver a colocar los beneficios blanqueados en la economía para crear la percepción de legitimidad.

Transacción Ocasional significa la transacción realizada por la Empresa en el curso de actividades económicas o profesionales con el fin de prestar un servicio o vender bienes o distribuirlos de otra manera al Cliente fuera del curso de una Relación Comercial establecida.

PEP significa una persona física que desempeña o ha desempeñado funciones públicas destacadas y con respecto a la cual subsisten riesgos relacionados.

Las sanciones significan una herramienta esencial de la política exterior destinada a apoyar el mantenimiento o el restablecimiento de la paz, la seguridad internacional, la democracia y el Estado de Derecho, siguiendo los principios de los derechos humanos.

[7] **Clave pública** significa un código de letras, números y/o símbolos diseñado para identificar al cliente y generar la Dirección de Moneda Virtual del cliente.

los derechos y el derecho internacional o la consecución de otros objetivos de la Carta de las Naciones Unidas o de la Política Exterior y de Seguridad Común de la Unión Europea. Las sanciones incluyen:

- Sanciones internacionales que se imponen con respecto a un Estado, territorio, unidad territorial, régimen, organización, asociación, grupo o persona por una resolución del Consejo de Seguridad de las Naciones Unidas, una decisión del Consejo de la Unión Europea o cualquier otra legislación que imponga obligaciones a Lituania;
- Sanciones del Gobierno de la República de Lituania que es una herramienta de política exterior que puede imponerse además de los objetivos especificados en la cláusula anterior para proteger la seguridad o los intereses de Lituania.

Las sanciones internacionales pueden prohibir la entrada de un sujeto de una sanción internacional en el Estado, restringir el comercio internacional y las transacciones internacionales e imponer otras prohibiciones u obligaciones.

El sujeto de las Sanciones es cualquier persona física o jurídica, entidad u organismo, designado en el acto jurídico por el que se imponen o aplican las Sanciones, con respecto al cual se aplican las Sanciones.

Por financiación del terrorismo (FT) se entiende la financiación y el apoyo de un acto de terrorismo y su comisión, así como la financiación y el apoyo de viajes con fines terroristas en el sentido de la legislación aplicable.

Tercer país significa un estado que no es miembro del Espacio Económico Europeo (EEE).

Moneda virtual: un valor representado en forma digital, que es digitalmente transferible, preservable o negociable y que las personas físicas o jurídicas aceptan como instrumento de pago, pero que no es la moneda de curso legal de ningún país o fondos a efectos del artículo 4, apartado 25, de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) nº 1093/2010, y por la que se deroga la Directiva 2007/64/CE (DO L 337 de 23.12.2015, pp 35-127) o una operación de pago a efectos de las letras k) y l) del artículo 3 de la misma Directiva.

Dirección de Moneda **Virtual** significa dirección/cuenta generada a partir de letras, números y/o símbolos en la cadena de bloques, mediante la cual la cadena de bloques asigna la Moneda Virtual al propietario o destinatario.

PRINCIPIOS PARA LA ESTRUCTURA Y LA GESTIÓN DE LA EMPRESA

La estructura organizativa de la Sociedad debe corresponder a su tamaño y a la naturaleza, alcance y nivel de complejidad de sus actividades y servicios prestados, incluyendo la propensión al riesgo y los riesgos relacionados, y debe estructurarse de acuerdo con el principio de **las tres líneas de defensa.** La estructura organizativa de la empresa debe corresponderse con la comprensión completa de los riesgos potenciales y su gestión. Las cadenas de información y subordinación de la Empresa deben garantizarse de tal manera que todos los Empleados conozcan su lugar en la estructura organizativa y conozcan sus obligaciones laborales.

El Consejo de Administración

El Consejo de Administración es el portador de la cultura de cumplimiento de los requisitos de prevención del Blanqueo de Capitales y de la Financiación del Terrorismo, garantizando que los miembros del Consejo de Administración y los Empleados de la Empresa operan en un entorno en el que son plenamente conscientes de los requisitos de prevención del Blanqueo de Capitales y de la Financiación del Terrorismo y de las obligaciones asociadas a dichos requisitos, y las consideraciones de riesgo pertinentes se tienen en cuenta en la medida adecuada en los procesos de toma de decisiones de la Empresa.

Los miembros del Consejo de Administración son los responsables últimos de las medidas adoptadas para evitar el uso de los servicios de la empresa para el blanqueo de dinero o la financiación del terrorismo. Se encargan de la supervisión y son responsables de:

- Establecer y mantener los procesos, procedimientos, riesgos y controles de ALD[8] ;
- adoptando estas Directrices y otras directrices e instrucciones internas;
- determinar las directrices de la empresa para las medidas de lucha contra el blanqueo de capitales;
- Nombrar a un MLRO y asegurarse de que éste dispone de las facultades, los recursos y la experiencia necesarios para desempeñar su cometido;
- asignar recursos suficientes para garantizar la aplicación efectiva de las Directrices y otros documentos relacionados y para mantener la organización;
- Garantizar que todos los Empleados pertinentes completen la formación anual en materia de lucha contra el blanqueo de capitales.

La primera línea de defensa: los empleados

La primera línea de defensa tiene la función de aplicar las medidas de diligencia debida en el momento de la relación comercial y de aplicar las medidas de diligencia debida durante la relación comercial. La primera línea de defensa comprende las unidades estructurales y los Empleados de la Empresa con cuyas actividades están asociados los riesgos y que deben identificar y evaluar estos riesgos, sus características específicas y su alcance y que gestionan estos riesgos mediante sus actividades ordinarias, principalmente mediante la aplicación de medidas de diligencia debida. Los riesgos derivados de las actividades y la prestación de servicios de la empresa pertenecen a la primera línea de defensa. Son los gestores (propietarios) de estos riesgos y responsables de los mismos.

[8] A efectos de simplificar estas Directrices, la relación con la "LLD" incluye también la prevención de la financiación del terrorismo y la aplicación de sanciones

Los Empleados de la Empresa deben actuar con la previsión y competencia que se espera de ellos y de acuerdo con los requisitos establecidos para sus puestos, partiendo de los intereses y los objetivos de la Empresa, y garantizar que el sistema financiero y el espacio económico del país no se utilicen para el Blanqueo de Dinero y la Financiación del Terrorismo. La Empresa toma medidas para evaluar la idoneidad de los Empleados antes de que empiecen a trabajar con la formación pertinente.

Por las razones antes mencionadas, los Empleados están obligados a:

- Cumplir todos los requisitos descritos en las Directrices y otros documentos relacionados;
- recopilar la información necesaria sobre el cliente de acuerdo con su función y sus responsabilidades;
- comunicar sin demora al MLRO la información, situaciones, actividades, transacciones o intentos de transacción que sean inusuales para cualquier tipo de servicio o relación con el Cliente, independientemente de su importe, tanto si la transacción se ha completado como si no;
- no informará ni hará saber de otro modo a los Clientes si el Cliente o cualesquiera otros Clientes son o pueden ser objeto de un informe o si se ha presentado o puede presentarse un informe;
- completar la formación AML apropiada requerida para el puesto del Empleado.

La segunda línea de defensa - Gestión de riesgos y cumplimiento, MLRO

La segunda línea de defensa está formada por las funciones de gestión de riesgos y cumplimiento. Estas funciones también pueden ser desempeñadas por la misma persona o unidad estructural dependiendo del tamaño de la Empresa y de la naturaleza, alcance y nivel de complejidad de sus actividades y servicios prestados, incluyendo el apetito de riesgo y los riesgos derivados de las actividades de la Empresa.

El objetivo de la **función de cumplimiento** es garantizar que la Empresa cumpla con la legislación vigente, las directrices y otros documentos y evaluar el posible efecto de cualquier cambio en el entorno legal o normativo sobre las actividades de la Empresa y sobre el marco de cumplimiento. La tarea del cumplimiento es ayudar a la primera línea de defensa, como propietarios del riesgo, a definir los lugares en los que se manifiestan los riesgos (por ejemplo, análisis de transacciones sospechosas e inusuales, para lo cual los Empleados de cumplimiento tienen las habilidades profesionales requeridas, cualidades personales, etc.) y ayudar a la primera línea de defensa a gestionar estos riesgos de manera eficiente. La segunda línea de defensa no se dedica a asumir riesgos.

La política de riesgos se aplica y el marco de gestión de riesgos está controlado por **la función de gestión de riesgos**. El ejecutor de la función de gestión de riesgos se asegura de que todos los riesgos se identifiquen, evalúen, midan, supervisen y gestionen, e informa de ellos a las unidades apropiadas de la empresa.

El ejecutor de la función de gestión de riesgos a efectos de la lucha contra el blanqueo de capitales realiza principalmente la supervisión del cumplimiento del apetito de riesgo, la supervisión de la tolerancia al riesgo, la supervisión de la identificación de cambios en los riesgos, realiza la visión general de los riesgos asociados y realiza otras tareas relacionadas con la gestión de riesgos.

El Consejo de Administración ha designado a un **MLRO** para desempeñar las funciones de segunda línea de defensa. Esta persona no está implicada operativamente en las áreas que el MLRO supervisará y verificará, por lo que es independiente en relación con las mismas.

En el marco actual de ALD de la empresa, es el MLRO quien toma las decisiones clave en relación con cuestiones individuales de ALD, como la aprobación de las PEP, la aceptación o el rechazo de los usuarios de alto riesgo etc.

El responsable de la lucha contra el blanqueo de capitales designado por la empresa es el responsable principal de la empresa y una persona que posee todos los conocimientos y la experiencia laboral necesarios.

El MLRO es responsable de las siguientes actividades:

- elaborar y, cuando sea necesario, actualizar las Directrices de la empresa;
- supervisar y verificar de forma continua que la empresa cumple los requisitos prescritos por estas Directrices y los documentos relacionados y de acuerdo con las leyes y reglamentos externos;
- proporcionar al personal de la empresa y a los miembros del Consejo de Administración asesoramiento y apoyo en relación con las normas relativas al blanqueo de capitales y la financiación del terrorismo;
- informar y formar a los miembros del Consejo de Administración y a las personas pertinentes sobre las normas relativas al blanqueo de dinero y la financiación del terrorismo;
- Investigar y registrar datos suficientes sobre las notificaciones internas recibidas y decidir si la actividad puede justificarse o si es sospechosa;
- presentar los informes pertinentes ante las autoridades reguladoras competentes de conformidad con la legislación aplicable;
- comprobar y evaluar periódicamente si los procedimientos y directrices de la empresa para evitar el uso de la empresa para el blanqueo de capitales o la financiación del terrorismo son adecuados y eficaces.

El MLRO informa trimestralmente al Consejo de Administración. Este informe debe realizarse por escrito e incluir al menos los siguientes puntos:

- número de clientes en todas las clasificaciones de riesgo
- número de respuestas positivas de personas en relación con las listas de sanciones y las medidas aplicadas;
- número de clientes o representantes de clientes identificados como PEP o personas con conexión con una PEP;
- número de notificaciones internas sobre actividades o transacciones sospechosas;
- número de los informes pertinentes comunicados al Servicio de Investigación de Delitos Financieros (SIDF);
- número y contenido de una solicitud de información al FCIS en el marco de una investigación;
- La confirmación de que la evaluación de riesgos de la empresa en materia de blanqueo de dinero y financiación del terrorismo está actualizada;
- confirmación de que estas Directrices y otros documentos relacionados están actualizados;
- La confirmación de que la dotación de personal con respecto a las medidas de lucha contra el blanqueo de capitales es suficiente;
- se han abordado todas las insuficiencias (si las hubiera) identificadas por la función de control;
- Lista de las formaciones obligatorias que se han impartido al personal en materia de medidas de lucha contra el blanqueo de capitales.

La tercera línea de defensa: la auditoría interna

La tercera línea de defensa está constituida por la función de auditoría interna independiente y eficaz. La función de auditoría interna puede ser desempeñada por un Responsable de Control Interno. Puede ser uno o varios Empleados, la unidad estructural de la Empresa con las funciones pertinentes o por el tercero, que presta el servicio pertinente a la Empresa. No se permite que el Responsable de Control Interno ocupe el cargo de MLRO y/o Miembro del Consejo de Administración de la Empresa o cualquier otro cargo, cuyas funciones incluyan la redacción y/o edición de los reglamentos y directrices internas de la Empresa en materia de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo.

Los Empleados, la unidad estructural de la Empresa o terceros, que realicen la función de auditoría interna deben tener la competencia, las herramientas y el acceso a la información relevante requeridos en todas las unidades estructurales de la Empresa. Los métodos de auditoría interna deben ajustarse al tamaño de la Empresa, la naturaleza, el alcance y el nivel de complejidad de las actividades y los servicios prestados, incluida la propensión al riesgo y los riesgos derivados de las actividades de laEmpresa.

La decisión de realizar una auditoría interna se toma por resolución del Consejo de Administración. El Consejo de Administración debe evaluar la necesidad de realizar una auditoría interna al menos una vez al año.

PRINCIPIOS DE APLICACIÓN DE LAS MEDIDAS DE DILIGENCIA DEBIDA CON RESPECTO AL CLIENTE

Las medidas de diligencia debida con respecto al cliente (DDC) son necesarias para verificar la identidad de un Cliente nuevo o existente como una supervisión continua basada en el riesgo de la relación comercial con el Cliente. Las medidas de DDC constan de 3 niveles, que incluyen medidas de diligencia debida simplificadas y reforzadas, tal y como se especifica a continuación.

Principios fundamentales

Las medidas de DDC se adoptan y ejecutan en la medida necesaria teniendo en cuenta el perfil de riesgo del Cliente y otras circunstancias en los siguientes casos:

- en el momento del establecimiento de la Relación Comercial y durante el seguimiento continuo de la misma;
- al ejecutar o mediar en Transacción(es) Ocasional(es) fuera de la Relación Comercial, cuando el valor de la(s) transacción(es) ascienda a 700 euros o más (o una cantidad igual en otros activos) en un plazo de 24 horas;
- al ejecutar o mediar en Transacción(es) Ocasional(es) fuera de la Relación Comercial, cuando el valor de la(s) transacción(es) ascienda a 10 000 euros o más (o una cantidad igual en otros activos) en el plazo de un mes;
- tras la verificación de la información recopilada al aplicar las medidas de diligencia debida o en caso de dudas sobre la suficiencia o veracidad de los documentos o datos recopilados anteriormente al actualizar los datos pertinentes;
- ante la sospecha de blanqueo de capitales o financiación del terrorismo, independientemente de las derogaciones, excepciones o límites previstos en estas directrices y en la legislación aplicable.

- la empresa no es capaz de adoptar y llevar a cabo ninguna de las medidas de DDC requeridas;
- la Empresa tiene cualquier sospecha de que los servicios o la transacción de la Empresa se utilizarán para el Blanqueo de Dinero o la Financiación del Terrorismo;
- el nivel de riesgo del Cliente o de la operación no se ajusta a la propensión al riesgo de la Empresa.

En el caso de recibir información en idiomas extranjeros en el marco de la aplicación de la DDC, la Empresa podrá solicitar que se le exija la traducción de los documentos a otro idioma apto para la Empresa. El uso de traducciones debe evitarse en situaciones en las que los documentos originales estén preparados en un idioma apto para la Empresa.

Lograr la DDC es un proceso que comienza con la aplicación de medidas de DDC. Una vez completado ese proceso, se asigna al Cliente un nivel de riesgo individual documentado que constituirá la base de las medidas de seguimiento, y que será objeto de seguimiento y actualización cuando sea necesario.

La empresa ha aplicado adecuadamente las medidas de DDC si tiene la convicción interna de que ha cumplido con la obligación de aplicar las medidas de diligencia debida. En la consideración de la convicción interna se observa el principio de razonabilidad. Esto significa que la Empresa debe, al aplicar las medidas de DDC, adquirir el conocimiento, la comprensión y la afirmación de que ha recopilado suficiente información sobre el Cliente, las actividades del Cliente, la finalidad de la Relación de Negocios y de las transacciones realizadas en el ámbito de la Relación de Negocios, el origen de los fondos, etc., de modo que comprenda al Cliente y las actividades (de negocios) del Cliente, teniendo en cuenta así el nivel de riesgo del Cliente, el riesgo asociado a la Relación de Negocios y la naturaleza de dicha relación. Dicho nivel de afirmación debe permitir identificar transacciones complicadas, de alto valor e inusuales y patrones de transacción que no tengan un propósito económico o legítimo razonable u obvio o que no sean característicos de las características específicas del negocio en cuestión.

La Compañía debe aplicar la DDC no sólo a los Clientes personas físicas sino también a las personas jurídicas. Todos los contraagentes y socios de la Compañía son comprobados manualmente por el Oficial MLRO con la ayuda de fuentes fiables e independientes.

Los servicios prestados

La principal actividad económica de la Empresa son los servicios de Moneda Virtual. Por este motivo, la Empresa ofrece a sus Clientes los siguientes tipos de transacciones:

- proporcionar el servicio de operador de cambio de Moneda Virtual, que permite al Cliente cambiar, comprar y vender Moneda Virtual.

La Empresa sólo prestará los servicios mencionados en el curso de una Relación Comercial establecida.

La verificación de la información utilizada para la identificación del cliente

La verificación de la información para la identificación del Cliente significa utilizar datos de una fuente fiable e independiente para confirmar que los datos son verdaderos y correctos, confirmando también, si es necesario, que los datos directamente relacionados con el Cliente son verdaderos y correctos. Esto, entre otras cosas, significa que el propósito de la verificación de la información es obtener la seguridad de que el Cliente, que desea establecer la Relación Comercial es la persona que dice ser. La fuente fiable e independiente (debe existir de forma acumulativa) es la verificación de la información obtenida en el curso de la identificación:

- que procede de dos fuentes diferentes;
- que haya sido emitida por (documentos de identidad) o recibida de un tercero o de un lugar que no tenga ningún interés o conexión con el Cliente o la Empresa, es decir, que sea neutral (por ejemplo, la información obtenida de Internet no es tal información, ya que a menudo procede del propio Cliente o no se puede verificar su fiabilidad e independencia);
- cuya fiabilidad e independencia puedan determinarse sin obstáculos objetivos y cuya fiabilidad e independencia sean también comprensibles para un tercero no implicado en la Relación de Negocios; y
- los datos incluidos en los cuales u obtenidos a través de los cuales están actualizados y son pertinentes y la Empresa puede obtener garantías al respecto (y las garantías también pueden obtenerse en ciertos casos sobre la base de las dos cláusulas anteriores).

Aplicación de medidas simplificadas de diligencia debida (nivel 1)

Las medidas de diligencia debida simplificada (SDD) se aplican cuando el perfil de riesgo del cliente indica un bajo nivel de riesgo de BC/FT.

Al aplicar las medidas SDD, la Empresa sólo debe obtener[9] los siguientes datos del Cliente que sea una persona física:

- nombre(s) y apellido(s);
- número personal;[10] o

en caso de que el Cliente sea una persona jurídica, los siguientes datos:

- nombre o razón social;
- forma jurídica;
- número de registro, si tal número ha sido emitido;
- sede social (dirección) y dirección de la operación real;
- nombre(s), apellidos y número personal o fecha de nacimiento del representante del Cliente; y

garantizar que el primer pago se realice a través de una cuenta en una entidad de crédito, cuando la entidad de crédito esté registrada en el EEE o en un Tercer País que imponga requisitos equivalentes a los establecidos en la legislación pertinente y sea supervisada por las autoridades competentes en cuanto al cumplimiento de dichos requisitos.

Las medidas de adeudos directos SEPA sólo podrán llevarse a cabo cuando la supervisión continua de la relación comercial del cliente se realice de conformidad con las directrices y exista la posibilidad de identificar operaciones y transacciones monetarias sospechosas.

Las medidas de SDD no deben llevarse a cabo en las circunstancias en las que deben aplicarse medidas de diligencia debida reforzada (como se describe a continuación).

---

9 Cuando el Cliente sea una institución o agencia estatal o municipal o el Banco de Lituania, la Empresa podrá, en el curso de la aplicación de las medidas de SDD, recopilar únicamente el número personal de dicha entidad y de su representante.

10 en el caso de un extranjero - la fecha de nacimiento (si está disponible - el número personal o cualquier otra secuencia única de símbolos concedida a esa persona, destinada a la identificación personal).

Cuando, en el curso de la realización de un seguimiento continuo de las Relaciones Comerciales del Cliente, se establezca que el riesgo de BC y/o FT ya no es bajo, la Empresa deberá aplicar el nivel pertinente de medidas de DDC.

Aplicación de medidas estándar de diligencia debida (nivel 2)

Las medidas estándar de diligencia debida se aplican a todos los Clientes en los que deben aplicarse medidas de DDC de conformidad con las Directrices. Deben aplicarse las siguientes medidas estándar de diligencia debida:

- identificación del Cliente y verificación de la información presentada basada en información obtenida de una fuente fiable e independiente;
- identificación y verificación de un representante del Cliente y su derecho de representación;
- identificación del Propietario Beneficiario y, con el fin de verificar su identidad, tomar medidas en la medida en que permitan a la Empresa asegurarse de que sabe quién es el Propietario Beneficiario y comprende la estructura de propiedad y control del Cliente;
- comprensión de la relación comercial, transacción u operación y, en su caso, recopilación de información al respecto;
- Recopilar información sobre si el cliente es una PEP, un miembro de su familia o una persona conocida como allegado;
- seguimiento de la relación comercial.

Las medidas de diligencia debida especificadas anteriormente deben aplicarse antes de establecer la relación comercial o realizar la transacción. Las instrucciones exactas para la aplicación de las medidas estándar de diligencia debida figuran en las Directrices.

Aplicación de medidas reforzadas de diligencia debida (nivel 3)

Además de las medidas estándar de diligencia debida, la empresa aplica medidas reforzadas de diligencia debida (EDD) para gestionar y mitigar un riesgo establecido de blanqueo de capitales y financiación del terrorismo en el caso de que se establezca que el riesgo es superior al habitual.

La empresa siempre aplica medidas de EDD, cuando:

- el perfil de riesgo del Cliente indica un alto nivel de riesgo de BC/FT;
- tras la identificación del cliente o la verificación de la información presentada, existan dudas sobre la veracidad de los datos presentados, la autenticidad de los documentos o la identificación del beneficiario efectivo;
- cuando se inicien relaciones de corresponsalía transfronteriza con el Cliente, que es una institución financiera de Tercer País;
- en caso de realización de una transacción o de una relación comercial con la PEP, el miembro de la familia de la PEP o una persona conocida como estrecho colaborador de la PEP;
- cuando se realicen transacciones o Relaciones Comerciales con personas físicas residentes o personas jurídicas establecidas en Terceros Países de alto riesgo identificados por la Comisión Europea;

- el Cliente es de dicho país o territorio o su lugar de residencia o sede o la sede del proveedor de servicios de pago del beneficiario se encuentra en un país o territorio que, según fuentes creíbles como evaluaciones mutuas, informes o informes de seguimiento publicados, no ha establecido sistemas eficaces de lucha contra el blanqueo de capitales y la financiación del terrorismo que sean conformes con las recomendaciones del GAFI.

Antes de aplicar las medidas EDD, el Empleado de la Empresa se asegura de que la Relación Comercial o la transacción tiene un alto riesgo y de que se puede atribuir un índice de alto riesgo a dicha Relación Comercial o transacción. Sobre todo, el Empleado evalúa antes de aplicar las medidas EDD si las características descritas anteriormente están presentes y las aplica como motivos independientes (es decir, cada uno de los factores identificados permite la aplicación de medidas EDD con respecto al Cliente).

Al aplicar las medidas EDD cuando se inicie una relación de corresponsalía transfronteriza con el Cliente, que es una entidad financiera de Tercer País, la Empresa deberá aplicar las siguientes medidas:

- reunir información suficiente sobre el Cliente para comprender plenamente la naturaleza de su actividad y determinar, a partir de la información disponible públicamente, la reputación del Cliente y la calidad de la supervisión;
- evaluar los mecanismos de control de la lucha contra el blanqueo de capitales del cliente y de la entidad receptora de los fondos;
- obtener la aprobación del miembro del Consejo de Administración antes de establecer nuevas relaciones de corresponsalía;
- documentar las responsabilidades respectivas del Cliente;
- estar convencido de que el Cliente ha llevado a cabo la diligencia debida con respecto al Cliente (incluida la verificación de la identidad de los Clientes que tienen acceso directo a las cuentas del Cliente y la realización de otras acciones de diligencia debida con respecto al Cliente) y de que es capaz de proporcionar los datos de identificación del Cliente pertinentes a la Empresa a petición de ésta.

Al aplicar las medidas EDD, cuando las transacciones o las Relaciones Comerciales se lleven a cabo con la PEP, el familiar de la PEP o una persona conocida como allegado de la PEP, la Empresa deberá aplicar las siguientes medidas:

- obtener la aprobación del miembro del Consejo de Administración antes de establecer una Relación Comercial con dicho Cliente o de continuar la Relación Comercial con el Cliente cuando éste se convierta en una PEP;
- tomar las medidas adecuadas para establecer la fuente de riqueza y el origen de los fondos que intervienen en la relación comercial o transacción;
- realizar un seguimiento continuo de la relación comercial con el cliente aumentando el número y el calendario de los controles aplicados y seleccionando patrones de transacciones que necesiten un examen más detallado.

Al aplicar las medidas EDD cuando se realicen transacciones o Relaciones Comerciales con personas físicas residentes o personas jurídicas establecidas en Terceros Países de alto riesgo identificados por la Comisión Europea, la Empresa deberá aplicar las siguientes medidas:

- obtener información adicional sobre el Cliente y sobre su Propietario Beneficiario;

- obtener información adicional sobre la naturaleza prevista de la Relación Comercial;
- obtener información sobre el origen de los fondos y la procedencia del patrimonio del Cliente y de su Propietario Beneficiario;
- obtener información sobre los motivos de las transacciones previstas o realizadas;
- obtener la aprobación del miembro del Consejo de Administración para establecer Relaciones Comerciales con el Cliente o continuar las Relaciones Comerciales con él;
- realizar un seguimiento continuo de la relación comercial con el cliente aumentando el número y el calendario de los controles aplicados y seleccionando patrones de transacciones que necesiten un examen más detallado;
- garantizar que el primer pago se realice a través de una cuenta a nombre del Cliente en una entidad de crédito, cuando la entidad de crédito esté registrada en el EEE o en un Tercer País que imponga requisitos equivalentes a los establecidos en la legislación aplicable y sea supervisada por las autoridades competentes en cuanto al cumplimiento de dichos requisitos.

Al aplicar las medidas EDD cuando el Cliente proceda de dicho país o territorio o su lugar de residencia o sede o la sede del proveedor de servicios de pago del beneficiario se encuentre en un país o territorio que, según fuentes creíbles como evaluaciones mutuas, informes o informes de seguimiento publicados, no haya establecido sistemas eficaces de lucha contra el blanqueo de capitales y la financiación del terrorismo que se ajusten a las recomendaciones del GAFI, la Empresa deberá aplicar las siguientes medidas:

- obtener la aprobación del miembro del Consejo de Administración para establecer Relaciones Comerciales con el Cliente o continuar las Relaciones Comerciales con él;
- obtener información sobre el origen de los fondos y la procedencia del patrimonio del Cliente y de su Propietario Beneficiario;
- realizar un seguimiento continuo de la relación comercial con el cliente aumentando el número y el calendario de los controles aplicados y seleccionando patrones de transacciones que necesiten un examen más detallado;

En cualquier otro caso en que deban aplicarse medidas de diligencia debida, la cantidad de medidas de diligencia debida y su alcance serán determinados por el Empleado, que es quien aplica dichas medidas. Se podrán seguir las siguientes medidas de diligencia debida adicionales y pertinentes:

- verificación de la información presentada adicionalmente tras la identificación del Cliente basada en documentos, datos o información adicionales procedentes de una fuente creíble e independiente;
- recabar información adicional sobre el propósito y la naturaleza de la relación comercial o la transacción y verificar la información presentada basándose en documentos, datos o información adicionales que procedan de una fuente fiable e independiente;
- recabar información y documentos adicionales sobre la ejecución real de las transacciones efectuadas en la Relación Comercial con el fin de descartar la ostensibilidad de las mismas;
- recabar información y documentos adicionales con el fin de identificar la fuente y el origen de los fondos utilizados en una transacción realizada en la Relación de Negocios para descartar la ostensibilidad de las transacciones;

- la realización del primer pago relacionado con una transacción a través de una cuenta que ha sido abierta a nombre del Cliente que participa en la transacción en una entidad de crédito registrada o que tenga su domicilio social en un Estado contratante del Espacio Económico Europeo o en un país en el que estén en vigor requisitos iguales a los de la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo;

- la aplicación de medidas de DDC en relación con el Cliente o su representante estando en el mismo lugar que el Cliente o su representante;
- recopilar información adicional sobre el Cliente y su Propietario Beneficiario, incluida la identificación de todos los propietarios del Cliente, incluidos aquellos cuya participación sea inferior al 25%;
- recopilar información sobre el origen de los fondos y el patrimonio del cliente y su beneficiario efectivo;
- mejorar la supervisión de la relación comercial aumentando el número y la frecuencia de las medidas de control aplicadas y eligiendo indicadores de transacciones o patrones de transacciones que se verifiquen adicionalmente;
- obtener la aprobación del miembro del Consejo de Administración para realizar transacciones o establecer relaciones comerciales con Clientes nuevos y existentes;

Al realizar la EDD, en determinados casos la Empresa está obligada a tomar medidas razonables para establecer el origen de los fondos y la fuente de riqueza de los Clientes. El origen de los fondos puede verificarse, *entre otras cosas, por referencia a*:

- una declaración fiscal anual;
- original o copia compulsada de una nómina reciente;
- Confirmación escrita del salario anual firmada por un empleador;
- un original o una copia certificada del contrato de venta del bien inmueble y un extracto original de una institución financiera que acredite la recepción de los fondos obtenidos de la venta del bien inmueble, si se dispone de él;
- original o copia certificada de un testamento o documento equivalente que acredite la herencia;
- un original o una copia certificada de un acuerdo de donación (ya sea en forma escrita simple o certificada por un notario público en caso de que la ley exija la forma notarial del acuerdo);
- un original o una copia certificada de un contrato de préstamo (ya sea en forma escrita simple, o certificada por un notario público en caso de que la forma notarial del contrato sea exigida por la ley), y un extracto de una institución financiera que demuestre la recepción o el envío de fondos relacionados con la recepción del préstamo o la devolución de un préstamo concedido; o un pagaré (ya sea en forma escrita simple, o certificado por un notario público en caso de que la forma notarial del contrato sea exigida por la ley);
- una búsqueda en Internet del registro mercantil para confirmar la venta de una empresa;
- original o una copia certificada del acuerdo de depósito.

El Empleado deberá notificar sobre las medidas EDD aplicadas dentro de los 2 días hábiles siguientes al inicio de la aplicación de las medidas EDD mediante el envío de la notificación pertinente al MLRO.

En el caso de la aplicación de medidas EDD, la Empresa reevalúa el perfil de riesgo del Cliente a más tardar cada seis meses.

MEDIDAS DE DILIGENCIA DEBIDA CON LOS CLIENTES

Identificación del cliente - persona física

La Empresa identifica al Cliente que es una persona física y, en su caso, a su representante y conserva los siguientes datos sobre el Cliente:

- nombre(s) y apellido(s);
- número personal;[11]
- ciudadanía;[12]
- fotografía;
- firma.[13]

Los siguientes documentos de identidad válidos que contengan los datos especificados anteriormente podrán utilizarse como base para la identificación de una persona física:

- un documento de identidad de la República de Lituania con excepción del permiso de residencia de la República de Lituania;
- un documento de identidad de un estado extranjero;

El Cliente, que es persona física, no puede utilizar un representante en el curso de la relación comercial con la Empresa.

Identificación del cliente - persona jurídica

La Empresa identifica al Cliente persona jurídica y a su representante y conserva los siguientes datos sobre el Cliente:

- nombre o razón social;
- forma jurídica;
- número de registro, si tal número ha sido emitido;

[11] en el caso de un extranjero - la fecha de nacimiento (si está disponible - el número personal o cualquier otra secuencia única de símbolos concedida a esa persona, destinada a la identificación personal);

[12] cuando un documento de identidad no contenga datos sobre la nacionalidad del cliente, las instituciones financieras y otras entidades obligadas deberán, al identificar al cliente que sea una persona física en presencia física del cliente, exigirle que facilite los datos sobre la nacionalidad.

[13] excepto en los casos en que sea opcional en el documento de identidad;

- nombre(s) y apellido(s), número personal (en el caso de un extranjero - fecha de nacimiento o cuando esté disponible - número personal o cualquier otra secuencia

única de símbolos concedida a esa persona, destinado a la identificación personal) y la ciudadanía del director o directores o miembro(s) del Consejo de Administración o miembro(s) de otro organismo equivalente, y sus autoridades en la representación del Cliente;

- un extracto del registro y su fecha de expedición;
- sede social (dirección) y dirección de la explotación real
- Para la identificación del Cliente pueden ser implícitos los siguientes documentos expedidos por una autoridad u organismo competente no antes de seis meses antes de su utilización:
    - tarjeta de registro del registro pertinente; o
    - certificado de inscripción del registro correspondiente; o
    - un documento equivalente con los documentos antes mencionados o los documentos pertinentes de establecimiento del Cliente.

La Empresa verifica la exactitud de los datos del Cliente especificados anteriormente, utilizando para ello información procedente de una fuente creíble e independiente. Cuando la Empresa tenga acceso al registro pertinente de personas jurídicas, no será necesario exigir al Cliente la presentación de los documentos especificados anteriormente.

La identidad de la persona jurídica y el derecho de representación de la persona jurídica pueden verificarse sobre la base de un documento especificado anteriormente, que haya sido autenticado por un notario o certificado por un notario u oficialmente, o sobre la base de otra información procedente de una fuente creíble e independiente, incluidos los medios de identificación electrónica y los servicios de confianza para las transacciones electrónicas, utilizando así al menos dos fuentes diferentes para la verificación de los datos en tal caso.

La identificación del representante del Cliente y su derecho de representación

El representante del Cliente deberá identificarse como el Cliente, que es una persona física de acuerdo con estas Directrices. Asimismo, deberá identificar y verificar la naturaleza y el alcance del derecho de representación del Cliente. Deberá averiguar y conservar el nombre, la fecha de emisión y el nombre del emisor del documento que sirve de base al derecho de representación, salvo en el caso de que el derecho de representación se haya verificado utilizando información procedente del registro pertinente.

La empresa debe respetar las condiciones del derecho de representación concedido a los representantes de la persona jurídica y prestar servicios únicamente dentro del ámbito del derecho de representación.

La autorización tiene que ajustarse a los requisitos del Código Civil lituano. La autorización expedida en el extranjero tiene que estar legalizada o llevar una Apostilla. En caso de que el derecho de representación del Cliente (persona jurídica) se desprenda del extracto del registro, de los estatutos o de documentos equivalentes que acrediten la identidad del Cliente (persona jurídica), no será necesario un documento de autorización aparte (por ejemplo, un poder notarial).

La identificación del beneficiario efectivo del cliente

La Empresa debe identificar al Propietario Beneficiario del Cliente - un individuo que en última instancia posee o controla al Cliente o en cuyo nombre se está realizando una transacción.

La Empresa también debe tomar medidas para verificar la identidad del Propietario Beneficiario hasta el punto que le permita asegurarse de que sabe quién es el Propietario Beneficiario.

La Empresa no puede suponer que los propios particulares son los BO del Cliente, y siempre debe obtener primero la información del Cliente sobre quién es el BO. Por identificación del BO se entiende la identificación de una persona física o de un grupo de personas físicas.

La empresa recopila los siguientes datos sobre el/los beneficiario(s) del cliente:

- nombre(s) y apellido(s);
- número personal;[14]
- ciudadanía.[15]

La Empresa solicitará al Cliente información al Propietario Beneficiario del Cliente (por ejemplo, proporcionando al Cliente la oportunidad de especificar su Propietario Beneficiario al recopilar datos sobre el Cliente).

La Empresa no establece la Relación Comercial, si el Cliente, que es una persona física tiene un Propietario Beneficiario que no es la misma persona que el Cliente.

El beneficiario efectivo de una entidad jurídica se identifica en etapas en las que la entidad obligada procede a cada etapa posterior si el beneficiario efectivo de la entidad jurídica no puede determinarse en el caso de la etapa anterior. Las etapas son las siguientes:

- es posible identificar, con respecto al Cliente que es una persona jurídica o una persona que participa en la transacción, a la persona o personas físicas que realmente controlan en última instancia la persona jurídica o ejercen influencia o control sobre ella de cualquier otra manera, independientemente del tamaño de las acciones, los derechos de voto o los derechos de propiedad o de su naturaleza directa o indirecta;
- si el Cliente que es una persona jurídica o la persona que participa en la transacción tiene una o varias personas físicas que poseen o controlan la persona jurídica a través de una participación directa[16] o indirecta[17] . En este caso también deben tenerse en cuenta las conexiones familiares y contractuales;
- quién es la persona física de la alta dirección[18] , que debe definirse como el Beneficiario Efectivo, como resultado de la ejecución de las dos etapas anteriores no ha sido posible para la entidad obligada identificar al Beneficiario Efectivo.

El alto directivo del cliente deberá indicarse como beneficiario efectivo sólo en casos excepcionales en los que la empresa ponga todos los medios razonables para determinar quién es el beneficiario efectivo y siempre que no haya motivos para sospechar que se está ocultando la identidad del beneficiario efectivo. En este caso, por alto directivo deberá entenderse el jefe (por ejemplo, el director general,

[14] en el caso de un extranjero - la fecha de nacimiento (si está disponible - el número personal o cualquier otra secuencia única de símbolos concedida a esa persona, destinada a la identificación personal);

[15] cuando un documento de identidad no contenga datos sobre la nacionalidad del cliente, las instituciones financieras y otras entidades obligadas deberán, al identificar al cliente que sea una persona física en presencia física del cliente, exigirle que facilite los datos sobre la nacionalidad.

[16] **la propiedad directa** es una forma de ejercer el control mediante la cual la persona física posee una participación del 25 por ciento más una acción o un derecho de propiedad superior al 25 por ciento en la empresa

[17] **La propiedad indirecta** es una forma de ejercer el control por la que una participación del 25 por ciento más una acción o un derecho de propiedad superior al 25 por ciento en la empresa es propiedad de una empresa controlada por una persona física o de varias empresas controladas por la misma persona física.

[18] un **miembro de la alta** dirección es una persona que toma las decisiones estratégicas que afectan fundamentalmente a las actividades y/o prácticas empresariales y/o a las tendencias generales (comerciales) de la empresa o que, en su ausencia, desempeña funciones cotidianas o habituales de gestión de la empresa en el ámbito del poder ejecutivo (por ejemplo, director general (CEO), director financiero (CFO), director o presidente, etc.).

director general, jefe de administración) del Cliente.

Los documentos utilizados para la identificación de la persona jurídica o los demás documentos presentados no indican directamente quién es el Propietario Beneficiario de la entidad jurídica, los datos pertinentes (incluidos los datos sobre la pertenencia a un grupo y la estructura de propiedad y gestión del grupo) se registran sobre la base de la declaración del representante de la entidad jurídica o del documento escrito a mano por el representante de la entidad jurídica.

La Empresa aplicará medidas razonables para verificar la exactitud de la información establecida sobre la base de declaraciones o de un documento manuscrito (por ejemplo, haciendo averiguaciones en los registros pertinentes), exigiendo la presentación del informe anual de la persona jurídica u otro documento pertinente. Si la Empresa tiene dudas sobre la exactitud o exhaustividad de la información pertinente, verificará la información facilitada a partir de fuentes de acceso público y, si es necesario, solicitará información adicional al Cliente.

Dificultades encontradas durante la identificación del beneficiario efectivo

La empresa debe ser consciente de que la información sobre la titularidad real puede quedar oscurecida mediante el uso de empresas ficticias, complejas estructuras de propiedad y control que implican muchas capas de acciones registradas a nombre de otras personas jurídicas, accionistas y directores nominales, como allegados y familiares, y de otras formas.

En muchos casos, el papel de los directores y accionistas nominados es proteger u ocultar la identidad del BO y controlador de una empresa o activo. Un nominado puede ayudar a superar los controles jurisdiccionales sobre la propiedad de la empresa y eludir las prohibiciones de dirección impuestas por los tribunales y las autoridades gubernamentales. Por lo tanto, la Empresa debe ser especialmente consciente de las estructuras societarias que fomentan la complejidad y aumentan la dificultad para obtener información precisa sobre la titularidad real. Además, la Empresa debe ser consciente de la posibilidad de que existan acuerdos de nominación en los que amigos, familiares o asociados afirmen ser los BO de personas jurídicas, acuerdos legales u otras empresas.

Por lo tanto, la empresa debe tomar medidas apropiadas y adecuadas para determinar los verdaderos propietarios efectivos e identificar las situaciones en las que se está ocultando la propiedad efectiva.

Para determinar el BO, la Empresa debe recopilar datos sobre la estructura de propiedad del Cliente y verificarlos sobre la base de documentos, datos o información obtenidos de una fuente fiable e independiente. En caso de propiedad a varios niveles, el esquema de la estructura de propiedad deberá ser redactado por el Cliente u obtenido de éste.

La Empresa también debe asegurarse de que entiende la estructura de propiedad y control del Cliente, especialmente si la estructura de propiedad y control es compleja (por ejemplo, los accionistas proceden de múltiples jurisdicciones diferentes; los accionistas son de diferentes tipos de entidad legal / acuerdo legal, hay fideicomisos y vehículos de inversión privada dentro de la estructura de propiedad y control, el Cliente ha emitido acciones al portador). La Empresa debe evaluar si la estructura de propiedad y control tiene sentido desde el punto de vista comercial, económico o jurídico.

Utilización del Sistema de Información de Entidades Jurídicas Participantes

A la hora de identificar a un Propietario Beneficiario, la Empresa debe utilizar además el Sistema de Información de Entidades Jurídicas Participantes (JADIS) del que se obtienen datos sobre los Propietarios Beneficiarios del Cliente y tendrá derecho a utilizar otros sistemas de información y registros estatales en los que se acumulen datos sobre los participantes de personas jurídicas.

Se puede acceder a JADIS a través del Centro Estatal de Registros de Empresas de Lituania (SECR) mediante la aplicación correspondiente. La solicitud puede presentarse:

- electrónicamente a través del sistema de autoservicio de usuarios del Centro deRegistros;
- por correo electrónico info@registrucentras.lt que deberá ser firmado mediante firma electrónica;
- en las Oficinas de Atención al Cliente del Centro de Registros presentando su original.

Los extractos de JADIS preparados y las copias de documentos pueden ser:

- descargado del autoservicio del Centro de Registros (sólo si la solicitud se ha presentado a través del autoservicio del Centro de Registros);
- recogidos en las Oficinas de Atención al Cliente del Centro deRegistros;
- recibido por correo a la dirección indicada por elcliente.

Tras la determinación de la discrepancia entre la información sobre los beneficiarios efectivos del cliente que sea una persona jurídica disponible en JADIS y la información sobre los beneficiarios efectivos del mismo cliente de que disponga, notificará al cliente al respecto y le propondrá que facilite información precisa sobre sus beneficiarios efectivos al procesador de datos de JADIS.

La Empresa no entablará una Relación de Negocios ni ejecutará una transacción (excepto las operaciones monetarias o transacciones concluidas y/o ejecutadas en el curso de una Relación de Negocios), cuando la información sobre los Beneficiarios Finales del Cliente que sea una persona jurídica no esté proporcionada en JADIS o cuando la información sobre los Beneficiarios Finales del Cliente que sea una persona jurídica, proporcionada en JADIS, sea incorrecta.

Identificación de la persona expuesta políticamente

La Empresa tomará medidas para averiguar si el Cliente, el Propietario Beneficiario del Cliente o el representante de este Cliente es un PEP, su familiar[19] o asociado cercano[20] o si el Cliente se ha convertido en tal persona.

La Empresa solicitará al Cliente información para identificar si el Cliente es una PEP, un miembro de su familia o un socio cercano (por ejemplo, proporcionando al Cliente la oportunidad de especificar la información relevante cuando se recopilen datos sobre el Cliente).

La Empresa verificará los datos recibidos del Cliente realizando consultas en las bases de datos pertinentes o bases de datos públicas o realizando consultas o verificando los datos en los sitios web de las autoridades o instituciones de supervisión pertinentes del país en el que el Cliente tenga su lugar de residencia o sede. El PEP deberá verificarse adicionalmente utilizando un motor de búsqueda internacional (por ejemplo, Google) y el motor de búsqueda local del país de origen del Cliente, si lo hubiera, introduciendo el nombre del Cliente tanto en alfabeto latino como en alfabeto local con la fecha de nacimiento del Cliente.

Además, la revisión del estatus de PEP se implementa y realiza mediante la solución automatizada AML Sum & Substance. La solución proporciona una revisión continua del estatus PEP y realiza la identificación de los familiares y allegados de las PEP.

Se considera que al menos las siguientes personas son PEP:

- el jefe del estado, el jefe del gobierno, un ministro, un viceministro o un viceministro, un secretario de estado, un canciller del parlamento, del gobierno o de un ministerio;
- miembro del parlamento;
- un miembro del Tribunal Supremo, del Tribunal Constitucional o de cualquier otra autoridad judicial suprema cuyas decisiones sean inapelables;
- un alcalde del municipio, un jefe de la administración municipal;
- un miembro del órgano de dirección de la institución suprema de auditoría o control del estado, o un presidente, vicepresidente o miembro del consejo del banco central;
- embajadores de estados extranjeros, un encargado de negocios ad interim, el jefe de las fuerzas armadas lituanas, el comandante de las fuerzas y unidades armadas, el jefe del estado mayor de la defensa o un oficial superior de las fuerzas armadas extranjeras;
- un miembro del órgano de dirección o supervisión de una empresa pública, una sociedad anónima o una sociedad de responsabilidad limitada, cuyas acciones o parte de las acciones, que representen más de la mitad del total de los votos en la junta general de accionistas de dichas empresas, sean propiedad del estado;

[19] **Por miembro de la familia** se entiende el cónyuge, la persona con la que se ha registrado la pareja de hecho (es decir, el conviviente), los padres, los hermanos, las hermanas, los hijos y los cónyuges de los hijos,
cohabitantes de los niños

[20] **Asociado cercano** significa una persona física que, junto con el PEP, es miembro de la misma entidad jurídica o de un organismo sin personalidad jurídica o mantiene otra relación comercial; o una persona física que es el único Propietario Beneficiario de la entidad jurídica o de un organismo sin personalidad jurídica creado u operando de facto con el objetivo de adquirir bienes u otro beneficio personal para el PEP.

- un miembro del órgano de dirección o de supervisión de una empresa municipal, una sociedad anónima o una sociedad de responsabilidad limitada cuyas acciones o parte de las acciones, que representen más de la mitad del total de los votos en la junta general de accionistas de dichas empresas, sean propiedad del Estado, y que estén consideradas como grandes empresas en términos de la Ley sobre los Estados Financieros de las Entidades de la República de Lituania;
- un director, un director adjunto o un miembro del órgano de gestión o de supervisión de una organización internacional intergubernamental;
- un dirigente, un dirigente adjunto o un miembro del órgano de dirección de un partido político.

La empresa identificará a los allegados y familiares de PEP sólo si su conexión con PEP es conocida por el público o si la empresa tiene motivos para creer que existe tal conexión.

Cuando a un PEP ya no se le encomiende una Función Pública Prominente, la Compañía deberá, en un plazo de 12 meses a partir de la fecha de renuncia del PEP a las funciones públicas, tener en cuenta los riesgos que permanecen relacionados con el Cliente. Transcurrido un plazo de 12 meses a partir de la fecha de renuncia del PEP a las funciones públicas, la Empresa deberá volver a evaluar los riesgos relacionados con dicho cliente.

Identificación del propósito y la naturaleza de la relación comercial o de una transacción

La Empresa deberá comprender el propósito y la naturaleza del establecimiento de la Relación Comercial o de la realización de la transacción. En relación con los servicios prestados, la Empresa podrá solicitar al Cliente la siguiente información para comprender el propósito y la naturaleza de la Relación Comercial o de la transacción:

- si el Cliente utilizará los servicios de la Empresa para sus propias necesidades o representará los intereses de otra persona;
- información de contacto;
- información sobre la dirección registrada y el domicilio real del Cliente;
- el volumen estimado de transacciones con la empresa por año civil;
- la fuente estimada de los fondos utilizados en la relación comercial o transacción;
- si la relación comercial o la transacción está relacionada con la realización de actividades económicas o profesionales por parte del Cliente y de qué actividades se trata;
- información sobre el origen de los fondos relacionados con la relación comercial o la transacción, si el importe de las transacciones (incluido el importe previsto) supera el límite establecido.

La Empresa aplicará medidas adicionales y recopilará información adicional para identificar el propósito y la naturaleza de la Relación Comercial en los casos en que:

- existe una situación que se refiere a un alto valor o es inusual y/o
- cuando el riesgo y/o el perfil de riesgo asociado al Cliente y la naturaleza de la Relación de Negocio den motivo a la realización de acciones adicionales para poder supervisar adecuadamente a Relación de Negociohiplater.

Si el Cliente es una persona jurídica, además de lo anterior, la Empresa deberá identificar el **área de actividad del Cliente**, donde la Empresa deberá entender con qué trata y pretende tratar el Cliente en el curso de la Relación Comercial y cómo se corresponde con el propósito y la naturaleza de la Relación Comercial en general y si es razonable, comprensible y plausible.

El área de actividad debe encajar en el perfil de experiencia del representante del Cliente (o de las personas clave) y/o del Propietario Beneficiario. Por lo tanto, la Empresa tiene que identificar de dónde procede la capacidad, la aptitud, las habilidades y los conocimientos (experiencia en general) del representante y/o del Propietario Beneficiario para operar en esta área de actividad, con estos volúmenes de negocio y con estos socios comerciales principales.

Seguimiento de la relación comercial

La Empresa supervisará las Relaciones Comerciales establecidas en las que se apliquen las siguientes medidas de diligencia debida permanente (periódicamente):

- asegurarse de que los documentos, datos o información recopilados en el transcurso de la aplicación de las medidas de diligencia debida se actualizan periódicamente y en caso de que se produzcan acontecimientos desencadenantes, es decir, principalmente los datos relativos al Cliente, su representante (incluido el derecho de representación) y el Beneficiario Principal, así como la finalidad y la naturaleza de la Relación Comercial;
- Seguimiento continuo de la relación comercial, que abarca las transacciones realizadas en la relación comercial para garantizar que las transacciones se corresponden con el conocimiento que tiene la empresa del cliente, sus actividades y su perfil de riesgo;
- identificación de la fuente y el origen de los fondos utilizados en la(s) transacción(es).

La Empresa **comprobará y actualizará** periódicamente **los documentos, datos e información** recopilados en el transcurso de la aplicación de las medidas de DDC y actualizará el perfil de riesgo del Cliente. La regularidad de las comprobaciones y de la actualización deberá basarse en el perfil de riesgo del Cliente y las comprobaciones deberán tener lugar como mínimo:

- una vez al semestre para el Cliente de perfil de alto riesgo;
- una vez al año para el Cliente de perfil de riesgo medio;
- una vez cada dos años para el perfil de bajo riesgo Cliente.

La Empresa ha implantado un sistema de almacenamiento, sistematización y control de los documentos de los Clientes. El sistema notifica automáticamente al empleado responsable la necesidad de solicitar un documento actualizado de acuerdo con el perfil de riesgo del Cliente. El sistema también incluye el control de la fecha de caducidad y envía una notificación si el documento de identidad/probante de domicilio del Cliente está próximo a su fecha de caducidad.

Los documentos, datos e información recopilados también deben comprobarse si se ha producido algún acontecimiento que indique la necesidad de actualizar los documentos, datos e información recopilados.

En el curso del **seguimiento continuo de la Relación Comercial**, la Empresa supervisará las transacciones concluidas durante la Relación Comercial de tal manera que ésta pueda determinar si las transacciones que se concluyan corresponden a la información previamente conocida sobre el Cliente (es decir, lo que el cliente declaró al establecer la Relación Comercial o lo que se ha conocido en el curso de la Relación Comercial).

La Empresa también supervisará la Relación Comercial para averiguar las actividades del Cliente o los hechos que indiquen actividades delictivas, Blanqueo de Capitales o Financiación del Terrorismo o cuya relación con el Blanqueo de Capitales o la Financiación del Terrorismo sea probable, incluidas las transacciones complicadas, de alto valor e inusuales y los patrones de transacción que no tengan ningún propósito económico o legítimo razonable u obvio o que no sean característicos de las características específicas del negocio en cuestión. En el curso de la Relación Comercial, la Empresa evaluará constantemente la
cambios en las actividades del Cliente y evaluar si estos cambios pueden aumentar el nivel de riesgo asociado al Cliente y a la Relación Comercial, dando lugar a la necesidad de aplicar medidas de EDD.

En el curso de la supervisión continua de la relación comercial, la empresa aplica las siguientes medidas:

- cribado, es decir, el seguimiento de las transacciones en tiempo real;
- el seguimiento, es decir, el análisis

posterior de las transacciones. El objetivo del

control es identificar:

- transacciones sospechosas e inusuales y patrones de transacciones;
- transacciones que superen los umbrales previstos;
- personas políticamente expuestas y circunstancias relativas a las sanciones.

El cribado de las transacciones se realiza automáticamente e incluye las siguientes medidas:

- umbrales establecidos para las transacciones del Cliente, en función del perfil de riesgo del Cliente y del volumen estimado de transacciones declarado por el Cliente;
- la puntuación de los monederos de Moneda Virtual donde se enviará la Moneda Virtual de acuerdo con el pedido del Cliente;
- la puntuación de los monederos de Moneda Virtual de los que se recibe la Moneda Virtual.

Si el Cliente da orden de transacción que supera el umbral establecido o de transacción al monedero de Moneda Virtual con puntuación de alto riesgo (por ejemplo, monederos relacionados con el fraude, la delincuencia, etc.), la transacción será aprobada manualmente por el Empleado, quien evaluará, antes de la aprobación, la necesidad de aplicar cualquier medida de DDC adicional (por ejemplo, aplicar medidas de DDC, preguntar la fuente y el origen de los fondos o solicitar información adicional sobre la transacción).

Al **supervisar las transacciones**, el Empleado evaluará la transacción con vistas a detectar actividades y transacciones que:

- se desvían de lo que hay motivos para esperar en función de las medidas de DDC realizadas, los servicios prestados, la información facilitada por el Cliente y otras circunstancias (por ejemplo, superación del volumen estimado de transacciones, envío de Moneda Virtual cada vez a un nuevo monedero de Moneda Virtual, volumen de transacciones superior al límite);
- sin desviarse según la cláusula anterior, puede ser asumido como parte de un Blanqueo de Capitales o Financiación del Terrorismo;
- puede afectar a la puntuación del perfil de riesgo del Cliente.

En el caso de que se detecte el hecho mencionado, el Empleado deberá notificarlo a MLRO y posponer cualquier transacción del Cliente hasta la decisión de MLRO al respecto.
Además de lo anterior, el MLRO revisará la transacción de la empresa con regularidad (al menos una vez por semana) para garantizar que:

- los Empleados de la Empresa cumplieron correctamente las obligaciones mencionadas;
- no hay transacciones ni patrones de transacciones que sean complicados, de alto valor e inusuales y que no tengan un propósito económico o legítimo razonable u obvio o que no sean característicos de las características específicas.

La Empresa **identifica la fuente[21] y el origen[22] de los fondos** utilizados en la(s) transacción(es) si es necesario. La necesidad de identificar la fuente y el origen de los fondos depende de las actividades previas del Cliente, así como de otra información conocida. Por lo tanto, la identificación de la fuente y el origen de los fondos utilizados en la transacción se realizará en los siguientes casos:

- las transacciones superan los límites establecidos por la Compañía;
- las transacciones no se corresponden con la información previamente conocida sobre el Cliente;
- la Empresa quiere o debe razonablemente considerar necesario evaluar si las transacciones corresponden a la información previamente conocida sobre elCliente;
- la empresa sospecha que las transacciones indican actividades delictivas, blanqueo de capitales o financiación del terrorismo o que la relación de las transacciones con el blanqueo de capitales o la financiación del terrorismo es probable, incl. transacciones complicadas, de alto valor e inusuales y patrones de transacción que no tienen ningún propósito económico o legítimo razonable u obvio o que no son característicos de las características específicas del negocio en cuestión.

APLICACIÓN DE SANCIONES

Tras la entrada en vigor, modificación o finalización de las Sanciones, la Empresa verificará si el Cliente, su Propietario Beneficiario o una persona que tenga previsto mantener la Relación Comercial o realizar una transacción con ellos es objeto de Sanciones. Si la Empresa identifica a una persona que es objeto de Sanciones o que la transacción prevista o realizada por ella incumple las Sanciones, la Empresa aplicará las Sanciones e informará de ello al FCIS en un plazo de 3 horas.

Procedimiento de identificación del sujeto de las sanciones y de una transacción que infringe las sanciones

La Empresa utilizará como mínimo las siguientes fuentes (bases de datos) para verificar la relación del Cliente con las Sanciones:

- Una lista consolidada de las sanciones de la UE;
- Una lista consolidada de las sanciones de las Naciones Unidas
- Oficina de Control de Activos Extranjeros (OFAC).

Además de las fuentes mencionadas, la Empresa podrá utilizar cualquier otra fuente por decisión del Empleado que esté aplicando medidas de DDC.

[21] **el origen de los fondos** utilizados en la transacción es la razón, la explicación y la base (relación jurídica y su contenido) por la que se transfirieron los fondos
[22] **el origen de los fondos** utilizados en la transacción es la actividad por la que se ganaron o recibieron los fondos

Para verificar que los nombres de las personas resultantes de la investigación coinciden con los de las personas que figuran en una notificación que contiene sanción(es), se utilizarán sus datos personales, cuyas características principales son, para una persona jurídica, su nombre o marca, código de registro o fecha de registro, y para una persona física, su nombre e identificación personal o fecha de nacimiento.

Con el fin de establecer la identidad de las personas especificadas en el acto o notificación legal pertinente que sean las mismas que las identificadas como resultado de la consulta a las bases de datos, la Empresa deberá analizar los nombres de las personas encontradas como resultado de la consulta basándose en el posible efecto de los factores que distorsionan los datos personales (por ejemplo, transcripción de nombres extranjeros, orden diferente de las palabras, sustitución de diacríticos o letras dobles, etc.).

La Empresa realizará la verificación mencionada de forma continua en el curso de una Relación Comercial establecida. La frecuencia de las verificaciones continuas dependerá del perfil de riesgo del Cliente:

- una vez por semana para el perfil de alto riesgo Cliente;
- una vez al mes para el Cliente de perfil de riesgo medio;
- una vez al trimestre para el Cliente de perfil de bajo riesgo.

Si el Empleado tiene dudas de que una persona sea objeto de Sanciones, deberá notificarlo inmediatamente al MLRO o al miembro del Consejo de Administración. En este caso, el MLRO o el miembro del Consejo de Administración decidirán si solicitan o adquieren datos adicionales de la persona o notifican inmediatamente su sospecha al FCIS.

La Empresa adquirirá principalmente información adicional por su cuenta sobre la persona que mantiene una Relación Comercial o está realizando una transacción con ella, así como sobre la persona que tiene la intención de establecer una Relación Comercial, realizar una transacción o un acto con ella, prefiriendo la información procedente de una fuente creíble e independiente. Si, por alguna razón, dicha información no está disponible, la Empresa preguntará a la persona que mantiene la Relación de Negocios o está realizando una transacción o un acto con ellos, así como a la persona que tiene la intención de establecer una Relación de Negocios, realizar una transacción o un acto con ellos, si la información procede de una fuente creíble e independiente y evaluará la respuesta.

Acciones al identificar al sujeto de las sanciones o una transacción que viola las sanciones

Si el Empleado de la Empresa tiene conocimiento de que el Cliente que mantiene una Relación de Negocios o está realizando una transacción con la Empresa, así como una persona que pretende establecer la Relación de Negocios o realizar una transacción con la Empresa, es objeto de Sanciones, el Empleado deberá notificar inmediatamente al MLRO o al miembro del Consejo de Administración, acerca de la identificación del objeto de Sanciones, de la duda al respecto y de las medidas adoptadas.

El MLRO o el miembro del Consejo de Administración se negarán a concluir una transacción o procedimiento, tomarán las medidas previstas en el acto sobre la imposición o aplicación de las sanciones y notificarán inmediatamente al FCIS sus dudas y las medidas adoptadas.

Al identificar al sujeto de las sanciones, es necesario identificar las medidas que se toman para sancionar a esta persona. Estas medidas se describen en el acto jurídico por el que se aplica la

Sanciones, por lo que es necesario identificar la sanción exacta que se aplica contra la persona para garantizar la aplicación legal y adecuada de las medidas.

RECHAZO A LA TRANSACCIÓN O RELACIÓN COMERCIAL Y SU TERMINACIÓN

Se prohíbe a la Empresa establecer una Relación Comercial y se pondrá fin a la Relación Comercial o transacción establecida (a menos que sea objetivamente imposible hacerlo) en caso de que:

- la empresa sospeche de blanqueo de dinero o financiación del terrorismo;
- es imposible que la Empresa aplique las medidas de DDC, porque el Cliente no presenta los datos pertinentes o se niega a presentarlos o los datos presentados no dan motivos para asegurarse de que los datos recopilados son adecuados;
- el Cliente cuyo capital está constituido por acciones al portador u otros títulos al portador desea establecer la Relación Comercial;
- el Cliente que es una persona física detrás de la cual se encuentra otra persona, realmente beneficiaria, quiere establecer la Relación Comercial (sospecha que se utiliza una persona que actúa como tapadera);
- el perfil de riesgo del Cliente se ha vuelto inadecuado con el apetito de riesgo de la Empresa (es decir, el nivel de perfil de riesgo del Cliente es "prohibido").

En caso de terminación de la Relación Comercial de conformidad con el presente capítulo, la Empresa transferirá los activos del Cliente en un plazo razonable, pero preferiblemente no más tarde de un mes tras la terminación y en su totalidad a una cuenta abierta en una entidad de crédito que esté registrada o cuyo domicilio social se encuentre en un estado contratante del Espacio Económico Europeo o en un país en el que se apliquen requisitos iguales a los establecidos en las directivas pertinentes del Parlamento Europeo y del Consejo. En casos excepcionales, los activos podrán transferirse a una cuenta distinta de la del Cliente o emitirse en efectivo. Independientemente del destinatario de los fondos, la información mínima facilitada en inglés en los datos de pago de la transferencia de los activos del Cliente es que la transferencia está relacionada con la finalización extraordinaria de la relación con el Cliente.

OBLIGACIÓN DE INFORMAR

La Compañía debe suspender la transacción sin tener en cuenta el importe de la misma (salvo en los casos en que sea objetivamente imposible debido a la naturaleza de la Operación Monetaria o transacción, la forma de ejecución de la misma u otras circunstancias) y a través de su MLRO debe informar al FCIS sobre la actividad o las circunstancias que identifiquen en el curso de las actividades económicas y por las que:

- la Empresa ha establecido que el Cliente está llevando a cabo una transacción sospechosa;

- la Empresa sepa o sospeche que se han obtenido activos de cualquier valor directa o indirectamente de una actividad delictiva o de la participación en dicha actividad.

Las características mínimas de las transacciones sospechosas figuran en las directrices elaboradas por el FCIS (uno de los anexos de estas Directrices).

Los informes especificados anteriormente deben realizarse antes de la finalización de la transacción si la Empresa sospecha o sabe que se están cometiendo delitos de Blanqueo de Dinero o Financiación del Terrorismo o delitos relacionados y si dichas circunstancias se identifican antes de la finalización de la transacción.

En caso de que surja la necesidad de dicho informe, el Empleado del que se tenga conocimiento de dicha necesidad deberá notificarlo inmediatamente al MLRO.

En cualquier caso (es decir, también en la situación en la que se identifique una actividad o circunstancia después de la realización de la transacción), **la obligación de notificación de los informes mencionados debe realizarse inmediatamente, pero no más tarde de tres horas laborables** después de la identificación de la actividad o circunstancia o de la aparición de la sospecha real (es decir, la situación en la que la sospecha no puede disiparse).

Obligación de informar sobre tipos específicos de transacciones

La Compañía a través de su MLRO debe enviar información al FCIS a más tardar dentro de los 7 días hábiles siguientes a la identificación de las transacciones de cambio de Moneda Virtual o transacciones en Moneda Virtual, si el valor diario de dicha(s) transacción(es) es igual o superior a 15.000 euros o la cantidad equivalente en moneda extranjera o Moneda Virtual, independientemente de si la transacción se concluye en una o más transacciones monetarias relacionadas.

En el caso especificado anteriormente la información presentada al FCIS deberá incluir:

- los datos que confirman la identidad del Cliente, y cuando la transacción se realiza a través de un representante - también los datos que confirman la identidad de su representante;
- el importe de la transacción;
- la divisa en la que se ejecutó la transacción;
- la fecha de ejecución de la transacción;
- la forma de ejecución de la Operación Monetaria;
- la entidad en cuyo beneficio se ejecutó la Operación Monetaria (si es posible);
- otros datos especificados en las instrucciones FCIS pertinentes.

Todos los informes descritos en este capítulo se enviarán de acuerdo con las directrices de información de la empresa a través de un canal seguro que garantice la total confidencialidad (uno de los anexos de estas directrices).

La Empresa, una unidad estructural de la Empresa, un miembro del Consejo de Administración, el MLRO y el Empleado tienen prohibido informar a una persona, su Propietario Beneficiario, representante o tercero sobre un informe presentado sobre ellos al FCIS, un plan para presentar dicho informe o la ocurrencia

de denuncia, así como sobre un precepto del FCIS o sobre el inicio de un procedimiento penal.

OBLIGACIÓN DE FORMACIÓN

La Empresa se asegura de que sus Empleados, sus contratistas y otras personas que participen en el negocio de forma similar y que realicen tareas laborales que sean de importancia para prevenir el uso del negocio de la Empresa para el Blanqueo de Dinero o la Financiación del Terrorismo ("Personas Relevantes") tengan las cualificaciones pertinentes para estas tareas laborales. Cuando se contrata o contrata a una Persona Relevante, las cualificaciones de la Persona Relevante se comprueban como parte del proceso de contratación/nombramiento mediante la realización de una verificación de antecedentes, que se documenta utilizando un formulario estándar especial que evalúa la idoneidad del empleado.

De conformidad con los requisitos aplicables a la Sociedad sobre la garantía de la idoneidad de las Personas Relevantes, la Sociedad se asegura de que dichas personas reciban la formación e información adecuadas de forma continua para poder cumplir con las obligaciones de la Sociedad de conformidad con la legislación aplicable. A través de la formación se garantiza que dichas personas tengan conocimientos en el ámbito de la lucha contra el blanqueo de capitales y la financiación del terrorismo en la medida adecuada teniendo en cuenta las tareas y la función de la persona. La formación debe proporcionar, ante todo, información sobre todos los métodos más contemporáneos de blanqueo de capitales y financiación del terrorismo y los riesgos que de ellos se derivan.

Esta formación hace referencia a las partes pertinentes del contenido de las normas y reglamentos aplicables, la evaluación de riesgos de la empresa, las directrices y procedimientos de la empresa y la información que debe facilitar a dichas Personas Relevantes la detección de sospechas de blanqueo de capitales y financiación del terrorismo. La formación se estructura en función de los riesgos identificados mediante la política de evaluación de riesgos.

El contenido y la frecuencia de la formación se adaptan a las tareas y la función de la persona en cuestiones relacionadas con las medidas ALD/CFT. Si las directrices se actualizan o modifican de algún modo, el contenido y la frecuencia de la formación se adaptan adecuadamente.

Para los nuevos Empleados, la formación comprende una revisión del contenido de las normas y reglamentos aplicables, la política de evaluación de riesgos de la Empresa, estas Directrices y otros procedimientos pertinentes.

Los empleados y los miembros del Consejo de Administración reciben formación continua bajo los auspicios del MLRO de acuerdo con el siguiente plan de formación:

- Periodicidad: al menos una vez al año para los miembros del Consejo de Administración. Al menos una vez al año para los Empleados de la Empresa y la Persona Relevante contratada.
- Alcance: revisión de las normas y reglamentos aplicables, las directrices de la empresa y otros procedimientos pertinentes. Información específica relativa a las características nuevas/actualizadas en las normas y reglamentos aplicables. Informe e intercambio de experiencias relativas a las transacciones revisadas desde la formación anterior.

Además de lo anterior, se mantiene informadas a las Personas Relevantes de forma continua sobre las nuevas tendencias, patrones y métodos y se les proporciona otra información relevante para la prevención del Blanqueo de Capitales y la Financiación del Terrorismo.

La formación impartida debe documentarse electrónicamente y confirmarse con la firma de la persona pertinente. Esta documentación debe incluir el contenido de la formación, los nombres de los participantes y la fecha de la formación.

RECOGIDA Y ALMACENAMIENTO DE DATOS, CUADERNOS DE BITÁCORA

La Empresa, a través de la persona (incl. Empleados, miembros del Consejo de Administración y MLRO) que reciba en primer lugar la información o los documentos pertinentes, registrará y conservará los siguientes datos:

- todos los datos recogidos en el marco de la aplicación de las medidas de DCC;
- información sobre las circunstancias de la denegación del establecimiento de la Relación Comercial por parte de la Empresa;
- las circunstancias de la negativa a establecer Relaciones Comerciales por iniciativa del Cliente si la negativa está relacionada con la aplicación de medidas de DDC por parte de la Empresa;
- información sobre todas las operaciones realizadas para identificar a la persona que participa en la transacción o al Propietario Beneficiario del Cliente;
- información si es imposible realizar las medidasCDD;
- información sobre las circunstancias de la finalización de la relación comercial en relación con la imposibilidad de aplicar las medidas DDC
- la fecha o el período de cada transacción y una descripción del contenido de la transacción, incluido el importe de la transacción, la divisa y el número de cuenta u otro identificador (incluido el hash de las transacciones en moneda virtual y los monederos de moneda virtual relacionados con la transacción);
- información que sirva de base para las obligaciones de información especificadas en las Directrices;
- datos de transacciones o circunstancias sospechosas o inusuales de las que no se haya notificado al SIF (por ejemplo, transacciones complejas o inusualmente grandes, transacciones realizadas siguiendo un patrón inusual y transacciones que no tengan un propósito económico o lícito aparente, Relaciones Comerciales u Operaciones Monetarias con clientes de Terceros Países en los que las medidas para prevenir el Blanqueo de Capitales y/o la Financiación del Terrorismo sean insuficientes o no cumplan las normas internacionales según la información publicada oficialmente por organizaciones intergubernamentales internacionales).

Algunos de los datos especificados anteriormente se anotarán en el libro de registro (como se describe más adelante) en orden cronológico sobre la base de los documentos que confirmen una Operación Monetaria o transacción u otros documentos legalmente válidos relacionados con la ejecución de Operaciones Monetarias o transacciones, inmediatamente, pero a más tardar dentro de los 3 días hábiles siguientes a la ejecución de una Operación Monetaria o transacción.

Los datos especificados anteriormente deberán conservarse durante 8 años después de la expiración de la relación comercial o de la transacción de finalización. Los datos relacionados con el cumplimiento de la obligación de informar deberán conservarse durante 5 años tras el cumplimiento de la obligación de informar.

La correspondencia de una Relación Comercial con el Cliente debe conservarse durante 5 años a partir de la fecha de finalización de las transacciones o de la Relación Comercial.

Los documentos y datos deben conservarse de forma que permitan responder de forma exhaustiva e inmediata a las consultas realizadas por el FCIS o, de conformidad con la legislación, por otras autoridades de supervisión, autoridades de investigación o el tribunal.

La Compañía implementa todas las normas de protección de datos personales en aplicación de los requisitos derivados de la legislación aplicable. La Empresa está autorizada a procesar los datos personales recogidos en la aplicación de la DDC únicamente con el fin de prevenir el blanqueo de capitales y la financiación del terrorismo, y los datos no deben procesarse adicionalmente de una manera que no cumpla el objetivo, por ejemplo, con fines de marketing.

La Empresa suprime los datos conservados tras la expiración del plazo, a menos que la legislación que regula el ámbito correspondiente establezca un procedimiento diferente. Sobre la base de un precepto de la autoridad de control competente, los datos de importancia para la prevención, detección o investigación del blanqueo de capitales o de la financiación del terrorismo podrán conservarse durante un período más largo, pero no durante más de dos años tras la expiración del primer plazo.

Mantenimiento de los libros de registro

A los efectos del cumplimiento de las obligaciones en materia de lucha contra el blanqueo de capitales, la empresa llevará (cumplimentará) los siguientes libros de registro en los que se reflejarán las operaciones y transacciones monetarias (en lo sucesivo, libros de registro):

- libro de registro de los clientes que realicen transacción(es) en Moneda Virtual independientemente de la circunstancia si la(s) transacción(es) se realizan ocasionalmente o en el curso de la Relación Comercial;
- Libro de registro de Operaciones Monetarias o transacciones realizadas entre el Cliente y la Empresa con anterioridad cuando la Empresa esté obligada a aplicar medidas de DDC;
- Libro de registro de informes[23] y transacciones y operaciones monetarias sospechosas;
- Libro de registro de los Clientes con los que se hayan rechazado o finalizado transacciones o Relaciones Comerciales en circunstancias relacionadas con infracciones del procedimiento de prevención del Blanqueo de Capitales y/o de la Financiación del Terrorismo.

El libro de registro de los Clientes que realicen transacciones en Moneda Virtual incluirá lo siguiente:

- datos que confirman la identidad del Cliente y de su representante (si la transacción monetaria se realiza o la transacción se concluye a través de un representante): nombre y apellidos de una persona física, código de identificación personal (fecha de nacimiento de un Cliente extranjero), ciudadanía; código personal, si se proporciona tal código;
- en el caso de transacciones o transacciones en Moneda Virtual, no sea objetivamente posible identificar al beneficiario, otra información que permita a la Dirección de Moneda Virtual ser

[23] como se describe en el capítulo correspondiente de estas Directrices

vinculadas a la identidad del propietario de la Moneda Virtual: dirección de Protocolo de Internet (IP), dirección de correo electrónico, etc;

- Dirección(es) de la moneda virtual relacionada(s) con la transacción y hash(s) de la transacción;
- método de transacción: depósito o retirada de Moneda Virtual, la Moneda Virtual se cambia por dinero o viceversa, la Moneda Virtual se cambia por otra Moneda Virtual, la transacción de cambio de Moneda Virtual fue mediada (cambio p2p);

El libro de registro de las Operaciones Monetarias o transacciones realizadas entre el Cliente y la Empresa con anterioridad cuando la Empresa esté obligada a aplicar medidas de DDC incluirá lo siguiente:

- datos que confirman la identidad del Cliente y de su representante (si la transacción monetaria se realiza o la transacción se concluye a través de un representante): nombre y apellidos de una persona física, código de identificación personal (fecha de nacimiento de un Cliente extranjero), ciudadanía; código personal, si se proporciona tal código;
- Datos sobre la transacción u operación monetaria: fecha de la transacción, descripción de los activos objeto de la transacción (dinero en efectivo, bienes inmuebles, moneda virtual, etc.) y su valor (cantidad de dinero, moneda en la que se realiza la transacción u operación monetaria, valor de mercado de los activos, etc.);
- método de transacción: La Moneda Virtual se cambia por dinero o viceversa, elCliente realiza un pago por adelantado para comprar Moneda Virtual, etc.

El libro de registro de informes, operaciones monetarias sospechosas y transacciones incluirá lo siguiente en orden cronológico:

- datos que confirman la identidad del Cliente y de su representante (si la transacción monetaria se realiza o la transacción se concluye a través de un representante): nombre y apellidos de una persona física, código de identificación personal (fecha de nacimiento de un Cliente extranjero), ciudadanía; código personal, si se proporciona tal código;
- el criterio aprobado por el Ministerio del Interior de la República de Lituania, según el cual se reconoce que la operación o transacción monetaria del Cliente se considera sospechosa, la operación o transacción cumple;
- Método de realización de la operación o transacción monetaria sospechosa;
- Fecha y hora de la operación o transacción monetaria sospechosa, caracterización de los activos objeto de la transacción (efectivo, etc.) y su valor (cantidad de dinero, divisa utilizada para la realización de la operación o transacción monetaria, valor de mercado de los activos);
- los datos del beneficiario o beneficiarios de la transacción: nombre completo y número de identificación personal de una persona física (en caso de un extranjero: fecha de nacimiento, si se dispone de ella, número de identificación personal o cualquier otra secuencia única de símbolos asignada al individuo en cuestión para su identificación personal), y en caso de una persona jurídica, título, forma jurídica, domicilio social y número de registro, si se le ha asignado;

- Datos de contacto del Cliente: número(s) de teléfono, dirección(es) de correo electrónico, persona(s) de contacto, sus números de teléfono, direcciones de correo electrónico, etc;
- Descripción de los activos que el Cliente no puede controlar o utilizar desde el momento de la suspensión de la operación o transacción monetaria sospechosa (lugar y otra información que caracterice los activos);
- En caso de que no se haya suspendido una transacción monetaria o una operación sospechosa, razones pertinentes;
- Métodos de gestión de cuentas;
- Otros detalles relevantes, según la decisión del empleado.

La Empresa incluirá en el libro de registro de clientes, donde se hayan terminado las transacciones o Relaciones Comerciales lo siguiente, en orden cronológico:

- datos que confirman la identidad del Cliente y de su representante (si la transacción monetaria se realiza o la transacción se concluye a través de un representante): nombre y apellidos de una persona física, código de identificación personal (fecha de nacimiento de un Cliente extranjero), ciudadanía; código personal, si se proporciona tal código;
- Datos sobre la transacción u operación monetaria: fecha de la transacción, descripción de los activos objeto de la transacción (dinero en efectivo, bienes inmuebles, moneda virtual, etc.) y su valor (cantidad de dinero, moneda en la que se realiza la transacción u operación monetaria, valor de mercado de los activos, etc.);
- en el caso de transacciones en Moneda Virtual o de transacciones en las que no sea objetivamente posible identificar al beneficiario, otra información que permita vincular la dirección de la Moneda Virtual a la identidad del propietario de la Moneda Virtual: dirección de protocolo de Internet (IP), dirección de correo electrónico, etc;
- en el caso de transacciones de Moneda Virtual Dirección(es) de Moneda Virtual relacionada(s) con la transacción y hash(s) de la transacción;
- los datos sobre el beneficiario o beneficiarios del Cliente: nombre completo y número de identificación personal de una persona física (en caso de un extranjero: fecha de nacimiento, si está disponible, número de identificación personal o cualquier otra secuencia única de símbolos asignada al individuo en cuestión para su identificación personal), y en caso de una persona jurídica, título, forma jurídica, domicilio social y número de registro, si éste le ha sido asignado;
- Motivos de rescisión de transacciones o Relaciones Comerciales relativos a infracciones del procedimiento de prevención del Blanqueo de Capitales y/o Financiación del Terrorismo.

Procedimiento para llevar y administrar los libros de registro

El almacenamiento de los datos de registro será completado y conservado en un soporte electrónico por el miembro del Consejo de Administración, si se encuentra en viaje de negocios, o no está disponible por otras razones válidas, otro Empleado, como se indica en la orden especial del director, estableciendo el alcance de las funciones y responsabilidades asignadas a una persona que actúe como sustituto.

El Consejo de Administración designará a un Empleado encargado de garantizar la protección de los datos incluidos en los libros de registro, y procesados en un soporte electrónico, frente a la supresión, alteración o utilización no autorizada por parte de terceros no autorizados.

Los detalles se almacenarán utilizando un software que permita la exportación de los detalles almacenados a Microsoft Office Excel, Word, o un software de código abierto equivalente, sin dañar la integridad de los detalles.

El mantenimiento de los libros de registro será verificado por un miembro del Consejo de Administración, si él/ella está en viaje de negocios, o no está disponible por otras razones válidas, otro Empleado responsable designado por la Empresa, como se indica en la orden especial del director, estableciendo el alcance de los deberes y responsabilidades asignados a una persona que actúe como sustituto.

Se prohíbe a los Empleados de la Empresa informar, o hacer saber de otro modo, a cualquier Cliente u otros individuos que se comunica al FCIS información sobre las Operaciones Monetarias que tienen lugar, o las transacciones realizadas por un Cliente, o la investigación resultante.

CONTROL INTERNO DE LA EJECUCIÓN DE LAS DIRECTRICES

La ejecución de las Directrices será controlada internamente por el miembro del Consejo de Administración, o por el Empleado designado por el Consejo de Administración para desempeñar las funciones pertinentes (en lo sucesivo en este capítulo - Responsable de Control Interno). El Responsable de Control Interno deberá disponer de la competencia, las herramientas y el acceso a la información pertinentes en todas las unidades estructurales de la Empresa.

El Responsable de Control Interno desempeñará funciones de control interno al menos en los siguientes ámbitos:

- el cumplimiento por parte de la empresa de la política de evaluación de riesgos establecida y de la propensión al riesgo;
- Aplicación de las medidas de DCC;
- aplicación de sanciones;
- la obligación de la empresa de negarse a la transacción o relación comercial y su terminación;
- la obligación de la empresa de informar al FCIS;
- la obligación de formación de la empresa en relación con los requisitos ALD/CFT;
- la obligación de la empresa de recopilar y conservar los datos.

Las medidas exactas para realizar el control interno serán determinadas por el Responsable de Control Interno y deben corresponder al tamaño de la empresa y a su naturaleza, alcance y nivel de complejidad de las actividades y servicios prestados. Las Oficinas de Control Interno deberán considerar al menos los campos de examen especificados anteriormente. Las medidas de control interno se realizarán en el momento que determine el Responsable de Control Interno con la frecuencia que éste fije, al menos una vez al mes, si la naturaleza de la medida no prevé expresamente otra cosa. Los resultados de la aplicación de las medidas de control interno (en adelante, en este capítulo, los Datos de Control Interno) se guardarán por separado de otros datos y se conservarán durante 5 años. Sólo los miembros del Consejo de Administración y el Responsable de Control Interno podrán tener acceso a los Datos de Control Interno.

Datos de Control. El Responsable de Control Interno podrá facilitar el acceso a los Datos de Control Interno a otros Empleados o a terceros (por ejemplo, asesores, auditores, etc.) únicamente con el consentimiento previo del Consejo de Administración. Las personas que tengan acceso a los Datos de Control Interno no deberán revelarlos a nadie sin el consentimiento previo del Consejo de Administración.

Los Datos de Control Interno se guardarán en orden cronológico con un formato que permita analizarlos y relacionarlos de forma comprensible con otros datos relevantes.

El responsable de control interno presentará el informe de control interno al Consejo de Administración al menos trimestralmente y a la junta general de accionistas de la empresa al menos una vez al año. El informe de control interno proporcionado incluirá como mínimo lo siguiente:

- periodo de ejercicio del control interno;
- nombre y cargo de la persona que ejecuta el control interno;
- descripción de las medidas de control interno que se han llevado a cabo;
- resultados del control interno;
- conclusiones generales del control interno ejercido;
- deficiencias determinadas, que fueron eliminadas en el periodo de ejercicio del control interno;
- deficiencias determinadas, que no fueron eliminadas al final del periodo de ejercicio del control interno;
- medidas que es necesario aplicar para la eliminación de las deficiencias determinadas.

El Consejo de Administración revisará el informe de control interno presentado y tomará una resolución al respecto. Se notificará al responsable de control interno la esencia de dicha resolución en un formato que pueda reproducirse por escrito. Por esta razón, el Consejo de Administración está obligado a:

- analizar los resultados del control interno realizado;
- poner en marcha acciones para eliminar las deficiencias ocurridas.

La empresa debe revisar y, si es necesario, actualizar el procedimiento de control interno al menos una vez al año y en los siguientes casos:

- tras la publicación por parte de la Comisión Europea de los resultados de una evaluación del riesgo de blanqueo de capitales y financiación del terrorismo en toda la UE (disponible en la página web de la Comisión Europea http://ec.europa.eu);
- tras la publicación de los resultados de la Evaluación Nacional del Riesgo de Blanqueo de Capitales y Financiación del Terrorismo (publicada en la sección "Evaluación Nacional del Riesgo de Blanqueo de Capitales y Financiación del Terrorismo" del apartado "Prevención del Blanqueo de Capitales" de la página web www.fntt.lt);
- tras recibir una instrucción del FCIS para reforzar los procedimientos de control interno aplicables;

- en caso de acontecimientos o cambios significativos en la gestión y las operaciones del operador de dinero virtual depositario y del operador de cambio de moneda virtual.

Evaluación y propensión al riesgo

El objetivo de la aplicación de medidas de control interno para el cumplimiento por parte de la empresa de la política de evaluación de riesgos establecida (incluido el apetito de riesgo establecido) es el examen de las siguientes circunstancias:

- La empresa establece y utiliza un enfoque basado en el riesgo cuando presta servicios a los clientes (por ejemplo, medidas de DDC aplicadas de acuerdo con el nivel de riesgo);
- La empresa determinó los factores que afectan al surgimiento de riesgos de BC/FT y los factores determinados son relevantes;
- La empresa determinó y evaluó el LD/FT de todos los servicios que presta;
- La empresa compone el perfil de riesgo del cliente antes de realizar las transacciones o crear la relación comercial;
- La empresa actualiza periódicamente el perfil de riesgo del cliente;
- La empresa sigue el apetito de riesgo establecido;
- La empresa mantiene registros de todos los incidentes de acuerdo con la política de evaluación de riesgos establecida;
- La política de evaluación de riesgos se revisó durante el año pasado y no hay información de que la MLRO hubiera requerido una revisión anterior.

Aplicación de medidas de diligencia debida con respecto al cliente

El objetivo de la aplicación de medidas de control interno para el cumplimiento por parte de la empresa de la aplicación de medidas de DDC es un examen de las siguientes circunstancias:

- la Empresa aplique las medidas de DDC prescritas por las Directrices a todos los Clientes pertinentes;
- la empresa recopila los documentos y la información adecuados al aplicar las medidas de DDC;
- la empresa verifica adecuadamente los datos y documentos recopilados al aplicar las medidas de DDC;
- la empresa aplica el nivel pertinente de medidas DDC (por ejemplo, medidas DDE, etc.);
- la empresa aplica medidas de EDD adecuadas a clientes específicos (por ejemplo, PEP, país de alto riesgo, etc.);
- la empresa realiza la identificación de los clientes de acuerdo con el procedimiento establecido;
- la empresa identifique correctamente al representante o representantes de los clientes;
- la empresa identifique correctamente a los beneficiarios efectivos de los clientes;
- la empresa identifique correctamente la condición de PEP de los clientes;

- la empresa identifique adecuadamente el propósito y la naturaleza de la relación comercial o transacción;
- la empresa supervisa adecuadamente las relaciones comerciales con los clientes.

Al aplicar las medidas EDD con respecto a las personas físicas/entidades jurídicas residentes/establecidas en terceros países de alto riesgo determinados por la Comisión Europea, la Compañía debe:

- obtener información adicional sobre el Cliente y BO;
- obtener información adicional sobre la naturaleza prevista de la Relación Comercial;
- obtener información sobre el origen de los fondos y el patrimonio del Cliente y BO;
- obtener información sobre los motivos de las transacciones previstas o realizadas;
- obtener la aprobación del Alto Directivo para establecer Relaciones Comerciales con estos Clientes o el consentimiento para continuar las Relaciones Comerciales con dichos Clientes
- realizar EDD aumentando el número y el momento de los controles y seleccionando los tipos de transacciones que requerirán una investigación más profunda;
- garantizar que el primer pago de un Cliente se realice desde una cuenta abierta en una entidad de crédito cuando dicha entidad de crédito esté establecida en un Estado miembro de la UE o en un tercer país que ofrezca requisitos equivalentes a los de la Ley y bajo la supervisión de las autoridades competentes.

Actualmente, los terceros países de alto riesgo determinados por la Comisión Europea figuran en el Reglamento Delegado de la Comisión nº 2016/1675, de 14 de julio de 2016, por el que se completa la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo mediante la identificación de terceros países de alto riesgo con deficiencias estratégicas y modificado por los siguientes reglamentos:

Reglamento Delegado nº 2018/105 de la Comisión, de 27 de octubre de 2017, por el que se modifica el Reglamento Delegado (UE) 2016/1675, en lo que respecta a la inclusión de Etiopía en la lista de terceros países de alto riesgo del cuadro del punto I del anexo;

Reglamento Delegado n.º 2018/212 de la Comisión, de 13 de diciembre de 2017, que modifica el Reglamento Delegado (UE) 2016/1675 por el que se completa la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, en lo que respecta a la adición de Sri Lanka, Trinidad y Tobago y Túnez al cuadro del punto I del anexo;

Reglamento Delegado nº 2018/1467 de la Comisión, de 27 de julio de 2018, que modifica el Reglamento Delegado (UE) 2016/1675 por el que se completa la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, en lo que respecta a la adición de Pakistán al cuadro del punto I del anexo.

Basándose en los resultados de la Evaluación Nacional de Riesgos de Blanqueo de Dinero y Financiación del Terrorismo, en caso de que se identifique un alto nivel de riesgos de BC/FT en la República de Lituania relacionados con los terceros países de alto riesgo determinados por la Comisión Europea, la Empresa, al entablar o llevar a cabo relaciones de corresponsalía internacional con instituciones financieras establecidas en estos países, deberá adoptar una o varias medidas adicionales para reducir eficazmente el riesgo de BC/FT:

- aplicar medidas adicionales de supervisión reforzada de las relaciones comerciales para reducir el riesgo de BC/FT;
- hacer más estricta la notificación de operaciones y transacciones monetarias sospechosas;
- limitar las Relaciones Comerciales o transacciones con personas físicas o jurídicas establecidas en terceros países de alto riesgo identificados por la Comisión Europea.

Si estas medidas adicionales no son suficientes para reducir dicho riesgo, la empresa deberá negarse a entablar o dejar de entablar, o poner fin a la relación de corresponsalía internacional con dichas instituciones financieras.

Actualmente, los terceros países de alto riesgo inscritos en las listas del GAFI de Estados que presentan graves deficiencias en materia de prevención del LA/FT y de lucha contra estos delitos son: http://www.fatf-gafi.org/countries/#high-risk. Sin embargo, dado que la lista es cambiante, la Compañía tiene que vigilar si no se ha modificado y tomar las medidas oportunas en caso necesario.

Al aplicar las medidas EDD con respecto a las personas físicas/jurídicas residentes/establecidas en terceros países de alto riesgo inscritos en las listas del GAFI de Estados que presentan graves deficiencias en materia de prevención del LA/FT y de lucha contra estos delitos, la Empresa deberá:

- recibir la aprobación del Administrador Principal para concluir la Relación Comercial con dichos Clientes o para continuar la Relación Comercial con dichos Clientes;
- tomar las medidas adecuadas para establecer la fuente de riqueza y el origen de los fondos relacionados con la relación comercial o la transacción;
- realizar un mejor seguimiento continuo de la Relación Comercial con dichos Clientes.

A la hora de determinar qué Clientes plantean altos riesgos de BC/FT, la Empresa debe realizar una evaluación de riesgos de las Relaciones Comerciales. Teniendo en cuenta los resultados de, al menos, la Evaluación de Riesgos de la Empresa, la Evaluación de Riesgos Nacional y la Evaluación de Riesgos Supranacional, la Empresa debe tener especial cuidado al evaluar los riesgos de BC/FT que potencialmente plantean las siguientes personas y entidades:

- comerciantes de mercancías que, en el curso de su actividad, realizan o reciben normalmente cantidades significativas de pagos en efectivo;
- entidades que operan en los subsectores o productos financieros que manejan efectivo (por ejemplo, oficinas de cambio, transferencias de fondos, determinados productos de dinero electrónico);
- determinadas empresas FinTech (es decir, de servicios financieros basados en la tecnología y apoyados por la tecnología), especialmente con un elevado número de relaciones comerciales no presenciales;
- operadores de plataformas de cambio de divisas virtuales y/o proveedores de monederos custodios;
- Otras Entidades Obligadas, especialmente proveedores de servicios de gabinete y/o loterías y máquinas recreativas;
- organizaciones sin ánimo de lucro y otros.

Además, al evaluar los riesgos de blanqueo de capitales y financiación del terrorismo que puedan plantear los clientes, la empresa deberá tener especialmente en cuenta:

- los Clientes para los que se presentó previamente un STR;
- los Clientes que en el pasado fueron incluidos en las listas de sanciones financieras internacionales o nacionales y otras;
- los clientes que sean objeto de una solicitud o información recibida de la UIF, de otras autoridades de investigación prejudicial, de la fiscalía o de un tribunal en relación con información sobre un cliente o sus operaciones o transacciones monetarias que puedan estar relacionadas con el blanqueo de capitales, el financiamiento del terrorismo u otras actividades delictivas.

A la hora de determinar la existencia de un mayor riesgo de BC/FT, la empresa debe evaluar al menos los siguientes factores:

- características del Cliente:
- la relación comercial del cliente se desarrolla en circunstancias inusuales que no tienen un propósito económico aparente o lícito visible;
- el domicilio del Cliente se encuentra en un tercer país;
- las personas jurídicas y los organismos sin personalidad jurídica se dedican a las actividades de empresa individual de gestión inmobiliaria;
- la sociedad tiene accionistas formales que actúan en nombre de otra persona, o posee acciones al portador;
- el efectivo domina el negocio;
- la estructura de capital de la entidad jurídica es aparentemente inusual o excesivamente compleja teniendo en cuenta la naturaleza de las actividades de la entidad jurídica,
- características del producto, servicio, transacción o canal de servicio:
- banca privada;
- producto o transacción puede crear condiciones favorables para el anonimato;
- Las relaciones comerciales o transacciones ocasionales se concluyen o realizan sin presencia física;
- se reciben pagos de terceros desconocidos o no relacionados;
- el producto o la práctica empresarial, incluido el mecanismo de prestación de servicios, son nuevos, también el uso de tecnologías nuevas o en desarrollo que intervienen en el trabajo tanto con productos nuevos como antiguos,
- características del territorio:
- de acuerdo con los datos de los informes o documentos similares del GAFI u otra organización regional similar, se establecen incumplimientos significativos en el sistema de lucha contra el blanqueo de capitales y la financiación del terrorismo con los requisitos internacionales;

- De acuerdo con los datos de las organizaciones gubernamentales y no gubernamentales reconocidas a nivel mundial que supervisan y evalúan el nivel de corrupción, un alto nivel de corrupción u otra actividad delictiva se establezca en el estado;
- el estado está sujeto a sanciones, embargos o medidas similares impuestas, por ejemplo, por la UE o las Naciones Unidas;
- el estado financia o apoya actividades terroristas, o en el territorio del estado operan organizaciones terroristas incluidas en las listas elaboradas por organizaciones internacionales.

Aplicación de sanciones

El objetivo de la aplicación de las medidas de control interno para el cumplimiento por parte de la empresa de la aplicación de las sanciones es un examen de las siguientes circunstancias:

- la Empresa aplica el procedimiento de identificación de un sujeto de Sanciones o de una transacción que viola las Sanciones;
- la Empresa lleva a cabo acciones si identifica a un sujeto de Sanciones o transacción que viole las Sanciones.

Obligación de rechazo de la transacción o relación comercial y su terminación

El objetivo de la aplicación de medidas de control interno para el cumplimiento por parte de la empresa de la obligación de rechazar la transacción o relación comercial y su terminación es un examen de las siguientes circunstancias:

- la Empresa rechaza la transacción o la relación comercial si es obligatoria de acuerdo con las Directrices;
- la empresa rechaza o pone fin a la transacción o a la relación comercial si es obligatorio de acuerdo con las Directrices.

Obligación de informar

El objetivo de la aplicación de las medidas de control interno para que la empresa cumpla con la obligación de informar es un examen de las siguientes circunstancias:

- la empresa envía informes e información al FCIS, si así lo exigen las directrices (incluidas las directrices pertinentes del FCIS);
- los informes enviados al FCIS se cumplimentan de acuerdo con las directrices del FCIS.

Obligación de formación

El objetivo de la aplicación de las medidas de control interno para el cumplimiento por parte de la empresa de la obligación de formación en el ámbito de la lucha contra el blanqueo de capitales y la financiación del terrorismo es un examen de las siguientes circunstancias:

- todos los empleados (incluidos los MLRO y los miembros del Consejo de Administración) reciban la formación pertinente;
- cada empleado (incluidos los MLRO y los miembros del Consejo de Administración) ha recibido formación durante los últimos 360 días.

Obligación de recogida y conservación de datos

El objetivo de la aplicación de medidas de control interno para el cumplimiento por parte de la empresa de la obligación de recopilación y conservación de datos es un examen de las siguientes circunstancias:

- todos los datos que se guardarán de acuerdo con las Directrices (en lo sucesivo, en este capítulo, los Datos guardados) se han guardado correctamente en orden cronológico con un formato que permite analizarlos y relacionarlos de forma comprensible con otros datos relevantes;
- Sólo los Empleados (incluidos MLRO y los miembros del Consejo de Administración) o terceros autorizados tienen acceso a los Datos Guardados;
- todos los cuadernos de bitácora pertinentes se lleven de acuerdo con las Directrices;
- los Datos Guardados en formato electrónico tienen copia de seguridad;
- los datos guardados en otros formatos (por ejemplo, en papel) tienen una copia de seguridad en formato electrónico;
- los Datos Almacenados se suprimen irrevocablemente de conformidad con las Directrices.

ANEXOS

Título del anexo	Descripción del documento
Política de evaluación de riesgos	Establece los principios para la gestión de riesgos de la empresa (incl. evaluación de riesgos y factores de riesgo) en relación con el blanqueo de dinero y Riesgos de financiación del terrorismo.
Perfiles de los clientes	Tabla para la evaluación de riesgos de los clientes y la documentación de esta evaluación. Incluye los factores de riesgo de cada categoría de riesgo.
Procedimiento de incorporación del cliente	Establece las instrucciones para la incorporación del cliente utilizadas en el marco de la aplicación de las medidas de DDC
Cuestionarios	Establece la cantidad de información que se solicitará al aplicar las medidas de DDC (incluida la aplicación de medidas de DDC, la solicitud de SoW/SoF, etc.)
Lista de fuentes	Contiene una lista no exhaustiva de los recursos que pueden utilizarse para la aplicación de las medidas de DDC.
Lista de criterios para el blanqueo de capitales y la identificación de operaciones o transacciones monetarias sospechosas	Instrucciones y ejemplos de transacciones y otras circunstancias que se considerarán sospechosas desde el punto de vista del BC/FT.
La lista de Empleados y sus responsabilidades	La lista de Empleados con sus responsabilidades dentro de las Directrices especificadas
Cuadernos de bitácora	La tabla se utilizará para el mantenimiento de los diarios de navegación.
Formulario de informe MLRO	El formulario de informe, que el MLRO proporcionará trimestralmente al Consejo de Administración
Directrices para cumplimentar los formularios de presentación de información al FCIS	Directrices del FCIS para cumplimentar los formularios pertinentes y los propios formularios.

Suspensión de operaciones o transacciones monetarias sospechosas y presentación de información sobre operaciones o transacciones monetarias sospechosas al FCIS	Las directrices pertinentes del FCIS.
Requisitos técnicos para la identificación del cliente mediante transmisión de vídeo en directo	Directrices del FCIS sobre los requisitos técnicos pertinentes
Protocolo de formación	Borrador del documento que se rellenará para cada formación realizada por la Empresa a las Personas Relevantes (incl. familiarización con las Directrices).
Resolución de aprobación de las Directrices	El proyecto de resolución del alto directivo de la empresa para la aprobación de estas Directrices.

TABLA DE CONTROL DE VERSIONES

Versión	**Fecha de aprobación**	**Cambios Descripción**
1.0	dd.mm.aaaa	Primer número
1.1	28.03.2023	Versión actualizada
1.2	11.07.2023	Versión actualizada
2.0	07.08.2023	Segunda edición
2.1	06.12.2023	Versión actualizada
2.2	18.03.2024	Versión actualizada

Mariana Achim
18.03.2024