EL ALTILLO INTERNATIONAL SCHOOL

PART OF ISP SCHOOLS

# POLÍTICA CONTRA EL BLANQUEO DE CAPITALES

**Fecha de publicación:**

**Fecha de revisión:** noviembre 2026

**Responsable de la política: Director financiero del grupo**

**Introducción y justificación**

Los cambios en la legislación relativa al blanqueo de capitales en todo el mundo han ampliado la definición de blanqueo de capitales y han aumentado el abanico de actividades contempladas en el marco legal. Ya no se trata de una cuestión que afecte únicamente a los bancos y al sector financiero, sino que ahora se aplica a todas las empresas, incluidas International Schools Partnership Limited, nuestras filiales y los colegios que gestionamos. Para combatir el riesgo de blanqueo de capitales y financiación del terrorismo, debemos aplicar políticas y procedimientos contra el blanqueo de capitales (AML) y la financiación del terrorismo (CTF).

Si tiene conocimiento o sospechas de blanqueo de capitales o financiación del terrorismo en relación con cualquier asunto dentro de nuestra empresa, comuníquelo por escrito inmediatamente a su director financiero regional («RFD») local. Realice la denuncia de forma confidencial y no comente el asunto con nadie más (en particular, con terceros externos), ya que hacerlo podría constituir un delito. Encontrará más detalles sobre cómo presentar un informe en la sección 6 más abajo.

Su RFD local, junto con los DCFO según corresponda, considerará entonces si presentar un informe interno al MLRO global: el director financiero del grupo, Darren Mee (correo electrónico: dmee@ispschools.com).

MLRO significa «responsable de notificación de blanqueo de capitales» y es el empleado de ISP designado para supervisar el cumplimiento de las prácticas AML de ISP.

**1. Ámbito de aplicación de la política**

1.1 Se trata de una política obligatoria que se aplica a todas las entidades y negocios propiedad de ISP, controlados o gestionados por ISP (incluidas las escuelas que gestionamos), así como a todos los directores, miembros y personal de ISP (incluidos todos los empleados, contratistas, consultores, asesores jurídicos, personal de apoyo, personal de RR. HH. y de operaciones), ya sean permanentes o con contratos de duración determinada o temporales, incluidos aquellos en prácticas u otras colocaciones temporales («ISP», «nosotros» y «nos»).

1.2 Esta política está diseñada para reflejar la legislación AML y CTF, así como las mejores prácticas aplicables a ISP a nivel mundial. Cuando ha sido necesario, se han creado cláusulas adicionales específicas para determinadas jurisdicciones; estas cláusulas se pueden encontrar en el Anexo A. Esta política debe leerse junto con dichas cláusulas adicionales.

1.3 Esta Política está diseñada para reflejar las conclusiones de la última evaluación de riesgos AML y CTF de ISP y forma parte del modelo general de prevención del delito de ISP. Esta Política se revisará periódicamente y podrá modificarse de vez en cuando.

1.4 Cualquier empleado que incumpla esta Política se enfrentará a medidas disciplinarias, de acuerdo con el procedimiento disciplinario regional local y la legislación laboral local, que podrían dar lugar al despido por falta grave, dependiendo de la gravedad del incumplimiento. Cualquier persona o organización ajena a la empresa que incumpla esta Política podrá ver rescindido su contrato de servicios con efecto inmediato.

**2. Definición de blanqueo de capitales**

2.1 En resumen, el blanqueo de capitales es el proceso de hacer que el dinero generado por una actividad delictiva, como el tráfico de drogas o la financiación del terrorismo, parezca proceder de una fuente legítima. El dinero procedente de la actividad delictiva se considera sucio, y el proceso lo «blanquea» para que parezca limpio.

2.2 Existen diferentes leyes en todo el mundo que regulan el blanqueo de capitales. Cada uno de los delitos de blanqueo de capitales gira en torno al concepto de «bienes delictivos», que debe definirse de manera amplia como cualquier bien; sin embargo, a los efectos de esta Política, los delitos relacionados con el blanqueo de capitales deben entenderse de la siguiente manera:

• ocultar, disimular, convertir o sacar del país bienes de origen delictivo;

• participar o involucrarse en un acuerdo que la persona sabe o sospecha que facilita (por cualquier medio) la adquisición, retención, uso o control de bienes delictivos por parte de otra persona o en su nombre;

• adquirir, utilizar o poseer propiedad delictiva;

• revelar a una persona información que pueda perjudicar una investigación sobre blanqueo de capitales;

• no revelar el conocimiento o la sospecha de blanqueo de capitales (incluida la realización de informes internos y externos pertinentes).

2.3 Determinadas normas sobre blanqueo de capitales se aplican a las transacciones en efectivo que superen determinados importes consulte nuestra Política de control de efectivo para obtener más información sobre los límites específicos de efectivo en su jurisdicción.

**3. Riesgos a los que puede estar expuesta ISP**

3.1 A medida que los bancos y los servicios financieros se someten a una regulación más estricta, los delincuentes pueden buscar lo que consideran objetivos más fáciles en otros sectores para blanquear dinero. Para mitigar el riesgo de que ISP se vea involucrado en el blanqueo de capitales, hemos: (i) llevado a cabo una evaluación de riesgos que identifica y evalúa los principales riesgos de blanqueo de capitales a los que estamos expuestos; (ii) implementado esta Política para abordar formalmente dichos riesgos.

3.2 La siguiente lista recoge ejemplos de actividades «sospechosas» que deberían despertar la preocupación o la sospecha de blanqueo de capitales o financiación del terrorismo. En cada uno de estos casos, ISP debe aplicar los procedimientos de «diligencia debida reforzada» («EDD») que se describen con más detalle a continuación:

• cualquier pago en efectivo de gran cuantía (incluidos varios pagos en efectivo de menor cuantía que sumen una cantidad mayor);

• cheques emitidos por fuentes inusuales;

• cualquier información secreta, engañosa o contradictoria proporcionada con respecto a datos personales como el nombre, la identidad, la dirección y los datos bancarios;

• pagos excesivos frecuentes o cuantiosos y solicitudes de reembolso (especialmente a una cuenta o persona diferente al pagador);

• el pago de tasas de matrícula reembolsables seguido de la no ocupación de una plaza escolar (especialmente cuando va acompañado de una solicitud de envío del importe reembolsable a una cuenta bancaria diferente);

• uso de agentes que no se ajustan a los procedimientos normales relacionados con los depósitos y las tasas de matrícula;

• Recepción de pagos inesperados de terceros, cuyo exceso se transfiere a una cuenta diferente.

• la participación de cualquier persona políticamente expuesta («PEP») y sus personas asociadas en una relación comercial; debemos estar muy atentos y ser cautelosos al tratar con PEP. Una PEP es, en términos generales, cualquier persona que ocupe un cargo público destacado y cuya posición la exponga a un mayor riesgo de blanqueo de capitales. Algunos ejemplos de PEP son:

• altos cargos actuales y antiguos del gobierno o del ejército (eleccionados o no);

• Miembros de alto rango de un partido político.

• altos ejecutivos de empresas comerciales de propiedad estatal;

• familiares de cualquiera de los anteriores o personas que se sepa que son allegadas a cualquiera de los anteriores, ya sea a nivel personal o profesional.

**3.3** La EDD también puede ser apropiada en el caso de solicitantes procedentes de países de alto riesgo y de transacciones realizadas en dichos países (véanse los registros de países de alto riesgo del GAFI y el anexo B). Los países considerados de alto riesgo están sujetos a cambios. Cualquier cambio en la lista de países de alto riesgo mantenida por el GAFI será supervisado por el

Departamento Jurídico del Grupo y comunicado al RFD correspondiente, tras lo cual se acordará un enfoque de EDD.

3.4 También se considerará sospechoso que una deuda sea liquidada por un tercero que no sea la persona directamente responsable del pago de las tasas del estudiante. Aunque en algunos territorios es habitual que las tasas de matrícula sean abonadas por un tercero (por ejemplo, los abuelos, tíos o tías), debemos comprender la relación entre el estudiante y el tercero que desea pagar sus tasas (por ejemplo, los padres) y, en caso necesario, se debe recabar más información y llevar a cabo la debida diligencia. ISP ha elaborado una guía adicional sobre las actividades que pueden dar lugar a una investigación más exhaustiva en la nota informativa «Ganancias procedentes del soborno y la corrupción para centros educativos».

**4. Identificación de alumnos y clientes: «diligencia debida con respecto al cliente» (CDD)**

4.1 Es importante que se establezcan controles para identificar al estudiante, al pagador de la matrícula, al cliente u otros terceros que traten con la escuela. La CDD debe llevarse a cabo siempre sobre la base de documentos e información fiables. Entre los ejemplos de documentación justificativa se incluyen (entre otros) los siguientes.

Estudiantes:

- Pasaporte u otro documento de identidad emitido por el gobierno;
- Visado/prueba de residencia;
- Certificado de nacimiento.

Padres y otras personas que pagan las tasas de matrícula (obtener el pasaporte u otro documento de identidad emitido por el gobierno, además de uno o más de los siguientes):

- Pasaporte u otro documento de identidad emitido por el gobierno;
- Visado/prueba de residencia;
- Identificación fiscal;
- Facturas/recibos que acrediten el nombre y la dirección;
- Carta(s) en la que se explique la relación con el estudiante.

Pagos recibidos por empresas:

- Se determinará caso por caso, consultando al Departamento Jurídico del Grupo sobre los documentos de CDD que deben obtenerse. Para ello, puede utilizar la siguiente dirección de correo electrónico: ISPCompliance@ispschools.com

4.2 Las comprobaciones CDD deben realizarse antes de establecer una nueva relación comercial.

No debe aceptarse dinero de ninguna persona hasta que se hayan completado todos los controles de CDD (y, cuando sea necesario, EDD) ISP debe adoptar un enfoque basado en el riesgo ante cualquier patrón concreto y aplicar las comprobaciones CDD y EDD en consecuencia.

4.3 Además de las medidas establecidas anteriormente, el RFD y el MLRO (que es el director financiero del grupo ISP; véanse

detalles más adelante) deben ser notificados de cualquier transacción o relación que implique a PEP.

**5. Diligencia debida reforzada**

5.1 Cuando se hayan identificado uno o más patrones de hechos que constituyan señales de alerta (incluidos los de la sección 3.2 anterior), su RFD local deberá aplicar medidas de EDD que se determinarán conjuntamente con el departamento jurídico del grupo.

Esto puede incluir lo siguiente:

• obtener información adicional sobre el cliente (incluida, cuando el cliente sea una empresa, su estructura corporativa y cualquier beneficiario efectivo) de fuentes independientes;

• obtener información relativa al origen de la riqueza del cliente y del beneficiario efectivo;

• obtener información adicional y documentos justificativos sobre el origen de los fondos que se utilizarán en una transacción;

• realizar investigaciones adicionales y un análisis de los medios de comunicación adversos en relación con el cliente o el beneficiario efectivo;

• realizar un análisis adicional de las personas asociadas con el cliente (como directores y personas que dan instrucciones) y los socios conocidos del beneficiario efectivo; y

• llevar a cabo un seguimiento continuo y reforzado de la relación comercial.

**5.2** Tenga en cuenta que, salvo que se especifique lo contrario, los requisitos de información adicional establecidos en la sección 5.1 pueden obtenerse del cliente o de fuentes independientes, o de una combinación de ambos.

**6. Elaboración de informes internos sobre AML/CTF**

6.1 Cuando se tenga conocimiento o se sospeche que se está llevando a cabo o se ha llevado a cabo una actividad de blanqueo de capitales o de financiación del terrorismo, se debe comunicar inmediatamente por escrito al RFD local («Informe de divulgación interna») (véase la sección 6.2 más abajo para conocer la información que se debe incluir). A continuación, el RFD puede recomendar y supervisar la aplicación de medidas EDD adicionales (véase la sección 5 anterior) y/o recomendar que se presente un informe de divulgación interna por escrito al MLRO de ISP (un «Informe MLRO»). El MLRO designado en ISP es el director financiero del grupo, Darren Mee (correo electrónico:dmee@ispschools.com ).

6.2 Un informe de divulgación interna al RFD debe contener tantos detalles como sea posible, incluyendo:

• todos los datos disponibles sobre las personas y empresas implicadas y todos los miembros del personal que

han tratado con la transacción sospechosa;

• las razones por las que tiene conocimiento o sospecha de que puede estar ocurriendo o ha ocurrido un caso de blanqueo de capitales o financiación del terrorismo;

• las fechas de las transacciones, los importes involucrados y el método de transferencia de dinero o activos; y cualquier otra información que pueda ayudar al MLRO a juzgar el caso por conocimiento o sospecha de blanqueo de capitales.

6.3 Si alguna persona presenta un informe al MLRO, dicha persona no deberá realizar más indagaciones a menos que lo solicite el RFD o el MLRO. Tras presentar un informe al MLRO, cualquier consulta recibida de una persona sospechosa de blanqueo de capitales (por ejemplo, solicitar la confirmación de que se han abonado las comisiones) deberá comunicarse al MLRO antes de dar cualquier respuesta.

6.4 Nadie debe comentar su conocimiento o sospecha (incluido el hecho de que se ha presentado un informe de divulgación interna o un informe MLRO) con la persona que sabe o sospecha que está involucrada en el blanqueo de capitales y/o la financiación del terrorismo. Esto ayudará a evitar hacer una divulgación que pueda perjudicar una investigación de blanqueo de capitales, lo cual es un delito penal en la mayoría de las jurisdicciones.

**7. Controles para mitigar el riesgo**

7.1 Los reembolsos de los pagos solo deben realizarse por el mismo método y a la misma cuenta en la que se realizó el pago original, siempre que se haya obtenido la aprobación previa del RFD. Para evitar dudas, no se deben realizar reembolsos en efectivo.

7.2 Cualquier persona que pague en exceso y solicite un reembolso más de una vez debe ser señalada inmediatamente al RFD y sometida a un EDD.

7.3 En caso de que se rechace un pago con tarjeta de crédito o débito, se deberá comprobar el motivo con el proveedor de la tarjeta antes de aceptar una tarjeta alternativa con datos diferentes.

7.4 Cuando las tasas pagadas por adelantado por estudiantes extranjeros a los que posteriormente se les ha denegado el visado sean reembolsables de acuerdo con los documentos de solicitud y/o matriculación, dichos reembolsos solo podrán efectuarse cuando se disponga de pruebas documentales adecuadas que demuestren las circunstancias de dicha denegación de visado.

Los reembolsos sólo se efectuarán a la persona que haya realizado el pago original o, cuando sea necesario, mediante transferencia a una nueva escuela.

**8. Obligaciones del responsable de informar sobre préstamos monetarios (MLRO)**

8.1 El MLRO tendrá en cuenta el informe MLRO y cualquier otra información interna disponible que se considere relevante, como por ejemplo:

- la revisión de otros patrones y volúmenes de transacciones;
- la duración de cualquier relación comercial implicada;
- el número de transacciones puntuales y transacciones puntuales vinculadas; y
- cualquier prueba de identificación que se posea,

y llevará a cabo otras investigaciones razonables que considere oportunas para garantizar que se tenga en cuenta toda la información disponible a la hora de decidir si es necesario informar a las autoridades competentes. El MLRO también puede necesitar discutir el informe con el empleado.

8.2 El MLRO considerará si presentar un informe externo a la autoridad o autoridades pertinentes.

**9. Registros y formación**

9.1 Toda la documentación relativa a la CDD y la EDD, incluidos todos los informes de divulgación interna y los informes del MLRO, así como la documentación asociada (por ejemplo, la correspondencia interna del MLRO relativa a los informes del MLRO), deberá conservarse de forma segura durante cinco años a partir de la fecha en que se haya obtenido.

9.2 Como parte de su incorporación formal, se puede indicar a todos los nuevos empleados que completen un módulo de formación sobre AML y CTF y que certifiquen que han leído las políticas y procedimientos de la empresa en materia de delitos financieros. Dichos nuevos empleados no superarán el período de prueba si no completan con éxito el curso.

9.3 El personal de ISP deberá completar el módulo de formación AML de ISP al menos cada dos años. Determinadas personas que desempeñan funciones clave (como finanzas, adquisiciones, recursos humanos, gestión) o a las que se les ha asignado la responsabilidad de llevar a cabo comprobaciones CDD y EDD, así como RFD y MLRO, deben completar el módulo de formación AML y CTF de ISP anualmente.

**Anexo: Cláusulas adicionales específicas de cada jurisdicción**

**Brasil**

• Es especialmente importante llevar a cabo la debida diligencia con respecto a los proveedores y los contratos gubernamentales en Brasil.

**Canadá**

• Algunas provincias también administran leyes y reglamentos relacionados con la actividad AML en la jurisdicción. A modo de ejemplo, el gobierno de Columbia Británica ha publicado una política que exige a las escuelas independientes ubicadas en Columbia Británica que establezcan una política AML y de pago en efectivo que aborde determinados aspectos enumerados. Sin embargo, no tenemos conocimiento de ninguna política o requisito similar en la provincia de Ontario (donde se encuentran las dos escuelas de ISP).

**Malasia**

• El artículo 66B(3)(d) de la Ley contra el blanqueo de capitales, la financiación del terrorismo y los productos de actividades ilícitas de 2001 exige comunicar inmediatamente al Inspector General de Policía la existencia de bienes en posesión o bajo control de una persona que tenga motivos para creer que son propiedad o están controlados por una entidad específica o en nombre de esta, así como la información sobre una transacción o una transacción propuesta en relación con dichos bienes.

**Panamá**

• Todos los registros contables de las entidades ISP que operan en Panamá deben conservarse, incluso durante los siete años siguientes al cierre de cualquier negocio relevante en Panamá. EE. UU.

• La FinCEN ha implementado recientemente un requisito de información sobre la propiedad efectiva que puede ser aplicable a los ISP. A partir del 1 de enero de 2024, la norma exige que las «empresas informantes nacionales» y las «empresas informantes extranjeras» comuniquen sus propietarios efectivos a la FinCEN, salvo que se aplique una exención. Una «empresa informante nacional» es, por lo general, una entidad jurídica creada con arreglo a la legislación de cualquier estado de los Estados Unidos. Una «empresa informante extranjera» es una entidad jurídica creada con arreglo a la legislación de cualquier país no estadounidense y registrada para operar en un estado de los Estados Unidos.

• En consecuencia, si ISP tiene la intención de constituir una entidad en los Estados Unidos con el fin de operar una escuela en ese país o de registrarse para hacer negocios en un estado de los Estados Unidos, deberá informar sobre sus beneficiarios efectivos a la FinCEN, a menos que se aplique una exención. La única exención que podría aplicarse a ISP es la exención para «grandes empresas operativas», que se aplica a las empresas que: (i) emplean a 20 o más empleados a tiempo completo en los Estados Unidos; (ii) tienen presencia operativa en una ubicación física en los Estados Unidos; y (iii) declaran más de 5 000 000 USD en ingresos brutos o ventas en su declaración de impuestos estadounidense. Según los requisitos de información de la FinCEN, un beneficiario efectivo es cualquier persona física que, directa o indirectamente, ejerza un control sustancial sobre la empresa declarante o posea o controle al menos el 25 % de las participaciones de la empresa.

**Vietnam**

• Lo ideal es que los ISP solo reciban transferencias bancarias (es decir, no pagos en efectivo).