



Verificación de los datos sobre beneficiarios finales

Informe de políticas

Mayo de 2020

Introducción 2

Verificación en el momento de la presentación 5

Garantizar la conformidad 6

Garantizar que los valores sean reales y existentes 6

Controlar las pruebas de respaldo 7

Verificar al responsable que realiza la presentación 8

Verificación después de la presentación 9

Garantizar que los datos se controlen con frecuencia 9

Garantizar que los datos se mantengan actualizados 10

Garantizar que se investigue la información que se sospecha que es incorrecta 11

Sanciones 13

Conclusión 14

Introducción

Para maximizar el impacto de los registros de beneficiarios finales, es importante que los usuarios y las autoridades puedan confiar en que los datos allí contenidos reflejan, en términos generales, la realidad auténtica y actualizada sobre quién es el propietario o controlante de una empresa determinada.

La verificación es **la combinación de controles y procesos** que elige un régimen de divulgación en particular para garantizar que los datos sobre los beneficiarios finales sean de alta calidad, es decir, que sean exactos y completos en un momento determinado.

La verificación implica la creación de sistemas para controlar que la información presentada al registro sea como mínimo verosímil; que aparezca en el formato correcto; que esté libre de omisiones; que haya sido proporcionada por una persona pertinente y autorizada; y que esté, idealmente, desprovista de todo error y falsedad.

Para la mayoría de las empresas con estructuras de titularidad relativamente simples, la tarea de identificar y verificar a sus beneficiarios finales será un ejercicio en cierta medida sencillo. La identificación de los beneficiarios finales es más ardua cuando se trata de la minoría de empresas que tienen estructuras de titularidad complejas y a menudo transnacionales en las que intervienen muchas entidades jurídicas diferentes. En esos casos, tal vez no sea posible llegar al 100 % de certeza de que los datos sobre los beneficiarios finales divulgados reflejan la realidad de forma exacta y completa.

Una divulgación sobre beneficiarios finales es una declaración que se hace en un momento determinado, y no una verdad absoluta. Es el caso de muchos otros tipos de información que las empresas presentan regularmente, como los estados contables. Por lo tanto, se necesita un buen sistema de verificación para que los usuarios puedan confiar en los datos. Los sistemas de verificación incrementan la confiabilidad de los datos al:

- proporcionar claridad sobre la **procedencia** de los datos y qué controles se han realizado;
- **reducir los riesgos** asociados a la falsedad de los datos; y
- **activar las alarmas apropiadas** cuando los datos de los beneficiarios finales son falsos o sospechosos.

No existe una solución universal para la verificación, por lo que el sistema de verificación adecuado para un régimen de divulgación concreto dependerá del contexto local específico. El presente documento tiene por objeto establecer los principios generales que sirven de base a todos los sistemas de verificación efectivos. Además, quienes trabajan en la transparencia sobre beneficiarios finales a veces utilizan el término “verificación” para referirse a una serie de cuestiones diferentes. Esta nota orientativa ofrece un vocabulario común a quienes trabajan en la verificación de los datos sobre beneficiarios finales.

Tipos de datos incorrectos que los sistemas de verificación pueden abordar

Un buen sistema de verificación se ocupará de:

- **Errores accidentales:** datos mal ingresados por accidente (por ejemplo, escribir incorrectamente un país de residencia).
- **Falsedad deliberada:** datos falsos ingresados con la intención de engañar.

Existen diferentes métodos y mecanismos de verificación, y tienen distintos niveles de eficacia con respecto a los errores accidentales y las falsedades deliberadas. Por lo general, los errores accidentales son más fáciles de abordar que las falsedades deliberadas.

Tipos de controles de verificación

La verificación se divide en una serie de controles que se pueden efectuar:

- en el momento de la presentación de la información sobre el beneficiario final y
- después de la presentación de la información sobre el beneficiario final.



Figura 1: pasos de la verificación de los datos sobre beneficiarios finales

Paso 1

Presentación de los datos

Se presenta una divulgación sobre beneficiarios finales que consiste en información sobre una persona, una entidad y la relación de control que las vincula (página 5).

Paso 2

Verificación en el momento de la presentación

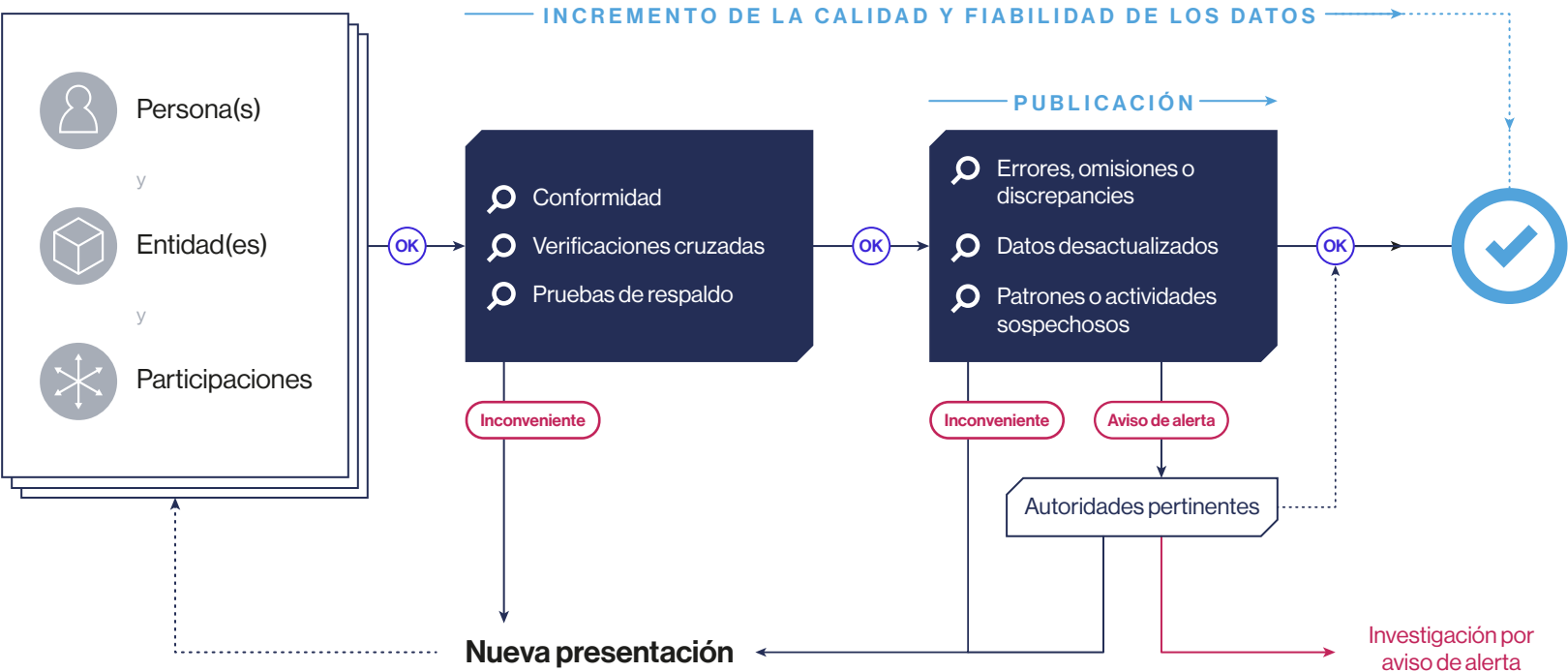
Se realizan una serie de controles (conformidad, verificaciones cruzadas, pruebas de respaldo) en el momento de la presentación (página 5). Los datos que no superan estos controles deben presentarse de nuevo. Los datos que sí los superan se someten a otra serie de controles posteriores a su presentación (página 9).

Paso 3

Verificación después de la presentación

Los errores/omisiones/discrepancias se comunican a la oficina registral y requieren corrección/nueva presentación (página 9); los datos desactualizados requieren una nueva presentación/la confirmación de que siguen siendo correctos (página 10); la actividad o los patrones sospechosos en los datos se pasan a una UIF, que determinará si son falsos positivos, si deben presentarse de nuevo, o si se debe elevar el asunto para una investigación más profunda (página 11).

La verificación es un proceso constante: con cada control de verificación, la calidad y la fiabilidad de los datos aumentan. Todas las medidas de verificación deberían hacerse cumplir en el marco de un régimen de sanciones integral, proporcionado y disuasorio (página 13).





Verificación en el momento de la presentación

La verificación en el momento de la presentación debería:

- Garantizar que la información guarde **conformidad con los patrones previstos** y sea clara y sin ambigüedades (por ejemplo, que un código postal siga el formato esperado en un país determinado; que el total de acciones no supere el 100 %).
- Garantizar que la información refleje **valores que efectivamente existan y sean reales, realizando verificaciones cruzadas** con sistemas autorizados y otros registros gubernamentales cuando sea posible (por ejemplo, que un determinado código postal exista de verdad).
- **Controlar las pruebas de respaldo** cotejando la información presentada con los documentos originales (ya sea en copia impresa o mediante identificación digital, por ejemplo, comprobante de domicilio; pasaportes para la identidad de los propietarios o los remitentes de la información; certificados de acciones para la titularidad).

La divulgación de beneficiarios finales abarca tres tipos de información:

1. Información sobre la(s) persona(s) involucrada(s) en una relación de propiedad o control
2. Información sobre la naturaleza de su propiedad o control
3. Información sobre la empresa u otra entidad jurídica de la que es propietaria o controlante

Se pueden realizar diferentes controles de verificación en cada una de estas declaraciones informativas. Es fundamental que los regímenes de divulgación puedan desambiguar entre diferentes individuos y entidades (puntos 1 y 3), tanto en el tipo de datos que recogen como en los mecanismos de verificación que emplean. El punto 2, correspondiente a la información sobre la naturaleza de su propiedad o control, es el más difícil de verificar, y donde se producen más falsedades deliberadas. La verificación de cada uno de estos tipos de información es mucho más fácil de hacer cuando los datos están estructurados (es decir, organizados de manera congruente en campos separados y legibles por medios informáticos en lo posible) en lugar de desestructurados. La información sobre el remitente de los datos es un metadato crucial para las tres declaraciones de información.

Los criterios para verificar estos tres tipos de información pueden dividirse en las tres categorías principales que se indican a continuación. Es importante tener en cuenta que un criterio no excluye al otro y que los diversos criterios se complementan entre sí y pueden reforzar recíprocamente la fiabilidad y la calidad de los datos.



Garantizar la conformidad

Controles de conformidad

¿Los datos siguen un patrón previsto? Por ejemplo, ¿la fecha de nacimiento tiene el formato esperable? ¿El sistema rechaza fechas inadmisibles como el 31 de febrero?

Los controles de conformidad son una herramienta eficaz para eliminar los errores accidentales. Son relativamente fáciles y económicos de implementar en formularios digitales. Sin embargo, son menos eficaces para contrarrestar las falsedades deliberadas.

Ejemplo: Bélgica

En el Registro de Beneficiarios Finales en Última Instancia (UBO) de Bélgica, el sistema impide la inscripción de más del 100% de las acciones/derechos de voto de una persona, ya que esto no sería técnicamente posible, con lo cual se garantiza que los datos estén en conformidad con los patrones previstos.¹

Garantizar que los valores sean reales y existentes

Verificación cruzada de datos

¿Es posible buscar los datos en un sistema autorizado, como otros registros gubernamentales, para controlar que sean exactos? Por ejemplo, ¿se puede cruzar la fecha de nacimiento con el registro civil? ¿O puede un sistema de identificación digital estatal verificar la identidad?

La verificación cruzada de datos puede automatizarse en gran medida, y es más eficaz que la conformidad, tanto en general como en lo que se refiere al abordaje específico de las falsedades deliberadas. Para que el cruce de datos sea eficaz se requiere una infraestructura y capacidad técnica básica, incluso en otras partes del gobierno, que proporcione datos para su cotejo. Es posible que haya que crear nuevos mandatos legales para utilizar estos datos si no existe ninguno. Estos controles dependen de la disponibilidad de registros autorizados y exactos (¿se han verificado los datos de esos registros?). Los controles solo podrían abarcar a los ciudadanos nacionales, dependiendo de la información disponible.

Ejemplo: China

En China, la información sobre los beneficiarios finales se cruza con varios otros registros gubernamentales, entre ellos el Sistema de Información de Registro de la Administración de Industria y Comercio, el Sistema Nacional de Publicidad de Información Crediticia Empresarial, el Sistema de Consulta del Código de Crédito Social Unificado del Sistema Nacional de Organizaciones, la Plataforma de Información de Registro de Entidades Comerciales, la Plataforma de Publicidad de Información Crediticia de Entidades Comerciales y el Sistema de Consulta de Registro Tributario.²

Ejemplo: Dinamarca

El Registro Central de Empresas de Dinamarca (CVR) cruza automáticamente la información presentada con diversos registros gubernamentales, incluidos el registro civil y el registro de direcciones danés. El sistema impide, por ejemplo, que se registre a una persona fallecida.³

¹ GAFI, "Best Practices on Beneficial Ownership for Legal Persons" [Mejores prácticas en torno a los beneficiarios finales de las personas jurídicas]. Octubre de 2019. Disponible en inglés en: <https://www.fatf-gafi.org/media/fatf/documents/Best-Practices-Beneficial-Ownership-Legal-Persons.pdf> [Consultado el 20 de abril de 2020].

² Ibid

³ Ibid



Controlar las pruebas de respaldo

Certificación o autenticación notarial

¿Ha controlado alguien con autoridad en la materia (por ejemplo, un abogado o un notario) de manera independiente las pruebas documentales de las que surgen los datos y confirmado su veracidad? Por ejemplo, ¿puede un notario certificar la fecha de nacimiento de una persona garantizando la veracidad de un pasaporte escaneado?

Los controles de certificación pueden utilizarse para los tres tipos de información. En ellos intervienen terceras personas físicas que son imparciales (a menudo bajo juramento) y que ponen en juego su reputación profesional con sus afirmaciones de veracidad y asumen responsabilidad por las presentaciones falsas. Los controles de certificación exigen requisitos y pautas estrictas a fin de que no se registren prácticas divergentes en la presentación de la información (ver ejemplo a continuación). Para los gobiernos menos adelantados técnicamente, la autenticación notarial como medio de verificación suele ser una opción viable, como puede verse en algunos países de ingresos más bajos.⁴ El uso de notarios y abogados podría constituir un obstáculo económico para realizar cambios, y sería relativamente más costoso para las empresas más pequeñas; además, podría traer aparejada la necesidad de hacer controles de verificación de esa persona (por ejemplo, ¿este abogado tiene licencia para ejercer?).

Ejemplo: Eslovaquia

En el Registro de Socios del Sector Público de Eslovaquia, intervienen terceros —abogados, notarios, bancos y auditores— que se encargan de controlar toda la información y que pueden ser responsabilizados si se descubre que proporcionaron información falsa. El análisis de las presentaciones realizado por OpenOwnership ha demostrado que puede haber divergencias en la calidad de las pruebas que respaldan los medios de propiedad y control, ya que algunos documentos notariales solo proporcionan una exposición descriptiva que no aporta suficiente claridad, mientras que otros incluyen diagramas claros de las estructuras de las empresas.

Ejemplo: Japón

En Japón, se exige a los notarios que controlen la identidad del beneficiario final examinando el contrato constitutivo y otros documentos presentados. También cotejan las identidades con su propia base de datos sobre grupos del crimen organizado y terroristas internacionales.⁵

Controles de la oficina registral

¿El encargado registral ha controlado las pruebas documentales y confirmado su veracidad?

Los controles de la oficina registral pueden utilizarse para los tres tipos de información, y aumentan aún más la confianza en la información suministrada. De este modo, se reduce la carga económica de las empresas en comparación con la exigencia de certificación por parte de terceros profesionales, pero el personal de la oficina registral podría necesitar capacitación complementaria para controlar la veracidad de las pruebas documentales. Esto también requiere un examen cuidadoso para determinar dónde recae la responsabilidad.

⁴ Por ejemplo, en Mali. Véase GIABA, "Anti-money laundering and counter-terrorist financing measures. Mali Mutual Evaluation Report". ["Medidas contra el lavado de dinero y la financiación del terrorismo. Informe de Evaluación Mutua de Mali"]. Noviembre de 2019. Disponible en inglés en: <http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/GIABA-Mutual-Evaluation-Mali-2019.pdf> [Consultado el 20 de abril de 2020].

⁵ GAFI, "Best Practices on Beneficial Ownership for Legal Persons" [Mejores prácticas en torno a los beneficiarios finales de las personas jurídicas]. Octubre de 2019. Disponible en inglés en: <https://www.fatf-gafi.org/media/fatf/documents/Best-Practices-Beneficial-Ownership-Legal-Persons.pdf> [Consultado el 20 de abril de 2020].

Verificar al responsable que realiza la presentación

La verificación de la información sobre la persona que remite una divulgación sobre beneficiarios finales puede ofrecer una protección adicional contra la presentación de información falsa. Según el régimen de divulgación, podría ser el propio beneficiario final, un representante de la empresa divulgadora o un tercero. La información sobre el responsable que realiza la presentación consiste esencialmente en metadatos, que son cruciales para aumentar la fiabilidad. Los controles de verificación descritos anteriormente pueden emplearse para verificar la identidad de quien remite la información. Además, podría ser necesario establecer que la persona está autorizada a presentar la información en nombre del beneficiario final o de la empresa.

Los sistemas antes mencionados reducirán los errores y las falsedades deliberadas, y ayudarán a mejorar la calidad de los datos. Sin embargo, aun así sería posible que alguien ocultara a un verdadero beneficiario final. Por ejemplo, una persona real, autorizada y verificada podría presentar información en nombre de una empresa legítima y consignar información de una persona real y verificada que no es el beneficiario final, con el propósito de ocultar al verdadero. Hay otros mecanismos de verificación que pueden implementarse después de la presentación para mejorar aún más la calidad de los datos.



Verificación después de la presentación

La verificación después de la presentación debería:

- Garantizar que los datos **se controlen con frecuencia**.
- Garantizar que los datos **se mantengan actualizados**.
- Garantizar **que se investigue la información que se sospecha que es incorrecta**.

Existen varios criterios generales para la verificación después de la presentación, incluidos los controles posteriores a la publicación de la información sobre los beneficiarios finales. Al igual que en la verificación en el momento de la presentación, pueden emplearse varios criterios que se complementan entre sí y que pueden reforzar recíprocamente la fiabilidad y la precisión.

Garantizar que los datos se controlen con frecuencia

Hacer que los registros de beneficiarios finales sean abiertos y públicos

Hacer públicos los registros permite que el sector privado, la sociedad civil y la ciudadanía en general los controlen, tanto para detectar errores accidentales como falsedades deliberadas. De las investigaciones se desprende que el hecho de divulgar los datos públicamente puede aumentar su calidad, ya que el mayor uso de los datos acrecienta la probabilidad de que se identifiquen incongruencias o posibles infracciones.⁶ Para que ello funcione eficazmente como medida de verificación, deberían establecerse mecanismos que permitan informar sobre los errores, las discrepancias y la información contradictoria. También hay una serie de beneficios adicionales para el sector privado, que se espera que sobrepasen los costos.⁷

Aunque no hay ejemplos documentados de perjuicios derivados de registros públicos,⁸ sus detractores citan con frecuencia cuestiones de privacidad como argumento en su contra. Los gobiernos no deberían revelar más datos de los necesarios para facilitar una supervisión y una transparencia significativas, y podrían incluir exenciones en caso de preocupaciones legítimas.

⁶ OpenOwnership, "Briefing: The case for beneficial ownership as open data" [Artículo: por qué conviene contar con datos abiertos sobre beneficiarios finales]. Julio de 2017. Disponible en inglés en: <https://www.openownership.org/uploads/briefing-on-beneficial-ownership-as-open-data.pdf> [Consultado el 20 de abril de 2020].

⁷ OpenOwnership, "Briefing: The case for public beneficial ownership registers" [Artículo: por qué conviene contar con registros públicos sobre beneficiarios finales]. Julio de 2017. Disponible en inglés en: <https://www.openownership.org/uploads/the-case-for-public-beneficial-ownership.pdf> [Consultado el 20 de abril de 2020].

⁸ OpenOwnership, The B Team y The Engine Room, "Data Protection and Privacy in Beneficial Ownership Disclosure" [La protección de los datos y la privacidad en la divulgación de los beneficiarios finales]. Mayo de 2019. Disponible en inglés en: <https://www.openownership.org/uploads/oo-data-protection-and-privacy-188205.pdf> [Consultado el 20 de abril de 2020].



Ejemplo: Reino Unido

En noviembre de 2016, Global Witness y un consorcio de distintas ONG analizaron 1,3 millones de empresas en el registro de beneficiarios finales (Personas con Control Significativo) del Reino Unido. De este modo, pudieron informar a Companies House —el organismo que supervisa el registro— acerca de más de 4.000 empresas con información inadmisible.⁹

Control/análisis de muestras de datos

Los organismos responsables de los registros de beneficiarios finales pueden llevar a cabo investigaciones profundas de muestras de datos o solicitar a terceros que lo hagan. Estas pruebas sirven para disuadir a las empresas de presentar información errónea. El análisis de muestras podría no ser muy eficaz como mecanismo de verificación, y puede demandar muchos recursos. Esto puede mitigarse utilizando un criterio basado en los riesgos para analizar las muestras.

Ejemplo: Dinamarca

Para garantizar que la información del Registro Central de Empresas (CVR) sea exacta y esté actualizada, la Autoridad Comercial Danesa (DBA) comenzó a controlar manualmente 500 empresas y el registro de sus beneficiarios finales en 2019.¹⁰

Garantizar que los datos se mantengan actualizados

Solicitar la actualización de la información en caso de que se produzcan cambios

Se debería exigir que los cambios referentes a los beneficiarios finales se actualicen rápidamente después de producirse. Especificar un plazo corto y definido para la presentación de las modificaciones en un registro asegura que la información de los beneficiarios finales se mantenga actualizada. Los registros públicos también pueden hacer visibles los datos desactualizados para alertar a sus usuarios. La exigencia de presentar actualizaciones frecuentes al registro conlleva el riesgo de aumentar los costos de cumplimiento, lo que debería contemplarse a la hora de diseñar del sistema de verificación.

Solicitar la ratificación de la información existente

Las entidades divulgadoras deberían controlar y ratificar de manera regular (al menos anualmente) que la información sobre sus beneficiarios finales sea exacta y esté actualizada. Esto puede integrarse con los procesos de las empresas ya existentes (por ejemplo, la presentación de declaraciones anuales). Sin embargo, si no se hacen otras verificaciones, esta medida resulta ineficaz.

Ejemplo: Ucrania

A fin de garantizar la actualización constante de la información sobre los beneficiarios finales, el Ministerio de Justicia de Ucrania dictó la Resolución 2824/5 “para la introducción de modificaciones a determinadas formas de solicitudes en el ámbito del registro estatal de entidades jurídicas, empresarios individuales y organizaciones públicas” en 2018, que obligó a las empresas a actualizar los datos sobre sus beneficiarios finales en última instancia cuando modifican cualquier información en el Registro Estatal Unificado, o a ratificar que la información allí contenida sigue siendo correcta.¹¹

⁹ Global Witness, “The Companies We Keep” [Las empresas de las que nos rodeamos], 2016. Disponible en inglés en: https://www.globalwitness.org/documents/19400/Briefing_The_Companies_We_Keep.pdf [Consultado el 20 de abril de 2020].

¹⁰ GAFI, “Best Practices on Beneficial Ownership for Legal Persons” [Mejores prácticas en torno a los beneficiarios finales de las personas jurídicas]. Octubre de 2019. Disponible en inglés en: <https://www.fatf-gafi.org/media/fatf/documents/Best-Practices-Beneficial-Ownership-Legal-Persons.pdf> [Consultado el 20 de abril de 2020].

¹¹ Basado en “Concept of a mechanism for verifying the reliability of information on UBO” [Concepto de un mecanismo para verificar la fiabilidad de la información sobre beneficiarios finales en última instancia], que el grupo de trabajo de verificación “Up to 100%” compartió con OpenOwnership, y en las conversaciones con los miembros del grupo de trabajo en febrero de 2020.

Garantizar que se investigue la información que se sospecha que es incorrecta

Solicitar que se denuncien las actividades y datos ingresados que resulten sospechosos

A las entidades que trabajan con los datos de los beneficiarios finales debería exigírseles que denuncien las presentaciones y actividades sospechosas a los entes correspondientes, y debería atribuírseles el mandato de investigarlas (por ejemplo, el sector privado que realiza procesos de debida diligencia podría denunciar a la UIF cuestiones relativas a la prevención del lavado de dinero [AML]). Es importante que las UIF cuenten con los recursos necesarios para poder investigar las denuncias (ver ejemplo).

Ejemplo: Reino Unido

A partir de enero de 2020, los sectores regidos por las normas sobre prevención del lavado de dinero y de la financiación del terrorismo (AML/CTF) deben informar las discrepancias entre la información sobre los beneficiarios finales disponible en el organismo de registro de las empresas (*Companies House*) y la información que obtienen mediante sus propios controles de cumplimiento.¹²

Ejemplo: Países Bajos

Se estima que cada año se lavan 16.000 millones de euros en los Países Bajos. Si bien las entidades obligadas notificaron 60.000 transacciones sospechosas en 2018, la UIF consideró que solo 15.000 eran realmente sospechosas, si bien se cree que solo es capaz de investigar un número mucho menor, debido a la falta de recursos (humanos).¹³

Avisos de alerta

Es posible configurar los sistemas para detectar patrones asociados con instrumentos legales que se utilizan con fines ilícitos. Esto probablemente esté muy vinculado a contextos específicos. Estos programas serán más fáciles de instalar en sistemas digitalizados donde la información sobre los beneficiarios finales esté disponible en forma de datos estructurados, y podría recurrirse a la inteligencia artificial y tecnologías de aprendizaje automatizado. Existe el riesgo de que al añadir controles adicionales de avisos de alerta y cruzar la información sobre los beneficiarios finales con otros registros, el número de datos marcados indebidamente como sospechosos también aumente, lo que disminuiría su utilidad. Por consiguiente, es importante también considerar la posibilidad de establecer mecanismos para reducir esos errores e instaurar un proceso operativo sencillo y basado en normas que responda a esas discrepancias.

Ejemplo: Ucrania

En Ucrania, el grupo de trabajo sobre verificación “Up to 100%” ha propuesto diversos sistemas de verificación que activan avisos de alerta automáticos, basándose en estrategias conocidas que se usan para fines ilícitos. Por ejemplo, en Ucrania es común inscribir a un trabajador de fábrica como beneficiario final. El sistema propuesto activaría automáticamente una señal de alerta para los investigadores cuando alguien figure en la lista de beneficiarios finales de una empresa rentable, mientras que los datos fiscales muestren que esa persona gana un salario considerablemente inferior al que podría esperarse del propietario de una empresa lucrativa.¹⁴

¹² HM Treasury [Tesoro del Reino Unido], “The Money Laundering and Terrorist Financing (Amendment) Regulations” [Regulaciones sobre el lavado de dinero y la financiación del terrorismo (Reforma)]. 2019. Disponible en inglés en: <http://www.legislation.gov.uk/ukSI/2019/1511/made/data.pdf> [Consultado el 20 de abril de 2020].

¹³ Trouw, “Belastingadviseurs: ‘Overheid is te slap tegen witwassen’”. 9 de febrero de 2020. Disponible en neerlandés en: <https://www.trouw.nl/economie/belastingadviseurs-overheid-is-te-slap-tegen-witwassen-b0f40eff/> [Consultado el 20 de abril de 2020].

¹⁴ Basado en “Concept of a mechanism for verifying the reliability of information on UBO” [Concepto de un mecanismo para verificar la fiabilidad de la información sobre beneficiarios finales en última instancia], que el grupo de trabajo de verificación “Up to 100%” compartió con OpenOwnership, y en las conversaciones con los miembros del grupo de trabajo en febrero de 2020.

La mayoría de los regímenes de divulgación sobre beneficiarios finales emplearán varios de estos mecanismos de verificación, que no constituyen en absoluto una lista exhaustiva, pero todos ellos se encuadran en líneas generales dentro de estos tres criterios. Ninguno de estos es por sí solo mejor que otro y, en última instancia, su éxito dependerá en gran medida del contexto en el que se adopte y de los demás controles que se lleven a cabo. En consecuencia, los países deberían aplicar un enfoque holístico e integral para la verificación, siguiendo un criterio centrado en los riesgos que tenga en cuenta los objetivos generales del sistema de verificación como medio para alcanzar un fin, que es el de facilitar el uso de los datos y, a su vez, incidir en las políticas.

Sanciones

Todas las medidas de verificación deberían hacerse cumplir en el marco de un régimen de sanciones integral, proporcionado y disuasorio, que incluya *multas pecuniarias y otras penalizaciones*, a fin de mejorar el cumplimiento y la calidad de los datos. Su alcance podría comprender a:

- la persona que presenta la declaración del beneficiario final (por ejemplo, un notario);
- representantes registrados de la empresa;
- el/los beneficiario(s) final(es); y
- la empresa que realiza la divulgación.

Las sanciones deberían abarcar la no presentación de información, la presentación de información incorrecta (de forma deliberada o no), y la no presentación de información a tiempo. Las sanciones pueden ampliarse para contemplar penas por no denunciar información sospechosa conforme a las obligaciones de denuncia que imponen las normas sobre prevención del lavado de dinero (AML). Las multas no pecuniarias pueden incluir la pérdida de ciertos derechos nacionales y empresariales, como la imposibilidad de constituir una empresa o la falta de pago de los dividendos de las acciones.

Ejemplo: Francia

En Francia, las presentaciones tardías o incorrectas pueden hacer que se impida a una persona dedicarse a ciertas actividades empresariales o que se la despoje de ciertos derechos nacionales y civiles (por ejemplo, que se la someta a supervisión judicial). Además, el responsable está sujeto a seis meses de prisión y una multa de 7.500 euros. La sanción para la empresa equivale a cinco veces el monto correspondiente a una persona.¹⁵

Ejemplo: Ghana

En Ghana las multas por no actualizar la información son de 350 dólares estadounidenses,¹⁶ Según un funcionario de la Corporación Nacional de Petróleo de Ghana, algunas empresas las consideran tan bajas que optan por pagarlas en lugar de actualizar la información.

¹⁵ GAFI, "Best Practices on Beneficial Ownership for Legal Persons" [Mejores prácticas en torno a los beneficiarios finales de las personas jurídicas]. Octubre de 2019. Disponible en inglés en: <https://www.fatf-gafi.org/media/fatf/documents/Best-Practices-Beneficial-Ownership-Legal-Persons.pdf> [Consultado el 20 de abril de 2020].

¹⁶ EITI, "Abordajes jurídicos de la transparencia sobre beneficiarios reales en los países EITI". Junio de 2019. Disponible en: https://eiti.org/files/documents/es_ic_paper_42-3_legal_approaches_to_beneficial_ownership_transparency_i.pdf [Consultado el 20 de abril de 2020].

Conclusión

La verificación es un sistema de diferentes controles y procesos que pueden desplegarse a lo largo de diferentes etapas de un sistema de divulgación de información sobre beneficiarios finales y que se hace cumplir con sanciones proporcionadas, con el objetivo de generar datos de alta calidad y fiables, y así maximizar la utilidad y el impacto de tener un registro de beneficiarios finales.

En la práctica, esto significa contar con un marco jurídico apropiado (por ejemplo, que permita a las instituciones gubernamentales compartir información) y con sistemas de programas y equipos informáticos efectivos y procesos administrativos que implementen los requisitos del marco jurídico de un modo que maximice el uso de los datos sobre beneficiarios finales para lograr un impacto en las políticas. Si bien es importante evaluar detalladamente los beneficios de las distintas combinaciones de criterios de verificación por adelantado, los gobiernos deberían tratar la divulgación sobre beneficiarios finales como un proyecto en desarrollo. Debería llevarse a cabo paso a paso, a la vez que se siguen estudiando formas de mejorar, llenar las lagunas y consolidar el uso de la información y los datos.

La verificación de los datos sobre beneficiarios finales es un campo en rápida evolución, pero relativamente novedoso, y sigue habiendo ámbitos en los que las buenas prácticas son aún incipientes. Por ejemplo, es mucho más fácil realizar controles de verificación de los ciudadanos nacionales que de los extranjeros. A medida que más países establezcan registros públicos de beneficiarios finales con sistemas de verificación y que estos últimos se vinculen entre sí, aumentará el potencial de lo que se puede lograr mediante una verificación rigurosa de los datos de los beneficiarios finales. También hay mucho que se puede aprender del sector privado, así como de los registros cerrados, con respecto a la verificación.¹⁷ Sin embargo, es poca la información al respecto que se encuentra en el dominio público, como lo demuestra el limitado alcance geográfico de los ejemplos de este informe. En el marco de una de sus líneas de investigación, OpenOwnership está estudiando el uso que hace el sector privado de los datos sobre beneficiarios finales y los mecanismos de verificación que emplean, y también está llevando a cabo análisis de casos de mecanismos de verificación en registros cerrados. A medida que otros países implementen la transparencia sobre beneficiarios finales, OpenOwnership seguirá aprendiendo más y actualizando sus ideas sobre las mejores prácticas en materia de verificación.

¹⁷ Véase, por ejemplo: Andres Knobel, "Beneficial ownership verification: ensuring the truthfulness and accuracy of registered ownership information" [La verificación de los beneficiarios finales: cómo garantizar la veracidad y la exactitud de la información sobre la titularidad registrada], Tax Justice Network. 2019. Disponible en inglés en: https://www.taxjustice.net/wp-content/uploads/2019/01/Beneficial-ownership-verification_Tax-Justice-Network_Jan-2019.pdf

Publicado por OpenOwnership

Autor Tymon Kiepe

con aportes de
Louise Russell-Prywata y Jack Lord

Revisión Andres Knobel

Edición Victor Ponsford

Diseño Convincible Media

openownership.org

 @openownership

1 St. Katherine's Way, London E1W 1UN

**OPEN
OWNERSHIP**

