Proyecto financiado por la UE

ESTUDIO DE EXPERIENCIAS COMPARADAS DE REGISTROS DE BENEFICIARIOS FINALES

Este Informe se ha realizado en el marco de la implementación de la acción de COPOLAD III *Asesoría técnica para el cumplimiento de los objetivos del III Plan de Acción de la Estrategia Nacional para la prevención y combate del lavado de activos, financiamiento del terrorismo y de la proliferación y la Política Nacional Contra el Crimen Organizado de la República de Chile.*

La información y opiniones expresadas en este Informe no reflejan necesariamente la opinión oficial de la Comisión Europea. Ni la Comisión Europea ni ninguna persona que actúe en nombre de la Comisión es responsable del uso que pueda hacerse de la información contenida en este documento.

ÍNDICE

Resumen ejecutivo

Aumentar la transparencia de los vehículos corporativos se ha convertido en una prioridad internacional debido a la creciente complejidad de las estructuras societarias utilizadas en operaciones que pueden estar vinculadas a actividades ilícitas como el lavado de activos y la evasión fiscal. En este contexto, el Grupo de Acción Financiera Internacional (GAFI) dispone que los países deben garantizar que haya información adecuada, precisa y actualizada sobre la propiedad efectiva y el control de personas jurídicas que pueda ser obtenida o accedida de manera rápida y eficiente por las autoridades competentes, ya sea a través de un registro de propiedad efectiva o un mecanismo alternativo.

Chile ha realizado progresos importantes a este respecto a partir del IV Plan de Gobierno Abierto 2018-2020. El 14 de diciembre de 2023 el Presidente de la República envió al Senado, mediante el Mensaje 267-371, un Proyecto de ley para la creación de un Registro Nacional de Personas Beneficiarias Finales (RNPBF). La configuración final del RNPBF estará en gran medida determinada por su reglamento, lo que justifica que las autoridades chilenas cuenten con información amplia y de calidad sobre las opciones regulatorias adoptadas en otras jurisdicciones para fundamentar adecuadamente las futuras decisiones reglamentarias.

El informe analiza la regulación vigente en materia de registros de beneficiarios finales en las 30 jurisdicciones estimadas como más significativas, exponiendo para cada una de ellas el régimen jurídico vigente, la autoridad responsable, los aspectos tecnológicos y la accesibilidad al registro.

Basándose en el análisis de la situación de las treinta jurisdicciones más significativas, el informe presenta y evalúa varias estrategias a considerar para el establecimiento del RNPFB. Examina las implicaciones derivadas de la autoridad o agencia responsable de la gestión, la configuración de controles previos como el uso de formularios estandarizados y campos obligatorios, los controles internos para detectar y corregir posibles inconsistencias o errores en los registros y las verificaciones automáticas con otras bases de datos gubernamentales. Además, se aborda la determinación del modelo de gestión de datos, considerando la opción entre sistemas propietarios y estándares abiertos, el régimen de acceso a los datos registrales y los costos asociados a la implementación y operación del registro.

I. Introducción

1. Antecedentes

En los últimos años, aumentar la transparencia de los vehículos corporativos ha emergido como una meta prioritaria en el ámbito internacional. La complejidad de las estructuras societarias que se utilizan en determinadas operaciones comerciales y financieras ha generado una preocupación creciente debido a su potencial vínculo con actividades ilícitas, tales como el lavado de activos y la evasión fiscal.

Diversos estudios y análisis de tipologías realizados tanto a nivel nacional como internacional han demostrado repetidamente que una serie de estructuras sofisticadas son empleadas con frecuencia en esquemas fraudulentos. Esta situación subraya la necesidad urgente de abordar este problema. La falta de transparencia en la propiedad y gestión de las empresas puede facilitar prácticas financieras irregulares y dificultar la detección y prevención de delitos económicos.

En este contexto, el acceso oportuno a información veraz sobre los beneficiarios finales de los vehículos corporativos se configura como una herramienta esencial. Para promover la transparencia de esta información, la Recomendación 24 del Grupo de Acción Financiera Internacional (GAFI) establece que los países deben evaluar los riesgos de uso indebido de personas jurídicas para el lavado de activos o el financiamiento del terrorismo, y tomar medidas para prevenir su mal uso. Específicamente, los países deben garantizar que exista información adecuada, precisa y actualizada sobre la propiedad efectiva y el control de las personas jurídicas, que pueda ser obtenida o accedida de manera rápida y eficiente por las autoridades competentes. Esto puede lograrse a través de un registro de propiedad efectiva o un mecanismo alternativo. La Recomendación 25 ofrece una previsión similar respecto a los instrumentos jurídicos.

Recomendación 24

2. Situación de Chile

El IX Informe de Tipologías y Señales de Alerta de Lavado de Activos de la Unidad de Análisis Financiero (UAF) señaló que en el periodo 2007-2022 el uso de testaferros era el mecanismo más frecuentemente utilizado para ocultar o disimular recursos obtenidos de forma ilícita, seguido de la creación y utilización de personas y estructuras jurídicas para disimular el origen o movimientos del dinero mal habido. En la misma línea, la Evaluación Nacional de Riesgo de Lavado de Activos de 2023 (ENR-LA), al desagregar la tipología de creación de personas y estructuras jurídicas en sentencias condenatorias, observó que las sociedades de pantalla se encontraban presentes en el 28,7% de los casos, las sociedades de fachada en el 27,0% y las sociedades de papel en el 13,1%. Por tipologías mercantiles, 32 casos de un total de 122 incluyeron el uso de 100 sociedades: 44 sociedades por acciones (44,0% del total de sociedades), 29 de responsabilidad limitada (29,0%), 10 empresas individuales de responsabilidad limitada (10,0%), 5 sociedades anónimas (5,0%), 3 empresas de menor tamaño pro-pyme (3,0%) y dos sociedades extranjeras (2,0%).

Evaluación Nacional de Riesgos

El IV Plan de Gobierno Abierto 2018-2020 incluyó como compromiso número 11 “construir colaborativamente una propuesta de política sobre la creación de un registro de dueños reales de empresas (beneficiarios finales)”. Esta propuesta, liderada por la UAF con la participación del Servicio de Impuestos Internos (SII), ChileCompra, Chile Transparente y la Fundación Observatorio Fiscal, fue desarrollada por la Mesa Intersectorial sobre Prevención y Combate al Lavado de Activos y al Financiamiento del Terrorismo (MILAFT). En septiembre de 2020 se realizó una consulta pública cuyos resultados fueron los siguientes: el 100% de los participantes consideró que un registro de

IV Plan de Gobierno Abierto

beneficiarios finales proporcionaría mayor transparencia a los negocios; el 92% consultaría la información de dicho registro; el 94% apoyó que el registro fuera público; el 96% estuvo de acuerdo en que las entidades públicas tuvieran pleno acceso; el 98% respaldó la imposición de sanciones penales por la entrega de información falsa; el 92% aprobó la aplicación de sanciones pecuniarias; y el 86% estuvo de acuerdo en mantener la información por un máximo de 10 años si la persona jurídica ya no está activa.

El Informe de Evaluación Mutua de Chile, aprobado por GAFILAT en 2021, calificó el cumplimiento técnico de la Recomendación 24 como "Parcialmente Cumplido" y el de la Recomendación 25 como "Mayormente Cumplido". En cuanto a efectividad, el Resultado Inmediato 5, que evalúa si las personas jurídicas y otras estructuras jurídicas no pueden ser utilizadas indebidamente para el lavado de activos y el financiamiento del terrorismo y si la información sobre sus beneficiarios finales está disponible para las autoridades competentes sin impedimentos, fue calificado como Bajo.

Acciones recomendadas

Entre las acciones recomendadas por GAFILAT se incluían: (i) Establecer la obligación de identificar al beneficiario final para las Actividades y Profesiones No Financieras Designadas (APNFD). (ii) Adecuar el marco normativo existente y procurar su plena implementación para obtener y actualizar la información del beneficiario efectivo de todas las personas jurídicas. (iii) Adoptar medidas para fortalecer el acceso a información actualizada, precisa y oportuna sobre el beneficiario efectivo por parte de las autoridades competentes. (iv) Realizar mayores esfuerzos para aplicar sanciones proporcionales y disuasivas contra las personas jurídicas que no actualicen la información ante el SII y contra los sujetos obligados que no obtengan y actualicen la información del beneficiario efectivo. (v) Continuar con la capacitación y la divulgación de estudios realizados por las autoridades competentes para mejorar la comprensión del riesgo de lavado de activos y financiamiento del terrorismo y de las vulnerabilidades de las personas jurídicas.

Proyecto de ley

Siguiendo los requerimientos internacionales, el 14 de diciembre de 2023 el Presidente de la República envió al Senado, mediante el Mensaje 267-371, un Proyecto de ley para la creación de un Registro Nacional de Personas Beneficiarias Finales (RNPBF). Este proyecto (Boletín Nº 16.475-05) tiene como objetivo fomentar la transparencia, detectar conflictos de intereses, proteger la libre competencia, servir como herramienta para el cumplimiento adecuado de las obligaciones tributarias, satisfacer los requerimientos de información de autoridades extranjeras en virtud de acuerdos de intercambio de información firmados por Chile, y permitir la prevención, investigación y sanción de infracciones administrativas, faltas, delitos menores y graves como el lavado de activos o el financiamiento del terrorismo.

Cabe destacar que, según el artículo 15 del proyecto, el Presidente de la República, a través del Ministerio de Hacienda y el Ministerio Secretaría General de la Presidencia, emitirá un reglamento que regulará aspectos clave: la forma en que la información será organizada en el portal previsto en el artículo 7, asegurando que sea estructurada en formato de datos abiertos y de fácil acceso para los interesados; la manera en que se garantizará el acceso completo y oportuno para los organismos del Estado y la verificación del certificado correspondiente por parte de los sujetos obligados a reportar operaciones sospechosas, tanto en el ejercicio de sus funciones como para verificar la información del beneficiario final de sus clientes, según lo dispuesto en los artículos 8 y 11; los medios para verificar la información utilizando múltiples fuentes públicas y privadas, especialmente en relación con

información de otros registros existentes; las normas de organización y funcionamiento del Consejo Consultivo del artículo 10; y las características de un canal administrado por el Servicio de Impuestos Internos para denunciar cualquier infracción a las normas de la ley. Por lo tanto, la configuración final del RNPBF estará en gran medida determinada por este reglamento, lo que justifica que las autoridades chilenas cuenten con información amplia y de calidad sobre las opciones regulatorias adoptadas en otras jurisdicciones.

En el momento de la redacción del presente informe, el Proyecto de ley para la creación de un Registro Nacional de Personas Beneficiarias Finales se encuentra aún en tramitación parlamentaria (primer trámite constitucional ante el Senado).

II. Análisis de las treinta jurisdicciones más significativas

Criterios de selección

Se analiza a continuación la regulación vigente en materia de registros de beneficiarios finales en las 30 jurisdicciones que estimamos como más significativas. El listado se ha compilado atendiendo a los siguientes factores: (1) Volumen de actividad económica medido por el Producto Interior Bruto. (2) Volumen de transacciones financieras, medido por el volumen total de operaciones en los mercados financieros, incluyendo transacciones en bolsas de valores, mercados de bonos, y otros instrumentos financieros. (3) Actividad en mercados de divisas (Forex). (4) Adopción de criptomonedas, medida por el número de exchanges operativos y el volumen total de transacciones. Este listado refleja no solo el tamaño y la actividad de las economías más grandes, sino también la importancia de ciertas jurisdicciones, como Hong Kong y Singapur, que juegan un papel crucial en el sistema financiero global gracias a sus regulaciones favorables, infraestructura avanzada y adopción de nuevas tecnologías.

1. Estados Unidos

En los Estados Unidos, el régimen aplicable en materia de registros de beneficiarios finales está contenido principalmente en la Ley de Transparencia Corporativa (Corporate Transparency Act, CTA), que se promulgó como parte del paquete de reformas de la Ley de Autorización de Defensa Nacional para el año fiscal 2021. Esta ley marca un cambio significativo en la normativa estadounidense, con el objetivo de combatir el lavado de activos, el financiamiento del terrorismo y otras actividades ilícitas mediante el aumento de la transparencia en la propiedad de las entidades jurídicas.

La Ley de Transparencia Corporativa requiere que todas las empresas y entidades jurídicas constituidas o registradas para hacer negocios en los Estados Unidos presenten información sobre sus beneficiarios finales al Departamento del Tesoro. La normativa se aplica a una amplia gama de entidades, incluidas corporaciones, sociedades de responsabilidad limitada (LLCs) y otras entidades similares. Sin embargo, existen algunas exenciones para ciertas entidades reguladas, grandes corporaciones y subsidiarias.

La ley exige que las entidades proporcionen información detallada sobre los beneficiarios finales, lo que incluye el nombre completo, la fecha de nacimiento, la dirección de residencia y un número de identificación aceptable, como el número de pasaporte o el número de licencia de conducir. Esta información debe ser actualizada regularmente y comunicada al Departamento del Tesoro.

Autoridad responsable

Corporate Transparency Register (CTR)

El Financial Crimes Enforcement Network (FinCEN), la Unidad de Inteligencia Financiera adscrita al Departamento del Tesoro de los Estados Unidos, es la autoridad encargada de implementar y supervisar el régimen de registro de beneficiarios finales. FinCEN ha desarrollado el Registro de Transparencia Corporativa (Corporate Transparency Register, CTR), que es el sistema en el que se almacenará la información comunicada por las entidades.

Las empresas deben enviar la información requerida a FinCEN, que la mantendrá en un sistema seguro y accesible únicamente para las autoridades competentes. FinCEN tiene la responsabilidad de asegurar que la información sea recopilada y mantenida de manera segura y confidencial.

Aspectos tecnológicos

El registro de beneficiarios finales en los Estados Unidos se gestiona a través de una plataforma tecnológica avanzada desarrollada por FinCEN denominada Beneficial Ownership Secure System

(BOSS). Este sistema digital permite a las entidades comunicar y actualizar la información de manera electrónica.

El sistema utiliza tecnologías de cifrado y autenticación para proteger la información sensible contra accesos no autorizados. Además, está diseñado para facilitar la accesibilidad y la eficiencia en la gestión de los datos, permitiendo a FinCEN y otras autoridades competentes realizar supervisiones y auditorías de manera efectiva.

Accesibilidad

La información contenida en el Registro de Transparencia Corporativa no estará disponible para el público general con el objetivo de proteger la privacidad de los individuos. Sin embargo, la información será accesible para ciertas autoridades competentes, como las fuerzas del orden y otras agencias gubernamentales que participan en la prevención y combate del lavado de activos y el financiamiento del terrorismo. También se permitirá el acceso a instituciones financieras en cumplimiento de sus obligaciones de diligencia debida de acuerdo con la Ley de Secreto Bancario.

FinCEN también puede compartir información con autoridades extranjeras en el marco de acuerdos de cooperación y asistencia mutua, contribuyendo a los esfuerzos globales contra las actividades financieras ilícitas.

2. China

China acaba de poner en funcionamiento su registro de propiedad beneficiaria, encontrándose en fase de implementación.

El 29 de abril de 2024, el Banco Popular de China (PBOC) y la Administración Estatal de Regulación del Mercado (SAMR) emitieron conjuntamente las Medidas Administrativas para la Información sobre la Propiedad Beneficiaria. Estas medidas, que han entrado en vigor el 1 de noviembre de 2024, requieren que entidades como empresas, sociedades, sucursales de empresas extranjeras y otras entidades especificadas presenten información sobre sus propietarios beneficiarios.

Autoridades responsables

El registro es una base de datos centralizada mantenida por la Administración Estatal de Regulación del Mercado (SAMR) y el Banco Popular de China (PBOC). Este enfoque centralizado asegura que todos los datos de los beneficiarios finales se recopilen y almacenen en un único repositorio seguro, facilitando una gestión y supervisión más sencillas.

Las entidades legales están obligadas a presentar información sobre los beneficiarios finales utilizando un sistema electrónico seguro. Este sistema está diseñado para garantizar la confidencialidad y la integridad de los datos presentados, minimizando los riesgos de acceso no autorizado o fuga de datos.

3. Japón

Japón no cuenta con un registro operativo de beneficiarios finales. A partir de enero de 2022, el sistema permite el registro opcional de los beneficiarios finales por parte de las sociedades anónimas. Sin embargo, esta declaración no es obligatoria para todas las empresas, lo que limita la exhaustividad y efectividad del registro.

4. Alemania

En Alemania, el régimen aplicable en materia de registros de beneficiarios finales está regulado por la Ley de Registro de Transparencia e Información Financiera (Transparenzregister und Finanzinformationsgesetz, TraFinG), que modifica y complementa la Ley de Blanqueo de Capitales (Geldwäschegesetz, GwG). Este marco legal se implementa para mejorar la transparencia en la propiedad de las entidades jurídicas y combatir el lavado de activos y el financiamiento del terrorismo, alineándose con las directivas de la Unión Europea. El derecho de la Unión Europea ha ido más allá del estándar del GAFI (cuya Recomendación 24 reconoce la posibilidad de "mecanismos alternativos") exigiendo a todos los Estados Miembros el establecimiento de registros de beneficiarios finales.

Desde el 1 de octubre de 2017, la Ley de Blanqueo de Capitales exige que todas las entidades jurídicas registradas en Alemania identifiquen y registren a sus beneficiarios finales en el Registro de Transparencia (Transparenzregister). Esta obligación se extiende a todas las empresas, fundaciones, asociaciones y otras entidades legales que operan en el país.

Transparenzregister

La normativa especifica que las entidades deben recopilar y registrar información detallada sobre los beneficiarios finales, incluyendo el nombre completo, la fecha de nacimiento, la nacionalidad, la dirección, y la naturaleza y extensión del control ejercido. Esta información debe mantenerse actualizada y ser comunicada al Registro de Transparencia.

Autoridad responsable

El Registro de Transparencia está gestionado por la Agencia Federal de Administración (Bundesverwaltungsamt, BVA). Las empresas y otras entidades deben presentar la información requerida electrónicamente a través del portal en línea del BVA. Las entidades deben asegurarse de que la información sea completa y esté actualizada, y deben revisar y confirmar los datos anualmente La BVA es responsable de mantener y supervisar el registro, así como de asegurar el cumplimiento de la normativa.

Aspectos tecnológicos

Alemania ha implementado un sistema tecnológico avanzado para la gestión del Registro de Transparencia. La plataforma permite a las entidades registrar y actualizar la información de sus beneficiarios finales en línea y utiliza protocolos avanzados de cifrado, como TLS (Transport Layer Security), para asegurar que los datos transmitidos entre los usuarios y el sistema estén protegidos contra accesos no autorizados y ciberataques. La autenticación se realiza mediante métodos seguros, incluyendo autenticación de dos factores (2FA), para garantizar que solo usuarios autorizados puedan acceder y modificar la información en el registro.

El sistema está diseñado para integrarse con otros registros y bases de datos gubernamentales, como el Registro Mercantil y el Registro de Empresas. Esta integración facilita el intercambio de información y asegura que los datos sean consistentes y estén actualizados en todas las plataformas. La integración permite la automatización de procesos, como la verificación de datos y la actualización automática de información, lo que reduce la carga administrativa y minimiza errores humanos.

Accesibilidad

La información contenida en el Registro de Transparencia es accesible para las autoridades competentes, incluyendo la policía, las autoridades fiscales, y otras agencias encargadas de la prevención y combate del lavado de activos y el financiamiento del terrorismo. Además, Alemania puede compartir información sobre beneficiarios finales en el marco de acuerdos de cooperación y asistencia mutua.

Al igual que en otros países europeos (véase anexo 3), el acceso a la información contenida en el Transparenzregister alemán por parte del público general ha sido modificado significativamente como consecuencia de una reciente sentencia del Tribunal de Justicia de la Unión Europea (TJUE). En noviembre de 2022, el TJUE dictaminó que el acceso público a la información sobre la titularidad real en los registros de transparencia de la UE constituye una grave interferencia con el derecho a la privacidad y la protección de datos personales, y que dicha interferencia no es necesaria ni proporcional a los objetivos de lucha contra el lavado de activos y el financiamiento del terrorismo.

Como resultado de esta sentencia, la accesibilidad pública a la información del Transparenzregister se ha restringido. Ahora, el acceso está limitado a ciertas entidades que pueden demostrar un "interés legítimo", como periodistas y organizaciones de la sociedad civil que trabajan en la prevención del lavado de activos. Esto ha llevado a que las solicitudes de acceso sean evaluadas caso por caso, lo que puede resultar en procesos más largos y restrictivos para obtener información del registro.

5. Reino Unido

Persons with Significant Control (PSC) Register

En el Reino Unido, el régimen aplicable en materia de registros de beneficiarios finales se encuentra regulado principalmente por la Ley de Sociedades de 2006 (Companies Act 2006), con modificaciones introducidas por la Ley de Pequeños Negocios, Empresas y Empleo de 2015 (Small Business, Enterprise and Employment Act 2015). Estas modificaciones han establecido la obligación de mantener un registro de personas con control significativo (Persons with Significant Control, PSC). Este régimen busca mejorar la transparencia en la propiedad de las empresas y combatir el lavado de activos y el financiamiento del terrorismo.

El Registro de PSC fue introducido en abril de 2016 y requiere que todas las empresas y sociedades de responsabilidad limitada (LLPs) registradas en el Reino Unido identifiquen y mantengan un registro de sus beneficiarios finales. A partir del 30 de junio de 2016, esta información debe ser enviada y mantenida actualizada en el Registro de Empresas (Companies House).

La normativa específica que regula este registro se encuentra en la Parte 21A de la Ley de Sociedades de 2006, desarrollada por las Regulaciones sobre Personas con Control Significativo de 2016 (The Register of People with Significant Control Regulations 2016). Las empresas deben registrar información como el nombre completo del beneficiario, la fecha de nacimiento, la nacionalidad, el domicilio y la naturaleza del control ejercido.

Autoridad responsable

El Registro de PSC está gestionado por la Companies House, la agencia ejecutiva del Departamento de Negocios, Energía y Estrategia Industrial del Reino Unido (BEIS). La Companies House es responsable de recopilar, mantener y publicar la información del PSC. Las empresas deben presentar la información requerida a través de los formularios oficiales y actualizarlos siempre que haya cambios significativos.

La obligación de mantener el Registro de PSC incluye conservar la información en el domicilio registrado de la empresa y proporcionar acceso a esta información cuando sea solicitado por las autoridades competentes.

Aspectos tecnológicos

La Companies House ha implementado una plataforma en línea avanzada que permite a las empresas registrar y actualizar la información de los beneficiarios finales de manera electrónica. Este sistema facilita la presentación de datos mediante un portal diseñado con el objetivo de permitir a las empresas cumplir con sus obligaciones legales de manera eficiente. Las tecnologías de cifrado, como el uso de TLS (Transport Layer Security), aseguran que los datos transmitidos estén protegidos contra accesos no autorizados, mientras que la autenticación de dos factores (2FA) proporciona una capa adicional de seguridad para el inicio de sesión.

El portal en línea de Companies House está integrado con otros sistemas gubernamentales a través de interfaces de programación de aplicaciones (API), lo que permite un intercambio fluido de información y una supervisión eficaz por parte de las autoridades competentes. Esta integración facilita la sincronización de datos y la actualización automática de la información registrada, asegurando que los datos sean consistentes y estén siempre actualizados. Además, el sistema emplea algoritmos de validación para verificar la exactitud de los datos ingresados, lo que minimiza la posibilidad de errores humanos y mejora la precisión de la información registrada.

Para garantizar la integridad de los datos, la plataforma mantiene un registro de auditoría detallado que rastrea todas las modificaciones realizadas en la información de los beneficiarios finales. Este historial de auditoría permite a las autoridades realizar verificaciones cuando sea necesario.

Accesibilidad

La información registrada en el Registro de PSC es accesible al público general a través del portal en línea de Companies House. Esto facilita la transparencia y permite a cualquier persona interesada verificar la información sobre los beneficiarios finales de una empresa.

Sin embargo, ciertos datos personales, como la dirección residencial completa y la fecha completa de nacimiento, están protegidos y solo son accesibles para las autoridades competentes. Esta protección se orienta a garantizar un equilibrio entre la transparencia y la privacidad de los individuos.

6. Francia

En Francia, el régimen aplicable en materia de registros de beneficiarios finales está regulado principalmente por el Código Monetario y Financiero (Code monétaire et financier) y por la Ordenanza 2016-1635 de 1 de diciembre de 2016, que introduce la obligación de mantener un registro de beneficiarios finales. Esta normativa se implementó para cumplir con las directivas de la Unión Europea sobre la prevención del lavado de activos y el financiamiento del terrorismo.

Desde el 1 de agosto de 2017, todas las entidades jurídicas registradas en Francia, incluyendo sociedades anónimas, sociedades de responsabilidad limitada, asociaciones y otras entidades similares, están obligadas a identificar y registrar a sus beneficiarios finales. Esta obligación se extiende

a todas las entidades que tengan una estructura de propiedad que permita identificar a los beneficiarios finales.

Según la normativa, las entidades deben recopilar y registrar información detallada sobre los beneficiarios finales, lo que incluye el nombre completo, la fecha de nacimiento, la nacionalidad, el país de residencia, y la naturaleza y el alcance del control ejercido. La información debe ser registrada en el Registro de Beneficiarios Finales (Registre des bénéficiaires effectifs, RBE).

Autoridad responsable

Registre des bénéficiaires effectifs (RBE)

El Registro de Beneficiarios Finales en Francia está gestionado por el Registro de Comercio y Sociedades (Registre du Commerce et des Sociétés, RCS). Las empresas deben presentar la información requerida al RCS, que es administrado por los Tribunales de Comercio. Esta información debe ser actualizada siempre que haya cambios significativos en la estructura de propiedad o control de la entidad.

Las entidades están obligadas a proporcionar la información a través de un formulario específico que se presenta electrónicamente a través del portal en línea Infogreffe, que centraliza y administra los registros de comercio y sociedades en Francia.

Aspectos tecnológicos

Francia ha implementado soluciones tecnológicas para facilitar el registro y la gestión de la información sobre beneficiarios finales. El sistema Infogreffe permite a las entidades registrar y actualizar la información de manera electrónica, asegurando así la eficiencia y la precisión de los datos. Este sistema digital está diseñado para ser seguro y proteger la información sensible mediante tecnologías de cifrado y autenticación.

Además, el sistema Infogreffe está integrado con otras bases de datos gubernamentales para posibilitar un intercambio de información fluido y una supervisión eficaz por parte de las autoridades competentes.

Accesibilidad

La información sobre los beneficiarios finales registrada en el RBE es accesible para las autoridades competentes, incluyendo la Autoridad de Supervisión Prudencial y de Resolución (Autorité de contrôle prudentiel et de résolution, ACPR), la policía, y otras agencias gubernamentales que participan en la prevención del lavado de activos y el financiamiento del terrorismo.

El acceso restringido a la información permite que las autoridades realicen investigaciones y supervisiones efectivas sin comprometer la privacidad de los datos personales. Además, Francia coopera con organismos internacionales y puede compartir información sobre beneficiarios finales en el marco de acuerdos de cooperación y asistencia mutua.

Al igual que en otros países europeos, en Francia el acceso al Registre des bénéficiaires effectifs (RBE) se ha visto modificado tras la sentencia del Tribunal de Justicia de la Unión Europea de 22 de noviembre de 2022. Como resultado, el acceso generalizado al público ha sido limitado, y ahora se requiere que quienes accedan a esta información demuestren un interés legítimo para proteger la privacidad y los datos personales de los individuos registrados.

7. India

La India no cuenta con un registro centralizado público de propiedad beneficiaria. En su lugar, el marco regulatorio requiere que las empresas mantengan sus propios registros de beneficiarios finales y que presenten los detalles relevantes al Registrador de Empresas según lo estipulado en las disposiciones de la Ley de Sociedades de 2013 y las reglas de Propietarios Beneficiarios Significativos (SBO, por sus siglas en inglés). Estos registros se mantienen internamente por cada empresa y no se compilan en un único registro centralizado accesible al público.

8. Italia

Italia ha establecido un registro central de beneficiarios finales para mejorar la transparencia y la lucha contra el lavado de activos. La colaboración con este registro es una medida obligatoria para todas las entidades legales, incluyendo empresas y otras organizaciones, que deben reportar y actualizar la información sobre sus beneficiarios finales.

En Italia, el régimen aplicable en materia de registros de beneficiarios finales está enmarcado principalmente en el Decreto Legislativo No. 231 de 2007, modificado por el Decreto Legislativo No. 90 de 2017, que implementa la Cuarta Directiva (AMLD4) y la Quinta Directiva (AMLD5) europeas contra el lavado de activos y el financiamiento del terrorismo.

Autoridad responsable

La autoridad principal encargada del registro de beneficiarios finales en Italia es el Registro de Empresas, bajo la supervisión del Ministerio de Desarrollo Económico (Ministero dello Sviluppo Economico). Las Cámaras de Comercio regionales gestionan los datos con el objetivo de asegurar que la información proporcionada por las entidades sea precisa y actualizada.

Registro delle Imprese

El sistema está organizado para que las empresas presenten la información requerida directamente a través del portal del Registro de Empresas. Esta información incluye detalles sobre la identidad de los beneficiarios finales, la naturaleza y el alcance del interés de propiedad o control que poseen. Las empresas deben actualizar esta información regularmente o cuando se produzcan cambios significativos en la estructura de propiedad.

Aspectos tecnológicos

Italia ha adoptado una infraestructura tecnológica para la gestión del registro de beneficiarios finales. El sistema está basado en una plataforma digital que permite la presentación y actualización de datos en línea, facilitando el acceso y la administración de la información por parte de las autoridades competentes. Concretamente, el sistema emplea tecnologías de cifrado avanzado como TLS (Transport Layer Security) para proteger los datos sensibles durante la transmisión, asegurando que la información no pueda ser interceptada o manipulada por terceros no autorizados. Además, implementa métodos de autenticación de dos factores (2FA) para garantizar que solo usuarios autorizados puedan acceder a la plataforma, añadiendo una capa adicional de seguridad. El sistema también está integrado con otras bases de datos gubernamentales a través de interfaces de programación de aplicaciones (APIs), lo que permite un intercambio de información eficiente y en tiempo real, facilitando la verificación cruzada de datos y la actualización automática de la información registrada. Además, emplea algoritmos avanzados para la validación y verificación de los datos

ingresados, minimizando los errores humanos y garantizando la precisión de la información registrada. Por último, el sistema implementa sistemas de monitoreo continuo y alertas automatizadas para detectar cualquier actividad sospechosa o inconsistencias en los registros, permitiendo una intervención rápida por parte de las autoridades competentes.

Accesibilidad

El acceso a la información del registro de beneficiarios finales está restringido a ciertas autoridades, como las autoridades judiciales, la Guardia di Finanza, y otros organismos de control y supervisión que requieran esta información para llevar a cabo sus funciones de supervisión y cumplimiento. Sin embargo, en conformidad con la AMLD5, el acceso a la información del registro puede ser concedido también a sujetos obligados como instituciones financieras y otros sujetos responsables de cumplir con las normas contra el lavado de activos.

La información contenida en el registro de beneficiarios finales no es accesible al público en general. El acceso está limitado para proteger la privacidad de los beneficiarios finales, aunque se prevé la posibilidad de que ciertos datos sean accesibles para sujetos con un interés legítimo, como periodistas o investigadores en casos específicos de interés público o relacionado con la lucha contra la corrupción y el crimen financiero.

9. Canadá

El marco legal principal que rige los registros de beneficiarios finales en Canadá se contiene en la Ley de Corporaciones de Canadá (Canada Business Corporations Act, CBCA), que fue enmendada significativamente con la introducción del Bill C-42, el cual recibió la sanción real el 2 de noviembre de 2023.

Autoridad responsable

Corporations Canada

El registro de beneficiarios finales en Canadá depende de Corporations Canada, parte de Innovation, Science and Economic Development Canada. Las corporaciones están obligadas a recopilar, mantener y actualizar la información sobre sus beneficiarios finales y poner esta información a disposición de las autoridades pertinentes cuando se les solicite. Además, ahora deben presentar esta información a Corporations Canada, asegurando que los registros se mantengan precisos y actualizados.

Aspectos tecnológicos y accesibilidad

Canadá ha implementado un sistema digital que facilita la gestión de los registros de beneficiarios finales por parte de las corporaciones. Aunque el registro de beneficiarios finales no es completamente accesible al público, cierta información será accesible a través de búsquedas en línea, equilibrando la transparencia con la protección de la privacidad.

Iniciativas Provinciales y Territoriales

Además de la ley federal, algunas provincias y territorios en Canadá, como Quebec y Columbia Británica, han implementado o están en proceso de implementar sus propias leyes y sistemas de registro de beneficiarios finales, lo que refleja un esfuerzo coordinado a nivel nacional y provincial para mejorar la transparencia corporativa.

10. Corea del Sur

Corea del Sur actualmente no tiene un registro público centralizado de beneficiarios finales. El país se ha comprometido a implementar medidas para la transparencia de la propiedad beneficiaria, pero hasta ahora, estas aún están en etapas de planificación. En el sector financiero, ciertas regulaciones exigen que las instituciones identifiquen a los beneficiarios finales de las personas jurídicas y empresas con las que tratan, especialmente para cumplir con las leyes contra el lavado de activos. Sin embargo, esto no se extiende a un registro público centralizado, y fuera del sector financiero, no existe un requisito general para que las compañías mantengan o divulguen públicamente la información sobre la propiedad beneficiaria.

11. Rusia

Rusia actualmente no tiene un registro público centralizado de beneficiarios finales. En su lugar, existen requisitos de informes específicos, principalmente para fines fiscales y cumplimiento de la lucha contra el lavado de dinero, que obligan a ciertas entidades a divulgar información sobre los beneficiarios finales. Estas divulgaciones están integradas en varios marcos regulatorios, pero no se consolidan en un único registro público centralizado.

En Rusia, el régimen aplicable en materia de beneficiarios finales se encuentra regulado principalmente por la Ley Federal No. 115-FZ Sobre la Prevención del Blanqueo de Dinero y la Financiación del Terrorismo. Esta legislación se complementa con diversas directivas y regulaciones emitidas por el Banco Central de Rusia y otros organismos reguladores.

La Ley Federal No. 115-FZ establece la obligación para las organizaciones, incluyendo instituciones financieras y no financieras, de identificar y registrar a sus beneficiarios finales. Esta obligación busca aumentar la transparencia en la propiedad de las empresas y prevenir actividades ilícitas como el lavado de activos y el financiamiento del terrorismo.

Según esta ley, las entidades deben recopilar, verificar y actualizar regularmente la información sobre sus beneficiarios finales. La información requerida incluye datos personales como el nombre completo, la fecha de nacimiento, la nacionalidad, y el porcentaje de participación o control sobre la entidad. Esta información debe ser conservada por un período mínimo de cinco años.

Autoridad responsable

La autoridad principal encargada de la supervisión de la normativa sobre beneficiarios finales es el Servicio Federal de Supervisión Financiera (Rosfinmonitoring).

Rosfinmonitoring tiene la facultad de realizar auditorías y supervisiones para verificar la precisión y la actualización de los registros de beneficiarios finales mantenidos por las entidades. Además, las organizaciones deben reportar cualquier discrepancia o cambio significativo en la información de los beneficiarios finales de manera oportuna.

Aspectos tecnológicos

Las entidades deben reportar y actualizar la información de manera electrónica a través de plataformas específicas proporcionadas por Rosfinmonitoring y otras autoridades regulatorias. El acceso a la información de los beneficiarios finales está restringido a las autoridades reguladoras y de aplicación

de la ley, garantizando la privacidad de los individuos involucrados. Sin embargo, en casos específicos y bajo ciertas condiciones, esta información puede ser compartida con otras entidades, tanto nacionales como internacionales, en el marco de investigaciones sobre actividades ilícitas.

12. Australia

Australia no cuenta actualmente con un registro público centralizado de beneficiarios finales. El gobierno federal ha iniciado pasos hacia el establecimiento de dicho registro, incluyendo la publicación de un documento de consulta en noviembre de 2022 para recopilar comentarios sobre el diseño y la implementación de la primera fase de un registro de propiedad beneficiaria accesible al público.

La Ley de Sociedades (Corporations Act 2001) exige que las empresas mantengan un registro de las personas que ostentan una participación significativa. Además, la Ley contra el Lavado de Dinero y la Financiación del Terrorismo (Anti-Money Laundering and Counter-Terrorism Financing Act 2006) establece obligaciones para las entidades de identificar y verificar la identidad de los beneficiarios finales.

Autoridad responsable

El organismo principal encargado de la supervisión y administración de la normativa de beneficiarios finales es la Comisión Australiana de Valores e Inversiones (Australian Securities and Investments Commission, ASIC). ASIC tiene la responsabilidad de garantizar que las empresas cumplan con sus obligaciones de registrar información sobre los beneficiarios finales.

El sistema está organizado de tal manera que las empresas deben mantener un registro interno de sus beneficiarios finales, el cual debe ser accesible para las autoridades competentes, incluyendo ASIC y AUSTRAC (Australian Transaction Reports and Analysis Centre).

13. Brasil

En Brasil, el marco regulatorio en materia de beneficiarios finales se rige principalmente por la Instrucción Normativa RFB No. 2119 del 6 de diciembre de 2022, que actualizó y reemplazó la Instrucción Normativa No. 1.863. Este reglamento establece que todas las entidades jurídicas registradas en Brasil, tanto nacionales como extranjeras operando en el país, deben identificar y reportar a sus beneficiarios finales a la Receita Federal. Los datos requeridos incluyen información personal del beneficiario final como nombre completo, fecha de nacimiento, nacionalidad, número de identificación fiscal, y el porcentaje de participación o control en la entidad.

Autoridad responsable

La Receita Federal de Brasil (RFB) es la autoridad encargada de supervisar y mantener el registro de beneficiarios finales. Las entidades deben proporcionar y actualizar la información requerida a través del Sistema Público de Escrituração Digital (SPED).

Receita Federal de Brasil (RFB)

Aspectos tecnológicos

El Sistema Público de Escrituração Digital (SPED) es una plataforma implementada por la Receita Federal para digitalizar el cumplimiento fiscal de las empresas. Este sistema permite la integración y procesamiento electrónico de datos contables, fiscales y financieros, facilitando a las entidades el

cumplimiento de sus obligaciones de reporte. A través del SPED, las empresas pueden transmitir sus libros contables, documentos fiscales y facturas electrónicas directamente a la Receita Federal.

El SPED incluye varios componentes, como la Escrituração Contábil Digital (ECD), la Escrituração Fiscal Digital (EFD) y la Nota Fiscal Electrônica (NF-e). La ECD permite la transmisión de los libros contables en formato digital, mejorando la precisión y reduciendo la posibilidad de errores. La EFD facilita la transmisión electrónica de documentos fiscales, asegurando que las declaraciones cumplan con las normas tributarias. La NF-e permite la emisión y almacenamiento de facturas electrónicas, reduciendo costos operativos asociados con la gestión de documentos en papel.

El SPED automatiza el proceso de reportes fiscales, reduciendo la carga administrativa y el tiempo necesario para cumplir con las obligaciones. Además, permite a la Receita Federal monitorear y auditar la información en tiempo real, garantizando que los datos sean precisos y estén actualizados. El sistema facilita la integración de los sistemas contables y fiscales de las empresas con la plataforma SPED, permitiendo una transferencia de datos más fluida.

Desde el punto de vista tecnológico, el SPED utiliza varios métodos avanzados para asegurar la integridad y confidencialidad de la información transmitida. Entre estos métodos se incluyen la autenticación mediante certificados digitales y el cifrado de datos utilizando algoritmos avanzados. Los certificados digitales, emitidos por una Autoridad Certificadora acreditada, permiten la verificación de la identidad de los usuarios, asegurando que solo las personas autorizadas puedan acceder y transmitir información a través del sistema. Esto garantiza que los documentos enviados no han sido alterados desde su creación.

El cifrado de datos en el SPED se realiza utilizando algoritmos avanzados como el AES (Advanced Encryption Standard) de 256 bits. Este cifrado asegura que la información sea ilegible para cualquier persona no autorizada que pueda interceptar los datos durante su transmisión, protegiendo tanto la integridad como la confidencialidad de la información fiscal y contable.

Además, el SPED implementa controles de acceso y auditorías de seguridad. Los controles de acceso aseguran que solo las personas autorizadas pueden acceder al sistema y realizar ciertas operaciones, mientras que las auditorías de seguridad monitorean y registran todas las actividades dentro del sistema. Estos controles permiten a la Receita Federal detectar y responder rápidamente a cualquier intento de acceso no autorizado o actividad sospechosa, mejorando la seguridad general del sistema.

El Sistema Público de Escrituração Digital (SPED) permite la integración y el procesamiento electrónico de datos, lo que facilita a las entidades el cumplimiento de sus obligaciones de reporte. El SPED permite a la Receita Federal monitorear y auditar la información y asegurar que se mantenga actualizada y accesible para las autoridades competentes en tiempo real.

Accesibilidad

La información en el registro de beneficiarios finales no es pública para proteger la privacidad de los individuos. Sin embargo, está disponible para autoridades fiscales y de aplicación de la ley para supervisión y cumplimiento, y puede ser compartida con otras agencias gubernamentales y organismos internacionales en investigaciones de lavado de dinero y otros delitos financieros.

14. España

En España, el régimen aplicable en materia de registros de beneficiarios finales ha sido recientemente reforzado con la aprobación del Real Decreto 609/2023, de 11 de julio. Este desarrollo legislativo responde a la necesidad de incrementar la transparencia en la propiedad de las entidades y de cumplir con las directivas europeas en materia de prevención del blanqueo de capitales y la financiación del terrorismo.

El Real Decreto 609/2023 establece la creación del Registro Central de Titularidades Reales (RCTR), que tiene como objetivo centralizar la información relativa a los beneficiarios finales de todas las entidades jurídicas registradas en España. Este registro complementa las disposiciones de la Ley 10/2010 y del Real Decreto 304/2014, proporcionando un marco más estructurado y accesible para la recopilación y gestión de esta información.

Autoridad responsable

Registro Central de Titularidades Reales (RCTR)

El Registro Central de Titularidades Reales depende del Ministerio de Justicia, a través de la Dirección General de Seguridad Jurídica y Fe Pública. Este organismo es el encargado de la supervisión y gestión del registro, asegurando que la información proporcionada sea precisa, actualizada y accesible para las autoridades competentes.

Las empresas y otras entidades jurídicas están obligadas a inscribir la información de sus beneficiarios finales en el RCTR, detallando los datos personales de estos, como nombre completo, fecha de nacimiento, nacionalidad, y el tipo y alcance de la participación o control ejercido. Esta información debe actualizarse anualmente o cuando se produzcan cambios significativos en la estructura de propiedad de la entidad.

Aspectos tecnológicos

El RCTR está diseñado para ser un sistema electrónico avanzado que facilita la presentación y actualización de la información de los beneficiarios finales. Las entidades pueden acceder al registro y realizar las inscripciones necesarias a través de una plataforma digital, lo que mejora la eficiencia y la seguridad del proceso. Esta plataforma está integrada con otros registros administrativos y sistemas de información para asegurar la coherencia y exactitud de los datos.

Accesibilidad

El acceso a la información del RCTR está restringido a las autoridades competentes, como la Agencia Tributaria, las autoridades judiciales y las fuerzas de seguridad, así como otras entidades que tengan un interés legítimo reconocido por la normativa. Esta restricción garantiza la protección de la privacidad de los beneficiarios finales mientras se facilita la labor de prevención y combate contra el blanqueo de capitales y la financiación del terrorismo.

La información contenida en el RCTR no es accesible al público general, en consonancia con la normativa de protección de datos personales.

15. México

En la actualidad, no existe en México un registro central operativo de beneficiarios finales. El país ha hecho compromisos formales hacia la transparencia de la propiedad beneficiaria, incluyendo su participación en la Iniciativa de Transparencia de las Industrias Extractivas (EITI) y su compromiso con la Alianza para el Gobierno Abierto (OGP).

En términos de implementación tecnológica, México está en proceso de adoptar el Estándar de Datos de Propiedad Beneficiaria (Beneficial Ownership Data Standard, BODS) desarrollado por Open Ownership para su registro piloto de beneficiarios finales en contrataciones públicas.

16. Indonesia

En Indonesia, el régimen aplicable en materia de registros de beneficiarios finales se regula principalmente en la Ley No. 8 de 2010 sobre la Prevención y Erradicación del Delito de Lavado de Dinero (UU 8/2010) y la Ley No. 9 de 2013 sobre la Prevención y Erradicación del Financiamiento del Terrorismo (UU 9/2013). Estas leyes establecen las obligaciones de las entidades para identificar y registrar a los beneficiarios finales, con el objetivo de mejorar la transparencia y combatir el lavado de activos y el financiamiento del terrorismo.

El gobierno de Indonesia ha adoptado regulaciones específicas para asegurar la implementación efectiva de estos registros. En particular, la Regulación Presidencial No. 13 de 2018 sobre la Implementación del Principio de Conocer al Beneficiario Final en la Prevención y Erradicación del Delito de Lavado de Dinero y del Financiamiento del Terrorismo es una pieza clave de esta estructura legal. Esta regulación obliga a todas las entidades legales a identificar, verificar y registrar a sus beneficiarios finales.

Autoridad responsable

El Ministerio de Justicia y Derechos Humanos de Indonesia es la principal autoridad responsable de la implementación y supervisión del registro de beneficiarios finales. Este ministerio, a través de la Dirección General de Administración de Leyes Generales (Ditjen AHU), administra el sistema de registro y asegura que todas las entidades cumplan con los requisitos establecidos por la ley.

Las entidades legales deben proporcionar información detallada sobre sus beneficiarios finales, incluyendo datos personales y la naturaleza de su participación o control. Esta información debe ser actualizada periódicamente y presentada al Ministerio de Justicia y Derechos Humanos.

Aspectos tecnológicos

Indonesia ha implementado un sistema tecnológico para facilitar la gestión de la información de los beneficiarios finales. El registro se realiza a través de una plataforma electrónica administrada por la Dirección General de Administración de Leyes Generales. Esta plataforma permite a las entidades registrar y actualizar la información en línea.

El sistema está diseñado para ser accesible tanto para las entidades obligadas como para las autoridades competentes. Las entidades pueden ingresar la información requerida electrónicamente, lo que facilita el cumplimiento de las normativas y mejora la precisión de los datos registrados.

Además, el sistema está integrado con otros registros gubernamentales, lo que permite un intercambio de información más efectivo y una mejor supervisión por parte de las autoridades.

Accesibilidad

La información registrada sobre los beneficiarios finales no está disponible para el público general, en cumplimiento de la normativa de privacidad y protección de datos personales. Sin embargo, esta información es accesible para las autoridades competentes, como las agencias de aplicación de la ley, las autoridades fiscales y otras entidades gubernamentales que tienen un interés legítimo en la prevención y erradicación del lavado de dinero y la financiación del terrorismo.

Además, la Comisión de Supervisión de Transacciones Financieras (PPATK) juega un rol crucial en el monitoreo y análisis de la información relacionada con los beneficiarios finales.

17. Países Bajos

En los Países Bajos, el régimen aplicable en materia de registros de beneficiarios finales se encuentra regulado por la Ley de Implementación del Registro de Beneficiarios Finales (Wet Implementatie UBO-Register), que entró en vigor el 27 de septiembre de 2020. La ley establece que todas las entidades jurídicas registradas en los Países Bajos, incluyendo sociedades anónimas (NV), sociedades de responsabilidad limitada (BV), fundaciones, asociaciones y otras estructuras legales, deben identificar y registrar a sus beneficiarios finales. Esta obligación también se extiende a ciertas estructuras extranjeras que operan en el país.

UBO-Register

La ley requiere que las entidades proporcionen información detallada sobre sus beneficiarios finales, incluyendo nombre, fecha de nacimiento, nacionalidad, dirección, y la naturaleza y el alcance del interés de propiedad o control. La información debe ser presentada al Registro de Beneficiarios Finales (UBO-Register) y actualizada cuando haya cambios significativos.

Autoridad responsable

El Registro de Beneficiarios Finales en los Países Bajos es administrado por la Cámara de Comercio de los Países Bajos (Kamer van Koophandel, KvK). La KvK es responsable de recibir, verificar y gestionar la información de los beneficiarios finales. Las entidades jurídicas deben registrar a sus beneficiarios finales a través de la plataforma en línea de la KvK, que está diseñada para facilitar el proceso de presentación y actualización de la información.

Aspectos tecnológicos

La plataforma digital de la KvK permite a las entidades jurídicas registrar y actualizar la información de sus beneficiarios finales de manera completamente electrónica. La autenticación en la plataforma se realiza mediante el uso de certificados digitales emitidos por autoridades certificadoras confiables, permitiendo la verificación de la identidad de los usuarios y garantizando que solo las personas autorizadas puedan acceder y modificar la información. El cifrado TLS (Transport Layer Security) se utiliza para proteger los datos en tránsito, asegurando que toda la información transmitida entre los usuarios y la plataforma esté cifrada durante la transferencia, evitando que sea interceptada y leída por terceros no autorizados. Para los datos en reposo, se emplea el cifrado AES (Advanced Encryption Standard) de 256 bits, un algoritmo de cifrado simétrico muy seguro que garantiza que incluso si los

datos almacenados fueran accedidos de manera no autorizada, estos serían ilegibles sin la clave de descifrado adecuada. Además, la plataforma KvK cuenta con sistemas de monitorización continua que registran todas las actividades dentro del sistema, permitiendo detectar y responder rápidamente a cualquier intento de acceso no autorizado o actividad sospechosa. La infraestructura de la KvK está equipada con soluciones avanzadas de ciberseguridad, incluyendo firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS) y software antivirus/malware, trabajando en conjunto para proteger la plataforma contra una amplia gama de amenazas cibernéticas.

Accesibilidad

Después de la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 22 de noviembre de 2022, el acceso del público general al Registro de Beneficiarios Finales (UBO) ha sido restringido. Esto ha supuesto que la información detallada sobre los beneficiarios finales, especialmente la información sensible como el día de nacimiento, la dirección completa y el número de identificación fiscal, ya no está disponible para el público general. Las autoridades competentes, como la Fiscalía, la policía, la Autoridad Fiscal y la Unidad de Inteligencia Financiera de los Países Bajos (FIU-Netherlands), siguen teniendo acceso completo a la información en el registro UBO para llevar a cabo sus funciones de supervisión y cumplimiento. Por otra parte, ciertas entidades con interés legítimo, como las instituciones financieras y otros sujetos con obligaciones de debida diligencia, pueden acceder a información básica sobre los beneficiarios finales, como el nombre, mes y año de nacimiento, nacionalidad, país de residencia y la naturaleza y alcance de su interés económico, bajo condiciones específicas.

18. Suiza

Aunque las empresas están obligadas a mantener registros internos detallados y actualizados de los beneficiarios finales y deben proporcionar esta información a las autoridades cuando se les solicite, no existe actualmente un registro central público de beneficiarios finales en Suiza. En octubre de 2022, el Consejo Federal instruyó al Departamento Federal de Finanzas (FDF) para que redactara un proyecto de ley destinado a incrementar la transparencia y simplificar la identificación de los beneficiarios finales de las entidades legales. Esta propuesta incluye la creación de un registro central de beneficiarios finales que, aunque no será accesible públicamente, estará disponible para las agencias pertinentes como las autoridades fiscales y las encargadas de la lucha contra el lavado de dinero y la financiación del terrorismo. El registro contendrá información detallada sobre los beneficiarios finales, como el nombre, fecha de nacimiento, nacionalidad y dirección, entre otros datos.

19. Arabia Saudita

En Arabia Saudita, la Circular No. 1/2020 de la Autoridad del Mercado de Capitales (CMA) y las directrices emitidas por la Unidad de Inteligencia Financiera de Arabia Saudita (SAFIU) establecen los requisitos específicos sobre beneficiarios finales, detallando la información que debe ser recopilada y mantenida.

Las empresas deben registrar a sus beneficiarios finales en el Registro de Sociedades, gestionado por el Ministerio de Comercio. Este registro incluye detalles como el nombre completo, la fecha de nacimiento, la nacionalidad y el porcentaje de participación o control ejercido por los beneficiarios finales. El hecho de que las empresas registren a sus beneficiarios finales en el Registro de Sociedades

gestionado por el Ministerio de Comercio y que este registro incluya detalles específicos sobre los beneficiarios finales no implica que este sistema pueda asimilarse a un registro de beneficiarios finales en el sentido más amplio y transparente que se busca a nivel internacional.

20. Turquía

En Turquía, el Comunicado No. 529 sobre Procedimiento Tributario, publicado en el Diario Oficial el 13 de julio de 2021, exige que las entidades registren a sus beneficiarios finales en un sistema centralizado gestionado por la Administración de Ingresos.

El Comunicado No. 529 establece la obligación de que los contribuyentes corporativos y otras entidades declaren anualmente la información sobre sus beneficiarios finales. La información debe incluir datos detallados como el nombre completo, ciudadanía, número de identificación, dirección, y detalles de contacto de los individuos que poseen o controlan más del 25% de la entidad. Además, deben declarar cualquier cambio en esta información dentro de un mes desde que ocurra.

Autoridad responsable

La Administración de Ingresos, dependiente del Ministerio de Hacienda y Finanzas, es la autoridad principal encargada de recibir, analizar y almacenar la información sobre los beneficiarios finales. Las instituciones financieras y otras entidades obligadas, como abogados y notarios, deben recopilar y reportar la información requerida sobre los beneficiarios finales a la Administración de Ingresos.

Gelir İdaresi Başkanlığı (GIB)

Aspectos tecnológicos

Turquía ha implementado una serie de soluciones tecnológicas avanzadas en su sistema electrónico para la presentación y actualización de la información sobre beneficiarios finales. En el acceso se utilizan certificados digitales para la autenticación de los usuarios, asegurando que solo personas autorizadas puedan ingresar y modificar la información, protegiendo así la integridad de los datos. Además, se emplea la autenticación de dos factores (2FA), que añade una capa adicional de seguridad requiriendo no solo una contraseña sino también un segundo factor de autenticación, como un código enviado al teléfono móvil del usuario.

En cuanto al cifrado de datos, todos los datos transmitidos entre los usuarios y la plataforma están cifrados utilizando el protocolo TLS (Transport Layer Security), asegurando que la información no pueda ser interceptada y leída por terceros no autorizados. Los datos almacenados en la plataforma están protegidos mediante cifrado AES (Advanced Encryption Standard) de 256 bits, garantizando que los datos sean inaccesibles sin las claves de descifrado adecuadas.

La plataforma permite a la Administración de Ingresos realizar análisis de datos en tiempo real para identificar patrones sospechosos y posibles actividades ilícitas mediante el uso de algoritmos avanzados y técnicas de análisis de big data. Además, el sistema incluye funcionalidades de alertas automáticas que notifican a las autoridades sobre cualquier irregularidad o actividad inusual detectada en los registros.

El sistema está diseñado para integrarse con otros sistemas y bases de datos gubernamentales, permitiendo una verificación cruzada automática de la información y mejorando la precisión de los

datos. La interfaz del sistema es intuitiva y fácil de usar, facilitando a las entidades la presentación y actualización de información sin necesidad de conocimientos técnicos avanzados.

Todas las actividades realizadas en la plataforma son registradas y auditadas, permitiendo a las autoridades revisar y rastrear cualquier cambio realizado en los registros.

Accesibilidad

La información sobre los beneficiarios finales no está disponible para el público general con el objetivo de proteger la privacidad de los individuos. Sin embargo, esta información es accesible para las autoridades competentes, como la Administración de Ingresos, las fuerzas del orden y otras agencias gubernamentales implicadas en la prevención del lavado de dinero y la financiación del terrorismo. La Administración de Ingresos puede compartir información con contrapartes internacionales en el marco de acuerdos de cooperación y asistencia mutua.

21. Argentina

El 15 de marzo de 2024 se aprobó en Argentina la Ley N° 27.739, la cual modifica la Ley 25.246 incorporando un artículo 4º bis con diversas definiciones. En este contexto, se define como beneficiario final a la persona humana que posee participación, derechos de voto o ejerza el control directo o indirecto de una sociedad, persona jurídica u otra entidad contractual o estructura jurídica. Asimismo, se considera beneficiario final a la persona humana que ejerza su control efectivo final, con el alcance definido en la reglamentación.

En el caso de contratos de fideicomisos y otras estructuras jurídicas similares, tanto nacionales como extranjeras, se incluye como beneficiarios finales a las personas humanas que actúen o participen en dicha estructura bajo cualquier denominación, así como aquellas que cumplan con las condiciones previamente mencionadas respecto de cada una de las partes del contrato. En situaciones donde no sea posible identificar a los beneficiarios finales según las definiciones anteriores, se considerará beneficiarios finales a las personas humanas responsables de la dirección, administración o representación de la persona jurídica, fideicomiso, fondo de inversión o cualquier otro patrimonio de afectación y/o estructura jurídica.

Autoridad responsable

El Capítulo III de la ley establece el Registro Público de Beneficiarios Finales (RPBF), cuya autoridad de aplicación será la Administración Federal de Ingresos Públicos (AFIP). Debe señalarse, no obstante, que la AFIP ha sido suprimida recientemente por Decreto 953/2024, habiéndose anunciado que sus funciones serían asumidas por una institución de nueva creación, la Agencia de Recaudación y Control Aduanero (ARCA).

Se centralizará y mantendrá la información adecuada, precisa y actualizada de las personas humanas que revisten el carácter de beneficiarios finales, en los términos definidos en el artículo 4° bis de la Ley 25.246. Este registro se conformará con la información proveniente de los regímenes informativos tributarios, así como con información que pueda ser requerida a organismos públicos.

Todas las sociedades, personas jurídicas u otras entidades contractuales o estructuras jurídicas constituidas en Argentina o de origen extranjero que realicen actividades en el país, posean bienes o

activos situados en el país, deberán informar sus beneficiarios finales dentro de los 60 días siguientes a la entrada en vigencia de la ley, para su incorporación al registro. También están obligadas las personas humanas residentes en el país que posean participaciones societarias en entidades constituidas en el exterior y aquellos que actúen o participen en fideicomisos o estructuras similares constituidas en el exterior.

La autoridad de aplicación tendrá facultades para incorporar y mantener actualizada la información de los beneficiarios finales, recibir información de la Unidad de Información Financiera (UIF) y otros organismos públicos, emitir normas complementarias para el funcionamiento del registro y suscribir convenios para el intercambio de información y acciones comunes.

Aspectos tecnológicos

Para acceder al registro, los sujetos deberán cumplir con ciertos requisitos. La "Clave Fiscal" con Nivel de Seguridad 3 o superior es una credencial de acceso que permite realizar trámites y consultas a través de su sitio web. El Domicilio Fiscal Electrónico es una dirección electrónica registrada que se utiliza para recibir notificaciones y comunicaciones oficiales, asegurando que el contribuyente esté informado de manera oportuna. El Administrador de Relaciones es una herramienta informática que permite a los responsables designados en una entidad delegar roles y autorizaciones a otros usuarios para efectuar consultas y realizar trámites en nombre de la entidad, según lo previsto en la Resolución General N° 5048.

Los sujetos autorizados para acceder al registro, como el Ministerio Público Fiscal (MPF), el Poder Judicial (PJ), la Unidad de Información Financiera (UIF), entre otros organismos, deberán cumplir con los requisitos de acceso, incluyendo el uso de la "Clave Fiscal" con Nivel de Seguridad 3 o superior y el Domicilio Fiscal Electrónico. Para los órganos de control, también se requerirá el uso de la herramienta "Administrador de Relaciones" y la remisión de una nómina de sujetos habilitados para realizar consultas.

Los sujetos comprendidos en el artículo 29 de la ley y otras personas humanas o jurídicas tendrán acceso a su información o la de sus beneficiarios finales a través del servicio correspondiente, realizando consultas por el número de la Clave Única de Identificación Tributaria (CUIT), el Código Único de Identificación Laboral (CUIL) o la Clave de Identificación (CDI).

Accesibilidad

El acceso a la información contenida en el registro será permitido al Ministerio Público Fiscal (MPF), el Poder Judicial (PJ), la Unidad de Información Financiera (UIF), organismos de control específicos como el Banco Central de la República Argentina (BCRA), la Comisión Nacional de Valores (CNV), la Superintendencia de Seguros de la Nación (SSN) y el Instituto Nacional de Asociativismo y Economía Social (INAES), así como a los sujetos obligados según el artículo 29 de la ley.

El incumplimiento o cumplimiento parcial de los deberes de información sobre beneficiarios finales resultará en la aplicación de sanciones previstas en la ley 11.683 y sus modificaciones.

El 17 de julio de 2024, se emitió la Resolución General 5529/2024, publicada en el Boletín Oficial (B.O.) el 19 de julio de 2024, que implementa el Registro Público de Beneficiarios Finales (RPBF) conforme al

Capítulo III de la Ley N° 27.739. En esta resolución, se establece que centralizará la información referida a los beneficiarios finales, incluyendo datos provenientes de regímenes informativos vigentes y de convenios de intercambio de información con otros organismos públicos.

El registro contendrá información sobre los beneficiarios finales conforme al artículo 4° bis de la Ley 25.246, considerando un umbral del 10% de participación o derechos de voto. Este umbral no aplicará a entidades extranjeras que no ofrezcan públicamente sus títulos valores.

22. Suecia

En Suecia, el régimen aplicable en materia de registros de beneficiarios finales se basa en la Ley de Blanqueo de Capitales y Financiación del Terrorismo (Lag om åtgärder mot penningtvätt och finansiering av terrorism, 2017:630) y la Ley del Registro de Beneficiarios Finales (Lag om registrering av verkliga huvudmän, 2017:631). Estas leyes implementan las directivas de la Unión Europea sobre la prevención del lavado de dinero y la financiación del terrorismo.

La Ley de Blanqueo de Capitales y Financiación del Terrorismo obliga a las entidades jurídicas a identificar y verificar la identidad de los beneficiarios finales. Además, la Ley del Registro de Beneficiarios Finales establece la obligación de registrar esta información en el Registro de Beneficiarios Finales. Este registro es obligatorio para todas las empresas y otras entidades legales establecidas en Suecia, incluyendo sociedades anónimas, sociedades de responsabilidad limitada, asociaciones, fundaciones y otros tipos de entidades.

Las entidades deben proporcionar información detallada sobre los beneficiarios finales, incluyendo nombre completo, fecha de nacimiento, nacionalidad y la naturaleza del control o participación. Esta información debe actualizarse regularmente y presentarse a la autoridad competente.

Autoridad responsable

La autoridad encargada de administrar y supervisar el Registro de Beneficiarios Finales en Suecia es la Agencia de Registro de Empresas (Bolagsverket). Bolagsverket es responsable de recibir, verificar y mantener la información de los beneficiarios finales. Las entidades jurídicas deben presentar la información requerida a través del portal en línea de Bolagsverket. Bolagsverket también colabora con otras autoridades suecas, como la Autoridad de Supervisión Financiera de Suecia (Finansinspektionen) y la Agencia Sueca contra el Crimen Económico (Ekobrottsmyndigheten), para asegurar el cumplimiento de las normativas y facilitar la lucha contra el lavado de dinero y la financiación del terrorismo.

Bolagsverket

Aspectos tecnológicos

Suecia ha implementado un sistema tecnológico para la gestión del Registro de Beneficiarios Finales. Las entidades pueden registrar y actualizar la información de manera electrónica a través del portal en línea de Bolagsverket. Este sistema digital permite que la información esté disponible para las autoridades pertinentes en tiempo real.

Accesibilidad

La información sobre los beneficiarios finales registrada en Bolagsverket no está disponible para el público en general. Sin embargo, ciertas autoridades competentes, como la policía, la fiscalía y otras agencias gubernamentales encargadas de la prevención y combate del lavado de dinero y la financiación del terrorismo, tienen acceso a esta información. Bolagsverket también puede compartir la información con otras autoridades reguladoras y de supervisión a nivel nacional e internacional, en el marco de acuerdos de cooperación y asistencia mutua.

Modificaciones Recientes

La Ley de Registro de Beneficiarios Finales ha sido enmendada, con la última modificación significativa entrando en vigor el 1 de enero de 2023, según la SFS 2022:1539. Esta modificación incluye ajustes en las obligaciones de notificación y registro, así como cambios en los requisitos de documentación y el proceso de actualización de la información sobre los beneficiarios finales. Las modificaciones refuerzan la necesidad de que las entidades mantengan la información actualizada y precisa, y facilitan la cooperación y el intercambio de información con otras autoridades y organizaciones nacionales e internacionales.

23. Tailandia

La Ley de Prevención y Supresión del Lavado de Dinero de 1999 establece las bases legales para la identificación de beneficiarios finales en Tailandia. En 2021, se introdujeron nuevas regulaciones para reforzar la obligación de registrar a los beneficiarios finales. Estas regulaciones requieren que todas las entidades legales, incluidas las sociedades anónimas, sociedades de responsabilidad limitada, fundaciones y asociaciones, identifiquen y registren a sus beneficiarios finales. La normativa específica de 2021 se centra en asegurar que las entidades recopilen y mantengan información precisa y actualizada sobre sus beneficiarios finales, incluyendo el nombre completo, la nacionalidad, la fecha de nacimiento y la naturaleza y extensión del interés de propiedad o control que ejercen sobre la entidad.

Ello no obstante, Tailandia no cuenta actualmente con un registro operativo de beneficiarios finales. Aunque ha habido iniciativas y esfuerzos para aumentar la transparencia en la propiedad real, Tailandia aún no ha implementado un sistema público o privado que cumpla con los criterios necesarios para un registro funcional de beneficiarios finales.

24. Polonia

Centralny Rejestr Beneficjentów Rzeczywistych (CRBR)

Polonia cuenta con un Registro Central de Beneficiarios Finales (Centralny Rejestr Beneficjentów Rzeczywistych, CRBR) plenamente operativo. La regulación del CRBR se contiene en la Ley de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo de 1 de marzo de 2018, que implementa las directivas europeas sobre la prevención del lavado de dinero y la financiación del terrorismo.

La Ley de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo establece que todas las entidades jurídicas, incluidas las sociedades de responsabilidad limitada, sociedades anónimas y otras entidades legales, deben identificar a sus beneficiarios finales y registrar esta información en el CRBR. Esta obligación se extiende también a las entidades extranjeras que operan en Polonia. Las entidades deben proporcionar información detallada sobre los beneficiarios finales, como el nombre completo, la nacionalidad, la fecha de nacimiento, el número de identificación y la naturaleza y el

alcance del control o la propiedad ejercidos. Esta información debe ser actualizada periódicamente y reportada al CRBR dentro de los siete días hábiles posteriores a cualquier cambio relevante.

Autoridad responsable

El Ministerio de Finanzas de Polonia es el órgano principal responsable de la supervisión y administración del CRBR. Este registro recoge y almacena la información de los beneficiarios finales, asegurando que esté disponible para las autoridades competentes y otros interesados legítimos. El registro se organiza de manera que las entidades puedan presentar y actualizar la información de los beneficiarios finales a través de un portal en línea gestionado por el Ministerio de Finanzas, facilitando el cumplimiento de las obligaciones legales y mejorando la accesibilidad y eficiencia de los datos.

Aspectos tecnológicos

Polonia ha implementado un sistema tecnológico para la gestión del CRBR. El registro es completamente electrónico y permite a las entidades reportar y actualizar la información de manera segura y eficiente. La plataforma digital del CRBR está diseñada para garantizar la protección de los datos sensibles mediante el uso de medidas de seguridad robustas, incluyendo el cifrado de datos y el control de acceso. Además, permite una integración fluida con otros registros y bases de datos gubernamentales, facilitando el intercambio de información y la colaboración entre diferentes agencias.

Accesibilidad

Debido a la decisión del Tribunal de Justicia de la Unión Europea (TJUE) de 22 de noviembre de 2022, el acceso a la información sobre beneficiarios reales ha sido restringido. En la actualidad, solo las autoridades competentes y los profesionales sujetos a obligaciones de lucha contra el lavado de dinero y la financiación del terrorismo pueden acceder a la información contenida en el CRBR, no estando disponible para el público en general.

25. Bélgica

En Bélgica, el régimen aplicable en materia de registros de beneficiarios finales está regulado principalmente por la Ley de 18 de septiembre de 2017 sobre la Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo y la Limitación del Uso del Dinero en Efectivo. Esta ley, junto con su Real Decreto de 30 de julio de 2018, obligan a las entidades legales, incluidas las sociedades anónimas, las sociedades de responsabilidad limitada, las fundaciones y las asociaciones sin fines de lucro, a identificar y registrar a sus beneficiarios finales en el Registro UBO (Ultimate Beneficial Owner). Este registro fue creado como parte de los esfuerzos de Bélgica para cumplir con las directivas europeas.

Autoridad responsable

El Registro UBO en Bélgica es gestionado por el Servicio Público Federal de Finanzas (SPF Finanzas). El SPF Finanzas es responsable de la recopilación, verificación y mantenimiento de la información sobre los beneficiarios finales. Las entidades legales están obligadas a presentar la información requerida a través de una plataforma en línea administrada por el SPF Finanzas. El registro debe contener información detallada sobre los beneficiarios finales, incluyendo el nombre completo, la fecha de

UBO-Register

nacimiento, la nacionalidad, la dirección y la naturaleza y el alcance del interés de propiedad o control. Las entidades deben actualizar esta información anualmente o cuando haya cambios significativos en la estructura de propiedad.

Aspectos tecnológicos

Bélgica ha implementado un sistema tecnológico para la gestión del Registro UBO. Las entidades pueden registrar y actualizar la información de manera electrónica a través de la plataforma digital del SPF Finanzas. Este sistema digital está diseñado para ser seguro, eficiente y fácil de usar, asegurando que la información sea precisa y esté disponible en tiempo real para las autoridades competentes. El sistema utiliza tecnologías avanzadas de seguridad de datos para proteger la información sensible contra accesos no autorizados y ciberamenazas. La integración con otros sistemas gubernamentales permite un intercambio fluido de información y facilita la supervisión y cumplimiento de las normativas.

Accesibilidad

Debido a la decisión del Tribunal de Justicia de la Unión Europea (TJUE) de 22 de noviembre de 2022, el acceso público general a la información sobre beneficiarios reales ha sido restringido. En la actualidad, solo las autoridades competentes y los profesionales sujetos a obligaciones de lucha contra el lavado de dinero y la financiación del terrorismo pueden acceder a la información en el Registro UBO, mientras que ciertas partes de la información pueden ser accesibles para individuos con un interés legítimo, como periodistas o investigadores en casos específicos. Este acceso restringido asegura que las autoridades puedan llevar a cabo investigaciones y supervisiones efectivas sin comprometer la privacidad de los datos personales. Además, el SPF Finanzas colabora con organismos internacionales y puede compartir información sobre beneficiarios finales en el marco de acuerdos de cooperación y asistencia mutua.

26. Noruega

En Noruega, el régimen aplicable en materia de registros de beneficiarios finales está regulado principalmente por la Ley de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo (Lov om tiltak mot hvitvasking og terrorfinansiering) y las directrices del Registro de Entidades (Enhetsregisteret).

La Ley de Prevención del Blanqueo de Capitales, que entró en vigor el 15 de octubre de 2018, obliga a todas las entidades legales en Noruega a identificar y registrar a sus beneficiarios finales. Este requisito se aplica a una amplia gama de entidades, incluidas sociedades anónimas, sociedades de responsabilidad limitada, asociaciones, fundaciones y otras estructuras legales.

La normativa exige que las entidades recopilen información detallada sobre sus beneficiarios finales, incluyendo nombre completo, fecha de nacimiento, nacionalidad y la naturaleza y el alcance del control ejercido sobre la entidad. Esta información debe ser reportada y mantenida actualizada en el Registro Central de Beneficiarios Finales (Register over reelle rettighetshavere).

Register over reelle rettighetshavere

Autoridad responsable

El Registro Central de Beneficiarios Finales es gestionado por el Registro de Entidades, que es parte de la Brønnøysundregistrene, la agencia responsable de varios registros nacionales en Noruega. Las entidades están obligadas a proporcionar la información requerida a través del sistema digital del Registro de Entidades, lo que facilita la recopilación y el mantenimiento de los datos.

El Registro de Entidades verifica la información proporcionada y asegura que esté disponible para las autoridades competentes. La Dirección de Impuestos de Noruega (Skatteetaten) y la Autoridad de Supervisión Financiera de Noruega (Finanstilsynet) también juegan roles cruciales en la supervisión y el cumplimiento de estas normativas.

Aspectos tecnológicos

Noruega ha implementado un sistema tecnológico para la gestión del Registro Central de Beneficiarios Finales. El sistema es completamente digital y permite a las entidades registrar y actualizar la información de manera electrónica a través del portal en línea del Registro de Entidades. Este enfoque digital tiene por finalidad facilitar que la información sea precisa, segura y accesible en tiempo real para las autoridades pertinentes.

El uso de tecnologías avanzadas, como la autenticación en línea (2FA) y el cifrado de datos (TLS), asegura que la información sensible esté protegida contra accesos no autorizados y ciberamenazas. Además, la integración con otros sistemas gubernamentales permite un intercambio eficiente de información y una mejor supervisión.

Accesibilidad

La información sobre los beneficiarios finales registrada en el Registro Central de Beneficiarios Finales no está disponible para el público general, en línea con las normativas de protección de datos personales. Sin embargo, esta información es accesible para las autoridades competentes, incluyendo la Dirección de Impuestos, la Autoridad de Supervisión Financiera y otras agencias encargadas de la prevención y combate del blanqueo de capitales y la financiación del terrorismo.

El acceso restringido a la información permite que las autoridades realicen investigaciones y supervisiones efectivas sin comprometer la privacidad de los individuos. Además, Noruega coopera con organismos internacionales y puede compartir información sobre beneficiarios finales en el marco de acuerdos de cooperación y asistencia mutua.

27. Austria

En Austria, el régimen aplicable en materia de registros de beneficiarios finales está regulado principalmente por la Ley de Beneficiarios Finales (Wirtschaftliche Eigentümer Registergesetz, WiEReG), que se implementó para cumplir con las directivas de la Unión Europea sobre la prevención del blanqueo de capitales y la financiación del terrorismo (AMLD4 y AMLD5).

La Ley de Beneficiarios Finales (WiEReG), que entró en vigor en enero de 2018, obliga a todas las entidades jurídicas y fideicomisos a registrar información detallada sobre sus beneficiarios finales. Esta normativa tiene como objetivo aumentar la transparencia en la propiedad de las entidades y facilitar la lucha contra el blanqueo de activos y el financiamiento del terrorismo. La ley exige que las entidades proporcionen datos personales completos de los beneficiarios finales, incluyendo nombre completo,

fecha de nacimiento, nacionalidad, domicilio, y la naturaleza y extensión del interés de propiedad o control. Esta información debe ser actualizada anualmente y siempre que se produzcan cambios significativos.

Actualizaciones Recientes (2023-2024)

La WiEReG-Novelle 2023 ha introducido varios cambios importantes:

Acceso al registro: Se permite el acceso al registro a individuos y organizaciones con un interés legítimo, mediante un proceso de solicitud electrónico. Profesionales como asesores fiscales, auditores, abogados y notarios pueden acceder en nombre de sus clientes si demuestran un interés legítimo, como en el caso de transacciones inmobiliarias.

Colaboración entre autoridades: La colaboración entre la autoridad del registro y otras entidades nacionales e internacionales ha sido mejorada. Las autoridades como la Oficina de Lavado de Dinero (Geldwäschemeldestelle), la Cámara de Comercio (WKO), y la Autoridad de Supervisión Financiera (FMA) pueden intercambiar datos y documentos para evaluar la propiedad económica en casos de delitos financieros.

Actualización automática y abastecimiento de datos: A partir del 12 de diciembre de 2023, el registro se actualizará automáticamente con listas de sanciones, permitiendo una detección más rápida y eficiente de coincidencias con registros de sanciones.

Requerimientos adicionales de información: Desde el 1 de julio de 2024, se ha ampliado la obligación de reporte de datos, especialmente en relación con fideicomisos, fundaciones y otras estructuras fiduciarias. Además, las autoridades fiscales pueden acceder a ciertos datos del registro para realizar análisis basados en modelos para identificar empresas ficticias y directores no declarados.

Autoridad responsable

El registro de beneficiarios finales en Austria está gestionado por el Ministerio de Finanzas, a través del Registro de Beneficiarios Finales (Register der wirtschaftlichen Eigentümer). Las entidades jurídicas deben presentar la información requerida utilizando el sistema de registro en línea proporcionado por el ministerio. El Ministerio de Finanzas tiene la responsabilidad de supervisar el cumplimiento de la WiEReG y de garantizar que la información registrada sea precisa y esté actualizada. Para ello, el ministerio realiza auditorías y puede imponer sanciones a las entidades que no cumplan con sus obligaciones de registro.

Register der wirtschaftlichen Eigentümer

Aspectos tecnológicos

Austria ha implementado una plataforma tecnológica para la gestión del Registro de Beneficiarios Finales. Este sistema permite a las entidades registrar y actualizar la información de manera electrónica a través de un portal en línea seguro. La plataforma está diseñada para facilitar el acceso y la gestión de los datos, asegurando la precisión y la seguridad de la información sensible. El sistema utiliza tecnologías de autenticación y cifrado para proteger los datos contra accesos no autorizados y garantizar la integridad de la información. La plataforma también está integrada con otros sistemas gubernamentales.

Accesibilidad

La información sobre los beneficiarios finales registrada en el Registro de Beneficiarios Finales no está disponible al público general, en consonancia con las normativas de protección de datos personales. Sin embargo, esta información es accesible para las autoridades competentes, incluyendo la policía, las autoridades fiscales y otras agencias reguladoras, que la utilizan para prevenir y combatir el blanqueo de capitales y la financiación del terrorismo. Además, Austria coopera con organismos internacionales y puede compartir información sobre beneficiarios finales en el marco de acuerdos de cooperación y asistencia mutua.

28. Emiratos Árabes Unidos

Los Emiratos Árabes Unidos (EAU) han modificado significativamente su régimen de registro de beneficiarios finales para alinearse con la normativa internacional sobre transparencia y prevención del lavado de activos y el financiamiento del terrorismo. Los cambios recientes se implementaron a través de la Resolución del Gabinete No. 109 de 2023 y la Decisión del Gabinete No. 132 de 2023 que obligan a todas las entidades legales registradas en los EAU a identificar y registrar a sus beneficiarios finales. Esta normativa se aplica tanto a las empresas establecidas en zonas francas comerciales como en tierra firme, excluyendo únicamente a las entidades propiedad del gobierno federal o local y aquellas ubicadas en las zonas francas financieras específicas como el Centro Financiero Internacional de Dubái (DIFC) y el Mercado Global de Abu Dhabi (ADGM).

Autoridad responsable

El Ministerio de Economía de los Emiratos Árabes Unidos es la autoridad principal responsable de la supervisión y el cumplimiento de la normativa sobre beneficiarios finales. Las entidades legales deben proporcionar la información requerida a través de un sistema centralizado administrado por el Ministerio de Economía. Sin embargo, cada emirato tiene la responsabilidad de implementar y supervisar el cumplimiento de estas normativas a nivel local. Los registros pertinentes en cada emirato están integrados en una plataforma nacional que permite la recopilación y el acceso a la información de beneficiarios finales en todo el país.

Las empresas deben presentar un informe detallado sobre sus beneficiarios finales, el cual debe ser actualizado anualmente o cuando ocurran cambios significativos. La Decisión del Gabinete No. 132 de 2023 introduce multas específicas por no revelar las capas de propiedad en estructuras complejas y la posibilidad de suspensión temporal de licencias comerciales o cierre de entidades para violaciones repetidas.

Aspectos tecnológicos

Los EAU han implementado plataformas tecnológicas para facilitar la recopilación, el registro y la actualización de la información sobre los beneficiarios finales. Las entidades pueden utilizar sistemas en línea proporcionados por las autoridades locales de cada emirato para registrar y actualizar la información requerida. Estas plataformas están diseñadas para garantizar la seguridad y la protección de los datos sensibles, utilizando tecnologías de cifrado y autenticación para prevenir accesos no autorizados.

Accesibilidad

La información registrada sobre los beneficiarios finales no está disponible para el público general. Sin embargo, esta información es accesible para las autoridades competentes, incluyendo agencias reguladoras y de aplicación de la ley, tanto a nivel federal como local. Los Emiratos Árabes Unidos pueden compartir información sobre beneficiarios finales con Estados terceros en el marco de acuerdos de cooperación y asistencia mutua.

29. Hong Kong

En Hong Kong, el régimen aplicable en materia de registros de beneficiarios finales está regulado principalmente por la Ordenanza de Sociedades (Companies Ordinance, Cap. 622) enmendada en 2018. El sistema vigente se basa en registros a nivel de empresa, no existiendo un registro central de beneficiarios efectivos.

Desde el 1 de marzo de 2018, todas las empresas registradas en Hong Kong (excepto las empresas cotizadas en bolsa) están obligadas a mantener un registro significativo de control (Significant Controllers Register, SCR). La SCR debe contener información sobre las personas que tienen control significativo sobre la empresa. Esta obligación se aplica tanto a las sociedades privadas como a las públicas no cotizadas. Las empresas deben identificar a las personas que tienen control significativo y registrar información como el nombre completo, la dirección, la fecha de nacimiento, la nacionalidad, y la naturaleza y extensión del control. Esta información debe mantenerse actualizada y estar disponible para inspección por las autoridades competentes.

Autoridad responsable

La responsabilidad principal del cumplimiento y supervisión del régimen de registros de beneficiarios finales en Hong Kong recae en el Registro de Empresas (Companies Registry). Sin embargo, es importante señalar que cada empresa es responsable de mantener su propio SCR. Las empresas deben mantener el SCR en su lugar de negocios registrado en Hong Kong o en otro lugar designado en la ciudad. El Registro de Empresas tiene la facultad de inspeccionar el SCR durante las auditorías y puede imponer sanciones a las empresas que no cumplan con los requisitos de registro. Además, las empresas deben designar a una persona responsable, que puede ser un director, un empleado de la empresa o una entidad externa, para proporcionar asistencia a las autoridades en relación con el SCR.

Aspectos tecnológicos

Hong Kong ha implementado una infraestructura tecnológica que facilita la gestión del SCR. Aunque la información no se presenta electrónicamente al Registro de Empresas, las empresas deben mantener los datos en formato electrónico o físico en su lugar de negocios registrado. El sistema interno de cada empresa debe garantizar que la información sea precisa y esté protegida contra accesos no autorizados.

Accesibilidad

La información contenida en el SCR no está disponible para público general. Sin embargo, es accesible para las autoridades competentes, como la Policía de Hong Kong y la Oficina de Servicios Financieros y del Tesoro, que pueden inspeccionar los registros como parte de sus funciones de supervisión y cumplimiento.

Las autoridades pueden solicitar acceso al SCR para investigar posibles actividades de lavado de dinero y financiación del terrorismo, garantizando así que la información sea utilizada efectivamente en la lucha contra las actividades ilícitas.

30. Singapur

En Singapur, el régimen aplicable en materia de registros de beneficiarios finales está regulado principalmente por la Ley de Sociedades (Companies Act) y la Ley de Sociedades de Responsabilidad Limitada (Limited Liability Partnerships Act). Cada empresa y sociedad de responsabilidad limitada (LLP) está obligada a mantener su propio registro con información detallada sobre las personas o entidades que tienen control significativo, no existiendo un registro central accesible al público.

Desde el 31 de marzo de 2017, las empresas constituidas en Singapur y las sociedades de responsabilidad limitada deben mantener un Registro de Beneficiarios Finales (Register of Registrable Controllers, RORC). Este requisito también se aplica a entidades extranjeras que operan en Singapur. La obligación incluye identificar a los beneficiarios finales y mantener un registro actualizado de esta información.

La información que debe ser registrada incluye detalles personales del beneficiario final, como el nombre completo, la nacionalidad, la dirección de residencia, la fecha de nacimiento, y la naturaleza y extensión del control o interés de propiedad. Las entidades deben actualizar este registro dentro de los dos días hábiles siguientes a cualquier cambio en la información.

Autoridad responsable

La Autoridad Contable y Corporativa de Singapur (Accounting and Corporate Regulatory Authority, ACRA) es el organismo encargado de la supervisión y el cumplimiento de las normativas relacionadas con el registro de beneficiarios finales. ACRA proporciona directrices detalladas sobre cómo mantener el RORC.

Las entidades deben mantener el RORC en su lugar de negocios registrado o en otro lugar especificado en Singapur. Este registro no se presenta a ACRA, pero debe estar disponible para inspección por las autoridades competentes cuando sea necesario.

Aspectos tecnológicos

Singapur ha implementado una infraestructura tecnológica para facilitar la gestión del registro de beneficiarios finales. ACRA proporciona una plataforma en línea para la presentación y actualización de información corporativa, aunque el RORC específico se mantiene internamente dentro de las entidades.

Accesibilidad

La información contenida en el RORC no puede ser obtenida por el público general para proteger la privacidad de los individuos. Por el contrario, la información es accesible para las autoridades competentes, incluyendo ACRA, la policía, y otras agencias gubernamentales que participan en la prevención y combate del lavado de dinero y la financiación del terrorismo.

Las autoridades pueden solicitar acceso al RORC durante inspecciones o investigaciones, garantizando que la información esté disponible para fines de cumplimiento y supervisión. Además, Singapur puede colaborar con organismos internacionales y compartir información sobre beneficiarios finales en el marco de acuerdos de cooperación y asistencia mutua.

Actualizaciones Recientes

La Ley de Registros Corporativos de 2022 introdujo cambios importantes para mejorar la transparencia, incluyendo la obligación de mantener un registro no público de accionistas nominales y la obligación de las empresas y LLPs de identificar y registrar a los individuos con control ejecutivo si no pueden identificar a los controladores significativos. Estas enmiendas entraron en vigor en 2023.

III. Líneas estratégicas para el establecimiento de un registro de beneficiarios finales

Con fundamento en el análisis de la situación de las treinta jurisdicciones más significativas, expondremos a continuación una serie de líneas estratégicas a considerar en el establecimiento de un registro de beneficiarios finales, examinando las implicaciones derivadas de la elección de la autoridad o agencia responsable de la gestión, el aseguramiento de la calidad de los datos a través de controles previos, como el uso de formularios estandarizados y campos obligatorios, la implantación de controles internos para identificar y corregir posibles inconsistencias o errores en los registros, y la verificación automatizada con otras bases de datos gubernamentales, la determinación del modelo de gestión de datos, examinando específicamente la opción entre sistemas propietarios y estándares abiertos, el régimen de acceso a los datos registrales y los costes asociados de implementación y operación del registro.

1. Aspectos organizativos

1.1. Agencia responsable

La determinación de la autoridad o agencia responsable de la gestión del registro de beneficiarios finales constituye una decisión fundamental en la medida en que determina importantes aspectos legales y organizativos.

Agencia responsable

El análisis de los treinta países más significativos pone de manifiesto una gran variabilidad en las autoridades o agencias encargadas legalmente de la llevanza de los registros de beneficiarios finales. Aunque algunas jurisdicciones importantes, como los Estados Unidos, han optado por su unidad de inteligencia financiera (FinCEN), la opción más frecuente ha sido atribuir la competencia a los registros mercantiles o de sociedades: es el caso del Reino Unido (Companies House), Francia (Registre du Commerce et des Sociétés), Italia (Registro delle Imprese) o los Países Bajos (Kamer van Koophandel, KvK).

Registros Mercantiles

Atribuir el registro de beneficiarios finales a los registros mercantiles tiene tanto ventajas como desventajas que deben ser consideradas detenidamente. Entre los argumentos a favor se encuentra la centralización y eficiencia en la recopilación y acceso a los datos, lo que facilita el trabajo de las autoridades fiscales, financieras y de cumplimiento de la ley. Además, los registros mercantiles suelen ser accesibles al público, incrementando la transparencia y permitiendo que cualquier persona pueda verificar quiénes son los beneficiarios finales de una empresa, lo cual ayuda a combatir el lavado de activos, la evasión fiscal y la corrupción. También se mejora la reputación y confianza en el entorno empresarial, atrayendo a los inversores y beneficiando a las empresas. La simplificación administrativa es otro punto a favor, ya que las empresas solo tienen que proporcionar la información a una entidad en lugar de múltiples organismos.

Sin embargo, hay argumentos en contra que deben ser considerados. Los registros mercantiles pueden no tener la capacidad ni los recursos adecuados para manejar esta responsabilidad adicional, lo que podría resultar en una gestión ineficiente y en posibles errores en la recopilación y verificación de la información. Además, la publicación de los datos de beneficiarios finales podría comprometer la privacidad y seguridad de los individuos, especialmente en países donde la divulgación de tal información podría poner a las personas en riesgo de acoso, extorsión o violencia. Mantener la

información actualizada es otro desafío, ya que las empresas pueden ser reticentes a proporcionar datos precisos o pueden tardar en actualizar la información sobre sus beneficiarios finales, lo que puede llevar a registros obsoletos o incorrectos.

En el caso de Chile, como se ha señalado anteriormente, el artículo 1 del proyecto de ley dispone que "El Registro será elaborado y administrado por el Servicio de Impuestos Internos, el que deberá velar por la integridad, disponibilidad y precisión de la información contenida en él, declarada por los obligados a informar, debiendo para ello actualizarse oportunamente." El mensaje no justifica esta opción regulatoria más allá de indicar que "Tal como ocurre en la generalidad de los países en que se ha regulado un registro de beneficiarios finales, se ha optado por entregar a la autoridad tributaria la administración del registro y su fiscalización". Lo cierto es que la atribución de la gestión del registro a la autoridad fiscal, aunque no puede calificarse de anómala, está lejos de ser la opción más común: el análisis de las 30 jurisdicciones pone de manifiesto que esta decisión de política legislativa se habría adoptado en cuatro países: Argentina (AFIP/ARCA), Brasil (Receita Federal, RFB), Turquía (Gelir İdaresi Başkanlığı, GIB) y Bélgica (Service Public Fédéral Finances / Federale Overheidsdienst Financiën).

Autoridades Fiscales

La atribución del registro de beneficiarios finales a las autoridades fiscales presenta claras ventajas. Dado que estas autoridades ya manejan datos económicos de los contribuyentes, integrar el registro de beneficiarios finales permite un análisis cruzado más completo, facilitando la identificación de inconsistencias, patrones de riesgo y posibles casos de evasión fiscal o lavado de dinero. Esta integración facilita optimizar recursos, potenciar las capacidades analíticas del Estado y mejorar la recaudación fiscal al desenmascarar estructuras corporativas opacas que buscan ocultar ingresos o activos mediante prácticas fiscales agresivas. Además, contribuye significativamente a la prevención del lavado de dinero y la financiación del terrorismo, ya que la administración tributaria puede identificar señales de alerta y mitigar riesgos con mayor eficacia. La centralización también evita la duplicación de esfuerzos entre distintas entidades, como registros mercantiles o bancos centrales, reduciendo costos administrativos y mejorando la coordinación gubernamental. Asimismo, la experiencia tecnológica y los recursos avanzados de que disponen estas administraciones garantizan el manejo seguro y eficiente de grandes volúmenes de datos, minimizando riesgos de filtraciones y asegurando un equilibrio entre transparencia y privacidad. Por último, la capacidad de cruzar información en tiempo real con registros fiscales, propiedades y transacciones financieras fortalece la verificación y fiscalización, permitiendo a las autoridades detectar irregularidades y tomar medidas correctivas de manera más ágil y precisa.

Ello no obstante, esta opción regulatoria requiere una política de comunicación clara en la medida en que la centralización de la información en la autoridad tributaria podría percibirse como un control adicional de naturaleza fiscal, lo que podría afectar negativamente el ambiente de negocios y la inversión extranjera. También puede suscitarse la preocupación de que las autoridades fiscales puedan utilizar esta información de manera excesiva o indebida, más allá de los propósitos de transparencia, lo que podría generar desconfianza entre los empresarios y el público en general.

Campaña de divulgación

Consecuentemente, sería muy recomendable que la puesta en funcionamiento en Chile del Registro Nacional de Personas Beneficiarias Finales (RNPBF) fuera acompañada de una campaña de divulgación pública exhaustiva y bien planificada. Esta campaña debería centrarse en comunicar los beneficios clave del registro, poniendo un énfasis particular en aquellos aspectos que son percibidos socialmente

como positivos. Entre estos beneficios, se destacaría la capacidad del RNPBF para prevenir el lavado de activos, una problemática que puede afectar gravemente a la economía y la seguridad del país. Además, se subrayaría cómo el registro contribuye al incremento de la transparencia en las operaciones comerciales y financieras, generando un entorno más confiable para los negocios y los inversionistas.

La lucha contra la corrupción es otro aspecto crucial que debe ser resaltado en esta campaña de divulgación. Es fundamental que la ciudadanía comprenda que el RNPBF es una herramienta poderosa para identificar y desmantelar estructuras corruptas, promoviendo así un sistema económico más justo y equitativo. De igual manera, es vital destacar el impacto del registro en la lucha contra el crimen organizado. El mensaje del proyecto de ley enfatiza que "este proyecto de ley permitirá debilitar el poder financiero o económico de las bandas organizadas, trazando la ruta del dinero respecto de delitos como el contrabando, el narcotráfico, la trata de personas, el tráfico ilícito de migrantes, la ciberdelincuencia, el robo de madera, el robo organizado de vehículos motorizados y otros ilícitos relacionados con delitos medioambientales, como son la minería ilegal, la pesca ilegal y el robo de cobre." Al comunicar claramente cómo el RNPBF ayudará a combatir el crimen organizado en todas estas áreas, se puede resaltar aún más su importancia y beneficio para la sociedad.

La campaña debería utilizar diversos medios de comunicación, incluyendo redes sociales, medios tradicionales como la televisión y la radio, y eventos comunitarios, para asegurar que el mensaje llegue a todos los sectores de la sociedad. Además, sería beneficioso involucrar a organizaciones civiles y expertos en la materia para que actúen como voceros y validadores del proceso.

Al hacer hincapié en estos puntos, se podría fomentar una mayor aceptación y apoyo de la iniciativa por parte del público, lo cual es crucial para el éxito y la efectividad del RNPBF. La transparencia, la prevención del crimen financiero, la lucha contra la corrupción y el poder financiero de las bandas organizadas no solo son beneficios para el gobierno, sino también para la sociedad en su conjunto, ya que contribuyen a la creación de un entorno económico más seguro y próspero para todos.

Gobernanza

Otro aspecto que sería conveniente subrayar es la existencia de un régimen de gobernanza orientado a evitar un uso indebido o excesivo de la información. En este contexto, debe valorarse muy positivamente que el proyecto de ley prevea procedimientos de control específicos centrados en el Consejo Consultivo, formado por consejeros representantes de distintos órganos del Estado, que brindará apoyo para monitorear el correcto funcionamiento del registro. El reglamento previsto en el proyecto de ley debería dotar de poderes amplios de monitoreo y control al Consejo Consultivo, permitiéndole supervisar de manera efectiva la aplicación correcta de las normativas y garantizar la protección de los datos sensibles de los beneficiarios finales. Este mecanismo institucional es una especialidad del sistema chileno y debería ponerse en valor en la campaña institucional de divulgación con objeto de disipar posibles preocupaciones del público respecto del uso del registro.

Protección de datos

Además, es importante destacar que el Consejo Consultivo no solo supervisará la aplicación correcta de las normativas, sino que también se encargará de garantizar la protección de los datos sensibles de los beneficiarios finales. Este enfoque holístico en la gobernanza asegura que la información recopilada se utilice exclusivamente para los fines establecidos por la ley, minimizando así el riesgo de abuso o mal uso de la misma. La transparencia en los procesos del Consejo Consultivo y la rendición de cuentas

periódica al público y a otras instituciones del Estado fortalecerán la confianza en el sistema y en la eficacia del RNPBF.

La campaña de divulgación debe incluir detalles sobre cómo estos controles internos y externos están diseñados para proteger los derechos de los individuos y para garantizar que el registro funcione dentro de un marco ético y legal estricto. Explicar de manera clara y accesible la composición, las responsabilidades y las acciones del Consejo Consultivo permitirá a la ciudadanía entender mejor el alcance de las medidas de protección y control. Esto contribuirá significativamente a reducir las preocupaciones sobre la privacidad y el posible uso indebido de la información.

Finalmente, se debería enfatizar que este régimen de gobernanza no solo protege a los individuos, sino que también fortalece la legitimidad del RNPBF. Al contar con un sistema robusto de supervisión y control, Chile demuestra su compromiso con la transparencia en el manejo de datos sensibles, lo que puede servir de modelo para otros países. La confianza pública en el registro es esencial para su éxito, y un régimen de gobernanza bien comunicado y comprendido es clave para lograr esta confianza. Por lo tanto, la campaña institucional de divulgación debe destacar este aspecto como un pilar fundamental del proyecto, asegurando que el público esté plenamente informado y confiado en la integridad del sistema.

1.2. Implementación gradual de la legislación

Implementación gradual

La implementación del registro de beneficiarios finales ha sido gradual en varias jurisdicciones. Un ejemplo notable es el Reino Unido, que introdujo el registro de Personas con Control Significativo (PSC) en 2016 como parte de sus esfuerzos para aumentar la transparencia en la propiedad de las empresas y combatir el lavado de dinero y la evasión fiscal. El Reino Unido sentó inicialmente las bases para el registro de PSC a través de la Ley de Pequeños Negocios, Empresa y Empleo de 2015, que requería que las empresas identificaran y registraran a las personas que tuvieran un control significativo sobre ellas. La obligación de mantener un registro de PSC entró en vigor para las empresas del Reino Unido y las Sociedades de Responsabilidad Limitada (LLPs) el 6 de abril de 2016, y estas entidades tuvieron que comenzar a llevar un registro de PSC y proporcionar la información a Companies House a partir del 30 de junio de 2016. Esta naturaleza gradual de la implementación permitió que las empresas tuvieran tiempo para entender y cumplir con los nuevos requisitos. Con el tiempo, el alcance del registro de PSC se ha ampliado para incluir Sociedades Limitadas Escocesas (SLPs) y ciertas otras entidades. Además, ha habido esfuerzos continuos para refinar y hacer cumplir las regulaciones, como medidas para garantizar la precisión de la información proporcionada y sanciones por incumplimiento. Otras jurisdicciones también han adoptado un enfoque gradual para implementar registros de propiedad beneficiaria, a menudo comenzando con sectores específicos o tipos de entidades y ampliando los requisitos con el tiempo. Este enfoque por fases ayuda a abordar desafíos prácticos, como asegurar que las empresas entiendan sus obligaciones y permitir que los organismos reguladores desarrollen la infraestructura necesaria para gestionar y hacer cumplir el registro de manera efectiva.

1.3. Potestades para asegurar el cumplimiento. Aplicación de sanciones

Requerimientos

Las legislaciones reguladoras de los registros de beneficiarios finales atribuyen a la autoridad responsable de su llevanza ciertas potestades para asegurar el cumplimiento de la obligación de declaración. Por ejemplo, en el Reino Unido, la Companies House tiene la capacidad de emitir requerimientos y cartas de advertencia a las empresas que no cumplan con la obligación de

proporcionar información precisa y actualizada sobre los beneficiarios finales. Estos mecanismos permiten a la autoridad recordar a las empresas sus obligaciones legales y ofrecerles la oportunidad de rectificar cualquier incumplimiento antes de que se adopten medidas más severas. De manera similar, en Estados Unidos, la Financial Crimes Enforcement Network (FinCEN) puede emitir avisos y requerimientos a las empresas que no cumplan con las obligaciones establecidas por la Ley de Transparencia Corporativa (CTA).

Sanciones económicas

En casos más severos, pueden imponerse sanciones económicas. Por ejemplo, en el Reino Unido, las empresas que no cumplan con las obligaciones del registro de Personas con Control Significativo (PSC) pueden enfrentarse a multas significativas. En Estados Unidos, las sanciones por no cumplir con la CTA pueden incluir multas coercitivas diarias. En Alemania, la Ley de Lavado de Dinero (Geldwäschegesetz, GwG) establece que el incumplimiento de los requisitos de transparencia puede resultar en multas de hasta un millón de euros o el doble de la ventaja económica obtenida del incumplimiento.

Acciones penales

Finalmente, en los casos más graves, cabe la posibilidad de acciones penales. En el Reino Unido, tanto la empresa como sus directivos pueden ser procesados penalmente por incumplir intencionalmente las obligaciones del registro de PSC. Las sanciones penales pueden incluir multas sustanciales y penas de prisión de hasta dos años. En Estados Unidos, las sanciones penales bajo la CTA pueden incluir multas de hasta 10,000 dólares y penas de prisión de hasta dos años.

Eliminación del Registro

Un mecanismo muy potente para asegurar el cumplimiento es la posibilidad de eliminar a una empresa del registro. La Companies House en el Reino Unido tiene la autoridad para cancelar la inscripción de las empresas que no cumplan persistentemente con los requisitos del registro de PSC. En 2020, varias empresas fueron eliminadas del registro oficial por no presentar repetidamente la información requerida. Este procedimiento de cancelación registral no solo disuelve legalmente a la empresa, sino que también implica que sus activos pueden ser distribuidos según las leyes de insolvencia.

2. Implementación de controles previos

Formularios estandarizados

Implementar controles estrictos en el momento de la declaración al RNPBF puede simplificar significativamente el proceso de verificación posterior. Una de las herramientas primordiales para garantizar desde el inicio la precisión de los datos en un registro de beneficiarios finales es el uso de formularios estandarizados con campos obligatorios. Al diseñar formularios que requieran información específica, como nombres legales completos, direcciones, fechas de nacimiento y números de identificación, las autoridades pueden asegurarse de que todos los datos necesarios se recopilen de manera uniforme. Estos formularios deben incluir reglas de validación que impidan la presentación si los campos obligatorios están incompletos o mal formateados.

Validaciones técnicas

Las validaciones técnicas en los formularios electrónicos son fundamentales para asegurar la calidad de los datos desde el primer momento. Estas validaciones se implementan a través de varias técnicas:

Validación de formato

Validación de formato: Se asegura que los datos ingresados sigan un formato específico. Por ejemplo, los campos de fecha pueden estar configurados para aceptar solo fechas válidas en el formato DD/MM/AAAA. Esto se puede lograr utilizando expresiones regulares (regex) que definen los patrones permitidos. Si el formato ingresado no coincide con el patrón, el sistema rechaza la entrada y solicita al usuario que la corrija.

Validación de longitud y tipo de caracteres: Para campos como números de identificación, los formularios pueden verificar que los datos ingresados tengan la longitud correcta y contengan solo los tipos de caracteres permitidos (por ejemplo, solo dígitos). Esto también puede lograrse mediante expresiones regulares y scripts de validación que verifican estos parámetros antes de permitir que el formulario se envíe.

Validación de longitud y tipo de caracteres

Validación de campos obligatorios: Antes de que el formulario pueda ser enviado, el sistema verifica que todos los campos obligatorios estén completos. Esta validación se realiza mediante scripts que comprueban que ningún campo obligatorio esté vacío. Si algún campo requerido está incompleto, el sistema muestra un mensaje de error indicando qué información falta.

Validación de campos obligatorios

La implementación de estos formularios de manera electrónica con validaciones integradas puede reducir significativamente los errores de entrada de datos y las omisiones en el registro de beneficiarios finales. Esto incluye no solo las validaciones básicas de formato, sino también reglas más avanzadas de verificación de consistencia. Así, el formulario puede comprobar automáticamente si la dirección proporcionada corresponde a un formato postal válido o si el número de identificación coincide con los registros nacionales. Además, los formularios electrónicos pueden integrarse con bases de datos externas para la verificación en tiempo real. Por ejemplo, cuando se introduce un número de identificación, el sistema puede verificarlo instantáneamente contra una base de datos gubernamental para asegurar que el número es válido y está activo. Esta verificación en tiempo real no solo asegura que los datos ingresados sean precisos, sino que también agiliza el proceso de validación al reducir la necesidad de comprobaciones manuales posteriores.

Verificación de consistencia

Los formularios estandarizados también pueden incluir funcionalidades de ayuda en línea, como indicaciones y ejemplos para cada campo, para guiar a los usuarios en el proceso de llenado. Estas ayudas pueden reducir la tasa de errores y mejorar la calidad de los datos ingresados en el registro de beneficiarios finales. Además, los formularios pueden ser diseñados para ser intuitivos y fáciles de usar, con una interfaz clara que minimice la confusión y facilite la entrada correcta de datos.

Funcionalidades de ayuda en línea

Para garantizar que los formularios electrónicos funcionen de manera óptima, es crucial que el sistema cuente con un sólido mecanismo de manejo de errores. Esto incluye mensajes de error claros y específicos que informen a los usuarios sobre qué campos necesitan corrección y por qué. Por ejemplo, en lugar de un mensaje genérico como "Error en la entrada de datos", el sistema debería proporcionar mensajes como "El campo 'Fecha de nacimiento' debe seguir el formato DD/MM/AAAA".

Manejo de errores

Otro aspecto importante es la capacidad de los formularios para manejar casos especiales y excepciones. Por ejemplo, deben poder acomodar diferentes tipos de estructuras familiares y empresariales, nombres alternativos o alias, y direcciones internacionales, todo ello sin comprometer la precisión y la integridad de los datos.

Casos especiales y excepciones

Finalmente, la seguridad de los datos es una consideración crítica en un registro de beneficiarios finales. Los formularios electrónicos deben diseñarse con características de seguridad robustas, como el cifrado de datos en tránsito y en reposo, y controles de acceso estrictos para proteger la información sensible de accesos no autorizados. Esto no solo protege la privacidad de los individuos, sino que también fortalece la confianza en el sistema de registro de beneficiarios finales.

Seguridad de los datos

Por tanto, el uso de formularios estandarizados con campos obligatorios, validados electrónicamente y diseñados para ser intuitivos y seguros, es un componente esencial para garantizar la precisión y la integridad de los datos en los registros de beneficiarios finales. Al implementar estas prácticas, las autoridades pueden asegurarse de que se recopile y verifique información precisa desde el principio, reduciendo la necesidad de correcciones posteriores y mejorando la fiabilidad del registro de beneficiarios finales.

Métodos organizativos

Además de los formularios estandarizados, para asegurar la calidad de los datos incorporados, pueden utilizarse diversos métodos organizativos. En primer lugar, asegurar que todas las personas involucradas en el proceso de entrada y verificación de datos estén bien capacitadas es esencial. Las sesiones de capacitación regular sobre la precisión de los datos, los errores comunes y la importancia de la integridad de los datos pueden ayudar a mantener altos estándares. Además, la realización de auditorías regulares de los datos ingresados en el registro de beneficiarios finales puede ayudar a identificar y corregir cualquier discrepancia. Las auditorías pueden ser automatizadas o manuales, dependiendo de los recursos disponibles y el volumen de datos. Asimismo, establecer bucles de retroalimentación donde los usuarios puedan reportar problemas o discrepancias puede ayudar a mejorar el sistema de manera continua. Esta retroalimentación puede utilizarse para refinar las reglas de validación, mejorar las interfaces de usuario y mejorar la calidad general de los datos. Por último, proporcionar directrices y documentación claras para la presentación de datos puede ayudar a los usuarios a entender los requisitos y la importancia de los datos precisos. Esto incluye instrucciones paso a paso, preguntas frecuentes y canales de soporte para asistencia.

3. Implementación de controles internos

Implementación de controles internos

Implementar controles internos rigurosos es importante para garantizar la integridad de los datos de los beneficiarios finales. A través de una combinación de verificaciones automáticas, verificación independiente por terceros y análisis algorítmico avanzado, las autoridades encargadas del registro pueden asegurar que los datos de los beneficiarios finales sean precisos y confiables.

3.1. Controles internos basados en el riesgo

Controles internos basados en el riesgo

Una opción clave para mejorar la eficacia de los registros de beneficiarios finales es establecer controles internos basados en el riesgo, adaptados específicamente al nivel de riesgo asociado con diferentes entidades. Este enfoque permite a las autoridades centrarse en las áreas de mayor riesgo, optimizando el uso de los recursos y aumentando la probabilidad de detectar actividades ilícitas.

Evaluaciones de riesgo

Los controles internos basados en el riesgo comienzan con la realización de evaluaciones de riesgo periódicas. Estas evaluaciones implican un análisis exhaustivo de diversos factores que pueden influir en el riesgo de una entidad. Entre los factores analizados se incluyen el país de origen del beneficiario final, el sector económico en el que opera la entidad, su estructura de propiedad, el historial de transacciones y cualquier conexión con personas expuestas políticamente (PEP).

El país de origen del beneficiario final es un factor crucial porque ciertos países presentan mayores índices de corrupción, regulaciones financieras laxas o son conocidos por ser refugios para el lavado de dinero. Las entidades con beneficiarios finales provenientes de estos países deben ser automáticamente clasificadas con un riesgo mayor. De igual manera, el sector económico puede influir

en el nivel de riesgo, ya que algunos negocios, como la industria extractiva o los juegos de azar, son más susceptibles a actividades ilícitas.

La estructura de propiedad de una entidad también debe examinarse cuidadosamente. Las estructuras complejas y opacas, donde los beneficiarios finales están ocultos detrás de múltiples capas de entidades intermedias, son indicativas de posibles intentos de evadir la detección y, por lo tanto, se deben considerar de alto riesgo. El historial de transacciones de la entidad puede revelar patrones de comportamiento sospechoso, como operaciones inusualmente grandes, frecuentes o con contrapartes en jurisdicciones de alto riesgo.

Las personas expuestas políticamente (PEP), debido a su posición y la influencia que pueden ejercer, presentan un riesgo adicional. Las entidades con conexiones directas o indirectas con PEPs requieren un escrutinio adicional debido al mayor riesgo de corrupción y abuso de poder.

Actualización

Con base en estas evaluaciones, las autoridades pueden actualizar los controles internos de manera continua. Este proceso de actualización asegura que los controles se mantengan relevantes y efectivos frente a las amenazas cambiantes y las nuevas tendencias en actividades ilícitas. Los resultados de estas evaluaciones de riesgo, generalmente, no se hacen públicos. Mantener esta información confidencial es crucial para proteger la integridad del proceso y prevenir que individuos malintencionados ajusten sus comportamientos para evadir la detección.

Controles reforzados

Las entidades identificadas como de mayor riesgo, tales como aquellas con beneficiarios finales de países de alto riesgo, deben estar sujetas a controles reforzados. Estos controles reforzados pueden incluir verificaciones adicionales, auditorías más frecuentes y un monitoreo más exhaustivo de sus actividades. Por ejemplo, una entidad de alto riesgo podría ser requerida a proporcionar documentación adicional para verificaciones de antecedentes o someterse a auditorías periódicas por parte de terceros independientes.

Este enfoque permite a las autoridades no solo identificar y mitigar los riesgos más significativos, sino también disuadir actividades ilícitas mediante un sistema de supervisión visible y riguroso. Además, al centrarse en las áreas de mayor riesgo, las autoridades pueden utilizar sus recursos de manera más eficiente, asegurando que los esfuerzos de supervisión tengan el máximo impacto.

En resumen, establecer controles internos basados en el riesgo es una estrategia esencial para garantizar la integridad de los registros de beneficiarios finales. Al realizar evaluaciones de riesgo periódicas y adaptar los controles internos según los resultados, las autoridades pueden gestionar mejor los riesgos asociados con diferentes entidades. Las entidades de mayor riesgo, identificadas a través de este proceso, se someten a controles reforzados, mejorando la capacidad de las autoridades para detectar y prevenir actividades ilícitas.

3.2. Detección avanzada de anomalías

Detección avanzada de anomalías

Se pueden emplear algoritmos avanzados para detectar posibles entradas sospechosas al identificar patrones y anomalías que puedan indicar actividades fraudulentas. Estos algoritmos son herramientas cruciales para analizar grandes volúmenes de datos y detectar comportamientos atípicos que podrían escapar a la revisión humana. Un enfoque común es el uso de métodos de detección de anomalías, que emplean técnicas estadísticas y modelos de aprendizaje automático para establecer patrones de

comportamiento normal dentro de los datos. Al identificar estos patrones normales, los algoritmos pueden señalar desviaciones que podrían indicar conductas sospechosas.

Por ejemplo, los modelos de aprendizaje automático pueden ser entrenados con datos históricos para aprender lo que constituye un comportamiento típico en el registro de beneficiarios finales. Una vez entrenados, estos modelos pueden aplicar este conocimiento para analizar nuevos datos y detectar anomalías. Entre los algoritmos utilizados para este propósito se encuentran los algoritmos de agrupamiento, como K-means y DBSCAN.

K-means

K-means es un algoritmo que agrupa datos en k grupos (clusters) basándose en características similares. Funciona asignando cada punto de datos al clúster más cercano, calculado mediante la distancia entre los puntos y el centroide del clúster. Este algoritmo es útil para identificar patrones comunes y señalar aquellos puntos de datos que no se ajustan a ninguno de los grupos establecidos, lo que puede indicar una actividad inusual o sospechosa.

DBSCAN

Por otro lado, DBSCAN (Density-Based Spatial Clustering of Applications with Noise) es un algoritmo que agrupa puntos de datos basándose en la densidad de puntos en un espacio de características. A diferencia de K-means, que requiere la especificación previa del número de clústeres, DBSCAN identifica automáticamente clústeres basándose en la densidad de puntos y puede manejar mejor los datos con formas de clústeres irregulares y detectar puntos de ruido. Este algoritmo es particularmente útil para identificar pequeños grupos de actividad intensa que podrían representar redes de fraude o colusión.

Además de estos algoritmos de agrupamiento, se pueden utilizar otros enfoques de detección de anomalías. Los métodos estadísticos tradicionales, como el análisis de series temporales, pueden identificar patrones inusuales en los datos a lo largo del tiempo. Los modelos de aprendizaje supervisado, como las máquinas de vectores de soporte (SVM) y los bosques aleatorios, pueden ser entrenados con ejemplos de actividades legítimas y fraudulentas para aprender a distinguir entre ellas.

Estos algoritmos no solo permiten identificar actividades sospechosas de manera eficiente, sino que también pueden priorizar los casos para una revisión humana más detallada. Al automatizar la detección inicial de anomalías, se libera tiempo y recursos para que los analistas humanos se concentren en investigar los casos más complejos y de mayor riesgo.

En resumen, el uso de algoritmos avanzados para la detección de anomalías y patrones inusuales en los datos de beneficiarios finales es una estrategia poderosa para identificar posibles actividades fraudulentas. Al combinar técnicas estadísticas y modelos de aprendizaje automático, estos algoritmos mejoran significativamente la capacidad de las autoridades para mantener la integridad y la transparencia en los registros de beneficiarios finales.

3.3. Sistemas basados en reglas y puntuación de riesgo

Sistemas basados en reglas

Los sistemas basados en reglas son otro componente crítico en la detección de actividades sospechosas dentro de los registros de beneficiarios finales. Estos sistemas utilizan un conjunto de heurísticas predefinidas y sistemas de puntuación para identificar y señalar actividades que coinciden con ciertos criterios de riesgo. Las heurísticas son reglas basadas en la experiencia y el conocimiento

experto que permiten identificar patrones de comportamiento típicos de actividades fraudulentas o sospechosas.

Los criterios utilizados en los sistemas basados en reglas pueden ser variados y abarcar diferentes aspectos de los datos de beneficiarios finales. Uno de los criterios comunes es la asociación con jurisdicciones de alto riesgo, es decir, países o regiones que tienen laxas regulaciones financieras, altos índices de corrupción o son conocidos por ser refugios para el lavado de dinero. La participación de personas expuestas políticamente (PEP) es otro criterio crucial.

Puntuación de riesgo

Los sistemas de puntuación asignan puntajes de riesgo a entidades y transacciones basándose en varios atributos relevantes. Estos atributos pueden incluir, entre otros, el número de entidades con las que un propietario beneficiario está involucrado, el país de origen del propietario beneficiario, la complejidad de la estructura de propiedad, y el historial de transacciones de la entidad. Cada atributo recibe un peso específico basado en su relevancia y contribución al riesgo total.

Por ejemplo, una entidad cuyo propietario beneficiario tiene conexiones con múltiples otras entidades en diferentes jurisdicciones podría recibir un puntaje de riesgo más alto que una entidad con una estructura de propiedad más simple. Asimismo, un propietario beneficiario de un país con altos índices de corrupción recibiría un puntaje de riesgo mayor en comparación con uno de un país con regulaciones financieras estrictas y transparentes.

Estos puntajes de riesgo permiten priorizar los casos que requieren un escrutinio adicional. Las entidades y transacciones con puntajes más altos se consideran de mayor riesgo y, por lo tanto, se someten a revisiones más detalladas y exhaustivas. Este enfoque asegura que los recursos de supervisión y cumplimiento se utilicen de manera eficiente, enfocándose en los casos más susceptibles de estar involucrados en actividades ilícitas.

Además, los sistemas basados en reglas pueden ser ajustados y mejorados continuamente. A medida que se recopila más información y se identifican nuevos patrones de riesgo, las reglas y los criterios de puntuación pueden actualizarse para reflejar mejor las amenazas actuales y emergentes. Este proceso de mejora continua es esencial para mantener la eficacia del sistema en un entorno de riesgo siempre cambiante.

Como conclusión, los sistemas basados en reglas y los sistemas de puntuación de riesgo son herramientas esenciales para la identificación y priorización de actividades sospechosas en los registros de beneficiarios finales. Al aplicar criterios específicos y asignar puntajes de riesgo basados en atributos relevantes, estos sistemas permiten una supervisión más efectiva y enfocada, mejorando la capacidad de las autoridades para detectar y prevenir delitos financieros.

3.4. Análisis de redes y procesamiento de lenguaje natural

Análisis de redes

El análisis de redes puede modelar las estructuras de propiedad como grafos, una representación matemática en la que los nodos representan entidades (como personas o empresas) y las aristas representan las relaciones entre ellas. Utilizando algoritmos como PageRank o medidas de centralidad, es posible identificar nodos influyentes y conexiones inusuales dentro de estas redes.

PageRank, un algoritmo desarrollado originalmente por Google para clasificar páginas web, puede adaptarse para evaluar la importancia relativa de los nodos en una red de propiedad. En el contexto

de los beneficiarios finales, PageRank puede ayudar a identificar aquellos individuos o entidades que, a pesar de no ser inmediatamente visibles, tienen una gran influencia debido a sus conexiones indirectas con muchos otros nodos.

Las medidas de centralidad son otro conjunto de herramientas importantes en el análisis de redes. Estas medidas, como la centralidad de grado, la centralidad de intermediación y la centralidad de cercanía, ayudan a identificar nodos clave dentro de la red.

Medidas de centralidad

- La centralidad de grado mide el número de conexiones directas que tiene un nodo, lo que puede indicar la importancia o actividad de un nodo específico.
- La centralidad de intermediación evalúa cuántas veces un nodo actúa como un intermediario en las rutas más cortas entre otros nodos, destacando aquellos nodos que pueden controlar el flujo de información o recursos dentro de la red.
- La centralidad de cercanía mide cuán cerca está un nodo de todos los demás en la red, proporcionando una visión de la rapidez con la que puede difundirse la información a través de ese nodo.

SNA

El análisis de redes sociales (SNA, por sus siglas en inglés) va un paso más allá al examinar la red de relaciones entre entidades para detectar posibles colusiones o comportamientos sospechosos. El SNA puede revelar patrones y estructuras que no son evidentes a través de métodos de análisis tradicionales. Por ejemplo, un grupo de entidades que forman una subred densamente interconectada podría indicar una red de colaboración para actividades ilícitas.

Procesamiento de lenguaje natural

Además, las técnicas de procesamiento de lenguaje natural (NLP, por sus siglas en inglés) pueden emplearse para analizar datos textuales en las presentaciones del registro. El NLP permite extraer y analizar información valiosa de textos escritos en lenguaje natural, como descripciones de actividades, contratos y correspondencia oficial. Utilizando técnicas como el análisis de sentimientos, la detección de entidades nombradas y el modelado de temas, se pueden identificar inconsistencias, frases inusuales o indicios de intención fraudulenta.

- El análisis de sentimientos puede evaluar el tono y la emoción detrás del texto, detectando posibles intenciones sospechosas o fraudulentas.
- La detección de entidades nombradas identifica y clasifica nombres de personas, organizaciones, ubicaciones y otras entidades importantes, facilitando la identificación de conexiones relevantes.
- El modelado de temas descubre temas ocultos dentro de grandes volúmenes de texto, ayudando a identificar áreas de preocupación que pueden no ser obvias a simple vista.

Estas técnicas combinadas permiten una comprensión más profunda y detallada de las relaciones y actividades dentro de los registros de beneficiarios finales. Al modelar las estructuras de propiedad y analizar las redes de relaciones, las autoridades pueden detectar patrones complejos de comportamiento sospechoso y tomar medidas más informadas y efectivas contra el fraude y otras actividades ilícitas.

En resumen, el análisis de redes y las técnicas de procesamiento de lenguaje natural son herramientas poderosas para identificar nodos influyentes, conexiones inusuales y comportamientos sospechosos en los registros de beneficiarios finales.

3.5. Analítica predictiva para la detección de actividades sospechosas

Analítica predictiva

La analítica predictiva es una herramienta poderosa que utiliza técnicas avanzadas de análisis de datos para prever la probabilidad de actividades sospechosas basadas en datos históricos. Esta técnica se basa en el análisis de regresión y modelos de aprendizaje supervisado para identificar patrones y tendencias que pueden indicar comportamientos ilícitos.

Análisis de regresión

El análisis de regresión es un método estadístico que examina la relación entre una variable dependiente y una o más variables independientes. En el contexto de la detección de fraude, se puede utilizar para identificar qué factores o características están más estrechamente asociados con actividades sospechosas. Por ejemplo, una regresión logística puede modelar la probabilidad de que una entidad esté involucrada en actividades fraudulentas en función de variables como el número de transacciones, la geografía, la industria, entre otros.

Además del análisis de regresión, se emplean varios modelos de aprendizaje supervisado para mejorar la precisión de las predicciones. Entre estos modelos se incluyen:

Aprendizaje supervisado

Árboles de decisión: Este modelo divide los datos en subconjuntos más pequeños basados en preguntas de sí/no en cada punto de decisión (nodo). Cada nodo representa una característica de los datos, y las ramas representan el resultado de esa característica. Los árboles de decisión son fáciles de interpretar y pueden manejar tanto variables categóricas como continuas. Son particularmente útiles para identificar las características más importantes que distinguen entre actividades legítimas y sospechosas.

Bosques aleatorios: Este método es una extensión de los árboles de decisión y consiste en la creación de múltiples árboles de decisión a partir de diferentes subconjuntos de los datos. Las predicciones de todos los árboles se combinan (promediando en el caso de regresión, o votando en el caso de clasificación) para mejorar la precisión y reducir el riesgo de sobreajuste. Los bosques aleatorios son robustos y efectivos para manejar grandes conjuntos de datos con muchas características.

Máquinas de vectores de soporte (SVM): Este modelo se utiliza para clasificar datos en diferentes categorías al encontrar el hiperplano óptimo que separa los datos en el espacio de características. Las SVM son especialmente útiles para problemas de clasificación binaria y son efectivas en situaciones donde el número de características es grande en comparación con el número de observaciones. Pueden ser ajustadas para manejar casos donde los datos no son linealmente separables utilizando trucos de kernel.

Estos modelos de aprendizaje supervisado son entrenados con datos históricos etiquetados, donde las actividades legítimas y sospechosas ya están identificadas. Al aprender de estos ejemplos, los modelos pueden generalizar y hacer predicciones precisas sobre nuevos datos no vistos. Por ejemplo, pueden predecir la probabilidad de que una nueva transacción o una nueva entidad esté involucrada en actividades sospechosas.

La principal ventaja de la analítica predictiva es su capacidad para priorizar los casos para una investigación más profunda. Dado que los recursos de investigación son limitados, es crucial enfocarlos en las actividades más propensas a ser fraudulentas. Al predecir qué entidades o actividades son más riesgosas, estos modelos permiten a las autoridades concentrar sus esfuerzos en los casos que tienen mayor probabilidad de resultar en actividades ilícitas. Esto no solo mejora la eficiencia operativa, sino que también aumenta la efectividad en la detección y prevención del fraude.

Además, la analítica predictiva puede adaptarse y mejorar continuamente. A medida que se recopilan más datos y se identifican nuevos patrones, los modelos pueden ser actualizados y refinados para reflejar mejor las amenazas actuales y emergentes. Esta capacidad de adaptación es crucial para mantenerse a la vanguardia en un entorno de riesgo en constante evolución.

Por tanto, la analítica predictiva, utilizando análisis de regresión y modelos de aprendizaje supervisado como árboles de decisión, bosques aleatorios y máquinas de vectores de soporte, es esencial para prever la probabilidad de actividades sospechosas. Estos modelos ayudan a priorizar los casos para una investigación más profunda, permitiendo a las autoridades concentrar sus esfuerzos en las entidades y actividades más propensas a ser fraudulentas, mejorando así la eficiencia y efectividad en la detección y prevención del fraude.

3.6. Flujo de trabajo

Flujo de trabajo

El flujo de trabajo para la gestión de registros de beneficiarios finales comienza con la ingestión y preprocesamiento de datos. Los datos se recopilan de varias fuentes, se limpian y se normalizan para garantizar la consistencia y exactitud. Se puede realizar un cribado inicial utilizando sistemas basados en reglas y modelos de puntuación para señalar entidades y transacciones de alto riesgo. Este cribado inicial ayuda a filtrar los casos más sospechosos desde el principio.

Luego, se puede realizar un análisis avanzado, utilizando algoritmos de detección de anomalías y análisis de redes para un examen más profundo. Estos algoritmos refinan la identificación de actividades sospechosas al detectar patrones de comportamiento más complejos que pueden no ser evidentes en el cribado inicial. Las entradas sospechosas señaladas por estos algoritmos pueden escalarse para una revisión humana detallada. Esta revisión humana garantiza un examen y validación exhaustivos de los casos señalados, aprovechando la experiencia de los analistas para tomar decisiones informadas.

Los casos identificados como sospechosos pueden remitirse a la Unidad de Inteligencia Financiera (UIF) o una entidad equivalente para una investigación más profunda. Estas unidades tienen habilidades especializadas y autoridad para realizar investigaciones más exhaustivas y tomar las acciones necesarias, asegurando una supervisión y aplicación completas.

Este enfoque de múltiples capas ofrece varios beneficios. La combinación de procesos de revisión automática y humana asegura un alto nivel de precisión e integridad en la información de beneficiarios finales. Un enfoque basado en el riesgo permite una asignación eficiente de recursos, enfocando los esfuerzos en entidades y actividades de mayor riesgo. Las actualizaciones periódicas de las evaluaciones de riesgo y los controles internos permiten una supervisión proactiva y la adaptación a amenazas emergentes. La fuerte comunicación y colaboración entre el registro y la UIF facilita una

supervisión y aplicación integrales, contribuyendo a la efectividad general del marco contra el lavado de dinero y la financiación del terrorismo.

Sin embargo, hay desafíos a considerar. Garantizar datos de alta calidad es crucial para el rendimiento efectivo de los algoritmos, ya que los datos inexactos o incompletos pueden llevar a falsos positivos o negativos. La afinación y validación cuidadosa de los algoritmos son necesarias para evitar sesgos. Equilibrar la efectividad de los algoritmos con la necesidad de transparencia y explicabilidad es importante, particularmente cuando se trata de implicaciones legales y regulatorias. La mejora continua es esencial, con los algoritmos necesitando actualizaciones y refinamientos regulares basados en nuevos datos y amenazas emergentes para mantenerse efectivos.

Adoptar estos enfoques integrales y dinámicos puede mejorar significativamente la robustez de los registros de beneficiarios finales y contribuir a los esfuerzos globales para combatir los delitos financieros. Este enfoque no solo fortalece la integridad de los sistemas financieros, sino que también fomenta una mayor confianza y transparencia en los mercados financieros globales.

4. Verificaciones cruzadas con otras bases de datos gubernamentales

Verificaciones cruzadas

Las verificaciones automatizadas contra otras bases de datos gubernamentales son un método efectivo para comprobar la exactitud de la información declarada sobre los beneficiarios finales. Este enfoque es empleado por varios países, como Austria, Dinamarca, Irlanda o Letonia. Al aprovechar las bases de datos gubernamentales existentes, las autoridades pueden mejorar la integridad y fiabilidad de sus registros de beneficiarios finales.

4.1. Bases de datos relevantes

Bases de datos

Los países que utilizan verificaciones cruzadas automatizadas integran sus registros de beneficiarios finales con una pluralidad de bases de datos cada una de las cuales cumple una función específica de verificación.

Administración tributaria

En este sentido, revisten una particular importancia las bases de datos de la Administración Tributaria. Al verificar la información de los beneficiarios finales con los registros fiscales, las autoridades pueden asegurarse de que los beneficiarios declarados sean consistentes con aquellos conocidos por las autoridades tributarias. Esto ayuda a identificar discrepancias y posibles incumplimientos fiscales, ya que los individuos que intentan ocultar sus ingresos o activos reales podrían informar de manera diferente a las autoridades fiscales en comparación con lo registrado en el registro de beneficiarios finales.

Registro Civil

Otra fuente importante es la base de datos de Registro Civil, que contiene detalles de identificación personal, como nombres, fechas de nacimiento y direcciones. Al verificar estos detalles contra los registros del registro civil, las autoridades pueden confirmar la identidad de los beneficiarios finales, reduciendo el riesgo de fraude de identidad. Esta base de datos asegura que las personas enumeradas en el registro sean quienes dicen ser, proporcionando una capa fundamental de verificación.

Pasaportes

La información de pasaportes también es crucial para la verificación de identidad. Al acceder a los registros de pasaportes nacionales e internacionales, las autoridades pueden confirmar las identidades de los beneficiarios finales. Esto es particularmente útil para identificar a personas que puedan utilizar múltiples pasaportes para ocultar su identidad. Los pasaportes a menudo contienen datos biométricos,

como huellas dactilares o reconocimiento facial, que pueden utilizarse para verificar que una persona no esté usando múltiples identidades para llevar a cabo actividades ilícitas.

Servicios sociales

La base de datos de Servicios Sociales es otro recurso valioso. Verificar los números de seguridad social y otros identificadores ayuda a asegurar que la información proporcionada en el registro de beneficiarios finales coincida con los registros en las bases de datos de servicios sociales. Esto puede permitir descubrir inconsistencias que podrían indicar actividad fraudulenta. Por ejemplo, las discrepancias entre los registros de seguridad social y las declaraciones de beneficiarios finales pueden señalar intentos de tergiversar u ocultar la verdadera propiedad.

Registros empresariales o mercantiles

Los registros empresariales o mercantiles proporcionan un medio para comparar la información de propiedad con otras presentaciones corporativas. Al hacerlo, las autoridades pueden asegurar que la información en el registro de beneficiarios finales sea consistente con los registros en los registros empresariales, destacando cualquier discrepancia que pueda sugerir propiedad o control ocultos. Esto es particularmente importante para descubrir estructuras corporativas complejas diseñadas para ocultar a los verdaderos propietarios de una empresa. La consistencia entre los registros empresariales y los registros de beneficiarios finales ayuda a mantener la transparencia y la responsabilidad en la gobernanza corporativa.

Registros de la propiedad

En el caso de los registros de la propiedad, su verificación cruzada con los registros de beneficiarios finales, puede permitir a las autoridades prevenir la ocultación de activos a través de bienes raíces. La propiedad de bienes inmuebles es un método común utilizado para ocultar riqueza y oscurecer la verdadera propiedad de los activos. Asegurar que los registros de propiedad inmobiliaria se alineen con las declaraciones de beneficiarios finales ayuda a prevenir este tipo de ocultación de activos.

Información electoral

Finalmente, las bases de datos de Información electoral se utilizan para asegurar que las personas enumeradas como beneficiarios finales sean ciudadanos registrados y reconocidos. Esto ayuda a verificar la legitimidad de los propietarios y prevenir el uso indebido del registro por parte de no ciudadanos o individuos ficticios. Las bases de datos electorales pueden confirmar el estado de residencia y ciudadanía, proporcionando una seguridad adicional.

Al integrar estas diversas bases de datos, los países pueden realizar verificaciones cruzadas automatizadas y exhaustivas que mejoran la exactitud y la fiabilidad de sus registros de beneficiarios finales. Este enfoque multifacético no solo asegura que la información sea consistente en diferentes registros gubernamentales, sino que también ayuda a identificar y prevenir actividades fraudulentas. Las verificaciones cruzadas automatizadas agilizan el proceso de verificación, permitiendo la detección inmediata de discrepancias y reduciendo la necesidad de revisiones manuales. Esta eficiencia es particularmente importante en jurisdicciones con un alto volumen de presentaciones de beneficiarios finales, ya que garantiza que los recursos se utilicen de manera efectiva y se prioricen los casos de alto riesgo.

4.2. Herramientas de tecnología de la información y técnicas de integración

APIs

Las herramientas de tecnología de la información y las técnicas de integración son cruciales para la implementación efectiva de verificaciones cruzadas automatizadas entre los registros de beneficiarios finales y las diversas bases de datos gubernamentales. Las Interfaces de Programación de Aplicaciones (APIs) juegan un papel fundamental en este proceso. Las APIs son esenciales para habilitar la

comunicación entre diferentes bases de datos y el registro de beneficiarios finales. Permiten el intercambio de datos en tiempo real y una integración no problemática, haciendo posible que diferentes sistemas compartan información instantáneamente y de manera eficiente. Esta capacidad en tiempo real es crítica para mantener información actualizada y precisa en el registro. Las APIs también admiten una gama de funciones, incluyendo la recuperación de datos, actualizaciones y procesos de validación, que son esenciales para el monitoreo continuo y la verificación de la información de beneficiarios finales.

Middleware

Otra herramienta importante es el middleware de datos. Las soluciones middleware facilitan el proceso de integración actuando como intermediarios que gestionan, transforman y enrutan datos entre diferentes sistemas. Manejan las complejidades de la traducción de datos y aseguran que la información se transfiera con precisión de un sistema a otro. El middleware puede simplificar la integración de sistemas dispares proporcionando una plataforma común para el intercambio de datos, reduciendo así la necesidad de soluciones de integración personalizadas para cada sistema. Además, el middleware ofrece funcionalidades como agregación de datos, filtrado y enriquecimiento, que mejoran la calidad y la utilidad de los datos integrados.

ESB

Un Bus de Servicio Empresarial (ESB) también puede ser empleado para conectar sistemas dispares. Un ESB permite el flujo de datos entre varias bases de datos gubernamentales y el registro de beneficiarios finales. Proporciona una solución de integración escalable y flexible que puede manejar los variados formatos de datos y protocolos utilizados por diferentes sistemas. El ESB actúa como un hub central que enruta datos hacia y desde el registro, asegurando que todos los sistemas puedan comunicarse de manera efectiva. Además, un ESB admite la transformación de mensajes, la conversión de protocolos y el enrutamiento inteligente, que son esenciales para gestionar escenarios de integración complejos y asegurar la entrega confiable de datos.

Integración

Las plataformas de integración basadas en la nube ofrecen otra solución robusta para integrar múltiples bases de datos. Estas plataformas proporcionan soluciones escalables y rentables que pueden crecer con las necesidades del registro. Ofrecen herramientas para el mapeo de datos, la transformación y la orquestación, lo que facilita la integración y gestión de datos provenientes de múltiples fuentes. Las plataformas basadas en la nube también proporcionan beneficios adicionales como flexibilidad y accesibilidad remota, permitiendo que los procesos de integración se gestionen y monitoreen desde cualquier lugar. Además, las soluciones en la nube a menudo vienen con características de seguridad integradas como cifrado, controles de acceso y gestión de cumplimiento, asegurando que los datos estén protegidos durante todo el proceso de integración.

Más detalles sobre las técnicas de integración incluyen:

Sincronización de datos en tiempo real

Sincronización de datos en tiempo real: La sincronización en tiempo real asegura que los cambios realizados en una base de datos se reflejen inmediatamente en el registro de beneficiarios finales. Esto minimiza el riesgo de discrepancias y asegura que la información más actualizada esté siempre disponible. Herramientas como la Captura de Datos de Cambio (CDC) pueden ser utilizadas para rastrear y propagar cambios en tiempo real.

Calidad de datos

Gestión de calidad de datos: Asegurar una alta calidad de los datos es crucial para el éxito de las verificaciones cruzadas automatizadas. Las herramientas de gestión de calidad de datos pueden

integrarse para realizar limpieza de datos, deduplicación y validación antes de que los datos se ingresen en el registro. Estas herramientas ayudan a mantener la integridad y fiabilidad de la información.

Transmisión segura de datos

Transmisión segura de datos: Proteger los datos durante la transmisión es esencial. Protocolos de transmisión segura de datos como la Capa de Conexión Segura (Secure Socket Layer, SSL) y la Seguridad de la Capa de Transporte (Transport Layer Security, TLS) se emplean para cifrar los datos y prevenir el acceso no autorizado durante el intercambio de datos. Las Redes Privadas Virtuales (VPNs) también pueden usarse para crear conexiones seguras entre sistemas.

Manejo de errores y registro

Manejo de errores y registro: Mecanismos robustos de manejo de errores y registro son importantes para diagnosticar y resolver problemas que puedan surgir durante la integración de datos. Alertas automatizadas y registros exhaustivos ayudan a los administradores a identificar y solucionar problemas rápidamente, asegurando una operación continua de los procesos de integración.

Escalabilidad y optimización del rendimiento

Escalabilidad y optimización del rendimiento: Las soluciones de integración deben ser escalables para manejar volúmenes crecientes de datos a medida que el registro crece. Técnicas de optimización del rendimiento como el balanceo de carga, el procesamiento paralelo y el diseño eficiente de consultas son esenciales para mantener un alto rendimiento y capacidad de respuesta del sistema de integración.

En general, estas herramientas de tecnología de la información y técnicas de integración —APIs, middleware de datos, ESB, plataformas de integración basadas en la nube, sincronización de datos en tiempo real, gestión de calidad de datos, transmisión segura de datos, manejo de errores y escalabilidad— son vitales para la integración exitosa de los registros de beneficiarios finales con varias bases de datos gubernamentales. Permiten un intercambio de datos sin problemas, aseguran la precisión de los datos, proporcionan soluciones escalables para satisfacer las necesidades cambiantes del registro y mantienen altos niveles de seguridad y rendimiento. Al implementar estas tecnologías, las autoridades pueden mejorar la fiabilidad e integridad de la información de beneficiarios finales.

4.3. Transmisión de datos

La transmisión de datos es un aspecto crítico para garantizar la integridad y precisión de los registros de beneficiarios finales. La transmisión segura de datos es fundamental, ya que protege la información sensible mientras se intercambia entre diferentes sistemas. Los protocolos ya mencionados SSL/TLS se utilizan comúnmente para salvaguardar los datos en tránsito. Estos métodos de cifrado previenen el acceso no autorizado y aseguran que los datos permanezcan confidenciales e inalterables durante la transmisión. Al cifrar los paquetes de datos, SSL/TLS garantiza que, incluso si los datos son interceptados, no puedan ser leídos o alterados por actores malintencionados. Esta medida de seguridad es vital para mantener la confianza y la integridad de los registros de beneficiarios finales.

Procesamiento por lotes

Procesamiento en tiempo real

En cuanto al método de transmisión de datos, existen dos enfoques principales: procesamiento por lotes vs. procesamiento en tiempo real. El procesamiento por lotes implica recopilar datos y transmitirlos en intervalos programados. Este método es eficiente para manejar grandes volúmenes de datos a la vez, pero puede resultar en ligeros retrasos en la disponibilidad de los datos. Por ejemplo, un registro de beneficiarios finales podría actualizarse cada noche con los datos recopilados durante el día. Este enfoque es menos intensivo en recursos y puede ser más fácil de gestionar, pero no proporciona actualizaciones inmediatas. Por otro lado, el procesamiento en tiempo real implica

transmitir datos inmediatamente a medida que están disponibles, ofreciendo verificación inmediata y actualización del registro de beneficiarios finales. Este método asegura que el registro esté siempre actualizado, reflejando los cambios y adiciones más recientes. Sin embargo, el procesamiento en tiempo real requiere una infraestructura más robusta y confiable para manejar el flujo continuo de datos sin interrupciones. Esto incluye conexiones de internet de alta velocidad, servidores potentes y software avanzado de gestión de datos capaz de procesar e integrar datos en tiempo real.

Sincronización de datos

La sincronización de datos es otro elemento crucial para mantener la precisión y consistencia de los registros de beneficiarios finales. Involucra actualizar regularmente el registro con los datos más recientes de varias bases de datos gubernamentales, como registros fiscales, registros civiles, información de pasaportes, servicios sociales, registros empresariales, registros de propiedad y padrones electorales. La sincronización asegura que todos los sistemas involucrados en el intercambio de datos estén alineados, previniendo discrepancias y garantizando que la información en el registro de beneficiarios finales esté actualizada y sea precisa. Este proceso puede incluir actualizaciones en tiempo real o tareas de sincronización programadas, dependiendo de las capacidades del sistema y la criticidad de los datos a sincronizar. Por ejemplo, la sincronización puede involucrar actualizaciones horarias desde la base de datos de la administración tributaria para asegurar que cualquier cambio en la propiedad o nuevas declaraciones fiscales se reflejen puntualmente en el registro de beneficiarios finales.

Además, se pueden emplear técnicas avanzadas como el espejado de datos y la replicación de bases de datos para asegurar alta disponibilidad y tolerancia a fallos. El espejado de datos implica crear una copia exacta de la base de datos de beneficiarios finales, que se actualiza continuamente con cada transacción. Esto asegura que siempre haya una copia de seguridad disponible en caso de fallo del sistema. La replicación de bases de datos implica copiar y distribuir datos a través de múltiples servidores de bases de datos, lo que puede mejorar el rendimiento y la fiabilidad. Estas técnicas aseguran que los datos no solo se sincronicen, sino que también estén protegidos contra la pérdida de datos y el tiempo de inactividad del sistema.

Además, los procesos de validación de datos son esenciales durante la transmisión y sincronización para asegurar que los datos integrados sean precisos y completos. Esto implica verificar la integridad de los datos, como asegurarse de que todos los campos requeridos estén completos y que los datos se ajusten a los formatos y reglas predefinidos. Los scripts de validación automatizados pueden ejecutarse durante la transmisión de datos para identificar y corregir errores antes de que se ingresen en el registro de beneficiarios finales.

En resumen, la transmisión segura de datos, ya sea mediante procesamiento por lotes o en tiempo real, y la sincronización efectiva de datos son esenciales para mantener la integridad y precisión de los registros de beneficiarios finales. Al implementar el cifrado SSL/TLS, elegir el método de transmisión apropiado según los requisitos del sistema y asegurar actualizaciones regulares de datos, las autoridades pueden garantizar que la información de beneficiarios finales esté protegida, sea precisa y esté actualizada. Medidas adicionales como el espejado de datos, la replicación de bases de datos y la validación de datos mejoran aún más la fiabilidad y resiliencia del sistema.

4.4. Coincidencia y validación de datos

La coincidencia y validación de datos son procesos críticos para garantizar la exactitud e integridad de los registros de beneficiarios finales. Estos procesos involucran varias técnicas para comparar y verificar datos de diferentes fuentes, asegurando la consistencia y confiabilidad de la información registrada.

Coincidencia exacta

Coincidencia Exacta es una técnica sencilla que implica comparar directamente campos de datos como nombres, fechas de nacimiento y números de identificación. Este método es altamente efectivo cuando la calidad de los datos es alta y consistente en diferentes bases de datos. Para los registros de beneficiarios finales, la coincidencia exacta puede confirmar rápidamente la identidad de los individuos al asegurar que los detalles proporcionados coincidan precisamente con los de registros oficiales como bases de datos fiscales, registros civiles e información de pasaportes. Por ejemplo, cuando se realiza una nueva entrada de beneficiarios finales, la coincidencia exacta puede verificar instantáneamente los detalles del individuo contra múltiples bases de datos gubernamentales, asegurando que la información sea precisa y esté actualizada. Sin embargo, esta técnica puede fallar cuando hay ligeras variaciones o errores en las entradas de datos, lo que da lugar a métodos más sofisticados.

Coincidencia difusa

Los Algoritmos de Coincidencia Difusa están diseñados para manejar variaciones e inconsistencias en los datos, como errores tipográficos o diferentes formatos. Técnicas como la distancia de Levenshtein, la similitud de Jaccard y Soundex se utilizan comúnmente para identificar registros que son similares pero no idénticos. Por ejemplo, la distancia de Levenshtein mide el número de ediciones de un solo carácter necesarias para cambiar una palabra a otra, lo que resulta útil para identificar errores tipográficos menores en los nombres. La similitud de Jaccard mide la similitud entre conjuntos de muestras, lo cual puede ser efectivo para emparejar registros con atributos diferentes pero relacionados. Soundex, un algoritmo que indexa palabras por su representación fonética, ayuda a emparejar nombres que suenan similares pero se escriben de manera diferente. Estas técnicas de coincidencia difusa son cruciales para los registros de beneficiarios finales, ya que ayudan a identificar y reconciliar registros que pueden haber sido ingresados con ligeras variaciones, asegurando una base de datos más completa y precisa. Por ejemplo, si un propietario beneficiario está listado como "Juan Pérez" en una base de datos y "Juan Perez" en otra, la coincidencia difusa puede identificar estas entradas como referidas probablemente a la misma persona, previniendo así errores que podrían oscurecer la verdadera propiedad.

Coincidencia Basada en Reglas

La Coincidencia Basada en Reglas implica definir reglas personalizadas para emparejar registros basados en criterios específicos. Estas reglas pueden adaptarse a las necesidades únicas del registro de beneficiarios finales. Por ejemplo, se podría crear una regla para emparejar direcciones parciales, donde solo el nombre de la calle y la ciudad deben ser iguales, o para combinar múltiples puntos de datos como nombre, fecha de nacimiento y dirección parcial para verificar una coincidencia. La coincidencia basada en reglas es flexible y puede ajustarse según sea necesario para acomodar diferentes requisitos de verificación. Esta técnica permite una mayor especificidad y control en el proceso de coincidencia de datos, asegurando que los criterios para emparejar se alineen con los requisitos regulatorios y el contexto específico de los datos de beneficiarios finales. Por ejemplo, si un propietario beneficiario está asociado con múltiples direcciones debido a tener varias residencias o

ubicaciones comerciales, la coincidencia basada en reglas puede usar reglas predefinidas para vincular con precisión todos los registros relevantes a la persona correcta.

Los Modelos de Aprendizaje Automático representan el enfoque más avanzado para la coincidencia y validación de datos. Estos modelos pueden entrenarse utilizando datos históricos para aprender patrones y relaciones dentro de los datos. Con el tiempo, los modelos de aprendizaje automático pueden mejorar su precisión adaptándose a nuevos patrones de datos. Para los registros de beneficiarios finales, el aprendizaje automático puede emplearse para identificar relaciones complejas y patrones que las técnicas de coincidencia tradicionales podrían pasar por alto. Por ejemplo, un modelo de aprendizaje automático puede aprender a reconocer que ciertos tipos de estructuras de propiedad son más propensos a involucrar tipos específicos de entidades o individuos, mejorando así la identificación de beneficiarios finales. Estos modelos también pueden actualizar y refinar continuamente sus algoritmos a medida que se dispone de más datos, asegurando que el proceso de coincidencia permanezca efectivo y preciso. Los modelos de aprendizaje automático también pueden manejar grandes volúmenes de datos y conjuntos de datos complejos, lo que los hace ideales para su uso en registros extensivos de beneficiarios finales donde los métodos de coincidencia tradicionales podrían tener dificultades para mantener la precisión y eficiencia.

Aprendizaje automático

En el contexto de los registros de beneficiarios finales, la combinación de estas técnicas de coincidencia y validación de datos proporciona un marco robusto para garantizar la precisión y confiabilidad de los datos. La coincidencia exacta asegura que las entradas de datos sencillas y consistentes se verifiquen rápidamente. La coincidencia difusa maneja variaciones y discrepancias, asegurando que los errores menores no impidan una identificación precisa. La coincidencia basada en reglas permite la personalización y especificidad en el proceso de verificación, mientras que los modelos de aprendizaje automático ofrecen capacidades avanzadas para identificar patrones complejos y mejorar la precisión con el tiempo. Juntas, estas técnicas aseguran que los registros de beneficiarios finales sean completos, precisos y confiables.

Al implementar un enfoque multifacético para la coincidencia y validación de datos, las autoridades pueden mejorar la integridad de los registros de beneficiarios finales, dificultando que las actividades fraudulentas pasen desapercibidas y asegurando que los verdaderos propietarios de las entidades sean identificados y registrados con precisión. Esto, a su vez, fortalece el sistema financiero en general al promover la transparencia y disuadir actividades ilícitas. Por ejemplo, un registro de beneficiarios finales que emplea estas avanzadas técnicas de coincidencia y validación de datos puede identificar de manera más efectiva empresas fachada y otras entidades utilizadas para el lavado de dinero o la evasión fiscal, mejorando así la capacidad de los reguladores financieros y las agencias de cumplimiento de la ley para combatir los delitos financieros.

4.5. Ventajas del uso de verificaciones automatizadas

El uso de verificaciones cruzadas automatizadas en los registros de beneficiarios finales proporciona varias ventajas clave que mejoran significativamente la precisión y la fiabilidad de la información consignada en estos registros.

Primero, la aplicación integral es una de las principales ventajas. Los procesos automatizados pueden aplicarse fácilmente a todas las entradas en el registro de beneficiarios finales, asegurando una

Aplicación integral

verificación amplia sin intervención manual. Esto significa que cada pieza de información ingresada en el registro se verifica automáticamente contra varias bases de datos gubernamentales, como registros fiscales, registros civiles, información de pasaportes, servicios sociales, registros empresariales, registros de propiedad y padrones electorales. Este enfoque integral asegura que ninguna entrada quede sin verificar, manteniendo un alto estándar de integridad de datos en todo el registro.

Prevención de inexactitudes

Segundo, las verificaciones cruzadas automatizadas son cruciales para prevenir inexactitudes. Ayudan a evitar la entrada de información claramente inexacta o fraudulenta en el registro al señalar automáticamente inconsistencias o errores en el punto de entrada. Al detectar estos problemas desde el principio, el sistema reduce la necesidad de auditorías y correcciones intensivas en recursos después de la entrada. Por ejemplo, si un nombre o número de identificación ingresado en el registro de beneficiarios finales no coincide con los registros correspondientes en las bases de datos de registro civil o pasaportes, el sistema puede alertar inmediatamente al usuario o bloquear la entrada hasta que se resuelva la discrepancia. Este enfoque proactivo asegura que solo se registre información precisa y verificada, manteniendo así la integridad del registro desde el inicio.

Optimización de recursos

Tercero, las verificaciones cruzadas automatizadas conducen a una optimización significativa de los recursos. Las autoridades pueden reasignar recursos que se habrían dedicado a la verificación manual y corrección de datos inexactos para centrarse en entidades de mayor riesgo y casos más sospechosos. En lugar de dedicar una cantidad sustancial de mano de obra a revisar manualmente cada entrada, estos recursos pueden redirigirse hacia la investigación de estructuras de propiedad complejas, la identificación de posibles casos de lavado de dinero y el escrutinio de entidades con perfiles de alto riesgo. Este cambio no solo mejora la eficiencia general del proceso de gestión del registro, sino que también aumenta la capacidad de las autoridades para detectar y prevenir delitos financieros.

Confianza en la precisión de la información

Cuarto, el uso de verificaciones cruzadas automatizadas proporciona una mayor confianza en la precisión de la información para todos los usuarios del registro. Los sistemas automatizados reducen el error humano y aseguran que los datos se hayan verificado consistentemente contra múltiples fuentes autorizadas. Esta fiabilidad es crucial para los interesados que dependen del registro para la debida diligencia, el cumplimiento y otros procesos de toma de decisiones. Las instituciones financieras, los organismos reguladores y las agencias de aplicación de la ley dependen de la precisión de la información de beneficiarios finales para realizar evaluaciones de riesgo, cumplir con las regulaciones contra el lavado de activos e investigar actividades sospechosas. Al asegurar que los datos en el registro sean precisos y estén actualizados, las verificaciones cruzadas automatizadas mejoran la confiabilidad y utilidad general del registro.

4.6. Desafíos asociados a las verificaciones automatizadas

Si bien las verificaciones cruzadas automatizadas en los registros de beneficiarios finales ofrecen ventajas significativas, también existen desafíos y consideraciones que deben abordarse para garantizar su implementación efectiva.

Integración de datos

Primero, la integración de datos plantea un desafío sustancial. Integrar varias bases de datos gubernamentales, como registros fiscales, registros civiles, información de pasaportes, servicios sociales, registros empresariales, registros de propiedad y padrones electorales, puede ser complejo y requiere una infraestructura de tecnología de la información robusta. Esta integración no solo implica

vincular estos sistemas dispares, sino también asegurar que puedan comunicarse eficazmente y compartir datos sin problemas. Requiere marcos avanzados de gobernanza de datos para gestionar el flujo de datos, asegurar la consistencia y mantener la integridad de los datos en todos los sistemas. Además, diferentes bases de datos pueden utilizar diferentes formatos y estándares de datos, lo que hace que el proceso de integración sea aún más desafiante. Desarrollar y mantener esta infraestructura necesita una inversión significativa en tecnología y experiencia.

Privacidad y seguridad de los datos

Segundo, la privacidad y seguridad de los datos son primordiales al implementar verificaciones cruzadas automatizadas. Asegurar la privacidad y seguridad de los datos que se están verificando implica implementar controles de acceso estrictos para limitar quién puede acceder y manipular los datos. Se deben emplear medidas de cifrado, como SSL y TLS, para proteger los datos durante la transmisión y el almacenamiento. Además, son necesarios mecanismos robustos de autenticación para verificar las identidades de los usuarios que acceden al sistema. Esto ayuda a prevenir el acceso no autorizado y las brechas de seguridad que podrían comprometer información sensible y socavar la confianza en el registro de beneficiarios finales. Además, las auditorías y actualizaciones de seguridad regulares son esenciales para abordar amenazas y vulnerabilidades emergentes.

Calidad de los datos

Tercero, la calidad de los datos en las bases de datos gubernamentales es crítica para la efectividad de las verificaciones cruzadas automatizadas. La fiabilidad del proceso de verificación depende en gran medida de la precisión, integridad y actualidad de los datos en estas bases de datos. Si los datos están desactualizados, incompletos o son inexactos, pueden conducir a falsos positivos o negativos, socavando la integridad del registro de beneficiarios finales. Por lo tanto, es esencial realizar actualizaciones y mantenimientos regulares de estas bases de datos para asegurar su fiabilidad. Esto incluye limpieza periódica de datos, validación y actualizaciones para reflejar la información más reciente. Las prácticas de gestión de calidad de datos, como el perfilado de datos y el monitoreo de calidad, pueden ayudar a identificar y rectificar problemas de datos antes de que impacten el proceso de verificación.

Cumplimiento legal y regulatorio

Cuarto, el cumplimiento legal y regulatorio es una consideración crucial para las verificaciones cruzadas automatizadas. Estos procesos deben cumplir con las leyes y regulaciones nacionales e internacionales sobre el intercambio y la privacidad de datos. Diferentes jurisdicciones pueden tener requisitos legales variados respecto a la recopilación, uso y compartición de información personal y sensible. Esto implica no solo asegurar que las prácticas de manejo de datos se adhieran a los estándares legales, sino también mantener una documentación completa y registros de auditoría para demostrar el cumplimiento. Los marcos legales también pueden imponer restricciones sobre las transferencias de datos transfronterizas, que deben gestionarse cuidadosamente para asegurar el cumplimiento mientras se facilitan los intercambios de datos necesarios.

En resumen, aunque las verificaciones cruzadas automatizadas en los registros de beneficiarios finales ofrecen beneficios significativos en términos de precisión, eficiencia y fiabilidad, también conllevan desafíos y consideraciones que deben gestionarse cuidadosamente. La integración de datos requiere una infraestructura de tecnología de la información robusta y marcos de gobernanza de datos para asegurar una comunicación sin problemas entre varias bases de datos gubernamentales. Asegurar la privacidad y seguridad de los datos implica implementar controles de acceso estrictos, medidas de cifrado y auditorías de seguridad regulares para proteger la información sensible. Mantener una alta

calidad de datos a través de actualizaciones y mantenimientos regulares es esencial para la efectividad de las verificaciones cruzadas automatizadas. Finalmente, el cumplimiento de los requisitos legales y regulatorios es crucial para asegurar que las prácticas de intercambio y procesamiento de datos se adhieran a las leyes nacionales e internacionales. Al abordar estos desafíos y consideraciones, las autoridades pueden maximizar los beneficios de las verificaciones cruzadas automatizadas mientras mantienen la integridad y confiabilidad de los registros de beneficiarios finales.

4.7. Procedimientos de resolución de discrepancias

Para resolver posibles discrepancias en la información al contrastarla con otras bases de datos gubernamentales, se pueden establecer procedimientos estandarizados que permitan corregir y actualizar la información de manera eficiente. A continuación, podemos señalar algunos procedimientos recomendados:

Notificación automática de discrepancias: Si se detecta una discrepancia al cruzar la información del registro con otras bases de datos (como las de identidad, tributación, o seguridad social), se puede enviar una notificación automatizada al declarante (empresa o entidad) y al beneficiario final, señalando los detalles de la discrepancia y solicitando la corrección o aclaración en un plazo determinado. Las notificaciones pueden estar acompañadas de un resumen de la información discrepante y las bases de datos consultadas.

Período de corrección o aclaración: Se puede establecer un período para que el declarante o beneficiario final corrija la información o proporcione documentación adicional que respalde la veracidad de los datos registrados. Este plazo suele variar entre 15 y 30 días, dependiendo de la complejidad de la corrección. El período de corrección permite a las partes involucradas presentar evidencia documental que explique o valide cualquier discrepancia.

Revisión manual y validación: En caso de que la discrepancia persista tras la corrección o no se reciba respuesta, se puede asignar un equipo de revisión para analizar manualmente la información e investigar las causas de la inconsistencia. Este equipo puede contactar a la entidad declarante para solicitar información detallada o realizar una verificación en persona, en caso necesario.

Integración de un sistema de escalamiento de alertas: Las discrepancias que no se resuelven en la etapa de revisión inicial pueden ser escaladas a una unidad de cumplimiento, auditoría, o a una autoridad competente para su investigación formal. Las alertas escaladas pueden activar auditorías financieras o de cumplimiento, si existen indicios de posible fraude, ocultamiento de beneficiarios, o errores reiterados en los registros.

Sanciones y medidas correctivas: Como medida de control, se pueden implementar sanciones en casos de incumplimiento o de declaración de información falsa, como multas o restricciones en los permisos de operación de la entidad declarante. Además, se puede considerar la inhabilitación temporal de la entidad hasta que corrija las discrepancias de manera satisfactoria.

Actualización y retroalimentación en tiempo real: Si es posible, se pueden utilizar sistemas de retroalimentación en tiempo real, que envíen recordatorios automáticos y guíen al declarante en la actualización de datos para reducir las probabilidades de discrepancia desde el principio. La interoperabilidad con otras bases de datos gubernamentales es crucial para que el sistema pueda

actualizar y corregir automáticamente la información de beneficiarios finales sin necesidad de intervención constante.

Protocolos de mantenimiento y actualización regular del registro: Establecer revisiones periódicas (anuales o semestrales) de la información del registro de beneficiarios finales, cruzando nuevamente los datos con otras bases gubernamentales, permite mantener la exactitud y actualidad de los registros. Los procedimientos de actualización regular también pueden ayudar a identificar patrones de error o fraude y a ajustar los protocolos de control.

Estos procedimientos permiten mejorar la exactitud del registro, reducir la carga administrativa de las entidades declarante y de los beneficiarios, y fortalecer la transparencia y la fiabilidad del sistema de registro de beneficiarios finales.

La existencia de discrepancias puede asimismo detectarse como consecuencia de información obtenida por los sujetos obligados. En el Reino Unido, una entidad obligada debe remitir un informe si detecta una discrepancia material entre la información que posee sobre una Persona con Control Significativo (PSC) y la información obrante en el registro de la Companies House. Una discrepancia material se produce cuando la información de que dispone una entidad obligada es significativamente diferente a la información registrada por la Companies House. La notificación de discrepancias materiales es una obligación bajo las Reglamentaciones de 2017 de Lavado de Dinero, Financiación del Terrorismo y Transferencia de Fondos (Información sobre el Pagador). No obstante, a partir de abril de 2023, las entidades obligadas únicamente deben informar una discrepancia material si se puede considerar razonablemente que está vinculada al lavado de dinero, al financiamiento del terrorismo o al ocultamiento de detalles del negocio del cliente. Sin perjuicio de ello, las entidades obligadas no necesitan considerar si el ocultamiento es deliberado o no. Una entidad obligada debe valorar si la información podría objetivamente considerarse que oculta los detalles del PSC de una empresa. Es importante destacar que la obligación de remitir un informe de discrepancia a la Companies House es independiente de la obligación de presentar un Reporte de Actividad Sospechosa (SAR) a la Unidad de Inteligencia Financiera (FIU).

5. Sistema de gestión de datos

Existen dos enfoques principales en relación con la gestión de datos de beneficiarios finales: los sistemas propietarios desarrollados específicamente para una agencia, como el Beneficial Ownership Secure System (BOSS) de FinCEN, y los estándares abiertos, como el Beneficial Ownership Data Standard (BODS) de OpenOwnership. A continuación se examinan ambos enfoques.

5.1. Sistemas propietarios

Sistemas propietarios

Los sistemas propietarios en el campo de la recopilación y gestión de datos de propiedad beneficiaria son soluciones desarrolladas ad hoc para una autoridad o agencia, teniendo en cuenta su marco legal aplicable y sus requerimientos y necesidades específicas. Un supuesto particularmente relevante de sistema propietario lo constituye el Beneficial Ownership Secure System (BOSS) desarrollado por FinCEN.

Beneficial Ownership Secure System (BOSS)

BOSS sirve como un repositorio centralizado para recopilar, almacenar y gestionar la información de beneficiarios finales remitida por las empresas informantes en cumplimiento de la Ley de Transparencia Corporativa (CTA). El sistema está integrado en la infraestructura informática de FinCEN,

lo que facilita el intercambio de datos y la interoperabilidad con otros sistemas internos. La arquitectura del sistema incluye una base de datos centralizada capaz de gestionar grandes volúmenes de datos, respaldada por herramientas robustas de gestión de datos y soluciones de almacenamiento seguro. Automatiza la recopilación de información de propiedad beneficiaria, que incluye datos personales detallados como nombres, fechas de nacimiento, direcciones residenciales o comerciales y números de identificación únicos de documentos emitidos por las autoridades. Las empresas informantes envían esta información a través de un portal en línea seguro.

La seguridad es un aspecto crítico de BOSS. El sistema emplea múltiples capas de protección para garantizar la integridad y confidencialidad de los datos almacenados y procesados. Entre estas medidas se incluye el cifrado de datos tanto en reposo como en tránsito. El cifrado en reposo asegura que los datos almacenados en las bases de datos y otros dispositivos de almacenamiento estén protegidos contra el acceso no autorizado, mientras que el cifrado en tránsito protege los datos que se transmiten entre el sistema y los usuarios o entre diferentes componentes del sistema, previniendo la interceptación de datos durante su transmisión.

Además del cifrado, BOSS implementa la autenticación multifactorial (MFA) para el acceso al sistema. La MFA requiere que los usuarios proporcionen dos o más formas de verificación de identidad antes de acceder al sistema. Esto puede incluir una combinación de contraseñas, tokens de seguridad, y datos biométricos como huellas dactilares o reconocimiento facial. Esta capa adicional de seguridad reduce significativamente el riesgo de acceso no autorizado debido a la pérdida o el robo de credenciales.

El sistema también aplica controles de acceso estrictos basados en roles (RBAC). Estos controles aseguran que los usuarios solo tengan acceso a la información y funciones necesarias para realizar sus tareas específicas. Cada usuario tiene permisos definidos según su rol dentro de la organización, minimizando así el riesgo de acceso indebido a datos sensibles. Las políticas de RBAC son regularmente revisadas y actualizadas para adaptarse a cambios en roles y responsabilidades del personal.

Para detectar y responder rápidamente a intentos de acceso no autorizado, BOSS utiliza monitoreo continuo y registro de todas las actividades. Este monitoreo incluye la supervisión en tiempo real de intentos de acceso, cambios en la configuración del sistema y otras actividades relevantes. Los registros detallados (logs) de todas las acciones realizadas en el sistema son almacenados y analizados para identificar patrones sospechosos o actividades anómalas. Los sistemas de alerta automática notifican al personal de seguridad sobre cualquier actividad sospechosa, permitiendo una respuesta rápida y eficaz.

Además de estas medidas de seguridad, BOSS incluye verificaciones automáticas de cumplimiento para asegurar que los datos enviados cumplan con los requisitos normativos. Estas verificaciones comprueban la precisión y la integridad de la información a través de reglas de validación predefinidas. Por ejemplo, el sistema puede verificar que los nombres, direcciones y números de identificación proporcionados sigan formatos específicos y que no haya campos obligatorios vacíos. Asimismo, BOSS realiza una comparación cruzada de la información con otras bases de datos gubernamentales para identificar y corregir discrepancias, asegurando que los datos sean consistentes y actualizados.

El acceso a BOSS está estrictamente controlado y limitado al personal autorizado, incluyendo agencias de aplicación de la ley, organismos reguladores y personal específico de FinCEN. El control de acceso basado en roles asegura que los usuarios solo puedan acceder a los datos necesarios para sus funciones específicas. Todos los intentos de acceso se registran y auditan regularmente para garantizar el cumplimiento de las políticas de seguridad. BOSS está diseñado para ser interoperable con los sistemas existentes de FinCEN, lo que permite la integración eficiente de la información sobre beneficiarios finales en flujos de trabajo más amplios de cumplimiento e investigación.

Se realizan actualizaciones y mantenimientos regulares para abordar las amenazas de seguridad en evolución, incorporar nuevos requisitos normativos y mejorar la funcionalidad general. Esto incluye parches de software, actualizaciones del sistema y revisiones periódicas de los protocolos de seguridad. El desarrollo y despliegue inicial de BOSS requirieron una inversión significativa en infraestructura de TI, desarrollo de software e integración con sistemas existentes, cubriendo los costos asociados con la adquisición de hardware, soluciones de software personalizadas y medidas iniciales de ciberseguridad. Los costos operativos continuos incluyen el mantenimiento del sistema, la verificación de datos, la supervisión del cumplimiento y la administración

5.2. Estándares abiertos: Beneficial Ownership Data Standard (BODS)

Estándares abiertos

Un estándar abierto es un conjunto de normas, especificaciones y directrices que se desarrollan de manera colaborativa y están disponibles públicamente para su uso y aplicación sin restricciones.

Beneficial Ownership Data Standard

El Beneficial Ownership Data Standard (BODS) de OpenOwnership (https://www.openownership.org/es/) es un estándar abierto diseñado para la recopilación y publicación de datos sobre la propiedad beneficiaria de empresas y entidades. Este estándar tiene como objetivo mejorar la transparencia y la trazabilidad de las estructuras de propiedad corporativa, permitiendo que se identifique a las personas que realmente poseen o controlan una entidad jurídica.

BODS establece una definición clara de términos esenciales como "Propietario Beneficiario", refiriéndose a la persona física que posee o controla una parte significativa de una empresa o entidad, y "Control", que implica la capacidad de influir significativamente en las decisiones de la entidad, ya sea de manera directa o a través de estructuras de propiedad complejas.

El estándar adopta una estructura de datos estandarizada que incluye información detallada sobre entidades jurídicas, como el nombre, tipo, dirección y jurisdicción de registro de la empresa o entidad; datos sobre las personas beneficiarias, incluyendo nombre, fecha de nacimiento, nacionalidad y dirección; y detalles sobre los intereses de propiedad, especificando la naturaleza y el alcance del control o propiedad que una persona tiene sobre la entidad.

Un ejemplo hipotético de estructura JSON en BODS sería el siguiente:

```
{
    "statementID": "1",
    "entityType": "person",
    "person": {
        "name": "Pedro Serrano",
        "birthDate": "1975-05-20",
        "nationality": "CL",
        "address": {
            "streetAddress": "Av. Libertador Bernardo O'Higgins 1234",
            "locality": "Santiago",
            "region": "Region Metropolitana",
            "postalCode": "8320000",
            "country": "CL"
        }
    },
    "interests": [
        {
            "interestID": "interest-1",
            "type": "shareholding",
            "percentage": 55,
            "entity": {
                "name": "Aplicaciones Modernas S.A.",
                "jurisdiction": "CL"
            }
        }
    ]
}
```


Este ejemplo de estructura JSON en BODS describe la información de una persona física, Pedro Serrano, que es beneficiario final de una entidad jurídica en Chile. Pedro Serrano nació el 20 de mayo de 1975 y es de nacionalidad chilena. Su dirección es Av. Libertador Bernardo O'Higgins 1234, en Santiago, Región Metropolitana, con el código postal 8320000. Pedro tiene un interés de propiedad del 55% en una empresa llamada Aplicaciones Modernas S.A., que está registrada en Chile. El ejemplo es meramente ilustrativo y no representa a personas ni a entidades existentes. Cualquier similitud con nombres, direcciones o entidades es completamente casual.

Componentes y tecnologías

BODS emplea JSON (JavaScript Object Notation) para la transmisión de datos estructurados a través de redes. Los archivos JSON de BODS contienen información sobre entidades jurídicas, personas, intereses de propiedad y otras relaciones relevantes, organizadas en una estructura jerárquica y fácilmente navegable.

Los esquemas JSON definen la estructura esperada de los datos, especificando qué campos son obligatorios, qué tipos de datos se permiten en cada campo y otras restricciones. Esto ayuda a garantizar la consistencia y la validez de los datos. Los esquemas JSON también permiten la validación automática de los datos antes de su publicación o procesamiento, lo que reduce errores y asegura la calidad de la información.

OpenOwnership proporciona documentación detallada sobre el estándar BODS, que incluye guías de implementación, ejemplos de datos y tutoriales para ayudar a los desarrolladores y usuarios a comprender y utilizar el estándar. Esta documentación abarca detalles sobre la estructura de los archivos JSON, el significado de cada campo y cómo interpretar las relaciones entre diferentes entidades y personas.

Para facilitar la implementación y el uso del BODS, OpenOwnership ofrece diversas herramientas de software. Entre estas herramientas se encuentran validadores de JSON, que validan los archivos JSON contra los esquemas proporcionados; conversores de datos, que permiten convertir datos de otros formatos como CSV o XML a JSON conforme al estándar BODS; y APIs (Interfaces de Programación de Aplicaciones), que permiten integrar datos de BODS en aplicaciones y sistemas existentes.

El BODS está diseñado para ser interoperable con otros estándares y sistemas de datos abiertos, facilitando la integración con registros comerciales, bases de datos gubernamentales y plataformas de transparencia. El uso de JSON y APIs RESTful permite la transmisión de datos entre diferentes sistemas y plataformas.

Implementación

Diseñado para ser compatible con otros estándares de datos abiertos y marcos de transparencia, BODS facilita la integración y el intercambio de información entre diferentes sistemas y jurisdicciones. Promueve la publicación de datos en formatos abiertos y accesibles, para que puedan ser utilizados por gobiernos, periodistas, investigadores y el público en general. Además, proporciona guías y herramientas para asegurar que los datos recopilados y publicados sean precisos, completos y verificables.

El estándar BODS se ha implementado en varios países alrededor del mundo, con el objetivo de mejorar la transparencia en la propiedad beneficiaria. El Reino Unido adoptó BODS en 2016 como el estándar oficial para la recolección y publicación de datos de propiedad beneficiaria con el objetivo de asegurar datos consistentes, interoperables y de alta calidad. Más recientemente, Canadá ha aprobado en noviembre de 2023 una ley para crear un registro público nacional de propiedad beneficiaria, utilizando BODS para estructurar los datos recopilados y facilitar la integración y el intercambio de información entre diferentes sistemas y jurisdicciones.

5.3. Valoración. Ventajas e inconvenientes de ambos enfoques

Optar por un sistema propietario como el Beneficial Ownership Secure System (BOSS) tiene varias ventajas. Uno de los principales beneficios es la personalización y el control completo que las autoridades gestoras, como FinCEN, pueden tener sobre el sistema. Esto permite que el sistema sea diseñado y modificado específicamente para cumplir con las normativas y requisitos legales de un país determinado, asegurando que la seguridad, la privacidad y la funcionalidad se ajusten perfectamente a las necesidades locales. Además, un sistema propietario puede ser más robusto en términos de seguridad, ya que los desarrolladores tienen control total sobre el código fuente y pueden implementar medidas de protección avanzadas que se ajusten a los estándares más rigurosos.

Sin embargo, optar por un sistema propietario también presenta inconvenientes significativos. Uno de los mayores desafíos es el costo, ya que el desarrollo y mantenimiento de un sistema propietario

pueden ser sustancialmente más elevados en comparación con la adopción de estándares abiertos. Además, los sistemas propietarios pueden limitar la flexibilidad y la innovación, ya que dependen de un único proveedor o desarrollador para las actualizaciones y mejoras, mientras que los estándares abiertos suelen beneficiarse de una comunidad más amplia de desarrolladores y expertos que contribuyen a su evolución continua.

En cuanto a los estándares abiertos como BODS, una de las principales ventajas es, como se ha indicado, la reducción de costos. Al no requerir el pago de licencias, las organizaciones pueden ahorrar significativamente en gastos asociados a la implementación y uso del estándar. Además, los costos de desarrollo son menores, ya que no es necesario crear soluciones personalizadas desde cero, permitiendo a las entidades utilizar y adaptar el estándar abierto disponible públicamente. Los estándares abiertos también promueven la interoperabilidad y la flexibilidad. Al estar diseñados para ser compatibles con una variedad de sistemas y plataformas, facilitan el intercambio de información y la integración entre diferentes entidades y jurisdicciones. Esto permite que los datos sean fácilmente compartidos y reutilizados, lo cual es esencial para la colaboración y la transparencia. Otro beneficio significativo es la innovación y la mejora continua. Una comunidad activa de usuarios y desarrolladores contribuye constantemente a la mejora del estándar, asegurando que se mantenga actualizado y eficaz. Las mejoras y correcciones de errores realizadas por la comunidad son accesibles para todos los usuarios sin costos adicionales. Además, los estándares abiertos fomentan la transparencia, ya que sus especificaciones están disponibles públicamente. Esto permite que cualquier persona pueda auditar y entender el estándar, aumentando la confianza y la transparencia en su uso.

Sin embargo, los estándares abiertos también tienen desventajas. Una de ellas es el soporte y el mantenimiento. Dado que no hay un proveedor propietario, el soporte técnico y el mantenimiento suelen recaer en las organizaciones que adoptan el estándar, lo que puede requerir recursos adicionales. Además, la posibilidad de que surjan múltiples versiones o adaptaciones del estándar puede llevar a problemas de compatibilidad y fragmentación. En términos de seguridad, los estándares abiertos pueden presentar vulnerabilidades, ya que su accesibilidad pública permite que potenciales atacantes también tengan acceso a ellos. Además, a diferencia de los sistemas propietarios, los estándares abiertos no suelen ofrecer garantías y responsabilidades contractuales, lo que puede ser un inconveniente para algunas organizaciones.

6. Control del acceso a los datos de beneficiarios finales

En relación con el régimen de acceso al Registro Nacional de Personas Beneficiarias Finales (RNPBF), el proyecto de ley prevé que se garantizará el acceso a la información pública contenida en el Registro, de forma adecuada, gratuita y oportuna, a través de un portal electrónico estructurado en formato de datos abiertos, de la forma en que determine el Reglamento. El resto de la información contenida en el Registro no será considerada información pública para efectos de lo dispuesto en el artículo primero de la ley N° 20.285, que aprueba la ley de transparencia de la función pública y de acceso a la información de la Administración del Estado.

Los organismos del Estado, en el marco de sus atribuciones legales y para dar cumplimiento a sus funciones, tendrán acceso completo y oportuno a toda la información contenida en el registro cada vez que lo requieran, ingresando directamente al portal, en la forma que determine el Reglamento. El acceso o uso de información del Registro no relacionado con los fines indicados configurará el delito

de acceso ilícito establecido en el artículo 2° de la ley N° 21.459, que establece normas sobre delitos informáticos. Asimismo, se considerará como una falta grave a la probidad y dará lugar a la destitución o cese de funciones del infractor, de acuerdo al estatuto respectivo, sin perjuicio de las demás responsabilidades que correspondan. Siempre se deberá garantizar la trazabilidad de los accesos a la información contenida en el Registro, con el objeto de resguardar su uso únicamente para los fines establecidos.

Se analizan a continuación una serie de opciones regulatorias y técnicas para dar cumplimiento a estas previsiones del proyecto de ley.

6.1. Autenticación multifactorial

MFA

La implementación de la autenticación multifactorial (MFA) para acceder a los registros de beneficiarios finales implica varios pasos clave para mejorar la seguridad y proteger la información sensible. El proceso comienza con una fase de evaluación y planificación, en la que la organización responsable (en este caso, el SII) identifica los grupos de usuarios que necesitan acceso, como funcionarios gubernamentales, organismos reguladores, fuerzas del orden o instituciones financieras autorizadas. A continuación, debe realizarse una evaluación de riesgos de seguridad y determinar el nivel de autenticación apropiado para cada grupo de usuarios. En esta fase se definen políticas y procedimientos para el uso de MFA, incluidos los métodos de autenticación, los procesos de inscripción y los mecanismos de recuperación.

Evaluación y planificación

Riesgos y nivel de autenticación

El siguiente paso implica la selección de soluciones adecuadas de MFA. Los métodos de autenticación se eligen en función de la conveniencia del usuario y los requisitos de seguridad. Los métodos comunes incluyen contraseñas de un solo uso (OTP) enviadas por SMS o correo electrónico, tokens de hardware, autenticadores basados en aplicaciones móviles como Google Authenticator o Authy, y autenticación biométrica, como huellas dactilares y reconocimiento facial. Es crucial garantizar que la solución MFA seleccionada pueda integrarse con la infraestructura de TI existente.

Selección de soluciones

La implementación implica la integración de la solución MFA con la plataforma de registro de beneficiarios finales, utilizando las API proporcionadas por los proveedores de soluciones MFA. Se establece un proceso de inscripción seguro y fácil de usar, donde los usuarios registran sus dispositivos o métodos MFA. Se configuran los ajustes de control de acceso para imponer el uso de MFA al iniciar sesión y durante acciones críticas o acceso a datos.

Integración

La capacitación y la concienciación de los usuarios son vitales para una implementación exitosa. Idealmente, deben llevarse a cabo sesiones de capacitación para familiarizar a los usuarios con el nuevo proceso de autenticación y proporcionar materiales de apoyo, como manuales, preguntas frecuentes y contactos de soporte, para ayudar a los usuarios durante la transición.

Capacitación

El monitoreo y el mantenimiento son procesos continuos. Las auditorías de seguridad regulares deben asegurar que el sistema MFA funcione correctamente y de manera segura. Se establecen protocolos para responder a incidentes relacionados con la autenticación, como tokens perdidos o credenciales comprometidas. El sistema MFA se mantiene actualizado con los últimos parches de seguridad y características para mantener su robustez.

Monitoreo y mantenimiento

Las mejores prácticas para la implementación de MFA incluyen el uso de métodos de autenticación sólidos, como biometría o autenticadores basados en aplicaciones, en lugar de métodos menos seguros como OTP basados en SMS. La combinación de MFA con otras medidas de seguridad, como el cifrado, auditorías regulares y educación del usuario, mejora la seguridad general. Es esencial equilibrar la seguridad con la conveniencia del usuario para asegurar el cumplimiento y reducir la resistencia al nuevo sistema. Se debe asegurar el cumplimiento de los requisitos legales y regulatorios pertinentes para la protección y privacidad de los datos durante todo el proceso.

Como vimos, en la sección anterior, el sistema BOSS de FinCEN prevé el uso de MFA para el acceso al registro de beneficiarios finales. Otros portales gubernamentales norteamericanos utilizan asimismo MFA para asegurar el acceso a información sensible. Un ejemplo destacado es el uso de tarjetas de Verificación de Identidad Personal (PIV), que son tarjetas inteligentes emitidas a empleados federales y contratistas como parte del Estándar Federal de Procesamiento de Información (FIPS) 201. Las tarjetas PIV están integradas con circuitos que almacenan certificados digitales encriptados, lo que permite un acceso seguro y autenticado a redes e instalaciones federales. Los usuarios deben insertar su tarjeta PIV en un lector de tarjetas e ingresar su PIN para autenticar su identidad. Además, muchos sistemas federales incorporan verificación biométrica, como huellas dactilares o reconocimiento facial, como una capa adicional de seguridad. Así, el personal del DHS (Departamento de Seguridad Nacional) utiliza tarjetas PIV junto con verificación biométrica para garantizar un acceso seguro y conforme a los datos y sistemas críticos. Este enfoque multifacético asegura que, incluso si una tarjeta PIV se pierde o es robada, el acceso no autorizado sigue siendo difícil sin el PIN y los datos biométricos correspondientes.

Recomendación

En el caso de Chile, si bien se prevén métodos robustos de acceso al portal del SII (Certificado Digital, RUT y Clave Tributaria, y ClaveÚnica), se recomienda valorar la implantación de un sistema MFA para el Registro de Personas Beneficiarias Finales (RPBF), especialmente en el supuesto de consultas de información de carácter no público por funcionarios de organismos del Estado.

6.2. Control de acceso basado en roles

RBAC

El sistema de control de acceso basado en roles (RBAC) es una metodología de seguridad informática que asigna permisos de acceso a usuarios según los roles específicos que desempeñan dentro de una organización. Este enfoque asegura que los usuarios solo tengan acceso a la información y funciones necesarias para realizar sus tareas específicas, evitando el acceso no autorizado a datos y recursos sensibles. En un sistema RBAC, cada usuario es asignado a uno o más roles, y cada rol tiene un conjunto predefinido de permisos que determinan qué operaciones puede realizar y a qué datos puede acceder el usuario. Por ejemplo, un empleado del departamento de recursos humanos puede tener acceso a los datos de los empleados, mientras que un contador puede acceder a los registros financieros de la empresa. La implementación de RBAC implica la definición de roles y permisos, la asignación de usuarios a roles, y el mantenimiento y revisión regular de las políticas de acceso para adaptarse a cambios en la estructura organizacional. Además, se monitorean y auditan las actividades de los usuarios para detectar y prevenir el acceso indebido.

El RBAC es especialmente apropiado para cumplir con las previsiones del proyecto de ley en materia de acceso al Registro Nacional de Personas Beneficiarias Finales (RNPBF), particularmente en relación con la información de carácter no público. Al aplicar RBAC, se asegura que solo los usuarios con roles

autorizados puedan acceder a la información del Registro, minimizando el riesgo de uso indebido o no autorizado. Cada rol tiene permisos claramente definidos que se revisan y actualizan regularmente para reflejar cambios en los roles y responsabilidades del personal. Esto garantiza que solo aquellos usuarios que necesitan acceso a ciertos datos para cumplir con sus responsabilidades laborales puedan hacerlo, reduciendo significativamente la posibilidad de acceso ilícito.

Fases

La implementación técnica de RBAC comienza con una evaluación y planificación que incluye el análisis de requisitos y la definición de objetivos de seguridad. Luego se definen los roles y permisos, identificando los roles necesarios y asignando permisos específicos a cada uno. Los usuarios se asignan a estos roles basándose en sus funciones y responsabilidades. La configuración del sistema RBAC en el software de gestión de identidad y acceso (IAM) utilizado por la organización es el siguiente paso, integrando el sistema con las aplicaciones y sistemas existentes. Se realizan pruebas de funcionalidad y seguridad para asegurar que los roles y permisos se han configurado correctamente y que no hay vulnerabilidades. El monitoreo y auditoría continuos permiten detectar y prevenir accesos no autorizados, registrando todas las actividades y realizando auditorías regulares. Finalmente, se revisan y actualizan regularmente los roles y permisos para adaptarse a cambios en la estructura organizacional, y se capacita a los usuarios sobre las políticas de acceso y la importancia de seguir los procedimientos de seguridad.

La implementación de RBAC facilita la asignación clara de responsabilidades, permitiendo identificar rápidamente al responsable en caso de acceso no autorizado, lo cual es crucial para aplicar las sanciones adecuadas según el estatuto respectivo, incluyendo el cese de funciones del infractor. Este enfoque no solo mejora la seguridad al limitar el acceso a datos sensibles a solo aquellos usuarios que realmente necesitan acceder a ellos, sino que también simplifica la administración de permisos y reduce la posibilidad de errores humanos que pueden ocurrir cuando los permisos se gestionan de manera manual y ad-hoc. En resumen, RBAC proporciona un marco sólido y efectivo para gestionar el acceso a la información del Registro de personas beneficiarias finales, garantizando el cumplimiento de las normativas legales y protegiendo los datos sensibles contra el acceso ilícito.

6.3. Accesos no autorizados

Para detectar y responder rápidamente a intentos de acceso no autorizado, se recomienda implementar un sistema de monitoreo continuo y registro de todas las actividades dentro del sistema. Este monitoreo debe incluir la supervisión en tiempo real de varios aspectos críticos, como los intentos de acceso al sistema, los cambios en la configuración del sistema, la modificación de datos y otras actividades relevantes que puedan indicar un posible riesgo de seguridad. Se sugiere utilizar herramientas avanzadas de detección de intrusiones y análisis de comportamiento para rastrear todas las interacciones con el sistema en tiempo real. Los Sistemas de Detección de Intrusiones (IDS) monitorean el tráfico de red y las actividades del sistema en busca de comportamientos sospechosos que puedan indicar una intrusión o un ataque. Existen dos tipos principales de IDS: basados en red (NIDS) y basados en host (HIDS). Los NIDS supervisan el tráfico de red en tiempo real, mientras que los HIDS monitorean las actividades y eventos en los dispositivos individuales. Los IDS utilizan firmas conocidas de ataques y análisis heurístico para identificar posibles amenazas; por ejemplo, pueden detectar intentos de acceso repetidos que podrían ser indicativos de un ataque de fuerza bruta.

IDS

Los Sistemas de Prevención de Intrusiones (IPS) no solo detectan amenazas como los IDS, sino que también toman medidas para prevenir o mitigar estas amenazas en tiempo real. Al integrarse directamente en la red o el sistema, los IPS pueden bloquear automáticamente el tráfico sospechoso, detener procesos maliciosos y realizar otras acciones defensivas. Esta capacidad de respuesta inmediata es crucial para minimizar el impacto de posibles ataques. El análisis de comportamiento y las herramientas de analítica avanzada complementan a los IDS/IPS al proporcionar una capa adicional de protección basada en el monitoreo y análisis continuo de las actividades del sistema y de los usuarios. Las soluciones de Análisis de Comportamiento de Usuarios y Entidades (UEBA) se centran en identificar comportamientos anómalos al analizar patrones normales de actividad de los usuarios y entidades dentro del sistema. Utilizan algoritmos de aprendizaje automático y análisis estadístico para establecer una línea base del comportamiento normal, y cualquier desviación significativa de esta línea base genera una alerta. Por ejemplo, si un usuario que normalmente accede al sistema durante el horario laboral comienza a acceder en horas inusuales o desde ubicaciones geográficas atípicas, el sistema UEBA generará una alerta para una investigación más profunda.

IPS

UEBA

Las plataformas de Monitoreo de Seguridad de la Información y Gestión de Eventos (SIEM) recopilan y analizan datos de múltiples fuentes dentro del entorno de TI, incluyendo registros de actividad, alertas de IDS/IPS y eventos de red. Los SIEM ofrecen una vista consolidada y en tiempo real de la seguridad del sistema, facilitando la detección de amenazas complejas y proporcionando herramientas para la correlación de eventos y análisis forense. Implementar un SIEM permite a los equipos de seguridad tener una visión integral y proactiva de la postura de seguridad del sistema, identificando patrones que podrían pasar desapercibidos en una vigilancia fragmentada. Es crucial almacenar los registros detallados (logs) de todas las acciones realizadas en el sistema en un repositorio seguro y analizarlos de manera continua. Estos logs deben incluir información detallada sobre quién hizo qué, cuándo y desde dónde. Al analizar estos registros, se podrán identificar patrones sospechosos o actividades anómalas que podrían indicar un intento de acceso no autorizado o una violación de seguridad.

SIEM

Para mejorar la eficiencia en la detección de actividades sospechosas, se recomienda utilizar sistemas de alerta automática. Estos sistemas deben configurarse para enviar notificaciones instantáneas al personal de seguridad cuando se detecte cualquier actividad que cumpla con ciertos criterios predefinidos de riesgo. Las alertas pueden enviarse por correo electrónico, mensajes de texto o a través de aplicaciones de mensajería segura. Estas notificaciones deben incluir detalles sobre la actividad sospechosa, permitiendo al personal de seguridad evaluar rápidamente la situación y tomar las medidas adecuadas. Se recomienda implementar una combinación de IDS, IPS, UEBA y SIEM para proporcionar una protección integral y en profundidad. Estas herramientas deben configurarse para trabajar juntas, proporcionando alertas en tiempo real y capacidades de respuesta automatizada. Por ejemplo, al detectar un comportamiento anómalo, el sistema UEBA puede notificar al SIEM, que correlacionará este evento con otros datos para determinar si se trata de una amenaza real. Si el SIEM confirma la amenaza, puede instruir al IPS para que bloquee el tráfico relacionado o aísle la parte comprometida del sistema.

Al adoptar estas herramientas avanzadas de detección de intrusiones y análisis de comportamiento, se asegura una protección robusta contra accesos no autorizados y actividades maliciosas, garantizando la integridad y seguridad del sistema de gestión de datos de beneficiarios finales.

Además, la implementación de RBAC complementará estas prácticas al asegurar que solo los usuarios con roles autorizados puedan acceder a la información crítica, estableciendo una defensa en profundidad contra accesos no autorizados y mejorando la seguridad global del sistema.

6.4. Seguridad Informática General

Además de las medidas de control de acceso, es fundamental implementar cifrado de datos tanto en reposo como en tránsito para proteger la información sensible contra accesos no autorizados e interceptaciones. También es crucial contar con un sistema robusto de copias de seguridad y planes de recuperación ante desastres para garantizar la continuidad del registro y la recuperación de datos en caso de fallos del sistema o ciberataques. Mantener todos los sistemas y software actualizados con los últimos parches de seguridad es esencial para proteger contra vulnerabilidades conocidas. La capacitación continua y la concienciación sobre seguridad para todos los usuarios aseguran que se sigan las mejores prácticas y se mantengan las políticas de seguridad de la organización. Finalmente, realizar evaluaciones de seguridad regulares y pruebas de penetración ayuda a identificar y mitigar posibles vulnerabilidades en el sistema, proporcionando una capa adicional de protección para el registro de beneficiarios finales. Estas medidas, junto con las prácticas de control de acceso mencionadas anteriormente, aseguran una protección integral de la información sensible, cumpliendo con las previsiones legales establecidas en la ley N° 21.459 de Chile y garantizando que el acceso a la información del Registro Nacional de Personas Beneficiarias Finales (RNPBF) se realice de manera segura y conforme a la normativa.

7. Costes del registro

Los costes de implementación y operación de un registro de beneficiarios finales pueden variar significativamente en función de diversos factores, como el tamaño de la jurisdicción, la cantidad de empresas que alberga, los servicios específicos que planea ofrecer y la manera en que se ponen a disposición los datos. La cantidad de empresas registradas es un factor crucial que afecta directamente la complejidad y el costo del sistema. Jurisdicciones como los Estados Unidos o el Reino Unido requieren sistemas escalables para asegurar que todos los datos se manejen adecuadamente, lo que puede aumentar significativamente los costos iniciales de configuración y los costos operativos continuos. Los servicios ofrecidos también influyen en los costos. Si el registro proporciona funcionalidades avanzadas, como búsquedas complejas, informes detallados y accesos en tiempo real, el costo de desarrollo y mantenimiento será mayor. Además, ofrecer acceso gratuito o de bajo costo al público en general puede incrementar el uso del sistema, lo que a su vez puede requerir una mayor capacidad de procesamiento y almacenamiento. La manera en que los datos se ponen a disposición también es un factor determinante. Si el registro de beneficiarios finales está diseñado para ser accesible en línea, la seguridad se convierte en una prioridad, lo que implica costos adicionales en ciberseguridad, como la implementación de medidas de autenticación multifactorial, cifrado de datos y sistemas de detección y prevención de intrusiones. Además, la integración con otras bases de datos gubernamentales y la interoperabilidad con sistemas internacionales también pueden incrementar los costos.

7.1. Chile. Informe Financiero sobre el proyecto de ley

Chile

El proyecto de ley que crea un registro de personas beneficiarias finales ha sido objeto de un Informe Financiero de la Dirección de Presupuestos del Ministerio de Hacienda (I.F. N°276/15.12.2023). El

Informe señala que la creación del registro implicará la creación de un Departamento de Personas Beneficiarias Finales en el Servicio de Impuestos Internos (SII) conformado por 11 funcionarios con un mayor gasto fiscal en el año 4 de 686.498 miles de $ de 2023. Asimismo, la creación del registro de personas beneficiarias finales implicará un costo transitorio en desarrollo de sistemas informáticos, así como costos permanentes en almacenamiento en la nube. El informe concluye que la implementación del proyecto de ley irrogará un mayor gasto fiscal de $583.063 miles al primer año presupuestario desde su publicación, y de $884.498 miles en régimen.

7.2. Ejemplos comparados

Reino Unido

En el Reino Unido, según los datos del Departamento de Negocios, Energía y Estrategia Industrial (BEIS), los costos de implementación del Registro de Personas con Control Significativo (PSC) se situaron en £48,5 millones (aproximadamente, 63 millones de USD) y los costos anuales superan los £10 millones (aproximadamente, 13 millones de USD) para el mantenimiento y acceso al registro.

Australia

En Australia, el último presupuesto federal asigna $41,7 millones en el periodo 2024-2028 y $9,6 millones anuales de forma continua al Tesoro, la Comisión Australiana de Valores e Inversiones (ASIC) y el Departamento del Fiscal General para regular y apoyar los nuevos requisitos de transparencia para las empresas australianas y otras entidades. Consecuentemente, se prevé un gasto de implementación a lo largo de cuatro años de 41,7 millones de dólares australianos (aproximadamente, 27,5 millones de USD) y un gasto recurrente anual de 9,6 millones de dólares australianos (aproximadamente, 6,3 millones de USD).

Países Bajos

En los Países Bajos, los costos de implementación del registro de beneficiarios finales (UBO-register) se presupuestaron en 9 millones de euros (aproximadamente, 9,7 millones de USD) de una sola vez, y posteriormente 600,000 euros anuales (aproximadamente, 650.000 USD) de manera continua (Evaluación de la implementación del registro UBO, Belastingdienst). Más allá de esta estimación, no constan publicadas cifras actualizadas respecto del coste real anual de mantenimiento del UBO-register dado que se engloba dentro del presupuesto general de la Cámara de Comercio de los Países Bajos (Kamer van Koophandel, KvK). Aunque la gestión del UBO-register junto al resto de la información mercantil puede haber dado lugar a una reducción de costes, la cifra estimada se aleja notablemente de la de otros ejemplos comparados por lo que pudiera no incorporar todos los costes asociados.

España

En España, la estimación de costes de creación del Registro de Titularidades Reales contenida en la memoria de análisis de impacto normativo (MAIN) se sitúa en 2.060.000 euros (aproximadamente, 2,3 millones de USD) desglosados en 220.00 euros (gestión de proyecto: 1 gerente de proyecto, 2 junior), 1.120.000 euros (gestión interna del registro / herramientas de gestión: 5 analistas de procesos, 5 programadores, 1 profesional de experiencia de usuario (UX), interconexión con otros registros) y 720.000 euros (interfaces). Asimismo, se prevé que la Dirección General de Transformación Digital de la Administración de Justicia tendrá que tramitar y supervisar el contrato de mantenimiento, desarrollo y CAU de la aplicación del Registro, así como la adquisición y renovación del software y hardware necesario, para lo cual deberá reservarse en los presupuestos del Ministerio de Justicia el crédito necesario al efecto. Dichas necesidades se cuantifican anualmente en 2.345.000 euros, desglosados en desarrollo / evolutivos (515.000 euros), mantenimiento / correctivos (515.000 euros), CAU / atención a incidencias (515.000 euros) y adquisición y renovación del SW y HW necesario (800.000

euros). En relación con estos costes, debe tenerse en cuenta que el registro creado en el Ministerio de Justicia de España supone fundamentalmente la centralización de la información ya existente en el Registro de Titulares Reales del Centro Registral Anti- Blanqueo y en la Base de Datos de Titularidad Real del Órgano Centralizado de Prevención del Consejo General del Notariado. Consecuentemente, en la medida en que el Registro de Titularidades Reales español se limita a centralizar información previamente obtenida por notarios y registradores, sus costes de establecimiento y operación serían substancialmente inferiores al previsto Registro Nacional de Personas Beneficiarias Finales (RNPBF) de Chile que deberá recibir, validar y gestionar la información remitida directamente por las personas y entidades obligadas a informar de conformidad con el artículo 4 del proyecto de ley.

En cuanto a los recursos humanos adscritos al Registro de Titularidades Reales, la MAIN los estima en siete (7) funcionarios a tiempo completo (1 Coordinador/Coordinadora de Área N29, 1 Jefe/Jefa de Área N28, 3 Jefes/Jefas de Servicio N26 y 2 Jefes/Jefas de Sección N22). Los costes de dicho personal se cuantifican anualmente en 325.012,64 euros (desglosados en 258.562,16 euros de retribuciones y 66.450,48 euros de cargas sociales). Además del personal administrativo directamente asignado al registro, se prevé la necesidad de contar con un equipo estable de técnicos informáticos, integrado por tres (3) funcionarios a tiempo completo (1 Jefe/Jefa de Área de Tecnologías para la coordinación y relaciones con colectivos N28, 1 Jefe/Jefa de Servicio de Tecnologías para los Registros N26, 1 Jefe/Jefa de Sección de Tecnologías para los Registros N24) con un coste anual de 148.360,67 euros (118.027,58 euros en concepto de retribuciones y 30.333,09 de cargas sociales). La MAIN indica asimismo que la Dirección General de Seguridad Jurídica y Fe Pública tendrá que tramitar y supervisar el contrato para prestar un servicio de tareas de apoyo al Registro de Titularidades Reales, consistentes fundamentalmente en la recepción, comprobación, grabación, consolidación y depuración de datos en el mismo, así como en la cumplimentación o comprobación de datos en modelos de propuesta. Se prevé que será necesario un equipo de aproximadamente 6 recursos externos (cuyo coste anual se puede cifrar en 300.000 euros) para la realización de las citadas tareas. Adicionalmente, para la ejecución del contrato de mantenimiento, desarrollo y CAU de la aplicación supervisado por la Dirección General de Transformación Digital de la Administración de Justicia se prevé que será necesario un equipo de aproximadamente 18 recursos externos que se encargará de mantener la información y realizar los análisis. Consecuentemente, los recursos humanos previstos para el Registro de Titularidades Reales español se situarían en dieciséis (16) personas a tiempo completo (7 funcionarios administrativos, 3 técnicos informáticos y 6 recursos externos) a los que habría que sumar los dieciocho (18) recursos externos del contrato de mantenimiento. Nuevamente, debe hacerse la salvedad de que el establecimiento y gestión del registro español presenta un nivel de complejidad substancialmente inferior al de previsto RNPBF chileno.

Los costes anteriores pueden sistematizarse en el siguiente cuadro:

	Coste de implementación	Coste anual
Reino Unido	48.500.000 GBP / 63.000.000 USD	10.000.000 GBP / 13.000.000 USD
Australia	41.700.000 AUD / 27.454.000 USD	9.600.000 AUD / 6.320.000 USD
Países Bajos	9.000.000 EUR / 9.700.000 USD	600.000 EUR / 650.000 USD
España	2.060.000 EUR / 2.228.000 USD	3.118.374 EUR / 3.365.000 USD

Además de estimar los costos para el Estado derivados de la implementación de registros de beneficiarios finales, es relevante desde una perspectiva de buena regulación considerar también los costos para las empresas. Estos costos pueden influir en el cumplimiento y la efectividad del sistema de registro. En los Estados Unidos, FinCEN ha estimado que el costo para una empresa de preparar y enviar un informe inicial de Información de Propietario Beneficiario (BOI) es aproximadamente 85 dólares, estimación que se basa en varios factores clave. Primero, incluye el tiempo requerido para que las empresas recopilen la información necesaria, lo cual implica identificar a todos beneficiarios finales que poseen o controlan el 25% o más de la empresa. Este proceso puede requerir revisar los registros de la sociedad y consultar con asesores legales o financieros para asegurar que todos los datos sean precisos y estén actualizados. Segundo, la estimación considera el esfuerzo administrativo necesario para completar el informe de BOI, que implica rellenar los formularios con información detallada sobre cada beneficiario final, como su nombre, fecha de nacimiento, dirección y números de identificación. FinCEN proporciona directrices y plantillas para facilitar este proceso. Tercero, el costo incluye el proceso de envío del informe a través del portal en línea de FinCEN, diseñado para minimizar el tiempo y esfuerzo requeridos para el cumplimiento.

En el diseño del Registro Nacional de Personas Beneficiarias Finales (RNPBF) de Chile sería conveniente estimar y tener en cuenta los costos para las empresas al evaluar distintas alternativas de desarrollo reglamentario. Esto asegurará que el sistema no solo sea efectivo en términos de cumplimiento y transparencia, sino también manejable y accesible para las empresas, especialmente las pequeñas, que forman una parte significativa de la economía del país.

7.3. Factores a considerar en la estimación de costos

Los costos de implementación y operación de un Registro Nacional de Personas Beneficiarias Finales (RNPBF) en Chile, gestionado por el Servicio de Impuestos Internos (SII), pueden ser significativos, abarcando diversos componentes cruciales que aseguran la eficacia y seguridad del sistema. La configuración y desarrollo de software a medida es un factor importante, que incluye el diseño de la plataforma, el desarrollo de aplicaciones y la personalización según las necesidades específicas del registro. Este proceso requiere una inversión considerable en ingenieros de software y diseñadores que puedan crear un sistema robusto y seguro.

La integración del registro con otras bases de datos y sistemas gubernamentales es esencial para asegurar que la información se pueda compartir y verificar eficazmente entre diferentes entidades. Esta integración puede implicar la utilización de APIs y otras tecnologías de interconexión para garantizar que los datos sean consistentes y accesibles en tiempo real, permitiendo al SII y a otras entidades gubernamentales realizar consultas y cruces de datos de manera eficiente.

La infraestructura de seguridad es otro componente crítico, incluyendo la implementación de medidas como el cifrado, la autenticación multifactorial (MFA) y sistemas de detección de intrusiones (IDS) para proteger la información sensible contra accesos no autorizados y ciberataques. Estas medidas son fundamentales para mantener la integridad y confidencialidad de los datos de los beneficiarios finales. Además, es necesario realizar auditorías de seguridad regulares para identificar y corregir vulnerabilidades, asegurando que el SII pueda cumplir con los más altos estándares de seguridad.

Los costos de hardware e infraestructura abarcan la configuración de servidores, soluciones de almacenamiento y equipos de red. En muchos casos, también se considera la utilización de servicios en la nube para el almacenamiento y procesamiento de datos, lo que puede ofrecer ventajas en términos de escalabilidad y flexibilidad. Sin embargo, estos servicios también implican costos continuos que deben ser considerados en el presupuesto operativo del SII.

La gestión de proyectos y la contratación de personal especializado son esenciales para el éxito del proyecto, incluyendo gerentes de proyectos, desarrolladores de software y personal de soporte técnico. Estos profesionales no solo supervisan el desarrollo e implementación del sistema, sino que también aseguran que se cumplan los plazos y se respeten los presupuestos. La capacitación continua del personal y el soporte técnico para los usuarios del sistema son también aspectos importantes a considerar para garantizar que todos los involucrados comprendan cómo utilizar el sistema de manera efectiva y segura.

Los gastos de cumplimiento y legales son necesarios para garantizar que el sistema cumpla con todos los requisitos regulatorios y normativos. Estos pueden incluir la consultoría legal, auditorías de cumplimiento y la implementación de políticas y procedimientos adecuados. Cumplir con las normativas internacionales y locales es crucial para la aceptación y uso del registro por parte de todas las partes interesadas.

Los costos operativos anuales incluyen el mantenimiento continuo del sistema, las actualizaciones de software y el soporte técnico necesario para mantener el registro funcionando de manera eficiente. El mantenimiento regular asegura que el sistema permanezca actualizado y libre de errores, mientras que las actualizaciones pueden agregar nuevas funcionalidades o mejorar las existentes. También es importante considerar los costos para gestionar y almacenar los datos de manera segura, así como las auditorías regulares de seguridad y cumplimiento para asegurar que el registro permanezca protegido y conforme a las normativas vigentes.

En resumen, los costos iniciales de implementación de un Registro Nacional de Personas Beneficiarias Finales (RNPBF) gestionado por el Servicio de Impuestos Internos (SII) en Chile y los costos operativos anuales pueden variar considerablemente en función de los requisitos específicos, la escala del proyecto y otros factores únicos de la implementación. Es fundamental realizar un análisis detallado de costos por parte de expertos relevantes o una firma de consultoría para obtener una estimación precisa y planificar adecuadamente la inversión necesaria.

8. Seguridad de los datos

La seguridad en la transmisión de datos sensibles es un aspecto fundamental en el diseño e implementación de un registro de beneficiarios finales. Garantizar que los datos transmitidos entre los usuarios y el registro estén protegidos contra accesos no autorizados y ciberataques es esencial para mantener la confidencialidad, la integridad y la disponibilidad de la información. Dado que una posible filtración o acceso indebido a estos datos podría tener consecuencias graves, la implementación de medidas de seguridad robustas es prioritaria.

Uno de los principales estándares para proteger la comunicación en redes informáticas es el protocolo TLS (Transport Layer Security). Este protocolo criptográfico proporciona cifrado, autenticación y preservación de la integridad de los datos transmitidos entre un navegador y un servidor. En el caso

de los registros de beneficiarios finales, TLS garantiza que la información sensible, como identificaciones, datos financieros, documentos legales o cualquier otro dato personal relacionado con los beneficiarios finales, esté protegida frente a interceptaciones, manipulaciones o accesos no autorizados. Dada su efectividad y amplia aceptación internacional, TLS es la base de confianza en sistemas que manejan datos críticos y se utiliza comúnmente en sectores como el bancario, el comercio electrónico y el gobierno electrónico. Su implementación en un registro de beneficiarios finales asegura el cumplimiento de estándares de seguridad reconocidos globalmente.

Como se ha indicado anteriormente, el diseño e implementación de un registro de beneficiarios finales también requiere considerar medidas complementarias para garantizar una protección integral. Además de TLS para la transmisión de datos, es necesario implementar cifrado en reposo para los datos almacenados, protegiéndolos incluso si los sistemas o bases de datos son comprometidos. De igual forma, es esencial establecer mecanismos de autenticación robustos, como autenticación multifactorial (MFA), para prevenir accesos no autorizados, tanto por parte de usuarios internos como externos.

Si bien existen otros protocolos de seguridad como IPSec o SSH, estos tienen aplicaciones más específicas y no son necesariamente los más adecuados para un registro de beneficiarios finales. IPSec, por ejemplo, es útil para garantizar la seguridad de redes privadas virtuales (VPNs) en entornos corporativos, mientras que SSH es más relevante para accesos remotos y transferencias seguras de archivos. En el contexto de un registro de beneficiarios finales, el enfoque debe centrarse en tecnologías como TLS, que están diseñadas específicamente para proteger la transmisión de datos entre usuarios y servidores en entornos públicos o semipúblicos.

Además de las medidas técnicas, un registro efectivo debe estar respaldado por políticas y procesos sólidos de gestión de riesgos. Esto incluye la realización de auditorías de seguridad periódicas, la implementación de planes de respuesta ante incidentes, y la capacitación continua de los empleados y administradores del sistema sobre mejores prácticas en ciberseguridad. La protección de los datos no se limita a la tecnología, sino que también depende de la correcta gestión y supervisión del sistema.

En última instancia, la implementación de un registro seguro no solo protege los datos sensibles frente a ataques malintencionados, sino que también promueve la confianza de las partes interesadas en el sistema, incluyendo los organismos estatales, las empresas y la sociedad civil.

9. Actualización y rectificación de la información

Un aspecto clave del éxito de un registro de beneficiarios finales radica en asegurar que la información contenida en el mismo sea en todo momento relevante y exacta. A estos efectos, es importante imponer legalmente la obligación de las personas o entidades declarantes de (i) actualizar la información declarada cuando se produzcan cambios sustantivos en la misma y (ii) corregir la información previamente remitida cuando resulte inveraz o inexacta.

Así, en los Estados Unidos, además de presentar un informe inicial de información de beneficiarios finales (BOI, por sus siglas en inglés), las empresas declarantes deben, en su caso, actualizar y corregir la información de los informes BOI presentados anteriormente. Asimismo, las personas físicas que obtienen identificadores FinCEN deben actualizar y corregir la información declarada previamente ante FinCEN. Consiguientemente, se distingue entre informes actualizados (que son obligatorios

cuando se produce un cambio en la información sobre la propia empresa declarante o sus beneficiarios finales) e informes corregidos (que son obligatorios cuando la información declarada era inexacta al declararse y sigue siendo inexacta).

Si hay algún cambio a la información requerida sobre la empresa o sus beneficiarios finales en un informe BOI presentado, la empresa debe presentar un informe BOI actualizado a más tardar 30 días después de la fecha en que se produjo el cambio. El mismo plazo de 30 días se aplica a los cambios en la información presentada por una persona física para obtener un identificador FinCEN. Una empresa que informa no está obligada a presentar un informe actualizado en caso de que se produzcan cambios en la información personal previamente declarada sobre un solicitante de una empresa. Los siguientes son algunos ejemplos de cambios que requerirían un informe BOI actualizado: (i) Cualquier cambio en la información declarada para la empresa que informa, como la alteración de su razón social. (ii) Un cambio en los beneficiarios finales, como una venta que modifique quién alcanza el umbral de participación del 25 %, o el fallecimiento de un beneficiario final. Si fallece un beneficiario final y se producen cambios en la lista de beneficiarios finales de la empresa que informa, dichos cambios deben notificarse en un plazo de 30 días a partir de la fecha de liquidación de la herencia del beneficiario final fallecido. En la medida en que corresponda, el informe actualizado deberá identificar a los nuevos beneficiarios finales. (iii) Cualquier cambio en el nombre, la dirección o el número de identificación único de un beneficiario final declarado en un informe BOI. Si un beneficiario final obtiene un nuevo permiso de conducir u otro documento de identificación que incluya el cambio de nombre, dirección o número de identificación, la empresa que informa también tendría que presentar un informe actualizado de información sobre beneficiarios finales ante FinCEN, incluyendo una imagen del nuevo documento de identificación. Cuando un beneficiario final que era menor de edad alcanza la mayoría de edad, debe presentarse un informe BOI actualizado, identificando a la persona como beneficiario final y, si se justifica, sustituyendo la información de su padre o tutor legal por la propia.

Al igual que los informes BOI iniciales, los informes BOI actualizados deben presentarse de forma electrónica a través del sistema presentación seguro. Por el contrario , no es obligatorio declarar el cese de actividad o la disolución de una empresa.

En cuanto a los informes corregidos, si se detecta una inexactitud en un informe BOI que presentó una empresa, ésta debe corregirla a más tardar 30 días después de la fecha en que la empresa tuvo conocimiento de la inexactitud o tuvo motivos para conocerla. Esto incluye cualquier inexactitud en la información requerida proporcionada sobre la empresa, sus beneficiarios finales o las personas solicitantes. El mismo plazo de 30 días se aplica a las inexactitudes en la información presentada por una persona física para obtener un identificador FinCEN. No hay sanciones por presentar un informe BOI inexacto siempre que se corrija en un plazo de 90 días naturales a partir de su presentación. Los informes BOI corregidos deben remitirse de forma electrónica a través del sistema de presentación seguro.

Anexo 1. Registros de beneficiarios finales. Cuadro resumen

Jurisdicción	Registro	Agencia	Acceso
1. Estados Unidos	Sí	FinCEN	Limitado
2. China	En curso	PBOC / SAMR	Limitado
3. Japón	No	-	-
4. Alemania	Sí	Bundesverwaltungsamt (BVA)	Limitado
5. Reino Unido	Sí	Companies House	Accesible
6. Francia	Sí	Registre du Commerce et des Sociétés (RCS)	Limitado
7. India	No	-	-
8. Italia	Sí	Registro delle Imprese	Limitado
9. Canadá	Sí	Corporations Canada	Limitado
10. Corea del Sur	No	-	-
11. Rusia	No	-	-
12. Australia	En curso	Securities and Investments Commission (ASIC)	Limitado
13. Brasil	Sí	Receita Federal de Brasil (RFB)	Limitado
14. España	Sí	Ministerio de Justicia	Limitado
15. México	No	-	-
16. Indonesia	Sí	Ministerio de Justicia y Derechos Humanos	Limitado
17. Países Bajos	Sí	Kamer van Koophandel (KvK)	Limitado
18. Suiza	No	-	-
19. Arabia Saudita	No	-	-
20. Turquía	Sí	Gelir İdaresi Başkanlığı (GIB)	Limitado
21. Argentina	En curso	AFIP / ARCA	Limitado
22. Suecia	Sí	Bolagsverket	Limitado
23. Tailandia	No	-	-
24. Polonia	Sí	Ministerio de Finanzas	Limitado
25. Bélgica	Sí	Servicio Público Federal de Finanzas	Limitado
26. Noruega	Sí	Brønnøysundregistrene	Limitado
27. Austria	Sí	WKO	Limitado
28. Emiratos (EAU)	Sí	Ministerio de Economía	Limitado
29. Hong Kong	No	-	-
30. Singapur	No	-	-

Anexo 2. Evaluaciones Mutuas. Calificaciones

1. Iniciales (MER)

Jurisdicción	Fecha	RI 5	REC 24	REC 25
1. Estados Unidos	2016	Bajo	NC	PC
2. China	2019	Bajo	NC	NC
3. Japón	2021	Moderado	PC	PC
4. Alemania	2022	Moderado	PC	LC
5. Reino Unido	2018	Sustancial	LC	C
6. Francia	2022	Sustancial	LC	LC
7. India	2024	Sustancial	LC	LC
8. Italia	2016	Sustancial	LC	LC
9. Canadá	2016	Bajo	PC	NC
10. Corea del Sur	2020	Moderado	PC	LC
11. Rusia	2019	Sustancial	LC	PC
12. Australia	2015	Moderado	PC	NC
13. Brasil	2023	Moderado	PC	PC
14. España	2014	Sustancial	LC	LC
15. México	2018	Moderado	PC	LC
16. Indonesia	2023	Moderado	LC	PC
17. Países Bajos	2022	Moderado	LC	LC
18. Suiza	2016	Moderado	LC	LC
19. Arabia Saudita	2018	Moderado	LC	LC
20. Turquía	2019	Moderado	PC	PC
21. Argentina	2024	ND	ND	ND
22. Suecia	2017	Moderado	PC	PC
23. Tailandia	2017	Bajo	PC	PC
24. Polonia	2021	Sustancial	LC	LC
25. Bélgica	2015	Moderado	LC	LC
26. Noruega	2014	Moderado	PC	PC
27. Austria	2016	Moderado	PC	PC
28. Emiratos (EAU)	2020	Bajo	LC	PC
29. Hong Kong	2019	Moderado	LC	PC
30. Singapur	2016	Moderado	PC	PC

NOTA: Las calificaciones son las correspondientes a Informe de Evaluación Mutua inicial

2. Actualizadas (tras un FUR, en su caso)

Jurisdicción	Fecha	RI 5	REC 24	REC 25
1. Estados Unidos	2024	Bajo	LC	PC
2. China	2022	Bajo	PC	NC
3. Japón	2024	Moderado	LC	LC
4. Alemania	2023	Moderado	PC	LC
5. Reino Unido	2022	Sustancial	LC	C
6. Francia	2022	Sustancial	LC	LC
7. India	2024	Sustancial	LC	LC
8. Italia	2019	Sustancial	LC	LC
9. Canadá	2021	Bajo	PC	NC
10. Corea del Sur	2020	Moderado	PC	LC
11. Rusia	2024	Sustancial	LC	LC
12. Australia	2024	Moderado	PC	NC
13. Brasil	2023	Moderado	PC	PC
14. España	2019	Sustancial	LC	LC
15. México	2023	Moderado	LC	LC
16. Indonesia	2023	Moderado	LC	PC
17. Países Bajos	2022	Moderado	LC	LC
18. Suiza	2023	Moderado	LC	LC
19. Arabia Saudita	2020	Moderado	LC	LC
20. Turquía	2023	Moderado	LC	LC
21. Argentina	2024	ND	ND	ND
22. Suecia	2020	Moderado	LC	LC
23. Tailandia	2023	Bajo	PC	PC
24. Polonia	2023	Sustancial	LC	LC
25. Bélgica	2018	Moderado	LC	LC
26. Noruega	2023	Moderado	PC	C
27. Austria	2018	Moderado	LC	LC
28. Emiratos (EAU)	2023	Bajo	LC	LC
29. Hong Kong	2023	Moderado	LC	PC
30. Singapur	2019	Moderado	LC	C

Anexo 3. Acceso a los registros de beneficiarios finales (TJUE)

La Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 22 de noviembre de 2022 se pronunció sobre la Directiva (UE) 2015/849, modificada por la Directiva (UE) 2018/843, que exigía a los Estados miembros establecer registros de beneficiarios finales accesibles al público, como parte de las políticas contra el lavado de activos y el financiamiento al terrorismo.

El TJUE analizó, en particular, si el acceso público a los datos de los registros era compatible con los derechos fundamentales de privacidad y protección de datos personales, recogidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE.

En su análisis, el TJUE consideró que la accesibilidad pública generalizada a los datos personales de los beneficiarios finales es desproporcionada y, por tanto, incompatible con los derechos fundamentales de privacidad y protección de datos personales. El Tribunal observó que, si bien el objetivo de transparencia para la lucha contra actividades ilegales es legítimo y necesario, el acceso irrestricto a esta información por cualquier persona del público no es proporcional, ya que no se limita al contexto de las investigaciones o actividades relacionadas con la prevención del crimen financiero. En particular, el TJUE señaló los siguientes problemas:

1. Exposición de información personal sensible: Los registros de beneficiarios finales incluyen datos personales como el nombre, apellidos, fecha de nacimiento, nacionalidad, y a veces incluso la dirección de residencia. El TJUE consideró que esta exposición de datos puede generar riesgos significativos para la seguridad y privacidad de los individuos, incluidas posibles amenazas de acoso, secuestro o extorsión, especialmente para aquellos que son titulares de empresas de alto perfil o con altos activos.

2. Desajuste con el principio de minimización de datos: El acceso público ilimitado va en contra del principio de minimización de datos, que exige que la recolección y el tratamiento de datos personales se limiten estrictamente a los fines necesarios. El TJUE concluyó que, aunque el registro tiene fines legítimos, permitir el acceso a todas las personas es una medida que va más allá de lo necesario para cumplir esos fines.

3. Ausencia de equilibrio adecuado: El TJUE destacó que la Directiva no proporcionaba suficientes medidas para limitar el acceso solo a quienes realmente necesitan esta información en el contexto de actividades legítimas. Por ejemplo, las autoridades competentes y ciertas entidades obligadas (como bancos y firmas de inversión) pueden tener un acceso regulado a estos registros para cumplir con sus obligaciones en prevención de lavado y delitos financieros. Sin embargo, el acceso irrestricto del público en general se considera desproporcionado frente al derecho a la privacidad de los beneficiarios finales.

4. Evaluación de proporcionalidad: El Tribunal aplicó el principio de proporcionalidad, que exige que cualquier restricción de derechos fundamentales debe ser adecuada, necesaria y proporcionada en sentido estricto. Concluyó que la Directiva no cumplía con estos criterios, ya que el acceso ilimitado no era "estrictamente necesario" para lograr el objetivo de transparencia y lucha contra el lavado de activos, considerando que existen otras formas de lograr estos fines sin afectar tan drásticamente la privacidad de los individuos.

El TJUE, al analizar el "interés legítimo" para el acceso al registro de titulares reales, se refirió a la idea de que no cualquier persona debe poder acceder a esta información, sino únicamente aquellas personas o entidades que puedan demostrar un motivo válido y justificado relacionado con el interés público, como el combate al lavado de activos y al financiamiento al terrorismo. En particular, el acceso a los registros debe estar vinculado directamente con un propósito que justifique la necesidad de conocer la identidad de los beneficiarios finales. Los intereses legítimos pueden incluir, entre otros, la investigación de delitos financieros. Así, el acceso debería estar restringido a aquellos que realmente requieren estos datos para llevar a cabo funciones legales o regulatorias en el ámbito de la transparencia financiera.

En este sentido, el TJUE sugiere que existen entidades y personas que, por su papel o actividad, tienen un interés legítimo. Esto incluye principalmente a las autoridades competentes (como cuerpos de policía, fiscales y reguladores financieros), que necesitan esta información para realizar investigaciones y controlar la actividad financiera ilícita, y a los sujetos obligados por la normativa contra el lavado de activos, tales como instituciones financieras, abogados y empresas de auditoría, que deben verificar la identidad de sus clientes para prevenir actividades ilegales. Estas entidades y personas, al tener responsabilidades directas en la detección y prevención de actividades ilícitas, cumplen con el "interés legítimo" de acceder a los registros.

El Tribunal afirmo, en particular, que el "interés legítimo" no se refiere al interés de cualquier persona o entidad con curiosidad o motivaciones comerciales, sino a un motivo concreto y justificado que cumpla con el principio de proporcionalidad, permitiendo el acceso solo a quienes puedan probar una conexión clara con la finalidad del registro.

El Tribunal concluyó, consecuentemente, que el acceso público ilimitado a los datos de los beneficiarios finales es desproporcionado. Aunque el objetivo de transparencia es legítimo, el TJUE determinó que permitir el acceso sin restricciones no respeta adecuadamente los derechos fundamentales de privacidad y protección de datos de los individuos afectados.

La sentencia ha provocado la revisión de las legislaciones de varios Estados miembros para alinearse con las orientaciones del Tribunal. Países Bajos cerró su registro al público general, limitando el acceso a autoridades competentes y entidades obligadas bajo la normativa de diligencia debida. Bélgica y Luxemburgo implementaron restricciones similares para proteger los derechos fundamentales al respeto de la vida privada y la protección de datos. Alemania adoptó modificaciones para restringir el acceso público y garantizar que la información solo estuviera disponible para autoridades pertinentes y entidades sujetas a prevención del lavado de activos y financiamiento del terrorismo. De manera similar, Austria ajustó su normativa en línea con el fallo del TJUE, mientras que Francia también revisó su legislación para limitar el acceso público a datos sensibles de titulares reales. En España, dado que la normativa aún estaba en desarrollo al momento de la sentencia, el acceso al Registro de Titularidades Reales se ajustó desde su implantación a los principios de proporcionalidad y restricción indicados por el TJUE. Estas modificaciones, implementadas principalmente a partir de 2023, buscan garantizar un equilibrio entre la transparencia financiera y la protección de los derechos fundamentales de los ciudadanos en el marco de la Directiva (UE) 2018/843.

Anexo 4. Recursos adicionales

A continuación, se presentan una serie de documentos internacionales considerados relevantes en materia de registros de beneficiarios finales. Además del enlace al texto completo de cada uno, se incluye un resumen de su contenido. Cabe destacar que las conclusiones expuestas en dichos documentos son responsabilidad exclusiva de sus respectivos autores y no deben interpretarse como parte del Informe "Estudio de Experiencias Comparadas de Registros de Beneficiarios Finales" de COPOLAD.

Building Effective Beneficial Ownership Frameworks. Global Forum and IDB (2021)

https://publications.iadb.org/es/publications/english/viewer/Building-Effective-Beneficial-Ownership-Frameworks-A-Joint-Global-Forum-and-IDB-Toolkit.pdf

El informe "Construcción de Marcos Efectivos de Propiedad Beneficiaria: Una Herramienta Conjunta del Foro Global y el BID" es una guía desarrollada por el Foro Global sobre Transparencia e Intercambio de Información para Fines Fiscales y el Banco Interamericano de Desarrollo. Su objetivo es proporcionar un marco comprensivo y práctico para ayudar a las jurisdicciones a implementar y mejorar sus sistemas de propiedad beneficiaria (BO) en línea con los estándares internacionales de transparencia.

La propiedad beneficiaria (BO) se refiere a las personas naturales que, en última instancia, poseen o controlan una entidad legal, como una empresa, un fideicomiso, o cualquier otra estructura jurídica. La transparencia en la BO es fundamental para:

- Prevenir el uso indebido de estructuras legales para ocultar la verdadera propiedad y las fuentes de ingresos.
- Luchar contra la evasión fiscal, el lavado de dinero, la corrupción y la financiación del terrorismo.
- Fortalecer la integridad del sistema financiero global y la confianza en los mercados.

La identificación de los propietarios beneficiarios se realiza mediante un enfoque escalonado que consta de tres niveles:

- Propiedad Directa: Identificar a las personas naturales que poseen un interés significativo en la entidad (por ejemplo, más del 25% de las acciones).
- Control Indirecto: Identificar a las personas que ejercen control a través de otros medios, como relaciones familiares o contractuales.
- Gerente Principal: Si no se puede identificar a ningún propietario beneficiario a través de los pasos anteriores, se identifica a la persona que ocupa un puesto de alta dirección en la entidad.

La información sobre la BO es un componente crucial en los estándares de transparencia e intercambio de información a pedido para fines fiscales (EOIR) y en el estándar de intercambio automático de información financiera (AEOI). Estos estándares ayudan a las autoridades fiscales a determinar la verdadera identidad de los propietarios de activos y cuentas financieras y prevenir y detectar la evasión fiscal transfronteriza.

Las revisiones de pares del Foro Global han revelado varias lecciones importantes:

- La implementación efectiva de los marcos de BO varía significativamente entre las jurisdicciones.

- Los enfoques combinados, que integran medidas de prevención del lavado de activos, registros centrales y mantenimiento de registros por las propias entidades, suelen ser más eficaces.

- La supervisión y el cumplimiento rigurosos son esenciales para asegurar la disponibilidad y precisión de la información sobre BO.

El informe presenta varios enfoques para asegurar la disponibilidad de información sobre BO, cada uno con sus propios parámetros y desafíos:

- Enfoque antilavado La información sobre BO es mantenida por instituciones financieras y profesiones no financieras designadas (APNFD) bajo obligaciones de diligencia debida. Este enfoque se centra en la prevención de actividades ilícitas a través de la identificación y verificación de los propietarios beneficiarios por parte de entidades obligadas.

- Enfoque de la Entidad: Las entidades mismas son responsables de mantener y reportar la información sobre sus propietarios beneficiarios. Este enfoque requiere que las entidades legales mantengan registros precisos y actualizados sobre sus BO y los proporcionen a las autoridades competentes cuando sea necesario.

- Registro Central: Un registro central de propietarios beneficiarios es mantenido por una autoridad pública, como un registro corporativo o una agencia gubernamental. Este registro centraliza la información sobre BO, facilitando el acceso para las autoridades fiscales y otras entidades relevantes.

- Enfoque de la Administración Tributaria: La administración tributaria recopila y mantiene la información sobre BO a través de declaraciones fiscales y otros mecanismos de reporte. Este enfoque puede ser particularmente útil en jurisdicciones donde la administración tributaria tiene una capacidad robusta de recopilación y análisis de datos.

El informe concluye que no existe un enfoque único para la implementación de marcos de BO efectivos. Las jurisdicciones deben evaluar sus propios contextos legales y operativos para determinar el mejor enfoque o combinación de enfoques. La supervisión continua y el ajuste de las políticas son esenciales para mantener la eficacia de los sistemas de BO.

La cooperación internacional y el intercambio de mejores prácticas también son vitales para mejorar la transparencia y combatir los delitos financieros a nivel global. El Foro Global y el IDB están comprometidos a proporcionar asistencia técnica y apoyo continuo a las jurisdicciones que buscan mejorar sus marcos de BO.

Regulation Around the World. Beneficial ownership registers: Norton Rose Fulbright (2023)
https://www.nortonrosefulbright.com/en/knowledge/publications/abe55ea5/beneficial-ownership-registers-regulation-around-the-world

El informe analiza la situación de los registros de beneficiarios reales a nivel mundial, destacando las reformas recientes impulsadas por el Grupo de Acción Financiera Internacional (GAFI) y las sanciones económicas relacionadas con la invasión rusa a Ucrania. Los registros de beneficiarios reales son cruciales para identificar la propiedad y el control de empresas, reduciendo el riesgo de actividades ilegales como el lavado de dinero y el financiamiento del terrorismo.

Como conclusiones indica que los registros de beneficiarios reales están siendo adoptados globalmente para mejorar la transparencia y combatir actividades financieras ilícitas. A pesar de los avances, hay desafíos significativos en la implementación y cumplimiento, y las regulaciones continúan evolucionando para abordar estas dificultades.

Beneficial ownership. Taking the extra step to data accuracy. ACAMS (2023)
https://www.acams.org/en/media/document/36425

El informe "Propiedad beneficiaria. Pasos adicionales para asegurar la exactitud de los datos" señala que la implementación de los registros de propiedad beneficiaria ha sido lenta y enfrenta desafíos significativos en términos de precisión y verificación de la información contenida.

No existe un único enfoque "correcto" para asegurar la precisión de la información de propiedad beneficiaria. Este documento presenta una variedad de opciones tácticas y mejoras estructurales que los responsables de políticas pueden considerar según sus circunstancias específicas.

El informe aborda seis formas de verificar la información de propiedad beneficiaria

(1) Controles en el momento de la formación de la entidad: Implementar controles estrictos durante la formación de la entidad para asegurar que la información de propiedad beneficiaria es completa y precisa desde el principio.

Este enfoque reduce significativamente el riesgo de que se incluya información incorrecta o fraudulenta en los registros de propiedad beneficiaria. A continuación, se describen los aspectos clave y las prácticas recomendadas para implementar controles efectivos durante la formación de la entidad:

1. Requerimiento de información completa y precisa:

Obligación de suministrar información detallada: Las jurisdicciones deben requerir que las nuevas entidades proporcionen información completa y precisa sobre los propietarios beneficiarios al momento de la formación. Esta información debe incluir nombres completos, fechas de nacimiento, nacionalidades, y detalles específicos sobre el tipo de control que ejercen (por ejemplo, porcentaje de acciones poseídas, derechos de voto, etc.).

Uso de formularios estandarizados: Utilizar formularios estandarizados puede ayudar a garantizar que se recopile toda la información necesaria de manera consistente y estructurada.

2. Verificación por terceros con obligaciones de prevención de lavado de dinero:

Participación de profesionales: Involucrar a terceros con obligaciones de prevención de lavado de dinero, como abogados, notarios, o proveedores de servicios de fideicomiso y empresa, para recopilar

y verificar la información de propiedad beneficiaria durante el proceso de formación. Estos profesionales deben asegurarse de que la información es precisa y cumplir con los requisitos de diligencia debida del cliente.

Responsabilidad de terceros independientes: Algunos países, como Eslovaquia, requieren que terceros independientes verifiquen la información de propiedad beneficiaria antes de que pueda ser presentada al registro. Estos terceros son responsables de certificar que la información es correcta y pueden ser responsables conjuntamente con la entidad por cualquier inexactitud.

3. Sistemas de registro automatizados:

Integración de controles en el sistema de registro: En jurisdicciones donde el sistema utilizado para registrar una nueva empresa es el mismo que se usa para recopilar información de propiedad beneficiaria, se pueden implementar controles automáticos. Por ejemplo, en Letonia, no es posible registrar una nueva empresa sin ingresar información completa de propiedad beneficiaria. El sistema rechaza automáticamente las solicitudes que no cumplen con estos requisitos.

Reconfirmación de información al registrar cambios: Cada vez que se solicita un cambio en el registro (como la adición de un nuevo miembro de la junta), tanto la entidad como los nuevos miembros deben reconfirmar o actualizar la información de propiedad beneficiaria para que el cambio sea aceptado.

4. Medidas de cumplimiento y supervisión:

Revisión y supervisión continua: Las autoridades responsables deben realizar revisiones periódicas y auditorías para asegurar que las entidades cumplen con los requisitos de presentación de información. Esto puede incluir la implementación de algoritmos y técnicas de análisis de datos para identificar entradas sospechosas o inexactas.

Sanciones y penalizaciones: Establecer sanciones efectivas para las entidades que no cumplan con los requisitos de presentación de información completa y precisa puede servir como un fuerte disuasivo contra el incumplimiento. Estas sanciones pueden incluir multas, la disolución de la entidad, o restricciones en su capacidad para operar.

5. Ejemplos Internacionales:

Letonia: No permite la formación de nuevas empresas sin la presentación completa de información de propiedad beneficiaria. Además, cualquier cambio en la junta directiva requiere la actualización simultánea de la información de propiedad beneficiaria.

Dinamarca e Israel: En estos países, los abogados con obligaciones de prevención de lavado de dinero están involucrados en el proceso de formación de la entidad y son responsables de recopilar y verificar la información de propiedad beneficiaria.

Implementar controles robustos durante la formación de la entidad ofrece varios beneficios:

1. Prevención proactiva: Detecta y previene la inclusión de información incorrecta desde el principio, reduciendo la necesidad de correcciones posteriores.

2. Confianza y transparencia: Aumenta la confianza en la precisión de los registros de propiedad beneficiaria, lo cual es crucial para las autoridades competentes y otras partes interesadas.

3. Cumplimiento con estándares internacionales: Ayuda a las jurisdicciones a cumplir con los estándares internacionales establecidos por el GAFI y otras organizaciones reguladoras.

En resumen, establecer controles rigurosos en el momento de la formación de la entidad es una estrategia efectiva para asegurar la precisión e integridad de la información de propiedad beneficiaria, contribuyendo significativamente a la lucha contra el lavado de dinero y otras actividades ilícitas.

(2) Verificaciones automáticas con otras bases de datos gubernamentales: Utilizar verificaciones cruzadas automáticas con otras bases de datos gubernamentales para verificar la precisión de la información.

Las verificaciones automáticas con otras bases de datos gubernamentales son un componente esencial para garantizar la precisión y fiabilidad de la información de propiedad beneficiaria. Este enfoque se basa en el uso de tecnología y sistemas integrados para cruzar y validar datos proporcionados por las entidades legales con información existente en diversas bases de datos gubernamentales. A continuación, se describen los aspectos clave y los beneficios de este enfoque, así como ejemplos de su implementación en distintas jurisdicciones.

Son aspectos clave de las verificaciones automáticas los siguientes:

1. Automatización del proceso de verificación:

Integración de sistemas: Las jurisdicciones deben integrar los sistemas de registro de propiedad beneficiaria con otras bases de datos gubernamentales, como registros fiscales, registros de población, bases de datos de pasaportes, registros de tierras, y otros registros relevantes. Esto permite que los datos se verifiquen automáticamente sin necesidad de intervención manual.

Algoritmos y herramientas de software: Utilizar algoritmos y herramientas de software para realizar verificaciones cruzadas automáticas de los datos. Estas herramientas pueden identificar discrepancias y posibles errores en la información de propiedad beneficiaria al compararla con datos confiables de otras fuentes.

2. Tipos de datos verificados:

Identificación personal: Verificar la identidad de los propietarios beneficiarios mediante el cruce de datos con registros de identificación nacional, pasaportes, y registros de población.

Información financiera y tributaria: Comparar la información de propiedad beneficiaria con los registros fiscales y otros datos financieros para asegurar que los datos presentados sean consistentes con la información mantenida por las autoridades fiscales.

Propiedad y activos: Verificar la información relacionada con la propiedad de tierras y otros activos al cruzar datos con registros de propiedad y catastros.

3. Beneficios del enfoque automático:

Eficiencia: La automatización reduce significativamente el tiempo y los recursos necesarios para realizar verificaciones, permitiendo que las autoridades se concentren en casos de mayor riesgo o sospechosos.

Precisión y confiabilidad: Las verificaciones automáticas con múltiples bases de datos proporcionan una capa adicional de precisión, reduciendo la probabilidad de errores o información fraudulenta en los registros de propiedad beneficiaria.

Detección temprana de discrepancias: Identificar y corregir discrepancias en los datos desde el inicio, evitando la acumulación de errores y facilitando la gestión de la información.

Ejemplos de Implementación

Letonia. Sistema Integrado de Registro: En Letonia, el sistema de registro de empresas está integrado con otras bases de datos gubernamentales. Este sistema rechaza automáticamente las solicitudes de registro de nuevas empresas si no se proporciona información completa y precisa sobre los propietarios beneficiarios. Además, cada cambio en la administración de la entidad requiere la actualización y verificación simultánea de la información de propiedad beneficiaria.

Dinamarca y Austria. Verificaciones Cruzadas Automáticas: Dinamarca y Austria utilizan verificaciones automáticas con diversas bases de datos gubernamentales, incluidas las bases de datos fiscales y registros de población, para validar la información de propiedad beneficiaria. Estos países han implementado sistemas que cruzan automáticamente los datos proporcionados con la información disponible en otras bases de datos gubernamentales, garantizando así la precisión y confiabilidad de los datos registrados.

Eslovaquia. Verificación por Autoridades Independientes: Eslovaquia requiere que la información de propiedad beneficiaria sea verificada por un "autorizado" antes de ser registrada. Este autorizado puede ser un abogado, notario, banco o asesor fiscal que no tenga conexión con la entidad y que verifique la exactitud de la información antes de su presentación al registro público.

Reino Unido. Registro de Entidades Extranjeras: El Reino Unido exige que las entidades extranjeras que poseen propiedades en el país registren y verifiquen su información de propiedad beneficiaria antes de realizar cualquier transacción. Esta información debe ser verificada por una "persona relevante" según las regulaciones de lavado de dinero del Reino Unido, garantizando así la precisión de los datos presentados.

Como desafíos pueden identificarse los siguientes:

1. Barrera técnica:

Interoperabilidad de Sistemas: Uno de los mayores desafíos para la implementación de verificaciones automáticas es la falta de interoperabilidad entre diferentes sistemas gubernamentales. Las bases de datos deben estar técnicamente conectadas y ser capaces de intercambiar información de manera eficiente.

Digitalización de datos: Algunos países aún recopilan información de propiedad beneficiaria en formato papel o a través de medios electrónicos no estandarizados (por ejemplo, correos electrónicos

o PDFs escaneados). La digitalización y estandarización de estos datos son pasos cruciales para permitir verificaciones automáticas.

2. Privacidad y seguridad:

Protección de datos: Es esencial garantizar que los datos personales y financieros utilizados en las verificaciones automáticas estén protegidos adecuadamente contra el acceso no autorizado y el uso indebido. Las jurisdicciones deben implementar medidas de seguridad robustas y cumplir con las regulaciones de protección de datos.

3. Capacitación y recursos:

Capacitación del personal: Los funcionarios y personal técnico deben estar debidamente capacitados para gestionar y operar sistemas de verificación automática. Esto incluye la capacitación en el uso de herramientas tecnológicas y en la interpretación de los resultados de las verificaciones automáticas.

Recursos financieros y tecnológicos: La implementación de sistemas de verificación automática requiere una inversión significativa en tecnología y recursos financieros. Las jurisdicciones deben planificar y asignar los recursos necesarios para desarrollar y mantener estos sistemas.

Como conclusión, las verificaciones automáticas con otras bases de datos gubernamentales son una estrategia eficaz para mejorar la precisión y confiabilidad de la información de propiedad beneficiaria. Al integrar sistemas y utilizar tecnologías avanzadas, las jurisdicciones pueden detectar y corregir discrepancias de manera eficiente, lo que contribuye a la transparencia y previene el uso indebido de entidades legales para actividades ilícitas. Aunque existen desafíos técnicos y de implementación, los beneficios de un sistema de verificación automática robusto son significativos para fortalecer los esfuerzos globales contra el lavado de dinero y la financiación del terrorismo.

(3) Verificación por terceros independientes: Requerir que terceros independientes, como abogados o notarios, verifiquen la información antes de que se registre.

La verificación por terceros independientes es una medida que fortalece la precisión y confiabilidad de la información de propiedad beneficiaria. Involucrar a profesionales externos y entidades especializadas para verificar esta información añade una capa adicional de control y asegura que los datos presentados sean fidedignos. A continuación, se describen los aspectos clave de esta práctica, sus beneficios, ejemplos de implementación y los desafíos asociados.

Son aspectos clave de la verificación por terceros independientes:

1. Definición y rol de los terceros independientes:

Profesionales calificados: Los terceros independientes pueden incluir abogados, notarios, contadores, bancos, y asesores fiscales. Estos profesionales están sujetos a regulaciones de prevención de lavado de dinero y deben seguir procedimientos estrictos de diligencia debida.

Verificación integral: Estos terceros no solo verifican la identidad de los propietarios beneficiarios sino que también aseguran que la estructura y los detalles de la entidad son consistentes y razonables.

2. Proceso de verificación:

Recolección de documentación: Los terceros independientes recopilan documentación relevante que incluye identificaciones personales, registros financieros, contratos, y cualquier otro documento que pruebe la titularidad y el control de la entidad.

Validación y confirmación: Se valida la autenticidad de los documentos y se confirma que los individuos identificados como propietarios beneficiarios son quienes realmente controlan la entidad.

Certificación y presentación: Una vez completada la verificación, los terceros independientes certifican la información y la presentan a la autoridad competente o registro correspondiente.

3. Responsabilidad y obligaciones:

Responsabilidad legal: En algunas jurisdicciones, los terceros independientes pueden ser responsables legalmente por la precisión de la información verificada. Esto incluye la posibilidad de ser sancionados si se descubre que la información presentada es incorrecta.

Revisiones periódicas: Los terceros independientes pueden estar obligados a realizar revisiones periódicas y recertificar la información de propiedad beneficiaria, especialmente si hay cambios en la estructura de la entidad.

Son beneficios de la verificación por terceros independientes:

1. Precisión mejorada:

Verificación detallada: Los profesionales independientes suelen tener los recursos y la experiencia necesarios para llevar a cabo verificaciones exhaustivas, lo que reduce el riesgo de errores y fraudes.

Reducción del riesgo: Al contar con una capa adicional de verificación, se disminuye significativamente el riesgo de que se registren datos inexactos o falsos.

2. Ahorro de recursos gubernamentales:

Delegación de tareas: Al delegar la verificación a terceros, las autoridades gubernamentales pueden ahorrar recursos y enfocarse en la supervisión y el control de calidad.

Menos carga administrativa: Las entidades registradoras pueden manejar volúmenes mayores de datos con mayor eficiencia, ya que no tienen que verificar cada entrada individualmente.

3. Confianza y credibilidad:

Aumento de la confianza: La participación de profesionales externos puede aumentar la confianza en la precisión de los registros de propiedad beneficiaria entre las autoridades, las instituciones financieras y otras partes interesadas.

Cumplimiento normativo: Ayuda a las jurisdicciones a cumplir con los estándares internacionales de transparencia y prevención de lavado de dinero establecidos por organizaciones como el GAFI.

Ejemplos de Implementación:

Eslovaquia. Registro de Socios del Sector Público: En Eslovaquia, la información de propiedad beneficiaria presentada al Registro de Socios del Sector Público debe ser verificada por una "persona

autorizada", como un abogado o notario, que debe certificar la exactitud de la información y ser corresponsable por cualquier inexactitud.

Reino Unido. Registro de Entidades Extranjeras: El Reino Unido requiere que las entidades extranjeras que poseen propiedades registren su información de propiedad beneficiaria en el Registro de Entidades Extranjeras. Esta información debe ser verificada por una "persona relevante" bajo las regulaciones de AML del Reino Unido.

Estados Unidos. Ley de Transparencia Corporativa: Bajo la Ley de Transparencia Corporativa de EE. UU., ciertas entidades deben proporcionar información de propiedad beneficiaria verificada a la Red de Control de Delitos Financieros (FinCEN), con verificaciones realizadas por profesionales sujetos a la normativa de prevención del lavado de activos.

Como desafíos y consideraciones pueden señalarse los siguientes:

1. Costos asociados:

Carga financiera: La verificación por terceros puede ser costosa para las entidades, especialmente las pequeñas empresas que pueden tener recursos limitados.

Costos de cumplimiento: Los costos de contratar a profesionales independientes pueden ser significativos, lo que podría ser una barrera para algunas entidades.

2. Capacitación y habilidad:

Competencia profesional: Es crucial que los terceros independientes estén debidamente capacitados y tengan la competencia necesaria para realizar verificaciones precisas y completas.

Estándares uniformes: Establecer estándares uniformes para la verificación puede ser un desafío, especialmente en jurisdicciones con recursos limitados o donde la capacitación profesional varía.

3. Responsabilidad y confianza:

Responsabilidad legal: La posibilidad de responsabilidad legal puede disuadir a algunos profesionales de participar en el proceso de verificación.

Confianza en los verificadores: Las autoridades deben asegurarse de que los verificadores sean confiables y cumplan con las normas éticas y profesionales.

Como conclusión puede señalarse que la verificación por terceros independientes es una estrategia efectiva para mejorar la precisión y confiabilidad de la información de propiedad beneficiaria. Al involucrar a profesionales externos en el proceso de verificación, se añade una capa crítica de control y se asegura que los datos registrados sean precisos y completos. Aunque existen desafíos asociados, los beneficios en términos de transparencia, confianza y cumplimiento normativo son significativos. Las jurisdicciones que implementen este enfoque deben considerar cuidadosamente los costos, la capacitación de los verificadores y las responsabilidades legales para maximizar la eficacia del sistema.

(4) Controles internos en el registro de propiedad beneficiaria: Establecer controles internos basados en el riesgo para identificar información inexacta o sospechosa.

Los controles internos en el registro de propiedad beneficiaria son esenciales para garantizar la precisión y confiabilidad de la información registrada. Estos controles incluyen un conjunto de procedimientos y sistemas implementados por las autoridades responsables del registro para identificar, verificar y corregir información inexacta o sospechosa. A continuación, se detallan los aspectos clave de estos controles, sus beneficios, ejemplos de implementación y los desafíos asociados.

Son aspectos clave de los controles internos

1. Evaluaciones de riesgo:

Análisis de riesgos: Las autoridades deben realizar evaluaciones periódicas de riesgo para identificar y clasificar a las entidades según su nivel de riesgo. Esto incluye evaluar factores como la jurisdicción de origen, la estructura de propiedad y la naturaleza de las actividades comerciales.

Actualización de riesgos: Mantener un proceso continuo de actualización de riesgos basado en cambios en la normativa, en el entorno económico y en la información obtenida de otras entidades gubernamentales y del sector privado.

2. Algoritmos y análisis de datos:

Algoritmos de detección: Utilizar algoritmos y técnicas de análisis de datos para detectar patrones sospechosos o inconsistencias en la información de propiedad beneficiaria. Estos algoritmos pueden identificar automáticamente entradas que requieran una revisión más detallada.

Inteligencia artificial y aprendizaje automático: Implementar soluciones de inteligencia artificial (IA) y aprendizaje automático para mejorar la capacidad de los sistemas en la detección de anomalías y en la predicción de posibles riesgos.

3. Procedimientos de revisión manual:

Revisión de alta prioridad: Establecer procedimientos para la revisión manual de las entradas identificadas como de alto riesgo por los sistemas automatizados. Los revisores deben ser capacitados para evaluar la veracidad de la información y para identificar señales de alerta.

Escalado de casos: Diseñar un sistema de escalado para que los casos sospechosos se remitan a unidades especializadas, como la Unidad de Inteligencia Financiera (UIF), para una investigación más exhaustiva.

4. Controles preventivos y correctivos:

Prevención de errores: Implementar controles preventivos que impidan la inclusión de información incorrecta desde el inicio. Esto puede incluir la obligatoriedad de llenar todos los campos requeridos y la verificación cruzada automática con otros datos registrados.

Corrección de errores: Establecer procedimientos para la corrección rápida y eficiente de cualquier información inexacta detectada. Esto incluye notificar a las entidades afectadas y requerirles que proporcionen documentación adicional para corregir los errores.

5. Supervisión y auditoría interna:

Auditorías periódicas: Realizar auditorías internas regulares para evaluar la efectividad de los controles y para asegurar que se cumplen las políticas y procedimientos establecidos.

Monitoreo continuo: Implementar sistemas de monitoreo continuo para detectar y responder rápidamente a cualquier anomalía o incumplimiento de las normas.

Pueden señalarse como beneficios de los controles internos

1. Precisión y fiabilidad mejoradas:

Reducción de errores: Los controles internos ayudan a minimizar la inclusión de información incorrecta o fraudulenta, mejorando así la precisión de los registros.

Confianza y transparencia: Al asegurar la calidad de los datos, se incrementa la confianza de las partes interesadas, incluyendo instituciones financieras, reguladores y el público en general.

2. Detección y prevención de fraudes:

Identificación temprana: Los sistemas de detección automatizados pueden identificar patrones sospechosos antes de que se conviertan en problemas mayores.

Mitigación de riesgos: Los controles internos permiten a las autoridades tomar medidas preventivas y correctivas rápidamente, mitigando así los riesgos asociados con la información incorrecta.

3. Cumplimiento normativo:

Adherencia a estándares internacionales: Implementar controles internos ayuda a las jurisdicciones a cumplir con los estándares internacionales, como los establecidos por el GAFI.

Evitar sanciones: Mantener registros precisos y confiables puede ayudar a evitar sanciones y mejorar la reputación de la jurisdicción a nivel internacional.

Ejemplos de Implementación

Letonia. Algoritmos de Detección: Letonia ha implementado algoritmos que analizan la información de propiedad beneficiaria en busca de entradas sospechosas. Los casos identificados se escalan para una revisión manual y, si es necesario, se remiten a la UIF para una investigación adicional. Asimismo, la autoridad responsable realiza evaluaciones de riesgo regulares para identificar entidades de alto riesgo y aplicar controles más estrictos a estas entidades.

Dinamarca. Verificaciones Cruzadas Automatizadas: Dinamarca utiliza verificaciones cruzadas con diversas bases de datos gubernamentales para validar la información de propiedad beneficiaria. Este proceso ayuda a identificar y corregir errores en los datos presentados.

Reino Unido. Auditorías Internas y Monitoreo: El Reino Unido realiza auditorías internas periódicas y monitoreo continuo de la información de propiedad beneficiaria para asegurar su precisión y detectar cualquier anomalía.

Como desafíos el informe señala los siguientes:

1. Recursos y capacitación:

Inversión en tecnología: Implementar sistemas avanzados de detección y análisis de datos requiere una inversión significativa en tecnología y en la capacitación del personal.

Capacitación del personal: Es crucial que el personal encargado de la revisión y auditoría esté debidamente capacitado para identificar y manejar adecuadamente las inconsistencias y fraudes.

2. Interoperabilidad y coordinación:

Sistemas integrados: La falta de interoperabilidad entre diferentes sistemas y bases de datos gubernamentales puede dificultar la implementación efectiva de controles internos.

Coordinación entre entidades: Asegurar una coordinación efectiva entre diversas entidades gubernamentales y privadas es esencial para el éxito de los controles internos.

3. Protección de datos y privacidad:

Cumplimiento de normativas: Las jurisdicciones deben asegurar que los controles internos cumplan con las normativas de protección de datos y privacidad, evitando el uso indebido de información personal.

Seguridad de la información: Implementar medidas robustas de seguridad de la información para proteger los datos contra accesos no autorizados y ciberataques.

Como conclusión, los controles internos en el registro de propiedad beneficiaria son una herramienta fundamental para garantizar la precisión y la confiabilidad de los datos registrados. A través de evaluaciones de riesgo, análisis de datos, procedimientos de revisión manual, y auditorías internas, las jurisdicciones pueden detectar y corregir información inexacta o fraudulenta de manera eficiente. Aunque existen desafíos, los beneficios en términos de transparencia, confianza y cumplimiento normativo son significativos. Implementar estos controles es esencial para fortalecer los esfuerzos globales contra el lavado de dinero y la financiación del terrorismo

(5) Utilización de instituciones financieras y actividades y profesiones no financieras designadas (APNFD): Permitir que estas entidades reporten discrepancias entre sus datos de diligencia debida del cliente y la información del registro.

(6) Aprovechamiento del público y la sociedad civil: Considerar hacer accesibles los registros de propiedad beneficiaria al público para permitir la verificación cruzada y la identificación de usos indebidos.

Finalmente, se abordan tres mejoras estructurales para asegurar información más precisa:

1. Mayor responsabilidad para las autoridades responsables de los registros: Establecer una clara responsabilidad sobre la precisión de la información en los registros.

2. Más recursos para los registros de propiedad beneficiaria: Asegurar que las autoridades responsables tengan los recursos necesarios para mantener la precisión de los registros.

3. Más aplicación de la ley para información intencionalmente inexacta o incompleta: Implementar sanciones efectivas, proporcionales y disuasorias para aquellos que presenten información inexacta o incompleta de manera intencional.

El informe concluye que garantizar la precisión de la información en los registros de propiedad beneficiaria es uno de los mayores desafíos para los países. Este documento destaca varias opciones tácticas y estructurales que las jurisdicciones están utilizando para cumplir con el requisito de GAFI de tener información adecuada, precisa y actualizada. La lucha contra el crimen financiero requiere limitar el abuso de las entidades legales, y ACAMS se compromete a colaborar con gobiernos y otras entidades para lograr este objetivo.

Guide to implementing beneficial ownership transparency. Open Ownership (2021)
https://www.openownership.org/en/publications/guide-to-implementing-beneficial-ownership-transparency/

El informe "Guía de implementación de la transparencia de la propiedad beneficiaria" detalla estrategias y buenas prácticas para establecer registros públicos que clarifiquen quiénes son los propietarios beneficiarios de entidades legales registradas. Esta transparencia es crucial para combatir el crimen financiero, mejorar la rendición de cuentas corporativas y fomentar un ambiente de negocios confiable y transparente.

La transparencia de la propiedad beneficiaria (BOT, por sus siglas en inglés) permite identificar a las personas naturales que finalmente poseen o controlan entidades legales. Más de 100 jurisdicciones globales se han comprometido con la BOT, que apoya una variedad de objetivos políticos como la inversión, la reducción de costos de diligencia debida, mejora de la rendición de cuentas corporativas, y la lucha contra la corrupción y evasión fiscal.

Implementar un registro público efectivo de propietarios beneficiarios requiere reformas políticas y tecnológicas. Los Principios de Open Ownership ofrecen un marco para implementar la BOT de manera que maximice el impacto de las reformas. Estos principios ayudan a identificar problemas legales, políticos y técnicos que podrían surgir durante la creación de un registro público efectivo.

Los beneficios de los registros públicos de propiedad beneficiaria incluyen la mejora de la transparencia en transacciones empresariales y sistemas fiscales, optimización de los procesos de adquisición pública, y la facilitación de investigaciones de cumplimiento y recuperación de activos robados. Además, la disponibilidad de esta información a autoridades, negocios y el público en general ayuda a combatir la opacidad utilizada por los criminales para encubrir actividades ilegales.

El proceso de implementación se divide en varias etapas que incluyen el compromiso, la creación de un marco legal, la configuración de sistemas de datos y la gestión de la publicación y acceso a los datos. Cada etapa requiere una consideración detallada de los desafíos técnicos y legales, y la guía ofrece recomendaciones para abordar estos desafíos de manera efectiva.

Para asegurar la efectividad y la integridad de los registros de propiedad beneficiaria, es crucial que la información sea de alta calidad y verificable. Esto significa que los datos recopilados deben ser

precisos, completos y actualizados, permitiendo a las autoridades y otras partes interesadas realizar verificaciones y análisis confiables. A continuación se detallan algunas estrategias clave para gestionar la privacidad y la seguridad de los datos, resaltando la necesidad de un equilibrio cuidadoso entre la transparencia y la protección de la información personal sensible:

1. Protección de Datos Personales:

La implementación de registros públicos de propiedad beneficiaria debe considerar seriamente la protección de datos personales. Esto incluye medidas como restringir el acceso público a ciertos detalles personales que podrían exponer a los individuos a riesgos de seguridad o privacidad, como direcciones residenciales o información de contacto directo. Sin embargo, esta información debe estar disponible para las autoridades competentes que la requieran para investigaciones legales o supervisión.

2. Acceso Graduado a la Información:

Un sistema de acceso graduado puede ser una solución eficaz, donde se proporcionan diferentes niveles de acceso a los datos según la identidad y la justificación del solicitante. Por ejemplo, mientras que el público general puede acceder a información básica sobre la propiedad beneficiaria, los detalles más sensibles solo estarían disponibles para las autoridades bajo circunstancias reguladas y justificadas.

3. Regímenes de Protección:

Introducir regímenes de protección para personas naturales en situaciones vulnerables (como riesgos de violencia doméstica o secuestro) es fundamental. Aunque la información personal se recolecta y se hace accesible a las autoridades, se pueden implementar exenciones de publicación muy específicas y justificadas para proteger a individuos en situaciones de alto riesgo.

4. Cumplimiento con la Legislación de Protección de Datos:

Al diseñar e implementar registros de propiedad beneficiaria, es esencial adherirse a la legislación nacional e internacional sobre protección de datos. Los implementadores deben asegurarse de que los procesos de recopilación, almacenamiento y procesamiento de datos personales estén claramente definidos y sean legales, seguros y justificados dentro del marco de los objetivos de política pública.

5. Minimización de Datos:

La minimización de datos es un principio clave en la protección de datos, que estipula que solo se deben recopilar y procesar los datos necesarios para cumplir con los objetivos específicos declarados. Esto ayuda a reducir los riesgos asociados con el almacenamiento y manejo de información personal y asegura que la recolección de datos no sea excesiva respecto a las necesidades de transparencia.

6. Infraestructura de Datos Segura:

Invertir en una infraestructura de datos segura y en tecnologías de protección de la información es vital para proteger los datos contra accesos no autorizados, alteraciones o pérdidas. Esto incluye medidas como encriptación de datos, sistemas robustos de autenticación y protocolos de seguridad

para el intercambio de información entre diferentes entidades gubernamentales y con el sector privado.

Estas estrategias no solo ayudan a proteger la privacidad y la seguridad de los individuos, sino que también aumentan la confianza del público y la cooperación con los registros de propiedad beneficiaria, asegurando así que los objetivos de transparencia y rendición de cuentas puedan ser alcanzados de manera efectiva y ética.

En resumen, este informe proporciona una hoja de ruta comprensiva para los gobiernos que buscan implementar o mejorar los registros de propiedad beneficiaria, destacando la importancia de la cooperación internacional, la estandarización de los datos y el mantenimiento de registros actualizados y accesibles al público.

Building an auditable record of beneficial ownership. Technical Guidance. EITI and Open Ownership (2022)
https://eiti.org/guidance-notes/building-auditable-record-beneficial-ownership

El documento "Construyendo un registro auditable de propiedad beneficiaria" proporciona orientación técnica sobre cómo desarrollar un registro auditado de la propiedad beneficiaria, dirigido especialmente a profesionales técnicos involucrados en la arquitectura tecnológica de registros que publican datos de propiedad beneficiaria. Este informe forma parte del programa Opening Extractives, implementado conjuntamente por el Secretariado Internacional de la Iniciativa para la Transparencia de las Industrias Extractivas y Open Ownership, con el objetivo de transformar la disponibilidad y uso de los datos de propiedad beneficiaria para una gobernanza efectiva en el sector extractivo.

El documento subraya la importancia de mantener registros actualizados e históricos de la propiedad beneficiaria como una base para cualquier iniciativa de transparencia sobre la propiedad y el control de las empresas. Destaca cinco características esenciales que soportan la capacidad de auditoría de los registros:

1. Fechas y horarios fiables y completos:

Las fechas y horarios son fundamentales para entender la cronología de los eventos relacionados con la propiedad beneficiaria. Este elemento del registro debe capturar cuándo ocurrieron ciertas acciones, como cambios en la propiedad, cuándo se reportaron estos cambios y cuándo se incorporaron los datos al registro. Esto permite recrear un historial exacto de la propiedad beneficiaria en cualquier punto dado, proporcionando una línea de tiempo clara y verificable que es esencial para la auditoría y la transparencia.

2. Identificadores fiables para personas y entidades:

La utilización de identificadores únicos y consistentes es crucial para asegurar que las personas y entidades puedan ser rastreadas de manera precisa a través de varios registros y a lo largo del tiempo. Esto incluye el uso de números de identificación personal, claves de bases de datos internas, o números

de registro de empresas, que deben estar acompañados de información sobre la autoridad emisora para garantizar la precisión y evitar duplicidades.

3. Información de fuente rastreable:

Es esencial saber quién aportó la información y cuándo fue aportada. Esto no solo ayuda en la verificación de los datos, sino que también es importante para las auditorías y las investigaciones regulatorias. La fuente de cada dato debe ser claramente identificable y accesible, permitiendo a los analistas y a las partes interesadas rastrear la autenticidad y la fiabilidad de la información reportada.

4. Huecos de información visibles:

Un registro auditable debe identificar claramente cualquier ausencia de información y explicar la razón de esta carencia. Esto puede incluir razones técnicas, errores humanos o exenciones legales. Al hacer visibles y explicar los huecos de información, los usuarios del registro pueden evaluar la integridad del registro y comprender mejor el contexto de la información presentada.

5. Política de publicación:

Una política de publicación clara es crucial para que los usuarios comprendan cómo interactuar con el registro. Esta política debería explicar cómo se recopila, maneja y presenta la información, y debería incluir detalles sobre la interpretación de los campos de datos, la resolución de discrepancias y la manera en que se deben entender las correcciones y actualizaciones. La política también debería incluir guías sobre cómo se protege la privacidad de las personas y cómo se asegura que los datos sean precisos y estén actualizados.

El enfoque del documento es asegurar que los registros de propiedad beneficiaria no solo sean transparentes, sino también útiles, accesibles y fiables para auditorías y revisiones. Resalta la necesidad de una estructura de datos estandarizada y legible por máquina para facilitar la búsqueda y el análisis de la información. Al final, recomienda que los registros capturen fechas cruciales de cambios y que estas se formateen de acuerdo con estándares reconocidos internacionalmente, como el ISO 8601, para garantizar la consistencia y la precisión a lo largo del tiempo.

Este enfoque no solo mejora la transparencia, sino que también fortalece la gobernanza y la rendición de cuentas dentro del sector empresarial, especialmente en las industrias extractivas donde la propiedad y el control pueden ser particularmente opacos y susceptibles a la corrupción.

Beneficial ownership and transparency of legal persons. Financial Action Task Force (2024)
https://www.GAFI-gafi.org/content/dam/GAFI-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf

Los vehículos corporativos como las empresas, fideicomisos, fundaciones, asociaciones y otras formas de personas jurídicas y arreglos legales realizan diversas actividades comerciales y empresariales. Aunque tienen un papel esencial y legítimo en la economía global, también pueden ser utilizados en esquemas complejos para ocultar los verdaderos propietarios beneficiarios y las razones reales para poseer activos y realizar transacciones. Estos vehículos pueden ser mal utilizados para diversos fines

ilícitos, como el lavado de activos (LA), el soborno y la corrupción, el fraude fiscal, la financiación del terrorismo (FT), la evasión de sanciones y otras actividades ilegales.

La transparencia en la información sobre la propiedad legal y beneficiaria, la fuente de los activos del vehículo corporativo y sus actividades puede reducir significativamente el uso indebido de estos vehículos. La falta de información adecuada, precisa y actualizada facilita el LA/FT al disfrazar la identidad de los delincuentes, el verdadero propósito de una cuenta o propiedad y el origen o uso de los fondos o propiedades asociadas con un vehículo corporativo.

Para abordar estos problemas, el Grupo de Acción Financiera Internacional (GAFI) estableció el primer estándar internacional sobre transparencia de la propiedad beneficiaria en 2003 y lo fortaleció en 2012. En respuesta al uso significativo indebido de personas jurídicas para el lavado de dinero, financiación del terrorismo y la financiación de la proliferación, el GAFI ha fortalecido recientemente los estándares internacionales sobre la propiedad beneficiaria de personas jurídicas para prevenir y disuadir mejor este uso indebido. Estos cambios también responden a los resultados de las Evaluaciones Mutuas del GAFI, que muestran un nivel generalmente insuficiente de efectividad en la lucha contra el uso indebido de personas jurídicas para LA/FT a nivel global.

La Recomendación 24 revisada requiere explícitamente que los países utilicen un enfoque multifacético, es decir, una combinación de diferentes mecanismos, para la recopilación de información sobre la propiedad beneficiaria. Esto asegura que la información sobre la propiedad beneficiaria de las personas jurídicas sea adecuada, precisa y actualizada y pueda ser accesible por las autoridades competentes de manera oportuna.

La audiencia principal de esta guía son los responsables de políticas y los profesionales de las autoridades nacionales, así como las partes interesadas del sector privado, como instituciones financieras, APFND y empresas que deben cumplir con los requisitos nacionales de prevención del LA/FT basados en los estándares del GAFI. El propósito de esta guía es ayudar a los responsables de políticas y profesionales a identificar, diseñar e implementar medidas apropiadas para prevenir el uso indebido de personas jurídicas en línea con los estándares del GAFI.

Esta guía se centra principalmente en la Recomendación 24, es decir, la transparencia de la propiedad beneficiaria de las personas jurídicas. En cuanto a los arreglos legales cubiertos por la Recomendación 25, el GAFI ha aprobado una Guía especifica.

Es crucial que los países comprendan los riesgos de LA/FT asociados con las personas jurídicas que pueden incorporarse bajo las leyes de su jurisdicción. Esto incluye identificar y describir los diferentes tipos, formas y características básicas de las personas jurídicas en el país, así como los procesos para crear esas personas jurídicas y obtener y registrar información básica y de propiedad beneficiaria sobre ellas. Además, es necesario hacer pública esta información y evaluar los riesgos de LA/FT asociados con los diferentes tipos de personas jurídicas para gestionar y mitigar los riesgos identificados.

Los países también deben identificar y evaluar los riesgos de LA/FT a los que están expuestos en relación con personas jurídicas extranjeras que tengan vínculos suficientes con el país y tomar medidas adecuadas para gestionar y mitigar los riesgos identificados.

La información básica y de propiedad beneficiaria debe ser adecuada para identificar a los propietarios beneficiarios naturales y los medios y mecanismos a través de los cuales ejercen la propiedad beneficiaria. La información debe ser precisa y actualizada, incluyendo detalles como el nombre completo, nacionalidad, fecha de nacimiento y otros identificadores relevantes.

La Recomendación 24 revisada exige un enfoque multifacético que incluye como mínimo un enfoque de empresa, un registro o mecanismo alternativo, y cualquier otra fuente suplementaria de información según sea necesario. Este enfoque debe permitir a las autoridades competentes acceder y compartir información sobre la propiedad beneficiaria para fortalecer la verificación y el control cruzado de la información.

El enfoque multifacético recomendado por el Grupo de Acción Financiera Internacional (GAFI) se basa en la experiencia acumulada de diversas evaluaciones mutuas que indican que utilizar múltiples fuentes de información es más efectivo que depender de una sola fuente para prevenir el uso indebido de personas jurídicas con fines criminales. Este enfoque combina diferentes mecanismos para recolectar información sobre la propiedad beneficiaria, garantizando así que la información sea adecuada, precisa y actualizada.

El núcleo de este enfoque multifacético combina:

1. Información proporcionada por las empresas: Información que las propias empresas mantienen y suministran.

2. Información mantenida por autoridades públicas: A través de registros públicos o mecanismos alternativos que aseguren un acceso rápido y eficiente a la información sobre la propiedad beneficiaria.

3. Medidas adicionales según sea necesario: Estas medidas pueden incluir información suplementaria que las autoridades competentes puedan necesitar para verificar y controlar la información .

Este enfoque asegura que las autoridades competentes puedan acceder y verificar la información sobre la propiedad beneficiaria desde diversas fuentes, lo que ayuda a mitigar problemas de precisión y a mejorar la calidad general de la información. Los países pueden decidir las medidas específicas dentro de sus sistemas nacionales basándose en su propio contexto, materialidad y riesgos.

El GAFI alienta a los países a permitir que las autoridades competentes intercambien información sobre la propiedad beneficiaria para fortalecer aún más la verificación y el control cruzado de la información. Esto incluye no solo la identificación de errores, sino también la mejora de la calidad de la información sobre la propiedad básica y beneficiaria.

Para que las autoridades competentes puedan realizar sus funciones de manera efectiva, deben tener acceso oportuno y eficiente a la información básica y de propiedad beneficiaria. Este acceso puede variar dependiendo de la parte que posee la información y del marco legal nacional:

1. Información mantenida por una autoridad pública o mecanismo alternativo: El acceso debe ser rápido y eficiente, es decir, sin demoras indebidas. Las autoridades competentes deben conocer qué autoridad pública o mecanismo alternativo posee la información adecuada, precisa y actualizada y cómo acceder a ella.

2. Información mantenida por las empresas: Las autoridades, especialmente las fuerzas del orden y las unidades de inteligencia financiera, deben poder acceder a esta información de manera oportuna con la cooperación total de la empresa misma. Esto es común en el contexto de investigaciones y generalmente requiere una orden de producción o un equivalente legal que obligue a la empresa a divulgar la información a la autoridad competente.

3. Partes que poseen información relevante: Deben comprender sus obligaciones de divulgación y cooperar plenamente con las autoridades competentes, proporcionando la información lo más rápido posible dentro de un marco de tiempo que permita a las autoridades cumplir con sus funciones. Los países deben asegurarse de que exista un marco legal o regulatorio claro que autorice dicho acceso y divulgación, y proteja, cuando sea necesario, a las fuentes de información contra la responsabilidad por divulgaciones autorizadas.

Las autoridades públicas, especialmente aquellas involucradas en la contratación pública, deben tener poderes adecuados para obtener acceso oportuno a la información básica y de propiedad beneficiaria sobre las personas jurídicas que participan en contratos públicos:

1. Requisitos de participación: Hacer que la provisión de información básica y de propiedad beneficiaria sea un requisito para participar en procesos de contratación pública.

2. Acceso a registros: Proporcionar a las autoridades de contratación pública acceso a la información mantenida en registros públicos o mecanismos alternativos, así como a través de cualquier medida suplementaria adicional.

3. Confianza en la información pública: Permitir a las autoridades confiar en información básica y de propiedad beneficiaria que esté disponible públicamente.

Respecto de los costos de acceso, si se contempla una estructura de tarifas para acceder a la información básica y de propiedad beneficiaria, los países deben asegurarse de que dicha estructura no cree retrasos innecesarios ni obstáculos al acceso eficiente y rápido por parte de las autoridades competentes. Se recomienda que las autoridades competentes y públicas puedan acceder a esta información sin costo para fomentar la disponibilidad suficiente de la información. Para otros, la estructura de tarifas debe ser proporcional o no exceder los costos administrativos de hacer la información disponible.

Este enfoque integral busca no solo facilitar el acceso a la información necesaria para prevenir el uso indebido de las personas jurídicas, sino también asegurar que la información sea precisa y utilizable por las autoridades en sus esfuerzos por combatir el lavado de dinero y la financiación del terrorismo.

El acceso a la información por parte de las autoridades competentes debe ser oportuno, y la información debe ser adecuada para identificar al propietario beneficiario, precisa basada en la verificación y actualizada. También se incluyen controles más estrictos para prevenir el uso indebido de acciones al portador y arreglos de nominados.

En conclusión, esta guía del GAFI sobre la propiedad beneficiaria de personas jurídicas proporciona un marco integral para mejorar la transparencia y prevenir el uso indebido de vehículos corporativos para

actividades ilícitas, asegurando que la información relevante sea accesible y utilizable por las autoridades competentes de manera efectiva.

Beneficial ownership and transparency of legal arrangements. Guidance for a risk-based approach. Financial Action Task Force (2024)
https://www.GAFI-gafi.org/en/publications/GAFIrecommendations/Guidance-Beneficial-Ownership-Transparency-Legal-Arrangements.html

El documento “Guía para un enfoque basado en el riesgo: propiedad beneficiaria y transparencia de arreglos legales" publicado por el Grupo de Acción Financiera Internacional (GAFI) ofrece directrices detalladas para mejorar la transparencia y el enfoque basado en el riesgo en la propiedad beneficiaria y la administración de arreglos legales, como los fideicomisos.

El documento subraya la importancia de identificar adecuadamente a los beneficiarios efectivos de los arreglos legales, como medida crucial para prevenir el lavado de dinero y la financiación del terrorismo. Las recomendaciones del GAFI buscan asegurar que los países implementen medidas efectivas para obtener, mantener y proporcionar acceso a información precisa y actualizada sobre la propiedad beneficiaria de estos arreglos.

Se define el alcance de la Recomendación 25, que abarca los fideicomisos expresos y otros arreglos legales similares. Se detallan los tipos de partes involucradas en un fideicomiso, incluidos el constituyente, el fideicomisario, el protector, los beneficiarios y cualquier otra persona que ejerza control efectivo sobre el arreglo. También se incluye la obligación de identificar estos arreglos similares y sus riesgos asociados.

El documento enfatiza la necesidad de que los países evalúen los riesgos de lavado de dinero y financiación del terrorismo asociados con los fideicomisos y otros arreglos legales. Esto incluye la evaluación del riesgo en función del país de gobernanza, el país de administración y otros vínculos significativos con el país. Los mecanismos para prevenir y mitigar estos riesgos son esenciales, incluyendo la necesidad de contar con información adecuada y actualizada sobre la propiedad beneficiaria.

Se subraya la importancia de que los fideicomisarios obtengan y mantengan información adecuada, precisa y actualizada sobre los beneficiarios y otras partes involucradas en el fideicomiso. Esto incluye la necesidad de validar periódicamente esta información y actualizarla en un tiempo razonable cuando ocurran cambios significativos, como la adición de nuevos beneficiarios o la modificación de detalles de identidad.

Los países deben asegurarse de que la información sobre la propiedad beneficiaria esté accesible de manera eficiente y oportuna a las autoridades competentes. Esto puede incluir el uso de registros centrales de fideicomisos, autoridades fiscales y otros proveedores de servicios, como abogados y contadores, para mantener y proporcionar acceso a esta información.

El documento establece que deben existir sanciones disuasivas y proporcionales para los fideicomisarios que no cumplan con las obligaciones de mantener y proporcionar acceso a la

información requerida. Además, los proveedores de servicios y fideicomisarios deben estar sujetos a la supervisión de una autoridad competente que garantice el cumplimiento de estas obligaciones.

La cooperación internacional es crucial para combatir el lavado de dinero y la financiación del terrorismo. Los países deben facilitar el acceso de las autoridades extranjeras a la información sobre la propiedad beneficiaria y cooperar en investigaciones internacionales. Esto incluye la eliminación de condiciones restrictivas que puedan impedir el intercambio efectivo de información, como el secreto bancario.

El documento incluye un anexo con una lista de propósitos comunes para los fideicomisos, que abarca desde la protección de activos hasta la gestión de inversiones y operaciones comerciales. Los fideicomisos pueden usarse para proteger activos contra riesgos externos, asegurar la continuidad empresarial y manejar activos en beneficio de los beneficiarios, especialmente en situaciones donde estos no pueden gestionar los activos por sí mismos debido a incapacidades o restricciones legales.

El GAFI proporciona un marco detallado para mejorar la transparencia y la gestión de riesgos en la administración de fideicomisos y otros arreglos legales. Estas directrices buscan fortalecer las medidas contra el lavado de dinero y la financiación del terrorismo, asegurando que la información sobre la propiedad beneficiaria sea precisa, adecuada y accesible a las autoridades competentes de manera eficiente y oportuna.