



**CERTIFICACIÓN DE TERCEROS:
UN ENFOQUE ESTRATÉGICO
Y SISTEMÁTICO DE MANEJO DE RIESGOS**

PREFACIO

Mientras los equipos de gestión y los directorios luchan con un conjunto de riesgos que enfrentan sus empresas y que se hallan en rápida evolución, la certificación de terceros se ha convertido en una herramienta cada vez más importante para generar confianza y eficiencia en las cadenas de suministro y en las relaciones con proveedores.

Actualmente, una de las cuestiones más críticas para las organizaciones es la identificación y mitigación del riesgo. A medida que la complejidad y los tipos de amenazas se multiplican, es cada vez más difícil para los equipos de gestión y los directores pensar de manera estratégica sobre los riesgos y abordarlos de forma tal que cumplan con los requerimientos de los reguladores y las necesidades de los clientes y demás partes interesadas. Estos desafíos son especialmente críticos para aquellas organizaciones que tercerizan aspectos de sus operaciones, infraestructura y controles.

La Certificación de Terceros (CT) implica certificar los procesos comerciales de proveedores de servicio tercerizado para garantizar que se están llevando a cabo los procedimientos adecuados y que dichos proveedores pueden cumplir con la provisión de las tareas asignadas. La CT puede tener un rol crítico para ayudar a los líderes de negocios a pensar de manera holística sobre los riesgos que sus organizaciones enfrentan y, al mismo tiempo, para impregnar de rigor y disciplina a los esfuerzos de la compañía relativos a cumplimiento y gestión de riesgos -tanto para sus proveedores tercerizados como para sus propios procesos internos.

En este documento brindaremos un resumen de la CT y discutiremos los beneficios de los informes sobre controles de empresa y sistema (CES), como una herramienta clave de gestión de riesgo. Describiremos cómo la CT puede ayudarlo a reforzar sus prácticas comerciales y el cumplimiento con cualquier normativa o regulación cuando fuese aplicable, y también a crear confianza. Luego exploraremos tendencias y riesgos emergentes en varias áreas críticas, desde la protección contra ciberataques hasta un reporte ambiental, social y de gobierno (ESG, por sus siglas en inglés) más transparente. Finalmente, detallaremos brevemente cómo los servicios de CT de BDO se hallan excepcionalmente posicionados para ayudar a su compañía a manejar los riesgos en un marco global cada vez más complejo.



Jeff Ward

Assurance Managing Partner
Third Party Attestation
National Practice Leader,
BDO in US



Christophe Daems

Global TPA workgroup leader,
BDO in Belgium



Términos claves

Certificación de Terceros:

Certificar los procesos comerciales de proveedores de servicio tercerizado para garantizar que se están llevando a cabo los procedimientos adecuados y que dichos proveedores pueden cumplir con la provisión de las tareas asignadas.

Informes sobre Controles de Empresa y Sistema (CES):

Afirmación escrita que certifica la validez del proceso interno o que verifica que un tercero posee y realiza procedimientos y controles adecuados para desarrollar una función tercerizada.

Certificación de tipo I:

Se confirma el diseño y la implementación de procedimientos relevantes de control y se emite un informe CT Tipo I ('momento en el tiempo').

Certificación de tipo II:

Se revisa la efectividad operativa de procedimientos de control y se emite un informe CT Tipo II ('periodo de tiempo').

LOS BENEFICIOS DE CT E INFORMES CES EN UN MUNDO EN EVOLUCIÓN

La CT puede ayudar a las organizaciones a focalizarse en sus principales áreas de fortaleza y, al mismo tiempo, a brindar tranquilidad cuando tercerizan determinados procesos o tareas a especialistas externos. Por ejemplo, un comerciante minorista dedicado a la venta en línea podría tener experiencia en ventas y marketing, pero no contar con empleados internos debidamente capacitados para prevenir la violación de datos o proteger los datos de clientes. Como resultado, este comerciante minorista podría tercerizar dichas actividades a un proveedor especializado en servicios de seguridad gestionada con experiencia en ciberseguridad.

Sin embargo, la tercerización de esta función también trae consigo riesgos propios. Esto incluye riesgos reputacionales, de control, de cumplimiento, de privacidad, financieros y operativos. Por ejemplo, si el comerciante minorista se viese afectado por un ciberataque, sus sistemas podrían estar fuera de línea e inaccesibles hasta que se resolviera la situación. Asimismo, los hackers podrían acceder a los datos del cliente, lo que incluye información personal (IP), y exponerlos. Una violación de datos podría ocasionar daño reputacional, como también gastos financieros directos e indirectos debido a una potencial pérdida de negocio, litigios, multas o cualquier otra

sanción regulatoria. Al confiarle a un tercero funciones tercerizadas como la ciberseguridad, una compañía necesita estar segura de que el proveedor puede proteger de manera adecuada esos activos valiosos. Para concluir, **mientras algunas actividades pueden ser tercerizadas, los riesgos subyacentes no.**



¿Cómo puede ayudarle el Aseguramiento a Terceros?

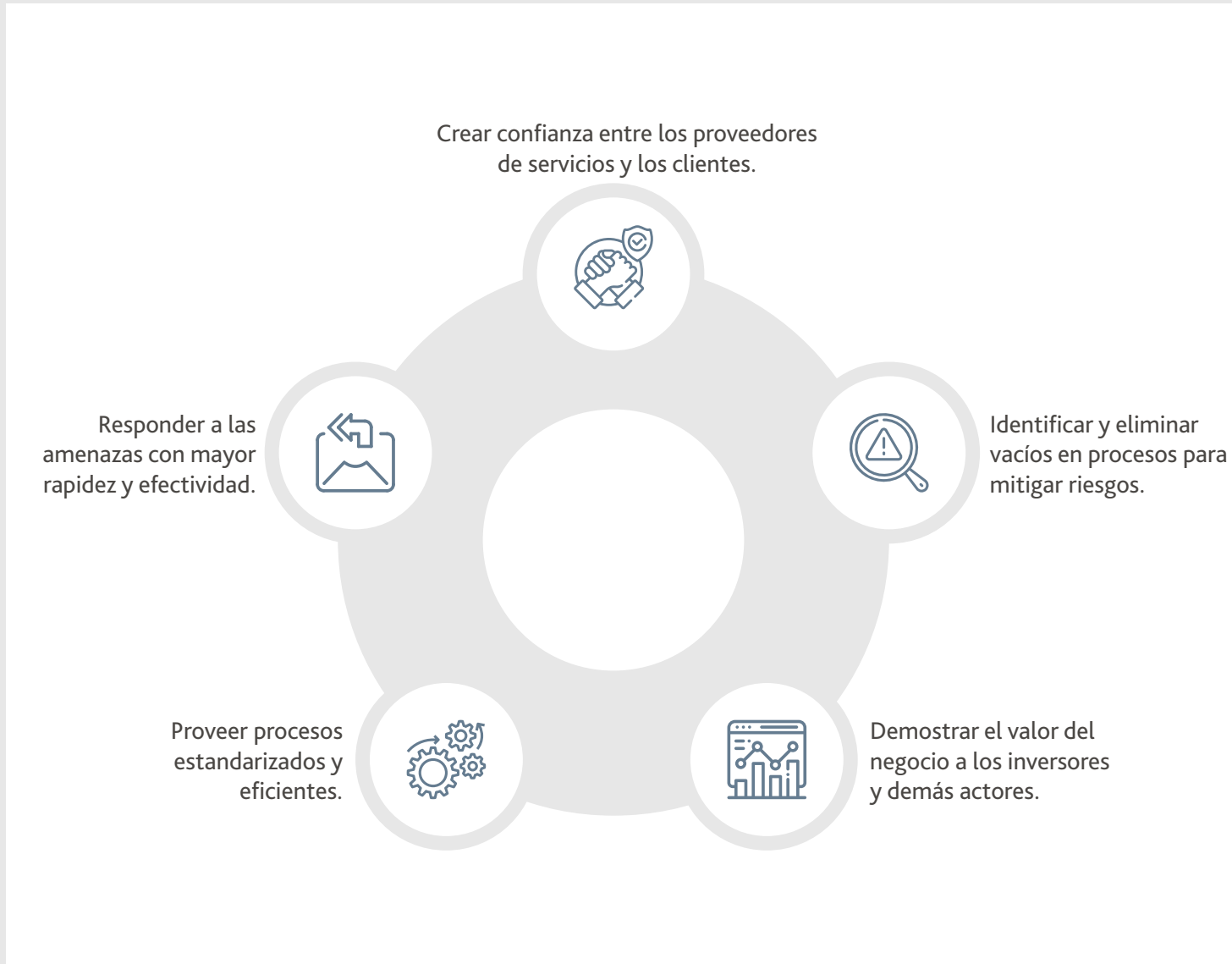
Y aquí es donde entra en escena la CT, la cual ofrece un lente objetivo para certificar que los procesos, ya sea internos o los realizados por terceros, constituyen las mejores prácticas y cuentan con controles adecuados. En nuestro ejemplo, el proveedor de servicios de seguridad gestionada podría usar la CT para certificar que posee las operaciones, los controles y la tecnología requeridos para combatir de manera proactiva los ciberataques y evitar la violación de datos. En este escenario, el comerciante minorista de venta en línea puede quedarse tranquilo de que un tercero ha revisado y aprobado las capacidades de su proveedor. Si bien no existe garantía alguna de que el comerciante estará protegido contra cualquier violación u otro incidente de seguridad, sí puede sentirse seguro de que realmente contrató a un experto certificado para protegerse.

Beneficios de la certificación de terceros

Para un proveedor de servicios, la CT puede brindar un «sello de aprobación» objetivo sobre la adecuación de sus controles y procesos comerciales. Esto puede otorgar una ventaja competitiva puesto que muchas compañías buscan contratar a proveedores de servicios que cuentan con CT. En este tipo de situación, los proveedores de servicios -al igual que nuestro proveedor de servicios de seguridad gestionada mencionado en nuestro ejemplo- a menudo recurren a compañías como BDO para crear informes CES. Los informes CES brindan una afirmación escrita que certifica la validez de procesos internos o que verifica que un tercero posee y realiza procedimientos y controles adecuados para desarrollar una función tercerizada. Existen muchos tipos de informes CES disponibles, pero básicamente todos ellos buscan crear confianza y permitirle a las compañías desarrollar el negocio con mayor seguridad. A continuación describimos varios beneficios claves de los informes CES.



PRINCIPALES BENEFICIOS DE LOS INFORMES CES EN LA CADENA DE VALOR





Crear confianza

En la economía global actual, no hay dudas de que las organizaciones deben confiar en sus contrapartes para realizar negocios. Esto es aún más crítico si operan en una gran variedad de jurisdicciones y ambientes regulatorios internacionales y locales, como también en un entorno cada vez más virtual. En estas circunstancias, los informes CES pueden proporcionar una verificación objetiva de que dichos proveedores de servicios cumplen con una amplia variedad de regulaciones. Los informes CES se han tornado imperativos en muchos procesos RFP y de *vendor management*, posibilitando más oportunidades de negocio sin la necesidad de empezar de cero por cada requerimiento o solicitud. Cuando se trata de crear confianza, los informes CES juegan un papel fundamental, reduciendo, en última instancia, los esfuerzos de cumplimiento año tras año y causando un número menor de auditorías de socio o proveedor en el lugar. Al promover la confianza, los informes CES permiten que las compañías cuenten con más formas eficientes y potencialmente redituables de realizar negocios unas con otras.



Identificar y eliminar vacíos

Mediante la evaluación de un tercero de los controles organizacionales se puede determinar si los sistemas son diseñados, implementados y operados tal como se esperaba, como también la forma en que pueden ser mejorados. Un informe CES puede indicar dónde y cuándo existen fallas en controles que posiblemente podrían causar una interrupción del negocio, permitiéndoles a los proveedores de servicios mitigar de manera proactiva estos riesgos. Además de resaltar fallas, los informes CES pueden focalizarse en las fortalezas de los procesos y controles de proveedores de servicios y ofrecer una guía sobre cómo mejorar aquellas áreas que requieren de mayor atención.



Demostrar el valor del negocio

Los informes CES pueden brindar una buena señal de salud corporativa tanto a los proveedores de servicio como a las compañías que los contratan. Tal como mencionamos anteriormente, muchas compañías buscan proveedores de servicios que estén objetivamente certificados como expertos en determinadas áreas. Para los proveedores de servicios los informes CES pueden ser valiosos cuando planifican un evento estratégico como, por ejemplo, una oferta pública inicial o una venta, puesto que los inversos generalmente utilizan estos informes en el proceso de due diligence y valoración. A menudo los inversionistas ven la efectividad de los programas de gestión de riesgo como un indicador de valor para el accionista.



Responder a las amenazas con rapidez y efectividad

La mejoría de la eficiencia también puede ayudar a las organizaciones a responder a las amenazas con mayor rapidez y efectividad. No importa cuán bien usted esté preparado, los incidentes probablemente ocurran, entonces la velocidad con la que pueda responder y mitigar el daño es esencial. Los informes CES que identifican riesgos y utilizan planes/medidas de respuesta antes de que el incidente tenga lugar permiten a las organizaciones ser más proactivas en vez de solo reactivas. Esta preparación puede ser crucial al momento de facilitar una respuesta ágil, especialmente cuando el tiempo es un elemento esencial.



PROCESOS DE OPTIMIZACIÓN DE INFORMES CES



Proveer procesos estandarizados y eficientes

Los informes CES también posibilitan procesos más estandarizados y eficientes, lo que potencialmente genera un ahorro de tiempo y gastos. El gráfico de abajo, «procesos de optimización de informes CES», muestra cómo estos informes pueden crear procesos más optimizados, permitiendo así operaciones comerciales diarias más rápidas. El diagrama de la izquierda muestra un enredo de solicitudes, preguntas y auditorías puntuales que requieren de las respuestas de diferentes actores internos. Sin un enfoque sistematizado, estas solicitudes pueden abrumar a los recursos y potencialmente generar interrupciones y demoras en la respuesta a clientes actuales o potenciales. El diagrama de la derecha muestra cómo los informes CES pueden simplificar y estandarizar de manera significativa los flujos de solicitud. Al crear un informe CES que claramente establezca los procedimientos requeridos de manera anticipada, es posible limitar la naturaleza específica de cada solicitud o pregunta y permitir respuestas más rápidas y ágiles. Esto también puede implicar un ahorro de tiempo para sus empleados y darle la posibilidad de brindar un mejor servicio a sus clientes actuales o potenciales.

Situación sin informe CES: solicitudes separadas, lo que conduce a la ineficiencia



Situación con informe CES: Un enfoque eficiente y estandarizado



TIPOS DE INFORMES CES

Con CES 1, CES 2, CES 2+, CES 3, CES para Ciberseguridad y CES para Cadena de Suministro, puede ser un desafío determinar qué informe aborda mejor las necesidades de una empresa. Considere los riesgos que su organización busca disipar y quién necesita saber que la seguridad de que su empresa cuenta con los controles adecuados.

	CES 1	CES 2	CES 2+	CES 3	CES para Ciberseguridad	CES para Cadena de Suministro
¿PARA QUIÉN ES ESTA CES?						
Una empresa de servicios (que provee servicios a compañías usuarias)	●	●	●	●		
Cualquier tipo de empresa					●	
Una empresa que produce, fabrica o distribuye productos						●
CON RESPECTO A DICHA EMPRESA, INFORMA SOBRE:						
Reporte financiero	●					
Seguridad		●	●	●	●	●
Disponibilidad		●	●	●	●	●
Integridad de procesos		●	●	●		●
Confidencialidad		●	●	●	●	●
Privacidad		●	●	●		●
DISTRIBUCIÓN						
Limitada (usuarios)	+	+	+			+
Ilimitada (uso general)				●	●	



LA CT EN ACCIÓN: TENDENCIAS Y DESARROLLOS EN ÁREAS FUNCIONALES

La CT y los informes CES pueden implementarse de diferentes formas. A continuación resaltamos desarrollos recientes en distintas áreas y explicamos cómo la CT puede ayudarlo a lograr una visión más holística e integrada de todos los riesgos que enfrenta su compañía y sus partes interesadas.



Ciberseguridad e inteligencia artificial

Las innovaciones tecnológicas requieren que las organizaciones profundicen en áreas nuevas y desconocidas, muchas de las cuales tienen el potencial tanto para crear como para exponer vulnerabilidades. En un mundo cada vez más digital, la protección contra los ciberataques y el aprovechamiento del poder de la inteligencia artificial son dos áreas en evolución que requieren especial atención. Los avances en tecnología les permiten a los atacantes utilizar nuevas herramientas y técnicas para robar información vulnerable e incluso tomar a organizaciones enteras de rehén por medio del «ransomware».

Mientras que no hay forma de prevenir de manera total los ciberataques, la CT ayuda a los proveedores de servicios a validar el hecho de que utilizan procesos y controles para prevenir amenazas o, al menos, que poseen procedimientos integrados para responder rápida y eficientemente ante su aparición. El informe CT debería claramente establecer diferentes pasos para monitorear, abordar y erradicar incidentes, y así brindar un plan de acción para la protección contra y en repuesta a los ciberataques. Por ejemplo, cuando una compañía contrata a un proveedor de servicios de seguridad gestionada para actividades relativas a la seguridad, un informe CT garantiza que se implementan controles de seguridad y que las tareas de seguridad se realizan con el debido cuidado.

El crecimiento continuo de la inteligencia artificial (IA) y el aprendizaje automático (machine learning) puede, entre muchas otras aplicaciones, abrir oportunidades para los negocios que desean automatizar tareas y lograr un mayor conocimiento de sus clientes. Pero si bien el hecho de aprovechar «big data» puede ayudar a las compañías a expandirse a nuevas áreas, también puede generar riesgos inesperados. Por ejemplo, ha habido controversia y un creciente interés político en el uso de algoritmos determinados por IA en la comprobación de antecedentes laborales. Otras compañías se han enfrentado a juicios y se han visto forzadas a pagar acuerdos descomunales por utilizar IA en programas de reconocimiento facial.

Debido a que las nuevas tecnologías avanzan a un ritmo cada vez más acelerado, y en un escenario regulatorio incierto y en evolución, usted necesita expertos que lo ayuden a identificar y adaptarse a estos nuevos tipos de riesgo. Contratar a un proveedor de CT con experiencia en inteligencia artificial puede ayudarlo a evitar riesgos conocidos y, al mismo tiempo, lo preparará para riesgos emergentes que puede que ni siquiera aparezcan en su radar.



¹ <https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/ai-based-hiring-concerns-academics-regulators.aspx>

² <https://www.cnet.com/news/facebook-privacy-lawsuit-over-facial-recognition-leads-to-650m-settlement/>



Privacidad de datos

La privacidad de datos acarrea varios desafíos y ya ha logrado atraer significativa atención política y regulatoria. A diferencia de un elemento tangible, los datos no se hallan dentro de determinado territorio o nación. En consecuencia, un mismo dato podría ser regulado de manera diferente en Europa, Estados Unidos y Asia. Las organizaciones multinacionales que operan en diferentes jurisdicciones deben asegurarse de cumplir con todos los marcos relevantes de privacidad de datos.

- En la Unión Europea, la violación de los requerimientos del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) puede dar lugar a multas y otras sanciones.
- En los Estados Unidos, no existe un régimen central de protección de datos; una combinación de regulaciones de diversos estados y ciudades dificulta aún más la tarea de cumplimiento. Se requiere prestar especial atención a la privacidad de datos, especialmente cuando una empresa (el controlador) y un proveedor de servicios (el procesador) intercambian datos personales. La empresa debería verificar que el proveedor de servicios cumple con los requerimientos y sus procesos se ajustan a la legislación relevante sobre privacidad de datos. Esta verificación puede lograrse a través de los informes CES.

Las leyes sobre privacidad de datos también continúan evolucionando, por lo tanto es imperativo mantenerse actualizado sobre nuevos desarrollos y tendencias regulatorias. Garantizar que su empresa o un tercero cumple con los requerimientos de las diferentes jurisdicciones requiere de un marco integral de gobierno de datos y de expertos con amplitud de conocimientos de regulaciones globales, como también profunda sagacidad sobre la industria.



Gestión de la cadena de suministro

Las cadenas de suministro globales son a menudo, extremadamente sofisticadas y complejas. Las compañías deben ser capaces de poder contar con terceros diversos para cumplir las promesas hechas a sus propios clientes. Las organizaciones que fabrican y distribuyen productos en varias geografías deben poder confiar en sus proveedores y demás contrapartes, independientemente de dónde se encuentran ubicados. Si bien obtener nuevos socios comerciales puede significar ahorro de tiempo, oportunidades de expansión y potencial para mayores ganancias, estas relaciones también pueden traer consigo riesgos imprevistos. Por ejemplo, su compañía podría no ser capaz de cumplir sus compromisos debido a la demora inesperada de un socio o una entrega de materiales que no cumple con los requerimientos específicos.

Una manera de mitigar estos tipos de riesgos es a través de una estructura de reporte que introduce más transparencia a la cadena de suministro global. Los informes CES específicos para cadena de suministro ayudan a los fabricantes y a las partes relacionadas a identificar vacíos y desarrollar un plan para eliminarlos. Los informes pueden hacerse a medida para propósitos específicos y, al mismo tiempo, seguir metodologías estandarizadas y aprobadas. El resultado es un mayor nivel de confianza y el potencial para facilitar algunas de las complicaciones de la cadena de suministro global.





Cumplimiento regulatorio

En las diversas industrias, los proveedores de servicios pueden beneficiarse de los informes CES que certifican su cumplimiento con varios regímenes regulatorios. Esto es especialmente cierto en áreas fuertemente reguladas, tales como salud, servicios financieros, servicios públicos y telecomunicaciones, entre otras. Por ejemplo, un proveedor de servicios de salud de Estados Unidos podría querer un informe CES que certifique su cumplimiento con las normas establecidas en la Ley de Transferencia y Responsabilidad de Seguro Médico (Health Insurance Portability and Accountability Act - HIPAA). De igual modo, un proveedor de servicios que trabaja con instituciones financieras probablemente quiera confirmar que sus procesos cumplen con las disposiciones de la Comisión de Bolsa y Valores de los Estados Unidos (SEC, por sus siglas en inglés) y de la Autoridad Reguladora de la Industria Financiera (FINRA, por sus siglas en inglés).

Los informes CES pueden ser especialmente valiosos para las compañías que operan en múltiples ambientes regulatorios. Como el mundo se halla cada vez más interconectado, una compañía con una base de clientes global debe asegurarse de que sus políticas de privacidad de datos cumplen con las leyes en geografías específicas. Por ejemplo, las compañías con clientes en la Unión Europea deben cumplir con el GDPR, incluso si estuviesen domiciliadas fuera de Europa. Un informe CES que certifica este cumplimiento puede no solo proteger a la compañía, sino también ofrecer una ventaja competitiva para nuevas oportunidades de negocios. En algunos casos, los entes reguladores requieren que los proveedores de servicios demuestren que cumplen con las regulaciones correspondientes en sus jurisdicciones. Una vez más, los informes CES pueden ayudar a cumplir con estos requerimientos.



Demandas de transparencia ambiental, social y de gobierno (ESG)

El reporte ambiental, social y de gobierno ha sido utilizado durante décadas y es probable que cobre mayor importancia en los próximos años. Muchas compañías privadas y que cotizan en la Bolsa están desarrollando iniciativas ESG para resaltar la forma en que están contribuyendo a la comunidad y protegiendo el medio ambiente.

Pero incluso aunque los inversionista, consumidores y reguladores demandan más transparencia en las prácticas corporativas ESG, aún no existe un modelo de reporte ESG estándar. Varios entes reguladores -desde la Comisión Europea hasta la Fundación de Normas Internacionales de Información Financiera-, y organizaciones sin fines de lucro, tales como el Consejo de Normas Contables de Sostenibilidad, la Iniciativa de Reporte Global y el Consejo de Estándares de Divulgación Climática, han emitido estándares y prioridades por separado para el reporte ESG. La falta de consistencia enfatiza los desafíos que las compañías enfrentan al intentar mantenerse actualizados en un escenario de reporte ESG en evolución.

De manera creciente, las compañías están utilizando la CT para comunicarles a los inversionista y demás actores su compromiso con la sustentabilidad y las prácticas sociales. Una certificación objetiva de fuertes principios ESG puede ayudarlas a diferenciarse y potencialmente mejorar su reputación frente al público y los reguladores.

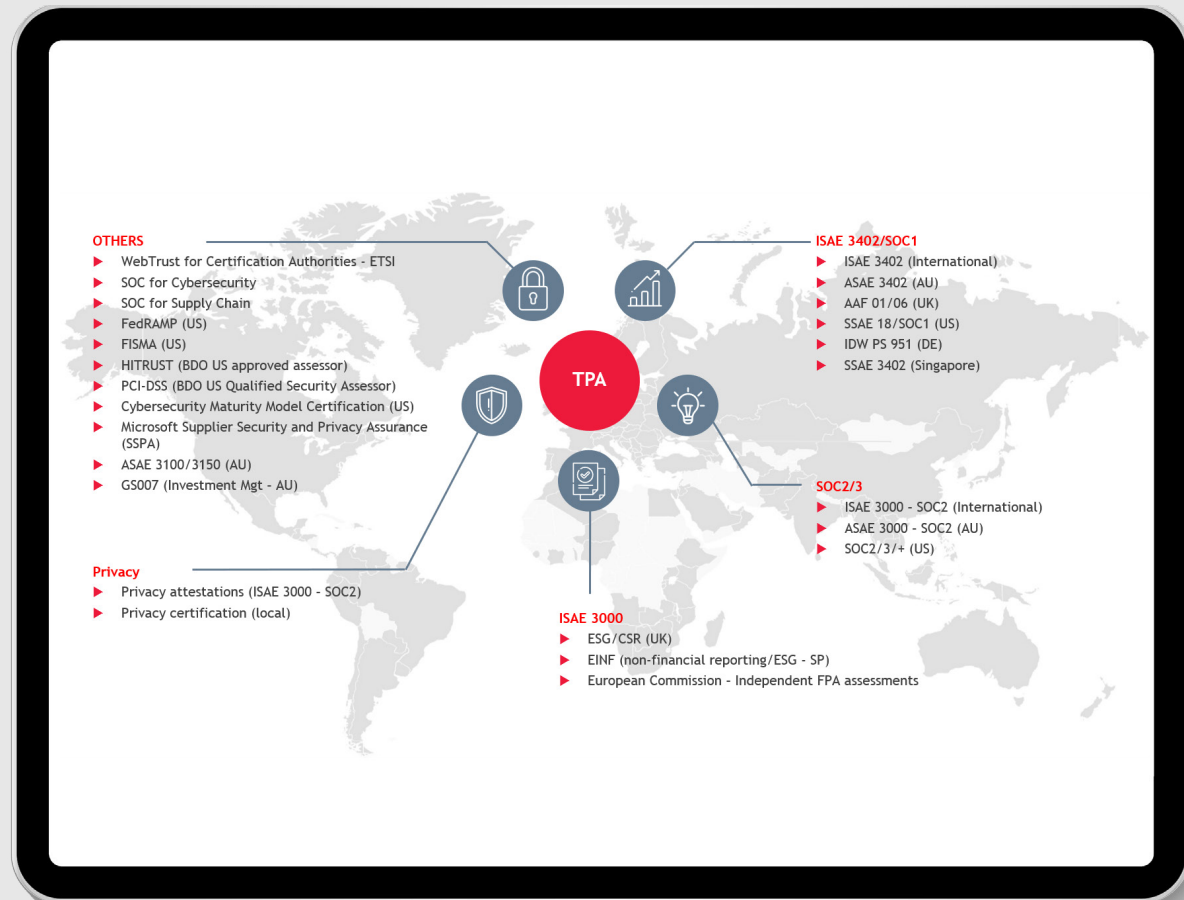


LA NECESIDAD DE EXPERIENCIA TRASCIENDE FRONTERAS E INDUSTRIAS

La CT puede permitir identificar y gestionar riesgos de una mejor manera en su compañía y para sus proveedores externos. Así como mantenerse a la vanguardia en gestión de riesgos y cumplimiento es todo un desafío para cualquier compañía, esta presión crece de manera exponencial para aquellas organizaciones que operan en múltiples países y/o industrias. Por eso es importante asociarse con un proveedor de servicios de aseguramiento, cuyas capacidades son verdaderamente globales -tanto en términos de alcance geográfico como experiencia en las industrias.

En BDO contamos con profesionales de CT en todas las principales regiones del mundo, quienes cuentan con experiencia por su trabajo en las industrias a las que prestamos nuestros servicios. BDO entiende sobre diversos estándares internacionales y trabaja con sus clientes para determinar los estándares más adecuados a adoptar. Estos profesionales cuentan con una práctica global de aseguramiento, que incluye profunda experiencia en todas las áreas principales de CT. Ya sea que usted desee CT para sus procesos internos o para proveedores externos, poseemos amplia práctica y experiencia para ayudarlo a entrar en un mundo complejo y lleno tanto de oportunidades como de amenazas.

Recursos y capacidades globales de CT de BDO



Presencia local en cada región



Norteamérica:
150+ empleados



Europa:
250+ empleados



Asia Pacífico:
75+ empleados




Sudamérica:
30+ empleados



África:
35+ empleados

CONTACTOS

País	Contacto clave	
 AUSTRALIA	Sean Pascoe, Partner	sean.pascoe@bdo.com.au
 BÉLGICA	Christophe Daems, Global TPA workgroup leader	christophe.daems@bdo.be
 CANADÁ	Sam Khoury, Partner	SKhoury@bdo.ca
 ISLAS CAIMÁN	Muzaffar Soomro, Partner	msoomro@bdo.ky
 REPÚBLICA CHECA	Martin Horicky, Partner, Digital services	martin.horicky@bdo.cz
 ALEMANIA	Luc Ernes, Partner	luc.ernes@bdo.de
 HONG KONG	Ricky Cheng, Director and Head of Risk Advisory	rickycheng@bdo.com.hk
 INDIA	Vishal Shah, Partner	VishalShah@bdo.in
 IRLANDA	Brían Gartlan, Partner	bgartlan@bdo.ie
 ISRAEL	Tal Dolev, Partner	TalDo@bdo.co.il
 JAPÓN	Yusuke Chifuku, Manager	chifuku@bdo.or.jp

País	Contacto clave	
 JERSEY	Tanya Grove, Manager	tgrove@bdo.je
 MARRUECOS	Zayed Fahim, Manager	zayedfahim@bdo.ma
 HOLANDA	Jeroen van Schajik, Partner IT audit	jeroen.van.schajik@bdo.nl
 NORUEGA	Siv Irene Aasen, Partner	siv.irene.aasen@bdo.no
 SINGAPUR	Willy Leow, Partner	willyleow@bdo.com.sg
 SUDÁFRICA	Suman Moonilal, Manager	Smoonilal@bdo.co.za
 ESPAÑA	Enrique Turrillo, RAS IT Director	enrique.turrillo@bdo.es
 SURINAME	Anamika Mangroo, Director	anamika.mangroo@bdo.sr
 REINO UNIDO	Fiona Davis, Partner	fiona.davis@bdo.co.uk
 ESTADOS UNIDOS	Jeff Ward, Partner Josh Ayers, Partner	jward@bdo.com jayers@bdo.com

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities. The BDO network (referred to as the 'BDO network') is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© Brussels Worldwide Services BV June 2021

www.bdo.global

