Servicios de Consultoría

En un mundo digital: ¿Sabe usted cuáles son los nuevos riesgos?

Consideraciones clave para su plan de auditoría interna que ayudarán a la gerencia a dirigir en la era de la transformación

The better question. The better answer. The better the world works.

EY
Building a better working world

En un mundo digital: ¿Sabe usted cuáles son los nuevos riesgos?

Bienvenida

Hoy en día, gestionar una organización de manera efectiva es cada vez más complejo. Los nuevos avances tecnológicos, las mayores exigencias regulatorias y la velocidad del ecosistema de negocios, generan que las organizaciones deban adaptarse de manera rápida y eficiente a estos cambios para mantener su competitividad y posición en el mercado. Esta adaptación exige una transformación disruptiva, por lo que aquellas empresas que se resistan al cambio se verán seriamente afectadas. La ausencia de visión y el pensamiento a corto plazo, así como la falta de seguimiento de las variables cambiantes del negocio, son ahora las grandes amenazas para el desarrollo de nuestras organizaciones.

Por esta razón es importante que la Auditoría Interna (AI), la Gerencia y el Directorio trabajen alineados en identificar y evaluar los nuevos riesgos, producto de la innovación y evolución continua del ambiente de negocios, de forma tal que puedan considerarlos en la gestión empresarial y les permita mitigarlos de manera exitosa.

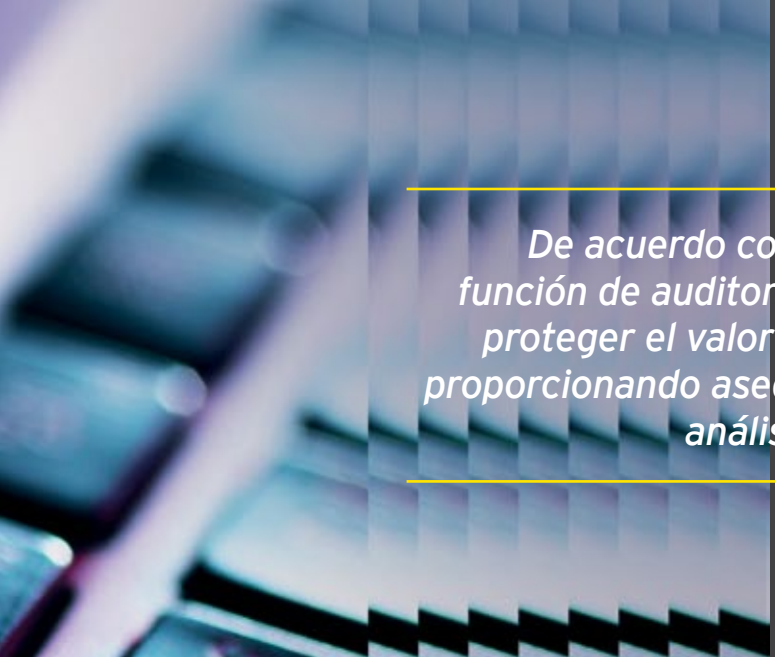
El entorno seguirá cambiando a un ritmo cada vez mayor, y es responsabilidad de los líderes de las organizaciones el conocer los riesgos que enfrentan, implementar controles internos más efectivos e indicadores de medición apropiados, orientados a proteger la reputación e integridad de las organizaciones.

La AI es una función independiente que constituyen las organizaciones para supervisar la labor de la Gerencia y velar por la seguridad y transparencia de los procesos del negocio, adaptados a los cambios globales que se relacionen con sus estrategias.

El Directorio, máximo ente de gobierno de toda organización, es elegido por el Directorio General de accionistas y tiene como principal función guiar el rumbo de la empresa. Por ello, es el responsable de implementar las buenas prácticas de gobierno corporativo y de supervisar su efectivo cumplimiento. Uno de los roles más importantes del Directorio es la supervisión de la gestión de riesgos en las organizaciones. El Directorio debe definir en qué enfocarse ante este panorama de riesgo cambiante.

Es oportuno ver estos riesgos emergentes y entorno cambiante como una oportunidad de mejora intrínseca de la vida del negocio. El Directorio, Auditoría Interna y la Gerencia deben ser capaces de responder ante estas nuevas adversidades a través de una mejora en su gestión de riesgos que finalmente se traducirá en la sostenibilidad de la organización a lo largo del tiempo.

Mirar el panorama actual a través de una orientación basada en riesgos estratégicos, prevenibles y externos, puede ayudar a agudizar el enfoque del Directorio para crear una organización más consciente del riesgo. Esto también se puede lograr a través de la implementación de actualizaciones frecuentes y regulares del perfil de riesgo de la organización.



De acuerdo con el IAI, la misión de la función de auditoría interna es mejorar y proteger el valor de las organizaciones, proporcionando aseguramiento, asesoría y análisis basados en riesgos.

A medida que operamos en la era digital, las empresas se ven obligadas a responder a una amplia gama de desafíos y exigencias a un ritmo cada vez mayor, y parece que no hay un final en el horizonte; lo que conlleva a AI establecer nuevas estrategias en sus funciones, adoptando agresivamente nuevas tecnologías para transformar sus modelos de negocios, impulsar el crecimiento y mejorar la eficiencia.

La evaluación de riesgos debe abarcar toda la empresa e incluir todas las categorías de riesgo: estratégico, operativo (incluida la tecnología), financiero y de cumplimiento. Debe incluir la participación de la gerencia y un enlace directo a la estrategia general de la organización y el programa de gestión del riesgo empresarial. También debería incluir consideraciones tanto cuantitativas como cualitativas, y debería incorporar perspectivas prospectivas, tales como riesgos asociados con objetivos corporativos, estrategias de crecimiento, nuevos productos, cambios ambientales y regulatorios.

Además, a la luz del rápido ritmo de cambio en el mercado, AI debería adoptar tecnología (por ejemplo, análisis de datos avanzados y modelos predictivos y de comportamiento) para permitir la identificación oportuna de los cambios en el perfil de riesgo de una organización.

En EY, tenemos una perspectiva integral en todos los aspectos que representan riesgos en las organizaciones, y somos líderes en el mercado en riesgos y controles. Como líder en servicios de consultoría de gestión de riesgos y auditoría interna, EY Perú trabaja de la mano con sus clientes de diversos niveles y sectores de la economía, aportando diversas experiencias y enfoques de trabajo.

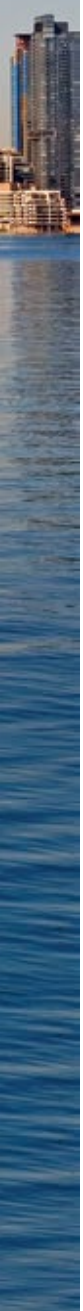
A través de nuestro trabajo con nuestros clientes, hemos identificado una serie de riesgos que son prioritarios para el Directorio, la Gerencia y la AI. En este sentido, la presente publicación tiene como objetivo compartir algunas estrategias innovadoras en Auditoría Interna, para que las distintas organizaciones del Perú puedan enfrentar los nuevos desafíos ante el actual panorama de riesgos y, de esta forma, llevar a cabo una evaluación de riesgos con mayor frecuencia, y de manera continua. Esto es lo que buscamos al colaborar con nuestros clientes y las distintas organizaciones de la comunidad de negocios peruana, buscando facilitar que AI y el negocio se centren en los riesgos que importan.

Atentamente,

Jorge Acosta
Socio Líder de Consultoría
EY Perú

Índice

Introducción



La innovación sigue mejorando el mundo en que vivimos. Solo es cuestión de mirar alrededor para ver los beneficios de la innovación (por ejemplo, acceso global a información a través de internet, elementos de nuestros automóviles y casas que se esfuerzan por mantenernos a salvo y hacer nuestras vidas más fáciles, y avances en medicina, producción y distribución de energía). Sin embargo, el volumen y la velocidad de cambio han transformado drásticamente el mundo comercial y han reorganizado el panorama. Un estudio descubrió que solo 37.6% de las compañías que estuvieron en la lista Fortune 500 en 1995 permanecieron en dicha lista en el 2016[1]. Esto no necesariamente significa que las compañías que ya no aparecen en la lista hayan fracasado; las fusiones y adquisiciones han cambiado la composición y algunas compañías simplemente han sido reemplazadas por nuevas organizaciones que han alcanzado una mayor capitalización del mercado. Sin importar la razón, la competitividad entre compañías para sobrevivir y prosperar es feroz, y la innovación es uno de los elementos diferenciadores clave.

A medida que trabajamos en la era de la transformación, las compañías se ven forzadas a enfrentar una gran variedad de retos y exigencias a un ritmo cada vez más rápido. Una potencial disrupción puede emerger por la introducción de nueva tecnología, nuevos modelos de negocio, un cambio en las preferencias de los consumidores o la llegada de nuevos competidores, que generalmente son de una industria diferente. Ya han desaparecido los límites que alguna vez influenciaron cómo los negocios definían su mercado y cómo operaban.

Por ejemplo, tomemos el caso del efecto que han tenido las compras en línea sobre establecimientos minoristas físicos o la llegada de compañías que ofrecen alquiler de casas para vacaciones sin ni siquiera poseer inmuebles.

En respuesta, las gerencias están adoptando agresivamente nuevas tecnologías para transformar sus modelos de negocio, impulsar el crecimiento y mejorar la eficiencia. Están haciendo uso de *big data* para impulsar el conocimiento competitivo y se involucran en las transacciones estratégicas (fusiones, adquisiciones, ventas de activos, alianzas y empresas conjuntas) para aumentar su ventaja competitiva. La gerencia también está observando su modelo de operaciones actual para identificar cómo ser más ágil y eficiente, y así obtener buenos resultados y aun ser capaz de responder rápidamente cuando surja un nuevo reto.

Todas estas presiones, sean a causa de factores internos o externos, crean tanto una oportunidad como un reto para la función de la Auditoría Interna (AI). La AI debe equilibrar las prioridades y los recursos para ayudar a la organización a abordar los riesgos que enfrenta actualmente, anticipar riesgos emergentes y brindar conocimientos sobre el negocio que ayuden a la gerencia a ganar una ventaja competitiva. La función de AI debe mantenerse enfocada en las actividades principales y básicas, pero también debe estar lista para asumir un rol más consultivo, y debe ser capaz de "ver lo que hay a la vuelta de la esquina" para ver hoy los riesgos del mañana.

[1] Mark J. Perry, "Fortune 500 firms 1955 vs. 2016

Anticorrupción

En muchos lugares del mundo, los pagos de sobornos que benefician de forma personal a aquellos que están en el poder, es algo usual. Sin embargo, a medida que las operaciones se han vuelto más globales y los países en desarrollo más prósperos, se ha generado un movimiento contra la cultura de corrupción. Estados Unidos, las naciones europeas y muchos otros países, incluido el Perú, ven la corrupción como el principal obstáculo para el comercio libre y justo, el cual finalmente impide el crecimiento económico, la confianza en el gobierno y la mejora de la calidad de vida de los ciudadanos alrededor del mundo.

El gobierno estadounidense ha realizado inversiones significativas con el fin de combatir el soborno y hacer cumplir de manera agresiva la Ley de Prácticas Corruptas en el Extranjero (FCPA, por sus siglas en inglés). Hemos visto a compañías pagar decenas y miles de millones de dólares en multas, así como personas declaradas culpables y sentenciadas a cumplir condenas en prisión. El esfuerzo por hacer cumplir la FCPA continúa cada vez más, y las compañías globales necesitan evaluar sus riesgos y tomar medidas al respecto. Esto no se trata solamente del acto de pagar sobornos a funcionarios extranjeros, esto es moralmente indefendible, ilegal y una violación muy grave de la ley.

Si bien es cierto que en el Perú no se han reportado, a la fecha, investigaciones o sanciones por incumplimientos al FCPA, es de público conocimiento que durante los últimos años los escándalos por actos de corrupción que involucran a empresas se han incrementado. En respuesta a esta realidad, en enero de 2017 se aprobó la modificatoria a la Ley de Responsabilidad Administrativa de las Personas Jurídicas, que entró en vigencia el 01 de Enero del 2018. Esta normativa penaliza a las personas jurídicas (independientemente de las sanciones a las personas naturales), los actos de corrupción a funcionarios públicos, el lavado de activos y el financiamiento del terrorismo; sin embargo, ofrece la posibilidad a las empresas de eximirse de esta responsabilidad si es que implementan un Modelo de Prevención para los delitos mencionados. Asimismo, en Octubre de 2016 se publicó el estándar ISO 37001 relacionado a la Gestión de Programas Anticorrupción (incluye corrupción pública y privada), el cual es certificable para las empresas.

Las compañías tienen que ser proactivas. Los riesgos de no hacer nada simplemente son demasiado grandes y generan también responsabilidades personales por el dejar de hacer, o no querer saber. El esfuerzo genuino anticorrupción comienza estableciendo el tono adecuado en el más alto nivel jerárquico y de dirección de las compañías. Los empleados necesitan conocer, en términos claros, cuál es la posición y actitud de la compañía respecto de los asuntos relacionados con la integridad y cumplimiento de la ley.

Las violaciones a la ley FCPA frecuentemente terminan en importantes multas y penalidades pagadas al gobierno. Las multas criminales para las compañías pueden ascender hasta los 25 millones de dólares por cada evento de violación de la ley o el doble de la ganancia bruta asociada con la violación. Las multas o reparaciones civiles y otras reparaciones, incluyendo medidas cautelares, órdenes de cese y desistimiento, devolución de ganancias ilícitas y prohibición de hacer negocios con el gobierno de Estado Unidos son otras posibilidades.

Las auditorías anticorrupción en las compañías actúan como un poderoso motivador para promover el cumplimiento de sus programas anticorrupción, así como para detectar y disuadir potenciales actividades inapropiadas. Las auditorías anticorrupción también contribuyen a evaluar la efectividad del programa anticorrupción, concientizar, brindar retroalimentación importante sobre cómo está operando el programa y, con frecuencia, descubrir nuevos riesgos que no hayan sido identificados o considerados previamente.

Para muchas compañías, las auditorías anticorrupción son el principal método de monitoreo anticorrupción. Estas deben tener dos enfoques principales:

- Auditar el cumplimiento de las diferentes exigencias y controles del programa de anticorrupción.
- Evaluar las transacciones de alto riesgo.

Anticorrupción

Auditorías de alto impacto	Preguntas clave a considerar
Evaluación de riesgos **Objetivo:** Realizar un análisis para ayudar a las compañías a evaluar el riesgo de violar las leyes anticorrupción	▸ ¿La organización evalúa el riesgo de violaciones a las leyes anticorrupción? ▸ ¿Se evalúan las interacciones con funcionarios públicos extranjeros en el contexto de ellos como clientes (contratos con el gobierno y funcionarios públicos como compradores), como reguladores (otorgadores de licencias) o como proveedores (se reciben servicios de entidades vinculadas al estado)? ▸ ¿Se identifican los riesgos de incumplimiento importantes frente al programa, las políticas y los procedimientos anticorrupción?
Auditorías anticorrupción **Objetivo:** Evaluar la efectividad del programa anticorrupción y el cumplimiento de las exigencias del programa	▸ ¿La organización tiene un programa anticorrupción efectivo que considere capacitaciones y certificaciones de empleados, procedimientos de debida diligencia sobre terceros, protocolos de escalamiento en relación con transacciones de alto riesgo, controles financieros sobre el efectivo y otros tipos de pago? ▸ ¿La organización tiene un mecanismo para realizar pruebas sustantivas a actividades de alto riesgo con el fin de identificar señales de alarma y detectar potenciales violaciones?

Auditorías de alto impacto

Análisis forense de datos

Objetivo: Evaluar la efectividad de la analítica avanzada de datos y del monitoreo

Preguntas clave a considerar

- ¿La organización usa técnicas avanzadas de analítica de datos como visualización de resultados, minería de textos y clasificación de riesgos transaccionales en su programa de auditoría anticorrupción?
- ¿La organización tiene capacidades de monitoreo en áreas como pagos a representantes, entrega de regalos, viajes, comidas y gastos de entretenimiento, caja chica y donaciones caritativas?

La SEC (Comisión de Bolsa y Valores) y el DOJ (Departamento de Justicia) han brindado orientación a las compañías al definir los 10 elementos de un programa efectivo:

Características de un programa de cumplimiento efectivo

1. Compromiso de la alta gerencia y una política anticorrupción clara y articulada
2. Código de conducta, y políticas y procedimientos de cumplimiento
3. Autonomía en la supervisión y recursos necesarios
4. Evaluación de riesgos
5. Capacitación y orientación continua
6. Incentivos y acciones disciplinarias
7. Sistemas de denuncias confidenciales e investigación interna
8. Debida diligencia sobre terceros
9. Debida diligencia antes la adquisición de empresas, e integración con los programas anticorrupción post adquisición
10. Mejora continua mediante pruebas y revisiones periodicas

Fuente: "A Resource Guide to the FCPA – US Foreign Corrupt Practices Act – By the Criminal Division of the US Department of Justice and the Enforcement Division of the US Securities and Exchange Commission".

Cadena de bloques (*Blockchain*)

Blockchain es una tecnología emergente y revolucionaria en cuanto a su enfoque a los datos, procesos y gestión de sistemas. Su objetivo es transformar datos, sistemas y procesos que han sido tradicionalmente ensilados y controlados por el negocio, en otros datos, sistemas y procesos controlados por un ecosistema distribuido.

Blockchain podría anular modelos de negocio enteros en algunos sectores al empoderar el crecimiento de "organizaciones virtuales", también conocidas como organizaciones autónomas descentralizadas (DAO, por sus siglas en inglés). Las DAO operan a través de programas de computadora conocidos como "contratos inteligentes", que ejecutan los deseos de los accionistas humanos al transmitir datos automáticamente y de forma segura. Por ejemplo, las transacciones podrían incluir procesamiento de pagos, votación en línea, celebración de contratos, firmas digitales, creación de rutas de auditoría verificables y registro de activos digitales como acciones, bonos y títulos de propiedad. Su potencial de aplicación dentro de la industria de servicios financieros basados en transacciones, es particularmente amplio pero es de valor para todos los sectores.

Blockchain es un tipo de base de datos conocido como un registro contable distribuido que no cuenta con un administrador central y opera de forma consensual. Siempre que un usuario registre un nuevo bloque de datos en *blockchain*, la mayoría de los otros usuarios debe confirmar que es válido. También permite que grupos descentralizados trabajen en conjunto, desde cualquier parte del mundo, de manera segura, confiable y verificable. Debido a que los sistemas basados en *blockchain* permiten procesos de trabajo seguros y distribuidos, también permite que las tareas sean realizadas por equipos distribuidos que operen juntos de una forma más libre, pero con la misma seguridad como si trabajaran lado a lado. Esto podría reducir los gastos de oficina y personal al llevar el trabajo a la gente en lugar de la gente al trabajo.

Puesto que *blockchain* diluye los límites de las organizaciones y necesita que los datos y los procesos sean compartidos fuera de la organización, las compañías deben entender totalmente cómo se implementa la tecnología para establecer estrategias adecuadas de gestión de riesgos. El rol de la auditoría interna puede ayudar a evaluar si se han implementado controles adecuados que aseguren la organización.

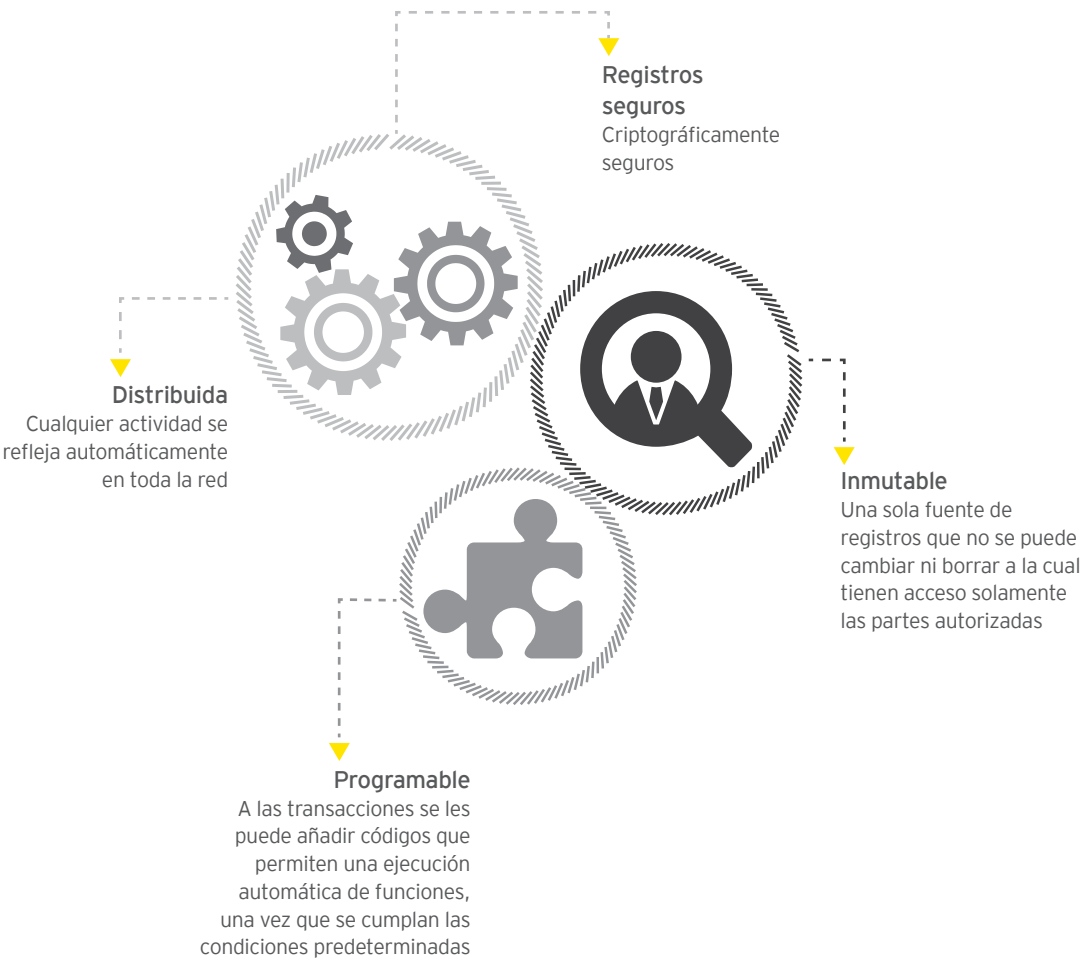
Un riesgo asociado con *blockchain* es el uso de una clave digital privada para la verificación de identidad. Si la clave digital privada se viera comprometida, agentes externos podrían obtener acceso al *blockchain*. Las compañías deben mantener una estructura de gobierno bien definida que administre el almacenamiento y uso de sus claves privadas de forma segura.

Otro riesgo reside en los contratos inteligentes que contienen un código de autoejecución que es diseñado para ejecutar reglas específicas cuando se cumplen ciertas condiciones. A medida que estos contratos inteligentes se vuelven más complejos, son más proclives a errores que podrían dar la oportunidad a agentes externos de poner en riesgo el sistema. Las compañías deben implementar estructuras de control para facilitar la integridad de estos contratos inteligentes.

Cadena de bloques (*Blockchain*)

Auditorías de alto impacto	Preguntas clave a considerar
Gobierno para la implementación de *blockchain* **Objetivo:** Gobierno para la implementación de *blockchain*	▸ ¿Se monitorea la estructura, las funciones, las responsabilidades y los controles concernientes a la separación de tareas de la organización? ▸ ¿Se desarrollan procesos y controles de gestión de proyectos? ▸ ¿El comité directivo o los líderes se involucran en las decisiones clave de los proyectos? ▸ ¿Está alineada la entrega del proyecto propuesto con el perfil de riesgos del proyecto?
Evaluación de riesgos y seguridad de *blockchain* **Objetivo:** Evaluar la estrategia y los controles establecidos en la organización para gestionar y mitigar riesgos relacionados con *blockchain*	▸ ¿La estrategia de codificación establecida es efectiva? ▸ ¿La estrategia de distribución de nodos es suficiente para limitar la pérdida de datos? ▸ ¿El uso de *blockchain* está alineado con las entidades regulatorias de la industria? ▸ ¿Se han implementado controles efectivos para gestionar el acceso al registro contable distribuido? ▸ ¿Hay algún proceso para brindar o retirar accesos? ▸ ¿La organización evalúa los controles de terceros en cuanto al uso de un registro contable distribuido o *blockchain*? ▸ ¿Cómo sabe la organización que la información contenida en el registro contable distribuido es completa o certera?

Blockchain es un registro contable compartido entre participantes de una red que es inmutable, distribuido, programable y criptográficamente seguro



Computación en la nube

La computación en la nube es más que una frase de moda; permite que las organizaciones renueven su compleja estructura de Tecnología de Información (TI), lo cual les ayuda a enfocarse en estrategias en lugar de operaciones y responder rápidamente a las condiciones cambiantes del mercado.

La computación en la nube es un modelo que permite un acceso de red conveniente y bajo solicitud a un grupo compartido de recursos informáticos configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente entregados y liberados con un mínimo de esfuerzo de gestión o de interacción con el proveedor de servicios. Está evolucionando rápidamente, dando a las compañías una variedad de opciones; sin embargo, como la mayoría de cambios en la tecnología, la nube presenta un porcentaje de riesgos y desafíos que frecuentemente se subestiman o no se comprenden totalmente.

Algunos de los riesgos más comunes relacionados con la computación en la nube

▸ **Riesgos de infraestructura y arquitectura**	Estos riesgos surgen cuando los proveedores no cumplen con los requisitos de desempeño que las organizaciones y los proveedores definieron y acordaron al inicio del contrato.
▸ **Estándares y riesgos de interoperabilidad**	Es vital que los sistemas de la organización y del proveedor puedan comunicarse unos con otros.
▸ **Riesgos regulatorios y de cumplimiento**	Las organizaciones que usan servicios de computación en la nube, particularmente *software* como servicio (SaaS[1] por sus siglas en inglés), tienen menos transparencia y menos posesión sobre los controles y procesos de seguridad implementados por los proveedores.
▸ **Riesgos de gestión y gobierno de proveedores en la nube**	Los riesgos contractuales se originan principalmente en los tipos de contratos que los clientes celebran con proveedores de servicios en la nube (CSP[2], por sus siglas en inglés).
▸ **Riesgos de continuidad del negocio**	Los usuarios de la nube dependen del programa de continuidad del negocio y las capacidades de recuperación ante desastres de sus CSP.
▸ **Riesgos de gobierno y alineamiento de estrategias**	Las organizaciones necesitan un modelo de gobierno que incluya un enfoque de gestión de riesgos en la nube para toda la empresa.

[1] *Software-as-a service*
[2] *Cloud Service Provicon*

Computación en la nube

Auditorías de alto impacto	Preguntas clave a considerar
Estrategia y gobierno de la nube **Objetivo:** Evaluar si la estrategia de la organización para la nube se encuentra alineada con los objetivos generales del negocio	▸ ¿Las políticas de la nube están integradas con las políticas legales, de adquisiciones y de TI? ▸ ¿Se han establecido políticas de soporte, incluyendo aquellas legales, de gobierno y de cumplimiento? ▸ ¿La aplicación de servicios en la nube se encuentra alineada con los objetivos generales de la compañía?
Seguridad y privacidad de la nube **Objetivo:** Evaluar las prácticas y los procedimientos de seguridad de la información del proveedor en la nube	▸ ¿Se han implementado procedimientos para la evaluación periódica de seguridad del o de los proveedores de servicios en la nube para evaluar las medidas de seguridad internas que han sido tomadas para proteger la información y los datos de la compañía? ▸ ¿La organización aplica protocolos seguros de autenticación para los usuarios que trabajan en la nube? ▸ ¿Los proveedores de servicios en la nube han presentado los informes SOC[1] (control de organización de servicio) tipo 1, 2 o 3 a la organización? ▸ ¿La organización utiliza acuerdos de nivel de servicio (ANS, por sus siglas en inglés) de seguridad o realiza auditorías al vendedor *in situ*? ▸ ¿Se han establecido salvoconductos en los contratos con el proveedor que cubran su implementación, incluyendo normas de seguridad de datos para la industria de tarjetas de pago (PCI[2] DSS[3]), privacidad de datos y cumplimiento regulatorio?

[1] Service Organization Control
[2] Payment Card Industry
[3] Data Security Standard

Auditorías de alto impacto

Servicios del proveedor en la nube

Objetivo: Evaluar la capacidad del proveedor que brinda los servicios de computación en la nube de cumplir o superar los ANS establecidos en el contrato y los planes de contingencia en caso de fallas, acuerdos de responsabilidad, soporte extendido, y la inclusión de otros términos y condiciones como parte de los contratos de servicio; así como la disponibilidad, la gestión de incidencias y capacidades y la escalabilidad

Preguntas clave a considerar

- ¿Se han establecido ANS para el tiempo de funcionamiento, la gestión de problemas y el servicio en general?
- ¿La organización monitorea y documenta el cumplimiento de los ANS por parte del proveedor de servicios en la nube, las alteraciones observadas, las causas principales y las acciones correctivas y preventivas realizadas por este?
- ¿Los planes de contingencia y recuperación del proveedor de servicios en la nube en caso de incidentes están alineados con los acuerdos contractuales?
- ¿Existe algún inventario de usos de proveedores externos de servicios en la nube, contratado por TI o por cada unidad de negocio?

Commodities

Las empresas con operaciones de producción, comercialización, negociación o cobertura de *commodities* operan en mercados tanto físicos como financieros y buscan gestionar sus riesgos relacionados con este tipo de bienes para impulsar el desempeño de sus negocios. Esto se logra comúnmente mediante el uso de una variedad de estrategias que son diseñadas específicamente para cada entidad.

Sin embargo, existen riesgos continuos durante todo el ciclo de vida de las operaciones con *commodities*, y pueden tener consecuencias significativas en el ámbito económico, financiero, regulatorio e incluso reputacional si no son controlados adecuadamente.

Por esta razón, las funciones de Auditoría Interna se enfocan cada vez más en los riesgos críticos que se derivan de transacciones con *commodities*.

▶ Riesgo de mercado	Debido a los niveles históricos de las fluctuaciones en los precios de *commodities*, no contar con controles suficientes a nivel gerencial podría exponer a la empresa a enfrentarse a niveles de riesgo de mercado inaceptables.
▶ Riesgo de fraude y comercio deshonesto	La exposición al fraude y a las actividades de comerciantes deshonestos siempre está latente. Por esa razón, controles inadecuados o insuficientes lo largo del ciclo de vida de las transacciones de *commodities* pueden dar lugar a su materialización.
▶ Riesgo de crédito y liquidez	El desafiante contexto económico de los *commodities* ha tenido un impacto en la posición de crédito y liquidez de las compañías y sus contrapartes; controles inadecuados o insuficientes podrían llevar a a las empresas a enfrentar niveles inaceptables de este riesgo.
▶ Riesgo del modelo de negocio	Los complejos modelos de hojas de cálculo son ampliamente utilizados como herramientas operativas en los sistemas de los distintos agentes de mercado. Controles inadecuados o insuficientes podrían traer como consecuencia el posible uso de información incorrecta como fuente para la toma de decisiones sobre transacciones de *commodities* y exponer indebidamente a la empresa.

• • •

Commodities

▸ Riesgo de transformación del negocio	La transformación del negocio impulsada por el alto dinamismo del contexto económico puede crear brechas en los procesos y controles e introducir riesgos en las organizaciones.
▸ Riesgo de implementación de un sistema de gestión de riesgos de comercialización de *commodities* (CTRM)	La implementación de un sistema CTRM puede exponer a la empresa a riesgos significativos como consecuencia de la implementación inadecuada o insuficientes controles.
▸ Riesgo de ciberseguridad	Los sistemas operativos usados en la gestión de *commodities* usan información sensible de la empresa y pueden estar expuestos a riesgos de ciberseguridad.

Auditorías de alto impacto

Riesgo de transformación del negocio

Objetivo: Evaluar el estado actual y futuro de los procesos y controles

Preguntas clave a considerar

- ¿Cómo se han adaptado las políticas y los controles para gestionar los riesgos de nuevas actividades del negocio? ¿Se requieren políticas y controles más sólidos para estar a la altura de actividades más complejas?
- ¿Cómo han impactado los cambios organizacionales en la separación de tareas en los procesos clave de *back office*, *middle office* y *front office*?

Auditorías de alto impacto	Preguntas clave a considerar
Riesgo de implementación de un sistema gestión de riesgos de comercialización de *commodities* (CTRM) **Objetivo:** Evaluar los riesgos del estado futuro de los procesos del negocio y del uso de la funcionalidad nativa del paquete CTRM para apoyar el diseño de controles del estado futuro	▸ ¿Se ha evaluado el conjunto completo de funciones de control de la CTRM para los procesos y controles del estado futuro? ▸ ¿Se han revisado los procesos en su estado futuro -tanto aquellos basados en sistemas, como los que no lo están- en cuanto a las implicancias de riesgos y controles?
Riesgos de ciberseguridad **Objetivo:** Evaluar el proceso y los controles tecnológicos para proteger los datos en la CTRM y el ecosistema tecnológico relacionado	▸ ¿Se ha protegido la CTRM, las hojas de cálculo clave y otros datos importantes contra amenazas internas y externas? ▸ ¿Se han considerado los riesgos de un incidente de ciberseguridad para la capacidad de hacer negocios de forma competitiva en los mercados y la capacidad de gestionar transacciones de forma operativa a lo largo del ciclo de vida de estas?
Revisión completa del *front office* al *back office* **Objetivo:** Evaluar el diseño y la efectividad operativa de los procesos y controles en todo el ciclo de vida de las transacciones	▸ ¿Los controles del *back office*, *middle office* y *front office* corresponden a las mejores prácticas de la industria? ▸ ¿Se están cumpliendo las políticas, y los controles relacionados? ¿Se diseñaron y están funcionando como espera la gerencia?

Proyectos de inversión en infraestructura

Cada año, las organizaciones destinan grandes cantidades de dinero a construir nuevas instalaciones o a actualizar, expandir o dar mantenimiento a las ya existentes, para así respaldar las necesidades operativas de sus negocios. Estas inversiones son elementos esenciales para alcanzar los objetivos estratégicos de una organización. Con frecuencia, las organizaciones carecen de las capacidades internas y las competencias necesarias para monitorear adecuadamente sus programas de inversión en infraestructura y mitigar adecuadamente los riesgos asociados a ellos.

Existen diversos factores, tanto internos como externos, con la capacidad de impactar en el éxito de un programa de inversión en infraestructura:

- Riesgos macroeconómicos: Las fluctuaciones en los precios de materias primas o la disponibilidad de mano de obra, material y equipo pueden causar impactos sustanciales en el programa y en el rendimiento del presupuesto.
- Gobierno del programa de capital: La falta de transparencia en los reportes, así como los problemas asociados con la confiabilidad en la integridad de la información, la elaboración de métricas de desempeño y la elaboración de informes, pueden impactar negativamente en la capacidad de la gerencia para alertar inconsistencias de manera oportuna.
- Cambios dinámicos: La existencia de nuevos y constantes requerimientos de los *stakeholders*, el establecimiento de cronogramas agresivos, los posibles cambios en el entorno regulatorio, así como el advenimiento de nuevas tendencias en mercado cambiante, pueden afectar adversamente la capacidad de gestionar adecuadamente el alcance, la calidad, los presupuestos y plazos de un proyecto.
- Fraude, desperdicio y mal uso: Una supervisión deficiente, con controles inefectivos o insuficientes, puede traer como consecuencia una inadecuada asignación de recursos e incluso en su apropiación indebida, y estas pueden resultar en el incumplimiento de las líneas base del proyecto.
- Sistemas, procesos y controles independientes: La falta de integración de los proyectos con los sistemas de la organización, y la incapacidad de compartir información en tiempo real, pueden tener un impacto negativo en la capacidad de la empresa para monitorear y controlar eficazmente las transacciones críticas del proyecto y de reportar su nivel de avance de forma precisa y oportuna.

La gestión de los riesgos relacionados con los programas de inversión en infraestructura es esencial para lograr los objetivos trazados.

Los beneficios potenciales de realizar evaluaciones sobre los programas de capital incluyen:

- Optimizar el gobierno y los controles.
- Mejorar la transparencia y elaboración de informes.
- Hacer que la gestión de riesgos sea más proactiva.
- Mejorar la eficiencia de procesos y controles.
- Hacer que el monitoreo de cumplimiento sea más sólido.
- Realizar auditorías en tiempo real de las transacciones del proyecto.
- Detectar y prevenir el fraude, el desperdicio y el mal uso.
- Alinear el programa de capital y los objetivos organizacionales.

Proyectos de inversión en infraestructura

Auditorías de alto impacto	Preguntas clave a considerar
Gobierno y controles **Objetivo:** Evaluar las políticas, procesos, controles, sistemas e informes que se utilizan en el control de gestión de los programas de inversión en infraestructura	▸ ¿Se monitorean la estructura, las funciones, las responsabilidades y los controles en cuanto a la segregación de funciones de la organización? ▸ ¿Se han desarrollado procesos y controles de gestión de proyectos? ▸ ¿El Comité de Dirección o los líderes de la organización se involucran en las decisiones críticas de los proyectos? ▸ ¿Está alineada la entrega del proyecto propuesto con el perfil de riesgos del proyecto?
Proceso de adquisiciones y contratos **Objetivo:** Evaluar la idoneidad e integridad del proceso de adquisiciones y contratos	▸ ¿La organización cumple con las políticas y procedimientos aplicables? ▸ ¿Existe un proceso estándar para la identificación, evaluación y selección de proveedores? ▸ ¿La estrategia de contratación está alineada con el perfil de riesgos de la empresa? ▸ ¿Se evalúan los controles durante la fase inicial del proyecto y se actualizan en cada etapa de su ciclo de vida?
Cumplimiento de contratos **Objetivo:** Evaluar los costos incurridos, así como también los procesos, metodologías e informes de un proyecto de construcción en relación con los requisitos contractuales aplicables	▸ ¿Los costos incurridos y facturados están en conformidad con las estipulaciones contractuales? ▸ ¿Las solicitudes de cambio se documentan y aprueban? ▸ ¿Se monitorean las obligaciones del contratista relacionadas con la supervisión, gestión y control?

Auditorías de alto impacto	Preguntas clave a considerar
Costo y programa del proyecto **Objetivo:** Realizar una evaluación detallada para determinar si los costos incurridos están adecuadamente soportados y son consistentes con los términos y condiciones del contrato	▸ ¿Los costos incurridos se ven apoyados y son admisibles bajo los términos y condiciones del contrato? ▸ ¿Se monitorean el programa del proyecto, las pruebas de integridad incluyendo la lógica y la duración, y la evaluación de los cambios en la ruta crítica en el transcurso del tiempo? ▸ ¿Se soportan y justifican los retrasos en los proyectos?
Procesos de construcción **Objetivo:** Evaluar la ejecución de procesos clave para el cumplimiento de directrices operativas y el alineamiento con las mejores prácticas de la industria	▸ ¿Los procesos clave cumplen con las directrices operativas y están alineados con las mejores prácticas de la industria? ▸ ¿Se revisan y aprueban los pagos de construcción? ▸ ¿Se toman, documentan y monitorean los cambios, la calidad, el presupuesto, el cronograma y la gestión de riesgos de los proyectos? ▸ ¿El cierre de proyecto se hace de forma correcta, oportuna y documentada?

Ciberseguridad

Las amenazas de ciberseguridad continúan evolucionando y creciendo aparentemente sin ninguna regla o restricción en cuanto a quién puede ser atacado sin poder predecirlo. Los usuarios ya no necesitan obtener acceso físico a una instalación para dañar una organización. Ahora pueden tener acceso a través de ataques de *malware* o *phishing*, conexiones con terceros, nuevas tecnologías y otras nuevas rutas en desarrollo.

Las organizaciones deben enfocarse en la seguridad de TI y la seguridad de la información para evitar ser víctimas de ciberamenazas mediante el desarrollo de un programa cibernético de auditoría que aborde lo siguiente:

- La necesidad de mejorar los procesos existentes para la gestión de riesgos cibernéticos.
- Las tecnologías nuevas y rápidamente cambiantes.
- La contabilidad compleja y los requisitos regulatorios.
- Los entornos cibernéticos rápidamente cambiantes que requieren cambios en políticas y procedimientos.
- La necesidad de habilidades y competencias especializadas para identificar y mitigar los riesgos.
- Evaluación proactiva de riesgos emergentes y nuevos.

Ciberseguridad

El mundo digital ofrece diversos beneficios y oportunidades; sin embargo, los riesgos pueden haber sido subestimados

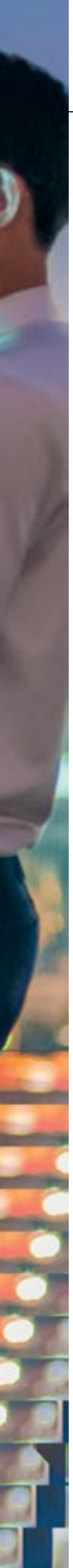
Auditorías de alto impacto	Preguntas clave a considerar
Gobierno y evaluación de riesgos **Objetivo:** Evaluar los procesos y los controles sobre la estructura y la supervisión del programa de gestión de riesgos de ciberseguridad de la entidad, incluyendo los procesos para identificar los riesgos que la organización enfrenta	▸ ¿La estructura de gestión de riesgos de la organización aborda los riesgos cibernéticos? ▸ ¿La organización cuenta con las habilidades especializadas necesarias para identificar y evaluar constantemente los riesgos cibernéticos?
Consciencia sobre la seguridad **Objetivo:** Evaluar los procesos y los controles de capacitación de usuarios para aumentar su consciencia y sensibilidad sobre los intentos de acceso no autorizado físico o lógico a la información y a los sistemas de la organización	▸ ¿Existen programas de capacitación para que los empleados aprendan a identificar mejor el acceso no autorizado físico o lógico a la información y los sistemas de la organización? ▸ ¿Los programas de capacitación se actualizan tomando en cuenta nuevos riesgos y se solicita que todos los empleados lo tomen?
Gestión de activos **Objetivo:** Evaluar los procesos y controles de la retentiva de un inventario integral de activos tecnológicos que tienen la capacidad de conectar la red de la organización	▸ ¿Se mantiene un listado integral de activos tecnológicos? ▸ ¿Los activos tienen dispositivos de seguridad adecuadamente instalados para proteger la información e identificar el acceso no autorizado? ▸ ¿Se dispone adecuadamente de los activos cuando es necesario?

Ciberseguridad

Auditorías de alto impacto	Preguntas clave a considerar
Gestión de identidades y accesos **Objetivo:** Evaluar los procesos y controles de identificación de usuarios autorizados, y de incorporación, modificación y eliminación de usuarios con acceso a la red de la organización	▸ ¿Se han implementado los siguientes procesos y controles? - Identificación de usuarios autorizados. - Incorporación, modificación y eliminación de usuarios con acceso a los sistemas y aplicaciones de la empresa.
Gestión de amenazas **Objetivo:** Determinar si los procesos y controles están listos para identificar, de forma temprana, amenazas potenciales o en desarrollo contra la organización	▸ ¿Se han implementado procesos y controles adecuados para identificar, de forma temprana, las amenazas potenciales o en desarrollo?
Gestión de vulnerabilidades **Objetivo:** Determinar si los procesos y controles están listos para abordar las vulnerabilidades de la organización	▸ ¿Existen los siguientes procesos y controles? - Identificación de vulnerabilidades en los activos tecnológicos conectados con la red. - Implementación de soluciones para abordar las vulnerabilidades.

Auditorías de alto impacto	Preguntas clave a considerar
Gestión de riesgos por proveedores **Objetivo:** Evaluar los procesos y controles de los servicios de terceros y los proveedores de la cadena de suministro	▸ ¿La organización puede dar un listado de todos sus proveedores? ▸ ¿Se comprende el propósito de una relación con cada proveedor? ▸ ¿Se han implementado procesos y controles para obtener proveedores adecuadamente? ▸ ¿Se realiza una evaluación de riesgos por proveedor para entender las vulnerabilidades que podría causar cada relación?
Clasificación de datos **Objetivo:** Evaluar los procesos y controles de la clasificación (por ejemplo: pública, interna, confidencial) de información en la red	▸ ¿La clasificación de información incluye información pública, interna y confidencial? ▸ ¿Se han implementado adecuadamente los requisitos de protección relacionados? ¿Son efectivos?
Monitoreo de seguridad **Objetivo:** Evaluar los controles del monitoreo de la actividad de la red y de la aplicación	▸ ¿Se han implementado procesos y controles suficientemente adecuados para detectar anomalías y otros comportamientos inusuales que pueden indicar que un usuario no autorizado ha obtenido o está obteniendo acceso al sistema?
Respuesta ante incidentes **Objetivo:** Evaluar los procesos y controles de los procedimientos de respuesta que la gerencia utiliza cuando se detecta una actividad inusual	▸ Cuando se detecta actividad inusual, ¿la organización cuenta con procesos para identificar oportunamente el incidente y abordar adecuadamente los problemas? ▸ ¿Existen procesos para abordar el punto débil que llevó al incidente?

Derivados y coberturas



Muchas compañías, independientemente de su tamaño, están expuestas a los riesgos de fluctuación de tipos de cambio, tasas de interés y precios de *commodities*. Algunas de ellas utilizan instrumentos derivados para gestionar la volatilidad de sus flujos de caja y su rentabilidad, causada principalmente por dichos riesgos.

Los instrumentos derivados y la contabilidad de cobertura son herramientas poderosas que las compañías utilizan para mitigar riesgos muchas veces con gran eficacia, pero requieren una gestión prudente ya que los derivados se reconocen a un valor razonable y son volátiles. Además, hay una literatura contable extensa y compleja sobre su utilización, y el uso de derivados es una de las mayores causas de revelaciones erróneas (particularmente las que se usan en relaciones de cobertura).

Los entornos débiles en cuanto a procesos y control interno podrían poner en riesgo a una compañía de muchas formas. Estos riesgos incluyen:

- El incumplimiento de las políticas corporativas al crear estrategias de cobertura.
- Una evaluación de riesgos inadecuada o respuestas inapropiadas a riesgos identificados.
- Un tratamiento contable inadecuado que afecte la valoración, los informes y las revelaciones.
- Inadecuada ejecución de una transacción comercial, de acuerdo con las políticas y procedimientos de la compañía.
- Inadecuada supervisión sobre la relación con las contrapartes en operaciones de cobertura.
- Falta de acceso a una tecnología adecuada y segura para dar soporte a las funciones de tesorería.

El uso de derivados toca diferentes áreas funcionales dentro de la compañía. Se necesitan procesos y controles sólidos en todas las funciones de la compañía para gestionar el riesgo y las declaraciones erróneas.

Derivados y coberturas

Auditorías de alto impacto

Gobierno y estrategia

Objetivo: Evaluar la estrategia de la organización para gobernar el uso de derivados y prácticas de cobertura

Preguntas clave a considerar

- ¿Las políticas y procedimientos existentes tienen brechas u oportunidades para implementar mejores prácticas de cobertura?
- ¿El Directorio supervisa las políticas y procedimientos del uso de derivados?
- ¿Los controles relacionados con los procesos del manejo de flujo de caja y la gestión de adquisiciones identifican potenciales brechas en la cobertura por exposición o inconsistencias?
- ¿Cuáles son los controles implementados para el proceso de selección de instrumentos de cobertura, incluyendo la comprensión de funciones del personal clave?
- ¿Hay algún proceso para seleccionar los socios comerciales y para saber si la recompensa del riesgo crediticio es apropiada?

Auditorías de alto impacto

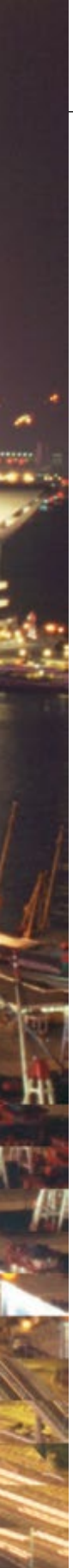
Ejecución de operaciones, contabilidad e informes, tecnología y cumplimiento regulatorio

Objetivo: Evaluar la idoneidad y eficacia de los procesos y controles

Preguntas clave a considerar

- ¿Hay procesos y aprobaciones para ejecutar operaciones y límites apropiados?
- ¿Existe un proceso formal y estándar para la proyección del flujo de caja y la recopiliación de información sobre exposiciones?
- ¿Se han implementado controles de segregación de funciones que sean la base para los protocolos de ejecución de coberturas y el proceso posterior de confirmación de operaciones?
- ¿Se implementaron controles de segregación de funciones que sean destinados a calificar para la contabilidad de cobertura realmente califican (designación, documentación y evaluación de eficacia)?
- ¿Se han implementado de manera efectiva controles para obtener y retar los valores razonables de los derivados, incluyendo una adecuada revelación de los niveles de jerarquía?
- ¿Se aprovecha adecuadamente la tecnología para apoyar las funciones de tesorería (p.e. sistemas bancarios, *softwares* de tesorería, hojas de cálculo)? ¿Existe una adecuada interfaz con los sistemas de contabilidad de la compañía?
- ¿Se han definido controles para garantizar el cumplimiento regulatorio aplicable?

Medio ambiente, salud y seguridad, y sostenibilidad



Riesgos clave del medio ambiente, la salud y seguridad, y la sostenibilidad

Estratégico

- Escasez de recursos naturales y materias prima — Alto
- Disminución de la participación en el mercado, de ingresos o precios de las acciones — Medio
- Exposición a riesgos imprevistos luego de realizar adquisiciones — Medio
- Riesgo por obligaciones legales, costo de cumplimiento — Medio
- Riesgos de mercado (p.e. precios de *commodities* o de los productos vendidos) — Medio

Cumplimiento

- El incumplimiento de normas y Reglamentos del Ministerio del Ambiente, de la Superintendencia Nacional de Salud, u otros órganos de regulación global o externa como la Administración de Seguridad y Salud Ocupacional (OSHA) — Alto
- Violaciones a la ley o políticas relacionadas al trabajo o derechos humanos — Medio
- Monitoreo e informes solicitados para las licencias y las regulaciones de medio ambiente, salud y seguridad — Medio
- Falta de monitoreo y cumplimiento de las directivas y regulaciones internacionales — Medio

Reputacional

- Auditorías de proveedores "*check-the-box*" ineficaces — Medio
- Exigencia de transparencia por parte de accionistas, clientes, empleados — Medio
- Leyes locales y normas emergentes para la elaboración de informes — Medio
- Licencia para operar — Medio
- Informes de sostenibilidad erróneos e incapacidad para "cumplir las promesas de marca" — Alto

Operativo

- Costos de energía y transporte en aumento — Medio
- Disrupciones en el negocio y en la cadena de suministro debido a climas extremos, retrasos en la obtención de licencias — Medio
- Gestión y eliminación de desechos peligrosos — Medio
- Riesgos operativos relacionados con el ambiente y la seguridad — Alto

Medio Alto

Medio ambiente, salud y seguridad, y sostenibilidad

Los temas relacionados con el medio ambiente, salud, seguridad y sostenibilidad se están convirtiendo rápidamente en temas centrales y estratégicos para la gestión de riesgos de las compañías.

Según el Informe Global de Riesgos 2017 del Foro Económico Mundial, los riesgos relacionados con el ambiente han sido considerados entre los mayores riesgos a nivel mundial durante los últimos siete años del Informe[1]. Los hallazgos recopilados para el año 2017 sostuvieron e incrementaron la postulación de esta tendencia, y los riesgos relacionados al medio ambiente (por ejemplo el fracaso en mitigar el cambio climático, la potencial crisis de agua, entre otros) se posicionaron en los top 5 riesgos a nivel global en términos de probabilidad e impacto. Además, mientras que los eventos recientes de climas extremos han intensificado los riesgos medioambientales aún más, el universo más amplio de riesgos de salud, seguridad ocupacional y sostenibilidad, continúan expandiéndose a temas sociales, reputacionales, y de salud y seguridad, entre otros asuntos.

Esto representa un gran desafío para las compañías con presencia global cuyas operaciones se basan en recursos naturales o generan importantes impactos ambientales y sociales, ya que sus principales *stakeholders* exigen cada vez más transparencia sobre el modo en que las compañías operan y abordan estos riesgos, lo cual termina convirtiendo un pedido en casi una orden de acción inmediata con carácter urgente.

Al respecto, la Auditoría Interna (AI) juega un rol clave al prestar asistencia específica a las compañías al identificar y responder a estos riesgos participando activa y colaborativamente con las áreas de seguridad y salud, sostenibilidad, asuntos legales, de cumplimiento y de finanzas. La AI puede ayudar a la organización a descubrir los riesgos que enfrenta, comprender sus impactos en el negocio y las operaciones, y determinar los pasos para abordarlos en la forma más eficiente como parte de su plan o programa de gestión de riesgos empresariales (ERM). Al hacer esto, la AI puede ayudar a la compañía a reducir el riesgo de afectar la imagen o la marca, la participación en el mercado, los ingresos y operaciones, penalidades por afectación a terceros y el riesgo de multas por incumplimiento.

Auditorías de alto impacto

Planeamiento y ejecución del programa

Objetivo: Evaluar programas y procesos de gestión medio ambiental y de seguridad y salud ocupacional

Preguntas clave a considerar

- ¿Los programas y procesos mediambientales y de seguridad y salud ocupacional abordan lo siguiente:
  - Gobierno del cumplimiento regulatorio mediambiental y de seguridad y salud ocupacional?
  - Identificación, cumplimiento y monitoreo de requisitos regulatorios?
  - Procesos y procedimientos internos mediambiental y de seguridad y salud ocupacional?

[1] Foro Económico Mundial, Informe Mundial de Riesgos 2017, 12va edición.

Auditorías de alto impacto	Preguntas clave a considerar
Cumplimiento regulatorio **Objetivo:** Evaluar los problemas o preocupaciones sobre el cumplimiento regulatorio	▸ ¿Se evalúan problemas o preocupaciones específicos sobre el cumplimiento regulatorio para apoyar lo siguiente: - Ahondar en los temas normativos y de cumplimiento a través de requisitos regulatorios identificados que guarden relación con la sostenibilidad?
Tecnología de la Información **Objetivo:** Evaluar la habilitación de TI que se aprovecha para apoyar las operaciones y las actividades de cumplimiento	▸ ¿Los procesos de recopilación de datos son consistentes en todas las unidades y geografías del negocio? ▸ ¿Se informa el cumplimiento de forma oportuna, exacta y eficiente? ▸ ¿Los informes y los tableros de indicadores internos son completos y exactos?
Informes de sostenibilidad **Objetivo:** Evaluar los controles de los informes públicos sobre información no financiera	▸ ¿Los controles de los informes públicos sobre información no financiera abarcan lo siguiente: - Gobierno, políticas y procedimientos? - Datos? - Tangibilidad de indicadores clave de desempeño? - Procedimientos para la elaboración de informes a través de normas aceptadas? - Afirmaciones y aseveraciones del informe?

Ley de Protección de Datos Personales (LPDP)

Desde mayo de 2015 se encuentra en pleno cumplimiento en Perú la Ley de Protección de Datos Personales (LPDP), la cual fue promulgada en 2011 y reglamentada en 2013. Esta normativa definió los principales conceptos asociados a la gestión de la información de personas por parte de las empresas y de la forma en que estos datos deben ser tratados.

Los avances tecnológicos y el cambio en la forma de hacer negocios han modificado la manera en que las organizaciones tratan la información personal de sus grupos de interés (colaboradores, clientes, proveedores, entre otros). En esa línea, tomando como referencia técnica las normas europeas de protección de información personal (que acaban de ser actualizadas en mayo de 2018, a través del nuevo Reglamento General de Protección de Datos - RGPD), el gobierno peruano genera exigencias de cumplimiento que incluyen requisitos estrictos y restrictivos respecto del uso indiscriminado de la información de las personas, poniendo énfasis en la obtención de consentimientos de uso de información, exposición de finalidades de utilización de la información y la adopción de medidas de seguridad para la protección y adecuado tratamiento de los datos. De no cumplirse, existen multas normadas que van desde 0.5 a 100 Unidades Impositivas Tributarias - UIT (que para el ejercicio fiscal 2018 asciende a S/4,150 por UIT).

La LPDP exige que la organización sea capaz de demostrar que cumple los requisitos de forma efectiva. Adoptar una estructura basada en controles internos que abarque las tres líneas de defensa de una organización brindará un enfoque disciplinado e integral para abordar el riesgo de privacidad y el cumplimiento.

Como parte de la LPDP, hay muchos riesgos de privacidad que las compañías deben cubrir y mitigar, y la AI es un gran elemento de defensa de una compañía para enfrentar esos riesgos. Las organizaciones deberían sacar provecho de los valiosos conocimientos de la AI sobre las áreas de negocio, procesos o sistemas clave, que generan el mayor riesgo de privacidad para la organización, y así realizar auditorías sobre el nivel de cumplimiento de la LPDP. La función de Auditoría Interna puede ayudar a una compañía a lograr el principio de finalidad y legalidad que está profundamente arraigado a la LPDP.

Ley de Protección de Datos Personales (LPDP)

Auditorías de alto impacto	Preguntas clave a considerar
Revisión del plan de implementación de la LPDP **Objetivo:** Realizar una revisión del plan de implementación de la LPDP de la organización para evaluar el alineamiento con la norma, los aportes considerados y la calidad del análisis	▸ ¿Cuáles son los conceptos que se considerarán dentro de la elaboración del plan de LPDP? ▸ ¿Existen criterios de priorización de elementos del plan de implementación claros y bien definidos? ▸ ¿Las actividades del plan de LPDP son claras para los responsables, así como su nivel de involucramiento y retroalimentación para llegar al nivel de avance requerido? ▸ ¿El plan es retado periódicamente y complementado con cualquier variación en la normativa de la LPDP?
Evaluación de madurez sobre el cumplimiento con la LPDP **Objetivo:** Realizar una evaluación rápida y de alto nivel del programa de privacidad de la organización y del nivel de cumplimiento con la LPDP	▸ ¿Existen áreas en las que los procedimientos y controles no se encuentren alineados con los requisitos regulatorios? ▸ ¿Cuál es el nivel de madurez que tiene la organización tomando como base las prácticas líderes y recomendaciones de la industria que involucran a las personas, los procesos y facilitadores tecnológicos?

Auditorías de alto impacto

Evaluación enfocada y profunda de las brechas en el programa de adecuación a la LPDP

Objetivo: Realizar la evaluación de un área del negocio en específico (por ejemplo, recursos humanos), un proceso (por ejemplo, desarrollo de productos) o sistemas (por ejemplo, almacenamiento en la nube), con el fin de evaluar los controles actuales que fueron implementados para cumplir con los requisitos de la LPDP

Preguntas clave a considerar

- ¿Cómo se recopila la información personal?
- ¿Quién tiene acceso a la información personal? (Sea personal interno o externo a la organización).
- ¿Cuánto tiempo se guarda la información personal una vez que ya no se necesita?
- ¿Existen brechas e ineficiencias en cuanto a la protección de datos personales?

Comercio internacional

El comercio internacional comprende una serie de leyes complejas relacionadas con la circulación transfronteriza de bienes, *software* y tecnología, que inlcuye la gestión con aduanas, controles de exportación, sanciones económicas, acuerdos de libre comercio, programas de ahorro arancelario y medidas *antidumping*, entre otros. Algunas de dichas leyes están armonizadas a nivel global, lo cual permite contar con procesos y controles comunes; en cambio, otras son propias de las jurisdicciones locales.

Las empresas que están involucradas en la circulación transfronteriza de bienes afrontan riesgos propios del comercio global, pero ciertos factores pueden generar incluso mayores riesgos. Los riesgos del comercio global se originan comúnmente debido a controles y procesos globales inadecuados en las funciones de exportación e importación. La naturaleza de los productos y tecnologías de una empresa podría incrementar el riesgo; por ejemplo, los productos tecnológicos, químicos, aeroespaciales o militares que están muy reglamentados.

Las empresas que pagan muchos aranceles o impuestos sobre consumos específicos, o aplican acuerdos de libre comercio u otras técnicas de reducción de aranceles e impuestos, pueden enfrentar mayores riesgos. Frecuentemente, los riesgos del comercio global se vuelven más visibles cuando la empresa cambia, ya sea a través de adquisición o desinversión, reorganización o entrada a nuevos mercados.

El entorno normativo para los comerciantes globales es muy dinámico, por eso se requieren habilidades que abarquen múltiples funciones y a través de múltiples países. Puede resultar difícil para los equipos internos evaluar con precisión la gestión del comercio internacional de su empresa; sin embargo, con una planificación eficaz, un uso de recursos específicos para esta área y un análisis de datos es posible para los equipos de Auditoría Interna evaluar con mayor precisión el nivel de cumplimiento de su empresa.

Comercio internacional

Auditoría interna sobre el comercio internacional

Análisis cualitativo

- Identificar áreas de riesgo
- Conocer el estado actual de la organización y sus procesos
- Evaluar el estado actual vs. prácticas líderes

- Conocer la organización en torno al comercio internacional
- Conocer sus procesos y controles internos
- Conocer la industria, el producto y el cliente
- Conocer la empresa y cómo esta encaja en la estructura de comercio del cliente
- Evaluar la capacidad de la empresa para gestionar riesgos
- Identificar áreas de mejora

Análisis cuantitativo

- Obtención de información (data) sobre la importación y exportación
- Anlisis de información (*Data analytics*)
- Comparación (*benchmarking*) y mejora

- Obtener información regulatoria sobre la importación y exportación
- Comprender y analizar los flujos de comercio
- Contrastar los análisis cualitativos con los resultados cuantitativos
- Aprovechar el equipo global de EY
- Comparar el estado actual con procesos globales análogos
- Identificar las oportunidades de ahorro

Auditorías de alto impacto

Gobierno

Objetivo: Evaluar la estructura, procedimientos y políticas existentes en la empresa para evaluar su grado de adecuación y efectividad

Preguntas clave a considerar

- ¿Cómo está organizada su función de comercio internacional? ¿Está centralizada o descentralizada? ¿Es global, regional o local?
- ¿Ha designado posiciones específicas para gestionar los procesos de exportación e importación?
- ¿La gerencia es consciente de los riesgos de exportación y aduanas?
- ¿Tiene políticas y procedimientos documentados sobre procesos de exportación y aduanas?
- ¿Cuenta con métricas para evaluar la efectividad de sus operaciones de comercio internacional?
- ¿Cuáles son los objetivos y estrategias definidas del área?

Comercio internacional

Auditorías de alto impacto

Procesos de importación

Objetivo: Evaluar los procesos de aduana y el cumplimiento de las normas aduaneras

Preguntas clave a considerar

- ¿En qué países usted es importador para fines aduaneros?
- ¿Cuál es su volumen de importación por país? ¿Cuáles son sus costos globales de aduanas por país?
- ¿La empresa puede acceder a reducción, eliminación o aplazamiento de aranceles a través de acuerdos comerciales o programas comerciales especiales (perfeccionamiento pasivo o activo, depósitos aduaneros, devoluciones)?
- ¿La empresa realiza auditorías post-importación y hace seguimiento a las observaciones identificadas?
- ¿La compañía ha sido auditada o tiene algún litigio en proceso con autoridades aduaneras en alguna jurisdicción?
- ¿La compañía importa productos de empresas relacionadas? De ser así, ¿tiene contratos con dichas empresas?
- ¿La compañía realiza adiciones (comisiones, regalías) o deducciones (gastos de flete, costos de instalación) sobre sus valores de importación?

Auditorías de alto impacto

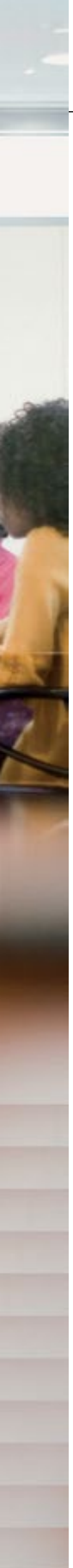
Procesos de exportación

Objetivo: Evaluar la efectividad de los procesos de exportación y el cumplimiento de las normas en materia de sanciones y controles de exportación

Preguntas clave a considerar

- ¿Para qué países la empresa es exportadora de productos?
- ¿Realiza negocios con países bajo embargo o sancionados?
- ¿Realiza ventas a través de distribuidores o directamente al cliente, o ambas?
- ¿Cuenta con un proceso para evaluar a sus socios potenciales, tanto externos como internos, comparándolos con listas negras?
- ¿Cuenta con un proceso de obtención de licencia y clasificación de exportaciones?
- ¿Exporta productos que requieren de algún tipo de especificación o que están sujetos a controles en el país de llegada?

Impuestos indirectos



En la evolución reciente de las economías de los países, muchos han enfocado sus esfuerzos de recaudación en el desarrollo e impulso de impuestos indirectos. Esta situación genera una exposición creciente de los contribuyentes a riesgos de incumplimiento, que podrían impactar adversamente a las empresas a través de penalidades y sanciones.

A continuación se incluyen ciertos asuntos relacionados con la gestión de impuestos indirectos que están despertando la atención de las empresas y podrían ser considerados en los procesos de evaluación de riesgos y diseño de un plan de auditoría:

1. **Fallas en la evaluación del impacto de las grandes iniciativas empresariales en el cumplimiento tributario**: Las grandes iniciativas empresariales, como la migración a un entorno de servicios compartidos, la implementación de sistemas de planificación de recursos, el desarrollo de cadenas de suministros o incluso las transformaciones de los modelos operativos de las empresas, son ejemplos de iniciativas en las que resulta crítico tener en cuenta un análisis del impacto de los impuestos indirectos. Cuando no se tiene en cuenta un análisis de esta naturaleza, el incumplimiento tributario, las ineficiencias en el uso de recursos y falta de información de soporte para fines de cumplimiento surgen como preocupaciones de la empresa y fuentes de exposición a riesgos.

2. **Falta de disponibilidad de información**: Las áreas responsables de la gestión tributaria están, por lo general, entre las áreas más demandantes de información en las empresas. La falta de información transaccional precisa y accesible para fines tributarios es una de las principales causas de incumplimiento, sin contar con las ineficiencias y costos en exceso que genera para la organización.

3. **IGV y otros impuestos indirectos**: Los impuestos transaccionales son una fuente de exposición continua a riesgos, ya que -debido a que gravan individualmente cada transacción- pueden generar obligaciones tributarias indirectas fuera del país. Además, para atender sus requerimientos, las empresas dependen en gran medida de la precisión de la información de la que disponen.

   Es un problema recurrente en las empresas la falta de recursos (conocimiento, personas, procesos y controles) adecuados para "unir los puntos" entre las transacciones comerciales realizadas por el negocio y su impacto tributario correspondiente.

   El cumplimiento tributario no consiste únicamente en la declaración y pago oportuno de impuestos. Este requiere una comprensión suficientemente minuciosa de las transacciones y procesos de negocio de la empresa, así como de sus implicancias tributarias y de cómo estas deben ser declaradas. Por esa razón, definir la estructura organizacional correcta para dar una adecuada atención a los requerimientos tributarios es un asunto complejo que las compañías deben siempre abordar.

Impuestos indirectos

Auditorías de alto impacto	Preguntas clave a considerar
Información tributaria **Objetivo:** Evaluar la naturaleza, disponibilidad e integridad de la información disponible y recursos de la empresa	▸ ¿Cuáles son las necesidades de información y recursos más críticos para el cumplimiento tributario eficaz y eficiente de la organización? ▸ ¿En qué parte de los procesos la falta de disponibilidad de información completa, precisa y confiable genera ineficiencias para la organización? ▸ ¿Cuál es el impacto de dichas ineficiencias y por qué se presentan? ▸ ¿Cómo se podrían resolver las brechas y cuáles podrían ser los beneficios de su solución?
IGV (impuestos indirectos) **Objetivo:** Evaluar la eficacia y eficiencia de los procesos existentes	▸ ¿La información requerida es recolectada de manera precisa, completa y confiable? ▸ ¿Existen controles para determinar si se ha calculado el impuesto con precisión? ▸ ¿Quién es responsable de los procesos relacionados con los impuestos indirectos? ¿Dicha persona tiene las habilidades necesarias para ejecutar las actividades de cumplimiento? ▸ ¿Existen oportunidades de ahorro en los impuestos?

Auditorías de alto impacto

Cumplimiento

Objetivo: Evaluar la efectividad, tanto del diseño como de la operatividad, de los controles relacionados con el cumplimiento tributario

Preguntas clave a considerar

- ¿Cuán eficiente es el proceso de recolección de información y cálculo de las provisiones de impuestos?
- ¿Los controles de cumplimiento están diseñados y funcionan eficazmente?
- ¿Se puede ser más eficiente sin perder confiabilidad?

Gestión de riesgos de seguros

El mundo de los seguros cambia constantemente, lo que genera que las compañías enfrenten incertidumbres al intentan responder las siguientes preguntas:

- ¿A dónde se está yendo el dinero de los seguros de la compañía?
- ¿El programa de seguros de la compañía es integral?
- ¿Todos los riesgos transferibles de la compañía están cubiertos por seguros?
- ¿Los proveedores relacionados con la gestión de riesgos de seguros están brindando el servicio correcto al precio correcto?
- ¿Se han implementado controles para asegurar razonablemente que los riesgos de seguros se están gestionando correctamente?

Con frecuencia, son las gerencias de finanzas quienes asumen la gestión de los riesgos de seguros, a pesar de que en ocasiones no cuentan con el personal especializado en este tipo de riesgos.

Asimismo, es común que las empresas confíen en la información y en las evaluaciones que obtienen de las compañías y corredores de seguros, sin cuestionar o retar su fiabilidad. Tampoco es raro encontrar que las funciones de gestión de riesgos de seguros de muchas empresas operan de forma aislada a la Gestión Integral de Riesgos de una compañía o que no se le supervisa adecuadamente.

Las compañías tienen la responsabilidad de mantener sus activos, sus obligaciones y a su personal adecuadamente protegidos mediante pólizas de seguros. Para lograrlo, deben tener presente las siguientes consideraciones:

1. Identificar y valorar los riesgos integrales del negocio
2. Evaluar la estrategia de retención y transferencia de riesgos
3. Gestionar los siniestros y el impacto potencial en los resultados del negocio
4. Revisar la gestión de los proveedores (p.e. corredores de seguros)
5. Evaluar la competencia del personal a cargo de la gestión de riesgos de seguros
6. Revisar los riesgos de cumplimiento de los contratos de seguros

Gestión de riesgos de seguros

Riesgos clave en la gestión de riesgos y seguros

▶ Medio ▶ Alto

Identificación y valoración de riesgos	▶ No identificar todos los riesgos críticos para el negocio.
	▶ No evaluar adecuadamente las contingencias operacionales.
	▶ Subestimar o sobreestimar el impacto potencial o la probabilidad de ocurrencia de un riesgo.
Estrategia de retención y transferencia de riesgos	▶ Subestimar o sobreestimar los límites de retención de riesgos de la compañía, generando un uso excesivo o insuficiente de la inversión en seguros.
	▶ Escoger los productos o formas inadecuadas de transferencia de riesgos.
Gestión de siniestros	▶ Tomar decisiones incorrectas o tardías sobre los siniestros debido al uso de información incompleta o inexacta.
	▶ Generar un impacto financiero negativo debido a las decisiones de los administradores de siniestros.
	▶ No contar con controles clave efectivos que permitan cumplir adecuadamente con los procesos de gestión de siniestros establecidos.
Gestión de proveedores	▶ No establecer cláusulas contractuales claras y precisas.
	▶ Inadecuado monitoreo o falta de transparencia en las relaciones con los proveedores.

Personal a cargo de la gestión de riesgos de seguros

- Las funciones y responsabilidades no están definidas o documentadas de forma clara y precisa, lo que no permite una adecuada medición del logro de objetivos.
- Uso ineficiente de recursos para la gestión de riesgos de seguros.

Cumplimiento

- Pérdidas económicas debido a procesos internos, personas, sistemas o eventos externos ineficaces o inadecuados.
- Incumplimiento de contratos, normas y regulaciones.
- Incapacidad de un tercero de cumplir con un contrato.

Gestión de riesgos de seguros

Auditorías de alto impacto	Preguntas clave a considerar
Evaluación del programa de seguros **Objetivo:** Identificar brechas en la estructura del programa de seguros de la compañía, para proponer recomendaciones basadas en prácticas líderes y estudios de *benchmark*	▸ ¿Las primas, deducibles y límites de retención de la compañía son similares a los de otras empresas? ▸ ¿Se ha realizado un análisis de brechas y coberturas del programa de seguros? ▸ ¿El departamento de riesgos de seguros opera de acuerdo a los controles y procesos formalizados?
Gestión de proveedores **Objetivo:** Revisar el proceso de gestión de proveedores de seguros, realizar un análisis de brechas e identificar oportunidades de mejora	▸ ¿Las cláusulas de las pólizas de seguros son claras y precisas? ▸ ¿Los contratos con los proveedores de la gestión de riesgos de seguros son claros y precisos? ▸ ¿Es posible reducir los costos y hacer más eficiente el proceso de gestión de proveedores?

Auditorías de alto impacto	Preguntas clave a considerar
Gestión de siniestros **Objetivo:** Revisar los procesos de gestión de siniestros, realizar un análisis de brechas e identificar oportunidades de mejora para reducir las pérdidas del negocio	▸ ¿Se han revisado los costos de siniestros para identificar algún ahorro de costos por siniestros? ▸ ¿Se manejan eficazmente las pérdidas? ▸ ¿Cómo determina la organización la razonabilidad y pertinencia de las obligaciones pendientes?
Procesos de exportación **Objetivo:** Hay dos opciones en lo que concierne a estudios de aseguradoras cautivas: 1. Realizar un análisis de viabilidad de la creación de una aseguradora cautiva 2. Realizar un análisis del desempeño de una aseguradora cautiva	▸ ¿Son adecuadas la determinación de las primas y la estructura de capital y reservas técnicas? ▸ ¿Existen deficiencias en el proceso de inversiones de la aseguradora cautiva? ▸ ¿Se aplican correctamente las regulaciones fiscales de los seguros cautivos?

Propiedad intelectual

Ahora más que nunca, las empresas se enfrentan directamente a cambios sin precedentes en lo que respecta a la adopción de nuevas e innovadoras tecnologías. La gran mayoría de las empresas se encuentra a la vanguardia como pioneras en este mundo de rápida evolución. Desde las gerencias de primer nivel hasta cada una de las áreas de la empresa, la innovación se ha convertido en una fuerza impulsora. A medida que las empresas avanzan rápidamente, deben preguntarse si han tomado las decisiones apropiadas para identificar adecuadamente sus activos de propiedad intelectual (PI) y si se han establecido los controles apropiados para proteger y mitigar los riesgos potenciales asociados a sus derechos.

Existen riesgos significativos asociados con la PI que son inherentes al ciclo de vida y que podrían dar lugar a consecuencias negativas en términos económicos, financieros, de competencia y reputación para las organizaciones, si es que no se controlan y gestionan apropiadamente.

Las empresas se deben preocupar por proteger sus activos de PI y confirmar que sus empleados no solo cuentan con el conocimiento apropiado, sino que son conscientes de sus responsabilidades y obligaciones para con la empresa en lo concerniente a los siguientes temas:

- Información confidencial
- Información de propiedad exclusiva
- Secretos comerciales
- PI de terceros
- Innovaciones
- Marca registrada
- Derechos de autor
- *Software*

Propiedad intelectual

Riesgos de la propiedad intelectual

▶ Medio ▶ Alto

Información sensible

- ▶ Los empleados involucrados en la generación de innovaciones, creaciones o mejoras que constituirían activos de PI podrían involuntariamente filtrar información sensible de la empresa, generando impedimento o bloqueo legal que resultarían en la pérdida de derechos de PI.
- ▶ Revelación de secretos comerciales que lleven a la exposición de información sensible, lo cual conllevaría a una pérdida en la ventaja competitiva.

Conocimiento y consciencia de los empleados

- ▶ Falta de conocimiento y consciencia sobre PI por parte de los empleados, lo cual conlleva a una ejecución ineficaz de políticas y procedimientos, así como a la incapacidad de identificar, recolectar y proteger adecuadamente los activos de PI de la empresa.

Daño a la reputación

- ▶ Daño a la reputación de la empresa o marca debido a un mal manejo y/o a la falta de protección y exposición de los derechos de PI de la empresa o de terceros.

Auditorías de alto impacto

Gobierno y evaluación de riesgos

Objetivo: Evaluar los controles relacionados al proceso de supervisión y monitoreo de la estrategia y gestión de la PI

Preguntas clave a considerar

- ¿Las políticas y procedimientos de la organización abordan adecuadamente los riesgos asociados a la PI?
- ¿La organización cuenta con las habilidades especializadas necesarias para identificar y evaluar constantemente los riesgos asociados a la PI?

Software de código abierto

- El uso de *software* y códigos abiertos obtenidos de comunidades con términos y condiciones desfavorables puede resultar en la pérdida de derechos de PI y de códigos desarrollados por la empresa.

Propiedad intelectual

- Uso no autorizado o inapropiado de los activos de PI de terceros como secretos comerciales y tecnologías patentadas (violación).
- Pérdida de los derechos de propiedad intelectual (DPI) por una protección o gestión inapropiada.

Gobernabilidad y estrategia

- Estrategia de PI no alineada con los requisitos comerciales.
- Falta de una estrategia estructurada y bien pensada mientras la organización desarrolla procesos de innovación, creación o mejora.

Auditorías de alto impacto

Conocimiento y consciencia

Objetivo: Evaluar los controles relacionados al proceso de capacitación de usuarios para aumentar su consciencia y cuidado frente a intentos físicos o informáticos de acceso no autorizado a los sistemas e información de la empresa

Preguntas clave a considerar

- ¿Existen programas de capacitación para aumentar la consciencia y mejorar los conocimientos de los empleados para que puedan identificar de manera eficaz los posibles activos de PI y entender sus obligaciones y riesgos asociados?
- ¿Los programas de capacitación están actualizados para enfrentar los nuevos riesgos y cambios en la legislación?

Propiedad intelectual

Auditorías de alto impacto	Preguntas clave a considerar
Gestión de accesos y activos **Objetivo:** Evaluar los controles relacionados al proceso de identificación y resguardo de los activos de PI que la organización posee o utilice	▸ ¿Existen procesos y controles para identificar activos obtenidos o creados recientemente? ▸ ¿Se mantiene un inventario de activos (por ejemplo, de secretos comerciales)? ▸ ¿Los sistemas tienen salvaguardas adecuadas para protegerlos contra accesos no autorizados y poseen un registro para identificar quiénes acceden y en qué momento?
Gestión de riesgos de terceros **Objetivo:** Evaluar los controles relacionados al proceso de uso y protección de los activos de PI de terceros	▸ ¿La organización puede proveer un listado de los activos de terceros que utiliza o posee, y las fuentes de dichos activos? ▸ ¿La organización entiende su obligación de proteger los derechos de PI de terceros? ▸ ¿Se cumplen los procesos y controles establecidos para contraer ciertas obligaciones contractuales relacionadas con la PI?

Auditorías de alto impacto	Preguntas clave a considerar
Monitoreo de seguridad **Objetivo:** Evaluar los procesos y controles relacionados con el monitoreo de la actividad de aplicaciones y redes	▸ ¿Los procesos y controles establecidos son suficientes para detectar anomalías u otros comportamientos inusuales que indiquen que un usuario no autorizado ha obtenido o está obteniendo acceso a información de PI en el sistema?
Respuesta ante incidentes **Objetivo:** Evaluar los procesos y controles relacionados con los procedimientos de respuesta que la gerencia emplea cuando se detecta alguna actividad inusual	▸ Si se identifica un incidente, ¿los empleados saben a qué persona deben reportarlo? ▸ ¿Los empleados conocen los protocolos para reportar el incidente con el fin de mitigar cualquier riesgo adicional?

Gobernanza de TI

A medida que el mundo de los negocios continúa digitalizándose y las plataformas tecnológicas se vuelven más complejas, las expectativas de las organizaciones de TI siguen aumentando. El rol de los ejecutivos de negocios también está evolucionando, ya que deben estar en condiciones de poder comprender y gestionar mejor la tecnología y los riesgos asociados para optimizar el desarrollo de su estrategia comercial. El riesgo de una iniciativa fallida, el aumento de los costos de TI y las inquietudes sobre incidentes relacionados con TI que vienen aparecido en las noticias ultimamente, como pérdidas de datos o fallas de seguridad, son solo algunas de las preocupaciones que surgen entre los ejecutivos y directivos de las empresas. Como resultado, los líderes empresariales exigen que los profesionales de TI proporcionen una diferenciación estratégica a través de sistemas, tecnologías de infraestructura y aplicaciones innovadoras con el nivel apropiado de supervisión y un sólido marco de control.

Los sistemas complejos representan perfiles de riesgo complejos, y se espera que los profesionales de TI desarrollen e implementen sistemas y aplicaciones bajo una tremenda presión de tiempo. Muchas veces, los perfiles de riesgo asociados con tales sistemas complejos no son completamente comprendidos, son subestimados o no son correctamente reportados. Asimismo, el riesgo de TI global y su impacto en las operaciones de la compañía, y potencialmente en la marca corporativa, pueden no ser completamente entendidos entre los más altos ejecutivos. Las empresas deben considerar ajustar su modo de pensar y su enfoque hacia el riesgo de TI con el fin de abordar la nueva norma, puesto que el perfil de riesgo de TI y el panorama de amenazas están cambiando rápidamente y los riesgos están aumentando.

Más que nunca, es necesario que el Directorio, el comité de auditoría, la gerencia ejecutiva, el asesor general y el director de riesgos trabajen junto con los líderes de TI, incluyendo a los oficiales de seguridad de la información, para comprender y abordar la exposición al riesgo, el enfoque y la preparación de la organización. Las empresas deben implementar un sólido programa de gestión de riesgos que gestione de forma proactiva y eficaz los riesgos de TI, incluidos los riesgos cibernéticos.

Es importante que las funciones de TI puedan abordar eficazmente las siguientes preguntas:

- ¿Puede la gerencia articular su estrategia para identificar, mitigar y monitorear los riesgos de TI para el comité de auditoría?
- ¿Cómo y cuándo la gerencia se convence de que ha identificado todos los riesgos de TI clave que impedirían a la empresa alcanzar sus objetivos e iniciativas estratégicas?
- ¿Cómo supervisa la gerencia la efectividad y relevancia del marco de evaluación de riesgos de TI, a la luz de las tecnologías en rápida evolución?

Los auditores internos de TI deben conocer los desarrollos tecnológicos y los riesgos asociados y deben participar de manera proactiva en los proyectos de implementación desde el principio. Solo entonces las organizaciones de auditoría interna estarán en la condiciones de evaluar objetivamente la dirección y el soporte de las estructuras y los procesos actuales de gobierno de TI.

Las revisiones y auditorías centradas en los sistemas y riesgos de TI a nivel de implementación son formas efectivas de ayudar a la gerencia a mitigar los riesgos tecnológicos.

Gobernanza de TI

Auditorías de alto impacto	Preguntas clave a considerar
Estrategia de gestión de riesgos de TI **Objetivo:** Evaluar la solidez de la estrategia de gestión de riesgos de TI de la organización y determinar si el marco de evaluación de riesgos es capaz de abarcar tecnologías nuevas y complejas	▸ ¿Qué tan bien TI identifica los riesgos? ▸ ¿Qué acciones se toman una vez que se identifica un riesgo? ▸ ¿Se siguen los procesos de gestión de riesgos de TI? ▸ ¿El programa de riesgos de TI cubre todas las tecnologías? ▸ ¿La responsabilidad de la cobertura de riesgos está claramente definida? ▸ ¿Cómo se identifican, remedian o aceptan los riesgos de TI?
Gobernanza de TI **Objetivo:** Evaluar el marco y las estructuras de gobernanza de la organización para mitigar los riesgos clave del gobierno de TI	▸ ¿Tiene la organización un marco de evaluación de riesgos de TI? ¿Este se alinea con los marcos de gobernanza establecidos? ▸ ¿Existen procesos formales de gobierno de TI? ▸ ¿Qué se puede hacer para aumentar la confianza empresarial en el gobierno de TI? ▸ ¿Los procesos y requisitos de gobierno de TI son aplicables a todas las tecnologías? ▸ ¿Existen estatutos, responsabilidades y mandatos formales documentados y seguidos por comités directivos clave?

Auditorías de alto impacto	Preguntas clave a considerar
Gestión de riesgos de TI **Objetivo:** Evaluar los riesgos de TI, los planes de medidas correctivas y el progreso en relación con esos planes para abordar los problemas observados	▸ ¿Se realiza una evaluación integral de riesgos para identificar todos los riesgos de TI? ▸ ¿Es efectivo el proceso de evaluación de riesgos de TI? ▸ ¿Cómo se puede mejorar el proceso? ▸ ¿Los planes de medidas correctivas incluyen suficientes detalles? ¿La gerencia monitorea el progreso? ▸ ¿Hay una hoja de ruta para iniciar mejoras?
Habilitación tecnológica **Objetivo:** Evaluar la necesidad del uso de un paquete de *software* de gobierno, riesgo y cumplimiento	▸ ¿Se utiliza algún *software* de gobernanza, riesgo y cumplimiento (GRC, por sus siglas en inglés) dentro de la organización? De ser así, ¿con qué eficacia se está utilizando (por ejemplo, nivel de madurez, uso de la funcionalidad e informes de riesgos)?

Arrendamiento (*Leasing*)

Los modelos de negocio de muchas empresas incluyen importantes operaciones de arrendamiento. Si este es el caso de su empresa, es recomendable considerar, en sus evaluaciones de riesgos y plan de auditoría, los riesgos de reporte financiero relacionados con el tratamiento contable de estas operaciones.

A continuación se muestran algunos de los aspectos más relevantes que deben ser incluidos en su evaluación:

- **Contabilidad y finanzas**: Es importante encargar a un experto en las Normas Internacionales de Información Financiera (NIIF), la evaluación de la correcta adaptación de las políticas contables de la compañía a las regulaciones aplicables. Es probable que exista la necesidad de realizar actualizaciones sobre dichas políticas y dar a estas una apropiada y oportuna divulgación en toda la organización. En esta evaluación, es clave identificar las áreas en las que la gerencia necesitará hacer más estimaciones contables, y evaluar la necesidad de reforzar sus capacidades y recursos para que pueda realizarlas de manera óptima.

- **Procesos de negocio**: Es recomendable revisar los procesos actuales y el sistema de control interno para evaluar la capacidad de gestionar adecuadamente los contratos existentes, que sean de arrendamiento o que contengan la figura de uno, con la finalidad de darle un adecuado tratamiento. En adición, es necesario determinar en qué casos se requiere hacer reevaluaciones sobre el tratamiento que se da a ciertos contratos, sobre la base del juicio experto.

Arrendamiento (*Leasing*)

- **Impuestos**: El tratamiento financiero de los activos y pasivos por arrendamiento financiero puede impactar en el cálculo del impuesto diferido. Las empresas pueden necesitar revisar sus procesos de negocio y herramientas de recopilación de información para identificar nuevos activos o pasivos por impuestos diferidos, así la evaluación su recuperabilidad.

- **TI**: Los sistemas pueden necesitar ser revisados y modificados. Como resultado de la adaptación a los requerimientos normativos, incluidos sus requisitos de divulgación, las empresas pueden necesitar procesar elementos de información que actualmente no son capturados por ninguno de sus sistemas informáticos. Por ejemplo, una empresa podría requerir que sus sistemas le permitan registrar, en su módulo de gestión contracutal, si sus contratos tienen componentes de arrendamiento financiero para facilitar su adecuada gestión.

- **Legal**: Puede ser necesario mejorar la comunicación entre el departamento legal y el contable. Como mínimo, es recomendable que el departamento legal comprenda los conceptos más relevantes de los estándares de reporte financiero (p.e. definición de arrendamiento financiero, criterios básicos para su identificación, implicancias financieras de no dar adecuado tratamiento contable a los arrendamientos, entre otras).

- **Recursos humanos**: Si el efecto de los estándares aplicables sobre los acuerdos de la entidad es significativo, quizá esta pueda requerir asignar recursos adicionales al esfuerzo de implementación. La entidad también deberá evaluar si el personal existente está suficientemente capacitado y goza de supervisión efectiva para darles un adecuado cumplimiento.

Consideraciones para evaluar la gestión de arrendamientos

Arrendamiento (*Leasing*)

Auditorías de alto impacto

Administración de la información de los contratos de arrendamiento

Objetivo: Evaluar el estado actual de la administración de la información de los contratos de arrendamiento, los sistemas de TI, las políticas y el sistema de control interno

Preguntas clave a considerar

- ¿Cómo recopila información la gerencia sobre los arrendamientos y qué procesos o sistemas de TI existen?
- ¿Cuál es el efecto anticipado del cumplimiento de la normativa aplicable sobre el tratamiento contable de arrendamientos en los procesos de negocio y los reportes financieros de la compañía?
- ¿Cuáles son los planes de la compañía para comunicar a sus partes interesadas los cambios en las políticas contables, procesos y sistemas, para cumplir con los requerimientos normativos?
- Si la entidad opera en un entorno descentralizado y tiene arrendamientos que están sujetos a diferentes procesos en diferentes ubicaciones; ¿cómo planea la gerencia analizarlos y determinar si son necesarios nuevos procesos, controles o sistemas?

Auditorías de alto impacto

Evaluación de controles

Objetivo: Identificar y evaluar los riesgos de reporte financiero y el sistema de control interno vinculado con la gestión de arrendamientos

Preguntas clave a considerar

- ¿Cuáles son los controles implementados por la gerencia sobre aspectos críticos de riesgo como:
  - Integridad de la población de contratos que constituyen un arrendamiento o contengan uno?
  - Separación de los elementos de arrendamiento operativo y financiero?
  - Determinación del plazo del arrendamiento?
  - Clasificación de los arrendamientos, modificaciones, registro contable y revelaciones?
- ¿Cuál es la fuente de la información (por ejemplo, el contrato) usada para identificar un arrendamiento financiero?
- ¿Cómo se asegura de que la información fuente (1) se ingresa correctamente en la aplicación de TI y (2) se descarga completa y correctamente (por ejemplo, de una aplicación de TI) o se ingresa manualmente en una herramienta informática (por ejemplo, Excel)?
- ¿Cómo se asegura de que los cambios o la manipulación de los datos en Excel son completos, precisos y correctos?

Informática móvil

Los dispositivos móviles avanzados han desempeñado un papel significativo y transformador en la forma en que las organizaciones respaldan todos los aspectos de sus operaciones comerciales y brindan a sus clientes información en tiempo real sobre la marcha. En los últimos 15 años, ha habido una afluencia masiva de dispositivos móviles en las organizaciones a través de los empleados que usan sus propios dispositivos en el trabajo y acceden a datos corporativos, o a través de las mismas organizaciones que reemplazan móviles antiguos y les brindan nuevos móviles a los empleados. Claramente, el consumismo ha tenido un impacto irreversible en la movilidad empresarial.

En particular, los dispositivos móviles se diseñaron y comercializaron como medios de voz y comunicaciones de datos para individuos y consumidores, no necesariamente para uso profesional. Su avanzada facilidad de uso y sus convenientes características, mas no la seguridad o protección de datos, fueron las razones subyacentes de la rápida adopción y popularidad de tales dispositivos por parte de las personas. El dispositivo móvil moderno se encuentra en la encrucijada del uso personal y la información comercial altamente confidencial. Como dice el viejo refrán, una cadena es tan fuerte como su eslabón más débil, y los datos comerciales que residen en los dispositivos móviles no son la excepción.

Esta tecnología permite a los empleados acceder y distribuir información de la organización en cualquier momento y lugar, lo cual aumenta su eficiencia y productividad. Sin embargo, esta misma capacidad de acceso y distribución también introduce riesgos importantes. Por ejemplo, el creciente uso de redes de Wi-Fi público por parte de usuarios comerciales expone información confidencial a completos desconocidos, si no se usa correctamente la encriptación. Al igual que con cualquier avance tecnológico, una organización debe primero identificar y abordar los riesgos y luego monitorear el ambiente para comprender mejor el impacto que tienen los moviles en el perfil de riesgo corporativo.

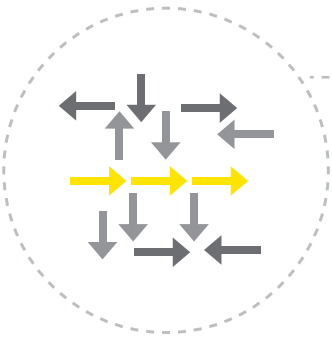
Informática móvil

Los riesgos informáticos móviles a considerar incluyen:

- Posible pérdida o filtración de información comercial importante y confidencial.
- Desafíos de seguridad, teniendo en cuenta la variedad de dispositivos, sistemas operativos y sus limitaciones.
- Robo de dispositivos móviles, en vista de la considerable cantidad de datos que almacenan.
- Incumplimiento de las normas de privacidad estatales, federales e internacionales que varían de una jurisdicción a otra a medida que los empleados viajan con dispositivos móviles.
- Balance entre el uso personal y profesional del dispositivo en cuanto a privacidad y monitoreo de información.

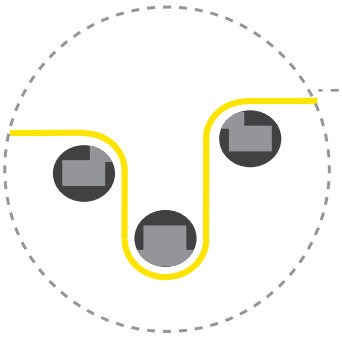
Las organizaciones deben aprovechar el poder de la informática móvil a la vez que minimizan y mitigan sus riesgos, y la función de auditoría interna desempeñará un papel vital en ello.

¿Cuáles son los beneficios de la informática móvil?



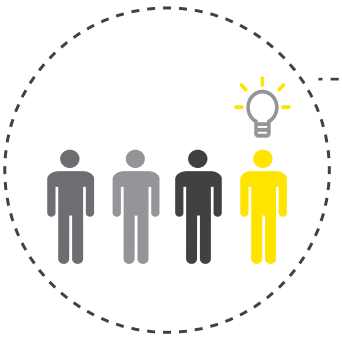
Mejora de productividad

Mejora la productividad de los empleados ampliando el alcance de las aplicaciones existentes, por ejemplo, hojas de datos móviles.



Habilitación de nuevos negocios

Identifica un nuevo público objetivo y ofrece a los clientes nuevos productos o servicios.



Habilitación de empleados

Habilita a los empleados a través de procesos comerciales nuevos o más eficientes, por ejemplo, soporte de campo móvil, CRM móvil.

Informática móvil

Auditorías de alto impacto

Configuración de dispositivos

Objetivo: Identificar los riesgos en las configuraciones de dispositivos móviles y las vulnerabilidades

Preguntas clave a considerar

- ¿La organización tiene políticas, normas y estrategias de gestión de dispositivos? ¿Están centralizados o descentralizados?
- ¿Se han establecido e implementado estándares de configuración y seguridad para el dispositivo móvil y se aplican a través de políticas aprobadas?
- ¿Se han establecido e implementado procesos de gestión de datos para dispositivos perdidos o robados y existen estrategias de comunicaciones, procedimientos forenses y de defensa legal?
- ¿Los dispositivos de usuario final utilizan aplicaciones no autorizadas?
- ¿La configuración de la red admite la activación y el uso de dispositivos de usuario final?
- ¿Existen políticas de seguridad y una segregación de data profesional y privada para terceros?

Auditorías de alto impacto	Preguntas clave a considerar
Caja negra de aplicaciones móviles **Objetivo:** Usar técnicas de prueba de interfaz de usuario y caja negra para intentar explotar las vulnerabilidades identificadas en las aplicaciones móviles	▸ ¿Existen vulnerabilidades, fallas de lógica de negocios y fallas de autorización? ▸ ¿La organización emplea un análisis no-intrusivo y uso de herramientas (por ejemplo, *cross-site scripting*, falsificación de solicitudes entre sitios y estructura de directorios)? ▸ ¿Se han implementado configuraciones de aplicaciones, mapeo de la funcionalidad de la aplicación y permisos? ▸ ¿La organización explota las vulnerabilidades de aplicaciones móviles basadas en dispositivos? ▸ ¿Existen mecanismos de encriptación?
Caja gris de aplicaciones móviles **Objetivo:** Priorizar las áreas de alto riesgo del código, maximizar la cobertura del código e identificar la causa de las vulnerabilidades identificadas	▸ ¿La organización lleva a cabo el reconocimiento y mapeo de aplicaciones, incluyendo: - Interfaces administrativas? - Formularios de varias partes? - Transmisión de información confidencial? - Uso de protocolos móviles? - Modelado visual de la aplicación y definición de límites de confianza? ▸ ¿La organización utiliza el análisis de códigos, incluido el análisis de permisos, análisis de flujo de control y análisis de flujo de datos?

Políticas y gobierno

Las políticas y los procedimientos son fundamentales para el entorno de control de una organización. Cuando son claros, coherentes y actuales, fortalecen no solo la función de control, sino también las relaciones entre la gerencia, los empleados y los inversores. Actúan como el pegamento que une y alinea las operaciones multifuncionales y geográficamente dispersas. Sin embargo, a menudo, las políticas pueden no apoyar el cumplimiento de estos objetivos, lo cual reduce la eficacia y la eficiencia de una organización y aumenta los riesgos. Asimismo, los profesionales de finanzas y gobierno constantemente clasifican las prácticas y políticas contables como una de sus principales preocupaciones. Para administrar estos riesgos, la gerencia debe ser proactiva.

Una serie de factores desencadenantes pueden convertir una preocupación sobre el estado de las políticas y procesos de gobierno en una necesidad crítica de diagnóstico y reparación inmediata. Los desencadenantes más comunes son aquellos factores propios de la compañía, los cuales generalmente implican cambios en el modelo operativo de una organización. Estos también pueden provenir de eventos transformacionales, desde ofertas públicas iniciales (IPO, por sus siglas en inglés) y reestructuraciones, hasta desinversiones, fusiones y adquisiciones. La falta de políticas estandarizadas puede causar que las empresas globales experimenten controles débiles y no cumplan con los plazos de presentación de informes. Otro conjunto de desencadenantes son propios de la industria, abarcando el *business as usual*, los cambios normativos y los cambios en el entorno empresarial que afectarán sus políticas y prácticas, ya sea de manera inmediata o en el transcurso del tiempo. Un desencadenante adicional es la frustración del personal frente a políticas inconsistentes, lo cual ocurre frecuentemente con organizaciones grandes, geográficamente dispersas y descentralizadas.

Políticas y gobierno

Auditorías de alto impacto	Preguntas clave a considerar
Gobierno de políticas **Objetivo:** Evaluar los procesos existentes de la organización para crear, revisar y retirar políticas	▸ ¿La gerencia tiene problemas relacionados con el proceso actual de gobierno de políticas de la organización? ▸ ¿La gestión organizacional tiene documentos, datos e información clave relacionados con el proceso de gobierno de políticas existente? ▸ ¿Los procesos actuales de gobierno de políticas a nivel funcional de empresa o corporación son suficientes? ▸ ¿La organización prioriza los pasos necesarios para revisar el marco de políticas contables y las políticas impactadas?
Integridad de la biblioteca de políticas **Objetivo:** Identificar áreas de mejora dentro de la biblioteca de políticas existente de una organización	▸ ¿Las políticas de contabilidad, finanzas, tesorería, recursos humanos, impuestos y riesgos están actualizadas? ▸ ¿Existe una biblioteca de políticas que incluya todos los requisitos de procesos comerciales e informes de la organización? ▸ ¿La organización utiliza prácticas líderes para el desarrollo de sus políticas desde una perspectiva de formato y diseño? ▸ ¿Las políticas de la organización son fáciles de usar (es decir, usan un lenguaje simple y ejemplos relevantes)? ▸ ¿Los hallazgos de la revisión de políticas destacan brechas y oportunidades de mejora?

Auditorías de alto impacto

Preparación para la implementación

Objetivo: Evaluar la capacidad de la organización para implementar efectivamente cambios de políticas y procedimientos en el personal

Preguntas clave a considerar

- ¿Las plataformas existentes implementan políticas y procedimientos para que la organización identifique oportunidades de mejora?
- ¿Los métodos y la frecuencia de los programas de capacitación de políticas se alinean con aquellos de empresas líderes o referentes en la industria?
- ¿Los hallazgos se resumen a partir de la revisión, destacando las brechas y oportunidades de mejora?

Gestión de riesgos de programas y proyectos

La complejidad de los programas y proyectos crece a un ritmo más rápido al que las compañías pueden adaptarse, y se están expandiendo las carteras y portafolio de proyectos para seguir el paso de las tendencias emergentes. Debido a que las compañías andan buscando formas de aumentar la eficiencia y reducir los costos, están emprendiendo iniciativas importantes para rediseñar y estandarizar procesos de negocio, reducir costos y mejorar la productividad. Frecuentemente, estas grandes iniciativas terminan siendo proyectos relacionados con tecnología.

Los riesgos asociados con la gestión de programas y proyectos se encuentran presentes a lo largo del ciclo de vida y, como resultado, puede haber importantes consecuencias económicas, financieras, regulatorias y reputacionales si no se les controla y gestiona adecuadamente. El margen para errores es pequeño, y el entorno necesario para la transformación continúa creciendo en complejidad. Sin embargo, muchas compañías no han demostrado la capacidad de adaptar su enfoque, su gobierno, sus procesos, sus controles y sus herramientas para abordar la complejidad de estos programas.

Los riesgos programáticos aumentan por la complejidad en los procesos del negocio y los avances tecnológicos como la nube, la robótica, tecnología móvil y nuevas tecnologías digitales. La auditoría interna puede agregar valor mediante evaluaciones proactivas del portafolio de proyectos para determinar los riesgos de amenazas clave que deben ser mitigados y las oportunidades que se deban perseguir y aprovechar. Estas capacidades son fundamentales para ser más competitivos en el mercado y mejorar la velocidad de la realización del valor del negocio, considerando los riesgos programáticos y operativos.

Gestión de riesgos de programas y proyectos

Auditorías de alto impacto	Preguntas clave a considerar
Metodología de gestión de proyectos Objetivo: Evaluar la metodología de gestión de programas y proyectos	▸ ¿La metodología de gestión de programas y proyectos y la estructura de gobierno se han definido considerando un enfoque de ejecución y planeamiento, una composición adecuada del equipo y protocolos de monitoreo y comunicación? ▸ ¿Se han incluido controles en la metodología para entregar el proyecto a tiempo y siguiendo el presupuesto? ▸ ¿Hay algún proceso para medir si se lograron los beneficios deseados?
Ejecución de programas y proyectos **Objetivo:** Evaluar la ejecución de programas y de proyectos	▸ ¿Se respeta la metodología de gestión de proyectos? ▸ ¿La oficina de gestión de proyectos monitorea el proyecto en cuanto al cronograma? ▸ ¿Hay una comunicación adecuada entre los miembros del equipo del proyecto?
Revisión de riesgos en la cartera **Objetivo:** Evaluar los riesgos del portafolio de proyectos	▸ ¿Se ha desarrollado e implementado un proceso sólido de gestión de portafolio de proyectos que incluya un planeamiento de demanda, priorización de proyectos, financiamiento y procesos de toma de decisiones? ▸ ¿El enfoque de evaluación de riesgos es integral? ¿Incluye algún proceso para mitigar riesgos? ▸ ¿Se ha implementado un proceso para responder a los cambiantes objetivos corporativos?

Auditorías de alto impacto	Preguntas clave a considerar
Revisión del rediseño de procesos **Objetivo:** Evaluar los procesos y controles para mitigar los riesgos asociados con el rediseño de procesos (en caso éste sea un proyecto)	▸ ¿Se han definido y comunicado las funciones de los miembros del equipo del proyecto? ▸ ¿Hay un flujo de trabajo en el control interno del proyecto que se enfoque en identificar y mitigar riesgos? ▸ ¿El equipo del proyecto utiliza al máximo los controles automatizados y del sistema?
Revisión del centro de servicios compartidos **Objetivo:** Evaluar procesos y controles relacionados a la transición a un centro de servicios compartidos (en caso éste sea un proyecto)	▸ ¿Se han desarrollado e implementado procesos para la transición al centro de servicios compartidos? ▸ ¿El equipo del proyecto ha validado la estructura y la tecnología del control utilizadas para facilitar la transición?

Cultura de riesgos

La cultura de riesgos en una organización se traduce en las acciones que realizan las personas que la integran para gestionar sus riesgos de negocio. Esta conecta la cultura más general de una organización con sus actividades de riesgo o de control de riesgos. Los reguladores a nivel mundial han enfatizado que la cultura se ha vuelto el aspecto más importante para abordar lo que ellos consideran como grandes fallas de conducta y de control que pueden tener un impacto sistemático si no se les aborda adecuadamente. Esto crea desafíos prácticos en su implementación y puede ser que los cronogramas designados necesiten soluciones tácticas a corto plazo.

Mejorar los comportamientos de una organización requiere considerar cuidadosamente otros aspectos del modelo de gobierno de riesgos. Para lograr una cultura de riesgos sólida, las organizaciones necesitan manifestar los principios base de la cultura de riesgos y articular los comportamientos que se espera que las personas emulen. La cultura de riesgos no es algo que se pueda diseñar y ejecutar; debe ser proactiva y todos deben entender que son responsables de sus propios comportamientos de riesgo, y que deberían informar, de forma proactiva, el comportamiento inaceptable de otras personas.

Iniciar el cambio cultural desde la alta gerencia corporativa es necesario para expresar claramente los comportamientos de riesgo deseados. Las organizaciones deberían enfocarse en tener métricas establecidas con miras al futuro para medir, tanto los riesgos financieros, como los no financieros. El apetito al riesgo debería ser consistente con la estrategia de negocio de la compañía y debería estar incluido en la toma de decisiones.

Las organizaciones deberían considerar cambiar el enfoque basado solamente en incentivos financieros para incluir incentivos no financieros. Los procesos de gestión de talento, reclutamiento, incorporación y desvinculación del personal, deberían ser diseñados para que los empleados compartan los valores y la cultura de riesgos deseados de la compañía.

El alineamiento del directorio, con la alta gerencia y las unidades del negocio de una organización, basado en un entendimiento común de la cultura de riesgos, es esencial para cambiar, monitorear y manejar el comportamiento. La gerencia de riesgos, el directorio, la alta gerencia y la auditoría interna tienen un rol que desempeñar para desarrollar y mantener la cultura de riesgos deseada.

Cultura de riesgos

¿Cómo puede una organización mejorar su cultura de riesgos?

Definir la cultura de riesgos, por ejemplo, buenos y malos comportamientos

- Entender las causas de las actitudes de los empleados.
- Definir los comportamientos esperados.
- Complementar la definición de los comportamientos deseados con ejemplos prácticos y personalizados.

Evaluar el estado actual e identificar las iniciativas clave

- Identificar las fortalezas y debilidades de la cultura de riesgos de la organización.
- Registrar y comunicar las políticas, procedimientos, controles y gobierno.
- Priorizar las oportunidades de mejora.

Calibrar y mejorar

- Calibrar y reforzar los comportamientos esperados de forma regular.
- Identificar un propietario para impulsar oportunidades de mejora.
- Colaborar con el negocio, riesgo, recursos humanos, cumplimiento y la auditoría interna para implementarla.

Auditorías de alto impacto

Estructura de la cultura del riesgo

Objetivo: Evaluar si la organización ha implementado políticas, procesos e incentivos adecuados para apoyar su misión, su visión y sus objetivos estratégicos

Preguntas clave a considerar

- ¿La misión, visión y valores de la organización se alinean y comunican de forma clara en toda la organización?
- ¿Los valores corporativos toman en cuenta los comportamientos deseados (buenos o malos)? ¿Son comunicados en toda la organización? ¿Son entendidos en todos los niveles de la organización?

Auditorías de alto impacto

Evaluación de la cultura del riesgo

Objetivo: Evaluar la cultura de riesgos general de la organización considerando acciones de liderazgo e incentivos; identificar y evaluar las brechas entre los comportamientos deseados y los reales, determinar el origen de estas y brindar recomendaciones

Preguntas clave a considerar

- ¿El mensaje es consistente, bien comprendido y aceptado en toda la organización? ¿Se refuerza de forma periódica?
- ¿Se le informa periódicamente al Directorio los resultados de la evaluación que la Gerencia hace sobre la cultura de riesgos?
- ¿Las métricas y los incentivos están diseñados para promover el comportamiento deseado?
- ¿Se realiza una buena capacitación para toda la organización?
- ¿El apetito al riesgo es considerado y difundido como parte de la cultura de riesgos deseada?
- ¿Existe alguna relación entre las compensaciones y los comportamientos de riesgo?
- ¿La cultura apoya la transparencia en cuanto a riesgos y permite que las preocupaciones se expresen?
- ¿Cómo se trata a los informantes de los comportamientos no deseados?
- ¿Qué requisitos regulatorios se han impuesto actualmente? ¿Qué es lo que probablemente influirá en los reguladores y directorios al establecer la cultura de riesgos deseada?

Automatización robótica de procesos (RPA)

Mientras que la robótica ayuda a las compañías a automatizar el trabajo manual dentro de las operaciones, la robótica de *software* o la Automatización Robótica de Procesos (RPA, por sus siglas en inglés), promete transformar el costo, la eficiencia y calidad de la ejecución de muchos procesos, tanto los de soporte, como los del negocio, tal como la gestión con clientes, los cuales son usualmente encargados a las personas. Sin embargo, esta automatización viene con su propio conjunto de riesgos. La AI debería involucrarse desde el comienzo y debe ser capaz de identificar y asesorar sobre el modo de mitigar los riesgos rápidamente, ya que la tecnología continúa cambiando a un ritmo acelerado.

Frecuentemente, más de uno de los problemas descritos a continuación se encuentra presente o relacionado, lo cual crea un efecto multiplicador importante. Se necesita mucha planificación o ayuda externa para mitigar estos problemas. Desafortunadamente, si más de uno de estos llega a ocurrir, lo cual sucede comúnmente, hay un efecto multiplicador que puede llevar a dejar de creer en el RPA o hacer que el proyecto se detenga. Ya sea que una organización esté migrando a un RPA o ya esté en camino, es probable que el RPA se convierta en parte fundamental de los procesos clave del negocio. Es esencial que una organización establezca una estrategia de RPA que incluya un gobierno integral, prácticas de riesgo y control. La AI puede ofrecer conocimientos sobre el negocio, riesgos y control interno sobre la estrategia.

Puede ser que las organizaciones acudan a la función de AI, luego de la implementación robótica, para que evalúe cómo van operando los procesos y controles, pero lo que no logran entender es el valor que AI puede ofrecer antes, durante y después de la implementación de RPA. La AI puede ayudar a la gerencia a involucrase profundamente en cada etapa de la implementación de RPA al ofrecerle evaluaciones independientes y asesoría estratégica. Las consecuencias financieras y reputacionales de esperar para actuar y de equivocarse son exorbitantes. La AI puede ayudar a trazar una ruta hacia el éxito.

Los riesgos y controles descritos a continuación deberían ser tomados en cuenta por la función de auditoría interna de una organización al desarrollar un programa de auditoría y análisis de riesgos del RPA:

1	La carencia de un gobierno de robótica puede llevar a una automatización de procesos ineficiente e ineficaz, y a una incapacidad para apoyar y cumplir los requisitos del negocio.
2	La gestión de accesos de un RPA, de ser administrada de manera inefectiva e ineficaz, comprometería el acceso a diversos sistemas, aplicaciones o datos sensibles o no autorizados para determinadas personas.
3	Los requisitos para la automatización de procesos no han sido identificados y documentados con exactitud, lo cual ocasiona que el desarrollo robótico no vaya de acuerdo a las necesidades del negocio o no apoye la estrategia de TI; esto causaría un impacto negativo en los procesos del negocio y las variables financieras.
4	Las implementaciones robóticas no han sido adecuadamente diseñadas o probadas, lo que ocasiona que los requerimientos no se cumplan o que haya un impacto negativo en los sistemas productivos; esto lleva a un impacto negativo en el negocio y a pérdidas financieras.
5	Los problemas de automatización no se han identificado oportunamente ni se han manejado bien, lo cual ocasiona un retraso para resolverlos y causa un impacto negativo en los procesos del negocio.
6	Los riesgos asociados a la gestión con proveedores o servicios subcontratados de robótica, no se han mitigado de forma eficaz, lo cual conlleva a una exposición financiera y reputacional para las compañías.

Automatización robótica de procesos (RPA)

Auditorías de alto impacto

Gobierno

Objetivo: Evaluar si la estructura de gobierno de robótica ha sido diseñada para cubrir riesgos clave y si considera la supervisión necesaria para el alineamiento con los objetivos del negocio

Preguntas clave a considerar

- ¿Se define y mantiene una estructura de gobierno sobre el uso de la robótica?
- ¿La estructura del gobierno incluye lo siguiente:
  - Liderazgo?
  - Funciones y responsabilidades?
  - Requisitos de información?
  - Procesos?
- ¿Se incluyen elementos importantes de la gestión del cambio como parte de los aspectos organizacionales, de procesos y técnicos?
- ¿Existen procesos para gestionar la implementación, la evaluación y los requisitos de apoyo de robótica en toda la organización?
- ¿Se mapean y documentan adecuadamente las necesidades de cambio y desarrollo de robótica de acuerdo a las necesidades del negocio?
- ¿Se evalúan y corrigen continuamente los problemas y errores de la automatización?

Auditorías de alto impacto	Preguntas clave a considerar
Inversiones **Objetivo:** Evaluar si la organización ha definido indicadores clave de desempeño con la capacidad de desplegar un adecuado monitoreo al gobierno de procesos de robótica	▸ ¿Se evalúan, aprueban y priorizan adecuadamente las decisiones de inversión en robótica? ▸ ¿La compañía ha definido quiénes son sus proveedores de robótica aprobados? ▸ ¿Los ratios o indicadores de la organización incluyen los objetivos de cumplimiento normativo, el retorno de la inversión (ROI, por sus siglas en inglés) y el desempeño de robótica?
Acceso al usuario **Objetivo:** Evaluar la estrategia de la organización para determinar si define 1) cómo se provee acceso a las capacidades robóticas, 2) cómo la organización protege sus activos robóticos y, 3) el método que utiliza la organización para determinar sus riesgos de seguridad relacionados al uso de robótica	▸ ¿Tiene la organización una estrategia integral para proteger sus activos robóticos? ▸ ¿Se han implementado controles adecuados para evitar que usuarios no autorizados tengan acceso a los robots? ▸ ¿La organización ha desarrollado una estrategia para brindar y restringir el acceso, que permita que los robots interactúen con los sistemas de producción de TI de forma controlada?

Redes sociales

Las redes sociales son una herramienta de comunicaciones y marketing poderosa que permite que las organizaciones construyan una mayor consciencia de sus marcas, fidelicen a sus clientes, y mejoren eficiencias y la conectividad entre los empleados corporativos y su base de clientes. La velocidad, la espontaneidad y la entrada profunda de las redes sociales en las operaciones diarias y rutinarias del negocio han transformado la relación entre las compañías y sus clientes, empleados, proveedores y reguladores.

Las compañías han aprovechado las redes sociales para:

- Fortalecer su marca
- Fidelizar a sus clientes
- Incrementar su participación en el mercado
- Mejorar la cadena de suministros

La falta de una estrategia integral y sólida para el manejo de redes sociales puede abrir paso a potenciales riesgos críticos de negocio, a veces imprevistos. En la definición de su estrategia de redes sociales, las compañías deben considerar varios aspectos organizacionales y culturales, tanto del uso actual de redes sociales, como de las plataformas tecnológicas y la infraestructura disponibles, con la finalidad de mitigar sus riesgos.

Sin una estrategia de redes sociales implementada adecuadamente, pueden emerger los siguientes riesgos:

- Filtración involuntaria de información confidencial por parte de empleados de la compañía.
- Transmisión y distribución intencional de información confidencial por parte de una persona externa.
- Daño a la reputación y a la marca.
- Gran riesgo de *hackeo* a cuentas de ejecutivos en las plataformas de redes sociales.
- Gran riesgo de virus, *malware* y *phishing*.
- Uso inadecuado o incorrecto de las plataformas de redes sociales por parte de empleados.
- Pagos a personas externas a través de las plataformas de redes sociales por parte de los empleados.

Una estrategia sólida para las redes sociales debería:

- Alinear el uso de las redes sociales con las estrategias organizacionales y los valores corporativos.
- Desarrollar, ejecutar y comunicar a los empleados las directivas del uso de las redes sociales.
- Identificar, mitigar y monitorear rápidamente los riesgos actuales y los que emergen a raíz del entorno cambiante de TI y redes sociales.
- Proteger los datos y la reputación de la compañía y el cliente.
- Responder rápidamente a los incidentes en las redes sociales.
- Monitorear la información que los empleados divulgan a través de las redes sociales.

Las auditorías internas a las redes sociales son formas efectivas y de gran impacto que ayudan a la gerencia a mitigar los riesgos.

Redes sociales

Auditorías de alto impacto	Preguntas clave a considerar
Evaluación de riesgos Objetivo: Analizar la metodología y la estructura de la evaluación de riesgos relacionada con las redes sociales; revisar las actividades en las redes sociales que crean los mayores niveles de exposición a los riesgos	▸ ¿La organización ha desarrollado una estrategia integral para el manejo de las redes sociales? ▸ ¿La organización ha establecido una metodología y estructura relacionada con el manejo de las redes sociales? ▸ ¿La gerencia comunica las expectativas de la gestión de riesgos y del cumplimiento regulatorio y los empleados las comprenden adecuadamente?
Gobierno **Objetivo:** Evaluar las políticas y procedimientos de las redes sociales, incluyendo una comparación contra las prácticas líderes, a fin de identificar brechas en dichas políticas y procedimientos	▸ ¿La organización ha establecido políticas y procedimientos para el manejo de las redes sociales que incluyan lo siguiente: - Alineamiento de la estrategia con las operaciones y valores? - Estructura y controles del gobierno de las redes sociales? - Cumplimiento del empleado y del proveedor? - Nivel apropiado de seguridad para el acceso y gestión de las redes sociales? - Indicadores clave de desempeño del manejo de las redes sociales? - Autorización para las publicaciones en redes sociales?

Auditorías de alto impacto

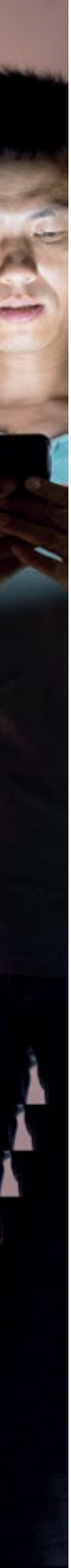
Operaciones

Objetivo: Evaluar la solidez de la integración en el negocio e identificar brechas en el alineamiento de las operaciones con las redes sociales

Preguntas clave a considerar

- ¿La organización ha integrado eficazmente las redes sociales en el negocio?
- ¿Se evalúan y monitorean las actividades de los empleados en cuanto a las políticas y procedimientos de las redes sociales?
- ¿Se han implementado herramientas y la infraestructura adecuada para monitorear las actividades de los empleados en las redes sociales?
- ¿Se ha comunicado la política a los empleados de forma eficaz?
- ¿La organización brinda capacitación a los empleados sobre las políticas y procedimientos en las redes sociales, y evalúa sus conocimientos sobre éstos?

Cadena de suministros



Una adecuada gestión de la cadena de suministros es crítica para que la estrategia organizacional cree una ventaja competitiva y contribuya con reducir costos operativos, mejorar los niveles de servicio al cliente, reducir inventario, gestionar mejor los riesgos y aumentar agilidad. Las funciones dentro de la cadena de suministros de una organización son investigación y desarrollo (I&D), servicios de ingeniería, planificación de ventas y operaciones, subcontratación y adquisiciones, operaciones de manufactura, logística y servicios posventa. Muchas organizaciones están buscando formas de respaldar el crecimiento mediante la mejora de sus márgenes en mercados desarrollados y, posiblemente, también están buscando oportunidades de crecimiento en mercados emergentes. Esto aumenta el grado de exigencia para la cadena de suministros de una organización.

Colocar esta presión en las funciones de la cadena de suministros durante una economía impredecible hace que las organizaciones cambien su enfoque hacia la mejora de la planificación de ventas y operaciones, de la gestión de subcontratación y de proveedores, la producción y la logística.

En este contexto, pueden surgir los siguientes riesgos:

- Falta de integración entre las ventas, el suministro y la producción, que cause una desconexión entre lo que se produce y la demanda de los clientes.
- Conflictos de interés, corrupción, fraude, una base de proveedores no diversificada, falta de capacidad de los proveedores, un bajo nivel en la gestión de contratos con proveedores, problemas con el cumplimiento regulatorio, y el error de no identificar proveedores de bajo costo en procesos de compras.
- Falta de conocimiento sobre las normas y tarifas de importaciones y exportaciones.
- Ineficacia operativa y pérdida de productividad.
- Riesgos de salud y seguridad ocupacional, así como riesgos medioambientales.

Cadena de suministros

Auditorías de alto impacto	Preguntas clave a considerar
Gestión de riesgos de proveedores Objetivo: Evaluar las políticas de la organización y la aplicación de estas para gestionar la relación con los proveedores y reducir el riesgo generado por la interacción con dichos proveedores	▸ ¿La organización tiene políticas, procesos y controles internos establecidos y adecuados para evaluar el riesgo de proveedores en general? ▸ ¿Cómo se seleccionan e incorporan a los proveedores? ▸ ¿Existe uniformidad en la aplicación de los procesos de gestión de riesgos de proveedores en toda la organización? ▸ ¿Existe un registro regular de resultados para proveedores de materiales directos? ▸ ¿Existen procesos y controles para evaluar a los proveedores de compras directas e indirectas?
Transporte y logística **Objetivo:** Evaluar las estrategias y políticas de la organización para mitigar el riesgo generado por los servicios de transporte e identificar oportunidades de ahorro	▸ ¿Se han implementado procesos de monitoreo y gestión de los gastos de transporte y logística? ▸ ¿Existen oportunidades para reducir los costos de transporte y servicios logísticos? ▸ ¿Existen acuerdos de nivel de servicio con proveedores? ¿Son monitoreados con regularidad? ▸ ¿La organización comprende y monitorea las regulaciones apropiadamente?

Auditorías de alto impacto	Preguntas clave a considerar
Planificación de ventas y operaciones **Objetivo:** Evaluar la estrategia y sostenibilidad de la organización para alinear la cadena de suministros, operaciones y ventas	▸ ¿Se documentan y comunican las políticas y procedimientos formales para la integración de las ventas, la cadena de suministros y las operaciones? ▸ ¿Los procesos de ventas, de la cadena de suministros y de las operaciones están integrados en toda la organización para cumplir, de esta forma, con la demanda estimada de los clientes? ▸ ¿Cómo se realiza la planificación de la demanda y los suministros? ▸ ¿Hay niveles elevados de escasez de algunos materiales?
Gestión de contratos **Objetivo:** Evaluar la estrategia y capacidad de la organización para realizar contratos con proveedores y clientes, y monitorear el cumplimiento de los contratos	▸ ¿La organización ha implementado procesos, tanto internos como externo, para monitorear el cumplimiento de los contratos? ▸ ¿Los precios y descuentos en las órdenes de compra son adecuados y están alineados con lo indicado en el contrato? ▸ ¿Se han implementado controles para verificar que los contratos estén aprobados por los funcionarios autorizados y para que cualquier cambio posterior sea aprobado oportunamente? ▸ ¿Se monitorean y se cumplen los términos y condiciones de los contratos?

Cadena de suministros

Auditorías de alto impacto	Preguntas clave a considerar
Manejo de residuos **Objetivo:** Evaluar la estrategia y capacidad de la organización para monitorear, desechar y reducir residuos	▸ ¿La organización monitorea adecuadamente los residuos en todas las instalaciones? ▸ ¿Se recibe información completa y exacta sobre los residuos de las instalaciones? ▸ ¿Se ha implementado procedimientos para reducir los residuos? ▸ ¿La organización ha definido métricas para el manejo de residuos, las cuales son monitoreadas periódicamente?
Lanzamiento de nuevos productos Objetivo: Evaluar el proceso de desarrollo de nuevos productos y los procedimientos para su eficacia	▸ ¿Se realizan análisis de fallas y posibles efectos durante el desarrollo de nuevos productos? ¿Existe un ciclo de retroalimentación para actualizar dichos análisis? ▸ ¿Se ha comprendido el gasto actual en investigación y desarrollo de nuevos productos? ▸ ¿En qué etapa del proceso de desarrollo de nuevos productos se involucra la subcontratación, las compras, la manufactura y la gestión de calidad? ▸ ¿Hasta qué punto se han utilizado soluciones de *software* para apoyar al desarrollo de nuevos productos?

Auditorías de alto impacto	Preguntas clave a considerar
Fiabilidad de los activos y mantenimiento productivo **Objetivo:** Evaluar la estrategia y prácticas para la fiabilidad de los activos y gestión del mantenimiento	▸ ¿Se ha documentado una estrategia para la fiabilidad de los activos a nivel de empresa? ▸ ¿El personal operario se involucra en el mantenimiento de equipos? ▸ ¿Qué técnicas de mantenimiento predictivo se utilizan? ▸ ¿Se ha implementado un sistema computarizado de gestión del mantenimiento para apoyar el mantenimiento? ¿El *software* de la empresa es utilizado al máximo? ▸ ¿Se utiliza la tasa de consumo de los repuestos de quipos para planificar el mantenimiento preventivo? ▸ ¿Existen procesos regulares para determinar la utilización o no utilización de equipos?
Gestión de servicios y repuestos **Objetivo:** Evaluar el enfoque para la gestión de servicios y repuestos	▸ ¿La gestión de servicios y repuestos es gestionada por terceros o por el fabricante original del equipo? ▸ ¿Se realiza una segmentación clientes de servicios? ▸ ¿Los repuestos se planifican y compran a través de procesos propios, o conjuntamente con otras partes involucradas en el proceso productivo? ▸ ¿Qué indicadores clave de desempeño (KPI) se utilizan para medir la gestión del servicio, y cómo se usan para mejorar el servicio y el rendimiento de los repuestos?

Cadena de suministros

Auditorías de alto impacto

Calidad

Objetivo: Evaluar la efectividad y eficiencia del enfoque de calidad de la organización

Preguntas clave a considerar

- ¿Cuán bien se entienden y documentan las especificaciones de los productos y de los procesos?
- ¿Ha habido retiros de productos recientemente? ¿Cómo se manejaron?
- ¿Qué técnicas se usan para conocer y analizar las causas raíz de las mejoras que fueron implementadas?
- ¿Hay indicadores clave de desempeño de calidad en toda la empresa?
- ¿Los sistemas de la empresa recopilan datos de no conformidades?
- ¿Qué porción de los costos totales de calidad se incurrieron por cada uno de los siguientes puntos:
  - Falla en procesos?
  - Valoración e inspección?
  - Prevención?

Auditorías de alto impacto	Preguntas clave a considerar
Gestión de inventarios Objetivo: Evaluar las prácticas de la gestión de inventarios	▸ ¿Cuáles son los niveles del inventario de lento movimiento, obsoleto, dañado o perdido? ▸ ¿Cómo se planifica el inventario? ▸ ¿Con qué frecuencia se realizan los conteos físicos? ▸ ¿En qué se diferencian o asemejan las rotaciones del inventario con las de otras empresas del sector? ▸ ¿Cómo se registran las transacciones del inventario en el *software* de planificación de recursos de la empresa?
Producción y manufactura **Objetivo:** Evaluar la eficiencia y efectividad de las políticas, procedimientos y prácticas asociadas con la producción	▸ ¿Los procedimientos y procesos se han mapeado de forma clara y están actualizados? ▸ ¿Las instrucciones de trabajo son claras y se encuentran en formato electrónico? ¿Cómo se actualizan? ▸ ¿Las instalaciones usan tableros o pantallas de gestión visual? ▸ ¿Las condiciones son seguras para los operadores? ▸ ¿La escasez de materiales retrasan las fechas de inicio de la producción? ▸ ¿Las materias primas defectuosas o no conformes tienen algún impacto en la producción?

Gestión de riesgos de subcontrataciones

La empresas de una amplia gama de industrias están confiando más que nunca en terceros para lograr sus objetivos comerciales. Esta creciente dependencia en proveedores externos introduce nuevos e importantes niveles de riesgo para las organizaciones.

Si bien las funciones y los servicios se pueden subcontratar, los riesgos asociados siguen siendo responsabilidad de la empresa.

Las empresas que no cuentan con un programa bien definido de Gestión de Riesgos de Subcontrataciones (GRS) pueden enfrentar diversos riesgos. Las organizaciones líderes del futuro deben ser capaces de transformar la incertidumbre en seguridad mediante el desarrollo de confianza con respecto a terceros.

Los riesgos generados por las subcontrataciones pueden tener un impacto significativo en las operaciones comerciales de la organización, exponer a la empresa a una contingencia legal o afectar su reputación y aumentar los costos innecesariamente a causa de multas, pérdida de clientes, etc. Resulta importante que la gerencia implemente controles y desarrolle un proceso de monitoreo de la gestión de subcontrataciones. Asimismo, la función de Auditoría Interna tiene un rol clave para ayudar a la empresa a responder a los diversos riesgos que se originan a raíz de la subcontratación de servicios.

Riesgos asociados a la gestión de subcontrataciones

Riesgo en el país
- Tipo de cambio y pérdidas en la conversión de moneda
- Daño reputacional

Riesgo regulatorio
- Multas
- Litigios
- Acciones legales contra la empresa o sus altos ejecutivos

Riesgo de servicio
- Interrupción del servicio
- Baja calidad

Riesgo reputacional
- Publicidad negativa
- Pérdida de clientes

Riesgo financiero
- Pérdida de rentabilidad
- Pérdida de valor para el accionista

Riesgo de TI
- Fallas cibernéticas
- Actividades maliciosas

Riesgo de continuidad del negocio
- Interrupción de la cadena de suministro
- Interrupción del servicio
- Daño reputacional

Riesgo de estrategia de salida
- Acciones legales
- Penalizaciones y sanciones

Gestión de riesgos de subcontrataciones

Auditorías de alto impacto

Programa de gestión de riesgos de subcontrataciones

Objetivo: Evaluar los componentes fundamentales del programa de gestión de riesgos de subcontrataciones

Preguntas clave a considerar

- ¿Tiene la organización un programa integral de gestión de riesgos para terceros?
- ¿La organización cuenta con un marco, procesos y controles de gobierno para abordar lo siguiente:
  - Cumplimiento del contrato (proveedores, alianzas, empresas conjuntas, colaboraciones, regalías y licencias y propiedad intelectual de *software*)?
  - Distribuidores y revendedores?
  - Contratos de marketing y publicidad?
- ¿La organización realiza un monitoreo continuo de las subcontrataciones?
- ¿Existe un programa de supervisión general de terceros?
- ¿Se monitorean las modificaciones en las regulaciones que tienen impacto en ciertos cambios en los contratos de terceros?
- ¿Existe un proceso para monitorear los indicadores clave de desempeño a nivel de servicio?
- ¿Ha realizado la organización una evaluación de riesgos de subcontrataciones?

Auditorías de alto impacto

Gestión de riesgos de contratos con terceros

Objetivo: Verificar el cumplimiento de las obligaciones contractuales

Preguntas clave a considerar

- ¿La organización realiza una evaluación de las obligaciones incluidas en el contrato?
- ¿La organización realiza un análisis de los contratos (análisis de gastos, análisis de cuentas por pagar, análisis de viajes y entretenimiento, validación de facturas y validación del precio de compra) para identificar problemas potenciales?
- ¿Los contratos con terceros incluyen lo siguiente:
  - Revisión del contrato: factores de riesgos legales y comerciales?
  - Perfiles de riesgos de contratos con terceros?
  - Comparación de controles y procesos con prácticas líderes?
  - Procedimientos de verificación de cumplimiento?
  - Hallazgos de cumplimiento y de pérdidas económicas?
  - Recomendaciones de mejora de procesos y controles?

Tesorería

El papel de tesorería dentro de las organizaciones se ha expandido notablemente, así como lo han hecho los riesgos inherentes asociados con sus actividades. Hoy más que nunca, tesorería tiene un conjunto completo de responsabilidades: la gestión de efectivo, capital de trabajo, liquidez y crédito; la necesidad de agregar valor a las ganancias, al flujo efectivo, a la cuota de mercado y a la ventaja competitiva; y la necesidad de comprender e incorporar regulaciones y guías contables nuevas y revisadas, entre muchas otras.

Esta función ahora ocupa un lugar clave en la mesa de toma de decisiones y se le confía el crecimiento estratégico del negocio global. Tesorería ya no es quien paga facturas o gestiona el flujo de caja de la empresa, sino un socio clave que está completamente integrado en la organización.

Con estos cambios, los riesgos inherentes del área de tesorería han incrementado, haciendo que las auditorías internas sean un elemento importante en la agenda. Las empresas se han visto en la necesidad de impulsar las habilidades del área de AI y su conocimiento en finanzas y tesorería para que puedan evaluar el área de tesorería de forma más efectiva. Estas evaluaciones deben considerar métodos de evaluación de los riesgos asociados a una tesorería moderna.

Políticas y gobierno	‣ Falta de supervisión de las actividades de tesorería (por ejemplo, no hay comité de tesorería). ‣ Falta de controles anti-fraude asociados a las autorizaciones, procesamiento y revisión de los desembolsos. ‣ Políticas de tesorería obsoletas o incompletas. ‣ Posible violación de la segregación de funciones, por no existir claridad en las funciones y responsabilidades de tesorería.
Gestión de liquidez en efectivo	‣ Poca visibilidad y control del efectivo de la organización. ‣ Monitoreo insuficiente de los riesgos de liquidez.

• • •

Tesorería

• • •

▶ Financiamiento y mercado de capital	▸ Insuficiente monitoreo de los posibles incumplimientos de acuerdos de financiamientos (créditos, compromisos y contingencias). ▸ Ausencia o deficiencia de la plataforma a nivel de sistemas que permitan efectuar actividad comercial no autorizada.
▶ Gestión de riesgos financieros	▸ Inadecuada gestión de coberturas para atender riesgos emergentes relacionados a volatilidad de tipos de cambio o tasas de interés, entre otros. ▸ Insuficiente monitoreo de los riesgos de crédito.
▶ Contabilidad y valuación	▸ Uso incorrecto de métodos de evaluación. ▸ Errores u omisiones en los reportes de tesorería para la toma de decisiones. ▸ Documentación de cobertura insuficiente o nula. ▸ Inadecuada aprobación de coberturas.
▶ Tecnología de tesorería	▸ Ausencia de una infraestructura de TI capaz de capturar, conservar y transferir información en un entorno seguro y confiable que cumpla con las necesidades de la compañía a un costo razonable. ▸ Inadecuados controles de aplicación.

Auditorías de alto impacto	Preguntas clave a considerar
Revisión de cumplimiento normativo **Objetivo:** Evaluar los procesos y controles establecidos para cumplir con las normativas internas y normas contables aplicables	▸ ¿Están los procesos y controles diseñados adecuadamente para cumplir con las normativas aplicables y políticas internas? Por ejemplo Normas Internacioles de Información Financiera (NIIF), reportes a la Superintendencia del Mercado de Valores (SMV), gestión de efectivo, préstamos externos, políticas y procedimientos.
Revisión del Gobierno Corporativo de tesorería **Objetivo:** Revisar la estructura de gobierno de tesorería	▸ ¿Es efectivo el diseño del marco de gobierno? ▸ ¿Las políticas de tesorería están actualizadas y son adecuadas para abordar el mercado actual y los riesgos operativos? ▸ ¿Se definen con claridad las funciones y responsabilidades? ¿Son comunicadas oportunamente?
Marco de control y auditoría de cumplimiento SOX **Objetivo:** Evaluar el marco de control existente y la ejecución de pruebas SOX	▸ ¿Existen procesos y controles para administrar adecuadamente la gestión de cuentas bancarias, la gestión de riesgos financieros, la gestión de efectivo y los préstamos entre compañías? ▸ ¿Existe un universo definido de riesgos de tesorería? ▸ ¿El marco de control SOX, de aplicar, mitiga adecuadamente los riesgos identificados?

Tesorería

Auditorías de alto impacto	Preguntas clave a considerar
Revisión del sistema de tesorería **Objetivo:** Revisar la configuración del sistema de tesorería y realizar un diagnóstico de TI de tesorería, para identificar oportunidades de mejora del uso y de la eficiencia general del sistema	▸ ¿Las correspondientes áreas funcionales de tesorería se gestionan en el sistema de tesorería? ▸ ¿Se ha establecido una configuración de seguridad del sistema de tesorería y se revisa periódicamente? ▸ ¿Se utiliza el sistema y se controlan eficazmente los procesos de tesorería en todas las locaciones?
Fraude e investigación de tesorería Objetivo: Revisar la efectividad de los procesos y controles operacionales clave para determinar la probabilidad de fraude y evaluar las estrategias de remediación y el nivel de capacitación vigente	▸ ¿Existen procesos y controles operacionales clave y estos operan efectivamente para determinar la probabilidad de fraude en la organización en las siguientes áreas: - Gestión de efectivo? - Gestión de cuentas bancarias? - Tecnología de tesorería y marco de gobierno? ▸ ¿Se desarrollan planes de remediación y se les hace seguimiento? ▸ ¿Ha proporcionado la organización la capacitación necesaria sobre fraude y es esta efectiva?

Auditorías de alto impacto

Evaluación de la gestión de tesorería y modelo de madurez

Objetivo: Evaluar las actividades de gestión de tesorería frente a las normas de la industria y las organizaciones comparables

Preguntas clave a considerar

- ¿Las actividades de gestión de tesorería son consistentes con las normas de la industria o las organizaciones comparables?
- ¿Cuán efectivas son las actividades de tesorería en las siguientes áreas:
  - Gestión de cuentas bancarias?
  - Gestión de riesgos financieros?
  - Gestión de efectivo?
  - Transacciones entre empresas?
  - Gestión de riesgos de tasa de interés?
  - Tecnología?

Información financiera y empresarial con lenguaje de negocios XBRL

El lenguaje de negocios (XBRL, por sus siglas en inglés) es el lenguaje, de libre uso, basado en los estándares XML, que permite la interoperabilidad y análisis de cualquier tipo de información financiera y empresarial, a través de Internet, al integrar directamente las reglas de negocio en su desarrollo.

El lenguaje XBRL permite trasparencia, confiabilidad, oportunidad, comparabilidad y ahorro de costos. Lo anterior ha conseguido atraer a una comunidad de profesionales y organizaciones, públicas y privadas, representando a un gran número de países que forman parte de XBRL Internacional.

El propósito de XBRL es contar con un formato y taxonomía estándar para publicar la información contable-financiera, directamente explotable, y de forma trasparente y comparable con confiabilidad. La interoperabilidad facilita el procesamiento, intercambio y publicación de la información financiera y empresarial. Permite comparar información proveniente de diferentes fuentes y formatos, reduce el riesgo de errores en el ingreso manual de datos, proporciona una información precisa y validada automáticamente, es el medio apropiado para el manejo de datos por diferentes usuarios y herramientas, reduce el costo regulatorio, eliminando el papel y aplicando un solo formato estandarizado que exige un menor esfuerzo en la preparación y utilización de informes y, por último, facilita el almacenamiento automático y la posterior publicación para los reguladores e inversionistas, en los ámbitos público y privado.

La información bajo el lenguaje de negocios XBRL permite lograr la trasparencia financiera, tal es así que los reguladores de las entidades financieras, aseguradoras y de las empresas que cotizan sus valores en bolsas locales e internacionales cuentan con normativas para que la información se presente bajo el formato XBRL.

En el Perú, desde diciembre del 2011, la Superintendencia del Mercado de Valores (SMV) viene ejecutando el proyecto de Implementación XBRL el cual incluye:

1. Creación de una taxonomía XBRL que extiende de la taxonomía de las Normas Internacionales de Información Financiera.
2. Plataforma tecnológica para el tratamiento de los informes en formato XBRL: recepción, validación y almacenamiento.
3. Realización de una herramienta en Excel para que las empresas peruanas puedan reportar de manera más simple a la SMV.

Para las empresas que cotizan sus valores en mercados americanos, la preparación de documentos en lenguaje XBRL para propósitos de presentación de información financiera a la Comisión de Bolsa de Valores de Estados Unidos (SEC, por sus siglas en inglés), puede ser un desafío. Muchas empresas confían en proveedores externos para implementar la preparación de documentos en este lenguaje, sin entender primero la complejidad y la amplitud de las reglas de la SEC. Es fundamental que la gerencia entienda estos requisitos para tomar decisiones informadas durante la generación y revisión de la información financiera bajo el lenguaje XBRL.

Información financiera y empresarial con lenguaje de negocios XBRL

La SEC continúa identificando errores significativos y recurrentes en documentos bajo el lenguaje XBRL, razón por la cual ha comenzado a informar a las empresas sobre estos errores, a través de cartas dirigidas a los Gerentes Financieros, en donde se les solicita incluir detalles de cálculo a manera de anexos en los documentos XBRL. Como resultado, docenas de compañías han modificado su presentación de documentos XBRL ante la SEC para corregir los errores detectados.

Los problemas más comunes en los documentos bajo el lenguaje XBRL incluyen:

- Selección inadecuada de etiquetas o etiquetas extendidas, en lugar de usar etiquetas estándar, como parte de la taxonomía estándar de este lenguaje documentario, ampliamente definida en los materiales de consulta.
- No etiquetar todos los niveles y montos exigidos, por ejemplo, cantidades entre paréntesis y cantidades en notas y anexos.
- Uso de signos incorrectos, como positivos y negativos.
- Errores en las fechas de los informes, decimales, unidades y cálculos faltantes.
- Exclusión indebida de documentos XBRL con declaraciones de registro de ofertas públicas.
- Falta de implementación de controles sólidos que permitan dar cumplimiento con las exigencias del lenguaje XBRL.

A fin de producir documentos confiables y de alta calidad, las empresas deben comprender las exigencias técnicas, ejercer la diligencia en la selección de etiquetas apropiadas y verificar que todos los detalles requeridos se capturen con precisión.

Las empresas deben considerar las siguientes inquietudes relacionadas con XBRL:

- La SEC continúa haciendo modificaciones y observaciones, generalmente actualizando los requisitos de XBRL de manera trimestral.
- El volumen de guías de la SEC es significativo, e incluso están escritas de manera compleja.
- Muchos solicitantes de registro no comprenden completamente la complejidad del etiquetado de manera detallada.
- La SEC ha reiterado que los controles sobre la preparación de documentos bajo el lenguaje XBRL deben ser un componente de los procesos y controles de divulgación del emisor.
- La quditoría interna podría aportar el conocimiento en la materia y del negocio, para proporcionar una evaluación objetiva del estado actual y ofrecer orientación sobre cómo desarrollar un proceso interno eficiente y efectivo sobre los informes bajo el lenguaje XBRL.

Auditorías de alto impacto

Regulación y cumplimiento

Objetivo: Revisar los documentos bajo el lenguaje XBRL para cumplir con las normas aplicables

Preguntas clave a considerar

- **Documentación:** ¿Se ha evaluado o creado documentación en torno a la selección de etiquetas para los estados financieros, incluyendo la carátula, las notas y los anexos, para verificar que refleja de manera precisa lo que se está divulgando?
- **Documentación completa:** ¿Se ha evaluado que los montos y conceptos en los estados financieros, las notas y los anexos están completos? ¿Se han identificado elementos que puedan no estar incluidos en todos los niveles requeridos? ¿Los artículos que no están etiquetados (si los hay) incluyen la correspondiente explicación documentada?
- **Selección de etiquetas:** ¿Se ha evaluado la selección de etiquetas y la identificación de posibles elementos o dimensiones alternativas que tengan definiciones similares a las de los elementos y dimensiones elegidos, así como conceptos financieros que no se ajustan a la guía XBRL?
- **Cumplimiento estructural y de consistencia del documento:** ¿Se ha evaluado el documento de XBRL en torno a los errores estructurales o de consistencia, incluido el cumplimiento de la señalización correcta (valores positivos vs. negativos), atributos decimales, tipos de unidades, ciertos contextos y relaciones de cálculo?

Información financiera y empresarial con lenguaje de negocios XBRL

Auditorías de alto impacto

Gobierno, política y procesos de control interno

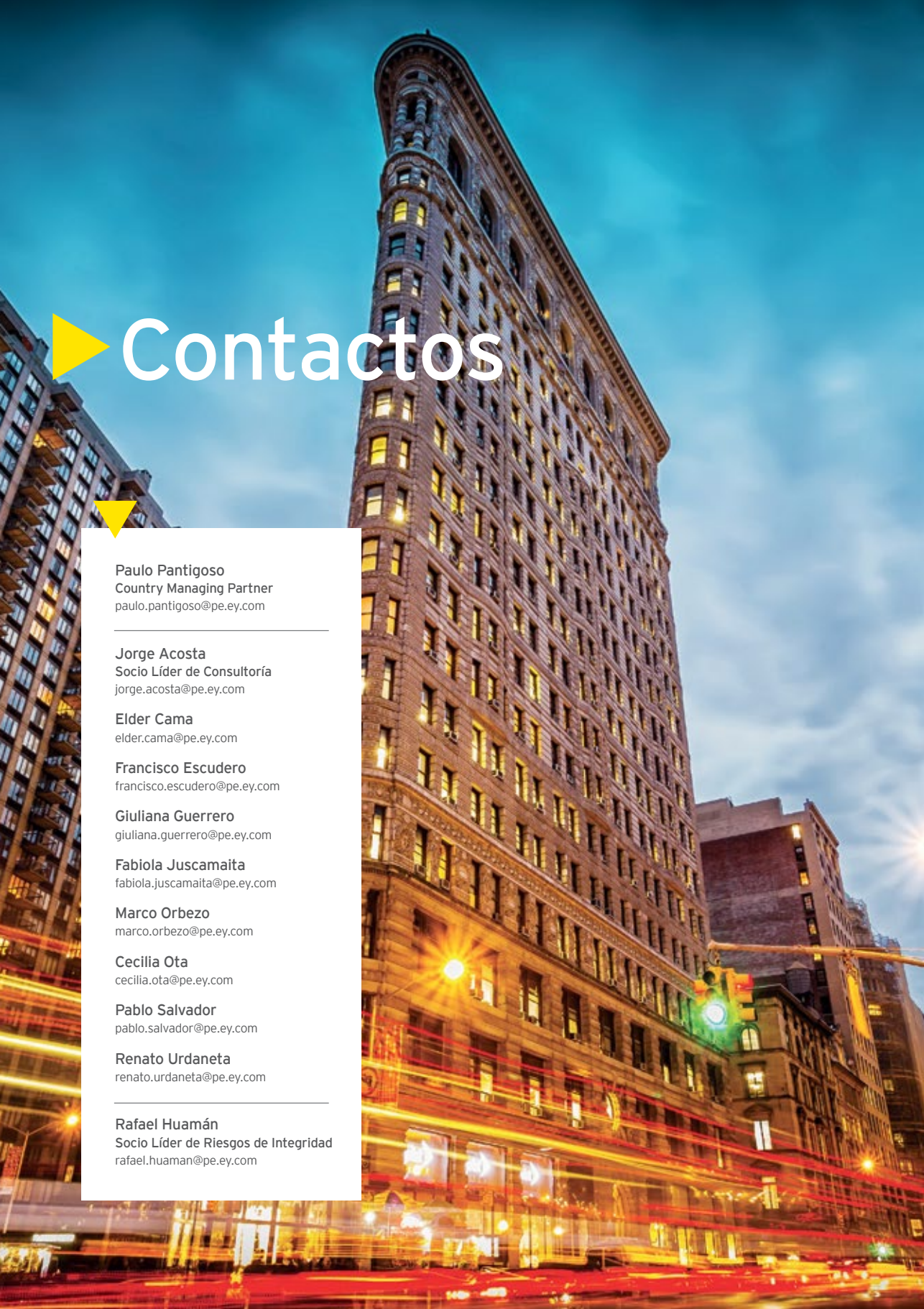
Objetivo: Evaluar la calidad y eficiencia del gobierno, las políticas y los controles asociados con la generación de los anexos XBRL

Preguntas clave a considerar

- ¿Existe un proceso formalizado de implementación y revisión de los documentos en el lenguaje XBRL?
- ¿Se ha comparado el estado actual de la empresa en relación a la implementación, proceso de revisión y procedimientos clave de los documentos a presentar bajo el lenguaje XBRL contra las prácticas líderes?
- ¿Hay suficientes procesos de implementación del lenguaje XBRL, gobierno, políticas y procesos de control interno y documentación aplicable para cumplir adecuadamente con las reglas XBRL y los requisitos de procesos y controles de divulgación aplicables?

¿Por qué debería ser importante para los solicitantes de registro ante la SEC, contar con la documentación bajo el lenguaje XBRL?

▸ Complejidades y observaciones más comunes	‣ Requisitos XBRL de la SEC incluidos por separado en el Manual del Presentador EDGAR de la SEC. ‣ Errores archivados, identificados por XBRL-US. ‣ Recordatorios y comentarios escritos de la SEC en relación a la calidad de datos. ‣ Información excluida por cientos de empresas, según XBRL-US. ‣ Formularios 10-K y 10-Q modificados, debido a problemas y errores en los documentos originales bajo el lenguaje XBRL. ‣ Procedimientos, principios y criterios operativos estándar emitidos por el Instituto Estadounidense de Contadores Públicos Certificados (AICPA) para abordar las complejidades. ‣ Datos XBRL utilizados en el Modelo de Dualidad Contable de la SEC para identificar las empresas que requieren una mejor inspección.
▸ Riesgos	‣ *Goodwill* del reporte financiero y riesgo reputacional. ‣ La misma responsabilidad sobre la presentación de la información financiera con el formato tradicional (por ejemplo, Formularios 10-Q, 10-K) y posible responsabilidad civil. ‣ Actualizaciones, cambios prospectivos u otras acciones de la SEC. ‣ Dentro del alcance de los "controles y procedimientos de divulgación" para cumplir con las normas 13a-15 y 15d-15 de la Ley y el artículo 307. ‣ Falta de aceptación por parte de la SEC de los documentos XBRL (es decir, no se cargará a través del portal EDGAR), en caso fallen las pruebas de validación. ‣ Cartas a los Gerentes Financieros por parte de la SEC, así como llamadas a las empresas, sobre los errores más comunes detectados en los documentos bajo el lenguaje XBRL. ‣ Aspectos de los anexos de los documentos XBRL incluidos por la SEC, en el proceso de comentarios a las cartas de la División de Finanzas de la Corporación (DCF, por sus siglas en inglés).



Contactos

Paulo Pantigoso
Country Managing Partner
paulo.pantigoso@pe.ey.com

Jorge Acosta
Socio Líder de Consultoría
jorge.acosta@pe.ey.com

Elder Cama
elder.cama@pe.ey.com

Francisco Escudero
francisco.escudero@pe.ey.com

Giuliana Guerrero
giuliana.guerrero@pe.ey.com

Fabiola Juscamaita
fabiola.juscamaita@pe.ey.com

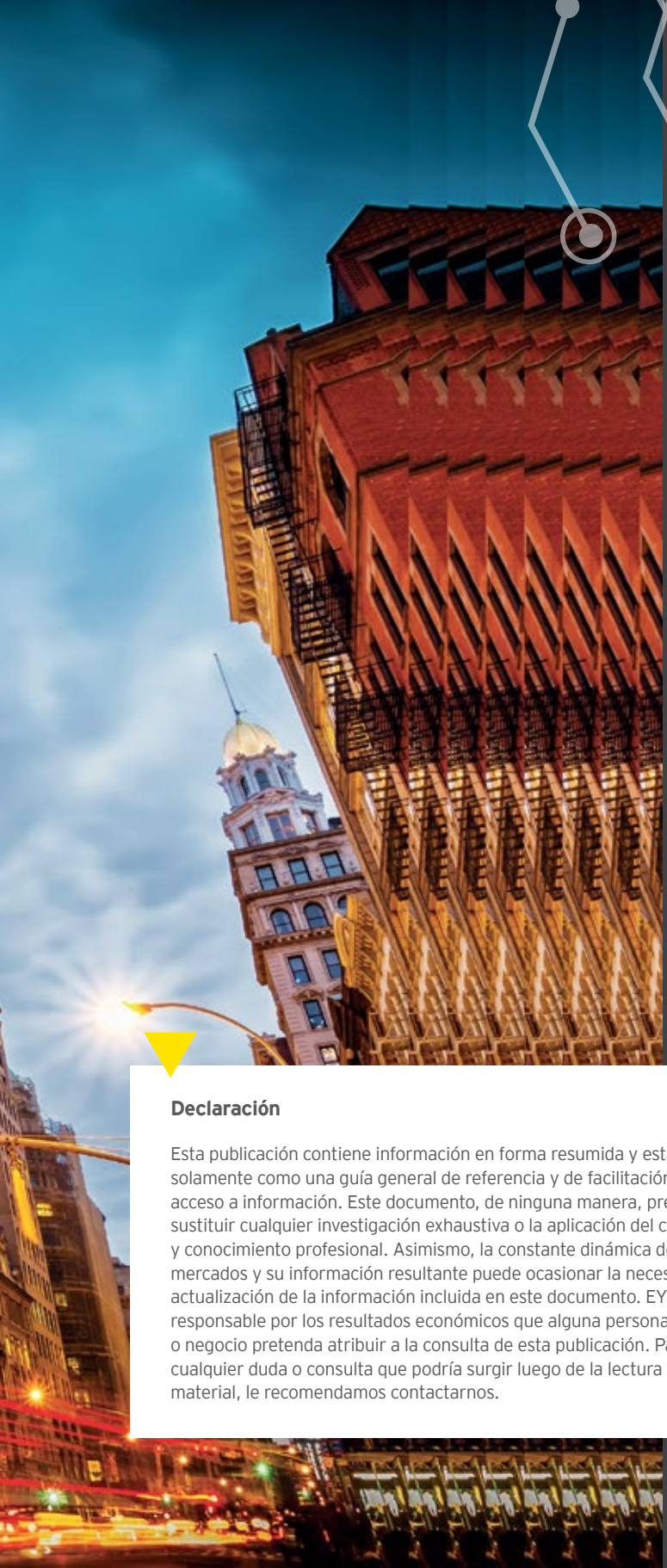
Marco Orbezo
marco.orbezo@pe.ey.com

Cecilia Ota
cecilia.ota@pe.ey.com

Pablo Salvador
pablo.salvador@pe.ey.com

Renato Urdaneta
renato.urdaneta@pe.ey.com

Rafael Huamán
Socio Líder de Riesgos de Integridad
rafael.huaman@pe.ey.com



Declaración

Esta publicación contiene información en forma resumida y está pensada solamente como una guía general de referencia y de facilitación de acceso a información. Este documento, de ninguna manera, pretende sustituir cualquier investigación exhaustiva o la aplicación del criterio y conocimiento profesional. Asimismo, la constante dinámica de los mercados y su información resultante puede ocasionar la necesidad de una actualización de la información incluida en este documento. EY no se hace responsable por los resultados económicos que alguna persona, empresa o negocio pretenda atribuir a la consulta de esta publicación. Para resolver cualquier duda o consulta que podría surgir luego de la lectura de este material, le recomendamos contactarnos.

EY | Auditoría | Consultoría | Impuestos | Transacciones & Finanzas Corporativas

Acerca de EY
EY es el líder global en servicios de auditoría, impuestos, transacciones y consultoría. La calidad de servicio y conocimientos que aportamos ayudan a brindar confianza en los mercados de capitales y en las economías del mundo. Desarrollamos líderes excepcionales que trabajan en equipo para cumplir nuestro compromiso con nuestros stakeholders. Así, jugamos un rol fundamental en la construcción de un mundo mejor para nuestra gente, nuestros clientes y nuestras comunidades.

Para más información visite:
www.ey.com/pe

EYPerú Library

Descargue nuestras publicaciones en:
ey.com/PE/EYPeruLibrary

/EYPeru
@EYPeru
/company/ernstandyoung
@ey_peru
/EYPeru
perspectivasperu.ey.com
ey.com/pe