Auditoría Pública nº 73 (2019), pp. 43 - 51

Sandra Barrio Carvajal
Auditora
Cámara de Cuentas de Andalucía

Nuevas tendencias en la gestión de riesgos del control interno

RESUMEN/ABSTRACT:

En la actualidad, el entorno en el que se desenvuelven las organizaciones es cada vez más complejo, ambiguo, incierto y volátil, por lo que cada vez son más los riesgos a los que deben enfrentarse. Por todos estos motivos, las organizaciones deben crear un aseguramiento continuo y actualizado de que los controles funcionan, de forma que los riesgos puedan ser mitigados y permitan adaptarse al cambio.

Este entorno cambiante incrementa la necesidad de la implantación de un buen sistema de control interno, que detecte y controle los riesgos a los que se enfrenta la organización dentro de unos niveles admisibles. En este artículo se abordan algunas de las tendencias actuales de los posibles riesgos con los que puede enfrentarse el control interno de una organización.

Currently, the environment in which organizations operate is increasingly complex, ambiguous, uncertain and volatile, so that there are more and more risks to be faced. For all these reasons, organizations must create a continuous and updated assurance that controls work, so that risks can be mitigated and adapt to change.

This changing environment increases the need for the implementation of a good internal control system, which detects and controls the risks faced by the organization within acceptable levels. This article addresses some of the current trends in the possible risks that an organization's internal control may face.

PALABRAS CLAVE/KEYWORDS:

CONTROL INTERNO, GESTIÓN DE RIESGOS, COMPLIANCE, CIBERSEGURIDAD, FRAUDE
INTERNAL CONTROL, RISK MANAGEMENT, COMPLIANCE, CYBERSECURITY, FRAUD

1. INTRODUCCIÓN

En la gestión del control interno y la auditoría, continúan apareciendo nuevos retos y riesgos que hacen que surja la necesidad de buscar nuevos conceptos y aportaciones, que permitan que el auditor preste un servicio lo más completo posible, con una perspectiva integral de la gestión y organización de la empresa.

Desde este artículo se pretende profundizar en el análisis de algunos de los nuevos riesgos que se proponen como los más actuales y que afectan al control interno y en consecuencia al trabajo del auditor. Es importante que tanto las organizaciones, como el auditor, sean conscientes de los mismos para poder prepararse y formarse de manera que la repercusión de los mismos afecte de la menor forma posible, permitiendo conseguir los niveles óptimos de eficacia y eficiencia en el diseño de los riesgos que afecten al control interno.

Las nuevas tendencias que se describen en este artículo son:

- Compliance
- Ciberseguridad
- Lucha contra la corrupción y prevención del fraude
- VUCA

2. COMPLIANCE

En primer lugar, se destaca el término compliance y el creciente interés por las empresas de incluir esta función, como un instrumento de prevención con el fin de evitar posibles sanciones penales por parte de las mismas, incluyendo nuevos elementos de carácter no normativo como son los principios éticos de la empresa.

Según Elena Moreno García en su artículo "¿Qué es el compliance?" (2017), el compliance o cumplimiento normativo es la necesidad de una empresa de establecer procedimientos adecuados para garantizar que tanto directivos, empleados y demás agentes relacionados cumplan con la normativa actual. Para ello, es necesario identificar y clasificar los riesgos legales a los que se enfrentan y establecer mecanismos de prevención, gestión, control y reacción. Cuando se habla de marco normativo no solamente nos referimos a leyes sino también a políticas internas, los compromisos con clientes, proveedores o terceros, y especialmente los códigos éticos que la empresa se haya comprometido a respetar, pues existen multitud de casos en los que una actuación puede ser legal pero no ética.

Este movimiento está llevando a que las empresas tiendan a una mayor cultura de la ética y mayor implicación con el cumplimiento normativo. Un ejemplo de ello es la aprobación de Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas de la Fiscalía General del Estado. En este documento se imparten instrucciones a los fiscales para valorar la eficacia de los planes de cumplimiento normativo o compliance en las empresas, que tras la reforma se configuran como una eximente de la responsabilidad penal, incorporando una completa regulación de los programas de cumplimiento normativo o compliance guides.

Además, con la entrada en vigor del Real Decreto 424/2017, de 28 de abril, por el que se regula el régimen jurídico del control interno en las entidades del Sector Público Local, se ha puesto en marcha el nuevo modelo de control interno en el ámbito local, a través de la función interventora y del control financiero. Este modelo de control se encuadra dentro de las nuevas políticas de compliance en el sector público y, en consecuencia, como un nuevo modelo de prevención de riesgos.

El sector público, está reconociendo la importancia del compliance y comenzando a aplicar dicha gestión, apostando por la necesidad de contar con mecanismos de cumplimiento normativo para el control de los delitos en la esfera pública. El 23 de mayo de 2018 se celebró el I Congreso de Compliance en el Sector Público, organizado por la WCA (*World Compliance Association*) y la Universidad de Castilla-La Mancha. Con grandes y reconocidos expertos en la materia se abordaron, a través de los siguientes bloques, las principales líneas de reflexión que centran el debate en estos momentos:

- Necesidad de Compliance en el Sector Público. Cumplimiento normativo y control de delitos
- Control Externo de Fondos Públicos y Cumplimiento normativo
- Implementación de Estrategias e Instrumentos de Compliance en el Sector Público
- Cumplimiento y Prevención del Fraude en la Gestión de Fondos estructurales y de Inversión Europeos
- Estatuto del Compliance Officer
- Contratación Pública y Compliance

Tal y como indican Sylvie Bleker y Dick Hortensius en "ISO 19600: *The development of a global standard on compliance management*" (2014), "la gestión del compliance va más allá de la mera satisfacción de los requisitos legales. El compliance también está relacionado con satisfacer las necesidades y expectativas de la mayoría de partes interesadas. Por lo tanto, tomar decisiones acertadas y establecer prioridades es una parte importante de la gestión del compliance. ISO 19600 sigue un enfoque basado en el riesgo para la gestión del compliance".

Sylvie Bleker y Dick Hortensius también indican que la gestión del compliance es mucho más que simplemente cumplir con los requisitos de las leyes y regulaciones. Las organizaciones tienen que lidiar con diferentes tipos

de requisitos de una gran variedad de partes interesadas, como son los certificados, estándares clave y puntos de referencia que se han elegido de forma voluntaria, así como con sus propias políticas de la empresa Normas y códigos de negocio.

Por tanto, la norma ISO 19600 se ha desarrollado como una guía para la gestión de cumplimiento y no como una especificación que proporciona requisitos.

A continuación, en la siguiente figura se detallan las definiciones clave de la ISO-19600:

Fuente: Elaboración propia basada en "*ISO 19600: The development of a global standard on compliance management*" (2014).

Con el nacimiento del compliance ha surgido la figura del Compliance Officer, que será el responsable de asegurar el cumplimiento de la normativa de aplicación o de cualquier tipo de legislación relacionada con el sector. El Compliance Officer ha cobrado más importancia porque desde el 1 de julio de 2015, la reforma del Código Penal obliga a toda empresa o profesional a contar en su plantilla con un Director de Cumplimiento Normativo o los servicios de una empresa externa para llevar a cabo esta labor.

Crespo Barquero, P (2016), define el compliance officer como el encargado en nombre de la persona jurídica, incluso en el caso de que sean agentes externos, de hacer efectivos los controles de prevención.

Las principales funciones de esta figura se recogen en la Norma ISO 19600, y Ana Díaz Escudero en "Análisis del marco teórico y legal de la evolución de la responsabilidad de las Personas jurídicas y las obligaciones del compliance officer" (2017,50) las resume en:

1. Es el órgano de administración al que se le asignan las funciones de supervisión del programa y su eficacia, órgano supervisor.
2. Es el órgano que ostenta el poder de control y vigilancia de los programas y su aplicación, responsable de cumplimiento normativo.
3. Es aquel que tiene la posición desde la cual debe apuntar los fallos, defectos, o carencias, tanto del programa como de su aplicación.

Por todo lo expuesto se pone de manifiesto la importancia que está cobrando el compliance en las nuevas tendencias en la gestión de riesgos de control interno, y

como las empresas tendrán que establecer controles en este sentido.

3. CIBERSEGURIDAD

Otra de las tendencias importantes en el control interno es la denominada Ciberseguridad. La vertiginosa aparición de nuevas tecnologías y su presencia online indudablemente proporciona un valor añadido a las organizaciones, y ningún dispositivo hardware o software existente está exento de sufrir un ataque informático.

Según Javier Carvajal Azcona, en su artículo "Definición de ciberseguridad y riesgo" (2017), la definición de ciberseguridad por parte de ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de Información) es la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

Según indican Samir M. El-Gazzar y Rudolph A. Jacob en su artículo *Integrating internal control frameworks for effective corporate information technology governance* (2017), las tecnologías de la información (en adelante TI) se han convertido en uno de los activos estratégicos más importantes y una herramienta crítica para garantizar la sostenibilidad y el desarrollo de un negocio. Se argumenta que la responsabilidad de diseñar, implementar y mantener muchos de los controles sobre los procesos de negocios de cualquier organización depende de la Tecnología de la Información. La función de las TI es la de recopilar, convertir, archivar, proteger, procesar, entregar y recuperar información de forma segura según sea necesario (Abu-Musa, 2008). Muchas organizaciones han estado utilizando varios marcos, como el Control de objetivos para información y tecnologías relacionadas (COBIT), Enterprise Risk Management (ERM) y el Comité de organizaciones patrocinadoras de la Comisión Treadway (COSO). Para un gobierno de TI óptimo, se sostiene que las organizaciones deben integrar estos marcos. Un marco integrado es uno que vincula los objetivos de control clave con los objetivos estratégicos del negocio y, al hacerlo, aborda los principios de gobierno de TI tanto a nivel estratégico como operativo, al mismo tiempo que alinea la comprensión de TI y la gestión empresarial de las áreas clave de riesgo que caracterizan los objetivos de la organización (Goosen y Rudman, 2013). Además, se espera que esta alineación fundamental elimine los controles y procesos innecesarios que, a su vez, ayudan a mejorar el gobierno de TI y el cumplimiento normativo.

Por todo esto, tal y como indica el Instituto de Auditores internos en "Ciberseguridad: Una guía de supervisión" (2016), la ciberseguridad representa actualmente una de las principales preocupaciones de todas las empresas e instituciones, con independencia del sector o ámbito al que pertenezcan.

El IAI, continúa diciendo que las ciberamenazas que han provocado algunas de las mayores infecciones y trastornos recientes en materia de seguridad informática son las siguientes:

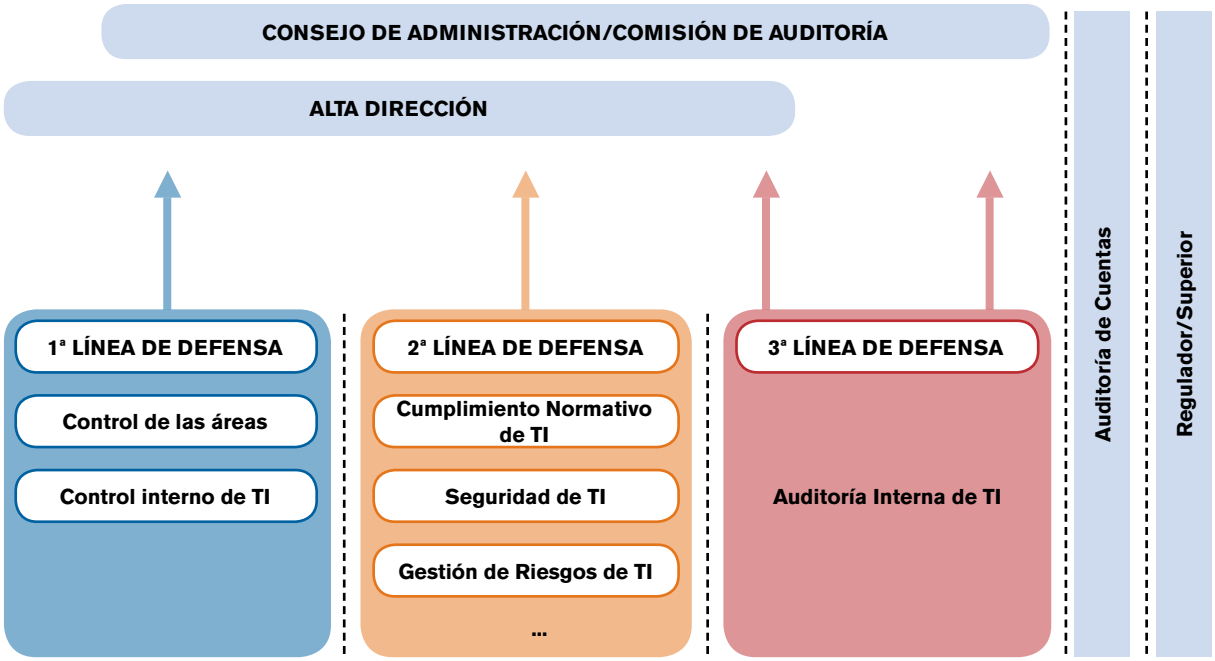
- Zeus. Malware3 orientado al robo de información personal de los usuarios: credenciales de cuentas de correo electrónico, redes sociales, datos de servicios financieros, etc.
- Flame y Agent BTZ. Software espía con gran capacidad de propagación capaz de obtener capturas de pantalla, pulsaciones de teclado, control del bluetooth, webcam o grabación de llamadas. Asimismo, posee la capacidad de transmitir la información recopilada ocultándola mediante técnicas de cifrado.
- Carbanak. Ataque Persistente Avanzado (APT) diseñado y dirigido al sector bancario, capaz de alterar y manipular el funcionamiento de las redes y software de control de los cajeros automáticos.
- Ransomware. También conocido como el "virus de la policía", cifra la información contenida en el sistema del usuario infectado, solicitando una compensación económica para su desbloqueo.
- Stuxnet. Software malicioso descubierto en 2010, capaz de controlar y manipular software de control y supervisión de procesos industriales (SCADA).

Por todos estos motivos, cada vez más, los ciberataques suponen uno de los principales riesgos de control interno a través de los que se puede captar información vital de una empresa.

Por tanto, en el control interno, se deben integrar controles para poder evitar que ocurran estos sucesos o, en el caso de que ocurran, se puedan detectar y minimizar los efectos que puedan producir. En el análisis de riesgos del control interno de una empresa, se deben tener en cuenta las posibles debilidades con respecto a la ciberseguridad.

El Instituto de auditores internos, comenta en la guía de ciberseguridad que una buena aproximación, en cuanto a los controles a establecer, puede consistir en integrar la ciberseguridad en el sistema comúnmente implantado en la mayoría de las organizaciones (modelo de las tres líneas de defensa). A continuación, se indica un esquema con el modelo de las tres líneas de defensa expuesto por la European Confederatión del Instituto de auditores internos internacional.

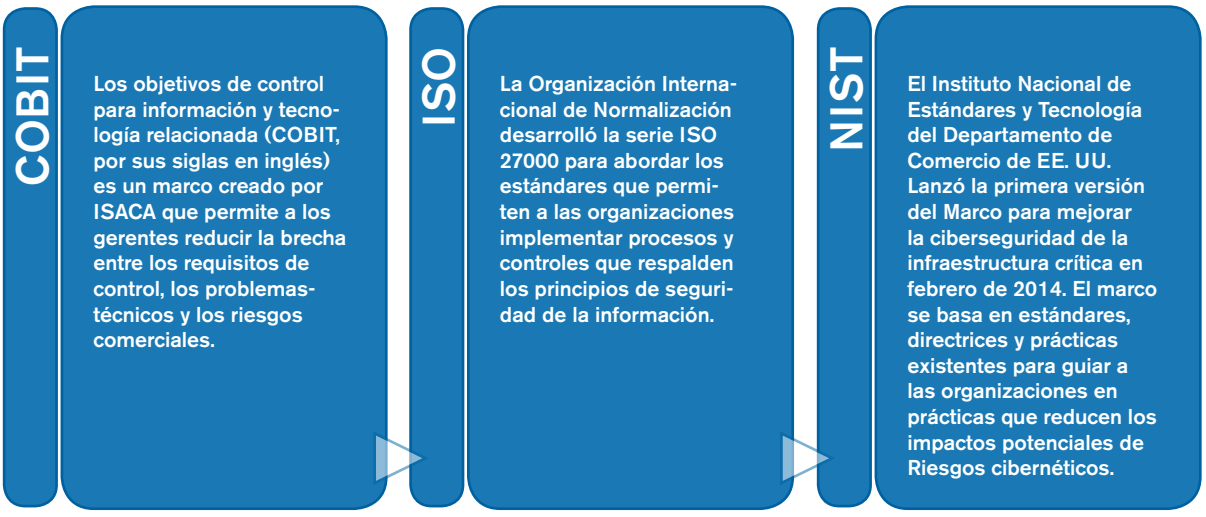
Modelo de las Tres Líneas de Defensa* adaptado al riesgo de Ciberseguridad



*European Confederation of Institutes of Internal Auditors/Federation of Risk Management Association - 2013. Endorse By Global Institute of Internal Auditors - 2014.

Fuente: *European Confederation of institutes of internal Auditors/Federation of risk Management Association* (2013)

Tal y como se indica en el informe *Coso in the cyber age* (2015), cada organización está gestionada por diferentes personas con habilidades y experiencias únicas que impulsan los juicios profesionales que se aplican para afectar el control interno. Al evaluar si la organización ha diseñado e implementado controles apropiados para mitigar los riesgos cibernéticos, es útil comparar las actividades de control con los estándares y marcos que están alineados con la gestión de los riesgos cibernéticos. La figura que se indica continuación proporciona referencias y antecedentes sobre los marcos y estándares centrados en el ciberespacio que pueden proporcionar asistencia adicional a las organizaciones al evaluar la suficiencia de los controles para estar seguros, vigilantes y resilientes.



Fuente: Elaboración propia basada en el documento *Coso in the cyber age* (2015).

Por tanto, con todo lo expuesto, queda claro el creciente aumento de los ciber ataques y como consecuencia, esto debe incidir en una mayor previsión de controles para evitarlos y detectarlos. Por lo que cada vez más, esta será una de las tendencias actuales en las que deberá centrarse el control interno.

4. LUCHA CONTRA LA CORRUPCIÓN Y PREVENCIÓN DEL FRAUDE

Otra de las nuevas tendencias en la gestión de riesgos del control interno consiste en la lucha contra la corrupción y la prevención del fraude.

Según el Transparency international, las denuncias de los medios de comunicación y el relevante eco social y atención prestada a los casos ahora aflorados han influido intensamente en la percepción ciudadana, generando un estado general de indignación que lleva a que España sea el país de la UE donde más ha crecido la percepción de corrupción en los últimos cinco años; también es cierto que la crisis económica ha incrementado el nivel de exigencia social, y aunque la justicia viene cumpliendo su función con cierto rigor, a pesar de su lentitud, se ha generado desde fines de 2009 un muy alto nivel de alarma social y una sensación de que al final habrá impunidad en los casos relevantes. El Proyecto de Ley integral contra la corrupción, pueden ser un avance muy importante en la lucha contra la misma, aunque actualmente, sigue en trámite parlamentario,

El 11 de septiembre de 2018 se ha celebrado la jornada: Diagnosis y propuestas sobre transparencia y corrupción en España (En el 25 Aniversario de Transparency International), organizada por Transparencia internacional España. En esta Jornada se realizó un amplio Diagnóstico integral de la situación en España en relación con la transparencia, la integridad, y la prevención y lucha contra la corrupción.

Las principales propuestas que se emitieron con respecto a la corrupción se resumen en las siguientes:

- El Consejo de Transparencia y Buen Gobierno y el resto de consejos autonómicos deben tener competencias sancionadoras e inspectoras.
- Se debe impulsar la aprobación de la Ley integral de lucha contra la corrupción y protección a los denunciantes, que está actualmente en tramitación parlamentaria.
- Se debe incorporar la transparencia como un verdadero principio rector de la cultura empresarial y de la cultura de cumplimiento, partiendo de un compromiso de la dirección de las compañías.
- La transparencia y el compliance deben formar parte del ADN de las empresas.
- Se debe apuntar hacia la formación y la educación para prevenir la corrupción dentro de las empresas.
- También se deben establecer mecanismos para identificar las malas prácticas, como canales de denuncias, auditorias, investigaciones y controles periódicos, y aplicar con dureza las consecuencias en caso de que se detecte alguna irregularidad.
- Apostar por el proceso de digitalización de la información, para garantizar la trazabilidad, la transparencia y la eficiencia en los procesos.
- Impulsar la profesionalización de quienes trabajan en el área de compliance, transparencia y buen gobierno dentro de las organizaciones deportivas.
- Mejorar la comunicación en la Fiscalía y los órganos de administración de justicia, para explicar bien los procedimientos a la ciudadanía. Así se pueden evitar las falsas expectativas en los procesos relacionados con la corrupción y la idea de que la justicia es ineficiente.
- Es indispensable que la Fiscalía Anticorrupción cuente con una mayor dotación de recursos y un acceso a técnicas modernas de investigación y análisis.
- Se debe modificar la regulación procesal para que se puedan perseguir adecuadamente los delitos en la actualidad.
- Es necesario dotar de más recursos al sistema de justicia, para que los jueces puedan trabajar de una mejor manera.
- Hay que incrementar los medios necesarios, tanto personales como materiales, para garantizar una mayor agilidad en la respuesta de las instituciones frente a la corrupción.
- Los partidos políticos deben cesar en su intento de politizar la justicia o de judicializar la política.
- Se debe reducir el número de aforados, los indultos y el clientelismo político.
- Es indispensable la profesionalización de los funcionarios de la administración pública.
- Se debe trabajar en la educación para fomentar el respeto hacia lo público.
- Hay que regular los lobbies y conectarlos con el sistema de control interno y de conflictos de intereses en las administraciones públicas.
- Se debe trabajar para mejorar la imparcialidad en la administración pública y fomentar la función directiva profesional.
- Hay que trabajar en la formación en ética, integridad e imparcialidad en todas las administraciones.
- Se debe impulsar la evaluación de los programas públicos, la elaboración de códigos éticos y los análisis de los riesgos de corrupción.

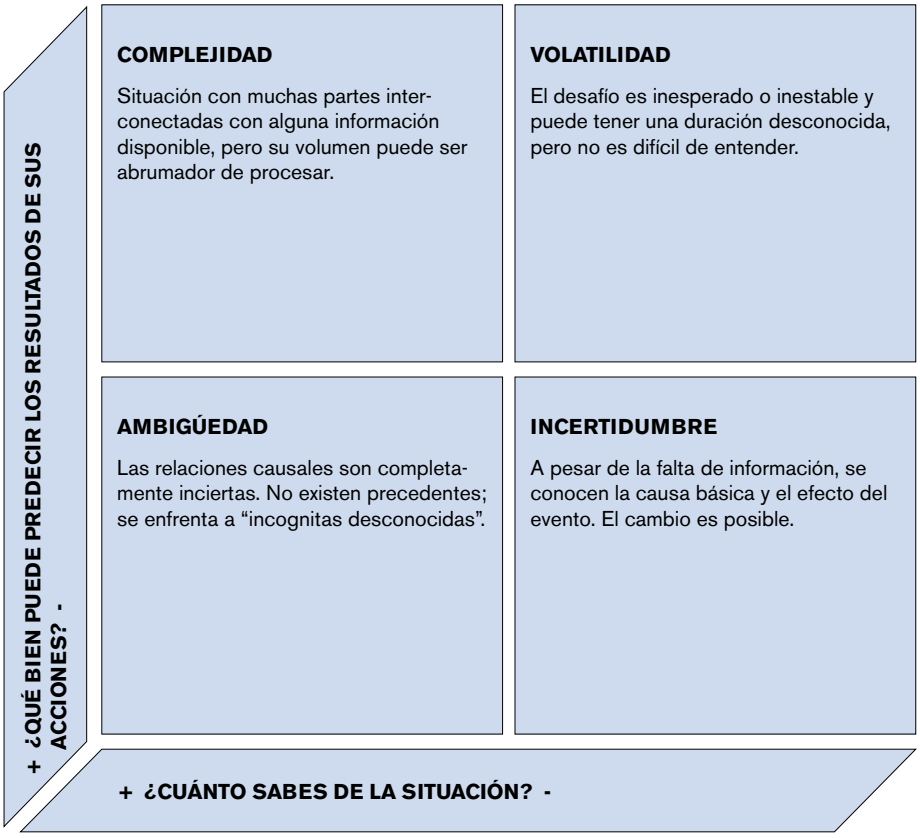
- Se debe mejorar la participación y la implicación de la ciudadanía para que los gobiernos aumenten la calidad de los servicios públicos.
- A corto plazo, se debe fomentar la aplicación efectiva del marco legal relacionado con la lucha anticorrupción.
- A medio plazo, los países deben adoptar las convenciones de la ONU y los acuerdos internacionales contra la corrupción.
- A largo plazo, se debe trabajar en la educación de los ciudadanos, la conciencia social y la formación en valores.
- Hay que trabajar en la ética y convencer a la ciudadanía de su importancia para garantizar la sostenibilidad, la rentabilidad y la felicidad.
- Se deben empezar a estudiar las herramientas para luchar contra la corrupción en el mundo actual, considerando los retos que imponen la inteligencia artificial, las criptomonedas y las grandes redes de corrupción en todo el mundo.
- Aplicar la fórmula de las 4 íes para luchar contra la corrupción: más Información, más Integridad, menos Impunidad y menos Indiferencia.

Las conclusiones que se deben sacar son la creciente preocupación por la lucha contra el fraude y la corrupción y la importancia que esto debe tener, y aun más en la administración pública. Por todo esto, será necesario que cuando se realice un análisis del control interno, se tengan en cuenta los riesgos que se derivan del fraude y la corrupción y que se tenga en cuenta cuando se establezcan los controles necesarios.

5. VUCA

Por último, se debe destacar el término VUCA, que hace alusión al entorno en el que se mueven las organizaciones en la actualidad, cuyas siglas que proceden del inglés significan: Volatility (V), Uncertatinty (U), Complexity (C) y Ambiguity (A) caracteriza por la volatilidad, la incertidumbre, la complejidad y la ambigüedad.

Por tanto, las empresas deben prepararse para actuar frente a este tipo de entornos. Nathan Bennettand y G.James Lemoine, en su artículo "What VUCA really means for you" (2014), indican una guía para que las empresas puedan actuar en un entorno VUCA. De forma esquemática se expone a continuación un resumen de dicha guía:



Fuente: Nathan Bennettand y G.James Lemoine (2014)

Si se detalla la guía que indican se reflejan los siguientes aspectos:

Complejidad

Características: La situación tiene muchas partes y variables interconectadas. Alguna información está disponible o puede predecirse, pero su volumen o naturaleza puede ser abrumador de procesar. Ejemplo: Usted está haciendo negocios en muchos países, todos con entornos regulatorios únicos, aranceles y valores culturales.

Enfoque: Reestructurar, atraer o desarrollar especialistas, y acumular recursos adecuados para abordar la complejidad.

Ejemplo: Usted está haciendo negocios en muchos países, todos con entornos regulatorios únicos, aranceles y valores culturales.

Enfoque: Reestructurar, atraer o desarrollar especialistas, y acumular recursos adecuados.

Volatilidad

Características: el desafío es inesperado o inestable y puede tener una duración desconocida, pero no es necesariamente difícil de entender; conocimiento a menudo está disponible.

Ejemplo: los precios fluctúan después de un desastre natural que lleva a un proveedor a la línea.

Enfoque: aumentar la flexibilidad y dedicar recursos a la preparación, por ejemplo, acumular inventario o sobrecompra talentos. Estos pasos son típicamente caros; su inversión debe coincidir con el riesgo.

Ambigüedad

Características: Las relaciones causales son completamente inciertas. No existen precedentes; se enfrenta a "incógnitas desconocidas". Ejemplo: decide mudarse a mercados emergentes o inmaduros o lanzar productos fuera de sus competencias principales.

Enfoque: Experimento. Comprender la causa y el efecto requiere generar hipótesis y probarlas. Diseña tus experimentos para que las lecciones aprendidas puedan aplicarse ampliamente.

Ejemplo: decide mudarse a mercados inmaduros o emergentes o lanzar productos fuera de sus competencias centrales.

Enfoque: Experimento. Comprender la causa y el efecto requiere generar hipótesis y probarlas. Diseña tus experimentos para que las lecciones aprendidas puedan aplicarse.

Incertidumbre

Características: a pesar de la falta de otra información, se conocen la causa básica y el efecto del evento. El cambio es posible pero no dado.

Ejemplo: el lanzamiento de un producto pendiente de un competidor confunde el futuro del negocio y del mercado.

Enfoque: Invertir en información: recopilarla, interpretarla y compartirla. Esto funciona mejor junto con cambios estructurales, como agregar redes de análisis de información, que pueden reducir la incertidumbre en curso.

Tal y como señala Kirk Lawrence "Developing leaders in a VUCA enviroment" en un estudio reciente del Boston Consulting Group, se llegó a la conclusión de que las organizaciones de hoy deben cambiar sus modelos de negocios, y sus habilidades de liderazgo, para convertirse en "firmas adaptativas". Las firmas adaptativas pueden ajustarse y aprender mejor, más rápido y más económicamente que sus similares, dándoles una "ventaja adaptativa". Las empresas adaptativas mencionadas en el estudio incluyen Apple, Google, 3M, Target y Amazon.

Kirk Lawrence continúa explicando en su trabajo que un informe del Centro para el Liderazgo Creativo (Petrie, 2011) también señala que el entorno empresarial actual de VUCA requiere que los líderes posean capacidades de pensamiento más complejas y adaptativas. También señala que los métodos utilizados para desarrollar estos nuevos requisitos de habilidades (como la capacitación en el trabajo, el coaching y el mentoring) no han cambiado mucho y, como resultado, los líderes no se están desarrollando lo suficientemente rápido ni en la forma correcta con respecto a lo que se requiere como la "nueva normalidad" para los negocios.

6. CONCLUSIONES

Como ya se ha comentado, este entorno cambiante en el que se mueven las organizaciones incrementa la necesidad de la implantación de un buen sistema de control interno que tenga en cuentas todos los posibles riesgos que puedan surgir.

El enfoque tratado en este artículo, sobre las nuevas tendencias en la gestión de riesgos en la metodología de control interno, por un lado, expone tendencias en los nuevos riesgos posibles que van a afectar al control interno y, por otra parte, debe contribuir a mantener actualizados los conocimientos del auditor, de forma que aporte un valor añadido en el ejercicio de su profesión.

BIBLIOGRAFÍA

-Real decreto 424/2017, de 28 de abril, por el que se regula el régimen jurídico del control interno en las entidades del sector público local.

- Circular 1/2016 sobre la responsabilidad penal de las personas jurídicas de la Fiscalía General del Estado.

Escudero, Ana Díaz (2017) *Análisis del marco teórico y legal de la evolución de la responsabilidad de las personas jurídicas y las obligaciones del compliance officer*. (pág. 50).

Moreno García, Elena (2017) "¿Qué es el compliance?"diciembre 2017). http://www.autonomo.es/opinion/item/5403-que-es-el-compliance.

Crespo Barquero, P, (2016) "La reforma del Código penal operada por LO 1/2015, de 30 de marzo: responsabilidad penal de las personas jurídicas".(pág. 24).

Bleker, Sylvie and Hortensius, Dick (2014) "Iso 19600: the development of a global standard on compliance management". Business compliance 02/2014. Baltzer science publishers.

- "Ciberseguridad: una guía de supervisión" (octubre 2016). La fábrica de pensamiento instituto de auditores internos de España.

Carvajal Azcona, Javier (2017) "Definición de ciberseguridad y riesgo". https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo.

- Coso in the cyber age. The committee of sponsoring organizations of the treadway commission (2015, pág. 9).

- Diagnosis y propuestas sobre transparencia y corrupción en España. En el *25 aniversario de transparency international*. Madrid (septiembre 2018).

Lawrence, Kirk (2013) "*Developing leaders in a vuca enviroment". UNC Executive Development.*(2013, pág 3-4). *UNC Executive Development*

Bennett, Nathan and Lemoine, G. James, (2014) *What VUCA really means for you. Harvard business review.Harvard Business Review, Vol. 92, No. 1/2, 2014.*