KPMG

La cultura ética, compliance y buen gobierno corporativo

en el ámbito empresarial venezolano

Diciembre, 2022

Índice

Presentación

La globalización ha entrado en una nueva fase donde se están creando retos nunca antes vistos para el cumplimiento. Existen dos grandes tendencias que están impulsando estos cambios. En primer lugar, el creciente número de gobiernos de todo el mundo que está intensificando las regulaciones o introduciendo nuevas leyes y, por otra parte, los organismos encargados de hacer cumplir la ley y que trabajan conjuntamente para poner freno a los delitos socioeconómicos. Por lo tanto, para poder cumplir con estas leyes, las empresas internacionales deberán crear una estrategia de cumplimiento que no solo sea global, sino que tome en cuenta las diferencias nacionales en la legislación. Estos programas de cumplimiento deben contar con una evaluación de riesgo global y con procedimientos adaptados al entorno local en el que la entidad opera. Hoy, las corporaciones dependen mucho más que antes de terceros para hacer negocios en lugares lejanos y a menudo en áreas en las que existe un alto riesgo de corrupción.

Desde KPMG hemos preparado el siguiente estudio para conocer cómo el sector empresarial venezolano ve la cultura ética, *compliance* y buen gobierno corporativo dentro de sus organizaciones, a fin de tener una visión más directa del grado de madurez que tienen las empresas venezolanas en cuanto al Compliance Corporativo se refiere. Dicho estudio tuvo por objetivo despertar el interés de los encuestados en contar con un programa de *compliance* para identificar y gestionar los riesgos operativos y legales a los que se enfrentan en su actividad. Esto con el fin de establecer mecanismos de prevención, gestión, control y reacción frente a estos.

Mauro J. Velázquez G

Socio Líder
Forensic Services
KPMG en Venezuela

Introducción

En América Latina, incluida Venezuela, los escándalos relacionados con fraude, estafas, legitimación de capitales, y otros delitos financieros, se repiten con frecuencia. Por lo que el sector privado ha integrado en sus organizaciones el *compliance* y buen gobierno corporativo, lo que se ha traducido en un factor clave en el desarrollo de sus organizaciones y equipos de trabajo.

El *compliance* invita a las empresas a establecer procesos internos para prevenir delitos, sirviendo como un escudo protector para las empresas ante la posibilidad de ser objeto de sanciones.

El objetivo del *compliance* es la prevención de casos relacionados con corrupción, fraude, legitimación de capitales y demás delitos conexos, mediante una serie de mecanismos que forjan un buen gobierno corporativo y una cultura ética que fortalece los controles internos de la entidad.

Así mismo, se entiende por cultura ética al desarrollo de políticas, procesos y mecanismos seguros y confidenciales como componente clave para forjar instituciones sólidas en el sector empresarial que aportan a los Objetivos de Desarrollo Sostenible (los ODS) de la Agenda 2030 de las Naciones Unidas. Un ejemplo de esto son los canales de denuncia en materia de discriminación, acoso laboral, violencia de género, entre otros, enmarcados en los ODS número 1, 5 y 16: Fin de la Pobreza, Igualdad de Género y Paz, y Justicia e Instituciones Sólidas, respectivamente.

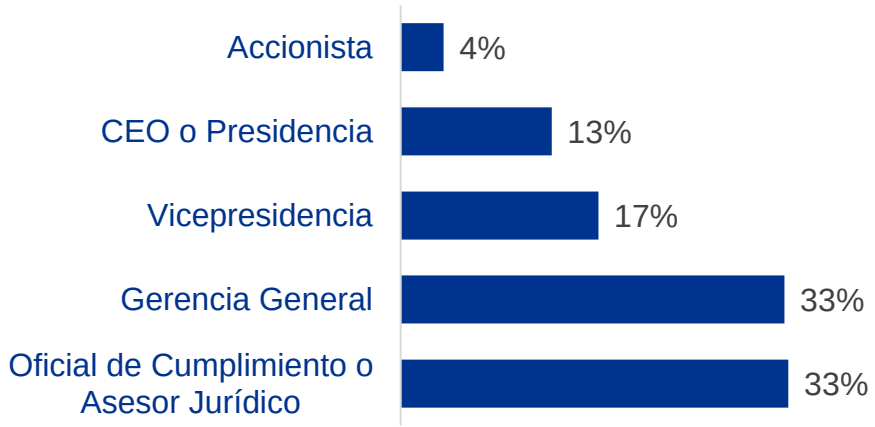
Siendo este un tema tan relevante, desde KPMG elaboramos un estudio para reflejar la visión que tienen las empresas venezolanas con respecto a cultura ética, *compliance* y buen gobierno corporativo.

Agradecemos la participación de representantes de diversas industrias de Venezuela e invitamos a la comunidad empresarial del país a considerar estos resultados para el óptimo desarrollo de sus negocios en materia de cultura ética, *compliance* y buen gobierno corporativo.

Resumen Ejecutivo

Nuestra encuesta de cultura ética, compliance y buen corporativo, gobierno realizado entre los meses de octubre y diciembre de 2022, tuvo como finalidad conocer la visión que tienen los empresarios venezolanos sobre estos tres tópicos, así como despertar el interés de los encuestados sobre estos temas a fin de concientizar sobre los riesgos operativos y legales a los que se enfrentan las entidades venezolanas en su actividad.

Las preguntas utilizadas en el cuestionario permitieron indagar sobre la experiencia de fraudes sufridos por las empresas que operan en Venezuela, así como sus percepciones de riesgo de fraudes futuros. La encuesta fue contestada por:



Para realizar este estudio, el concepto de fraude se definió como “un acto deliberado de abuso de confianza que, aprovechándose de engaños, se realiza para obtener un beneficio sin consentimiento de la empresa afectada”.

Durante los últimos años hemos visto como las empresas suelen poner mayor atención a los riesgos que se perciben fuera de la organización, dejando de ver que el enemigo en ocasiones también puede estar adentro. La experiencia nos indica que, en épocas de crisis, las condiciones para que la “tormenta perfecta” de fraudes suceda son mucho más latentes. Esto es así porque las personas tienen mayores presiones para obtener ingresos adicionales o mostrar mejores resultados de los que realmente se han logrado, y la racionalización de ciertas conductas para justificar actividades ilegales suele ser más frecuente. Si estas situaciones se combinan además con una deficiente capacidad de control por parte de las empresas, no es difícil deducir que las oportunidades para que los empleados cometan algún tipo de fraude se incrementen.

La muestra está distribuida de manera casi uniforme en las siguientes industrias:

- Servicios profesionales
- Energía y recursos naturales
- Farmacia
- Banca y otros servicios financieros
- Telecomunicaciones, medios y tecnología
- Industria y Manufactura

Análisis de resultados

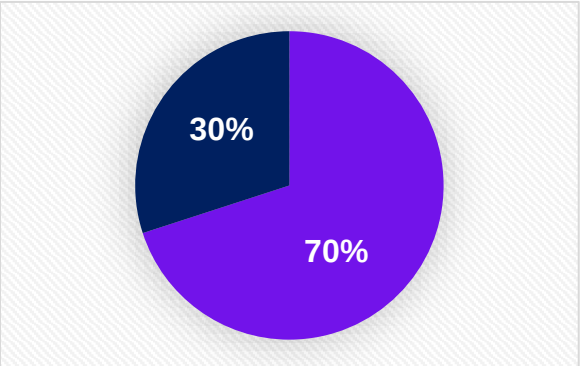
Perfil de los encuestados

El tema de *compliance* corporativo ha tomado relevancia en los últimos años, es por esto que desde KPMG elaboramos esta encuesta, para conocer la perspectiva del mercado venezolano sobre este tema; para esto, se tomó en consideración un grupo de empresas de diversos sectores económicos.

Del universo de encuestados, las entidades de Banca y otros servicios financieros, Energía y recursos naturales, Farmacia, Industria y manufactura, Telecomunicaciones, medios y tecnología, Servicios profesionales y Seguros, fueron los que tuvieron mayor participación.

En el estudio realizado, el 70% de los encuestados afirmaron que las empresas donde trabajan tiene regulaciones especiales por su actividad económica y 30% afirmó que no poseen regulaciones.

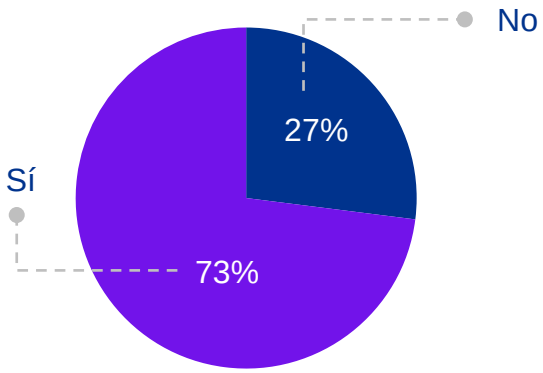
¿La entidad por su actividad económica u otro factor está sujeta o expuesta a regulaciones?



Durante la encuesta, pudimos conocer que 44% de los consultados indicó que su programa de PLC/FT/FPADM y otros ilícitos ha sido sujeto a evaluación (por la autoridad, por auditor interno o por un externo independiente) en los últimos 12 meses.

Además, el 14% de los encuestados afirman haber sufrido pérdidas derivadas de multas regulatorias o fallas en el cumplimiento.

¿El área de cumplimiento posee plena autonomía e independencia para la ejecución de sus funciones?



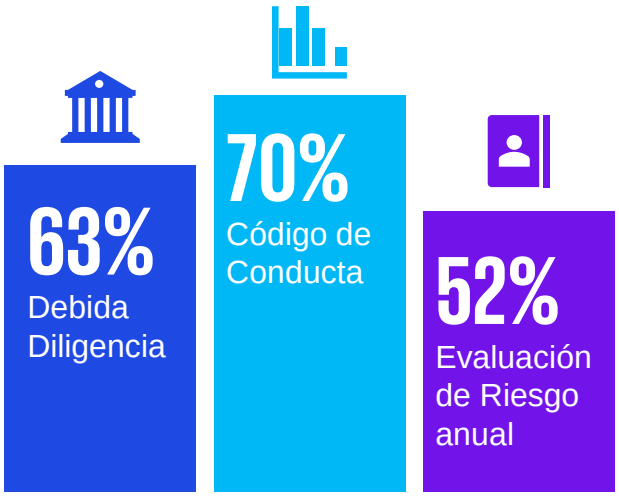
Frente a las nuevas regulaciones, el desconocimiento de estas en un determinado sector económico pudiera ser perjudicial para una empresa. De igual forma, no proporcionar una autonomía total a las áreas de cumplimiento pudiera traducirse en riesgo operativo, derivando en consecuencias como pérdidas financieras en las empresas.

Análisis de resultados

Prevención, detección y respuesta ante potenciales casos de fraude

Dentro de un buen gobierno corporativo, el control interno es una pieza clave. Aún más para la prevención de conductas irregulares dentro de la organización. Trabajar en la prevención, detección y respuesta al fraude y otros ilícitos evita pérdidas económicas significativas, siendo esto una inversión que contribuye a mitigar el riesgo de que se produzcan situaciones irregulares.

De acuerdo con los resultados obtenidos, los tres elementos más utilizados para conformar un programa integral de prevención, detección y respuesta ante potenciales casos de fraude son:



El 85,19% de los encuestados afirma que su entidad puede ser víctima de algún fraude; aunque 72,22% opine que la empresa no ha sido víctima de ninguno.

Al consultar a nuestros encuestados sobre los mecanismos con los que cuentan dentro de su organización para la prevención, detección y respuesta ante potenciales casos de fraude, respondieron lo siguiente:

Mecanismo	%
Código de conducta	70.37%
Debida diligencia de proveedores y empleados	62.96%
Evaluaciones de riesgo anuales	51.85%
Entrenamiento en temas de ética	46.30%
Políticas antifraude	42.59%
Monitoreo de datos a tiempo real	37.04%
Líneas de denuncia	35.19%
Controles antifraude en todos los procesos de la empresa	31.48%
Matrices de fraude	24.07%

Análisis de resultados

Línea de Denuncia anónima, una defensa contra los actos irregulares

En la experiencia de KPMG, para que una línea de denuncia anónima pueda ser realmente efectiva no basta con habilitar un número telefónico o un correo electrónico para recibir las denuncias. Es necesario implementar un programa integral que cubra cuando menos los siguientes aspectos:

• **Comunicación y difusión de la disponibilidad de una línea de denuncia.** Es necesario que el lanzamiento de una línea de denuncia esté acompañado de un programa que sensibilice y comunique tanto el propósito como los mecanismos implantados para realizar denuncias. Esta comunicación además deberá ser reforzada periódicamente, de tal forma que la gente siempre tenga presente esta opción de interlocución con la empresa.

• **Protocolos de seguimiento e investigación.** Es indispensable que la empresa cuente con un protocolo claro sobre los procedimientos a seguir y los responsables de atender todas las denuncias recibidas por medio de la línea de denuncia.

• **Garantía de no represalias.** Es imperativo que la compañía adopte las medidas necesarias para que las denuncias recibidas mediante este mecanismo no resulten en represalias en contra de las personas que han utilizado la línea de denuncia. De lo contrario, se puede generar un ambiente adverso dentro de la organización, generando actitudes de simulación y cinismo.

• **Comunicación directa con los más altos niveles de gobierno de la empresa.** Es necesario que las denuncias realizadas se reporten de manera directa a los más altos órganos de gobierno de la empresa, como puede ser el Comité de Auditoría o la Junta de Gobierno, de tal forma que pueda establecerse un contacto directo con los tomadores de decisiones y evitar así que ciertas denuncias sean bloqueadas por altos directivos, que pueden estar involucrados en los hechos denunciados o que están tratando de encubrir a las personas reportadas.

> **“Una línea de denuncia o Línea Ética es esencial para ganarse la confianza de los empleados y captar aquellas anomalías y violaciones a las políticas internas de la empresa, que de otra forma quizá no se comunicarían”.**

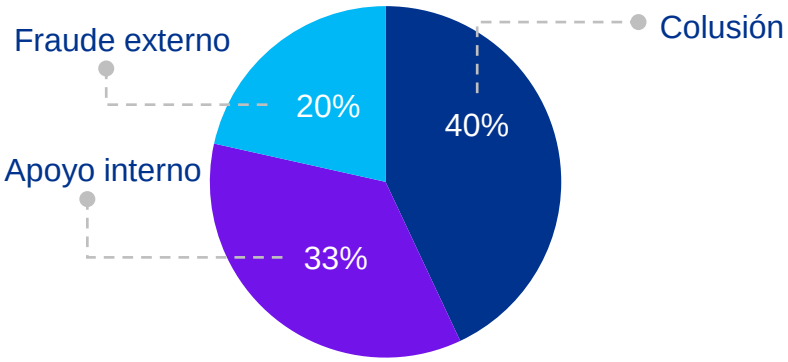
Análisis de resultados

Prevención, detección y respuesta ante potenciales casos de fraude

Al preguntar a los encuestados si creían que su organización podía ser víctima de algún fraude, 86% de los encuestados respondieron que sí. En general, el nivel de posible incidencia de fraude es altamente grave; y se pueden observar hallazgos significativos en las empresas venezolanas en términos del tipo de fraude cometido.

No obstante, al consultar si la organización fue víctima de algún fraude, solo 28% de los encuestados respondieron que sí.

Al preguntar bajo qué modalidad ocurrió el fraude, 40% contestó que fue por colusión y 33% contestó que fue realizado con apoyo interno.

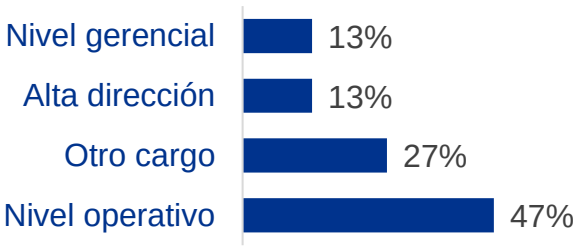


El fraude interno es aquel que comete un empleado de la propia organización, sea de manera solitaria o en colusión; en su minoría significativa, los fraudes cometidos al 28% del universo de encuestados fueron realizados con apoyo interno. Por el contrario, el fraude externo es el que realiza una persona ajena a la organización, como puede ser un proveedor o un cliente. Con base en esta clasificación, solo una población de 20% indica que el fraude cometido a su entidad fue netamente externo.

El perfil del defraudador

La encuesta reveló algunas características interesantes en cuanto al perpetrador de los ilícitos cometidos. De esta forma, el defraudador actuó en complicidad con personas externas a la organización en el 73% de los casos. Es decir, siendo un miembro interno de la entidad, el defraudador actuó en conjunto con un tercero.

En relación con el cargo que ocupaba el defraudador al momento, los encuestados contestaron lo siguiente:



La prevención es la forma de reducir el riesgo de ocurrencia de fraudes y conductas impropias. Los fraudes tienen efectos secundarios, especialmente en la moral de los trabajadores.

Análisis de resultados

Algunas prácticas fraudulentas comunes

En la experiencia de KPMG los fraudes en estados financieros se relacionan con múltiples formas de manipular y falsear la información financiera o contable. Algunas de las prácticas fraudulentas más comunes en este sentido son las siguientes:

• **Registro de ingresos ficticios** para sobredimensionar el comportamiento real de la compañía y de esta manera tener, por ejemplo, una mejor posición a la hora de negociar una posible venta de la compañía.

• **Registrar como venta un desplazamiento** de mercancía de un almacén a otro o no registrar devoluciones de inventario, de tal forma que se mantengan un nivel de ventas alto y con ello obtener bonos asociados a "productividad" de los altos ejecutivos.

• **Reconocer como ingresos presentes perspectivas de ingresos futuros** (por ejemplo, aquellos derivados de contratos a largo plazo o beneficios obtenidos de instrumentos financieros), para reflejar una liquidez a corto plazo que asegure un préstamo bancario más generoso.

• **Registrar como un gasto futuro** un pasivo presente, de tal forma que las cuentas de resultados muestren mayores rendimientos y también menores pasivos y de esta manera alterar los ratios de las razones financieras presentadas a los accionistas de la empresa.

• **Registrar la depreciación de un activo** en un plazo de tiempo mayor a la de su vida útil estimada, de tal forma que el valor de los activos mostrados en libros no corresponda con la realidad.

• **Registrar de manera imprecisa** o incluso no registrar una contingencia derivada, por ejemplo, de un litigio legal que se estima se va a perder y, no obstante, no reconocerla para no afectar los deberes de hacer y no hacer ("covenants") con los bancos acreedores.

• **Registrar como arrendamiento** puro cierta maquinaria en lugar de arrendamiento financiero, para reducir así la deuda en estados financieros y reflejar una mejor posición financiera.

Para mitigar riesgos relacionados con los diversos tipos de crímenes financieros, resulta indispensable prevenir, detectar y responder de manera oportuna ante la materialización de todo tipo de conductas inapropiadas, que pueden incrementar la exposición al riesgo".

Análisis de resultados

Políticas de Discriminación, Acoso Laboral y Violencia de Género

Todas las entidades tienen una cuota de responsabilidad social con el desarrollo y mejora de las condiciones profesionales para la igualdad de género y la reducción de las desigualdades, tanto para aportar al cumplimiento de los ODS como para promover una de cultura ética, *compliance* y buen gobierno corporativo dentro de sus equipos de trabajo. Esta fue la razón por la cual queríamos conocer si empresas venezolanas cuentan con políticas, procesos y mecanismos seguros y confidenciales que aborden los temas de discriminación, acoso laboral y violencia de género.

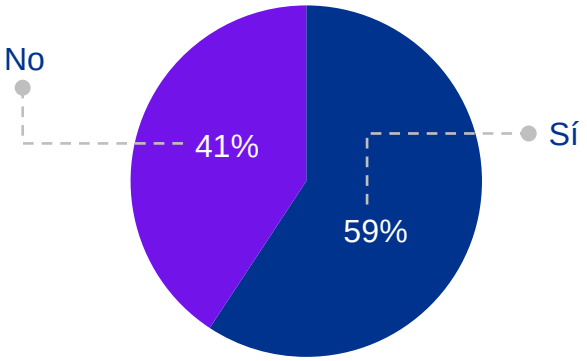
Del total de encuestados, 59% afirma que en las empresas que representan cuentan con políticas y procesos enmarcados en temas de discriminación, acoso laboral y violencia de género.

Aunque más de la mitad de los encuestados aseguran contar con estas políticas, solo 54% afirma contar con mecanismos seguros y confiables que aborden los temas previamente mencionados.

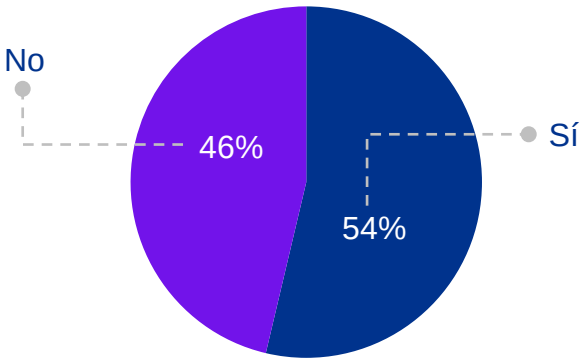
Observando estos números podemos apreciar que, aunque puedan existir políticas, procesos y mecanismos que aborden la discriminación, el acoso laboral y la violencia de género en el entorno empresarial; estos no transmiten completa seguridad y confidencialidad a sus empleados.

El compromiso con la construcción de entornos empresariales incluyentes, diversos e igualitarios, están alineados con la generación de igualdad de oportunidades y la promoción de valores, como la equidad, en una estrategia de inclusión y diversidad. Abrazar la inclusión, la diversidad y la equidad abre paso a una amplia gama de oportunidades de coexistencia, forjando experiencias únicas y enriqueciendo los lazos que nos unen.

¿Dentro de su empresa se contemplan políticas y procesos que aborden los temas de discriminación, acoso laboral y violencia de género?



¿Existen en su empresa mecanismos seguros y confidenciales para abordar los temas de discriminación, acoso laboral y violencia de género?



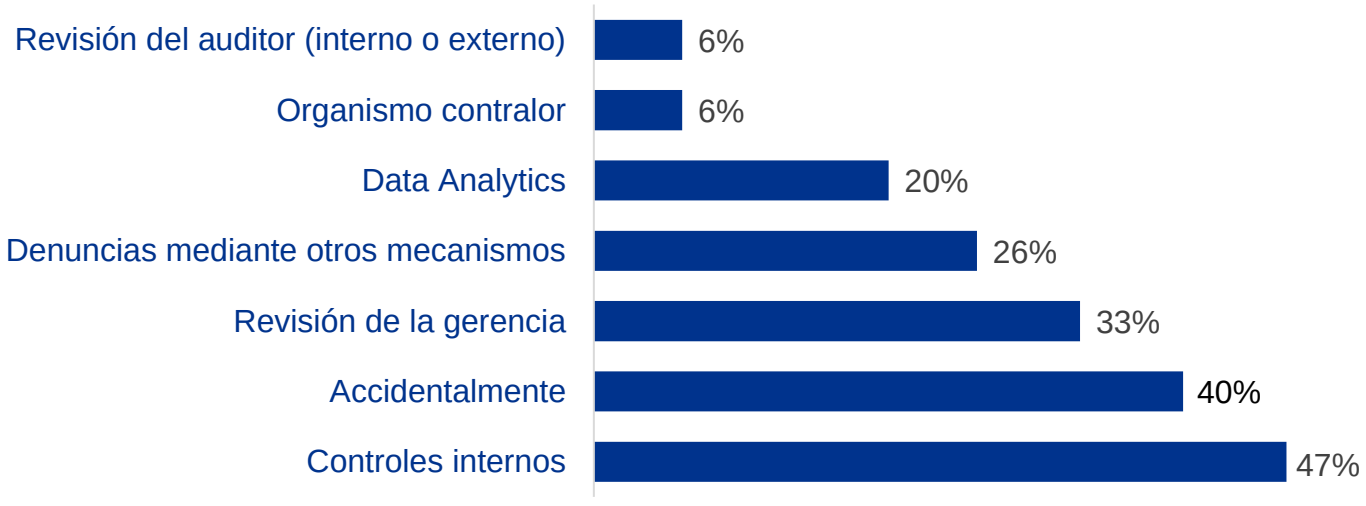
Análisis de resultados

Tipos de riesgos que se han materializado en su compañía

El fraude, como cualquier otro tipo de delito económico, suele tener múltiples causas. Ahora bien, la situación económica agudizó ciertos factores, como el debilitamiento de los controles internos y el aletargamiento de la infraestructura ética de las compañías. Del universo de encuestados, la población que afirmó haber sufrido alguna situación irregular indicó que fueron detectadas en sus organizaciones las siguientes tipologías de fraude:

Malversación de efectivo	27%
Sobre precios en los gastos	27%
Conflicto de interés	20%
Malversación (robo) de activos (como inventarios, etc.)	14%
Compras para uso personal	14%

Al preguntar a los encuestados cómo se detectaron los fraudes dentro de sus organizaciones, indicaron varias alternativas. Se destaca la Línea de Denuncia, ya que ésta representa un mecanismo que genera múltiples beneficios para las organizaciones por ser una herramienta segura y anónima. Entre otros mecanismos de detección, se incluyen los siguientes:



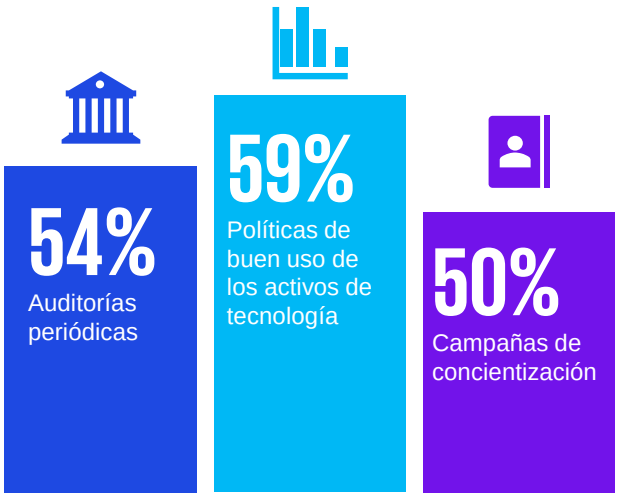
50% de los encuestados manifestó que a raíz de la situación irregular detectada se despidió al personal sin acción penal y 50% manifestó que, adicionalmente a esto, se implementaron nuevos controles para prevenir la ocurrencia de estas conductas. Solo 10% afirma haber iniciado acciones legales para la recuperación de los montos defraudados.

Análisis de resultados

Lineamientos y políticas en materia de ciberseguridad

La seguridad cibernética representa un escudo de protección que va más allá de la tecnología de la información. Una sólida estrategia cibernética permite resguardar uno de nuestros activos más valiosos en el mundo empresarial: los datos. El hecho de implementar estrategias en torno a la seguridad digital de forma efectiva puede traducirse en una mejora de la reputación de la marca, el cumplimiento normativo, las operaciones, la confianza del equipo de trabajo y más.

De acuerdo con los resultados obtenidos, los tres elementos más utilizados entre los lineamientos y políticas en materia de ciberseguridad son:



Solo 7,41% de los encuestados afirma que su empresa tiene Políticas de BYOD (*bring your own device*), al igual que solo 24,07% contempla Políticas de Desarrollo seguro de Software.

Al examinar la diversidad de elementos que los resultados arrojaron en relación con los componentes de los lineamientos y políticas en materia de ciberseguridad, se presentan los elementos utilizados frecuentemente:

Elemento	%
Políticas de buen uso de los activos de tecnología	59.26%
Auditorías periódicas	53.70%
Campañas de concientización	50.00%
Políticas para el manejo de dispositivos IoT (internet of things)	35.19%
Procedimientos de respuesta a incidentes de seguridad	35.19%
Pruebas de penetración a los sistemas de información	35.19%
Asignación de un responsable de la ciberseguridad (p. ej. un CISO)	33.33%
Políticas de desarrollo seguro de software	24.07%
Políticas de BYOD (bring your own device)	7.41%

Análisis de resultados

Lineamientos y políticas en materia de ciberseguridad

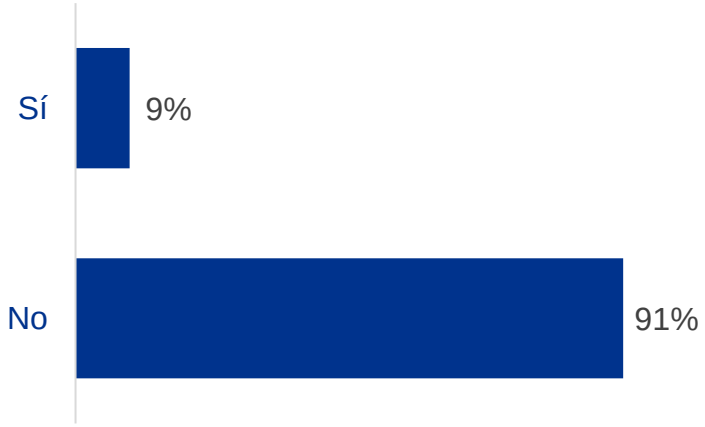
Para el óptimo funcionamiento de un sistema en materia de seguridad digital, se requieren controles operativos que aseguren su correcta gestión y desarrollo. Estos son los resultados obtenidos tras consultar al universo de encuestados la siguiente pregunta:

¿Qué clase de controles utiliza la organización?

Control	%
Antivirus	88.89%
Firewalls internos / externos	70.37%
Redes privadas virtuales (VPN)	59.26%
Monitoreo proactivo de amenazas	46.30%
Sistemas de detección / Prevención de intrusos	42.59%
Mecanismos para prevenir la pérdida de información	37.04%
Cifrado de información (p. ej. en bases de datos / discos duros)	29.63%
Software de gestión de dispositivos móviles	24.07%
Hardening de componentes tecnológicos (servidores, computadoras redes inalambricas, etc)	14.81%

Considerando el uso de uno o más de los controles previamente mencionados por parte de las entidades que los encuestados representan, se les plantea la siguiente pregunta:

En los últimos 12 meses, ¿su empresa fue víctima de un incidente de ciberseguridad?

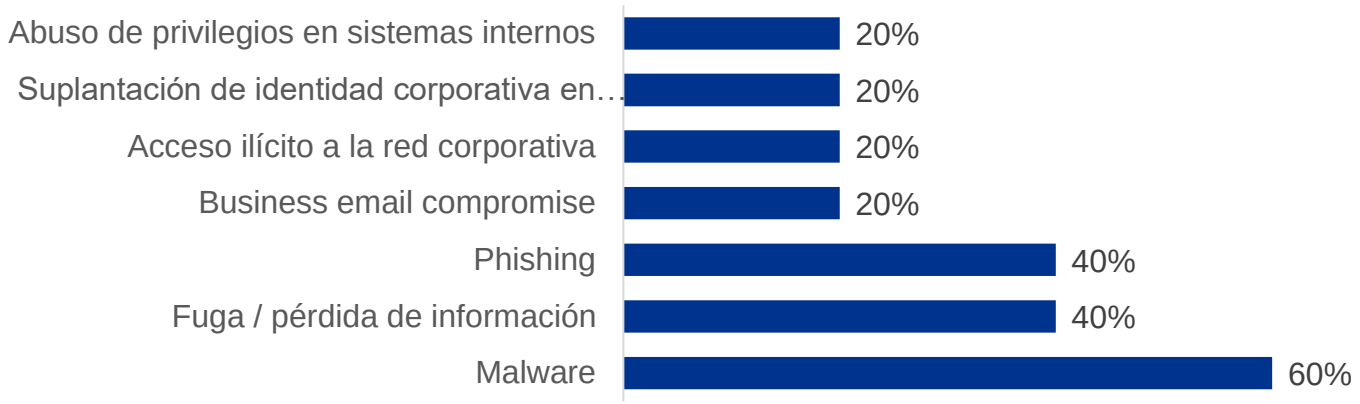


Del universo de encuestados, una población que representa 9,26% afirma haber sufrido incidentes en materia de ciberseguridad. Siendo el *malware* el más frecuente con 60% entre los resultados obtenidos.

Análisis de resultados

Lineamientos y políticas en materia de ciberseguridad

Existen diversos tipos de incidentes que pueden significar un riesgo significativo en materia tecnológica e informática para las empresas que no poseen los controles correspondientes y alineados a sus lineamientos y políticas en materia de seguridad digital. Del universo de encuestados, una población de 9,26% afirmó los siguientes resultados, desglosando los tipos de incidentes sufridos en los últimos 12 meses.



En relación con la pregunta anterior, también se les consultó:
¿Cuál era el origen del incidente?

No fue identificado	40%
Grupos "hacktivistas"	40%
Crimen organizado	20%

Adicionalmente, actuar a tiempo y responder oportunamente son factores fundamentales para mitigar posibles riesgos y detener el ataque de manera segura y eficaz. Por lo cual, se comparten los resultados en respuesta a la siguiente pregunta:

¿Cuánto tiempo le tomó identificar el incidente?

Un día	60%
Una semana	20%
Más de seis meses	20%

Identificar el incidente es el primer paso para dar una respuesta oportuna, en un 60% esta etapa tomó un día.

Además, una respuesta oportuna, eficaz y estratégica al incidente ayuda a mitigar su impacto y prevenir futuros riesgos.

¿Cómo respondió al incidente?

Investigación interna	40%
Investigaciones internas y externas	40%
El incidente no fue atendido	20%

Pese a que la denuncia es un mecanismo efectivo para la detección de fraudes, las entidades no suelen visualizar esta herramienta como parte de su arsenal de detección. En nuestra experiencia, un mecanismo de recepción de denuncias operado internamente suele ser menos efectivo, ya que no garantiza el anonimato, a diferencia de un servicio externo.

Análisis de resultados

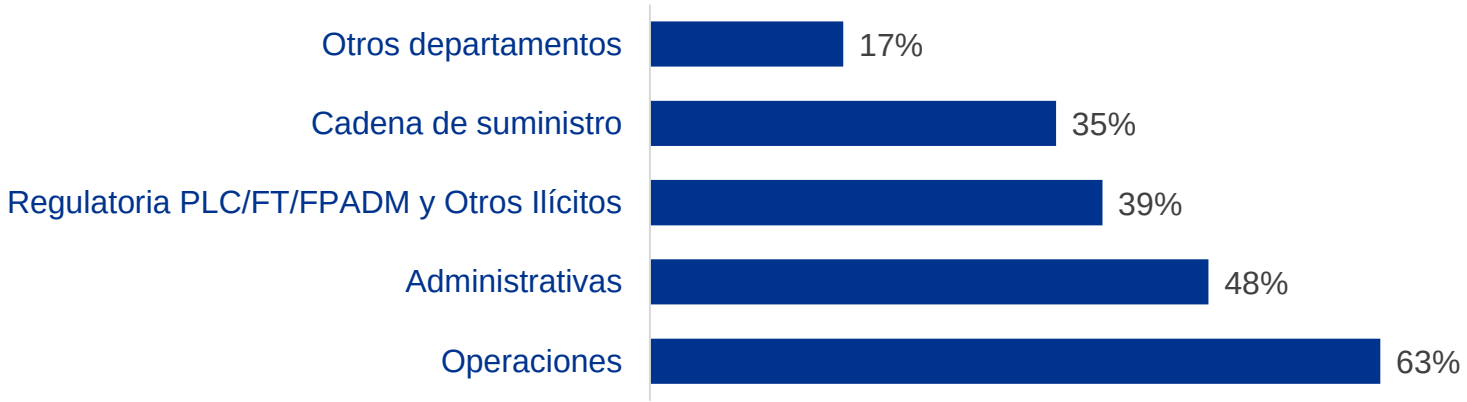
Soluciones *blockchain* en materia de ciberseguridad

Los criptoactivos y las tecnologías afines a ellos han significado una evolución constante tanto en su adopción como en los casos y la capacidad de uso. El auge y desarrollo de la industria de las criptomonedas está generando un impacto en las estrategias financieras del entorno empresarial y, sin un soporte regulatorio enfocado en cumplimiento normativo, ética y transparencia, la entidad podría ser susceptible a incidentes que signifiquen un riesgo.

A medida que avanza la denominada criptoeconomía, esta ha llamado la atención de las instituciones financieras y no financieras, que han mostrado públicamente su compromiso con los activos digitales. En los últimos dos años, las institucionales financieras a nivel global han comenzado a adoptar criptomonedas en diferentes grados. Adicionalmente, la evolución de las regulaciones a nivel global permitirá definir un tablero de juego sobre el que construir nuevos productos y servicios. La tecnología *blockchain* surge como una herramienta para generar soluciones que respondan a la prevención y mitigación de riesgos, fortaleciendo diversas áreas operativas para su desarrollo óptimo e innovador en materia digital.

Por esta razón, se consultó a los encuestados:

¿Desarrollaría soluciones *blockchain* para mejorar alguna de estas áreas?



Las soluciones *blockchain* surgen como una estrategia confiable para el manejo, validación y almacenamiento de información, siendo una respuesta eficiente y automatizando procesos en las operaciones".

Conclusiones

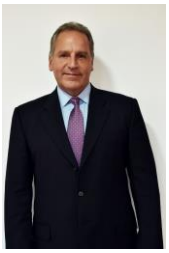
Al diseñar este estudio, la intención era conocer el grado de madurez que tienen las empresas venezolanas en cuanto a cultura ética, *compliance* y buen gobierno corporativo se refiere. El estudio tuvo por objetivo despertar el interés de los encuestados en contar con una cultura ética, *compliance* y buen gobierno corporativo para identificar y gestionar los riesgos operativos y legales a los que se enfrentan en su actividad. Esto con el fin de establecer mecanismos de prevención, gestión, control y reacción frente a los mismos. Concluimos que actualmente en Venezuela la cultura ética, *compliance* y buen gobierno corporativo no ha evolucionado. Aun mucha empresa no se han dedicado a diseñar e implementar programas de vigilancia y cumplimiento normativo, más allá de las exigidas por el tipo de actividad a la que se dedican.

Las políticas de *compliance*, o de prevención de riesgos legales, son una práctica que poco a poco debe desarrollarse con mayor frecuencia en las empresas para detectar, mitigar y prevenir riesgos.

En conclusión, la crisis económica mundial ha potenciado los riesgos que enfrentan las compañías y ha puesto en evidencia las principales debilidades de control de las empresas. Una estrategia de administración de riesgos de fraude que sea efectiva y orientada a la empresa abarcará actividades, mecanismos y controles que tengan tres objetivos: prevención, detección y respuesta.

> **Las políticas de *compliance* son la forma en que las empresas cumplen con la sociedad, ya que ésta acaba expulsando a las compañías que no tienen un marco regulatorio y de cumplimiento normativo".**

Contactos



Mauro Velázquez

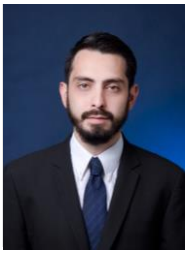
Socio Líder
Forensic Services

E: mjvelazquez@kpmg.com

Yanelly Márquez

Socia Líder
Governance, Risk and Compliance services

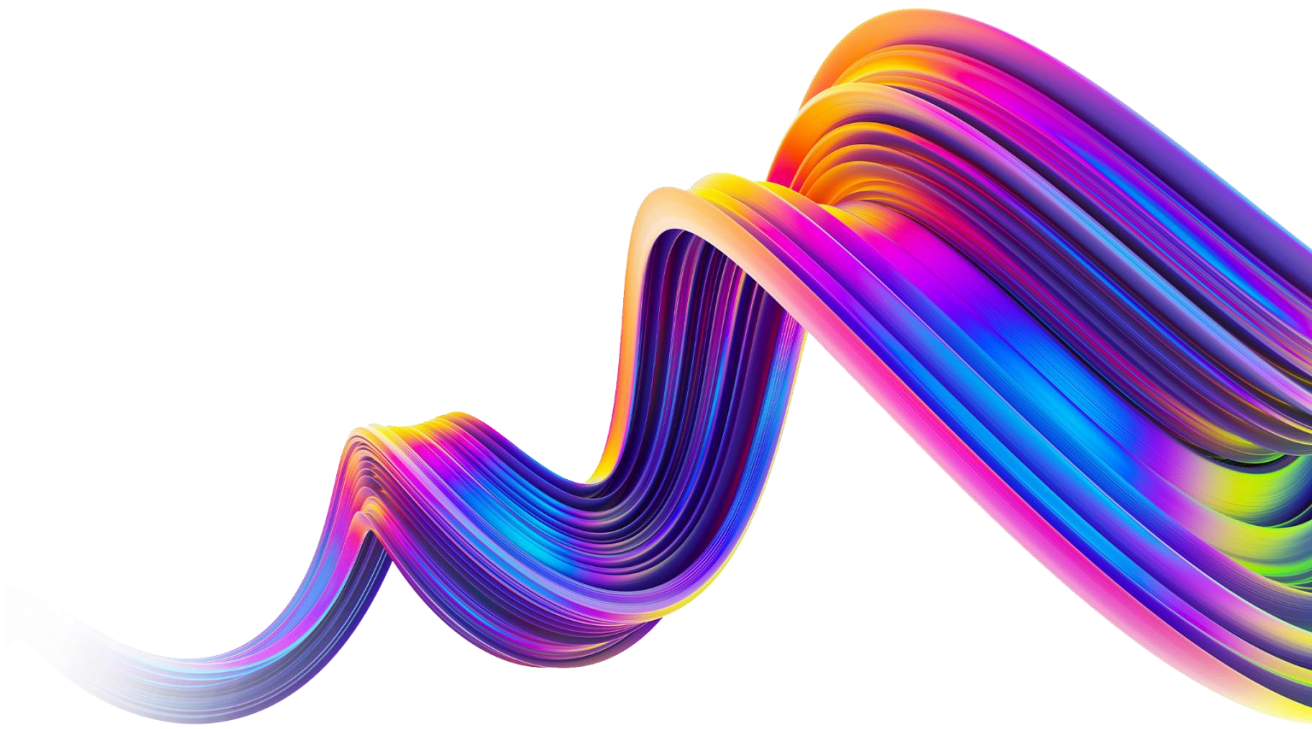
E: ymarquez@kpmg.com



Alfredo Sthory

Gerente Senior
Forensic Services

E: asthory@kpmg.com



Acceda a la oferta de servicios de KPMG en Venezuela.

Encontrará, entre otros elementos, las situaciones que las empresas viven con mayor frecuencia y de qué forma podemos apoyarles.

brochure.kpmg.com.ve/

Algunos de los servicios descritos en el presente pueden no ser permisibles para clientes actuales de KPMG en Auditoría y sus afiliados o entidades relacionadas.