



Universidad Autónoma de San Luis Potosí
Facultad de Ingeniería
Centro de Investigación y Estudios de Posgrado

**Controles internos de Tecnologías de la Información, un
estudio sobre la prevención del fraude en empresas mexicanas**

T E S I S

Que para obtener el grado de:

Maestría en Planeación Estratégica e Innovación

Presenta:

Vianney Verónica Hernández Agundis

Asesor:

Dr. Jorge Edgardo Borjas García

San Luis Potosí, S. L. P.

Junio de 2019



ÍNDICE DE CONTENIDO

INTRODUCCIÓN	5
Antecedentes	6
Planteamiento del problema	8
Justificación del estudio	10
Objetivo general.....	13
Objetivos específicos	13
Supuestos de investigación	13
Alcance	14
Limitaciones	14
1. ANTECEDENTES DE LOS CONTROLES INTERNOS	15
1.1 Marco referencial	15
1.1.1 Comienzos del Control interno	15
1.1.2 Definición de conceptos	16
1.1.3 Antecedentes de la Ley Sarbanes Oxley y su apartado 404.....	17
1.1.4 Controles internos para los Sistemas de Información	20
2. LA FALTA DE UN EQUIVALENTE AL APARTADO 404 DE LA LEY SARBANES OXLEY EN MÉXICO EN RELACIÓN A LAS TECNOLOGÍAS DE LA INFORMACIÓN QUE IMPIDA LOS FRAUDES FINANCIEROS	27
2.1 Marco contextual.....	27
2.1.1 Incremento de incidentes de fraude en México.....	27
2.1.2 Regulaciones en otros países	34
2.1.3 Toma de perspectiva.....	36
3. METODOLOGIA DE OBTENCIÓN DE INFORMACIÓN PARA LA ELABORACIÓN DEL ESTUDIO	40

3.1 Enfoque.....	40
3.2 Muestreo	41
3.3 Técnica para recopilar información	42
3.4 Técnicas para analizar la información.....	42
3.4.1 Análisis de contenido	42
3.4.2 Hermenéutica.....	43
3.5 Etapas de la metodología	44
3.6 Análisis de datos	46
3.6.1 Alineación de la Ley SOX y el marco COSO	46
3.6.2 Los principios del marco de referencia COSO	47
3.6.3 Los principios del apartado 404 de la Ley SOX	55
3.6.4 Relación COSO – apartado 404 de la Ley SOX	59
4. ANÁLISIS Y DISCUSIÓN DE RESULTADOS	61
4.1 Resultados	61
4.2 Análisis de resultados	65
4.3 Aplicación a una empresa en México.....	73
4.4 Recomendaciones futuras	78
CONCLUSIONES	80
REFERENCIAS	83
ANEXOS.....	87
Anexo 1: Resumen ejecutivo del reporte COSO 2013.....	87
Anexo 2: Indicador mensual de la actividad industrial, cifras desestacionalizadas, al cierre del año 2017 de acuerdo al INEGI.....	103
Anexo 3: Clasificación de los Sectores industriales de acuerdo a los registros del INEGI para el año 2017.	104

Anexo 4: Boleta de evaluación de fraude para México del Informe Anual de Fraude Global de Kroll 2014/2015.....	105
Anexo 5: Boleta de evaluación de fraude para México del Informe Anual de Fraude Global de Kroll 2015/2016.....	106
Anexo 6: Multas por Tipo de Régimen (fraude) de acuerdo al Reporte Anual de Fraude y Abuso Organizacional de la Asociación de Examinadores de Fraude Certificados 2016.	107
Anexo 7: Glosario.	108

ÍNDICE DE FIGURAS Y TABLAS

Figura 1. Ejemplo de control interno automatizado	22
Figura 2. Vulnerabilidad identificada en el control interno automatizado	23
Figura 3. Objetivos de control interno para prevenir deficiencias	24
Figura 4. Incidentes de fraude en México en el año 2015	28
Figura 5. Porcentaje de fraude ocasionado por proveedores en 2015	29
Figura 6. Latinoamérica y el Caribe	38
Figura 7. Ciclo hermenéutico.....	43
Tabla 1. Cuadro metodológico.....	44
Figura 8. Etapas de la metodología	46
Figura 9. Principios COSO	48
Figura 10. Entorno de control	49
Figura 11. Evaluación de riesgos	51
Figura 12. Actividades de control	52
Figura 13. Sistemas de información	53
Figura 14. Monitoreo del sistema de control.....	54
Figura 15. Principios del apartado 404 de la Ley SOX	56
Figura 16. Evaluación formal de control interno	57
Figura 17. Confluencia SOX-COSO	59
Figura 18. Relación entre fraudes más comunes en México y áreas clave para empresas mexicanas.	62
Tabla 2. Controles internos de TI en áreas clave para empresas mexicanas	63
Figura 19. Relación entre fraudes más comunes en México, áreas clave y estrategias de control propuestas.	72
Figura 20. Proceso general de una empresa en México que sigue SOX y COSO	75
Figura 21. Comparación del acceso físico restringido en una empresa en México	77
Figura 22. Comparación del monitoreo de conflictos en una empresa en México.....	78

INTRODUCCIÓN

Constantemente acontecen cambios tecnológicos que conllevan a más cambios, por ejemplo, los negocios y la complejidad de sus operaciones, o las redes informáticas que traen consigo la creación de nuevas formas y canales de comunicación (Castells, 1996). Vivimos una “sociedad de la información”.

Como afirma Garduño (2004), las investigaciones referentes a este concepto deben enfocarse al contexto presente del país para que cubra aspectos tanto como políticos como sociales, económicos o culturales y de esta forma se pueda comprender totalmente el concepto. Igualmente, el país debe enfrentarlo a través de cambios que puedan resultar de aportaciones metodológicas y teóricas, cimentadas en información y tecnología.

Por tal motivo, el presente trabajo tiene como objetivo proponer una serie de estrategias de controles internos empresariales utilizables en el área de Tecnologías de la Información, adaptados a empresas mexicanas del sector industrial, para reducir las posibilidades de fraude.

Para lograr dicho objetivo, se plantea la problemática de no tener en México un equivalente a la Ley Sarbanes Oxley en el ámbito referente a las tecnologías de información. Se esboza un breve esclarecimiento acerca del surgimiento de esta ley (SOX) e igualmente se realiza una revisión de incidentes de fraude en México en años recientes, se incluye una breve recopilación de regulaciones en otros países, seguido por el establecimiento de los supuestos de investigación y continuando con la metodología utilizada a lo largo de este trabajo. Por último, se alude a los resultados para finalizar con un análisis de los mismos, recomendaciones futuras, conclusiones, anexos y bibliografía utilizada.

Antecedentes

Conforme se dieron los primeros asentamientos de hombres dando origen a pueblos y, posteriormente a ciudades, surgió la necesidad de intercambiar productos para abastecerse. Los hombres estaban dispuestos a cambiar todos aquellos sobrantes después de haber consumido lo que requerían y fue así como nació el trueque.

Muchos años después, se crean zonas de intercambio (que dieron origen al término mercado) y aparece lo que en términos económicos conocemos como moneda, a esto se le suman los conceptos de crédito y transacción. En un momento dado, nace también la necesidad de registrar las transacciones ya que el trueque se convirtió en lo que ahora conocemos como comercio, donde existen tanto la oferta como la demanda.

Sin embargo, fue hasta el siglo XVI cuando un monje franciscano de nombre Fray Luca Paccioli contribuyó a la sistematización del principio de partida doble, base de lo que ahora conocemos como contabilidad (Granados et al., 2010). La evolución de la contabilidad continúa a finales de los siglos XIX y XX, permaneciendo en ambos siglos un proceso de adecuación para las organizaciones y sus necesidades respecto a la información financiera.

México, cuenta a su vez con hechos históricos particulares de la contabilidad, por mencionar uno: los aztecas llevaban a cabo un control de sus transacciones mercantiles (Romero, 2006).

La información financiera, mencionada anteriormente, se entiende como un medio de las empresas para comunicar información que sea de utilidad a sus usuarios para que éstos puedan tomar decisiones. Si bien las necesidades que pudieran tener los usuarios en la actualidad no son iguales a las tuvieron en el pasado ni serán las mismas en el

futuro, siempre van a existir usuarios que hagan uso de la información, como lo son los inversionistas, empleados, prestamistas, proveedores, y clientes.

Dadas las diferencias entre empresas, incluso cuando se realicen el mismo tipo de actividades o tengan tamaño similar, sus necesidades difieren, por lo cual, cada empresa requiere un sistema adecuado para su contabilidad y sus finanzas (Romero, 2006).

Además, con la finalidad de proporcionar cierta seguridad sobre el logro de objetivos de una organización, existe un proceso que las mismas organizaciones llevan a cabo, llamado control interno. Este proceso, cubre cuatro objetivos fundamentales, los cuales son contar con eficiencia operacional además de eficacia, proporcionar confianza respecto a la información financiera de la empresa, protección de activos en general, y acatamiento de obligaciones y/o regulaciones que conciernen a la organización (Mantilla, 2013).

Hablando de control interno, los sistemas que lo conforman incluyen más departamentos que contabilidad y finanzas, como el departamento de tecnologías de la información, así lo expone Mantilla (2013) basándose en propuestas de expertos, que mencionan la importancia de la difusión de los controles entre todos los individuos que laboran en la empresa al mismo tiempo del entrenamiento necesario que requieren éstos mismos con la finalidad de que los controles puedan ser aplicados.

Se puede decir, igualmente, que las auditorías implementadas internamente son esenciales ya que los auditores otorgan seguridad de que tan efectivos son o no los procesos que conforman el control interno.

Cabe señalar que los marcos de referencia, los estándares y los criterios de control son instrumentos importantes para los sistemas de control interno ya que son ellos quienes dan una base para su creación. Detrás de estos escritos, se encuentran

documentos con mayor alcance tal como la Ley Sarbanes Oxley, cuyo propósito es evitar tanto los fraudes como el riesgo de bancarrota.

Desde los últimos tiempos, el fraude financiero ha sido una gran preocupación para muchas organizaciones a lo largo de variadas industrias y países, ya que trae consigo grandes pérdidas para los negocios. Las herramientas de detección de fraude financiero han sido llevadas a escena con el fin de abordar este problema y proporcionar soluciones fiables a las organizaciones.

El fraude financiero normalmente se descubre a través del proceso de detección de valores atípicos habilitado por las técnicas de “minería de datos”, que también identifican información valiosa revelando tendencias ocultas, relaciones y patrones encontrados en una base de datos.

Aunque la detección de fraude financiero es considerada una prioridad para muchas organizaciones, la literatura actual carece de una revisión actualizada, exhaustiva y en profundidad que pueda ayudar a las empresas a seleccionar una técnica apropiada de detección de fraude. En cuanto a la prevención del fraude, esta puede considerarse como el paso adelante en la detección de riesgos (Albashrawi, 2016).

Planteamiento del problema

En México, no existe un equivalente a la Ley Sarbanes Oxley. La carencia de un completo programa de control interno deja a las empresas expuestas a ciertos riesgos tales como el fraude.

La propuesta de Ley SOX fue aceptada con el propósito de mejorar la precisión y confiabilidad de la información financiera mostrada en reportes, además de proteger a

los inversores. Debido a su amplio impacto, la Ley SOX se considera una de las más grandes reformas de los últimos tiempos.

En España y otros países, regulaciones similares a las señaladas por SOX en Estados Unidos han sido establecidas con el propósito de prevenir escándalos financieros (Cortijo-Gallego y Yezegel, 2008). En el caso de México, y a iniciativa del Consejo Coordinador Empresarial (ECCE), se emitió en 1999 un Código de Mejores Prácticas Corporativas con la finalidad de establecer recomendaciones para un mejor Gobierno Corporativo de las empresas mexicanas, sin embargo, se dejan fuera los controles internos referentes a los procesos de Tecnologías de la Información (TIC's) que tengan un impacto en la información financiera, área que está incluida en el apartado 404 de la Ley SOX.

La Ley Sarbanes Oxley (SOX) surgió a raíz de los escándalos financieros de las empresas estadounidenses Enron, Peregrine Systems y Worldcom, entre otras, que ocasionaron desastres financieros además de un desplome de la confianza de inversionistas y de la sociedad estadounidense en general.

De acuerdo a Rozen (2008), la eficacia de la Ley SOX ha probado que es posible asegurar la generación de información financiera confiable, asimismo ha demostrado que los inversores están dispuestos a pagar más por recibir a cambio confiabilidad de la situación de los negocios. Como parte de su apartado 404, la Ley SOX también estableció la Junta de supervisión de contabilidad de las empresas públicas, mejor conocida en inglés como PCAOB, para inspeccionar las auditorías de empresas públicas.

Empresas que están obligadas a cumplir con la Ley SOX han tenido reacciones reacias hacia el apartado 404, así lo afirma Gupta (2008) quien además señala que un motivo a estas resistencias son los requisitos de certificación instaurados en torno a los controles empresariales internos, al mismo tiempo de puntualizar la importancia de utilizar el marco

de referencia del Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO por su abreviatura en el idioma inglés).

Todas las empresas que cotizan en las bolsas de valores de Estados Unidos están obligadas a cumplir con la Ley SOX, pero no todas las empresas mexicanas cotizan en esas bolsas, por lo tanto, existen empresas mexicanas fuera del alcance de la Ley SOX.

Justificación del estudio

Stewart (1998) expone que entender la era informática en la que nos encontramos da partida a la buena gestión del término conocido como “capital intelectual”. A su vez, señala de este último que tanto la información como el conocimiento son los instrumentos competitivos de nuestra época. También comenta que este capital otorga una ventaja competitiva que se logra por la adición de los conocimientos con los que cuentan los empleados de una organización y que es además material formado por la experiencia de los trabajadores, sus conocimientos, y la propiedad intelectual de la organización, entre otros.

Dicho material intelectual puede rendir frutos creando riqueza, ya que, la importancia del conocimiento en el ambiente laboral se acentúa en que las empresas que hacen frente a esta sociedad del conocimiento podrán desenvolverse mejor que las que siguen teniendo enfoques al estilo de la era industrial.

Otra tarea importante para las organizaciones es el control interno, el cual se desprende del control administrativo. El control puede ser de tres tipos: legislativo, judicial/jurisdiccional (particular de México) y administrativo. En México, se cuenta con regulación en materia de control administrativo y, específicamente hablando de controles internos, la regulación es escasa (Béjar y Orrico, 2013). Las deficiencias en este tipo de

controles, dejan a las empresas expuestas a fraudes, amenazando el logro de objetivos entre los cuales se puede mencionar la eficacia de las operaciones, además del cumplimiento de reglamentación aplicable a la organización (Briones, 2014).

El fraude, es uno de los inconvenientes con mayor seriedad al que se enfrentan las empresas en México (KPMG Cárdenas Dosal, S.C., 2008). Las conductas impropias o actos deshonestos pueden perjudicar el ámbito de negocios provocando vulnerabilidad en la confianza de los inversionistas, clientes y socios estratégicos de las empresas. En situaciones como ésta, es necesario vislumbrar el impacto que tienen estos actos entre las empresas localizadas en nuestro país para, una vez entendidas las causas y consecuencias de estos problemas, se definan estrategias de prevención y remediación que las organizaciones puedan poner en funcionamiento.

Más adelante en este trabajo (ver Figura 4, página 28) se explica como el ochenta y dos por ciento de empresas encuestadas por Kroll en México para el año 2016 reportaron incidentes de fraude en los doce meses previos a la encuesta, con un incremento del dos por ciento respecto a la encuesta anual anterior y quedando por arriba del veintiséis por ciento que fue la media mundial.

Hablando particularmente de México, este país obtuvo la tasa más significativa en fraudes ocasionados por proveedores, a la par obtuvo la tercera tasa más elevada en la categoría de malversación de fondos con un diez por ciento a la vez de alcanzar un segundo lugar en empresas que sobrellevaron uno o más daños financieros con un setenta y tres por ciento. Las cifras conllevan a la conjetura de una necesidad de las empresas a enfrentar el fraude de una manera más activa.

Un ejemplo de fraude ocurrido en México, se describe en la página 30, dónde la empresa adquirió contratos irregulares desviando dinero a otros negocios además de

proporcionar documentos falsos a diversos acreedores. La misma empresa contaba con información insuficiente que permitiera conocer a detalle su condición financiera y su número de acreedores ascendía a doscientos cuatro, con créditos en su mayoría fraudulentos y equivalentes a varios millones de pesos. De haber existido un buen manejo de control interno, muchos de estos acreedores pudieron haber prevenido el fraude y de esta forma, no se hubieran perdido cantidades exorbitantes de dinero.

A pesar de que todos los sectores están expuestos al fraude, el sector industrial en México puede ser considerado uno de los más distinguidos para ser parte del presente estudio, ya que, si hablamos de la producción industrial en México, ésta tiene una tendencia al alza desde el año 2006 (ver Anexo 2) de acuerdo a datos del INEGI.

Con una cobertura nacional, el sector industrial comprende las actividades de: generación, transferencia y distribución de energía eléctrica, minería, abastecimiento de gas y agua; construcción; e industrias manufactureras en general (ver Anexo 3). Dada su gran relevancia al ser un componente primordial del incremento de la economía del país, y con el 97% de representatividad en el valor agregado bruto, puede decirse que, en México, el sector industrial es el más notable, razón por lo cual se ha decidido enfocarse a este sector para la presente investigación.

En síntesis, el presente estudio pretende guiar a las empresas mexicanas del sector industrial que no cotizan en las bolsas de valores de Estados Unidos de América y utilizan programas de software en su proceso financiero, mediante la propuesta de una serie de estrategias de controles internos, sirviéndoles como una base para la toma de decisiones y que les permitan reducir las posibilidades de fraude, todo desde un enfoque a los sistemas de tecnologías de la información.

Monetariamente hablando, este trabajo intenta ayudar a las empresas a evitar pérdidas económicas ocasionadas por el fraude; administrativamente, se impulsa la cultura de prevención de fraude y transparencia aparte de promover la lealtad empresarial de los trabajadores; estratégicamente, las empresas se verán beneficiadas con la facilitación al logro de sus objetivos empresariales.

Objetivo general

Proponer una serie de estrategias de control interno en el área de Tecnologías de la Información a través de la adaptación del apartado 404 de la Ley Sarbanes Oxley, que puedan ser implementadas en empresas mexicanas del sector industrial que no coticen en las bolsas de valores de Estados Unidos y hacen uso de tecnologías de información en su proceso financiero, para reducir las posibilidades de fraude.

Objetivos específicos

- Identificar los controles que existen alrededor del apartado 404 de la Ley Sarbanes Oxley relacionados a tecnologías de la información.
- Determinar áreas de oportunidad en México para aplicar controles internos de tecnologías de la información.
- Proponer estrategias de control interno en el área de tecnologías de la información que puedan adaptarse a empresas mexicanas del sector industrial.

Supuestos de investigación

Para el presente trabajo, al ser un estudio cualitativo, se plantean dos supuestos de investigación, los cuales se listan a continuación.

1) Tener un marco de referencia de control interno para Tecnologías de la Información basado en SOX disminuye las posibilidades de fraude.

2) Empresas mexicanas que utilizan Tecnologías de la Información para consolidar su información financiera requieren controles internos robustos.

Alcance

El presente trabajo está conducido a resaltar la importancia de implementar controles internos sólidos en el área de Tecnologías de la Información en empresas mexicanas del sector industrial que no cotizan en las bolsas de valores de E.U.A. y hacen uso de programas de software en su proceso financiero. Esto mediante la propuesta de una serie de estrategias para controles internos adaptadas a empresas mexicanas, con la finalidad de que obtengan elementos que les permitan llevar a cabo un mejor ejercicio de su práctica de control interno, disminuyendo así los riesgos de fraude.

La propuesta de una serie de estrategias de controles internos pretende ser una base para la toma de decisiones empresariales desde un enfoque orientado a los sistemas de tecnologías de la información asegurando a las empresas contar con controles internos sólidos.

Limitaciones

Al momento del estudio, se cuentan con seis limitaciones:

- a) La falta en México de un equivalente del apartado 404 de la Ley SOX en relación a tecnologías de la información, al momento del estudio.
- b) Se considera únicamente a empresas mexicanas del sector industrial.
- c) Las estrategias de control interno abarcan exclusivamente el área de Tecnologías de la Información

- d) El periodo de tiempo de recolección de la información comprende un año a partir de enero 2017.
- e) Banco de datos restringido a bases de datos, tales como de EBSCO y su Academic Search Complete.
- f) El diseño no experimental de la investigación no permitirá establecer relaciones causa y efecto, únicamente establecerá relación.

1. ANTECEDENTES DE LOS CONTROLES INTERNOS

1.1 Marco referencial

1.1.1 Comienzos del Control interno

Aunque no se sabe a ciencia cierta la fecha exacta en que surgió el control interno, estudiosos consideran que sus inicios se remontan a épocas primitivas cuando surgen los números ya que estos les ayudaban a los hombres a controlar sus patrimonios. Con el paso del tiempo, surge el término de “comprobación interna”, el cual es precursor de lo que ahora conocemos como control interno, y es entonces cuando se hace su primera referencia a principios del siglo XX.

Posteriormente, en los años treinta, se empieza a utilizar el término “control interno” definiéndose como una coordinación entre la contabilidad y los procedimientos llevados a cabo en oficinas para comprobar que el trabajo de algún empleado no tenga posibilidad de fraude (Ballesteros, 2013).

El entendimiento del término “control” ha evolucionado de ser un mero elemento de las verificaciones de detección o verificaciones correctivas y se ha vuelto para las empresas

un elemento de la prioridad de la prevención. Existe una diferencia entre el entendimiento que tienen los países anglosajones y los países latinos en cuanto al concepto de control, ya que países anglosajones adoptan el término como una guía mientras los países latinos lo interpretan como una verificación.

Asimismo, la noción de control interno a nivel global y en tiempos pasados tenía un enfoque contable hasta que modelos como el de COSO (Marco Integrado de Control Interno del Comité de Organizaciones Patrocinadoras de la Comisión Treadway) cambiaron la percepción acerca de que es un control interno. A través del marco de referencia COSO se puede apoyar a la gestión organizacional, favoreciendo al logro de objetivos empresariales (Laski, 2006).

1.1.2 Definición de conceptos

Para Coopers & Lybrand (1997), el control interno se entiende como el proceso ejecutado tanto por los directores, como la administración y en general todos los trabajadores de una organización, simultáneamente el diseño del control interno está orientado a proveer seguridad encaminada al logro de objetivos relacionados a la efectividad y/o eficiencia de los procedimientos, a la confiabilidad de la información financiera, y al acatamiento de las reglamentaciones o leyes correspondientes. El control interno también puede prevenir el fraude.

De acuerdo a la Norma Internacional de Auditoría 240 (International Auditing and Assurance Standards Board ,2013), el fraude se define como “acto intencional por parte de una o más personas de la administración, los encargados del gobierno corporativo, empleados o terceros, implicando el uso de engaño para obtener una ventaja injusta o ilegal”. Tratándose de organizaciones lucrativas, el fraude puede acontecer en cualquier

nivel jerárquico y en cualquier tipo de empresa, sin embargo, suele tener mayor presencia en aquellas que cuentan con escasos o ineficientes controles internos (Briones, 2014).

Existen diversos medios para implementar los controles internos y prevenir el fraude, por ejemplo, la innovación tecnológica. Para la sociedad moderna, las innovaciones tecnológicas son parte de nuestras vidas ya que las facilidades con que se cuentan usualmente están impulsadas por estas innovaciones.

La tecnología también da forma a las organizaciones al originar cambios a la manera en que las empresas operan, y la innovación tiene un rol notable en la competitividad. De acuerdo a Shepherd et al. (2012), la tecnología es una habilidad que permite generar una manera de crear procesos, bienes o servicios, ya sea totalmente nuevos y/o mejorados. Igualmente la definen como “el estudio de las técnicas”.

1.1.3 Antecedentes de la Ley Sarbanes Oxley y su apartado 404

La Corporación Enron era una compañía estadounidense considerada, a finales de los noventa, una de las empresas más innovadoras de Estados Unidos, la cual tenía grandes activos a favor del mundo libre del comercio electrónico. La compañía también construía plantas eléctricas y operaba líneas de gas, pero se volvió más conocida por sus negocios únicos y la creación de nuevos mercados para productos extraños en aquel entonces, entre ellos, el tiempo de transmisión para los anunciantes y el ancho de banda de internet (Li, 2010).

Enron fue fundada en mil novecientos ochenta y cinco, dieciséis años después, a finales del año dos mil uno, se informó que su situación financiera se sustentaba en un fraude planeado e institucionalizado, en otras palabras, altos mandos efectuaron el fraude, haciendo perder a los accionistas cerca de doscientos mil millones de pesos.

Además, la revisión a los últimos estados financieros reveló que había once mil millones de pesos en pérdidas. Enron Corporation finalmente se declaró en bancarrota el dos de diciembre de dos mil uno. Dado el alto impacto que provocó el escándalo de Enron a empleados, inversionistas y, hablando en general, la sociedad, además de la aparición de casos similares en empresas por aquella época, se promulgó una ley (SOX) que monitorea a las corporaciones y filiales que cotizan en las bolsas de valores de los Estados Unidos de América tales como la NYSE (Bolsa de Nueva York) y NASDAQ (Asociación Nacional de Concesionarios de Valores).

La Ley Sarbanes Oxley entró en vigor en el año dos mil dos e introdujo cambios importantes en la regulación de la práctica financiera y el gobierno corporativo estadounidenses. Nombrada así debido al senador Paul Sarbanes y el representante Michael Oxley, quienes eran sus principales elaboradores, la ley también fijó una serie de plazos para su cumplimiento. La Ley SOX se organiza en once títulos, en los cuales las secciones más importantes suelen considerarse las secciones 302, 404 y 906 (Leech, 2004).

La sección 404 del título IV Evaluación Gerencial de los Controles Internos, instituye los criterios y el lapso de una valoración ejecutada por la Administración en relación a los controles internos. A su vez se menciona que auditores externos deben pronunciar un veredicto respecto a la eficacia del control. Simultáneamente, se plantea que la dirección es responsable de instaurar procesos y procedimientos referentes al control interno igualmente de ser responsable de una evaluación interna a estos mismos.

Para alcanzar la eficacia del control, se requiere un marco de referencia apropiado. El marco de referencia recomendado por la Comisión Nacional del Mercado de Valores (Securities and Exchange Commission en inglés) es el marco COSO (Santa Cruz, 2014).

La mayoría de las empresas estadounidenses (The Institute of Internal Auditors, 2008) han utilizado el marco COSO, aunque algunos han utilizado el marco de los Objetivos de Control para la Información y la Tecnología Relacionada abreviado como COBIT, por sus siglas en inglés, como complemento al marco COSO para los controles concernientes a Tecnologías de la Información.

Como se menciona en el resumen ejecutivo del reporte COSO, el control interno puede definirse como un proceso, el cual es ejecutado por diversos empleados de la organización incluidos la dirección y la administración; este proceso pretende proveer una “seguridad razonable” en torno al logro de objetivos categorizados en tres partes.

La primera categoría del logro de objetivos, cubre los objetivos empresariales considerados básicos para las organizaciones, incluyendo a los objetivos de rendimiento y rentabilidad aparte del aseguramiento de recursos. La segunda categoría se refiere a la elaboración de estados financieros que sean fiables, incluidos estados financieros provisionales y condensados y los datos que deriven de dichas declaraciones. La tercera categoría trata de cumplir con la legislación y reglamentación a la que la entidad está sujeta (Committee of Sponsoring Organizations of the Treadway Commission, 2013).

En términos generales, la Ley SOX ha tenido un gran impacto. Srinivasan y Coates (2014) realizaron una evaluación de más de ciento veinte resultados de investigaciones en contabilidad, finanzas y leyes que pudieran ser utilizadas para valorar el impacto de la Ley SOX y establecer pasos para orientar la elaboración de legislación a futuro. Las derivaciones obtenidas de la evaluación, revelaron que los mercados han evaluado a las empresas de forma más eficaz, los gerentes han mejorado los procesos internos, y las pruebas de control interno se volvieron más rentables con el paso del tiempo desde la aparición de la Ley SOX.

Estudiosos afirman que la parte más preocupante de la Ley SOX, en el aspecto comercial, es la disposición que obliga a las organizaciones que cotizan en bolsa a contratar una firma de auditoría externa para que evalúe sus prácticas de control interno. Este requisito ha causado un impacto negativo para empresas pequeñas debido a que es elevado el costo, sin embargo, las compañías con ciertos límites de mercado han podido diferirlo.

A pesar de que implicó un costo adicional el poder efectuar su ejecución (Flores, 2014), la Ley SOX se ha vuelto un medio indispensable para lograr en las compañías un mejor control interno, asegurando un incremento en la autenticidad de la información financiera de todas aquellas compañías que cotizan en las bolsas de valores de Estados Unidos. Aunque la Ley SOX no evita el fraude, la ley establece una responsabilidad donde una persona garantiza a los auditores externos que la información es completa y veraz además que los auditores externos avalan dicha información, reduciendo de esta manera las posibilidades de fraude.

1.1.4 Controles internos para los Sistemas de Información

En el ámbito del control interno, se distingue el término de control clave. Un control clave es un control que, si fracasa, significa que hay al menos una “probabilidad razonable” de que un error material en los estados financieros no sería prevenido o detectado en forma oportuna. Por lo tanto, un control clave es aquel que se requiere para otorgar un nivel de seguridad sobre los errores materiales (The Institute of Internal Auditors, 2008).

Grosso modo, los controles generales de tecnologías de la información, mejor conocidos en inglés como ITGC, aseguran que las aplicaciones se desarrollan y posteriormente se mantienen, de tal forma que proporcionan la funcionalidad necesaria para procesar las transacciones y proporcionar controles automatizados. También garantizan el correcto funcionamiento de las aplicaciones y la protección de datos y programas contra cambios no autorizados.

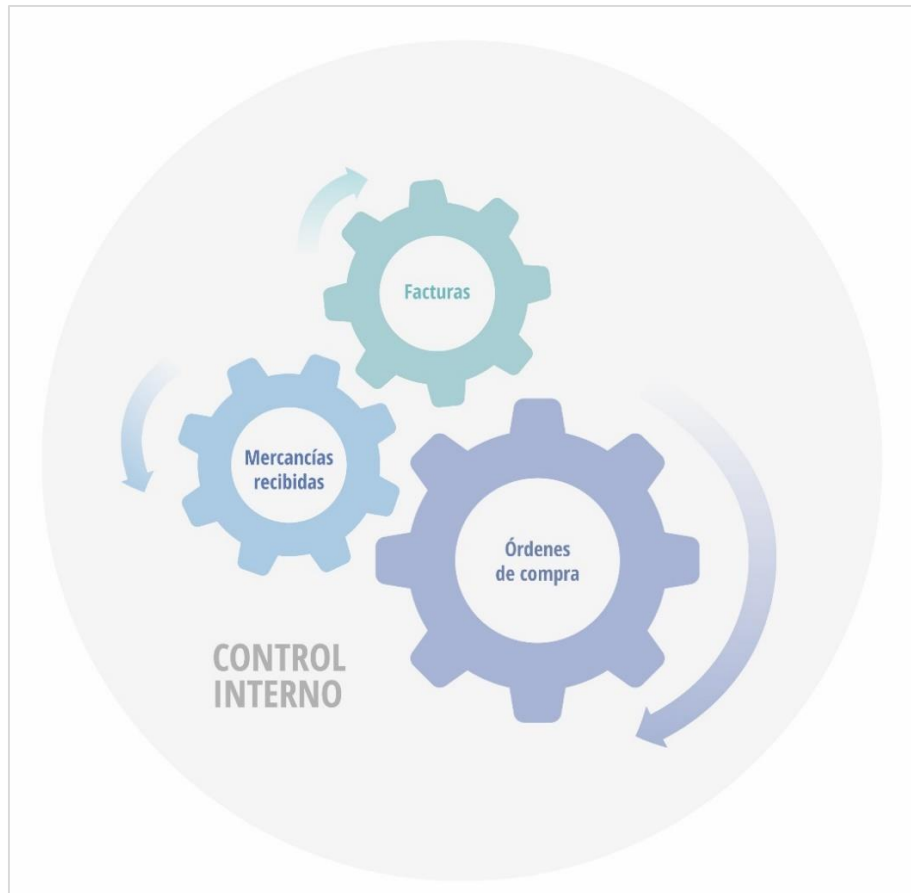
El desafío de identificar los controles clave dentro de ITGC es que no tienen un efecto directo en los estados financieros. Debido a que los ITGC proporcionan garantías sobre el funcionamiento continuo y adecuado de los controles automatizados claves, un fallo en un control clave de ITGC implica la pérdida de esa garantía. En otras palabras, la dependencia de ITGC es indirecta a través de la confianza en los principales controles automatizados. Si los controles clave de ITGC fallan, los controles automáticos clave pueden no ser confiables y podrían incumplir su función de prevenir o detectar un error material.

En término de sistema, un control interno bien concebido y operado puede garantizar tanto a la dirección como a la administración, un “grado razonable” acerca de la consecución de los objetivos de una empresa (The Institute of Internal Auditors, 2008). Sin embargo, las posibilidades de tener éxito están perjudicadas por todas aquellas restricciones inherentes a los sistemas de control. Estos incluyen que las resoluciones en la toma de decisiones pueden tener omisiones y que los malos desgloses financieros pueden ocurrir a causa de un simple error. A continuación, un ejemplo.

En las siguientes líneas, se describe un hipotético caso de riesgos de proceso de ITGC, específicamente relacionado a objetivos de control de TI. En una empresa, cuentan con un control interno automatizado que es fundamental, y el cual es la combinación de tres

vías entre las órdenes de compra, los registros de las mercancías recibidas y las facturas de los vendedores. Ver la Figura 1 para una referencia visual.

Figura 1. Ejemplo de control interno automatizado

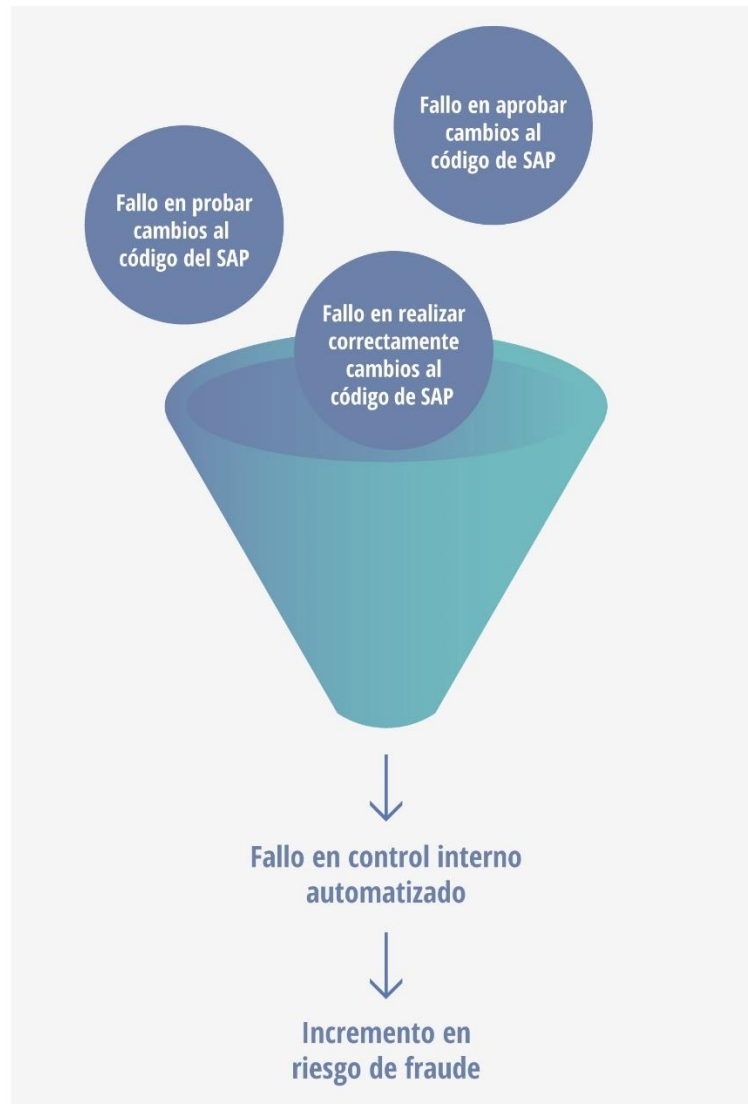


Fuente: Elaboración propia

SAP es la aplicación financiera que contiene este proceso crítico de TI, siendo considerado crítico por el impacto que tiene sobre la información financiera empresarial. En un momento dado, la administración determina que una falla al aprobar, probar y realizar correctamente cambios en el código de SAP (cambios erróneos al sistema) podría resultar en un fallo de la combinación de las tres vías para operar apropiadamente,

de esta misma manera el cambio en el código puede ocasionar fraude. Ver la Figura 2 para una mejor explicación.

Figura 2. Vulnerabilidad identificada en el control interno automatizado



Fuente: Elaboración propia

Entonces, en este ejemplo, los objetivos identificados alrededor del control interno de TI son tres: primero, todos los cambios al sistema de SAP deben ser debidamente

aprobados, segundo, todos los cambios al sistema de SAP deben ser adecuadamente probados en el ambiente de prueba (ambiente utilizado por desarrolladores de software), y, tercero, los cambios en el sistema de SAP deben moverse con precisión al ambiente de producción (ambiente visto y utilizado por usuarios finales de SAP). Ver Figura 3.

Figura 3. Objetivos de control interno para prevenir deficiencias



Fuente: Elaboración propia

Para que los sistemas de información alcancen plenamente los beneficios y objetivos de optimización de recursos y riesgos, es necesario abordar el riesgo que podría prevenir el logro de estos objetivos. Las organizaciones suelen diseñar, desarrollar, implementar y monitorear sistemas de información a través de políticas, procedimientos y estructuras organizacionales para enfrentar precisamente estos tipos de riesgos, en otras palabras, controles internos.

El ciclo de vida del control interno es de naturaleza dinámica y está formulado para otorgar un aseguramiento de cierta manera razonable acerca de que los objetivos organizacionales se lograrán además de que las deficiencias serán prevenidas,

detectadas oportunamente y en este último escenario también serán corregidas (Information Systems Audit and Control Association, 2015).

De acuerdo a COSO, la base de todos los elementos que conforman el control interno es precisamente el ambiente que gira en torno al control y está presente en la compañía. Este ambiente, llamado “ambiente de control” se entiende como la actitud que tienen los empleados de la empresa hacia la importancia de contar con un control interno. En términos generales, el ambiente se conforma por acciones, políticas, procedimientos que reflejan la actitud de los trabajadores y además tiene una gran atribución a la forma en la cual la organización valora riesgos, establece objetivos, y estructura sus actividades.

Dentro del “ambiente de control”, se identifican la integridad y ética, el compromiso por la competencia, la organización jerárquica, la filosofía gerencial, la repartición de responsabilidades, la junta de auditoría y/o un consejo formado por directores (Rivas, 2011). Si una organización cuenta con un ambiente de control efectivo, éste puede ser de ayuda para mitigar las probabilidades de tener irregularidades, de igual manera, si el ambiente de control es débil éste puede reducir la efectividad del control.

Además del “ambiente de control”, los objetivos de control son importantes. Los objetivos de control de los sistemas de información, proporcionan una serie de requisitos que deben ser considerados para lograr un control efectivo de los procesos de TI.

Los objetivos de control para los sistemas de información, son declaraciones del resultado o propósito deseado que se lograrán mediante la ejecución de controles en torno a los procesos llevados a cabo por los sistemas de información; un compromiso de estándares, políticas, procedimientos, y estructuras organizacionales; y diseñados para otorgar un aseguramiento razonable de que se lograrán los objetivos de negocio y los

eventos no deseados se evitarán, detectarán y corregirán (Information Systems Audit and Control Association, 2015).

Cabe resaltar que, los controles generales no se limitan al área de TI ya que pueden ser aplicados a cualquier área de una empresa, incluida la infraestructura de TI y sus servicios de soporte.

Los controles generales envuelven a los controles contables internos que son aquellos referentes a la protección de los activos empresariales y a la confianza que se tiene sobre los datos financieros; controles operativos relativos a las operaciones, funciones y actividades cotidianas, además de asegurarse de que las operaciones cumplen los objetivos comerciales; controles administrativos referentes a la eficiencia operacional en una cierta área funcional y al cumplimiento de políticas de gestión; procedimientos de seguridad organizacional que garanticen un uso apropiado de activos; políticas generales para el diseño y utilización de documentos y registros adecuados para garantizar el registro adecuado de las transacciones; procedimientos y prácticas para avalar la protección adecuada del acceso y uso de activos e instalaciones; y políticas de seguridad físicas y lógicas para todas las instalaciones, centros de datos y recursos de tecnologías de la información (Information Systems Audit and Control Association, 2015).

2. LA FALTA DE UN EQUIVALENTE AL APARTADO 404 DE LA LEY SARBANES OXLEY EN MÉXICO EN RELACIÓN A LAS TECNOLOGÍAS DE LA INFORMACIÓN QUE IMPIDA LOS FRAUDES FINANCIEROS

2.1 Marco contextual

2.1.1 Incremento de incidentes de fraude en México

En la Figura 4 se observa, de acuerdo al Informe anual de Fraude Global de Kroll 2015-2016, que el ochenta y dos por ciento de empresas encuestadas en México reportaron incidentes de fraude en los últimos doce meses, con un incremento del dos por ciento respecto al informe anual previo 2014-2015 (Ver Anexo 1), teniendo principalmente incidentes de fraude por parte de proveedores y quedando por arriba de la media mundial del veintiséis por ciento.

Los resultados del Informe revelaron además que la principal amenaza para las empresas a nivel mundial reside al interior de las mismas empresas y, de las empresas donde se cometió fraude y el responsable fue identificado, éste provenía primordialmente de un empleado con experiencia menor a dos años, seguido en porcentaje por un empleado en puesto medio o de alto cargo.

Figura 4. Incidentes de fraude en México en el año 2015



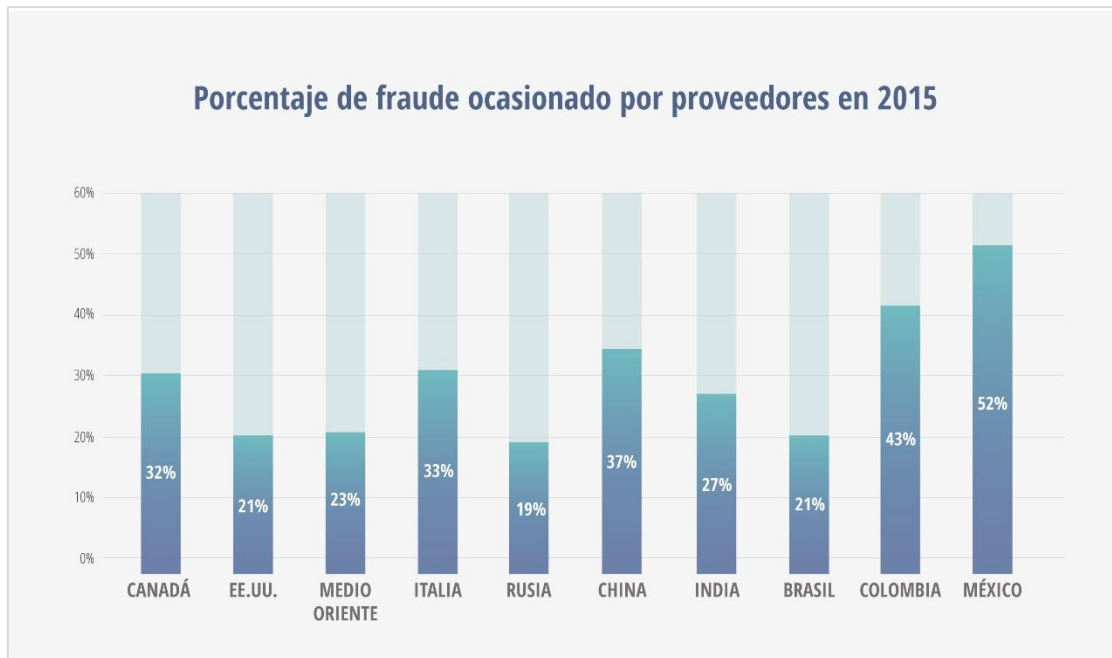
Fuente: Elaboración propia de acuerdo al Informa Anual de Fraude Global de Kroll 2014-2015.

Al mismo tiempo, en la Figura 5 observamos que, de todos los países encuestados, México registró la tasa más alta en fraudes ocasionados por proveedores siendo el promedio un porcentaje de veintiséis por ciento, igualmente obtuvo la tercera tasa más alta en malversación de fondos con diez por ciento y el segundo lugar en empresas que sufrieron uno o más daños financieros con un setenta y tres por ciento.

Del mismo modo, los dos mecanismos más utilizados por los encuestados en México para combatir el fraude son: la diligencia debida del proveedor, cliente o compañero de negocios; los controles financieros; y los controles de riesgo (Ver Anexo 3). Brian Weihs, director de Kroll México, sugirió a mediados de 2016 que, a fin de evitar que el porcentaje de fraude en el país continúe creciendo, las empresas requieren sistemas de detección de fraude fuertes y bien establecidos que puedan prevenir, responder e investigar el

fraude cuando se presente. Detener el crecimiento del porcentaje de fraude, otorga la facilidad de hacer negocios en México.

Figura 5. Porcentaje de fraude ocasionado por proveedores en 2015



Fuente: Elaboración propia de acuerdo al Informa Anual de Fraude Global de Kroll 2014-2015.

Para García (2013), es indispensable que las empresas, sin importar su tamaño, posean un robusto programa de control, el cual pueda otorgarles certidumbre acerca de la obtención de sus metas y objetivos. Especialistas señalan que el “ambiente de control” es indispensable para las bases de los elementos que conforman el control interno, consecuentemente, es un segmento primordial en la estructura del control interno además de estar conformado por actitudes, conocimientos, gestiones directivas, y personal clave.

El “ambiente de control” también implanta el nivel de exigencia empresarial para que los controles sean implementados e interviene en el conocimiento de los trabajadores

acerca de los controles internos, beneficiando a la eficacia de los controles internos y a la confiabilidad representada en la información financiera. Cabe resaltar que un ambiente de control próspero requiere del soporte y orientación de los niveles superiores de administración de la empresa.

Un caso en México donde claramente no existía un ambiente de control próspero, es el de la empresa naviera Oceanografía S.A. de C.V., también conocida como OSA, la cual fue fundada en 1968 con la finalidad de proporcionar servicios de ingeniería marina a Pemex. A finales del año 2016, la empresa fue declarada en quiebra.

En 2013 OSA fue acusada de adquirir contratos irregulares equivalentes a más de dos mil doscientos millones de pesos (Rosas, 2014), desviando dinero a otros negocios; además de proporcionar documentos falsos a diversos acreedores, con lo cual quedó comprometido su futuro. Por otra parte, OSA contaba con información insuficiente que permitieran conocer a detalle su condición financiera, en particular información acerca de las obligaciones, contratos, bienes, y personal con el que contaba (Carriles, 2014).

Para finales de 2014 la deuda de OSA de acuerdo a Orozco (2015) se estimaba alrededor de los catorce mil trescientos millones de pesos, teniendo un total de doscientos cuatro acreedores para doscientos cuarenta y cinco créditos de diferentes categorías, de los cuales muchos de ellos eran fraudulentos y siendo el más hablado el caso de fraude ocasionado a Banamex. Para ese entonces, la empresa OSA era ya insolvente y, de no haber intercedido el Servicio de Administración y Enajenación de Bienes (SAE), la producción petrolera mexicana pudiera haberse visto afectada.

Carriles (2014) plantea que el acreedor más afectado fue Banamex con una cuenta por seis mil setecientos cuarenta y cinco millones de pesos; seguido de Senior Secure

Notes con cuatro mil setecientos tres millones; y en tercer lugar Candies Mexican Investments con dos mil ciento setenta y cinco millones.

Asimismo, OSA le adeudaba al Servicio de Administración Tributaria (SAT) mil doscientos cuarenta millones de pesos, a Banorte quinientos diecisiete millones, además de los acreedores menos afectados quienes fueron Arrendadora Banamex Sofom con diecinueve millones de pesos, Financiera Bajío Sofom con treintaicuatro millones y Caterpillar Crédito con treinta millones pesos.

Particularmente, el fraude de OSA a Banamex fue resultado de que fallaron los controles internos del banco en materia de riesgo y supervisión además de monitoreo (Juárez, 2014). Los débiles controles internos de Banamex le llevaron a tener pérdidas próximas a los siete mil millones de pesos, conjuntamente el daño a la reputación del banco pudo haber ocasionado tanto una pérdida de negocio como una menor rentabilidad.

La Comisión Nacional Bancaria y de Valores (CNBV) otorgó millonarias multas a Banamex por descubrimientos de actividades que iban en contra de la normativa financiera bancaria, así como por no contar con mecanismos eficientes que permitieran verificar el cumplimiento de contraloría interna. Una de las multas más significativas fue debido a un conflicto de interés detectado en las autorizaciones para líneas de crédito, donde un empleado que estuvo a cargo de autorizar los aumentos de las líneas para OSA formaba parte del área de negocio de Banamex y simultáneamente era responsable de las relaciones con clientes.

Otras multas fueron debido a la falta de control que se tuvo sobre los manuales de políticas y de procedimientos del banco, por otorgar a OSA un aumento en su línea de

crédito sin tener un expediente relativo a la solicitud, y la falta de evaluación y vigilancia del riesgo operativo que OSA representaba.

Más del noventa por ciento de todos los ingresos de OSA provenían de contratos con Pemex. Rosas (2014) expone que control interno de Pemex no consideró siquiera algún daño trascendente a Pemex para 2015 debido que entre los años 2006 y 2014 se llevaron a cabo ochenta y dos contratos con OSA de los cerca de quinientos mil contratos totales celebrados. Sin embargo, cuatro mil millones de pesos fueron parte de los contratos que Pemex tuvo con OSA, cantidad que no pasa desapercibida.

Lozoya (2014) afirma que Pemex implementó un mecanismo de control interno llamado “Bóveda Electrónica” para que los contratos celebrados con cualquier empresa y la relación bancaria de la misma puedan ser analizados por medio de internet, esto con la finalidad de prevenir otro caso como el de OSA.

También defiende la idea de que si este mecanismo hubiera existido anteriormente, el fraude cometido por OSA hacia Banamex, por mencionar una de las tantas empresas afectadas, hubiese sido evitado. Simultáneamente, explica que Pemex implementó a la par una gestión para que su documentación existiera electrónicamente y estuviera disponible para ser consultada por los empleados involucrados, promoviendo así la transparencia, integridad y el uso eficiente de tecnologías de la información.

Otro caso reciente de fraude, en América Latina, fue el acontecido hacia El Puerto de Liverpool S.A.B. de C.V., quien fue víctima de fraude por un monto superior a los mil treinta y siete millones de pesos, por parte de su filial Grupo Unicomer (Celis, 2017). El fraude se consumó en 2015 sin embargo fue hasta dos años después cuando Unicomer identificó, a través de una auditoría interna, irregularidades después de haber comprado

una empresa en Paraguay llamada Wisdom Product, descubriendo quince mil operaciones de crédito que no contaban con respaldo documental.

Asimismo, a través de un analista y gerente de tecnología de la empresa (“Crearon 15.000 créditos fantasmas para sobrevalorar firma Electrofácil”, 2017), se identificó que en el 2013 un alto mando comunicó a diversos funcionarios la concepción de un sistema que servía para optimizar la demora que se tenía con la cartera de clientes, con la finalidad de obtener indicadores favorables. La investigación arrojó que altos funcionarios de la empresa crearon un centro de documentación en un inmueble donde generaban una gran cantidad de documentación falsa. El sistema informático con el que contaban, estaba establecido de un modo donde la fraudulenta cartera de crédito era visible únicamente para un reducido número de personas.

Los perpetuadores del fraude crearon alrededor de cuarenta mil facturas falsas correspondientes a cuotas de créditos fantasma, además de una gran cantidad de otro tipo de documentos falsos entre los cuales se incluyeron pagarés y cobros inexistentes por parte de clientes. Unicomer logró pasarse los controles internos, los cuales resultaron ser ineficientes e incluso se saltaron los controles de la Comisión Nacional de Valores y la Bolsa de Valores y Productos de Asunción de Paraguay, ya que ambas permitieron una emisión de bonos final (“Crearon 15.000 créditos fantasmas para sobrevalorar firma Electrofácil”, 2017),

Como consecuencia (Iñiguez, 2017), Unicomer tuvo que emprender variados procesos legales contra los previos accionistas de Wisdom Product, igualmente tuvo que volver a elaborar sus estados financieros previos sancionando el capital contable en más de mil treinta y siete millones de pesos, cantidad que incorpora tanto el efecto ocasionado por el fraude como ajustes relativos. El impacto para El Puerto de Liverpool fue también

negativo ya que tuvo que asumir un importe de quinientos dieciocho millones de pesos, derivado de su participación del cincuenta por ciento en Unicomer.

Uno de los elementos fundamentales del control interno efectivo es la segregación de funciones, proceso en el cual se dividen los deberes entre varias personas. Como tal, ninguna persona puede aprovechar la situación para obtener beneficios personales o de otro tipo. Aunque la segregación de funciones sobresale en las organizaciones grandes y burocráticas, puede presentar un desafío para las empresas pequeñas ya que cuentan con personal y recursos limitados.

Esto no significa que empresas pequeñas que deben cumplir la sección 404 de SOX tengan siempre debilidades en materia de segregación de deberes (Gramling et. al., 2010). Para Unicomer, si el control interno hubiera incluido la segregación de deberes, las posibilidades de fraude se hubieran visto reducidas.

2.1.2 Regulaciones en otros países

La transparencia y el gobierno corporativo se han vuelto una cuestión sumamente importante, especialmente después de las olas de escándalos corporativos y la promulgación de la Ley SOX en 2002 (Cortijo-Gallego y Yezegel, 2008). En la era post SOX, los reguladores de todo el mundo adoptaron caminos diferentes para combatir escándalos y sanar los daños corporativos que estos casos de fraude ocasionaron en la confianza de los inversionistas.

En el caso de España Cortijo-Gallego y Yezegel (2008), mencionan que el impacto de SOX en la normativa española es significativo. No obstante, se ha realizado un esfuerzo sustancial por parte de los reguladores españoles para incrementar los estándares de

divulgación y gobierno en España, pero esos esfuerzos a menudo carecen de la aplicación que se estableció en los Estados Unidos.

En Canadá, las regulaciones correspondientes a seguridad adoptaron la Ley SOX y otras regulaciones estadounidenses como un modelo útil al gobierno corporativo canadiense, desafortunadamente éste nuevo régimen tiende a interpretarse como una respuesta a una solución en vez de un problema. SOX fue un modelo inapropiado para Canadá, de acuerdo a Sibold (2009), debido a las características distintas de los mercados de capitales canadienses en comparación con los de Estados Unidos.

Sibold expone que la armonización del régimen de gobierno corporativo de Canadá con el de los Estados Unidos es un objetivo político necesario o deseable y no se somete a pruebas adecuadas, conjuntamente, los reguladores de valores canadienses no evaluaron críticamente, en su momento, los fundamentos teóricos de SOX, especialmente su dependencia de auditores independientes como asesores efectivos de la administración.

El Gobierno de Australia promulgó en 2004 el Acta del Programa de Reforma Económica de la Ley de Sociedades Anónimas (CLERP por sus siglas en inglés), con el propósito de regular aspectos concernientes al registro de firmas de auditoría, independencia y supervisión de estas. Además, estableció disposiciones orientadas a optimizar la confianza otorgada por la información financiera proveída por las empresas, adicionando disposiciones para penalidades civiles.

La Agencia de Servicios Financieros y Junta de Negocios de Contabilidad de Japón, emitió en 2007 las Guías para los Informes de Control Interno e Implementación (Anderson, 2008). Las guías, también conocidas como J-SOX, comprenden orientaciones tales como la evaluación de controles relacionados con procesos de las unidades de

negocios y deficiencias identificadas en la evaluación de controles internos, conjuntamente los controles de TI son un punto central de atención. Anderson (2008) expone que estas leyes y regulaciones crearon en Japón nuevas demandas al mismo tiempo que oportunidades de negocio, por ejemplo, los proveedores de soluciones y servicios de TI, sin embargo, con la escasez de auditores de Japón en comparación con el número de auditores en los Estados Unidos, se pronostica que para años futuros aumente el requisito de la eficiencia del proceso de auditoría interna, el número de auditores y el software que puede apoyar los procesos de auditoría.

En el ámbito de modelos de control, a nivel mundial se han publicado numerosos modelos y lineamientos que pretenden mejorar el gobierno corporativo de las empresas que los aplican (Fonseca, 2011). Los modelos que se han distinguido a nivel global son COSO por parte de Estados Unidos, COCO por parte de Canadá, Cadbury en Reino Unido, Vienot en Francia, King en Sudáfrica, y en Latinoamérica el modelo MICIL que es una adaptación de COSO para América Latina.

Este último, se diferencia primordialmente de COSO en sus fundamentos ya que mientras COSO establece que los valores éticos son la base de todo modelo de control, MICIL no los considera fundamentales, pero si los toma en cuenta. Para el caso de empresas ubicadas en el continente americano, suelen optar por los modelos COSO, MICIL y COCO.

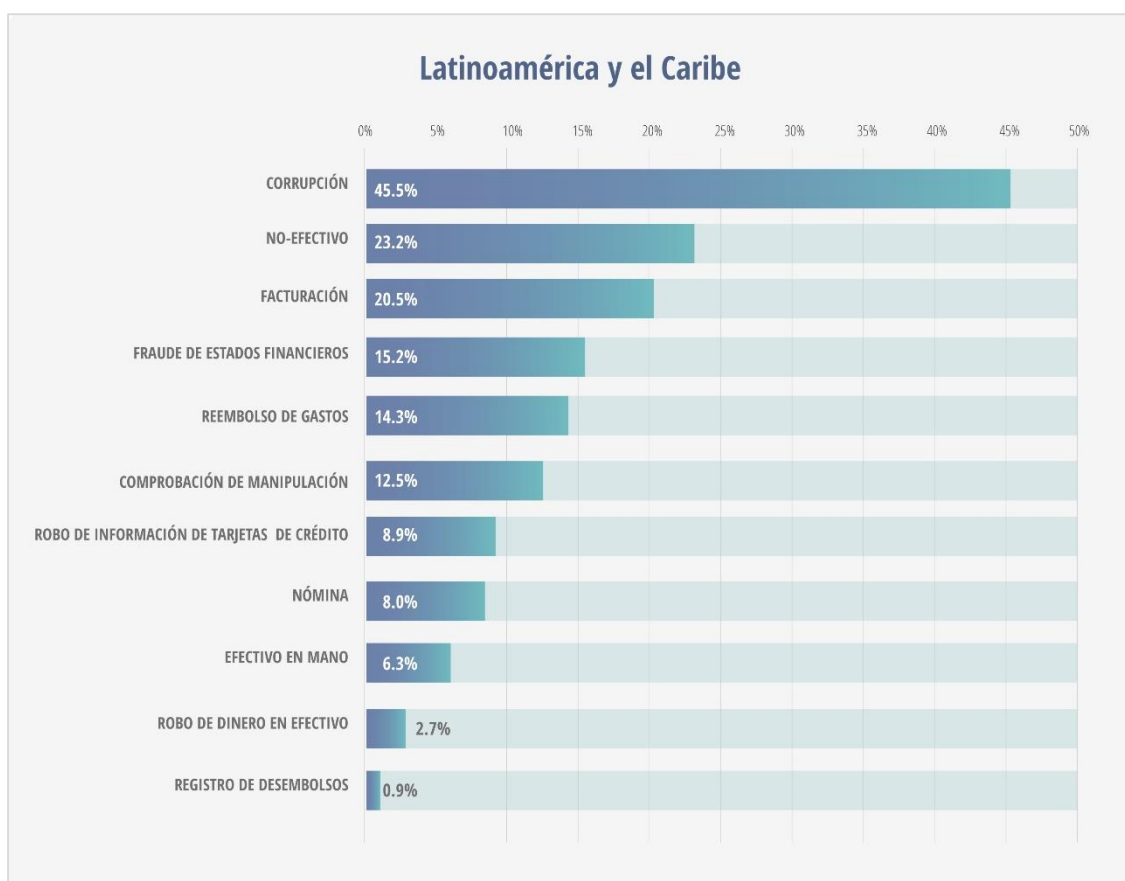
2.1.3 Toma de perspectiva

La Asociación de Examinadores de Fraude Certificados (2016), conocida como ACFE por sus siglas en inglés, realiza cada año un reporte de fraude organizacional tomando

como muestra países de diversos continentes. Para el reporte que cubre el año 2016, los examinadores calcularon que la empresa tradicional pierde el 5% de sus ingresos debido a casos de fraude. Los casos en el estudio mostraron que las pérdidas ocasionadas superaron los cien mil millones de pesos, además de tener un déficit promedio por caso de cincuenta millones.

La usurpación de activos ocupó el puesto del fraude laboral más frecuente, ocurriendo en un porcentaje ligeramente por encima del ochenta por ciento de los casos estudiados, a la vez ocasionando la menor pérdida mediana de dos mil millones mientras que el fraude de los estados financieros estaba ocurriendo en menos del diez por ciento de los casos, pero causando una pérdida de dieciocho millones de pesos, por último, los casos clasificados como corrupción se ocuparon en la media con poco más de treinta y cinco por ciento y una merma media de tres mil millones (Ver Anexo 4). A continuación, se muestra la Figura 6 con los resultados de las empresas latinoamericanas evaluadas.

Figura 6. Latinoamérica y el Caribe



Fuente: Elaboración propia con información de la Asociación de Examinadores de Fraude Certificados, 2016.

El reporte de ACFE (2016), plantea que las empresas pequeñas tenían una tasa de implementación significativamente menor de los controles antifraude en comparación con las grandes organizaciones. El reporte también señala que estas brechas en la prevención del fraude y la cobertura de detección, dejan a las pequeñas empresas considerablemente susceptibles a fraudes, los cuales pueden ocasionar perjuicios significativos dados sus limitados recursos. Finalmente, la debilidad organizacional más destacada que contribuyó a los fraudes en el estudio fue la falta de controles internos,

que fue citada en el 29,3% de los casos, seguida de una anulación de los controles internos existentes, lo que contribuyó a poco más del 20% de los casos.

La información financiera llega a ser útil y confiable para los interesados cuando se prepara con certeza. La administración es quien proporciona seguridad de que sea confiable al establecer políticas, normas y procedimientos referentes al control interno, además de asegurarse de su cumplimiento. Es, por lo tanto, preciso que la administración demuestre interés por cumplir los controles internos establecidos, teniendo como base la vigilancia y supervisiones del control interno. Si las empresas encuestadas en el reporte de ACFE hubieran tomado en cuenta estas consideraciones, los resultados habrían sido muy diferentes.

Además de interés por cumplir los controles internos, las organizaciones deben considerar el tipo de control que se llevaría a cabo, si sería manual o con poca intervención humana. Los controles que no tienen intervención humana, o muy poca, son llamados automatizados. Shepherd et al. (2012) consideran que un tema frecuente en las variadas definiciones del término tecnología es la perspectiva de la tecnología como una capacidad para lograr objetivos, y no se equivocan.

Actualmente los controles internos son mayoritariamente automatizados (Braganza y Franken, 2007), dado el extenso uso de herramientas de IT, mediante la incrustación dentro de las aplicaciones o bien los controles son una combinación de controles automatizados con controles manuales.

La sección 404 de la Ley SOX no tiene una orientación hacia algún tipo de control en particular, siempre y cuando sea un control robusto, pero engloba una gran categoría de aplicaciones que no solo incluyen a sistemas como SAP mejor conocidos en el ambiente informático como sistemas ERP (Planeamiento de Recursos Empresariales) sino también

bases de datos e incluso hojas de cálculo. Bilancio (1996) menciona como las empresas deben tener una estrategia que, junto a sus áreas funcionales, tenga la intención de lograr mejores niveles de inversión de capital y puntualiza que una estrategia no es un plan sino una decisión. Con esto resalta una vez más la importancia de llevar a cabo controles internos robustos.

3. METODOLOGIA DE OBTENCIÓN DE INFORMACIÓN PARA LA ELABORACIÓN DEL ESTUDIO

3.1 Enfoque

La investigación con enfoque cualitativo, de acuerdo a Hernández et al. (2006), se diferencia del cuantitativo “al llevar a cabo una recolección de datos sin medición numérica con la finalidad de revelar o perfeccionar las preguntas de investigación a lo largo de la interpretación”. Los planteamientos del problema no son totalmente específicos, además de que el proceso se basa en explorar y descubrir logrando generar una perspectiva teórica. Otra diferencia es la indagación, proceso que considera la realidad y, consecuentemente, es flexible.

Por las razones anteriormente expuestas, en la elaboración del presente trabajo de investigación se optó por llevar a cabo una investigación con un enfoque cualitativo, descriptivo y exploratorio. Como expone Bernal (2010), el alcance descriptivo tiene la capacidad de escoger aquellas características primordiales del objeto estudiado para poder dar una descripción minuciosa de las mismas. Por lo tanto, un alcance descriptivo permite enfocarse a un apartado exclusivo de la Ley Sarbanes Oxley. Entre las ventajas

de los estudios descriptivos, Abreu (2012) señala que utiliza ayudas visuales que permiten un mejor entendimiento del estudio cualitativo y permite el encuentro de nuevos conocimientos que, de otra manera, no podrían obtenerse. En cuanto sus limitaciones, no permite establecer relaciones de causa y efecto, además de que puede ser mal utilizado si no se entiende su propósito.

Se adoptó el alcance exploratorio porque no existe en México un equivalente a la Ley Sarbanes Oxley en su apartado 404, donde las ventajas de los estudios exploratorios de acuerdo a Abreau (2012), se encuentran el ayudar a explicar mejor el fenómeno de investigación, termina cuando se tiene información suficiente del tema, garantiza un estudio riguroso cuando se tiene conocimiento o experiencia limitada sobre el tema de investigación, y cuando se requieren aclaraciones la información puede ser investigada de manera informal. En cuanto a sus desventajas, la investigación puede perder flexibilidad si el investigador tiene sesgos en cuanto al manejo de información, si el investigador no realiza análisis matemáticos exigentes dando como resultado el no ser idónea para investigaciones cuantitativas.

3.2 Muestreo

Hernández et al. (2006) sugiere que no existe alguna etapa determinada dentro del proceso cualitativo para elaborar una muestra además que el concepto de muestra es tentativo. Asimismo, la muestra está afectada por la profundidad que la misma investigación pretende, dejando fuera la importancia probabilística. El trabajo de investigación que se expone en el presente documento, al tener un enfoque cualitativo y ser de corte documental, no cuenta con parámetros definidos para delimitar una muestra.

3.3 Técnica para recopilar información

Con la finalidad de fundamentar el trabajo de tesis se utiliza la técnica documental. La investigación documental se distingue por el uso de documentos gráficos para la recopilación de información, permitiendo al investigador fundamentar e integrar la investigación dadas las aportaciones de diversos autores (Muñoz, 2011).

3.4 Técnicas para analizar la información

Las investigaciones de enfoque cualitativo, no cuentan con una clasificación o listado específico de técnicas a diferencia de las investigaciones cuantitativas, sin embargo, existen propuestas de técnicas tales como el análisis de contenido o el análisis del discurso (Marradi et al., 2010). A continuación, se detallan las técnicas elegidas para el presente trabajo de investigación.

3.4.1 Análisis de contenido

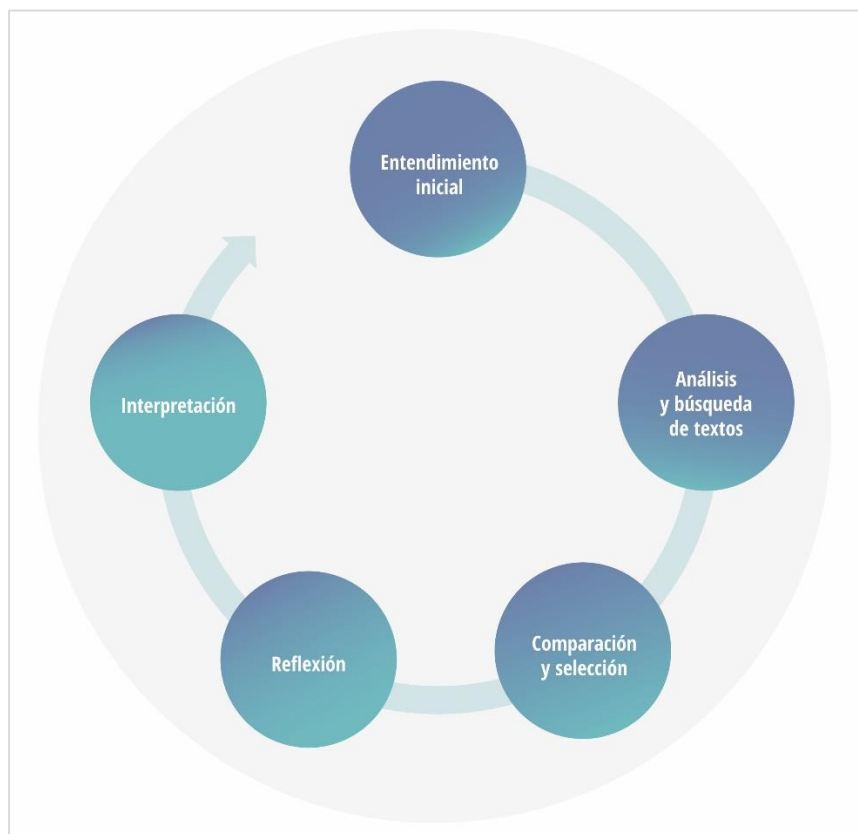
Para el marco metodológico de la presente tesis, se ha elegido la técnica de análisis de contenido. El análisis de contenido se entiende como un conglomerado de procedimientos interpretativos, donde los textos o discursos resultan de procesos de comunicación preliminarmente registrados, y cuyo objetivo es procesar y elaborar datos que sean relevantes acerca de las condiciones en que se han producido o bien, sobre aquellas condiciones que puedan suscitarse para su empleo posterior. El análisis de contenido va encaminado a lograr que el sentido latente de los textos y discursos surja (Piñuel, 2002).

3.4.2 Hermenéutica

En cuanto a la investigación hermenéutica, ésta estudia, analiza y genera conocimiento a raíz de interpretaciones, proceso en el cual desaparece la separación entre el investigador y el objeto de investigación (Cisterna, 2005). De acuerdo a Heidegger (2005), un texto puede ser interpretado únicamente como parte de un todo y para esta interpretación se debe seguir un ciclo, conocido como círculo hermenéutico.

Como parte de las técnicas utilizadas en el presente trabajo para analizar la información, se utilizará el ciclo hermenéutico el cuál puede ser observado a continuación en la Figura 7.

Figura 7. Ciclo hermenéutico



Fuente: Elaboración propia.

3.5 Etapas de la metodología

En resumen, y como lo muestra la Tabla 1, el enfoque tomado para la elaboración de este trabajo tiene una orientación a la investigación cualitativa, con un alcance descriptivo y exploratorio. La técnica fundamental es el análisis de contenido, llevando a cabo procedimientos documentales y hermenéuticos.

Tabla 1. Cuadro metodológico

OBJETIVO GENERAL	SUPUESTOS DE INVESTIGACIÓN	OBJETIVOS ESPECÍFICOS	VARIABLE Y NIVEL DE LA VARIABLE	TÉCNICAS	RESPUESTA AL OBJETIVO ESPECÍFICO
Proponer una serie de estrategias de control interno en el área de tecnologías de la información a través de la adaptación del apartado 404 de la Ley Sarbanes Oxley, que puedan ser implementadas en empresas mexicanas del sector industrial que no	1) Tener un marco de referencia de control interno para tecnologías de la información basado en SOX disminuye las posibilidades de fraude. 2) Empresas mexicanas que utilizan tecnologías de la información para consolidar su información financiera requieren controles internos robustos.	Identificar los controles que existen alrededor del apartado 404 de la Ley Sarbanes Oxley relacionados a tecnologías de la información.	Variable: Controles de TI conexos a la Ley SOX. Nivel de la variable: Vínculo de los controles.	Documental para recabar información y análisis de contenido para analizar la información.	La Ley SOX no define los controles a seguir, propone utilizar marcos de referencia como COSO y COBIT, sin embargo, sugiere una evaluación obligatoria del control una vez al año.
		Determinar áreas de oportunidad en México para aplicar controles internos de tecnologías de la información para prevenir el fraude.	Variable: Áreas de oportunidad en México. Nivel de la variable: Contexto de las áreas.	Documental para recabar información, análisis de contenido y hermenéutico para analizar la información.	1) Separación de responsabilidades. 2) Salvaguarda de activos. 3) Acceso a sistemas de información. 4) Funcionalidad, disponibilidad,

coticen en las bolsas de valores de estados unidos y hacen uso de tecnologías de información en su proceso financiero, para reducir las posibilidades de fraude.				confiabilidad y exactitud de los sistemas de información.
	Proponer estrategias de control interno en el área de tecnologías de la información que puedan adaptarse a empresas mexicanas del sector industrial.	Variable: Estrategias de control interno de TI. Nivel de la variable: Coherencia de las estrategias de control	Documental para recabar información y hermenéutico para analizar la información.	5)Respaldo y retención de información. 1)Manejo de acceso a aplicaciones basado en roles y división de funciones. 2)Manejo de transacciones sensibles. 3)Monitoreo de conflictos. 4)Acceso físico restringido. 5)Protección contra fuga de información. 6)Otorgamiento de acceso. 7)Revisión y cancelación de acceso. 8)Manejo de contraseñas. 9)Manejo de cambios. 10)Respaldo y salvaguarda de información.

A continuación, se muestra en la Figura 8 un diagrama de flujo con las etapas llevadas a cabo en la metodología del presente trabajo de tesis, y posteriormente, se da una breve explicación de lo que comprende cada etapa.

Figura 8. Etapas de la metodología



Fuente: Elaboración propia.

La primera etapa de metodología se enfoca en la búsqueda de textos y casos de estudio relacionados con el fenómeno de investigación, donde los medios utilizados para encontrar los textos son bases de datos, libros, revistas y publicaciones en línea. Debido a la gran cantidad de textos encontrados, como segundo paso se procedió a seleccionar aquellos cuyo contenido fuera relevante con el tema estudiado y por lo tanto pudieran ser interpretados. La tercera etapa de la metodología es aquella dónde se opta por enfocarse únicamente a algunos de los textos y se descartan los demás, con la finalidad de analizar sólo aquellos que tengan mayor relevancia y concluir con esto las etapas de la metodología.

3.6 Análisis de datos

3.6.1 Alineación de la Ley SOX y el marco COSO

Empresas pequeñas, o que nunca han establecido una cultura de manejo de riesgos empresariales, pudieran tener una preocupación hacia la aplicación del marco COSO

debido a los dos volúmenes con que cuenta el reporte: uno explicando el marco de referencia y el otro guiando la implementación del marco. Si a esto le sumamos la inversión significativa de tiempo y recursos además de las complicaciones que pudieran presentarse y la falta de participación de los ejecutivos y directores, así como el cambio de cultura empresarial requerida, la implementación inicial de COSO representa el mayor reto antes de que el proceso llegue a su potencial (Ballou y Heitger, 2005).

De acuerdo a Gupta (2008), estudios anteriores han aislado una situación que abarca a muchas empresas estadounidenses, y es precisamente el hecho de que las empresas utilizan el marco de referencia COSO para dar cumplimiento con la Ley SOX en su sección 404. Igualmente, otros de sus estudios, muestran que las empresas estadounidenses suelen confiar más en auditorías de control interno que en la utilización y guía del marco de referencia COSO, lo cual podría servir de referencia a otros países para evaluar la practicidad y viabilidad de implementar reglas similares en su jurisdicción.

Dada la técnica elegida para este trabajo de investigación, la cual es el análisis de contenido, se interpretan los textos por medio de la descomposición y clasificación de los mismos, siempre tratando de buscar el sentido latente de los mismos. Por lo tanto, para efectos de esta investigación, se procedió a agrupar las ideas centrales del apartado 404 de la Ley SOX y las ideas centrales del marco de referencia COSO con la finalidad de encontrar la relación entre ambos objetos de estudio.

3.6.2 Los principios del marco de referencia COSO

Dados los procedimientos documentales seleccionados para elaborar la investigación, se parte del uso de documentos gráficos para la recopilación de información, consecuentemente, se procedió a elaborar un diagrama que mostrara los principios

fundamentales del marco de referencia COSO, obteniendo como resultado la Figura número 9. La Figura 9 muestra los cinco principios en los cuales se sustenta el marco de referencia COSO y que se clasifican en: ambiente de control interno, valoración de los riesgos; actividades de control; sistemas de información utilizados; y monitoreo.

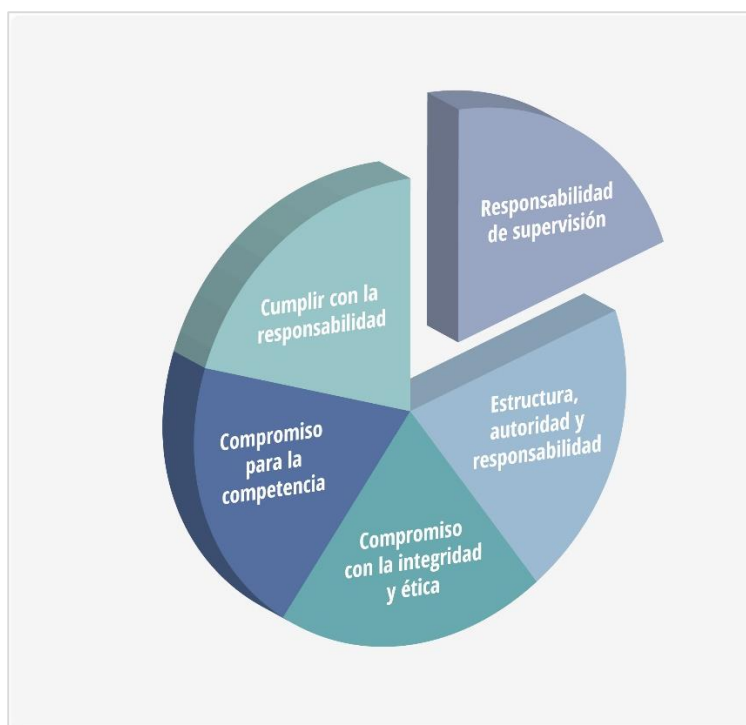
Figura 9. Principios COSO



Fuente: Elaboración propia de acuerdo al Marco de referencia COSO.

Posteriormente, y continuando con el análisis de contenido, se procedió a realizar un desglose de cada uno de los principios COSO mencionados anteriormente. A continuación, se muestra el Entorno de control en la Figura 10.

Figura 10. Entorno de control



Fuente: Elaboración propia de acuerdo al Marco de referencia COSO.

Como se aprecia en la Figura 10, el entorno de control comprende el ambiente donde se llevan a cabo las responsabilidades de control. Sus factores abarcan desde la integridad y ética de los empleados hasta la responsabilidad que tiene el gobierno corporativo en fomentar e implantar códigos de conducta aceptables para el buen comportamiento ético y moral de los empleados.

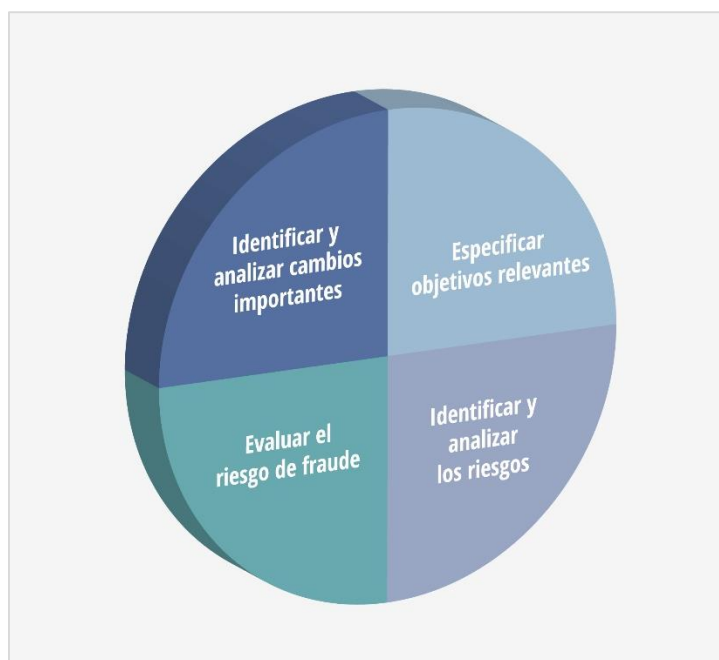
Además del compromiso con la integridad y ética, el entorno de control hace énfasis en el compromiso para la competencia profesional, entendiéndose como la capacidad de los empleados para que puedan desarrollar sus actividades y cumplan con las responsabilidades de control que les competen. Se alude, así mismo, a la importancia de

contar con descripciones de puesto formales a la par de analizar los conocimientos y habilidades de los empleados.

Hablando de la responsabilidad, se hace hincapié en que es una responsabilidad compartida el mantener un ambiente de control propicio. Por un lado, los empleados que ejecutan funciones de control están obligados a cumplir con la responsabilidad de su puesto, mientras que es responsabilidad de la organización el que los empleados cuenten con la debida supervisión para llevar a cabo sus funciones, y finalmente un Comité de Auditoría o Consejo de Administración marcarán la estructura, autoridad y también responsabilidad para la eficacia del control interno visto como un proceso.

El segundo principio COSO que se analizó fue el referente a la evaluación de riesgos, a los cuales las organizaciones deben hacer frente. A continuación, se localiza la Figura 11, donde se muestran las cuatro tareas imprescindibles a efectuar por parte de las organizaciones donde se evalúen y afronten los riesgos, tanto internos como externos.

Figura 11. Evaluación de riesgos



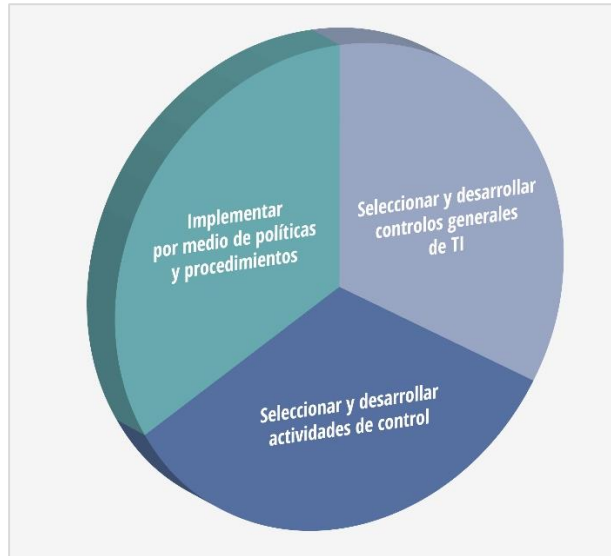
Fuente: Elaboración propia de acuerdo al Marco de referencia COSO.

Previo a la valoración de los riesgos, se deben especificar los objetivos relevantes para la empresa, abarcando los relacionados a la eficiencia y eficacia de las operaciones, los objetivos de cumplimiento de leyes y otras regulaciones como normas, y los objetivos de confiabilidad de la información financiera que genera la organización. Al establecerse los objetivos, la organización puede proceder a identificar y analizar los riesgos, ya sea a nivel general como a nivel particular de las actividades realizadas, de esta manera se facilita la valoración de riesgos en las funciones más importantes de la empresa.

Dentro de la evaluación de riesgos se encuentra la evaluación de fraude y, aunque existen diversos métodos y técnicas para identificarlo, estos varían de empresa a empresa. Por último, se recomienda que la organización identifique y analice los cambios importantes de su entorno, siempre orientándose a futuro con motivo de prevención.

Las Actividades de control son el tercer principio del marco COSO que se desglosó en tres subtemas, como lo indica la Figura 12.

Figura 12. Actividades de control



Fuente: Elaboración propia de acuerdo al Marco de referencia COSO.

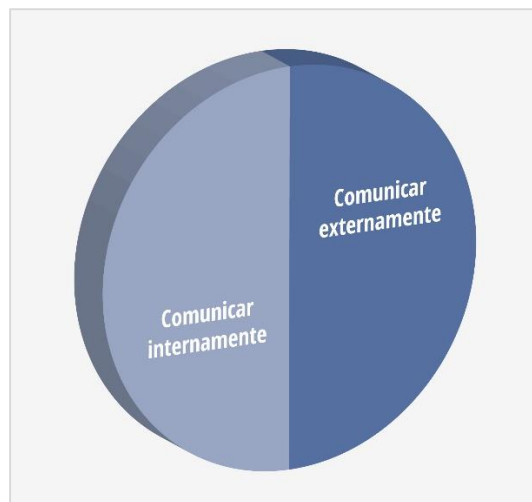
Las Actividades de Control se pueden simplificar en tres pasos, los cuales son seleccionar y desarrollar los controles referentes a las tecnologías de la información, seleccionar y desarrollar actividades que formen parte del control interno dentro de las tecnologías de la información, y, por último, implementar dichas actividades por medio de políticas que contribuyan al aseguramiento del control de riesgos.

Cabe indicar que como parte de los controles generales de TI se encuentran los controles de aplicación, los cuales se ejecutan sobre las aplicaciones o en otras palabras sobre el software que procesa la información empresarial. Se entiende entonces que, para que la información financiera sea confiable, se deben evitar los riesgos que puedan

impactarla (tales como el fraude), mediante controles de aplicaciones y controles generales de TI.

Continuando con los principios de COSO, el cuarto principio habla de los Sistemas de información, los cuales se explican a través de la Figura 13.

Figura 13. Sistemas de información



Fuente: Elaboración propia de acuerdo al Marco de referencia COSO.

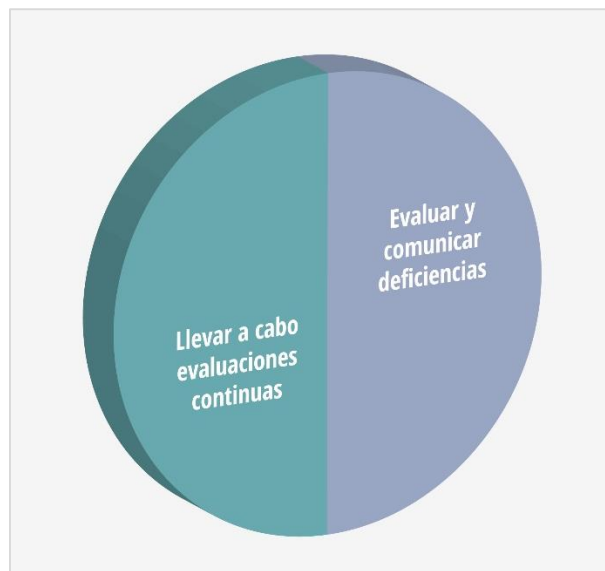
Los empleados de la organización podrán cumplir con sus responsabilidades siempre y cuando tengan en tiempo y forma la información que les compete a sus funciones. Los sistemas de información requieren comunicar eficazmente a todos las áreas y niveles de la empresa, pero es importante que cada empleado comprenda el papel que juega dentro del sistema, igualmente que los directivos y empleados de niveles superiores deben contar con la disposición de escuchar.

Si bien la comunicación interna es importante, la comunicación externa también lo es. Los usuarios externos como lo son los clientes, requieren una comunicación eficaz pero

también proporcionan información a la empresa, permitiendo que la entidad tenga conocimiento de los cambios a los que debe hacer frente.

Prosiguiendo con el cuarto principio de COSO, se realizó la Figura 14 acerca del Monitoreo del sistema de control.

Figura 14. Monitoreo del sistema de control



Fuente: Elaboración propia de acuerdo al Marco de referencia COSO.

Para comprobar el funcionamiento adecuado del sistema de control, se requiere de una evaluación continua, siempre considerando los riesgos además de la eficiencia de las personas encargadas de supervisar. Es decir, no tiene sentido evaluar un control de uso de una aplicación para realizar presentaciones con diapositivas, sin embargo, tiene sentido evaluar quién tiene acceso a modificar registros monetarios en una aplicación financiera.

Un ejemplo referente a la eficiencia de los procesos de supervisión, sería el no evaluar un control que se ha comprobado es deficiente y aún no se remedia, ya que esto representaría únicamente tiempo perdido para los evaluadores, sin embargo, tendría sentido el incentivar al responsable del control para que la remediación ocurra lo más pronto posible.

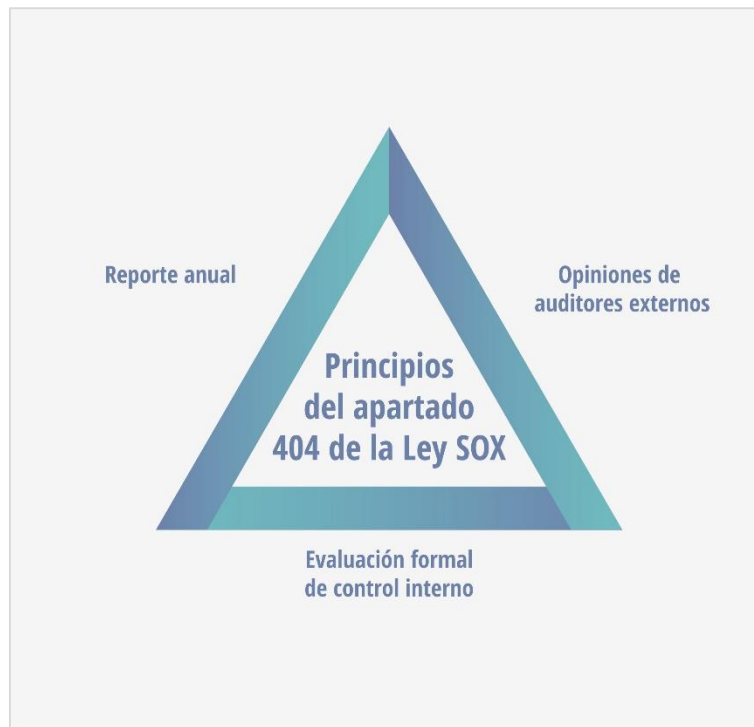
En la Figura 14 se muestra también que los resultados obtenidos por medio de las valoraciones al sistema de control deben ser siempre comunicados a los responsables del control cuando el control sea deficiente. Asimismo, las deficiencias deberán ser evaluadas una vez que el responsable de control notifique su remediación para comprobar que efectivamente el control es efectivo.

Como conclusión al análisis del marco de referencia COSO, se puede decir que las empresas que lo toman como base se enfocan a la ejecución de un control interno efectivo que prevenga riesgos y simultáneamente impulsan la mejora continua, favoreciendo la consecución de objetivos empresariales.

3.6.3 Los principios del apartado 404 de la Ley SOX

Prosiguiendo con el análisis de contenido y de acuerdo a los procedimientos documentales seleccionados, se partió del uso de documentos gráficos para la compilación de información y se procedió a elaborar un diagrama que muestra los tres principios fundamentales del apartado 404 de la Ley SOX, obteniendo como resultado la Figura 15.

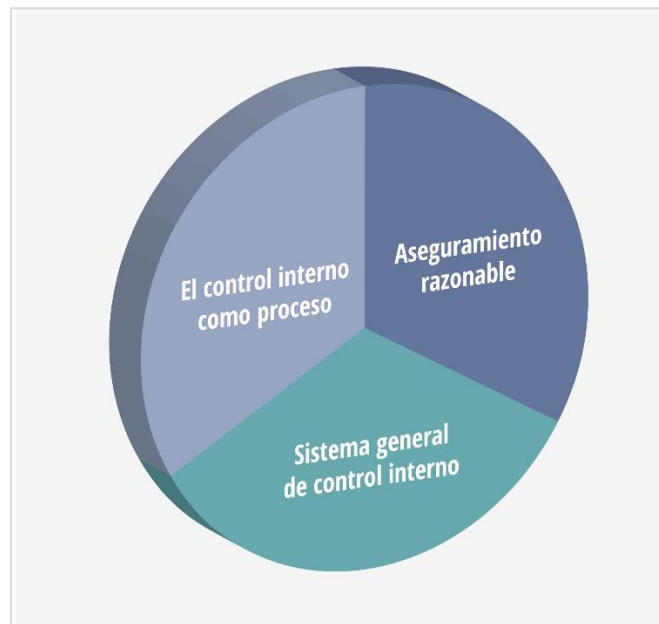
Figura 15. Principios del apartado 404 de la Ley SOX



Fuente: Elaboración propia de acuerdo al apartado 404 de la Ley SOX.

Posteriormente, se continúa con el desglose de los principios mencionados anteriormente. A continuación, se muestra la Evaluación formal de control interno, por medio de la Figura 16.

Figura 16. Evaluación formal de control interno



Fuente: Elaboración propia de acuerdo al apartado 404 de la Ley SOX.

Las empresas que cotizan en las bolsas de Estados Unidos deben establecer controles y procedimientos internos para la información financiera al mismo tiempo de documentar, probar y mantener esos controles y procedimientos para asegurar su efectividad. El propósito es reducir las posibilidades de fraude corporativo aumentando la rigurosidad de los requisitos fundamentales para generar información financiera, así como de los procedimientos en torno a la generación de la misma.

La gerencia de la empresa es responsable del control interno, y en ningún momento es responsabilidad de los evaluadores, ya sean auditores internos o externos, ni tampoco del departamento de finanzas. Sin embargo, el control interno visto como un proceso, es una tarea conjunta donde deben participar tanto la gerencia, como finanzas y el director general de la organización. El sistema general de control interno debe estar basado en

un marco de referencia reconocido en el ámbito de tecnologías de la información, se pueden mencionar COSO y COBIT como ejemplos.

En cuanto al aseguramiento razonable, éste pretende cumplir con tres categorías de objetivos, siendo la primera categoría la de los objetivos comerciales. Los objetivos comerciales primordiales de una organización engloban a su vez a las expectativas de rendimiento, rentabilidad y protección de recursos. En la segunda categoría de objetivos, se encuentra la preparación de declaraciones financieras confiables y datos financieros derivados de dichas declaraciones, tales como los informes de ganancias, que deben ser informados públicamente. Finalmente, la tercer y última categoría de objetivos trata de cumplir las regulaciones, incluidas las leyes, a las que la entidad está sujeta.

El segundo principio del apartado 404 de la Ley SOX establece que anualmente se efectúe un reporte de evaluación hacia los sistemas de control. Esto se traduce en una valoración de todos los procesos llevados a cabo por los administradores y equipo de soporte del software utilizado para producir la información financiera, teniendo como propósito el comprobar que tan efectiva es su protección ante los riesgos que pudieran presentarse. La evaluación debe ser terminada al final del año en curso y ésta podrá tener restricciones en su ejecución, dependiendo de las vulnerabilidades identificadas.

Por último, el tercer principio del apartado 404 de la Ley SOX habla de las dos opiniones que los auditores externos deben emitir como parte de una sola auditoría integrada sobre una empresa. La primera opinión será en relación al control interno sobre los reportes financieros, mientras que la segunda opinión será enfocada a la parte financiera, siendo ésta la opinión tradicional sobre los resultados financieros.

3.6.4 Relación COSO – apartado 404 de la Ley SOX

Como una derivación de las técnicas hermenéuticas y análisis de contenido, se identificó la intersección entre la sección 404 de la Ley SOX y el marco de referencia COSO, la cual puede observarse en la Figura 17.

Figura 17. Confluencia SOX-COSO



Fuente: Elaboración propia de acuerdo al apartado 404 de la Ley SOX y el marco de referencia COSO.

Si bien la sección 404 de la Ley SOX establece primordialmente la obligación que tienen las organizaciones de mantener políticas y procedimientos enfocados a mantener íntegra la información, simultáneamente la evaluación formal al sistema de control interno es fundamental ya que es esta evaluación la que permite dar un aseguramiento razonable sobre la efectividad que tiene la información financiera que es originada por medio de los

sistemas de información. En cuanto a COSO, se propone monitorear y supervisar constantemente los controles internos para evitar desviaciones en relación a objetivos previamente establecidos.

Este monitoreo y supervisión constantes, son un proceso que deberá tener una frecuencia y alcance establecidos considerando la magnitud de los riesgos asociados con cada control interno, además al momento de valorar el sistema de control, se tendrá que considerar las metas que se requieran cumplir tales como objetivos operacionales, financieros o simplemente de cumplimiento.

Se puede decir entonces que tanto SOX como COSO consideran la valoración de los controles internos como un elemento primordial. La forma en que los controles internos son aplicados suele cambiar con el tiempo, así como los procesos y procedimientos pueden perder su eficacia o incluso dejar de llevarse a cabo. Por lo tanto, el tener una supervisión del control interno, se podrá identificar la capacidad que tiene la empresa para enfrentar riesgos.

Por un lado, y de acuerdo a COSO, el modelo de supervisión tiene como base un punto de referencia que permite identificar que se considera como efectividad del control interno. Partiendo de un ámbito de TI y haciendo una alineación con SOX, este punto de referencia sería la prevención de fraude en los estados financieros y la detección del mismo, en otras palabras, el punto de referencia es la preservación de la confiabilidad que manejan los sistemas de información que pueda afectar a los reportes financieros empresariales. Una vez que se identifica la base del modelo de supervisión, se puede proceder a identificar y priorizar riesgos para entonces diseñar los controles (estrategias) que se deberán llevar a cabo.

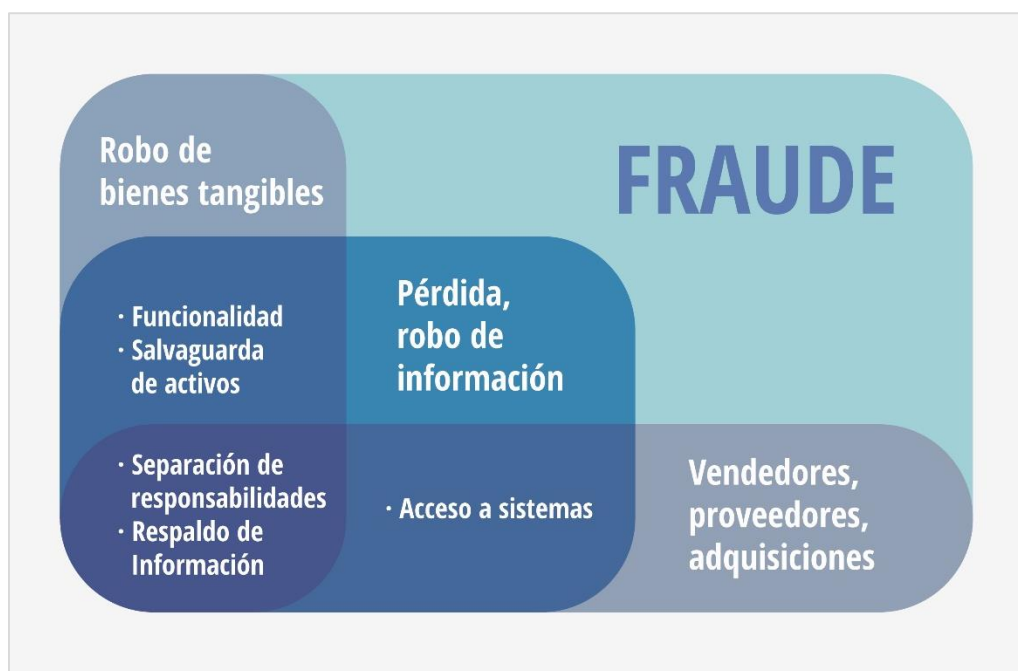
4. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

4.1 Resultados

Como se menciona en el capítulo dos, de acuerdo al reporte global de Fraude Kroll para el año 2016, México se ha enfrentado a diversos casos de fraude donde sobresalen: el robo de bienes tangibles; el robo de información, pérdida o ataque; y el fraude ocasionado por vendedores, proveedores o por adquisiciones. Tomando en cuenta dicha información, se realizó un análisis (ver Tabla 1) donde se identificaron las áreas de oportunidad para México en donde podrían aplicarse estrategias de control interno en el campo de TI para prevenir los tipos de fraudes mencionados.

Como parte de la interpretación de los resultados del estudio, se observó la relación entre los tres casos más comunes de fraude en México y las cinco áreas clave donde se pueden aplicar estrategias de control interno. Se observó que ninguna de las áreas clave puede por sí sola combatir los tres tipos de fraude, por lo tanto, el conjunto de las cinco áreas clave representa un esfuerzo con mayor cobertura hacia los fraudes habituales. Se procedió a realizar una figura que representa visualmente dicha relación, dando como resultado la Figura 18.

Figura 18. Relación entre fraudes más comunes en México y áreas clave para empresas mexicanas.



Fuente: Elaboración propia.

En la Figura 18 se observa en color azul cielo la representación de los diversos fraudes que existen y de todos ellos se separan los tres tipos más comunes en México. A cada uno de los tres fraudes se le asignó una tonalidad de azul más oscuro, asociando uno de ellos con el robo de bienes tangibles; otro tono con el robo de información, pérdida o ataque; y el fraude ocasionado por vendedores, proveedores o por adquisiciones con un tono más de azul.

Dado que algunas áreas clave explicadas en el capítulo tres se asocian con más de un fraude, se intersecan los fraudes dando como resultado una variación de color diferente y se colocaron los nombres de las áreas dentro de las intersecciones. El área clave referente a la funcionalidad, disponibilidad, confiabilidad y exactitud de los sistemas de información, se agrupó en el mismo cuadrante que la salvaguarda de activos tangibles

e intangibles, cuadrante donde cruzan los fraudes de robo de bienes tangibles y el robo de información, pérdida o ataque.

Para el cuadrante que cruza con los fraudes de robo de bienes tangibles y proveedores, vendedores o adquisiciones, se colocaron las áreas de separación de responsabilidades y respaldo y salvaguarda de información. Por último, el área referente al acceso a los sistemas de información se colocó en el cruce de los fraudes robo de información, pérdida o ataque y proveedores, vendedores o adquisiciones.

A continuación, la Tabla 2 muestra las áreas clave para prevenir los fraudes más comunes en México, las cuales se identifican como: la separación de responsabilidades correspondiente, la salvaguarda de activos, el aseguramiento de la propia configuración de los sistemas de información, el aseguramiento del debido acceso a los sistemas de información, el aseguramiento de la funcionalidad y/o disponibilidad y/o confidencialidad y/o exactitud de los sistemas de información, el respaldo y retención de la información.

Tabla 2. Controles internos de TI en áreas clave para empresas mexicanas

ÁREA CLAVE	RIESGO	ESTRATEGIAS (CONTROLES INTERNOS)	OBJETIVO DEL CONTROL
SEPARACIÓN DE RESPONSABILIDADES	La falta de procedimientos para una separación de responsabilidades en los sistemas donde intervienen actividades que impactan a los estados financieros, así como su monitoreo puede resultar en fraude por parte de vendedores, proveedores o adquisiciones; robo de bienes tangibles; y robo, pérdida o ataque de información.	1.-Manejo de acceso a aplicaciones basado en roles y división de funciones. 2.-Manejo de transacciones sensibles. 3.-Monitoreo de conflictos.	Asegurar la existencia de procedimientos formales de separación de responsabilidades en los sistemas donde intervienen actividades que impactan a los estados financieros, así como asegurar el apego a reglas y la

			ejecución de monitoreo que reduzcan las posibilidades de acceso a sistemas que puedan permitan a un individuo perpetrar un fraude.
SALVAGUARDA DE ACTIVOS TANGIBLES E INTANGIBLES	La falta de procedimientos para la salvaguarda de activos puede resultar en robo de bienes tangibles además de fraude cibernético por robo de información, pérdida o ataque.	1.-Acceso físico restringido. 2.-Protección contra fuga de información.	Asegurar la existencia de procedimientos formales y periódicos orientados a la salvaguarda de los activos tanto tangibles como intangibles, que protejan a la organización de la malversación de activos.
ACCESO A LOS SISTEMAS DE INFORMACIÓN	La falta de procedimientos formales de acceso a los sistemas donde intervienen actividades que impactan a los estados financieros, así como una apropiada configuración de contraseñas, puede resultar en acceso a los sistemas no autorizado impactando confidencialidad, exactitud, y disponibilidad de la información, así como de los sistemas mismos, además de incrementar el riesgo de fraude de vendedores, proveedores o adquisiciones y robo, pérdida o ataque de información.	1.-Otorgamiento de acceso. 2.-Revisión y cancelación de acceso. 3.-Manejo de contraseñas.	Asegurar la existencia de procedimientos formales de manejo de acceso y configuración de contraseña a los sistemas que intervienen en actividades que impactan a los estados financieros, así como asegurar el monitoreo de acceso periódico, que reduzcan las posibilidades de que se acceda a los sistemas sin autorización.
FUNCIONALIDAD, DISPONIBILIDAD, CONFIABILIDAD Y EXACTITUD DE LOS SISTEMAS DE INFORMACIÓN	La falta de procedimientos formales de configuración, y manejo de cambios y problemas, puede dar lugar a cambios no autorizados que pudieran afectar la	1.-Manejo de cambios	Asegurar la existencia de procedimientos formales en los sistemas donde intervienen

		funcionalidad o la disponibilidad del sistema, así como la integridad de los datos financieros, además de poder resultar en la corrupción de los datos o fraude por robo, pérdida o ataque de información.			actividades que impactan a los estados financieros para asegurar la funcionalidad, disponibilidad, confiabilidad y exactitud de los sistemas y los datos financieros.
RESPALDO RETENCIÓN INFORMACIÓN	Y DE	La falta de procedimientos formales de respaldo y retención de información puede afectar la disponibilidad y precisión de los sistemas de información críticos en caso de interrupción en las operaciones normales de la organización, así como incrementar las posibilidades de fraude de vendedores, proveedores o por adquisiciones y posibilidades de robo, pérdida o ataque de información.	1.-Respaldo salvaguarda información.	y de	Asegurar la existencia de procedimientos formales de respaldo y retención de información en los sistemas donde intervienen actividades críticas que impactan a los estados financieros.

4.2 Análisis de resultados

A pesar de que la Figura 18 no muestra las estrategias (controles) correspondientes a cada área clave, se esclarece cada una de ellas en los párrafos siguientes.

Área 1. Separación de Responsabilidades

Dentro del área de Separación de Responsabilidades, se establecieron tres estrategias que trabajan bajo el mismo objetivo (mencionado en el capítulo tres), las cuales se explican a continuación.

- **Manejo de acceso a aplicaciones basado en roles y división de funciones.**

Con la finalidad de prevenir el abuso de operaciones críticas dentro de un proceso, las responsabilidades dentro de una organización deben estar separadas (división de funciones) pero, primeramente, los conflictos deben ser identificados. Uno de los caminos para identificar los conflictos es precisamente realizar un análisis de los privilegios asignados a un usuario en los sistemas de información utilizados por la empresa.

Posterior al análisis, las combinaciones de privilegios, también llamadas roles, dentro de la aplicación que causan conflictos se pueden separar o en última instancia mitigar. Un ejemplo son las aplicaciones de software de Oracle que cuentan con una función de seguridad donde se controla el acceso de los usuarios mediante roles que están restringidos, de igual manera los derechos de los usuarios sobre los procesos son gestionados mediante privilegios.

- **Manejo de transacciones sensibles en los sistemas de información.**

Todas las empresas tendrán una opinión diferente sobre lo que es una transacción sensible o crítica, aunque probablemente coincidan en algunas de esas transacciones. El manejo de transacciones sensibles incluye la operación y supervisión de transacciones individuales que corren a lo largo de la infraestructura de una aplicación.

Algunos sistemas intentan realizar un seguimiento de las transacciones insertando un identificador único en cada solicitud de etiqueta mientras que otros usan la información única dentro de cada solicitud del sistema para armar la transacción. El monitoreo de transacciones proporciona al equipo de operaciones la capacidad de asignar sistemas comerciales específicos, por ejemplo, todos los componentes que componen un sistema bancario en línea o una aplicación de administración de inventario, por mencionar algunos.

La mejor representación de este control se encuentra en los sistemas SAP. En el mundo de SAP, un t-code es un conjunto de cuatro dígitos que dan acceso directo a diversas transacciones, así cuando un usuario tiene acceso a un t-code crítico, como lo es FI12 para realizar cambios en cuentas bancarias, el usuario podría hacer modificaciones que en caso de no estar autorizadas y no ser monitoreadas, el impacto a la empresa puede ser perjudicial. Por lo mismo, los sistemas SAP permiten a los administradores del sistema limitar el acceso a las transacciones, de manera que los t-codes no siempre autorizan derechos de escritura, únicamente lectura.

- **Monitoreo de conflictos.**

El control cubre que los conflictos potenciales de Separación de Responsabilidades sean monitoreados y revisados y que la administración confirme que cualquier conflicto, si llegara a presentarse, esté vinculado a los controles de mitigación previamente aprobados por la misma administración suponiendo que el conflicto no pueda ser remediado.

Para aplicaciones donde no exista una configuración de separación de Responsabilidades, las cuentas, roles, o perfiles activos en el sistema deberán ser consistentes con las reglas que cuenta la aplicación. Todos los conflictos deberán ser monitoreados y deberá guardarse el reporte del monitoreo, así como las acciones tomadas, por un plazo sugerido de mínimo un año.

Como un ejemplo, supongamos que una empresa utiliza algún software de administración de presupuesto donde la persona que solicita la autorización para el uso de cierta cantidad significativa de dinero es también la persona que se encarga de aprobar la solicitud. En este caso, se puede identificar el conflicto de separación de responsabilidades ya que pudiera presentarse el caso donde la persona que solicita y

aprueba el uso de ese dinero participe en un fraude de adquisiciones, por mencionar un tipo de fraude.

Área 2. Salvaguarda de Activos Tangibles e Intangibles

Dentro del área de Salvaguarda de Activos Tangibles e Intangibles, se establecieron dos estrategias, las cuales son: Acceso físico restringido, y protección contra fuga de información. Cada una de las estrategias se explica en los párrafos siguientes.

- **Acceso físico restringido.**

Mientras que el acceso lógico se refiere a las conexiones a redes de computadoras, archivos de sistema y datos, el acceso físico habla del acceso a edificios, salas, áreas y activos de TI. La restricción del acceso físico, es una parte cubierta por los controles internos de acceso a las instalaciones de las empresas, donde se restringe de manera selectiva el acceso a un espacio.

Algunos ejemplos de control de acceso físico son las puertas controladas por el control remoto y puertas con lector de identificación por radiofrecuencia. Además, existen diversas aplicaciones que llevan un registro de las entradas y salidas por medio de la información enviada por los lectores, lo cual ayuda a identificar las personas ya sean empleados o visitantes, que entran y salen del lugar, incluyendo la fecha, hora y tiempo que permanecen.

- **Protección contra fuga de información.**

A pesar de que la información pudiera, en algún momento dado, presentar fugas de manera accidental, hay posibilidades de un suceso planeado que además afecte económicamente a la empresa o a su reputación. En la parte técnica para la prevención de fugas de información, entran las herramientas que detectan y previenen la fuga de

información. Independientemente de que tamaño tenga la empresa, se sugiere considerar utilizar software que facilite el cifrado de información, instalación y actualización de cortafuegos, además de actualizar las aplicaciones cada que se necesite.

Otro ejemplo de cómo proteger la fuga de información es la utilización de software DLP, el cual va enfocado precisamente a la prevención de pérdida de datos además de su monitoreo y control, sin embargo, este software suele tener un enfoque avanzado y consecuentemente requiere que las entidades tengan grandes recursos económicos que sustenten su uso.

Área 3. Acceso a los Sistemas de Información

Para el área clave de Acceso a los Sistemas de Información, se establecieron tres estrategias: Otorgamiento de acceso, revisión y cancelación de acceso, manejo de contraseñas. Dichas estrategias se explican a continuación.

- **Otorgamiento de acceso.**

La estrategia se refiere a los procesos alrededor del otorgamiento de acceso a las aplicaciones únicamente a usuarios no autorizados. Por ejemplo, un nuevo empleado al llegar a laborar a la empresa se le otorga acceso a todas las aplicaciones manejadas por la empresa independientemente de que tengan relevancia para su puesto, se estaría poniendo en riesgo a la empresa ya que no existiría una barrera que previniera el uso indebido de la información.

Además, suponiendo que la empresa lleva a cabo un proceso donde el superior del empleado autorizara la solicitud hecha por el mismo empleado para acceder a alguno de los sistemas de información y posteriormente el equipo o individuo encargado de otorgar

el acceso validara la solicitud, la empresa estaría siguiendo un control sobre el acceso lógico a los sistemas de información en su otorgamiento.

- **Revisión y cancelación de acceso.**

Es importante mencionar que, aunque el control de otorgamiento de acceso es importante, si el acceso con el que cuentan los usuarios no es revisado periódicamente ni cancelado cuando ya no se requiera, la empresa queda expuesta nuevamente a la posibilidad de acceso de usuarios no autorizados a sus aplicaciones y por lo tanto queda expuesta a un mal uso de información.

Supóngase que, un antiguo empleado de la empresa cuyo acceso a un software administrador de gastos no fue removido una vez que el usuario dejó de laborar en la empresa, a sabiendas de la situación toma ventaja y logra entrar al sistema y realiza movimientos que le benefician económicamente. En este caso, la empresa habrá sido víctima de fraude.

- **Manejo de contraseñas.**

Todo usuario requiere una clave de ingreso (contraseña) para los sistemas de información que sólo él mismo usuario y el administrador del sistema podrán cambiar, a la vez que la contraseña debe cumplir con ciertos requisitos de complejidad previamente establecidos. Por otro lado, a empresa deberá inculcar una cultura de uso personal de las claves de acceso o en otras palabras de no compartir las mismas con nadie, esto para evitar que usuarios no autorizados a ingresar a los sistemas lo hagan.

Área 4. Funcionalidad, Disponibilidad, Confiabilidad y exactitud de los Sistemas de Información

Dentro del área de funcionalidad, disponibilidad, confiabilidad y exactitud de los sistemas de información, se estableció una estrategia: Manejo de cambios.

- **Manejo de cambios.**

En ciertas ocasiones, las aplicaciones requieren cambios ya sea para mejorar su desempeño o hacer frente a transformaciones que la empresa está teniendo. Existiendo un proceso para planificar, probar, aprobar, e implementar el cambio, además de documentarlo, el proceso reduce las posibilidades de cambios no autorizados y garantiza que los cambios a los sistemas sean implementados en un ambiente administrado. Como se menciona en el capítulo tres a través de un ejemplo de un sistema SAP, un fallo al aprobar, probar y realizar correctamente cambios en el sistema, podría resultar en un fraude.

Área 5. Respaldo y Retención de Información

Por último, dentro del área respaldo y retención de información, se estableció una estrategia. La cual es el Respaldo y salvaguarda de información, misma que se encuentra explicada en las líneas siguientes.

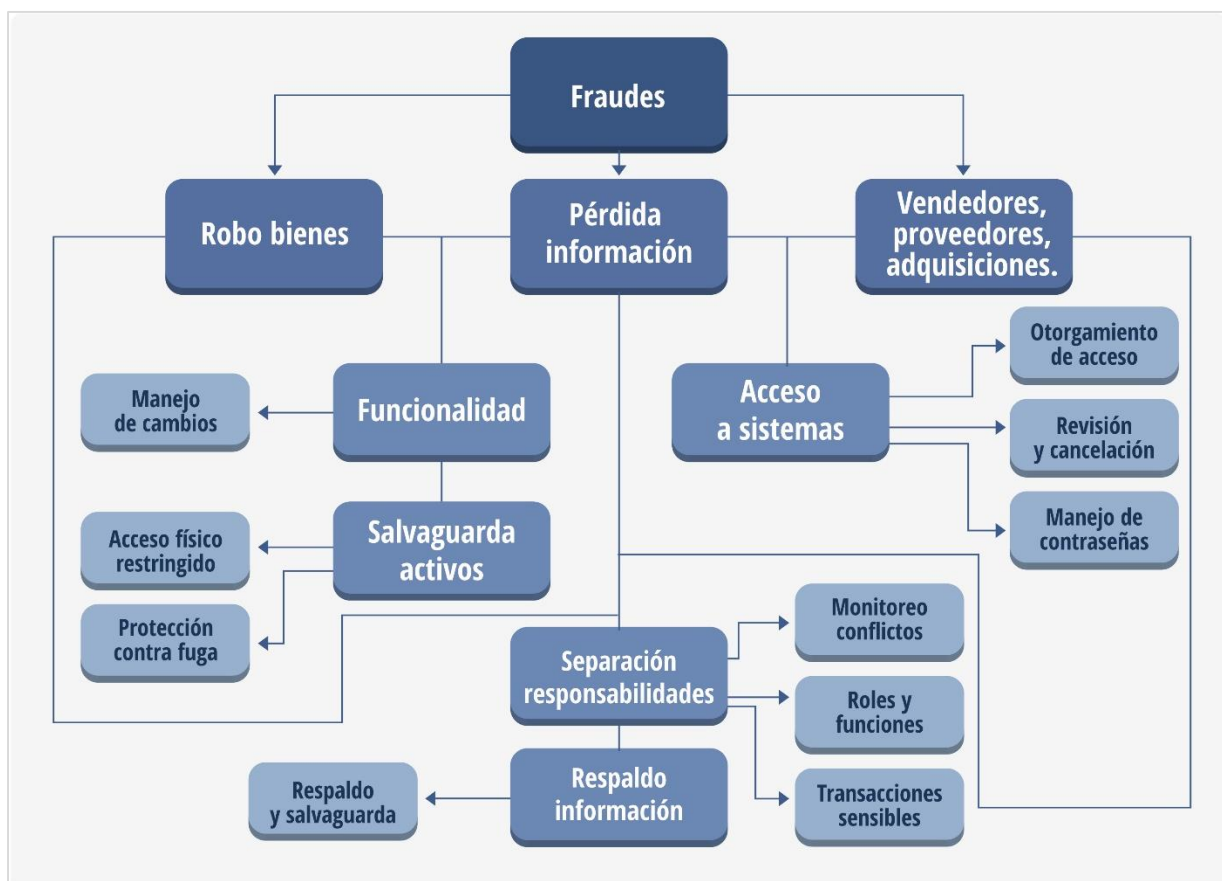
- **Respaldo y salvaguarda de información.**

Contar con una política de salvaguarda de copias de seguridad para toda aquella información considerada como sensible, ayudará a tener determinado el lapso de retención de los datos, los medios permitidos de almacenamiento, acceso y protección. En algunos casos, como el fraude, será importante examinar criterios tales como cuándo

se accedió por última vez a los datos y el tipo de datos, por lo tanto, implementar procesos alrededor del respaldo de la información son necesarios.

Para finalizar con lo propuesto, se muestra en la Figura 19 una breve síntesis de los resultados anteriormente expuestos.

Figura 19. Relación entre fraudes más comunes en México, áreas clave y estrategias de control propuestas.



Fuente: Elaboración propia.

4.3 Aplicación a una empresa en México

Para ejemplificar lo anteriormente expuesto, a continuación, se detalla una aplicación a una empresa multinacional con filial en México. Una empresa multinacional con filiales en cinco estados de México, dedicada a la producción de diversos bienes de consumo y sistemas aeroespaciales, debe demostrar a organizaciones externas el cumplimiento de requisitos contractuales y normativos. Asimismo, la empresa tiene la responsabilidad de garantizar la conservación de contratos existentes y ganancia de nuevos contratos, mientras que gestiona el riesgo de diversos departamentos incluido el de Tecnologías de la Información.

Particularmente, el área de Tecnologías de la Información, está legalmente obligado a cumplir con siete marcos de control, entre ellos la Ley Sarbanes Oxley. El gobierno corporativo se encargó en un momento dado, de asegurar la creación de políticas, estándares y líneas de base que cumplieran con los siete marcos de control, basándose en el marco de referencia COSO. Al cumplir con las políticas, estándares y líneas de base de la empresa, todas las obligaciones se cumplirían además de que impulsarían a los sistemas de información para que pudieran realizar plenamente los beneficios y objetivos de optimización de recursos y riesgos.

Recordando cómo se menciona en los párrafos anteriores que las compañías desarrollan, implementan y monitorean sistemas de información a través de políticas, procedimientos, prácticas y estructuras organizacionales para abordar ciertos riesgos, cabe resaltar que este control interno está designado para proporcionar cierto grado de seguridad sobre el logro de objetivos del negocio y se evitarán o detectarán y corregirán los eventos no deseados, consiguientemente, la auditoría es conveniente.

Siendo la empresa en cuestión consciente de la importancia de contar con un equipo de auditoría, se crea un equipo de auditores internos exclusivamente dedicados al área de Tecnologías de la Información, y cumpliendo con uno de los requerimientos de la Ley SOX, se contrata el servicio de auditoría externa proveniente de una de las firmas de auditores más importantes a nivel internacional.

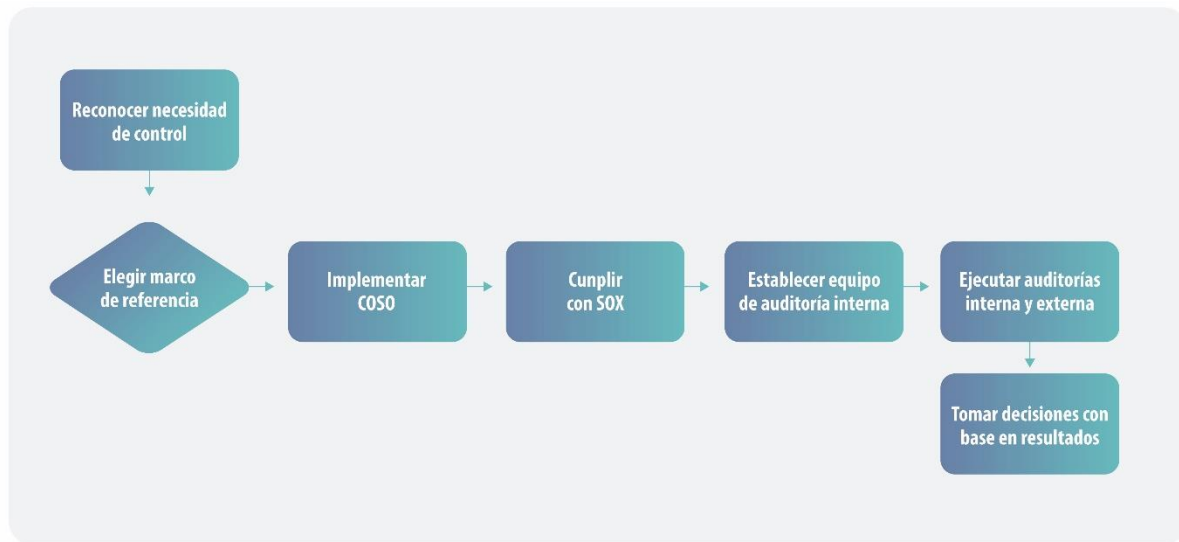
Una vez que el alcance y objetivos de los servicios otorgados por la empresa externa están documentados en un contrato formal, los equipos internos y externos de auditoría financiera (existentes previos al equipo de auditores de TI) determinan el alcance que deberá tener la auditoría del año en curso. Al terminar, obtienen aprobación por parte de la junta de directores y el comité de auditorías, posteriormente el alcance es compartido con los equipos de auditoría de TI interno y externo.

Los auditores de TI internos elaboran los documentos que deberán utilizar para valorar la efectividad de los controles internos de TI implementados por la compañía. Se encargan de incluir pruebas que determinen el acatamiento de los sistemas de información con la Ley SOX y que identifiquen si los sistemas de información cuentan con niveles apropiados de confidencialidad, integridad y disponibilidad de datos e información manejados por los sistemas.

Una vez que comienza el ciclo de auditoría, los responsables de que se lleven a cabo los controles internos proporcionan a los auditores una explicación de los procesos de control implementados y proveen la evidencia solicitada por los auditores para que éstos últimos lleven a cabo las pruebas necesarias.

Ver la Figura 20 para una representación gráfica del proceso, en términos generales, llevado a cabo por la empresa en cuestión.

Figura 20. Proceso general de una empresa en México que sigue SOX y COSO



Fuente: Elaboración propia.

Si bien el caso de la empresa que se describe en el presente capítulo no es una empresa mexicana y sí cotiza en la bolsa de valores de E.U.A., cuenta con dos criterios planteados en el alcance de este trabajo de investigación, la empresa pertenece al sector industrial y hace uso de programas de software en su proceso financiero.

Suponiendo que la tenacidad de los controles internos de TI requiriera incrementarse, las estrategias presentadas en el capítulo cuatro pudieran ser adoptadas, siempre y cuando se considerara que ninguna de las áreas clave por sí sola lograría combatir los tres tipos de fraude identificados en este trabajo y que las necesidades del negocio pueden ser mayores a las que se cubrirían implementando las estrategias aquí descritas. Los siguientes párrafos ejemplifican dos estrategias de control propuestas en este trabajo y como podrían ser implementadas por la empresa señalada.

Comenzando con la estrategia referente al acceso físico restringido, la empresa en cuestión ya cuenta con puertas que permiten únicamente la entrada a las oficinas a

empleados, esto a través de tarjetas asignadas a los empleados y lectores de identificación por radiofrecuencia, además de tener vigilantes y cámaras de seguridad. Debido a la obligación de la empresa ante la Ley SOX, se lleva a cabo un control únicamente de las entradas y salidas a los cuartos donde se encuentran los servidores de aplicaciones con alcance SOX. Esto deja a la empresa expuesta a dos de los fraudes más comunes en México: robo de bienes tangibles, y robo y pérdida de información.

Si se implementara la estrategia propuesta, como complemento al control actualmente efectuado, se llevaría a cabo un acceso físico restringido que incluyera un registro y monitoreo de todas las entradas y salidas al área de TI, incluyendo a los almacenes donde se guarda todo el hardware que no está siendo utilizado o que aún no ha sido asignado a algún empleado o departamento. Ver figura 21 para una comparación entre el Acceso restringido actualmente en la empresa y la propuesta que se hace.

Figura 21. Comparación del acceso físico restringido en una empresa en México



Fuente: Elaboración propia.

Como un segundo ejemplo, se toma la estrategia referente a monitoreo de conflictos. Al ser una empresa de gran tamaño y con presencia global, se cuenta con diversos sistemas ERP a lo largo del mundo de los cuales sólo algunos son considerados como críticos y por ende, solo los sistemas críticos forman parte del alcance cubierto por los auditores de TI.

Tomando en cuenta que existen sistemas ERP y algunos otros programas financieros de software utilizados exclusivamente por las filiales en México, la estrategia de monitoreo de conflictos se les pudiera implementar también a ellos. De esta forma, los conflictos potenciales de Separación de Responsabilidades exclusivos de las oficinas de

México serían monitoreados, revisados, corregidos, y existirían controles de mitigación en caso de ser necesarios. Ver figura 22 para una comparación entre el Monitoreo de conflictos actualmente y la propuesta.

Figura 22. Comparación del monitoreo de conflictos en una empresa en México



Fuente: Elaboración propia.

4.4 Recomendaciones futuras

Dado que las empresas difieren una de otra, se sugiere tomar en cuenta los siguientes puntos:

Se sugiere que las empresas evalúen la viabilidad de llevar a cabo las estrategias descritas en este trabajo. Empresas que no forman parte del objetivo de investigación de

este trabajo, pueden analizar si alguna de las estrategias aquí propuestas les puede ser de utilidad. Se deberá considerar el tiempo, esfuerzo y presupuesto necesario para implementar las estrategias para identificar que tiene mayor impacto, las posibilidades de fraude o implementar las estrategias.

A pesar de que se recomienda un enfoque considerando las cinco áreas, habrá empresas que no tengan posibilidades de enfocar sus esfuerzos a todas las áreas, por lo tanto, sería conveniente que priorizaran la Separación de responsabilidades antes que cualquier otra área. En caso de implementar alguna de las estrategias, las empresas deberán desarrollar controles específicos que apliquen a su caso particular.

Es importante recalcar que, aunque este trabajo considera cinco áreas fundamentales, cada una de las empresas deberá realizar un análisis de riesgos correspondiente para identificar si las áreas propuestas en este trabajo cubrirán sus necesidades. Se recomienda incluso indagar a cerca de la elaboración de una matriz de riesgos y como se pudiera implementar en la empresa. Como lo indica el marco de referencia COSO, la administración del riesgo empresarial es primordial.

Se sugiere para las futuras investigaciones en relación al objeto de estudio de este presente trabajo, contrastar las áreas clave con los fraudes de mayor recurrencia en el ámbito de estudio, considerando sector comercial, tamaño de las empresas y ubicación geográfica, esto con la finalidad de obtener resultados mejor encaminados a la situación particular de las empresas que se pretenden beneficiar de los resultados de investigación.

Sería interesante enfocarse en el caso de una empresa particular para llevar la investigación más allá de estrategias generales, y proponer una serie de procesos específicos para cada control identificado. En caso de abundar en la investigación, se

podría proseguir a una observación directa a cerca de la efectividad de las estrategias y procesos de control implementados.

CONCLUSIONES

Cumpliendo con el objetivo general del estudio, se propuso una serie de diez estrategias de control interno en el área de Tecnologías de la Información como lo muestra la Tabla 2 (1.-Manejo de acceso a aplicaciones basado en roles y división de funciones, 2.-Manejo de transacciones sensibles, 3.-Monitoreo de conflictos, 4.-Acceso físico restringido, 5.-Protección contra fuga de información, 6.-Otorgamiento de acceso, 7.-Revisión y cancelación de acceso, 8.-Manejo de contraseñas, 9.-Manejo de cambios, 10.-Respaldo y salvaguarda de información.), divididas en cinco áreas determinadas que van encaminadas a la prevención de los tres fraudes más comunes en México al momento del estudio.

La propuesta se realizó a través de la adaptación del apartado 404 de la Ley Sarbanes Oxley y considerando específicamente a las empresas mexicanas del sector industrial que no cotizan en las bolsas de valores de Estados Unidos y hacen uso de tecnologías de información en su proceso financiero.

Se alcanzaron los objetivos específicos al identificar que el apartado 404 de la Ley Sarbanes Oxley no define controles en el área de tecnologías de la información pero sugiere basarse en marcos de referencia como COSO o COBIT; se determinaron las áreas de oportunidad en México en materia de controles internos de Tecnologías de la Información para prevenir el fraude; y, por último, las estrategias de control interno

propuestas en la Tabla 2 (1.-Manejo de acceso a aplicaciones basado en roles y división de funciones, 2.-Manejo de transacciones sensibles, 3.-Monitoreo de conflictos, 4.- Acceso físico restringido, 5.-Protección contra fuga de información, 6.-Otorgamiento de acceso, 7.-Revisión y cancelación de acceso, 8.-Manejo de contraseñas, 9.-Manejo de cambios, 10.-Respaldo y salvaguarda de información.), fueron previstas para su adaptabilidad a empresas mexicanas del sector industrial.

De los resultados obtenidos, se deriva que las empresas con operaciones en México están expuestas al fraude como uno de sus problemas más serios, siendo tres tipos de fraude los más comunes al momento del estudio: el robo de bienes tangibles; el robo de información, pérdida o ataque; y el fraude ocasionado por vendedores, proveedores o por adquisiciones.

Simultáneamente, la Ley SOX y el marco COSO coinciden en que la evaluación de los controles internos es indispensable para las organizaciones para detectar su capacidad ante los riesgos. Entonces, si una organización lleva a cabo controles internos capaces de hacer frente a riesgos como el fraude, las posibilidades de que la organización experimentara un problema de este tipo se verían reducidas.

El área de TI se considera un área fundamental que deberá contar con controles internos que puedan prevenir el fraude. La prevención de fraude en los estados financieros y la detección del mismo, van de la mano con los sistemas de información utilizados para obtener la información financiera, por lo tanto, una vez identificados los riesgos de la organización y priorizados, se deberán elaborar las estrategias o en otras palabras los controles que deberán ser implementados para reducir las posibilidades de riesgo y estos controles deberán considerar a los sistemas de información.

Posteriormente, se deberá evaluar la efectividad de los controles internos para asegurar que la organización puede hacer frente a los riesgos, por tal motivo los controles existentes alrededor del apartado 404 de la Ley SOX relacionados a TI varían de empresa a empresa.

En definitiva, empresas mexicanas que utilizan Tecnologías de la Información para consolidar su información financiera requieren controles internos robustos, siendo variadas las opciones de controles internos. Finalmente, se puede decir que tener un marco de referencia de control interno para Tecnologías de la Información basado en SOX puede ayudar a las empresas a disminuir las posibilidades de fraude a las que se ven expuestas. Sin embargo, es importante mencionar que las empresas deberán evaluar la viabilidad de llevar a cabo las estrategias descritas en este trabajo en caso de que decidan tomarlas como referencia.

REFERENCIAS

- Abreau, J. Hipótesis, Método & Diseño de Investigación. (2012) *International Journal of Good Conscience*. 7(2), 187-197. Recuperado de [http://www.spentamexico.org/v7-n2/7\(2\)187-197.pdf](http://www.spentamexico.org/v7-n2/7(2)187-197.pdf)
- Association of Certified Fraud Examiners. (2016) *Report to the Nations on occupational fraud and abuse, 2016 global fraud study*. Estados Unidos: ACFE Inc.
- Albashrawi, M. Detecting Financial Fraud Using Data Mining Techniques: A Decade Review from 2004 to 2015. (2016) *Journal of Data Science*. 14, 553-570.
- Anderson, D. (2008) Japanese SMB IT Market Dynamics 2008 And The Impact of J-SOX. Forrester Research, Inc Recuperado de <https://www.forrester.com/report/Japanese+SMB+IT+Market+Dynamics+2008+And+The+Impact+of+JSOX/-/E-RES59880#>
- Ballesteros, L. Nociones generales de control interno. *Control interno*, (2013). Extraído el 22 de Agosto de 2018 de <https://lballesteroscontrolinterno.wordpress.com/category/nociones-generales-de-control-interno/>
- Ballou & Heitger A building-block approach for implementing COSO's enterprise risk management-integrated framework (2005). *Management Accounting Quarterly*, invierno, 1-10.
- Bernal, C. (2010) *Metodología de la investigación*. Colombia, Pearson Educación.
- Béjar Rivera & Orrico Gálvez. El control administrativo en México. (2013) *Revista de Derecho*, 12 (22), 25-36. Recuperado de <http://web.b.ebscohost.com/ehost/detail/detail?vid=12&sid=6ca7eed9-a050-4995-94a7-acf392d8b7fe%40sessionmgr101&hid=125&bdata=Jmxhbm9ZXMmc2l0ZT1laG9zdC1saXZl#AN=110006304&db=a9h>
- Bilancio, G. El planeamiento estratégico en la Auditoría Interna. (1996) *Cuadernos de Investigación Nueva Epoca*. 43, 9-21. Recuperado de <http://web.b.ebscohost.com/ehost/detail/detail?vid=4&sid=6ca7eed9-a050-4995-94a7-acf392d8b7fe%40sessionmgr101&hid=125&bdata=Jmxhbm9ZXMmc2l0ZT1laG9zdC1saXZl#AN=20596818&db=a9h>
- Braganza & Franken, SOX, Compliance, and Power Relationships (2007). *Communications of the ACM*, 50 (9), 97-102 Recuperado de <https://cacm.acm.org/magazines/2007/9/5570-sox-compliance-and-power-relationships/fulltext>
- Briones, M. El fraude y el control interno (2014). *Puntos finos*, 222, 132-135. Recuperado de <https://www.ccpm.org.mx/avisos/132-135Fraude.pdf>
- Carriles, L. OSA litiga contra Citi, ahora en EUA. *El economista*, (2014). Extraído el 27 de Mayo de 2017 de <https://www.eleconomista.com.mx/empresas/OSA-litiga-contra-Citi-ahora-en-EU-20170317-0035.html>
- Castells, M. (1996) La era de la información. *Economía, sociedad y cultura*. México: Siglo XXI.
- Cázares, L. (1990) *Técnicas actuales de investigación documental*. México, Trillas.


- Celis, F. Liverpool detecta fraude por 52 mdd en filial paraguaya. *Forbes México*, (2017). Extraído el 5 de Marzo de 2018 de <https://www.forbes.com.mx/liverpool-detecta-fraude-filial-paraguay-52-mdd/>
- Cisterna, F. Categorización y triangulación como procesos de validación del conocimiento en investigación cualitativa (2005). *Theoria*, 14 (1), 61-71. Recuperado de <http://www.redalyc.org/html/299/29900107/>
- Committee of Sponsoring Organizations of the Treadway Commission. (2013) *Internal Control. Integrated Framework. Framework and Appendices*. Estados Unidos: COSO
- Coopers & Lybrand. (1997) *Marco general de referencia (Marco integrado)*. En *Los nuevos conceptos de control interno. (Informe COSO)*. Madrid: Ediciones Díaz Santos.
- Cortijo-Gallego & Yezegel. (2008) Contagion effect of the Sarbanes-Oxley Act: Evidence from Spain. *International Journal of Disclosure & Governance*. 5, (2), 140-152. Recuperado de <http://web.b.ebscohost.com/ehost/results?sid=6ca7eed9-a050-4995-94a7-acf392d8b7fe%40sessionmgr101&vid=9&hid=125&bquery=Contagion+effect+%20of%22+the+Sarbanes-Oxley+Act&bdata=JmRiPWE5aCZsYW5nPWVzJnR5cGU9MCZzaXRIPWVob3N0LWxpdmU%3d>
- Crearon 15.000 créditos fantasmas para sobrevalorar firma Electrofacil. *Última hora*, (2017). Extraído el 3 de marzo de 2018 de <http://www.ultimahora.com/crearon-15000-creditos-fantasmas-sobrevalorar-firma-electrofacil-n1088964.html>
- Fonseca Luna, O. (2011) *Sistemas de Control Interno para Organizaciones: Guía práctica y orientaciones para evaluar el control interno*. Lima: IICO
- García, R.. El control interno en la prevención del lavado de dinero en México. *Control Capital.net Info & Analisis ad Integritas*. (2013) Extraído de <https://www.controlcapital.net/noticia/2529/firmas/el-control-interno-en-la-prevencion-del-lavado-de-dinero-en-mexico.html>
- Garduño, R. (2004) La sociedad de la información en México frente al uso de internet. *Revista Digital Universitaria*, 5 (8), 1-13. Recuperado de http://www.revista.unam.mx/vol.5/num8/art50/sep_art50.pdf
- Gramling, et. al. Addressing problems with the Segregation of Duties in Smaller Companies. Estados Unidos. (2010) *The CPA Journal*, 80 (7), 30-34. Recuperado de <https://search.proquest.com/openview/247c71cd2a611a7be4a5cd3aa2e5395d/1?pq-origsite=gscholar&cbl=41798>
- Granados et al. (2010) Control en la administración para una información financiera confiable. *Contabilidad y Negocios*, 5, (9), 68-75. Recuperado de <http://revistas.pucp.edu.pe/index.php/contabilidadyNegocios/article/view/208>
- Gupta, P. (2008). Management's evaluation of internal controls under Section 404(a) using the COSO 1992 control framework: Evidence from practice. *International Journal of Disclosure & Governance*. 5, (1), 48-68. Recuperado de <http://web.b.ebscohost.com/ehost/detail/detail?vid=8&sid=6ca7eed9-a050-4995-94a7-acf392d8b7fe%40sessionmgr101&hid=125&bdata=Jmxhbm9ZXMmc2l0ZT1laG9zdC1saXZl#AN=28635640&db=a9h>

- KPMG Cárdenas Dosal, S.C. (2008) Encuesta de Fraude y Corrupción en México 2008. Recuperado de http://biblioteca.iiec.unam.mx/index2.php?option=com_content&do_pdf=1&id=5664
- Heidegger, M. (2005). *Ser y tiempo*. Trad. de Jorge Eduardo Rivera Cruchaga, Chile, Editorial Universitaria.
- Hernández et. al. (2006) *Metodología de la investigación*. México, Mc Graw Hill.
- International Auditing and Assurance Standards Board. (2014) Norma Internacional de Auditoría 240. Responsabilidades del auditor en la auditoría de estados financieros con respecto al fraude. Recuperado de <http://www.icac.meh.es/NIAS/NIA%20240%20p%20def.pdf>
- Information Systems Audit and Control Association, (2015) *CISA Review Manual*. Estados Unidos:ISACA
- Iñiguez, D. Bursatris: Liverpool: Fraude en Subsidiaria. *Análisis y Estrategia BX+*, (2017). Extraído el 5 de Marzo de 2018 de <http://estrategia.vepormas.com/2017/10/23/bursatris-livepol-fraude-en-subsidiaria/#close-modal>
- Juárez, E. Oceanografía le cuesta otros 30 millones de pesos a Banamex. *El economista*, (2014). Extraído el 26 de Mayo de 2017 de <https://www.eleconomista.com.mx/sectorfinanciero/Oceanografia-le-cuesta-otros-30-millones-de-pesos-a-Banamex-20141015-0071.html>
- Kroll Inc. (2015) Global Fraud report. Vulnerabilities on the Rise. Recuperado de http://anticorrupzione.eu/wp-content/uploads/2015/09/Kroll_Global_Fraud_Report_2015low-copia.pdf
- Kroll Inc. (2016) Global fraud & risk report. Building Resilience in a Volatile World. Recuperado de <http://www.kroll.com/en-us/global-fraud-report>
- Krüger, K. (2006) El concepto de sociedad del conocimiento. *Revista bibliográfica de geografía y ciencias sociales*. 9. Recuperado de https://www.researchgate.net/publication/245535884_El_concepto_de_'sociedad_del_conocimiento'
- Laski, J. (2006) El control interno como estrategia de aprendizaje organizacional: el modelo COSO y sus alcances en América Latina. *Gestión y Estrategia*, 30, 9-24. Recuperado de <http://web.b.ebscohost.com/ehost/detail/detail?vid=6&sid=6ca7eed9-a050-4995-94a7-acf392d8b7fe%40sessionmgr101&hiñd=125&bdata=Jmxhbm9ZXMmc2l0ZT1laG9zdC1saXZl#AN=32480714&db=a9h>
- Leech, T.. Distilling SOX 302, 404 & 906. *Compliance week*. (2004) Extraído el 8 de Febrero de 2017 de https://www.complianceweek.com/news/opinion/distilling-sox-302-404-906#.W_N_DOhKjIU
- Li, Y. (2010) The Case Analysis of the Scandal of Enron. *Internationals Journal of Business and Management*, 5 (10), 37-41. Recuperado de <http://www.ccsenet.org/journal/index.php/ijbm/article/viewFile/7627/5855.&ei>
- Mantilla, S. *Auditoría del control interno*. (2013) Bogotá: Ecoe Ediciones.
- Marradi, A. et. al. *Metodología de las Ciencias Sociales*. (2010) Argentina, Cengage Learning.

- Martínez, M. (2006) La investigación cualitativa, Síntesis conceptual. *Revista de Investigación en Psicología*. 9, (1), 123-146. Recuperado de https://www.researchgate.net/publication/28144043_La_Investigacion_Cualitativa_Sintesis_conceptual
- Muñoz Razo, C. *Cómo elaborar y asesorar una investigación de tesis*. (2011) México, Pearson Educación.
- Piñuel, J. (2002) *Estudios de Sociolingüística*, 3 (1), 1-42. Recuperado de https://s3.amazonaws.com/academia.edu.documents/31156298/A.Contenido.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1520789715&Signature=6yvJee%2Bn%2FPNI3SzWisbuPqQsWgE%3D&response-content-disposition=inline%3B%20filename%3DEpistemologia_metodologia_y_tecnicas_del.pdf
- Rivas, G. (2011) Modelos contemporáneos de control interno. *Fundamentos teóricos*, 4, (8), 115-136. Recuperado de <http://www.redalyc.org/html/2190/219022148007/>
- Romero, J. *Principios de contabilidad*. (2006) México: McGraw Hill
- Rosas, T. Fin de la relación Oceanografía-PEMEX. *El economista*, (2014). Extraído el 27 de Mayo de 2017 de <http://eleconomista.com.mx/industrias/2014/10/29/2015-fin-relacion-oceanografia-pemex>.
- Rozen, C. (2008) Sarbanes-Oxley act y el control interno sobre el reporte financiero. *Temas de management*, 1, 8-13 Recuperado de http://www.ucema.edu.ar/cimeibase/download/research/53_Rozen.pdf
- Santa Cruz, M. (2014) El control interno basado en el modelo COSO. *Revista de investigación de contabilidad*. 1 (1), 36-43 Recuperado de https://revistas.upeu.edu.pe/index.php/ri_vc/article/download/832/800
- Shepherd, C. et. al. (2012) *Administración de la Innovación*. México: Pearson Educación.
- Sibold, S. (2009) Canada's regulatory response to the Sarbanes-Oxley act of 2002: Lessons for Canadian Policy makers. *Alberta Law Review*, 46 (3), 769-797. Recuperado de <https://www.albertalawreview.com/index.php/ALR/article/view/225>
- Srinivasan, S. & Coates, J. (2014) SOX after Ten Years: A multidisciplinary Review. *Accounting Horizons*, 28 (3), 627-671. Recuperado de https://dash.harvard.edu/bitstream/handle/1/12175242/Srinivasan_Suraj_J2_SOX%20After%20Ten%20Years%20-%20A%20Multidisciplinary%20Review.pdf?sequence=1
- Stewart, T. (1998) *Intellectual Capital: The New Wealth of Organization*. New York: Doubleday / Currency.
- The Institute of Internal Auditors. (2008) *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners*. Lake Mary: IIA

ANEXOS

Anexo 1: Resumen ejecutivo del reporte COSO 2013.



LOS NUEVOS CONCEPTOS DEL CONTROL INTERNO

(INFORME COSO)

RESUMEN

El informe COSO, es el resultado de la investigación de un grupo de trabajo integrado por la Comisión Treadway con el objetivo de definir un nuevo marco conceptual de Control Interno capaz de integrar las diversas definiciones y conceptos que se utilizan sobre este tema.

En Estados Unidos de América, el Informe COSO ha permitido que académicos, legislativos, directores de empresas, auditores internos y externos y líderes empresariales tengan una referencia conceptual común de lo que significa el Control Interno, no obstante las diferentes definiciones y conceptos que sobre este tema existen.

El estudio ha tenido gran aceptación y difusión en los medios financieros y en los Consejos de Administración de las organizaciones, resaltando la necesidad de que los administradores y altos directores presten atención al Control Interno, tal como COSO lo define, enfatizando la necesidad de los Comités de Auditoría y de una calificada Auditoría Interna y Externa, recalcando la necesidad de que el Control Interno forme parte de los diferentes procesos y no de mecanismos burocráticos.

LO QUE SE ENTIENDE POR CONTROL INTERNO

Los controles internos se diseñan e implantan con el fin de detectar, en un plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos para cada empresa y de prevenir cualquier evento que pueda evitar el logro de los objetivos, la obtención de información confiable y oportuna y el cumplimiento de leyes y reglamentos.

Los controles internos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la confiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes.

No todas las personas entienden lo mismo por "Control Interno", esto se agrava cuando sin estar claramente definido se utiliza en la normatividad.

En sentido amplio, se define como: ***un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:***

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

Los nuevos conceptos del Control Interno

Página 1 de 16

La anterior definición refleja ciertos conceptos fundamentales:

- ❑ El Control Interno es un **proceso**, un medio utilizado para la consecución de un fin, no un fin en sí mismo.
- ❑ El Control Interno lo llevan a cabo las **personas**, no se trata solamente de manuales de políticas e impresos, sino de **personas** en cada nivel de la organización.
- ❑ El Control Interno sólo puede aportar un **grado de seguridad razonable**, no la seguridad total, a la Dirección y al Consejo de Administración de la Entidad.
- ❑ El Control Interno esta pensado para facilitar la consecución de **objetivos** propios de cada entidad.

COMPONENTES DEL CONTROL INTERNO

El Control Interno **consta de cinco componentes relacionados entre sí**, se derivan de la manera en que la dirección dirige la empresa y están integrados en el proceso de dirección, los componentes del Control son:

1. Ambiente de Control
2. Evaluación de Riesgos
3. Actividades de Control
4. Información y Comunicación
5. Supervisión.

Los cuales se detallan a continuación:

1. AMBIENTE DE CONTROL

El entorno de control aporta el ambiente en el que las personas desarrollan sus actividades y cumplen con sus responsabilidades de control, marca la pauta del funcionamiento de una organización e influye en la percepción de sus empleados respecto al control.

Es la base de todos los demás componentes del Control Interno, aportando disciplina y estructura. Los factores del ambiente de control incluyen la integridad, los valores éticos y la capacidad de los empleados de la entidad, la filosofía de dirección y el estilo de dirección, la manera en que la dirección asigna la autoridad y las responsabilidades y organiza y desarrolla profesionalmente a sus empleados así como la atención y orientación que proporciona el Consejo de Administración.

El ambiente de control tiene una incidencia generalizada en la estructuración de las actividades empresariales, en el establecimiento de objetivos y en la evaluación de riesgos.

FACTORES DEL ENTORNO DE CONTROL (COMO EVALUAR EL ENTORNO DE CONTROL)

Para evaluar el entorno de control, el evaluador debe considerar cada factor del ambiente de control a la hora de determinar si éste es positivo. Algunos aspectos son altamente subjetivos y obligan a que se formule una opinión subjetiva, generalmente inciden de forma significativa en la eficacia del ambiente de control.

Integridad y valores éticos.

- La existencia e implantación de códigos de conducta u otras políticas relacionadas con las prácticas profesionales aceptables, incompatibilidades o pautas esperadas de comportamiento ético y moral.
- La forma en que se llevan a cabo las negociaciones con empleados, proveedores, clientes, inversionistas, acreedores, competidores y auditores.
- La presión por alcanzar objetivos de rendimiento poco realistas.

Compromiso de competencia profesional.

- La existencia de descripciones de puestos de trabajo formales.
- El análisis de conocimientos y habilidades para llevar a cabo el trabajo adecuadamente.

Consejo de Administración o Comité de Auditoría.

- El ambiente de control y la cultura de la organización están influidos de forma significativa por el Consejo de Administración y el Comité de Auditoría, el grado de independencia del Consejo o del Comité de Auditoría respecto de la dirección, la experiencia y la calidad de sus miembros, grado de implicación y vigilancia y el acierto de sus acciones son factores que inciden en la eficacia del Control Interno.
- La independencia de los consejeros o miembros del Comité.
- La frecuencia y oportunidad de las reuniones con el director financiero y/o contable, auditores internos y externos.
- La suficiencia y oportunidad con que se facilita información a los miembros del Consejo o Comité de Auditoría para permitir supervisar los objetivos y las estrategias, la situación financiera, así como los resultados de explotación de la entidad.

Situaciones que pueden incitar a los empleados a cometer actos indebidos.

- Falta de controles o controles ineficaces.
- Alto nivel de descentralización sin las políticas de apoyo necesarias, que impide que la dirección esté al corriente de las acciones llevadas a cabo en los niveles mas bajos.
- Una función de auditoría interna débil.
- Consejo de Administración poco eficaz.
- Sanciones por comportamiento indebido insignificantes o que no se hacen públicas.

2. EVALUACIÓN DE RIESGOS

Toda entidad debe hacer frente a una serie de riesgos tanto de origen interno como externo que deben evaluarse. Una condición previa a la evaluación de los riesgos es el establecimiento de objetivos en cada nivel de la organización que sean coherentes entre sí. La evaluación del riesgo consiste en la identificación y análisis de los factores que podrían afectar la consecución de los objetivos y, en base a dicho análisis, determinar la forma en que los riesgos deben ser administrados y controlados, debido a que las condiciones económicas, industriales, normativas continuarán cambiando, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio.

CATEGORÍAS DE OBJETIVOS

A pesar de su diversidad, pueden agruparse en tres grandes categorías:

Objetivos relacionados con las operaciones.- Se refieren a la eficacia y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y la salvaguarda de los recursos contra posibles pérdidas. Estos objetivos varían en función de la elección de la dirección respecto a estructuras y rendimiento.

Objetivos relacionados con la información financiera.- Se refieren a la preparación de estados financieros confiables y a la prevención de la falsificación de información financiera, a menudo, estos objetivos están condicionados por requerimientos externos.

Objetivos de cumplimiento.- Estos objetivos se refieren al cumplimiento de las leyes y normas a las que está sujeta la entidad, dependen de factores externos como: la reglamentación en materia de medio ambiente, tienden a ser parecidos en algunos casos, o en todo un sector.

RIESGOS

A nivel de empresa los riesgos pueden ser la consecuencia de factores externos como internos, se presentan algunos ejemplos:

Factores externos:

- Los avances tecnológicos.
- Las necesidades o expectativas cambiantes de los clientes pueden influir en el desarrollo de productos, el proceso de producción, el servicio a cliente, la fijación de precios etc.
- Los cambios económicos pueden repercutir en las decisiones sobre financiamiento, inversiones y desarrollo.

Factores internos:

- Problemas con los sistemas informáticos pueden perjudicar las operaciones de la entidad.
- Los cambios de responsabilidades de los directivos pueden afectar la forma de realizar determinados controles.
- Un Consejo de Administración o un Comité de Auditoría débil o ineficaz pueden dar lugar a que se produzcan fugas de información.

Se han desarrollado muchas técnicas para identificar riesgos, la mayoría desarrolladas por auditores internos y externos en el momento de determinar el alcance de sus actividades, comprenden métodos cualitativos o cuantitativos para identificar y establecer el orden de prioridad de las actividades de alto riesgo.

Además, de identificar los riesgos a nivel de empresa debe hacerse a nivel de cada actividad de la empresa, esto ayuda a enfocar la evaluación de los riesgos en las unidades o funciones más importantes del negocio, como ventas, producción y desarrollo tecnológico. La correcta evaluación de los riesgos a nivel de actividad contribuye también a que se mantenga un nivel aceptable de riesgo para el conjunto de la entidad.

Análisis de riesgos

Una vez identificados los riesgos a nivel de entidad y por actividad deben llevarse a cabo un análisis de riesgos que puede ser:

- Una estimación de la importancia del riesgo.
- Una evaluación de la probabilidad o frecuencia de que se materialice el riesgo.
- Que medidas deben adoptarse.

Existe una diferencia entre el análisis de los riesgos, que forman parte del Control Interno, y los planes, programas y acciones resultantes que la dirección considere necesarios para afrontar dichos riesgos, estas acciones son parte del proceso de gestión, pero no son un elemento del Sistema de Control Interno.

Administración del cambio

Los cambios en la economía, nuevos empleados, sistemas de información nuevos, crecimiento rápido o cambios en la reglamentación pueden hacer que un sistema de control eficaz ya no lo sea, en el contexto del análisis de riesgos resulta fundamental que exista un proceso para identificar las condiciones que hayan cambiado y tomar las acciones pertinentes.

Deben existir mecanismos para identificar los cambios ocurridos, o susceptibles de ocurrir a corto plazo, en la medida de lo posible, los mecanismos deben estar orientados hacia el futuro, de manera que la entidad pueda prever los cambios significativos y elaborar los planes correspondientes.

COMO EVALUAR LOS RIESGOS

El evaluador deberá concentrarse en el proceso por parte de la dirección, de fijar los objetivos, de análisis de los riesgos y gestión de cambios, incluyendo sus vinculaciones y su relevancia para las actividades del negocio.

3. ACTIVIDADES DE CONTROL

Son las políticas y los procedimientos que ayudan a asegurar que se llevan a cabo las instrucciones de la dirección, ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la entidad.

Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones, incluyen una gama de actividades tan diversa como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones de rentabilidad operativa, salvaguarda de activos y segregación de funciones.

Las actividades de control pueden dividirse en tres categorías, según el tipo de objetivo de la entidad con el que están relacionadas: las operacionales, la confiabilidad de la información financiera y el cumplimiento de la legislación aplicable.

TIPOS DE ACTIVIDADES DE CONTROL

Existen muchas descripciones de tipos de actividades de control, que incluyen desde controles preventivos a controles detectivos y correctivos, controles manuales, controles informáticos y controles de dirección.

Algunos ejemplos:

Análisis efectuados por la dirección.- Los resultados obtenidos se analizan comparándolos con los presupuestos, las previsiones, los resultados de ejercicios anteriores y de los competidores, con el fin de evaluar en que medida se están alcanzando los objetivos.

Gestión directa de funciones por actividades.- Los responsables de las diversas funciones o actividades revisan los informes sobre resultados alcanzados.

Proceso de información.- Se aplican una serie de controles para comprobar la exactitud, totalidad y autorización de las transacciones. Se controla el desarrollo de nuevos sistemas y la modificación de los existentes, al igual que el acceso a los datos, archivos y programas informáticos.

Controles físicos.- Los equipos de fabricación, las inversiones financieras, la tesorería y otros activos son objeto de protección y periódicamente se someten a recuentos físicos cuyos resultados se comparan con las cifras que figuran en los registros de control.

Indicadores de rendimiento.- El análisis combinado de diferentes conjuntos de datos (operativos o financieros) junto con la puesta en marcha de acciones correctivas, constituyen actividades de control.

Segregación de funciones.- Con el fin de reducir el riesgo de que se cometan errores o irregularidades, las tareas se reparten entre los empleados.

INTEGRACIÓN DE LAS ACTIVIDADES DE CONTROL CON LA EVALUACIÓN DE RIESGOS.

De forma paralela a la evaluación de los riesgos, la dirección deberá establecer y aplicar el plan de acción necesario para afrontarlos. Una vez identificadas, estas acciones también serán útiles para definir las operaciones de control que se aplicarán para garantizar su ejecución de forma correcta y en el tiempo deseado.

NECESIDADES ESPECÍFICAS

Dado que cada entidad tiene sus propios objetivos y estrategias de implantación, surgen diferencias en la jerarquía de objetivos y en las actividades de control correspondientes, incluso en el caso de que dos entidades tuvieran los mismos objetivos y jerarquía, sus actividades de control serían diferentes; en efecto, cada una está dirigida por personas diferentes que aplican sus propias ideas sobre el Control Interno, además, los controles reflejan el entorno de la entidad y el sector en el que opera, así como la complejidad de su organización, su historia y su cultura.

El entorno en el que una entidad opera influye en los riesgos a los que está expuesta, en particular, puede estar sujeta a requerimientos de información a terceros particulares o a cumplir exigencias legales o normativas específicas.

La complejidad de una entidad, así como el tipo y el alcance de sus actividades, repercuten en sus actividades de control. Hay otros factores que influyen como la complejidad de una organización, la localización y dispersión geográfica, la importancia y la complejidad de las operaciones o los métodos de proceso de datos entre otros.

COMO EVALUAR LAS ACTIVIDADES DE CONTROL

Las actividades de control tienen que evaluarse en el contexto de las directrices establecidas por la dirección para afrontar los riesgos relacionados con los objetivos de cada actividad importante. La evaluación, por lo tanto, tendrá en cuenta si las actividades de control están relacionadas con el proceso de evaluación de riesgo y si son apropiadas para asegurar que las directrices de la dirección se cumplan. Dicha evaluación se efectuará para cada actividad importante, incluidos los controles generales de los sistemas informáticos. La evaluación deberá tener en cuenta no solamente si las actividades de control empleadas son relevantes en base al proceso de evaluación de riesgos realizando, sino también si se aplican de manera correcta.

4. INFORMACIÓN Y COMUNICACIÓN

Hay que identificar, recopilar y comunicar información pertinente en tiempo y forma que permitan cumplir a cada empleado con sus responsabilidades.

Los sistemas de información generan informes, que contienen información operativa, financiera y la correspondiente al cumplimiento, que posibilitan la dirección y el control del negocio. Dichos informes contemplan, no sólo, los datos generados internamente, sino también información sobre incidencias, actividades y condiciones externas, necesaria para la toma de decisiones y para formular informes financieros.

Debe haber una comunicación eficaz en un sentido amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa.

Las responsabilidades de control han de tomarse en serio. Los empleados tienen que comprender cuál es su papel en el sistema de Control Interno y cómo las actividades individuales están relacionadas con el trabajo de los demás. Asimismo, tiene que haber una comunicación eficaz con terceros, como clientes, proveedores, organismos de control y accionistas.

CALIDAD DE LA INFORMACIÓN

La calidad de la información generada por los diferentes sistemas afecta la capacidad de la dirección de tomar decisiones adecuadas al gestionar y controlar las actividades de la entidad. Resulta imprescindible que los informes ofrezcan suficientes datos relevantes para posibilitar un control eficaz.

Contenido ¿Contiene toda la información necesaria?

Oportunidad ¿Se facilita en el tiempo adecuado?

Actualidad ¿Es la más reciente disponible?

Exactitud ¿Los datos son correctos?

Accesibilidad ¿Puede ser obtenida fácilmente por las personas adecuadas?

Por otra parte, los sistemas de información, si bien forman parte del sistema de Control Interno, también han de ser controlados.

COMUNICACIÓN INTERNA

Además, de recibir la información necesaria para llevar a cabo sus actividades, todo el personal, especialmente los empleados con responsabilidades importantes deben tomar en serio sus funciones comprometidas al Control Interno.

Cada función concreta ha de especificarse con claridad, cada persona tiene que entender los aspectos relevantes del sistema de Control Interno, como funcionan los mismos, saber cuál es su papel y responsabilidad en el sistema.

Al llevar a cabo sus funciones, el personal de la empresa debe saber que cuando se produzca una incidencia conviene prestar atención no sólo al propio acontecimiento, sino también a su causa. De esta forma, se podrán identificar la deficiencia potencial en el sistema tomando las medidas necesarias para evitar que se repita.

Asimismo, el personal tiene que saber cómo sus actividades están relacionadas con el trabajo de los demás, esto es necesario para conocer los problemas y determinar sus causas y la medida correctiva adecuada. El personal debe saber los comportamientos esperados, aceptables y no aceptables.

Los empleados también necesitan disponer de un mecanismo para comunicar información relevante a los niveles superiores de la organización, los empleados de primera línea, que manejan aspectos claves de las actividades todos los días, generalmente son los mas capacitados para reconocer los problemas en el momento que se presentan. Deben haber líneas directas de comunicación para que esta información llegue a niveles superiores, y por otra parte debe haber **disposición de los directivos para escuchar**.

COMUNICACIÓN EXTERNA

Además de una comunicación interna, ha de existir una eficaz comunicación externa. Los clientes y proveedores podrán aportar información de gran valor sobre el diseño y la calidad de los productos o servicios de la empresa, permitiendo que la empresa responda a los cambios y preferencias de los clientes. Por otra parte toda persona deberá entender que no se tolerarán actos indebidos, tales como sobornos o pagos indebidos.

COMO EVALUAR LA INFORMACIÓN Y COMUNICACIÓN

Se deberá considerar la adecuación de los sistemas de información y la comunicación a las necesidades de la entidad, a continuación se relacionan algunos aspectos posibles a considerar:

Información.

- La obtención de información externa e interna y el suministro a la dirección de los informes necesarios sobre la actuación de la entidad en relación a los objetivos establecidos.
- El suministro de información a las personas adecuadas, con el suficiente detalle y oportunidad.
- El desarrollo o revisión de los sistemas de información, basado en un plan estratégico para los sistemas de información.
- El apoyo de la dirección al desarrollo de los sistemas de información necesarios.

Comunicación.

- La comunicación eficaz al personal, de sus funciones y responsabilidades de control.
- El establecimiento de líneas de comunicación para la denuncia de posibles actos indebidos.
- La sensibilidad de la dirección a las propuestas del personal respecto de formas de mejorar la productividad, la calidad, etc.
- La adecuación de la comunicación horizontal.
- El nivel de apertura y eficacia de las líneas de comunicación con clientes, proveedores y terceros.
- El nivel de comunicación a terceros de las normas éticas de la entidad.
- La realización oportuna y adecuada del seguimiento por parte de la dirección de las informaciones obtenidas de terceros, clientes, organismos de control, etc.

5. SUPERVISIÓN

Los Sistemas de Control Interno requieren supervisión, es decir, un proceso que compruebe que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continua, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continua se da en el transcurso de las operaciones, incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y frecuencia de las evaluaciones dependerá de la evaluación de riesgos y de la eficiencia de los procesos de supervisión.

Los Sistemas de Control Interno y en ocasiones, la forma en que los controles se aplican, evolucionan con el tiempo, por lo que procedimientos que eran eficaces en un momento dado, pueden perder su eficacia o dejar de aplicarse. Las causas pueden ser la incorporación de nuevos empleados, defectos en la formación y supervisión, restricciones de tiempo y recursos y presiones adicionales. Asimismo, las circunstancias en base a las cuales se configuró el Sistema de Control Interno en un principio también pueden cambiar, reduciendo su capacidad de advertir de los riesgos originados por las nuevas circunstancias. En consecuencia, la dirección tendrá que determinar si el Sistema de Control Interno es en todo momento adecuado y su capacidad de asimilar los nuevos riesgos.

SUPERVISIÓN CONTINUA

Existe una gran variedad de actividades que permiten efectuar un seguimiento de la eficacia del Control Interno, como comparaciones, conciliaciones, actividades corrientes de gestión y supervisión así como otras actividades rutinarias.

ALCANCE Y FRECUENCIA

El alcance y la frecuencia de la evaluación del Control Interno variarán según la magnitud de los riesgos objeto de control y la importancia de los controles para la reducción de aquellos. Así los controles actuarán sobre los riesgos de mayor prioridad y los más críticos para la reducción de un determinado riesgo serán objeto de evaluación más frecuente.

La evaluación del Control Interno forma parte de las funciones normales de auditoría interna y también resulta de peticiones especiales por parte del Consejo de Administración, la dirección general y los directores de filial o de división.

Por otra parte, el trabajo realizado por los auditores externos constituye un elemento de análisis a la hora de determinar la eficacia del Control Interno. Una combinación del trabajo de las dos auditorías, la interna y la externa, posibilita la realización de los procedimientos de evaluación que la dirección considere necesarios.

EL PROCESO DE EVALUACIÓN

La evaluación de un Sistema de Control constituye un proceso, si bien los enfoques y técnicas varían, debe mantenerse una disciplina en todo el proceso. El evaluador deberá entender cada una de las actividades de la entidad y cada componente del Sistema de Control Interno objeto de la evaluación. Conviene centrarse en el funcionamiento teórico del sistema, es decir en su diseño, lo cual implicará conversaciones previas con los empleados de la entidad y la revisión de la documentación existente.

La tarea del evaluador es averiguar el funcionamiento real del sistema. Es posible que, con el tiempo determinados procedimientos diseñados para funcionar de un modo determinado se modifiquen para funcionar de otro modo, o simplemente se dejen de realizar. A veces se establecen nuevos controles, no conocidos por las personas que en un principio, describieron el sistema, por lo que no se hallan en la documentación existente, a fin de determinar el funcionamiento real del sistema, se mantendrán conversaciones con los empleados que aplican y se ven afectados por los controles, se revisarán los datos registrados sobre el cumplimiento de los controles, o una combinación de estos dos procedimientos.

El evaluador analizará el diseño del Sistema de Control Interno y los resultados de las pruebas realizadas. El análisis se efectuará bajo la óptica de los criterios establecidos, con el objeto último de determinar si el sistema ofrece una seguridad razonable respecto a los objetivos establecidos.

METODOLOGÍA

Existe una gran variedad de metodologías y herramientas de evaluación, incluyendo hojas de control, cuestionarios y técnicas de flujogramación, técnicas cuantitativas, relaciones de objetivos de control, identificando los objetivos genéricos de Control Interno. Algunas empresas, comparan sus Sistemas de Control Interno con los de otras entidades, lo que se conoce generalmente como "benchmarking".

DOCUMENTACIÓN

El nivel de documentación soporte del Sistema de Control Interno de la entidad varía según la dimensión y complejidad de la misma, y otros aspectos análogos. Las entidades grandes normalmente cuentan con manuales de políticas, organigramas formales, descripciones de puestos, instrucciones operativas, flujo gramas de los sistemas de información etc.

Muchos controles son suaves y no tienen documentación, sin embargo se aplican asiduamente, resultando muy eficaces, se puede comprobar este tipo de controles de la misma manera que los controles documentados.

El hecho de que los controles no estén documentados no impide que el Sistema de Control Interno sea eficaz o que pueda ser evaluado.

PLAN DE ACCIÓN

Sugerencias básicas respecto a qué hacer y por dónde empezar:

- Determinar el alcance de la evaluación en términos de categoría de objetivos, componentes de Control Interno y actividades objeto de la evaluación.
- Identificar las actividades de supervisión continua que normalmente aseguran la eficacia del Control Interno.
- Analizar el trabajo de evaluación del control realizado por los auditores internos y reflexionar sobre las conclusiones relacionadas con el control presentadas por los auditores externos.
- Establecer las prioridades de las áreas de mayor riesgo, por unidad, componente de Control Interno u otros, para su atención inmediata.
- En base a lo anterior, elaborar un programa de evaluaciones que conste de actividades a corto y largo plazo.
- Reunir a las personas que efectuarán las evaluaciones y considerar juntos el alcance y el calendario a establecer, así como la metodología y las herramientas a utilizar, examinar las conclusiones de los auditores internos y externos y de los organismos públicos, definir la forma de presentación de las conclusiones y determinar la documentación a entregar a la finalización de la evaluación.
- Seguir el avance de la evaluación y revisar las condiciones obtenidas.
- Asegurar que se tomen las acciones de seguimiento necesarias, modificando los apartados correspondientes de las evaluaciones posteriores, según proceda.

DEFICIENCIAS

Las deficiencias en el Sistema de Control Interno pueden ser detectadas tanto a través de los procedimientos de supervisión continua realizados en la entidad como de las evaluaciones puntuales del Sistema de Control Interno, así como a través de terceros.

El término "deficiencia" se usa aquí en un sentido amplio como referencia a un elemento del Sistema de Control Interno que merece atención, por lo que una deficiencia puede representar un defecto percibido, potencial o real, o bien una oportunidad para reforzar el Sistema de Control Interno con la finalidad de favorecer la consecución de los objetivos de la entidad.

FUENTES DE INFORMACIÓN

Una de las mejores fuentes de información relativa a las deficiencias de control es el propio Sistema de Control Interno. Las actividades de supervisión continua de una entidad, incluyendo las de gestión y supervisión diarias del personal, proporcionan la percepción de las personas directamente involucradas en las actividades de la entidad. El personal puede advertir aspectos de relevancia en tiempo real que pueden servir para identificar las deficiencias existentes rápidamente. Las evaluaciones puntuales del Sistema de Control Interno constituyen otra fuente de detección de las deficiencias de control, las evaluaciones realizadas por la dirección, los auditores internos u otros empleados pueden señalar áreas que necesiten mejoras.

¿QUÉ DEFICIENCIAS SE DEBEN INFORMAR?

Todas las deficiencias que puedan afectar la consecución de los objetivos de la entidad deben ponerse en conocimiento de las personas que pueden tomar las medidas necesarias, para determinar qué deficiencias se deben comunicar, conviene examinar el impacto de las mismas.

Al detectar una deficiencia del Control Interno, se debe comunicar el hecho a la persona responsable de la función o actividad implicada, que podrá tomar medidas correctivas, así como al nivel superior en la entidad. Este proceso permite que el responsable dé el apoyo y la supervisión necesarios para las acciones correctivas a tomar e informe a las otras personas en la organización cuyas actividades pueden verse afectadas.

En el caso de que la deficiencia tenga un efecto horizontal, la comunicación del hecho también debe ser horizontal y alcanzar el nivel suficiente para asegurar que se tomen las medidas correspondientes.

COMO EVALUAR LA SUPERVISIÓN

Para llegar a una conclusión sobre la eficacia de la supervisión del Control Interno, conviene considerar tanto las actividades de supervisión continua como las evaluaciones puntuales del Sistema de Control Interno, o de partes del mismo. A continuación se detallan algunos aspectos, sirviendo esta relación únicamente de punto de referencia.

Supervisión continua

- Hasta que punto el personal al realizar sus actividades normales obtiene evidencia de que el Sistema de Control Interno está funcionando adecuadamente.
- En que medida las comunicaciones procedentes de terceros corroboran la información generada internamente o indican problemas.
- Comparaciones periódicas entre los importes registrados por el sistema contable con los activos físicos.
- Receptividad ante las recomendaciones del auditor interno y externo respecto de la forma de mejorar los controles internos.
- En que medida las reuniones facilitan información a la dirección sobre si los controles operan eficazmente.
- Si se hacen encuestas periódicas al personal para que manifieste si entiende y cumple el código de conducta de la entidad y si se realizan normalmente las tareas de control críticas.
- Eficiencia de las actividades de auditoría interna.

La evaluación puntual

- Alcance y frecuencia de las evaluaciones puntuales del Sistema de Control Interno.
- Idoneidad del proceso de evaluación
- Si la metodología para evaluar el sistema es lógica y adecuada
- Adecuado volumen y calidad de la documentación

Comunicación de deficiencias

- Existencia de un mecanismo para recoger y comunicar cualquier deficiencia detectada en el Control Interno.
- Idoneidad de los procedimientos de comunicación.
- Idoneidad de las acciones de seguimiento.

LIMITACIONES DEL CONTROL INTERNO

LO QUE SE PUEDE LOGRAR CON EL CONTROL INTERNO

El Control Interno puede ayudar a que una entidad consiga sus objetivos de rentabilidad y a prevenir la pérdida de recursos, puede ayudar a la obtención de información financiera confiable, puede reforzar la confianza de que la empresa cumple con la normatividad aplicable.

LO QUE NO SE PUEDE LOGRAR CON EL CONTROL INTERNO

Un Sistema de Control Interno, no importa lo bien concebido que esté y lo bien que funcione, únicamente puede dar un grado de seguridad razonable, no absoluta, a la dirección y al consejo en cuanto a la consecución de los objetivos de la entidad.

El Control Interno no puede hacer que un gerente malo se convierta en un buen gerente. Asimismo, los cambios en la política o en los programas gubernamentales, las acciones que tomen los competidores o las condiciones económicas pueden estar fuera de control de la dirección.

El Control Interno (incluso un Control Interno eficaz) funciona a diferentes niveles con respecto a los diferentes objetivos. En el caso de los objetivos relacionados con la eficacia y eficiencia de las operaciones (consecución de su misión básica, de los objetivos de rentabilidad y análogos) el Control Interno puede ayudar a asegurar que la dirección sea consciente del progreso o del estancamiento de la entidad.

JUICIO HUMANO

La eficacia de los controles se verá limitada por el riesgo de errores humanos en la toma de decisiones, estas decisiones se tienen que tomar basadas en el juicio humano, dentro de unos límites temporales, en base a la información disponible y bajo la presión diaria de la actividad laboral.

DISFUNCIONES DEL SISTEMA

A pesar de estar bien diseñados, los controles internos pueden fallar, puede que el personal comprenda mal las instrucciones o que se cometan errores de juicio.

ELUSIÓN DE LOS CONTROLES POR LA DIRECCIÓN

El Sistema de Control Interno no puede ser más eficaz que las personas responsables de su funcionamiento, incluso aquellas entidades que tienen un buen ambiente de control (aquellas que tienen elevados niveles de integridad y conciencia del control) existe la posibilidad de que el personal directivo eluda el Sistema de Control Interno.

El término "elusión de los controles por la dirección" en el sentido en que se emplea en éste documento se refiere a la omisión de políticas o procedimientos establecidos con finalidades ilegítimas, con ánimo de lucro personal o para mejorar la presentación de la situación financiera o para disimular el incumplimiento de obligaciones legales.

La elusión incluye prácticas tales como actos deliberados de falsificación ante bancos, abogados, contadores y proveedores, así como la emisión intencionada de documentos falsos entre otras.

La elusión no se debe confundir con la intervención, términos que se refiere a los actos de la dirección efectuados con finalidades legítimas, que se desvían de las políticas y procedimientos establecidos. La intervención de la dirección es necesaria para hacer frente a transacciones o acontecimientos puntuales y no recurrentes que, de otra forma no serían procesados correctamente por el Sistema de control.

Las intervenciones se hacen de manera abierta y tienen su correspondiente soporte documental, mientras que la elusión normalmente ni se documenta ni se comunica, en un claro intento de encubrir los hechos.

CONFABULACIÓN

La confabulación de dos o más personas puede provocar fallas en el Sistema de control. Cuando las personas actúan de forma colectiva para cometer y encubrir un acto, los datos financieros y otras informaciones de gestión pueden verse alterados de un modo no identificable por el Sistema de Control.

RELACIÓN COSTO / BENEFICIO

Las entidades deben considerar los costos y beneficios relativos a la implantación de controles. A la hora de decidir si se ha de implantar un determinado control, se considerarán tanto el riesgo de fracaso como el posible efecto en la entidad, junto a los costos correspondientes a la implantación del nuevo control.

Existen distintos niveles de precisión en cuanto a la determinación del costo y el beneficio de la implantación de controles. Generalmente resulta mas fácil determinar el costo, pudiéndose cuantificar de forma bastante precisa, normalmente se tienen en cuenta todos los costos directos correspondientes a la implantación de un control, así como los costos indirectos si resultan cuantificables. Algunas empresas también incluyen los costos de oportunidad asociados al uso de recursos.

FUNCIONES Y RESPONSABILIDADES

Todos los miembros de la organización son responsables del Control Interno.

- ❑ **La Dirección.-** O cualquier denominación para el máximo ejecutivo, en el cual recae en primer lugar la responsabilidad del control, el cual debe liderar y revisar la manera en que los miembros controlan el negocio, estos a su vez designan responsables de cada función y establecen políticas y procedimientos de Control Interno más específicos. La responsabilidad se organiza en cascada.
- ❑ **Responsables de las Funciones Financieras.-** Los directores financieros y sus equipos tienen una importancia vital porque sus actividades están estrechamente vinculadas con el resto de unidades operativas y funcionales de una entidad. Normalmente están involucrados en el desarrollo de presupuestos y en la planificación financiera. Controlan, siguen y analizan el rendimiento, no sólo desde una perspectiva financiera sino también, en muchas ocasiones, en relación al resto de operaciones de la entidad y al cumplimiento de requisitos legales.

El director financiero, el jefe de contabilidad, el "controller" y otros responsables de las funciones financieras de una entidad son claves para determinar la forma en que la dirección ejerce el control.

- ❑ **El Consejo de Administración.-** La dirección es responsable ante el Consejo el cual debe de ofrecer asesoría, pautas de actuación y conocer a profundidad las actividades de la entidad. Debe de estar preparado para una posible falla de la dirección a través de una comunicación con los niveles altos, con los responsables financieros, jurídicos y de auditoría.

Muchos consejos de administración llevan a cabo sus tareas a través de comités. Sus funciones y la

importancia de sus trabajos varían de una entidad a otra, pero suelen incluir las áreas de auditoría, remuneraciones, finanzas, nombramientos etc. Cada comité puede poner un énfasis específico en determinados elementos del Control Interno.

- ❑ **Comité de Auditoría.-** El Comité de Auditoría o en su defecto el consejo, está en una posición privilegiada, tiene la autoridad para interrogar a los directivos sobre la forma en que están asumiendo sus responsabilidades en cuanto a la información financiera, y para asegurar que se tomen medidas correctivas. El Comité de Auditoría, junto con, o además de una función de auditoría interna fuerte, está muchas veces en la mejor posición dentro de una entidad para identificar situaciones en que los altos directivos intentan eludir los controles internos o tergiversar los resultados financieros y actuar en consecuencia. Por ello, existen situaciones en las que el Comité de Auditoría o el consejo deben afrontar directamente asuntos o circunstancias graves.

La Comisión Treadway ha emitido directrices generales sobre el tamaño del Comité de Auditoría, los plazos de nombramiento, calendarios de reuniones y participantes, información al consejo, el conocimiento por parte de cada miembro de las operaciones de la empresa, la revisión de los planes de los auditores internos y externos, la adopción de nuevos principios de contabilidad, estimaciones importantes, reservas, contingencias y las variaciones de un ejercicio a otro.

- ❑ **Auditores Internos.-** Desempeñan un papel importante en la evaluación de la eficiencia de los Sistemas de control y recomiendan mejoras a los mismos. Según las normas emitidas por el Institute of Internal Auditors los auditores internos deberían:
 - "Revisar la confiabilidad y la integridad de la información financiera y operativa y los procedimientos empleados para identificar, medir, clasificar y difundir dicha información".
 - "Revisar los sistemas establecidos para asegurar el cumplimiento de aquellas políticas, planes, procedimientos, leyes y normativas susceptibles de tener un efecto importante sobre las operaciones e informes, así como determinar si la organización cumple con los mismos".
 - "Revisar los medios utilizados para la salvaguarda de activos y verificar la existencia de los mismos".
 - "Valorar la eficiencia en el empleo de los recursos".
 - "Revisar las operaciones o programas para cerciorarse de si los resultados son coherentes con los objetivos y las metas establecidas y si se han llevado a cabo según los planes previstos".

Todas las actividades de una entidad recaen, potencialmente, dentro del ámbito de responsabilidad de los auditores internos.

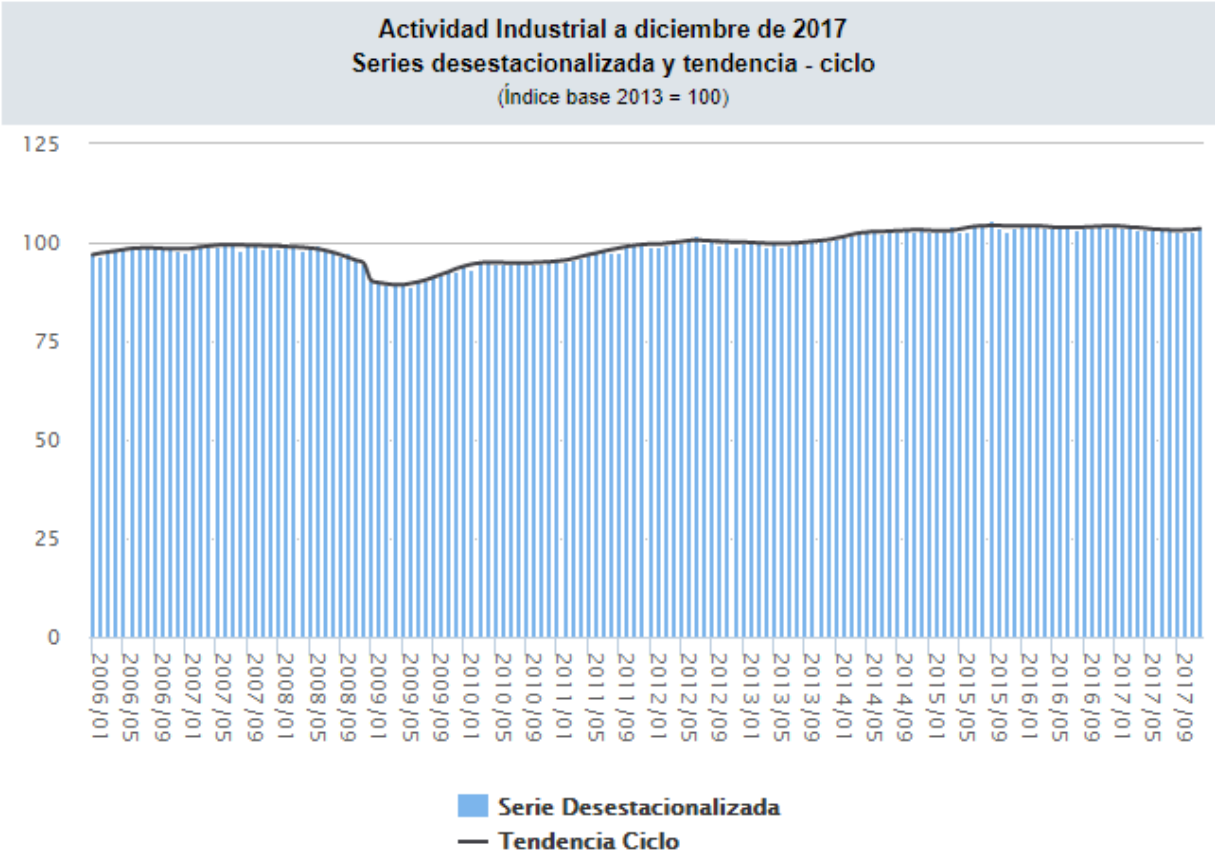
Los auditores internos sólo pueden ser imparciales cuando no están obligados a subordinar su juicio sobre asuntos de auditoría al juicio de otros. El principal medio de asegurar la objetividad de la auditoría interna es la asignación de personal adecuado para la función de auditoría, evitando posibles conflictos de intereses y prejuicios. Debería haber una rotación periódica en el personal asignado y los auditores internos no deberían asumir responsabilidades operativas. Igualmente, no deberían estar asignados a la auditoría de actividades en las cuales hubiesen tenido alguna responsabilidad operativa reciente.

Debe recordarse que la función de auditoría interna, en contra de lo que cree algún sector de opinión, no tiene como responsabilidad principal el establecimiento o mantenimiento del Sistema de Control Interno.

Otros Empleados.- El Control Interno es hasta cierto punto responsabilidad de todos los empleados, casi todos producen información utilizada en el Sistema de Control o realizan funciones para efectuar el control.

Auditores Externos.- Algunos terceros como los auditores externos contribuyen al logro de los objetivos, aportan opinión independiente y objetiva, contribuyen directamente mediante la auditoría a los estados financieros

Anexo 2: Indicador mensual de la actividad industrial, cifras desestacionalizadas, al cierre del año 2017 de acuerdo al INEGI.



Anexo 3: Clasificación de los Sectores industriales de acuerdo a los registros del INEGI para el año 2017.



Minería	Construcción	Industrias manufactureras
<ul style="list-style-type: none"> • Extracción de petróleo y gas • Minería de minerales metálicos y no metálicos, excepto petróleo y gas • Servicios relacionados con la minería • Generación, transmisión y distribución de energía eléctrica, suministro de agua y de gas por ductos al consumidor final • Generación, transmisión y distribución de energía eléctrica • Suministro de agua y de gas por ductos al consumidor final 	<ul style="list-style-type: none"> • Edificación • Construcción de obras de ingeniería civil • Trabajos especializados para la construcción 	<ul style="list-style-type: none"> • Industria alimentaria • Industria de las bebidas y del tabaco • Fabricación de insumos textiles y acabado de textiles • Fabricación de productos textiles, excepto prendas de vestir • Fabricación de prendas de vestir • Curtido y acabado de cuero y piel, y fabricación de productos de cuero, piel y materiales sucedáneos • Industria de la madera • Industria del papel • Impresión e industrias conexas • Fabricación de productos derivados del petróleo y del carbón • Industria química • Industria del plástico y del hule • Fabricación de productos a base de minerales no metálicos • Industrias metálicas básicas • Fabricación de productos metálicos • Fabricación de maquinaria y equipo • Fabricación de equipo de computación, comunicación, medición y de otros equipos, componentes y accesorios electrónicos • Fabricación de accesorios, aparatos eléctricos y equipo de generación de energía eléctrica • Fabricación de equipo de transporte • Fabricación de muebles, colchones y persianas • Otras industrias manufactureras

Anexo 4: Boleta de evaluación de fraude para México del Informe Anual de Fraude Global de Kroll 2014/2015.

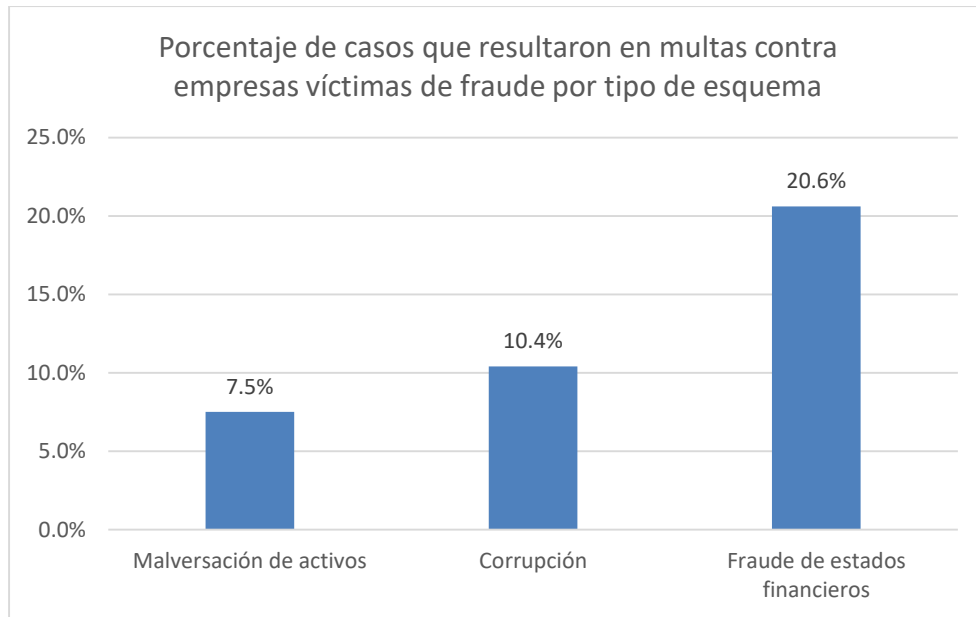
BOLETA DE CALIFICACIONES DE MÉXICO		
	2015-2016	2013-2014
Predominio Compañías afectadas por fraude	80%	63%
Pérdidas Porcentaje promedio de ingresos perdidos debido a fraude	0.8%	1.9%
Áreas de pérdida frecuente Porcentaje de empresas reportando pérdida por este tipo de fraude	Vendedor, proveedor o fraude de adquisiciones (23%) Robo de bienes tangibles o stock (23%) Robo de información, pérdida o ataque (17%)	Robo de bienes tangibles o stock (30%) Corrupción y soborno (25%) Fraude financiero interno (25%)
Incremento en exposición Componentes donde la exposición al fraude ha incrementado	67%	93%
Mayores factores de mayor exposición Factor mas extendido conduciendo a una mayor exposición al fraude y porcentaje de compañías afectadas	Alta rotación de personal (23%) Incremento de subcontratación y deslocalización (20%)	Alta rotación de personal (45%)

Anexo 5: Boleta de evaluación de fraude para México del Informe Anual de Fraude Global de Kroll 2015/2016.

BOLETA DE CALIFICACIONES DE MÉXICO

Fraude		Porcentaje de encuestados afectados por fraude en los últimos 12 meses	<div>2%</div> 	Puntos por encima de 2015 Equivalente al porcentaje global de 82%
Tipos más comunes de fraude	Fraude de proveedores o adquisiciones Robo de bienes tangibles o stock Fraude o sobornos	52% 30% 18%		26% 29%
Perpetradores más comunes	Ex empleados Empleados junior de la misma compañía Freelancers/trabajadores temporales Proveedores Agentes y/o intermediarios	33% 30% 30% 30%		27% 39% 27% 26%
Medidas anti-fraude más comunes	Socios, clientes y proveedores (debida diligencia) Financieras (controles financieros, detección de fraude, auditoría interna, auditoría externa, políticas anti lavado de dinero) Riesgo (oficial de riesgo y sistema de manejo de riesgo)	82% 82% 81%		77% 77% 78%
Medios de descubrimiento más comunes	Mediante una auditoría interna	82%		77%

Anexo 6: Multas por Tipo de Régimen (fraude) de acuerdo al Reporte Anual de Fraude y Abuso Organizacional de la Asociación de Examinadores de Fraude Certificados 2016.



Anexo 7: Glosario.

Acceso lógico. En Tecnologías de la Información, el término se refiere a las interacciones con el hardware por medio de acceso remoto. Identificación, autenticación y autorización de protocolos.

Acreedores. Personas físicas o morales que otorgan en un momento dado un crédito a otra persona (deudor) con el derecho de recibir el pago en una fecha acordada.

Activos. Recursos con valor que generan un beneficio futuro. Son los bienes y derechos de las organizaciones.

Ambiente de control. Entorno generado por las actitudes de los empleados de la empresa respecto al control interno. Incluye factores formales como la estructura organizacional y factores informales como los valores éticos empresariales.

Ambiente de producción. Entorno en tiempo real donde los usuarios ponen en funcionamiento el software (ejecutan los programas) para su uso previsto y donde se instalan las configuraciones de hardware para operaciones comerciales o de organización.

Ambiente de prueba. Es una réplica del ambiente de producción, con configuraciones de hardware y software lo suficientemente cercanas a producción, donde se realizan las pruebas del producto de software recién construido.

Ancho de banda. Capacidad de transmisión de un sistema de comunicación de red física o inalámbrica.

Aplicaciones. Una aplicación de software es un programa o grupo de programas diseñados para los usuarios finales. Algunos ejemplos son los procesadores de texto y las hojas de cálculo.

Audidores internos. Profesionales capacitados y experimentados que están designados a realizar auditorías de la empresa donde labora o alguna filial.

Audidores externos. Profesionales capacitados y experimentados que están designados a realizar Auditorías, siendo independientes de la entidad auditada.

Auditorías. Procesos llevados a cabo en diversas áreas de la organización para investigar cualquier problema que pudiera existir, sus causas e impacto.

Bancarrota. Situación dónde la empresa no puede hacer frente a sus obligaciones de pago porque superan a sus activos.

Base de datos. Sistema electrónico que permite acceder, manipular y actualizar datos fácilmente.

Bienes de consumo. En términos económicos, son aquellos utilizados directamente por el consumidor al ser los bienes finales en la cadena de producción.

Bienes tangibles. Bienes físicos que son apreciables a simple vista y ocupan un espacio.

Bolsas de valores. Lugares físicos o virtuales donde se realizan transacciones de compra y venta de capital a través de intermediarios autorizados.

Capital intelectual. Es el conocimiento con el que cuentan los empleados de una organización y que en conjunto otorgan una ventaja competitiva a la empresa.

Cartera de crédito. Es el conjunto de créditos y financiamientos que el sistema bancario otorga a las empresas.

Centros de datos. Espacios físicos donde se almacenan equipos informáticos y donde se procesan datos digitales.

Código. En informática, es el conjunto de instrucciones que recibe un sistema operativo para poder codificar y decodificar la información y poder así mostrársela al usuario.

Códigos de conducta. Son la declaración formal de los valores y estándares éticos de una organización.

Comercio. Intercambio de bienes y servicios a cambio de dinero.

Comercio electrónico. Es el comercio que ocurrió en línea (internet).

Configuración. Es la manera en que los componentes están dispuestos para formar el sistema informático.

Conflicto de interés. Situación en la que un individuo tiene intereses o lealtades en conflicto que llevan al riesgo de consecuencias.

Contraloría interna. En relación a controles internos, es una sección de la empresa que se encarga de brindar información veraz y confiable a la administración

Control interno. Proceso ejecutado por todos los trabajadores de una organización para proveer seguridad encaminada al logro de objetivos relacionados a la efectividad y/o eficiencia de los procedimientos, a la confiabilidad de la información financiera, y al acatamiento de las reglamentaciones o leyes correspondientes.

Controles automatizados. En TI, son los controles realizados por un sistema automatizado, sin interferencia de una persona.

Controles manuales. Son los controles de TI donde interfiere al menos una persona.

Crédito. Operación de financiamiento donde una persona física o moral (acreedor) presta una cantidad monetaria a otra persona (deudor). Se diferencia de un préstamo al no ser una cantidad fija la que se pone a disposición del deudor.

Créditos fantasmas. Fraude ocasionado por medio de créditos inexistentes.

Déficit. En economía, es cuando los gastos superan a los ingresos dando como resultado un balance negativo.

Demanda. En economía, es el total de lo que el mercado quiere adquirir, ya sean bienes o servicios.

Diligencia. En auditorías, es el desempeño de aquellas acciones que generalmente se consideran prudentes, responsables y necesarias para llevar a cabo la investigación.

Empresas públicas. Son aquellas que cotizan en alguna bolsa de valores.

Epistemológica. Proveniente de la rama filosófica que se encarga de estudiar el conocimiento.

Error material. Es aquel error, identificado por medio de una auditoría, en la información financiera que afecta la precisión general de los estados financieros.

Esquema de codificación. Herramienta utilizada para estandarizar la codificación de datos.

Estados financieros. Son los informes utilizados por las organizaciones para dar a conocer su situación financiera a las diversas partes interesadas.

Estrategias. Acciones encauzadas a un fin específico.

Fraude. Acto intencional para obtener una ventaja injusta o ilegal.

Gobierno corporativo. Consiste en el liderazgo, estructuras y procesos organizativos que aseguran que la empresa mantenga y extienda las estrategias y objetivos.

Hardware. Componentes físicos de un sistema computacional.

Hojas de cálculo. Aplicación informática capaz de organizar y gestionar datos para obtener resultados.

Identificación por radiofrecuencia. Forma de comunicación inalámbrica para identificar de forma única un objeto, animal o persona.

Información financiera. Aquella información de una empresa, expresada económicamente y utilizada para la toma de decisiones de las partes interesadas.

Infraestructura de TI. Es el conjunto de dispositivos físicos y software utilizado para dar servicios de TI a una organización.

Insolvente. Que está en bancarota.

Inversión de capital. Dinero que invierte una empresa para adquirir activos físicos.

Inversionistas. Personas físicas o morales que utilizan parte de sus recursos en instrumentos financieros para obtener un rendimiento futuro.

Malversación de fondos. Desfalco. Acción de utilizar dinero ajeno en cuestiones diferentes a las cuales ese dinero estaba destinado.

Mercado. Contexto donde ocurren los intercambios de bienes y servicios por dinero.

Mercados de capitales. Es aquél donde se lleva a cabo la compra y venta de acciones, activos financieros y títulos de las empresas.

Minería de datos. Proceso de analizar patrones ocultos de datos según diferentes perspectivas para la categorización en información útil.

Obligaciones. Deudas que tienen las empresas tanto a corto como a largo plazo.

Oferta. En economía, es el total de lo que el mercado puede vender, ya sean bienes o servicios

Organizaciones lucrativas. Sinónimo de empresas.

Partida doble. Método contable para registrar las operaciones de una empresa.

Penalidades civiles. En los Estados Unidos de América, son aquellos conflictos legales que ocurren entre particulares y no representan una ofensa contra el estado.

Quiebra. Sinónimo de bancarota.

Rendimiento. Rentabilidad que se obtiene por medio de una inversión.

Rentabilidad. Beneficios que se obtienen al invertir.

Roles. En TI, la seguridad basada en roles consiste en limitar el acceso de los usuarios a un sistema de acuerdo con un rol previamente construido.

SAP. Software utilizado por las empresas para gestionar sus modelos de negocios.

Segregación de funciones. En el ámbito de control interno, es la separación de responsabilidades con la finalidad de prevenir el fraude interno en las empresas.

Seguridad razonable. En materia de control interno, es el grado de comodidad de que los objetivos de la organización se consigan ya que existen limitaciones inherentes a los sistemas de control.

Servicios de soporte. En TI, son los servicios técnicos que proporcionan asistencia a los usuarios para resolver problemas de software y hardware.

Sistema de control. Es el proceso de control interno que se conforma por las actividades operativas de las organizaciones que lo llevan a cabo.

Sistemas de información. Son la combinación de actividades estratégicas, administrativas y operativas involucradas en la recopilación, el procesamiento, el almacenamiento, la distribución y el uso de la información y sus tecnologías relacionadas.

Sistemas ERP. Programas de software utilizados en diversas operaciones internas de una empresa.

Sociedad de la información. Es un entorno en que las tecnologías de la información facilitan la creación de conocimiento.

Software. Programas y documentación de apoyo que facilitan el uso de una computadora.

Software DLP. El software de prevención y pérdida de datos identifica y monitorea datos confidenciales para garantizar que solo los usuarios autorizados accedan a ellos, además de asegurar que existan medidas de protección contra la pérdida de datos.

T-code. El código de transacción en SAP es aquél utilizado para acceder a funciones o correr programas dentro de SAP de una forma rápida.

Tecnología. Habilidad que permite generar una manera de crear procesos, bienes o servicios.

Tecnologías de la Información. Hardware, software, comunicación y otras instalaciones utilizadas para ingresar, almacenar, procesar, transmitir y generar datos en cualquier forma.

Transacción. Eventos empresariales o información agrupada ya que se tiene un propósito único o similar.

Transacciones mercantiles. Transacciones de compra-venta entre un comprador y un vendedor.

Trueque. Intercambio de bienes y servicios sin la intervención del dinero.

Valor agregado bruto. Es la medición del valor total de bienes y servicios en conjunto que se producen en un país.