Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas y Telemática

Análisis de la norma ISO 37001 y su relación con las ISO utilizadas en la gestión de riesgos

Tesis de grado previo a la obtención del título de Ingeniero de Sistemas y Telemática

Autor: Edisson Arias Ortiz.

Director: Ing. Esteban Crespo.

Cuenca, Ecuador

2018

DEDICATORIA

El presente trabajo va dedicado a las personas que hoy no se encuentran a mi lado, mis abuelos Guillermo, Julio y Mercedes. También a mis padres y hermanas, en especial a mi madre Juana y mi abuela Inés que han sido un gran pilar en mi desarrollo profesional.

AGRADECIMIENTOS

A mis familiares, con especial énfasis a mi querida madre que es un gran apoyo desde mi infancia. A mis compañeros y amigos que me han acompañado en la carrera universitaria. A los profesores, en especial al querido profesor Esteban Crespo que se ha tomado el tiempo para apoyar y colaborar en la construcción de este proyecto.

ÍNDICE DE CONTENIDOS

DEDICATORIA i

AGRADECIMIENTOS ii

ÍNDICE DE CONTENIDOS iii

ÍNDICE DE GRÁFICOS vi

ÍNDICE DE TABLAS viii

RESUMEN.....ix

ABSTRACT.....x

INTRODUCCIÓN: xi

Objetivo General: xiii

Objetivos Específicos: xiii

Metodología: xiii

CAPÍTULO 1: Fundamentos 1

1.1. Sistemas de Gestión de la Seguridad de Información (SGSI).....1

1.2. Seguridad de la información.....7

1.3. Riesgos 11

1.3.1 Análisis de riesgos. 12

1.3.2 Tratamiento y gestión de riesgos. 16

1.3.3 Riesgo Informático. 21

1.4 Las MPYMES y la Seguridad de la información en Ecuador 22

1.5. Los marcos de referencia internacionales utilizados en la gestión de riesgo 25

1.5.1 ISO/IEC 27001. 26

1.5.2 ISO/IEC 27002. 37

1.5.3 ISO 27005. 44

1.5.4 ISO 31000: 2009. 44

1.6 Marcos de referencia 46

1.6.1 COBIT 5. 46

1.6.2 COSO III:2013. 47
CAPÍTULO 2 – El sistema de Gestión Anti Soborno ISO 37001 52
2.1 Introducción a las organizaciones y sociedades 52
2.2 La lucha contra la corrupción y el soborno 57
2.2.1 Los beneficios de la lucha contra la corrupción. 58
2.2.2 Riesgos de Corrupción. 59
2.2.3 Lucha contra la corrupción de las PYMES. 60
2.2.4 Denunciar la corrupción. 61
2.2.5 Normas contra la corrupción. 66
2.2.6 Ley FCPA en América Latina. 72
2.2.7 Índice de Percepción de la Corrupción. 75
2.2.8 Índice de corrupción en América. 79
2.2.9 Índice de Fuentes de Soborno. 82
2.3 Introducción a la ISO 37001 85
2.3.1 Cláusulas clave de ISO 37001: 2016. 87
2.3.2 Integración de ISO 37001 con otros sistemas de gestión. 96
2.3.3 Sistema de gestión contra el soborno - los beneficios del negocio. 96
2.3.4 Requisitos que establece la norma. 97
2.3.5 Metodología para la implementación de un Sistema de Gestión Anticorrupción. 98
2.4 Conclusiones del capítulo 2 99
CAPÍTULO 3 – Alineación de ISO 37001 con las normas ISO utilizadas en la Gestión de Riesgos de la Información. 101
3.1 Alineación con ISO 27001 101
3.2 Alineación con ISO 27002 103
3.3 Alineación con ISO 27005 106
3.4 Alineación con ISO 31000 109
3.5 Conclusiones del capítulo 3 112

CAPÍTULO 4 – Alineación de ISO 37001 con los marcos de referencia. 114
4.1 Alineación con COBIT 5.....114
4.2 Alineación entre COBIT 5 y COSO III.....122
4.3 Alineación de ISO 37001 con COSO III.....125
4.4 Conclusiones del capítulo 4.....129
CAPÍTULO 5 – Cuadro comparativo entre ISO 37001 y los marcos de referencia.....131
5.1 Cuadro comparativo entre la ISO 37001 y los marcos.....131
5.2 Conclusiones del capítulo 5.....136
Conclusiones 137
Recomendaciones.....141
Bibliografía 142
ANEXOS: 147

ÍNDICE DE GRÁFICOS

Ilustración 1: Esquema de gestión de seguridad de la información. 1
Ilustración 2: Un SGSI dentro de una organización. 2
Ilustración 3: Relación entre componentes de la gestión de la seguridad. 4
Ilustración 4: Factores de éxito para un plan de gestión de la seguridad. 5
Ilustración 5: Implantación del SGSI. 6
Ilustración 6: Atributos de la SI, y contextos. 8
Ilustración 7: Visión organizacional de la seguridad de la información. 11
Ilustración 8: Componentes del proceso de riesgos. 12
Ilustración 9. Normas acogidas por el mercado corporativo. 23
Ilustración 10. Estructura del nuevo estándar. 29
Ilustración 11. Alineación de la ISO 27001 con otros estándares. 31
Ilustración 12. Cambio en dominios de la ISO 27001. 32
Ilustración 13. Comparación ISO 27001:2005 con ISO 27001:2013. 32
Ilustración 14. Requisitos ISO 27001:2013. 33
Ilustración 15. Similitudes y diferencias entre revisiones ISO 27001:2013. 33
Ilustración 16. Mapeo de controles del Anexo A. 34
Ilustración 17. Nuevos controles de seguridad ISO 27001:2013. 35
Ilustración 18. Relación entre 27002 y 27001. 38
Ilustración 19. Cláusulas ISO 27002:2013. 39
Ilustración 20. Gobierno y Gestión en COBIT 5. 47
Ilustración 21. Relación entre componentes y objetivos en COSO. 49
Ilustración 22. Relación entre sectores. 54
Ilustración 23. Riesgos de corrupción en las distintas esferas de la actividad corporativa. 60
Ilustración 24. Efectividad y porcentaje de compañías con sistemas de denuncia de irregularidades 62
Ilustración 25. Provisión de protección jurídica a los denunciantes en el sector público. 63
Ilustración 26. Cronograma de entrada en vigor de las leyes de protección de denunciantes. 64
Ilustración 27. Países de la OCDE que garantizan el anonimato del sector público 64
Ilustración 28. Incentivos para que los denunciantes denuncien hechos ilícitos. 65
Ilustración 29. Las Diez Multas Más Altas a Empresas por FCPA (Global). 69
Ilustración 30. Ubicación de pagos indebidos 2008 - 2017. 70

Ilustración 31. Top ten de pagos indebidos 2008 - 2017. 70
Ilustración 32. Sanciones por año entre 2008 - 2017. 71
Ilustración 33. Casos procesados por año 2008-2017. 71
Ilustración 34. Individuos y Empresas Demandadas, 1977-2016. 72
Ilustración 35. Casos de FCPA en América Latina, 2006-2016. 73
Ilustración 36. 10 condenas Privativas de Libertad Más Altas por FCPA (América Latina). 73
Ilustración 37. Las 10 Multas Más Altas a Individuos por FCPA (América Latina). 74
Ilustración 38. Las 10 Multas Más Altas a Empresas por FCPA (América Latina). 74
Ilustración 39. Índice de percepción de la corrupción 2016. 76
Ilustración 40. Los países menos corruptos del mundo según TI 2016. 77
Ilustración 41. Los países más corruptos del mundo según TI 2016. 77
Ilustración 42. Los países menos corruptos del mundo 2012-2016. 78
Ilustración 43. Los países más corruptos del mundo 2012-2016. 79
Ilustración 44. Ranking de corrupción en América Latina. 81
Ilustración 45. Índice de corrupción en América Latina. Diferencias de puntaje con 2015. 82
Ilustración 46. Índice de Fuentes de Soborno 2011 por PAÍSES. 83
Ilustración 47. Índice de Fuentes de Soborno 2011 por SECTORES. 84
Ilustración 48. Cambios en las puntuaciones del Índice de Fuentes de Soborno 2008–2011. 85
Ilustración 49. Beneficios del ABMS. 97
Ilustración 50. PDCA en la ISO 37001. 98
Ilustración 51. Tratamiento de Riesgo ISO 27005. 108
Ilustración 52. Cláusulas ISO 31000. 110
Ilustración 53. Procesos de Gobierno de TI Empresarial. 114
Ilustración 54. Proceso EDM01. 115
Ilustración 55. Matriz RACI de EDM01. 115
Ilustración 56. Proceso EDM02. 116
Ilustración 57. Matriz RACI de EDM02. 117
Ilustración 58. Proceso EDM03. 118
Ilustración 59. Matriz RACI de EDM03. 118
Ilustración 60. Proceso EDM04. 119
Ilustración 61. Matriz RACI de EDM04. 120

Ilustración 62. Proceso EDM05. 121
Ilustración 63. Matriz RACI de EDM05. 121

ÍNDICE DE TABLAS

Tabla 1: Vulnerabilidades y frecuencias. 15
Tabla 2: Metodologías para el control de Riesgos 20
Tabla 3: Productos de seguridad informática que se ofrecen en Ecuador 25
Tabla 4: PHVA aplicado a la norma ISO/IEC 27001. 27
Tabla 5: Nuevos conceptos ISO 27001:2013 30
Tabla 6: Controles que no forman parte del estándar ISO 27001:2013 35
Tabla 7: PHVA aplicado a la norma ISO/IEC 27.005 44
Tabla 8: Integración de la ISO 37001 con otros sistemas de Gestión. 96
Tabla 9: Integración de COBIT 5 y COSO III 123
Tabla 10: Procesos de Gobierno de TI. 131
Tabla 11: Cláusulas relacionadas con los Marcos de Referencia. 132
Tabla 12: Relación entre los Marcos de Referencia e ISO 37001 en los procesos de gobierno. 132
Tabla 13: Relación entre los Marcos de Referencia e ISO 37001 en los procesos de gestión. 135

RESUMEN

En este trabajo se indagará sobre aspectos de gestión de riesgo que mantiene la recién norma publicada en enero de 2017, ISO 37001, y determinar su relación con los capítulos de gestión de riesgo que contemplan las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000.

Además, se estudiará la relación que mantiene esta norma con los marcos de gobierno COBIT 5 y COSO III, utilizados en el aseguramiento y gestión de riesgos de activos de la información.

ABSTRACT

This work dealt with risk management aspects of the ISO 37001 standard recently published in January 2017, and determined its relationship with the risk management chapters referred in the ISO 27001, ISO 27002, ISO 27005, and ISO 31000 standards. In addition, this paper studied the relationship between this standard and the COBIT 5, and COSO III governance frameworks used in the underwriting and risk management of information assets.

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by
Lic. Lourdes Crespo

INTRODUCCIÓN:

Muchos temas de la actualidad están relacionados con los sobornos y los actos de corrupción, como explica Alessi (2017), que la constructora brasileña Odebrecht presente en 27 países, acepto pagar 3500 millones de dólares de multa por ser acusada de otorgar 439 millones a partidos y funcionarios con el fin de garantizar contratos en obras públicas. Los conocidos Panamá Papers que salieron a la luz en abril del 2016 desenmascarando a la firma panameña Mossack Fonseca, en los que unos once millones de documentos dejaron al descubierto los secretos detrás de los paraísos fiscales. Otro como es el caso de WikiLeaks que apareció en 2007 y se ha encargado de publicar al mundo documentos, archivos que se han mantenido de manera secreta y que hoy en día salieron a la luz; y otros casos más que deberían ser estudiados a profundidad para entender que la corrupción no tiene límites.

Este tipo de actos conlleva sin duda al riesgo, que finalmente termina como un elemento habilitante para la interrupción o negación de los procesos de negocio, afectando a cualquier tipo de organización o empresa.

La problemática se presenta en relación de como los sobornos pueden generar escenarios de riesgo a los activos de información que forman parte de los procesos de negocio, elementos que deben ser contemplados por las normas de gestión de riesgo, las metodologías y los marcos de gestión. Debido a estos antecedentes se plantea el análisis de la norma anti soborno ISO 37001 y su relación con la gestión de riesgos.

En este trabajo se abordan temas correspondientes a la Seguridad de la Información, los Sistemas de Gestión de Seguridad de la Información, los Riesgos; las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000 junto a los marcos de gobierno como COSO III y COBIT 5. Todos estos temas se profundizan en el capítulo 1, la manera de comprender adecuadamente el concepto de Seguridad de la Información.

En el capítulo 2 se explica el tipo de organizaciones y sociedades existentes en el medio para entender un poco el contexto de las mismas; a partir de este punto se indaga sobre la corrupción a nivel internacional y de Latinoamérica, que es el tema principal a tratar para explicar la importancia de la lucha contra el soborno que existe en la actualidad. Para finalizar el capítulo es indispensable describir la ISO 37001 y los beneficios que trae el estudio de la misma.

La ISO 37001 hace referencia a riesgos de soborno, por cuanto es importante conocer, a nivel del riesgo operativo y de la seguridad de la información, como esta norma se relaciona con ciertas normas de la familia ISO 27000, y la ISO 31000; así como con los marcos de gobierno COSO III y COBIT 5. En los capítulos siguientes es importante conocer o encontrar la alineación que puede mantener la norma ISO 37001 con las normas utilizadas en la gestión de riesgos de la información y los marcos de gobierno.

Objetivo General:

Analizar el estándar ISO 37001 referente a sistemas de lucha contra el soborno y su relación con las ISO utilizadas en la gestión de riesgos.

Objetivos Específicos:

- Evaluar el estado del arte de la gestión de riesgo en las MPYMES
- Estudiar la norma ISO 37001 y resumir su alineación con las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000 en un cuadro comparativo.
- Identificar la aplicabilidad de la norma ISO 37001 en los marcos de referencia COBIT 5 y COSO III utilizados como marcos de gobierno.

Metodología:

Para el desarrollo del proyecto mencionado se realizará una revisión de las normativas ISO 27001, ISO 27002, ISO 27005, ISO 31000 e ISO 37001, además de los marcos de referencia COBIT 5 y COSO III. También se procederá a realizar un análisis sobre estudios referentes a los temas mencionados realizados por terceros con el fin de indagar y recopilar la información necesaria para tener un conocimiento mucho más amplio sobre las normativas de la gestión de la seguridad.

Al final se realizará una comparativa entre dichas normas para encontrar la alineación entre las mismas.

CAPÍTULO 1: Fundamentos

1.1. Sistemas de Gestión de la Seguridad de Información (SGSI)

En su texto de investigación Minchala, (2016) citando a ISO 27001 en Español (2016) indica que, "El SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de *Information Security Management System.*"

Minchala (2016) indica que el SGSI es el concepto sobre el que está basado la norma ISO 27001. También expresa que la garantía de llegar a un nivel de protección total es virtualmente imposible, aun disponiendo de recursos de manera ilimitada. Es por esto, indica, que en una organización el propósito de un SGSI es asegurar que los riesgos en la seguridad de la información sean identificados y gestionados de manera estructurada, eficiente, documentada y que se adapte a los cambios que se puedan producir en los riesgos, tecnologías o el entorno.

La gestión de la seguridad de la información tiene que ser un proceso ordenado, documentado y de conocimiento para todas las partes interesadas en la organización. (ISO 27001 en Español, 2016)

Ilustración 1: Esquema de gestión de seguridad de la información.
Fuente: ISO 27001 en Español, 2016

Un sistema de Gestión es un conjunto en el que interactúan, la estructura, los recursos, los procesos y procedimientos que ayudan a poner en práctica, las políticas y los objetivos que se han establecido en una organización. (Giraldo, 2016)

Un SGSI abarca las actividades que están relacionadas con el control y dirección de la seguridad de los activos de información. Dichas actividades consisten en la evaluación del estado actual en lo que refiere a la seguridad de la información en una organización y en la valoración de las amenazas, en el diseño de controles de seguridad administrativos y su implementación. (Areitio, 2008)

El desafío de un SGSI es que pueda mantenerse a largo plazo, que sea operativo y se mantenga acorde a la misión, objetivos y políticas determinadas por la organización. Impulsados por la misión, la visión y respetando el marco legal establecido, el SGSI debe garantizar las necesidades del negocio y tener en cuenta los planes estratégicos establecidos por la organización. (Pallas, 2009)

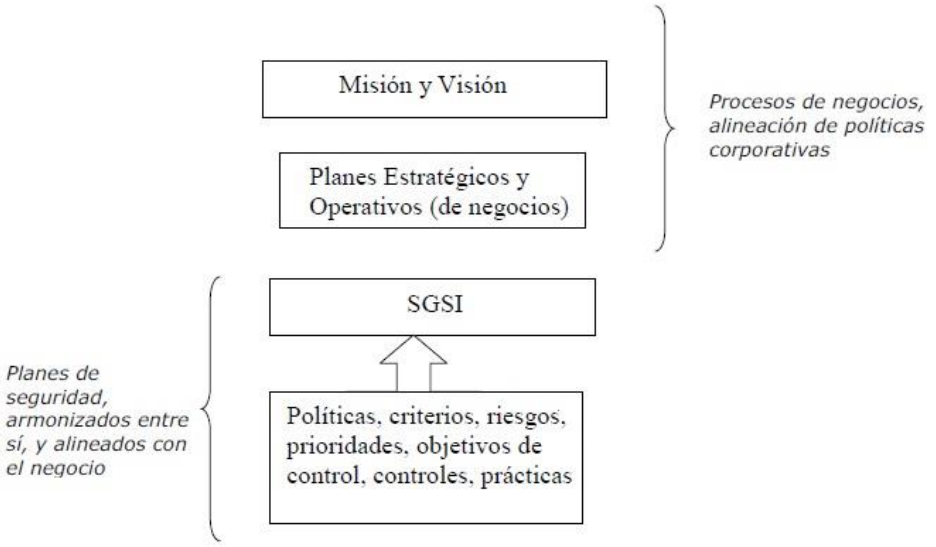

Ilustración 2: Un SGSI dentro de una organización.
Fuente: Creado por el autor

Existen varias preocupaciones por parte de los responsables del correcto funcionamiento de un sistema de gestión. Las más destacadas son: la pérdida de confianza por parte de los clientes o la pérdida de reputación en el mercado, la pérdida o continuidad del negocio, la recuperación

ante eventos inoportunos o desastres, la pérdida de datos, inversión en seguridad, responsabilidades legales, entre otros. (Areitio, 2008)

La persona responsable a la que se le fue asignada la función de responsable de la gestión de seguridad de la información en una entidad u organización, es el gestor de seguridad de la información. Un SGSI forma parte de un sistema de gestión global, que se basa en los riesgos del negocio y que monitoriza, establece, revisa, implementa, mantiene, opera y mejora la seguridad de la información. Este sistema incluye, los procedimientos, procesos, las prácticas, la estructura organizacional, las responsabilidades, los recursos y las políticas; por lo que es un concepto amplio que busca preservar la seguridad de la información en entidades u organizaciones mediante esfuerzos sistemáticos y organizados. (Areitio, 2008)

Como Areitio (2008) explica, “Un buen SGSI puede verse como un ciclo cerrado que comienza con la prevención de amenazas, la reducción de las mismas, la detección de incidentes y la contención de los mismos”. Es decir, se trata de un ciclo de mejora continua, donde se planifica, se ejecuta, se evalúa y se corrige cualquier acción tomada a cabo.

La capacidad, aptitud de un sistema de información se basa en la detección, la disuasión, la protección, la respuesta y la capacidad de recuperación, de esta manera proporcionando las debidas garantías en los activos, basándose en propiedades como la disponibilidad, la confidencialidad, auditoria o responsabilidad, la integridad, la fiabilidad y la autenticidad, sin dejar a un lado las amenazas detectadas. (Areitio, 2008)

Como Areitio (2008) indica, “En el proceso de gestión de la seguridad de los sistemas de información hay una serie de elementos involucrados”. Estos elementos son:

- Identificación de todos los activos.
- Identificación de amenazas a los activos.
- Identificación de vulnerabilidades.
- Identificación de impactos.

- Identificación del riesgo.
- Aplicación de salvaguardas.
- Identificación de riesgos residuales.
- Limitaciones.

Los componentes de gestión de seguridad se pueden relacionar.

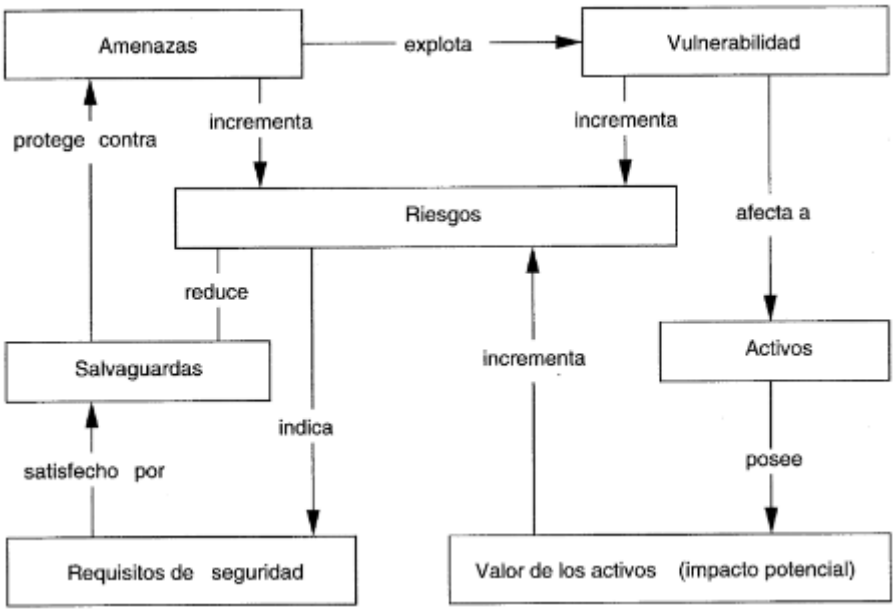

Ilustración 3: Relación entre componentes de la gestión de la seguridad.
Fuente: Areitio, 2008

La implantación de un SGSI es primordial para tratar aspectos de seguridad, mediante la asociación de recursos técnicos y humanos, avalados por medios administrativos, ya que serán los que garanticen la implantación de los controles necesarios y efectivos para lograr un nivel de seguridad aceptable, en correlación con los objetivos de la organización, para mantener los riesgos en un nivel asumible por la organización. (Giraldo, 2016)

En la imagen se muestra cómo conseguir un plan de seguridad con éxito:

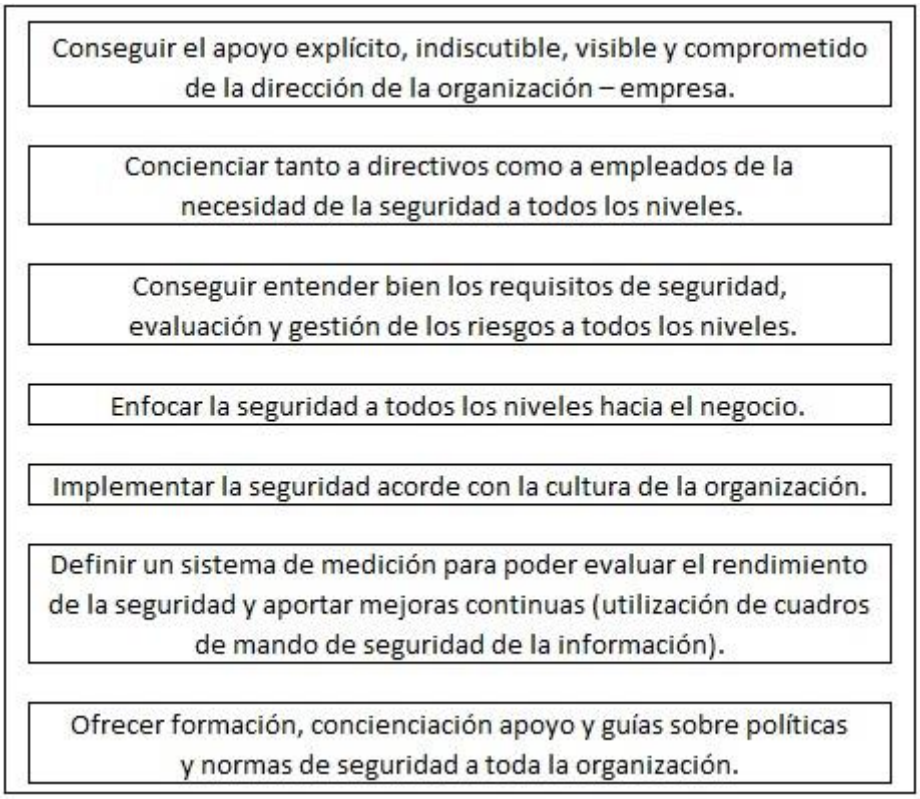

Ilustración 4: Factores de éxito para un plan de gestión de la seguridad.
Fuente: Areitio, 2008

Un SGSI, como se ha explicado, es un sistema de gestión referente a la seguridad de la información y por lo tanto debe relacionarse con otros ya conocidos sistemas de gestión, normas internacionales, marcos de gobierno, entre otros. (Pallas, 2009)

Es por esto que en este documento se profundizará en las normas de la familia ISO 27000, específicamente en la ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, así como la norma ISO 31000 y los marcos de gobierno COBIT 5 y COSO III.

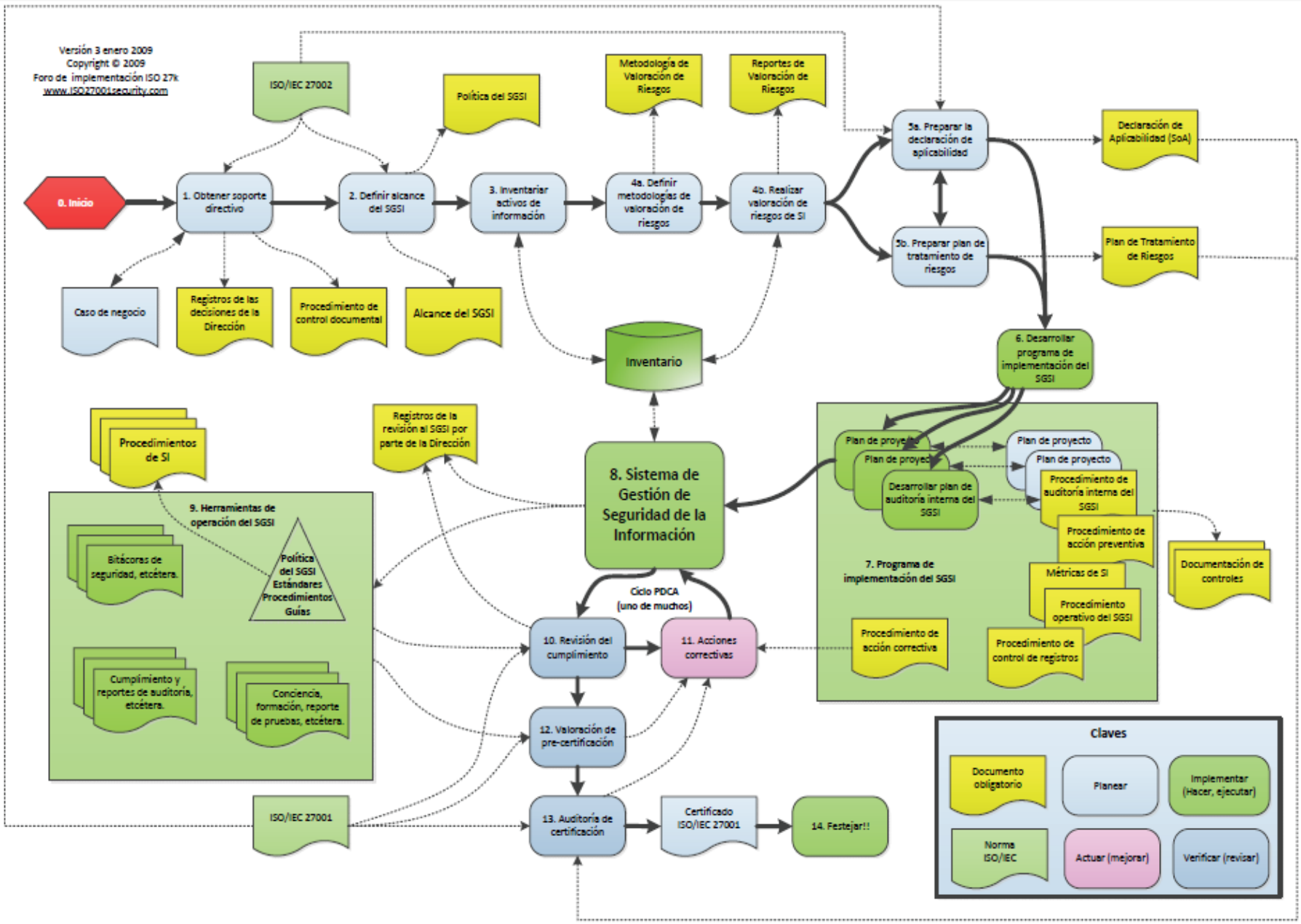

Ilustración 5: Implantación del SGSI.
Fuente: ISO 27001 en Español, 2016.

1.2. Seguridad de la información

Según Crespo (2016), la información es el activo más valioso para cualquier persona u organización en el siglo actual, la cual puede sirve como un arma para crear ventajas competitivas.

Como Giraldo (2016) explica, la seguridad de la información se refiere a las medidas que toda entidad u organización debe establecer con el fin de proteger la información.

La seguridad de la información se basa en tres principios fundamentales:

- La Integridad, hace referencia a que la información debe estar libre de alteraciones o modificaciones no planificadas
- La Disponibilidad, indica que la información debe ser utilizable cuando se la requiera
- La Confidencialidad, solo debe ser accedida por los que lo requieren (Crespo E. , 2016)

La seguridad de la información consiste en la preservación de las tres dimensiones o principios básicos explicados anteriormente, así como de los sistemas implicados en su tratamiento. Mantener estos principios, plantea la necesidad de contar con el personal capaz de asegurar, gestionar y mantener la seguridad de la información libre de amenazas del presente y también amenazas futuras. Todo esto puede ser esencial para mantener un nivel de buena imagen, conformidad legal, rentabilidad y competitividad empresarial necesarios para asegurar beneficios económicos y lograr los objetivos de la entidad u organización.

Para López & Vásquez (2016), existen otros términos involucrados en la SI como:

- Activo: Todo bien o recurso, tangible o intangible, valorado por una entidad u organización.
- Autenticidad: Se refiere a que la información debe ser legitima. Para ello se necesita que la información sea creada en la misma organización.

A continuación, se mostrará como la confidencialidad, integridad y disponibilidad deben situarse dentro del marco estratégico empresarial, del contexto del negocio y del marco legal.

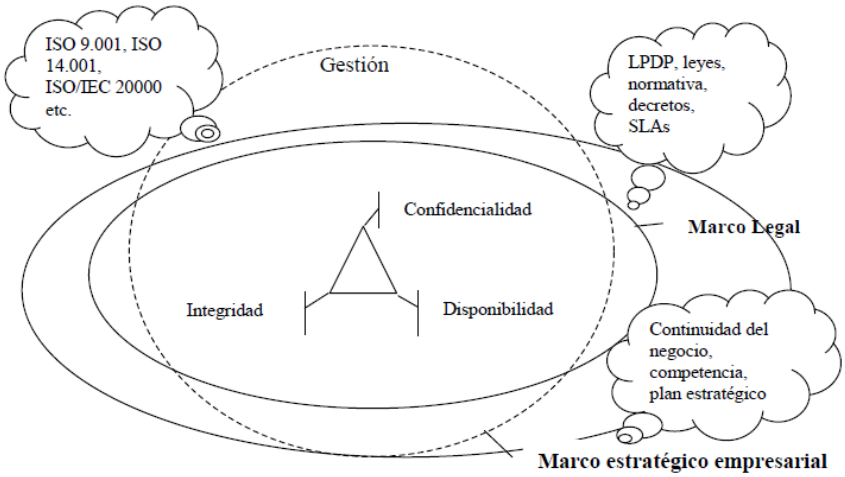

Ilustración 6: Atributos de la SI, y contextos.
Fuente: Pallas, 2009

Existen diferentes metodologías que sirven de ayuda en la seguridad de la información, muchas de ellas, de amplia divulgación son: Magerit, CRAMM, OCTAVE-S, *Microsoft Risk Guide*, COBIT 5 y COSO III que son utilizadas alrededor del mundo en la gestión del riesgo de la información.

Según ISO 27001 en Español (2016), el nivel de seguridad alcanzado por medios técnicos no es suficiente y limitado, por lo que, recomienda que toda la organización debe intervenir, con la gerencia al frente, tomando en cuenta clientes y proveedores.

En la seguridad de la información se trata sobre diferentes elementos como: aspectos tecnológicos, recursos humanos, aspectos del negocio, de índole económica, de tipo legal, etc. Y de igual manera no solo abarcando aspectos de telecomunicaciones e informáticos, sino también otros como aspectos humanos, físicos, medioambientales, etc.

Existen diferentes áreas en las que la seguridad de la información resulta ser un factor crítico:

- Banca y otras organizaciones financieras.
- Instituciones públicas y privadas de salud.
- Empresas de servicios profesionales (inmobiliarias, constructoras, promotores inmobiliarios, bufetes de abogados, notarios, empresas de proyectos de ingeniería).
- Empresas industriales.
- Administración pública (estatal y local)
- Educación.
- Aseguradoras.
- Telecomunicaciones y empresas del sector.
- Compañías de suministro energético.
- Empresas de logística y de gestión de mercancías. (Areitio, 2008)

Cordero (2015) indica que existen varios involucrados en la seguridad de la información como son:

- Talento Humano. – Personas con conocimientos para planificar, organizar y administrar sistemas informáticos.
- Tecnología. – Conjunto de software, hardware, sistemas operativos, gestión de BD, redes, etc.
- Procesos. – Se caracteriza por ejecutar una secuencia de instrucciones, que posee un estado actual y se relaciona con recursos de otros sistemas.

- Riesgos Informáticos. – Más conocidas como amenazas al sistema u otras como atentados a la seguridad etc. Hay tres tipos:
    - Riesgos de Datos
    - Riesgos de Control
    - Riesgos Estructurales
- Gestión de Riesgos. – Establece medidas que permiten controlar o mitigar los riesgos dentro del sistema. (Cordero, 2015)

La implantación y desarrollo de las TIC (Tecnologías de la Información y las Comunicaciones) en los últimos años, en sistemas de información en una entidad u organización, ha cambiado el modo de actuar en muchos ámbitos. En la actualidad, la adecuada gestión de la seguridad de la información, debido al entorno competitivo de la sociedad de la información, es de vital importancia para que una organización pueda sobresalir.

Según Pallas (2009), la Seguridad de la Información no es un activo que se pueda comprar; la información debe ser gestionada, debe poder medirse. La información permanece en constante evolución, por lo que debe ser evaluada y monitoreada, con métricas de comparación, con diferentes escenarios para poder tomar decisiones, dependiendo de los riesgos que se afronten y los recursos disponibles.

La seguridad de la información es un aspecto del negocio de carácter estratégico, por lo que debe ser primordial optimizar la relación Costo/Beneficio. Como explica Pallas (2009), hay que minimizar los riesgos, maximizando el logro de los objetivos sin salirse del presupuesto de acuerdo a los parámetros establecidos por la empresa u organización.

La meta a la que se desea llegar con la seguridad de la información, es permitir que una entidad u organización cumpla con sus objetivos de negocio o su misión.

Así como los SGSI requieren estar relacionados con las metas, objetivos, misión etc., de la organización, en la Seguridad de la Información existen relaciones entre procesos de negocio y los sistemas de información, y entre los mismos sistemas de información, también entre los propios procesos del negocio. Estas relaciones se toman en cuenta para lograr una efectiva seguridad. (Pallas, 2009)

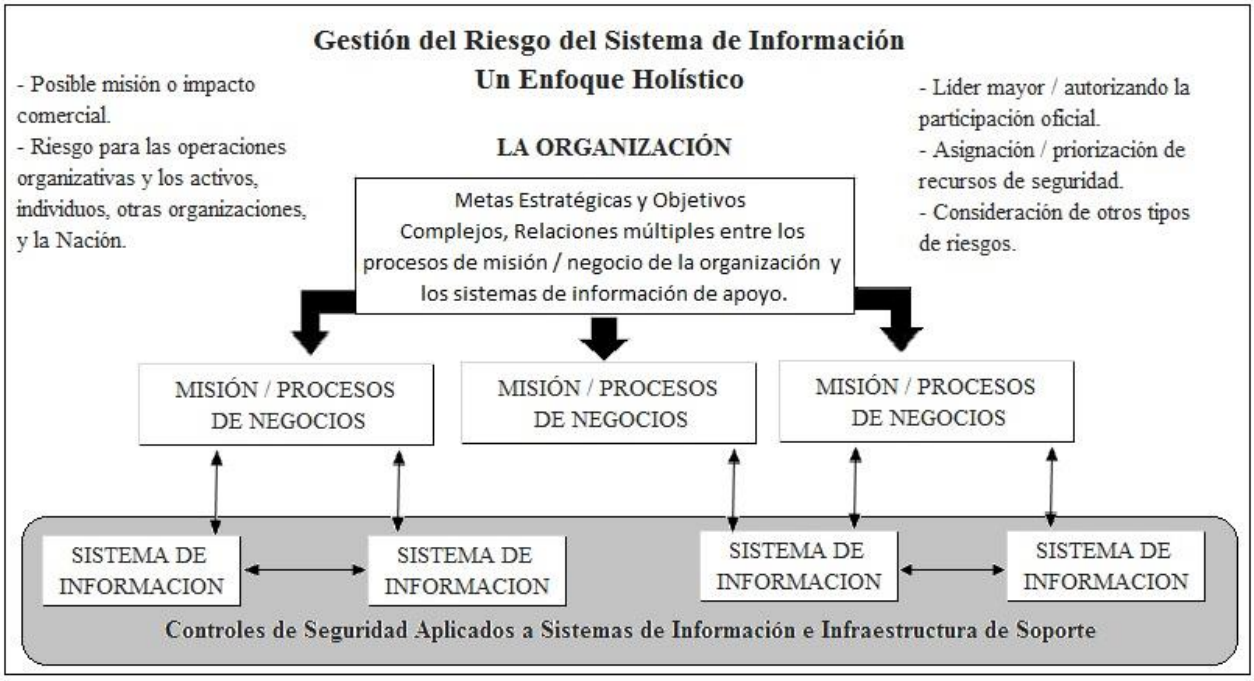

Ilustración 7: Visión organizacional de la seguridad de la información.
Fuente: Pallas, 2009

1.3. Riesgos

Como Areitio (2008) explica, la gestión del riesgo es parte importante en la gestión de la seguridad y se lo define como el proceso en el cual se puede identificar y cuantificar la probabilidad de que se pueda producir alguna amenaza y de establecer un rango aceptable de riesgo para una entidad u organización. La valoración de los riesgos consiste en identificar los problemas antes de que se produzcan.

Una circunstancia no deseada presenta tres componentes: amenaza, vulnerabilidad e impacto. Si ninguno de estos factores aparece, puede que no se ocasione una circunstancia de seguridad o que aparezca riesgo alguno.

Ilustración 8: Componentes del proceso de riesgos.
Fuente: Areitio, 2008

Las salvaguardas o conocidas como controles, medidas o contramedidas ayudan a reducir la intensidad o gravedad de los riesgos. Estas pueden actuar contra lo antes explicado, la amenaza, la vulnerabilidad, el impacto o incluso actuar contra el riesgo. Sin embargo, debido al alto coste económico y a incertidumbres asociadas, no se puede atenuar todos los riesgos en un cien por ciento, por lo que, siempre debe aceptarse algún riesgo residual.

1.3.1 Análisis de riesgos.

Este análisis es el estudio que toda organización debe realizar, para identificar las vulnerabilidades a las que se encuentran comprometidos sus activos, también para poder identificar cuáles son las amenazas que se pueden presentar a raíz de estas vulnerabilidades. La organización debe identificar los riesgos para poder establecer medidas que ayuden en la seguridad de la información.

Giraldo (2016), citando a Juan Manuel, dice que “el análisis de riesgos es una herramienta que permite identificar, clasificar y valorar los eventos que pueden amenazar la consecución de los objetivos de la organización y establecer las medidas oportunas para reducir el impacto esperable hasta un nivel tolerable”.

Para entender la seguridad en un sistema de información, hay que conocer los elementos que lo integran, analizar el nivel de vulnerabilidad de cada uno frente a ciertas amenazas y valorar el impacto que un ataque ocasionaría sobre el sistema.

Activos de información. – aquellos recursos que forman parte del sistema de información o que se relacionan, la presencia de los mismos facilita o colabora con el funcionamiento de una organización y la consecución de sus objetivos. Se pueden clasificar como:

- Datos
- Software
- Hardware
- Redes
- Soportes
- Instalaciones
- Personal
- Servicios (Aguilera, 2010)

Amenazas. – uno o varios factores de diferente naturaleza (máquinas, personas o sucesos), que de una u otra forma podrían atacar al sistema causando daños aprovechando su nivel de vulnerabilidad. Pueden dañar o alterar la información de una u otra forma.

Para Aguilera (2010), las amenazas en función de la intervención, alteración o daño que pueden causar sobre la información se pueden clasificar como:

- De interrupción: su objetivo es deshabilitar el acceso a la información; por ejemplo, bloqueando el acceso a los datos, saturando los canales de comunicación o destruyendo componentes físicos.
- De interceptación: captar información confidencial de la empresa u organización por medio de equipos, programas o personas no autorizadas.
- De modificación: los equipos, programas o personas no se limitan al acceso de la información, sino que también la modifican.
- De fabricación: agregarían información falsa en el conjunto de información del sistema.

Según el origen, las amenazas se pueden clasificar en:

- Accidentales: se pueden dar mediante errores humanos, fallos en los equipos, ambientales, en las redes, en el software, accidentes meteorológicos, etc.
- Intencionados: siempre se deben a los actos humanos, como inserción de código malicioso, intrusión informática, robos o hurtos. Este tipo de amenazas intencionadas se pueden originar fuera de la organización o dentro de ella.

Riesgos. – hace referencia a la materialización de una amenaza aprovechando el nivel de vulnerabilidad existente, generando un cierto impacto en la organización. Cuanto mayor es la vulnerabilidad, mayor es el riesgo, cuando no existe vulnerabilidad es casi nula la existencia de un riesgo. Para hacer frente a los riesgos, una organización puede optar por:

- Asumir el riesgo sin hacer nada: resulta lógico cuando el perjuicio no tiene mucha importancia o cuando los costes son demasiado elevados superando el coste de la reparación del daño.

- Mitigar el riesgo: se toman las adecuadas medidas para suavizar el nivel del impacto.
- Transferirlo: se traspasa el riesgo a terceros, por ejemplo, a una aseguradora.

Vulnerabilidad. – es el grado de exposición de un activo de información, que puede ser aprovechado por una amenaza para materializarse como un riesgo. No todos los activos pueden ser vulnerables a una misma amenaza. Mediante el análisis de los riesgos hay que tener en cuenta la vulnerabilidad en cada activo.

Hacen referencia a las debilidades existentes en un sistema de información, lo que conlleva a que dicho sistema pueda ser atacado. Deben ser expresadas en escala numérica para poder cuantificar su impacto, se sugiere que sean evaluadas individualmente. (Crespo E. , 2016)

Crespo (2016) dice que la vulnerabilidad se da por el numero de ocurrencias que puedan presentarse en un tiempo, es por esto que debe expresarse mediante la formula: Vulnerabilidad=Frecuencia estimada / Días al año. Sugiere la siguiente escala de frecuencias de repetición.

Tabla 1:
Vulnerabilidades y frecuencias.

Vulnerabilidad	Rango	Valor
Frecuencia extrema	1 vez al día	1
Frecuencia alta	1 vez cada dos semanas	26/365 = 0.071
Frecuencia media	1 vez cada dos meses	0.016
Frecuencia baja	1 vez cada 6 meses	0.005
Frecuencia muy baja	1 vez al año	0.002

Fuente: (Crespo, 2016)

Ataques. – cuando se ha materializado una amenaza. En función del impacto causado a un activo, se clasifican en:

- Activos: cuando dañan, modifican, suprimen, agregan información, o saturan los canales de comunicación.

- Pasivos: son los más difíciles de detectar. Únicamente acceden sin autorización al contenido del sistema.

Impactos. – la consecuencia de que una amenaza se haya materializado sobre uno o varios activos, es el daño causado.

Dichos impactos pueden ser cuantitativos, si los daños se pueden cuantificar económicamente o cualitativos, si son daños no cuantificables, por ejemplo, los causados a los derechos de una persona.

1.3.2 Tratamiento y gestión de riesgos.

Es un punto primordial que toda organización debe realizar para evitar pérdidas económicas e inestabilidad generada por algún tipo de riesgo.

Dentro de una auditoria se toman medidas para reducir el riesgo y establecer la forma de soportar pérdidas que genera. Según Minchala (2016) existen varias medidas de tratamiento para los riesgos y son:

- Evitar el riesgo: Para prevenir un riesgo se sostiene que, la probabilidad de que suceda es alta, por ende, representa un alto peligro para la organización. Es por esto que es recomendable no proceder con la actividad que incorporaría el riesgo, eliminarla, sustituirla o escoger medios alternativos no peligrosos. El problema de evitar riesgos, es que riesgos no identificados puedan volverse más significativos o perder oportunidades de negocio.
- Prevenir el riesgo: Para prevenir un riesgo se habla de anticiparse a que pueda ocurrir un evento de riesgo. Para esto se pueden establecer procedimientos, medidas, políticas o controles que disminuyan la probabilidad o que eliminen el evento generador del riesgo.

Existen diversas formas de prevención como son:

- Inspecciones y pruebas de seguridad.
- Mantenimiento preventivo.
- Diversificación.
- Inversión en información.
- Disminución del nivel de exposición.
- Entrenamiento. (Minchala, 2016)

- Protegerse de un riesgo: Medidas que actúan al momento de presentarse el riesgo, por ejemplo, un antivirus que actúa y trata de eliminar los virus en un ordenador. Las medidas de protección más usadas son:
  - Plan de contingencia
  - Sistemas automáticos de protección
  - Plan de emergencia
  - Equipo de protección personal. (Minchala, 2016)
- Aceptar el riesgo: Se asume el riesgo y las consecuencias que traiga al momento de presentarse. Se asume debido a que está por debajo de un valor de riesgo aceptable; es decir, su frecuencia es baja e impacto leve, por lo tanto, queda documentado que se conoce del riesgo y se acepta. Estos riesgos asumidos deben ser controlados y revisados periódicamente para evitar la evolución y así también evitar que la estabilidad de la organización no entre en peligro.
- Retener: Los riesgos se los conserva cuando se ha planeado, con un fondo y otras cosas para dar respuesta a las posibles pérdidas ocasionadas si es que ocurre el riesgo.

- Transferir el riesgo a un tercero: ocurre cuando se pasa la responsabilidad del riesgo a otro compañía o persona para su debido análisis. Esta transferencia de responsabilidad se puede dar mediante un contrato outsourcing o una póliza de seguro. Un método usual para transferir un riesgo es cubrirlo mediante un seguro, pero esta opción tiene sus ventajas como ser una opción económica y sencilla de aplicar y su desventaja más clara es que se trata de una medida atenuante; es decir, que se aplicaría únicamente cuando los daños ya se han producido y por esto se permitirá recuperar solo los aspectos económicos. (Minchala, 2016)
- Eliminar el riesgo: no suele ser una opción muy viable debido al alto costo o la complejidad que implica, si se cree necesario, se establecerán los pasos para conseguirlo como, por ejemplo, eliminar el activo o el proceso que es la fuente del riesgo.

La gestión de riesgos hace referencia a una secuencia de actividades, de procesos para que los riesgos sean identificados, clasificados, evaluados y controlados en su totalidad. (López & Vásquez, 2016)

López (2016) citando a UTE (2013), dice que la gestión de riesgos está formada por cuatro etapas:

- Análisis de Riesgo: establece una valoración y priorización de los riesgos basado en la información disponible y obtenida en el proceso de identificación, para así establecer el nivel del riesgo y las acciones correctivas a implementar en el siguiente paso. En el análisis, la probabilidad de que ocurra y el impacto son valores necesarios para determinar la magnitud de las consecuencias.

  Cuando se habla de la probabilidad de que ocurra se tiene que tener en cuenta las siguientes consideraciones:

- Interés o la alteración por parte de individuos externos.
- Nivel de vulnerabilidad.
- Frecuencia en que ocurren los incidentes. (Erb, 2008)

Las probabilidades se pueden valorar como:

- Baja: la posibilidad de un ataque es muy lejana debido a ciertas condiciones.
- Mediana: es poco probable un ataque a corto plazo debido a ciertas condiciones, pero no suficientes para evitarlo a largo plazo.
- Alta: Ninguna condición puede impedir el desarrollo del ataque.

La magnitud del impacto se puede valorar como:

- Bajo: el daño no perjudica ningún componente de la organización.
- Mediano: provoca daño en algún componente de la organización. A largo plazo puede provocar daños incontrolables.
- Alto: en corto plazo puede provocar mucho daño a la organización.

- Clasificación de riesgos: una vez que se han analizado los riesgos existentes se realiza una clasificación dependiendo de la magnitud del impacto y su probabilidad de ocurrencia para dar prioridades y tomar acciones contra cada uno de estos.
- Control de riesgos: Acciones que se realizan para controlar y reducir los riesgos y minimizar pérdidas analizando el funcionamiento, la efectividad, y el correcto cumplimiento de las medidas de protección. Las conclusiones que dan como resultado del control de riesgos, ayudan cuando se entra otra vez en el proceso de análisis de riesgo y se usan como fuente de información.

Mediante un análisis costo-beneficio se realizará un análisis para determinar si los riesgos pueden ser aceptados, mitigados, transferidos o evitados de ser posible.

- Reducción de riesgos: se logran mediante la implementación de medidas de protección, basados en los resultados del análisis y la clasificación de los riesgos

  Según Erb (2008), existen mediades que ayudarian en la reduccion de los riesgos:

  - Medidas fisicas y tecnicas: como control de acceso, antivirus, datos cifrados, contraseñas inteligentes, etc.
  - Medidas personales: como la capacitacion, contratacion, sensibilizacion, etc.
  - Medidas organizativas: como auditoria, normas y reglas, seguimiento de control, etc.

"La implementación de las medidas no es una tarea aislada, única, sino un proceso continuo, su manejo y mantenimiento debe estar integrado en el funcionamiento operativo institucional, respaldado por normas y reglas que regulan su aplicación." (Erb, 2008)

Existen varias metodologías que ayudan a la gestión del riesgo como:

Tabla 2:
Metodologías para el control de Riesgos

Metodología	Descripción	Organización	País
CMMI	*Capability Maturity Model Integration.*	SEI *(Software Engineering Institute).*	Estados Unidos
SPICE	*Software Process Improvement and Capability Determination.*	ISO *(International Organization for Standardization).*	Suiza
PMBOOK	*Project Management Body of Knowledge.*	PMI *(Project Management Institute).*	Estados Unidos
COBIT	*Control Objectives for Information and related Technology.*	ISACA *(Information Systems Audit and Control Association).*	Estados Unidos
OCTAVE	*Operationally Critical Threat*	*Carnegie Mellon* SEI *(Software Engineering*	Estados Unidos

	Asset and Vulnerability Evaluation.	*Institute)* y CERT *(Computer Emergency Response Team).*	
MAGERIT	Metodología de Análisis y Gestión de Riesgos de IT	MAP (Ministerio de Administración Pública).	España
SECURITY RISK MANAGMENT GUIDE	Administración de Riesgos de Seguridad.	Microsoft.	Estados Unidos
ECU@RISK	Metodología para la gestión de riesgos de información.	Universidad del Azuay	Ecuador

Fuente: (López & Vásquez, 2016)

1.3.3 Riesgo Informático.

Como se ha explicado anteriormente, la información es el activo más importante que toda entidad u organización posee, es por esto que deben existir técnicas o medidas que aseguren el resguardo de estas, sin dejar a un lado la protección de los equipos que la contienen.

Existen diversas medidas o técnicas que brindan seguridad con procedimientos o barreras que resguardan el acceso a los datos y solo permitiendo el acceso a las personas autorizadas por la organización. Para López (2016) y compañero citando a Ulloa (2015), existen medidas como:

1. Restringir el acceso (de personas dentro y fuera de la organización) a los programas y archivos.
2. Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
3. Asegurar que se utilicen los datos, archivos y programas correctos.
4. Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no se desvié.

5. Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
6. Organizar a cada uno de los empleados por jerarquía informática, con clases distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
7. Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

1.4 Las MPYMES y la Seguridad de la información en Ecuador

Diversos factores como recursos insuficientes, poca inversión en software y hardware, falta de acceso a servicios técnicos y la poca conciencia o conocimiento sobre las Tecnologías de la Información (TI), hacen que una organización avance de manera desacelerada en nivel económico y de conocimientos.

Para López (2016), una parte importante de las TI es el Internet, debido a que es el medio más utilizado para tener acceso a los últimos avances tecnológicos, compartir información y sobre todo la conexión con el resto del mundo; así mismo, como se puede obtener beneficios de este medio se puede ser vulnerables a ataques poniendo en riesgo el activo más valioso, la información.

En la actualidad se puede notar la importancia del internet para el negocio ya que un 100% de MPYMES tienen contratado un servicio de internet, lo que favorece los ataques cibernéticos de manera evidente. Esto hace que sea necesaria la adopción de mecanismos y metodologías que aporten a la seguridad de la información para el desarrollo del negocio, ya que sin las mismas serían muy vulnerables.

Esto conlleva a que las organizaciones tengan que cumplir con ciertas normas de seguridad informática dependiendo de su modelo de negocio. Las principales normas acogidas por el mercado corporativo son: ITIL 35%, COBIT 12%, PCI-DSS con un 10%, JB 2005-834 con 4%, y el estándar ISO 27001 con un 4%. (Solorzano, Rezabala , & Aranda, 2013)

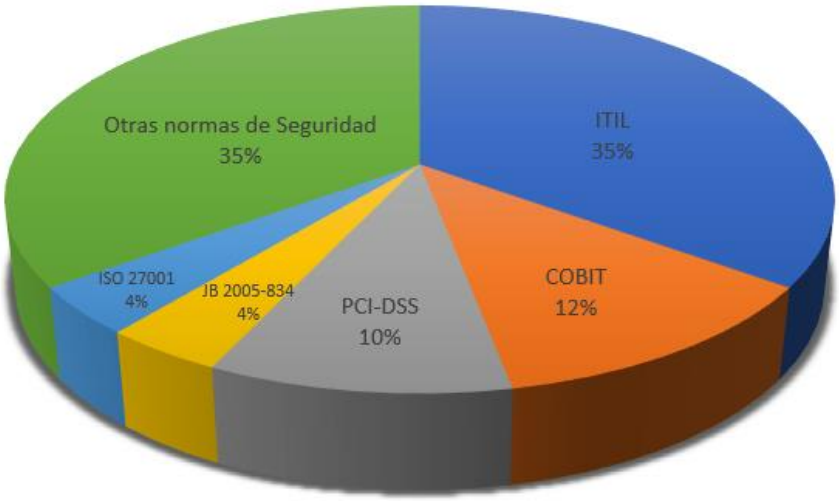

Ilustración 9. Normas acogidas por el mercado corporativo.
Fuente: Creado por el autor.

Como se explicó anteriormente, ITIL es el marco de referencia más utilizado por el mercado corporativo ecuatoriano ya que detalla las mejores prácticas y recomendaciones para la administración de servicios de Tecnologías de la Información. Otro marco de referencia con gran acogida por el mercado corporativo es COBIT ya que es buena guía de las mejores prácticas para el control y supervisión de Tecnologías de la Información, seguido de PCI-DSS, JB 2005-834, ISO 27001 y otras normas que proporcionan buenas prácticas en temas referentes a TI.

Solorzano (2013) y compañeros, señalan que un 80% tiene definidas políticas globales de seguridad dentro de una organización a pesar de que el 98% está consciente de que es posible perder información por robo u otros factores. Lo que preocupa señala, que solo el 39% cree que cuenta con un alto nivel de seguridad informática.

Como la información es el activo más importante de las organizaciones, puede verse afectada por diversos factores y la medida más eficiente para la protección de los datos es determinar buenas políticas para la copia de seguridad o *backups*. El mercado corporativo indica que el 94% realizan copias de seguridad y casi en la totalidad cuentan con procedimientos para realizar las copias, únicamente el 69% de dichas copias es automatizada y solo el 59% es guardada en lugares con

acceso restringido, también indica que solo el 65% de las copias son guardadas fuera del lugar de trabajo.

La mayoría de los ataques físicos ocurren generalmente cuando una persona tiene o puede acceder al sistema informático, es por esto que los controles de acceso físico deben estar bien definidos por una organización. El mercado corporativo ecuatoriano indica que el 89% de las organizaciones cuentan con controles de acceso, el 67% cuenta con log o ficheros indicando los accesos autorizados e intentos de acceso ilícitos, un 63% de estas organizaciones indican tener separados los recursos a los que pueden acceder los usuarios autorizados una vez que pasaron los filtros de seguridad.

Los datos que Solorzano (2013) y compañeros han obtenido, también señalan que un 87% indica contar con herramientas corporativas para la protección contra virus, el 85% indica que su antivirus protege los correos electrónicos y las descargas web, 89% señala actualizar su antivirus y el 69% ha indicado que alguna vez ha experimentado algún problema con algún tipo de virus.

El mercado corporativo ecuatoriano indica que un 72% cuenta con un plan de seguridad y un 78% con un plan de contingencia lo que indica que de alguna manera hay preocupación por parte de las organizaciones.

El acelerado desarrollo de la tecnología a nivel mundial y el incremento del acceso a internet en el Ecuador donde casi en un 100% las empresas tienen contratado servicio de internet han generado que las empresas ecuatorianas dedicadas a la venta de servicios y productos de tecnología ofrezcan productos de seguridad informática que vayan a la par con dicho desarrollo. Entre los productos de seguridad informática que se ofrece en el medio están los siguientes.

Tabla 3:
Productos de seguridad informática que se ofrecen en Ecuador

Productos
Seguridad Perimetral Gestionada
Análisis de Tráfico
Análisis del Riesgo
Test de Penetración
Ethical Hacking
Informática Forense
Diagnóstico de Seguridad de los Sistemas
Diagnóstico de Vulnerabilidades y Riesgos
Planeación y Administración de la Seguridad Informática
Planeación Estratégica de Sistemas de Información
Asesoría Implantación ISO 27001
Auditorias de Seguridad de Información
Auditoria IT
Software de Seguridad Informática
Planes para Contingencias y Seguridad de la Información
Capacitación
Seguridad en Redes

Fuente (Solorzano, Rezabala , & Aranda, 2013)

1.5. Los marcos de referencia internacionales utilizados en la gestión de riesgo

Según Giraldo (2016) citando al gobierno de España indica que las normas ISO son estandares que han sido establecidos por la Organización Internacional para la Estandarizacion (ISO) y la Comision Electronica Internacional (IEC) que proporcionan buenas prácticas para el aseguramiento de la seguridad de la información.

Las normas de la familia ISO 27000, principalmente la ISO 27001 e ISO 27002 tienen como objetivos los siguientes:

- Revisión y mejora continua del SGSI.
- Establecer un marco metodológico para un SGSI.

- Uso de métricas para evaluar efectividad y eficiencia de los controles y del propio SGSI.
- La documentación de políticas, procedimientos, controles y tratamiento de riegos.
- Gestión de Riesgos
- La adopción de controles proporcionales a los riesgos percibidos.
- Tratamiento de los incidentes de seguridad.
- Identificación y asignación de responsabilidades al nivel adecuado.
- Generación y preservación de evidencias.
- Formalización, seguimiento y revisión de los controles y riesgos, de forma periódica y metodológica. (Pallas, 2009)

1.5.1 ISO/IEC 27001.

Publicada el 15 de octubre de 2005 y basada en el modelo de Deming. Para Pallas (2009), esta norma específica los requisitos para implementar, operar, monitorear, sostener y mejorar un sistema de gestión de seguridad de la información. La norma puede ser aplicada en cualquier tipo de organización, además especifica los requerimientos para la implementación de controles de seguridad, fomenta la importancia de entender los requerimientos de seguridad de la información y la necesidad de establecer una política para la seguridad de la información en una organización.

A continuación, según Pallas (2009) se presentará los principales procesos que indica la norma ISO 27001 en cada etapa del ciclo PHVA:

Tabla 4:
PHVA aplicado a la norma ISO/IEC 27001.

Ciclo PHVA	Procesos
Planificar - Plan	Establecer el contexto. Alcance y Limites. Definir Política del SGSI. Definir Enfoque de Evaluación de Riesgos. Identificación de riesgos. Análisis y Evaluación de riesgos. Evaluar alternativas para el Plan de tratamiento de riesgos. Aceptación de riesgos. Declaración de Aplicabilidad.
Hacer – Do	Implementar plan de tratamiento de riesgos. Implementar los controles seleccionados. Definir las métricas. Implementar programas de formación y sensibilización. Gestionar la operación del SGSI. Gestionar recursos. Implementar procedimientos y controles para la gestión de incidentes de seguridad.
Verificar - Check	Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad. Revisión de la evaluación de riesgos periódicamente. Realizar auditorías internas. Revisión de alcance y líneas de mejoras del SGSI por la Dirección. Actualizar los planes de seguridad. Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI.
Actuar - Act	Implementar las mejoras identificadas para el SGSI. Implementar las acciones correctivas y preventivas pertinentes. Comunicar acciones y mejoras a todas las partes involucradas. Asegurarse que las mejoras logren los objetivos previstos.

Fuente: (Pallas, 2009)

Para Cordero (2015) la norma ISO 27001 tiene los siguientes dominios:

Política de Seguridad: El objetivo es garantizar el soporte y gestión necesarios para la seguridad, según los requisitos institucionales y normativos.

Organización de la seguridad de la información: Tiene como fin instaurar un marco de referencia para la implementación y control de la seguridad de la información.

Gestión de activos: Cuyo objetivo es asegurar los activos de la organización.

Seguridad de los recursos humanos: Tiene como objetivo fijar las medidas necesarias para controlar la seguridad de la información, que sea manejada por los recursos humanos.

Seguridad física y del ambiente: Permite proteger las instalaciones y la información manejada en ellas.

Gestión de comunicaciones y operaciones: Tiene como objetivo determinar el procedimiento y responsabilidades de las operaciones que realiza la organización

Control de acceso: Asegura el acceso autorizado a los sistemas de información que se encuentran en la organización.

Adquisición, desarrollo y mantenimientos de los sistemas de información: Dirigida a organizaciones que desarrollen software internamente o que tengan un contrato con otra organización que sea la encargada de desarrollarlo.

Gestión de incidentes en la seguridad de la información: Aplica un proceso de mejora continua en la gestión de percances de seguridad de la información.

Gestión de la continuidad del negocio: Tiene como objetivo asegurar la continuidad operativa de la organización.

Cumplimiento: Tiene como fin asegurar que los requisitos legales de seguridad referidos al diseño, operación, uso y gestión de los sistemas de información se cumplan.

Nueva revisión ISO 27001 2013 - ¿Qué ha cambiado?

"ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) para cualquier organización sin importar su tipo o tamaño." (BSI Group México)

La ISO 27001: 2013 se ha desarrollado basada en el anexo SL, en el cual se proporciona una serie de especificaciones a seguir, un formato a seguir para el desarrollo documental de un sistema de gestión. Para evitar problemas de integración con otros marcos de referencia, la ISO 27001 alinea todos los documentos bajo una misma estructura de sistemas de gestión. (González, 2013)

Ilustración 10. Estructura del nuevo estándar.
Fuente: González, 2013

Se han introducido nuevos conceptos o han sido actualizados, y son los siguientes:

Tabla 5:
Nuevos conceptos ISO 27001:2013

Concepto nuevo/actualizado	**Explicación**
Contexto de la organización	El ambiente en el que la organización opera
Problemas, riesgos y oportunidades	Reemplaza acciones preventivas
Partes interesadas	Reemplaza accionistas (*stakeholders*)
Liderazgo	Requerimientos específicos para la alta dirección
Comunicación	Hay requerimientos específicos tanto para comunicaciones internas como externas
Objetivos de seguridad de la Información	Los objetivos de seguridad de la información ahora se establecen como funciones relevantes y niveles
Evaluación de riesgos	La identificación de activos, amenazas y vulnerabilidades ya no es un pre requisito para la identificación de riesgos de seguridad de la información
Propietario de riesgo	Reemplaza propietario de los activos
Plan de tratamiento de riesgos	La efectividad del plan de tratamiento de riesgos es ahora considerada como más importante que la efectividad de los controles
Controles	Los controles ahora son determinados durante el proceso de tratamiento de riesgos, en lugar de ser seleccionados del Anexo A
Información documentada	Reemplaza documentos y registros
Evaluación del desempeño	Cubre las mediciones del SGSI y de la efectividad del plan de tratamiento de riesgos
Mejora continua	Se pueden utilizar metodologías distintas a Planear-Hacer-Verificar-Actuar (PDCA por sus siglas en inglés)

Fuente: (BSI Group México)

Alineación.

El estándar ISO 27001 ya no se basa en el modelo en el modelo PDCA, sino aplica la estructura de alto nivel, principales definiciones expuestas en el Anexo SL, etc. Es por esto que mantiene compatibilidad con otros estándares de sistema de gestión que han adoptado el Anexo SL.

Ilustración 11. Alineación de la ISO 27001 con otros estándares.
Fuente: https://advisera.com/27001academy/knowledgebase/infographic-new-iso-27001-2013-revision-what has-changed/

Comparación ISO 27001:2005 – ISO 27001:2013.

La nueva estructura del Anexo A agrega 3 dominios de control:

- Criptografía, separada del dominio Adquisición, desarrollo y mantenimiento de la información.
- Relación con proveedores
- Tercero que da como resultado de la división del dominio Gestión de comunicaciones y operaciones en dos nuevos dominios: Operaciones de seguridad y Seguridad de las comunicaciones. (Gutierrez, 2013)

Los dominios en la nueva revisión se ven tal como se lo presenta a continuación:

ISO 27001:2005	ISO 27001:2013
1. Manual del SGSI	1. Políticas de seguridad
2. Organización de la seguridad	2. Organización de la seguridad de la información
3. Gestión de Activos	3. Seguridad de los RRHH
4. Seguridad de RRHH	4. Gestión de Activos
5. Seguridad Física	5. Control de acceso
6. Gestión de comunicaciones y operaciones	6. Criptografía
7. Control de Acceso	7. Seguridad física y ambiental
8. Adquisición, desarrollo y mantenimiento de la información	8. Operaciones de seguridad
9. Gestión de incidentes	9. Seguridad de las comunicaciones
10. Continuidad del negocio	10. Sistemas de adquisición, desasrrollo y mantenimiento
11. Cumplimiento	11. Relaciones con proveedores
	12. Gestión de incidentes
	13. Seguridad de la información para la continuidad del negocio
	14. Cumplimiento

Ilustración 12. Cambio en dominios de la ISO 27001.
Fuente: El autor

Ilustración 13. Comparación ISO 27001:2005 con ISO 27001:2013.
Fuente: https://advisera.com/27001academy/knowledgebase/infographic-new-iso-27001-2013-revision-what-has-changed/

Aunque los cambios del Anexo A no han sido drásticos, es importante que las organizaciones que estén certificadas o aquellas que utilicen este estándar como guía revisen los cambios.

El Anexo A es ahora “objetivos de control de referencia y controles” y se ha es simplificado la introducción. Establece que los objetivos de control y los controles derivan directamente de ISO/IEC 27002:2013 y que el Anexo es utilizado en el contexto de la Cláusula 6.1.3. (BSI Group México)

Requisitos.

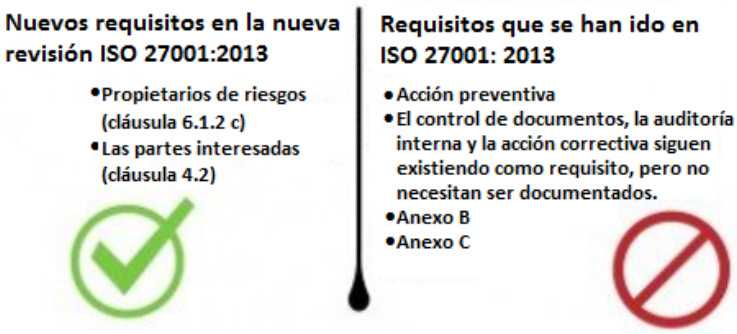

Ilustración 14. Requisitos ISO 27001:2013.
Fuente: https://advisera.com/27001academy/knowledgebase/infographic-new-iso-27001-2013-revision-what-has-changed/

Similitudes y diferencias.

Ilustración 15. Similitudes y diferencias entre revisiones ISO 27001:2013.
Fuente: https://advisera.com/27001academy/knowledgebase/infographic-new-iso-27001-2013-revision-what-has-changed/

La siguiente imagen ilustra la relación entre ISO/IEC 27001:2013 e ISO/IEC 27001:2005. Esta imagen esta simplificada únicamente para motivos ilustrativos. Para un mapeo de datos más detallado está disponible en www.bsigroup.com/27kmapping.

ISO/IEC 27001: 2013 (Número de controles)	ISO/IEC 27001:2005										
	Política de seguridad	Organización	Gestión de activos	Recursos Humanos	Físicos	Comunicaciones	Control de acceso	Adquisiciones	Incidentes	Continuidad del negocio	Cumplimiento
	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15
A.5.1 Dirección de la gestión de la seguridad de información (2)	X										
A.6.1 Organización interna (5)		X		X		X					
A.6.2 Dispositivos móviles y tele trabajo (2)							X				
A.7.1 Antes de emplear (2)				X							
A.7.2 Durante el empleo (3)				X							
A.7.3 Despido y cambio del empleado (1)				X							
A.8.1 Responsabilidad para los activos (4)			X	X							
A.8.2 Información clasificada (3)			X			X					
A.8.3 Manejo de medios (3)						X					
A.9.1 Requerimientos del negocio de control de acceso (2)							X				
A.9.2 Gestión de acceso de usuario (6)				X			X				
A.9.3 Responsabilidades de los usuarios (1)							X				
A.9.4 Sistema y aplicación de acceso de control (5)							X	X			
A.10.1 Controles criptográficos (2)								X			
A.11.1 Áreas de seguridad (6)					X						
A.11.2 Equipo (9)					X		X				
A.12.1 Procedimientos operacionales y responsabilidades (4)						X					
A.12.2 Protección contra el mal uso						X					
A.12.3 Copia de seguridad (1)						X					
A.12.4 Acceso y monitoreo (4)						X					
A.12.5 Control de software operacional (1)								X			
A.12.6 Gestión de la vulnerabilidad técnica (2)								X			
A.12.7 Consideraciones de auditoría del sistema de información (1)											X
A.13.1 Gestión de seguridad de la red (3)						X	X				
A.13.2 Transferencia de información (4)		X				X					
A.14.1 Requerimientos de seguridad de los sistemas de información (3)						X		X			
A.14.2 Seguridad en el desarrollo y procesos de soporte (9)						X		X			
A.14.3 Datos de prueba (1)								X			
A.15.1 Seguridad de información en relaciones con proveedores (3)		X									
A.15.2 Gestión de prestación de servicios del proveedor (2)						X					
A.16.1 Gestión de los incidentes y mejoras de la seguridad de información (7)									X		
A.17.1 Continuidad de la seguridad de información (3)										X	
A.17.2 Redundancias (1)											
A.18.1 Cumplimiento con requerimientos legales y contractuales (5)											X
A.18.2 Revisiones de seguridad de la información (3)		X								X	

Ilustración 16. Mapeo de controles del Anexo A.
Fuente: BSI Group México

En la columna del lado izquierdo se enlista los grupos de control en el Anexo A para ISO/IEC 27001:2013. Del lado derecho hay once columnas que corresponden a los controles en el Anexo A de ISO/IEC 27001:2005.

Una X significa que hay una correspondencia entre los controles del ISO 27001:2013 y la ISO 27001:2005. Para ver las relaciones exactas consulte el mapeo de datos detallado.

Nuevos controles de seguridad.

Nuevos controles de seguridad en la revisión de 2013 que no existían en la revisión 2005

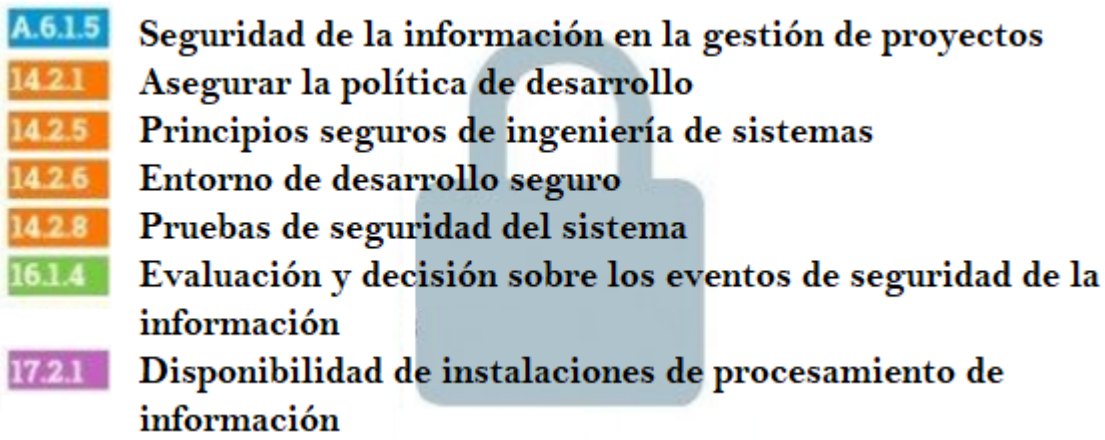

Ilustración 17. Nuevos controles de seguridad ISO 27001:2013.
Fuente: https://advisera.com/27001academy/knowledgebase/infographic-new-iso-27001-2013-revision-what-has-changed/

A continuación, se enlista los controles que González (2013) explica, ya no forman parte del estándar:

Tabla 6:
Controles que no forman parte del estándar ISO 27001:2013

Control	Descripción	Cambia por	Incluye los controles de la ISO 27001:2005
A.6.1.1	Comité de gestión para la seguridad de la información	Roles de la seguridad de la información y sus responsabilidades	A.6.1.3 y A.8.1.1
A.6.1.2	Coordinación de seguridad de la información	Contacto con autoridades	A.6.1.6

A.6.1.4	Procesos de autorización para instalaciones para procesamiento de información	Seguridad de la información en la gestión de proyectos	
A.6.2.1	Identificación de riesgos relacionados con agentes externos	Política de dispositivo móvil	A.11.7.1
A.6.2.2	Direccionamiento de seguridad al tratar con clientes	Trabajo a distancia	A.11.7.2
A.10.2.1	Entrega del servicio		
A.10.7.4	Seguridad del sistema de documentos		
A.10.8.5	Sistema de información de negocios		
A.10.10.2	Seguimiento al uso de sistema		
A.10.10.5	Falla en el registro		
A.11.4.2	Autenticación de usuarios para conexiones externas		
A.11.4.3	Identificación de equipos		
A.11.4.4	Puerto remoto de diagnóstico y configuración de protección		
A.11.4.6	Control para la conexión de redes		
A.11.6.2	Aislamiento del sistema sensible		
A.12.2.1	Validación de datos de entrada	Controles contra malware	A.10.4.1
A.12.2.2	Control de procesamiento interno		
A.12.2.3	Integridad de mensaje		
A.12.2.4	Validación de datos de salida		
A.12.5.4	Filtración de la información		
A.15.1.5	Prevención del uso indebido de las instalaciones para el procesamiento de información		
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información		

Fuente: (González, 2013)

Áreas donde el cambio será mínimo.

- Información documentada
- Políticas
- Evaluación de riesgos

- Control documental
- Términos de referencia para la alta dirección
- Responsabilidades
- Conciencia
- Auditoría interna
- Revisión de la gestión
- Acciones correctivas
- Mejora

Áreas que necesitan actualización.

- El enunciado de aplicabilidad

Nuevos requerimientos que deben de cumplirse ya.

- Partes interesadas y sus requerimientos
- Integración
- Comunicación

1.5.2 ISO/IEC 27002.

ISO/IEC 27002:2005.

Es una guía de buenas prácticas para la gestión de la seguridad de la información que describe objetivos de control y controles recomendables. Este código de buenas prácticas recomienda las medidas a implementar para que se aseguren los sistemas de información en las entidades u organizaciones. (Giraldo, 2016)

Contiene las mejores prácticas de los objetivos de control y controles en las siguientes áreas de gestión de seguridad de la información:

- Información de gestión de incidentes de seguridad
- Política de seguridad
- Gestión de continuidad del negocio
- Organización de la seguridad de la información
- Los sistemas de información de adquisición, desarrollo y mantenimiento
- Gestión de activos
- Comunicaciones y gestión de operaciones
- Recursos humanos de seguridad
- Control de acceso
- Seguridad física y ambiental
- Cumplimiento (Gonzales, 2016)

Para esta norma no es posible la certificación. Minchala (2016) explica que contiene 39 objetivos de control y 133 controles agrupados en 11 dominios.

ISO/IEC 27002:2013.

Ilustración 18. Relación entre 27002 y 27001.
Fuente: PECB, 2016

Proporciona pautas para las normas de seguridad de la información en la organización y las prácticas de gestión de seguridad de la información incluyendo la selección, implementación y administración de los controles. (International Organization for Standardization, 2013)

Diseñado para organizaciones con la intención de:

- Seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información que se basa en ISO/IEC 27001.
- Implementar controles de seguridad de la información comúnmente aceptados.
- Desarrollar sus propias directrices de gestión de la seguridad de la información.

ISO / IEC 27002: 2013 se organiza en las siguientes cláusulas principales:

Contiene 14 cláusulas de control de seguridad, que contienen conjuntamente un total de 35 categorías de seguridad principales y 114 controles. (PECB, 2016)

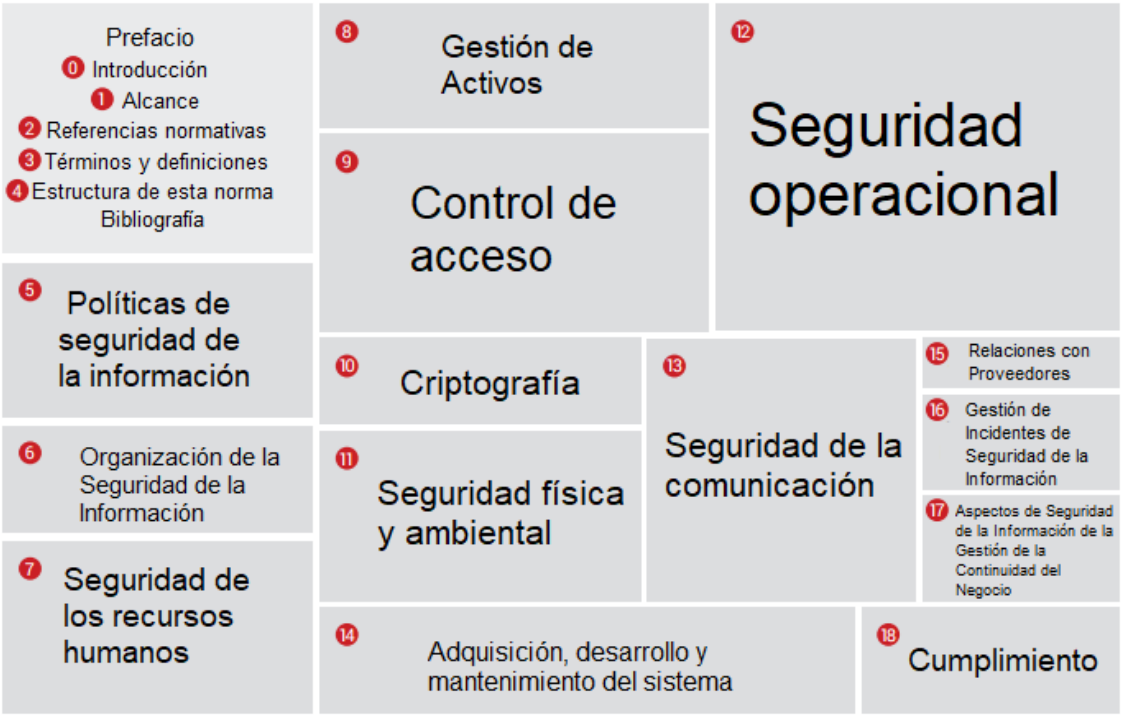

Ilustración 19. Cláusulas ISO 27002:2013.
Fuente: PECB, 2016

PECB (2016), describe cada uno de los objetivos y los controles requeridos y se enumeran a continuación.

Cláusula 5: Políticas de seguridad de la información

Objetivos:

- Facilitar apoyo y dirección de gestión para la seguridad de la información en conformidad con los requisitos del negocio, leyes y regulaciones relacionadas.

Cláusula 6: Organización de la Seguridad de la Información

Objetivos:

- Establecer un marco de gestión, iniciar la implementación y operación de la seguridad de la información dentro de la organización.
- Garantizar la seguridad en el uso de los dispositivos móviles y del teletrabajo.

Cláusula 7: Seguridad de los recursos humanos

Objetivos:

- Garantizar que empleados y contratistas comprendan sus responsabilidades y cumplan las funciones que les corresponda.
- Garantizar que empleados y contratistas cumplan conozcan y cumplan las responsabilidades de la seguridad de la información.
- Respaldar los intereses de la organización hasta culminar el empleo.

Cláusula 8: Gestión de Activos

Objetivos:

- Identificar los activos de la organización y determinar las responsabilidades de protección adecuadas.
- Asegurar que la información, de acuerdo a su importancia, reciba un nivel adecuado de protección.

- Prevenir la modificación, divulgación destrucción o eliminación no autorizada de la información.

Cláusula 9: Control de acceso

Objetivos:

- Limitar y controlar el acceso a la información e instalaciones de procesamiento de información.
- Evitar el acceso no autorizado a los servicios y sistemas y garantizar el acceso a los usuarios autorizados.
- Hacer que los usuarios sean responsables para proteger sus identificaciones de autenticación.

Cláusula 10: Criptografía

Objetivos:

- Garantizar el uso adecuado de la criptografía para la confidencialidad, integridad y autenticidad de la información.

Cláusula 11: Seguridad física y ambiental

Objetivos:

- Prevenir accesos físicos no autorizados, interferencias y daños en las instalaciones de procesamiento de la información.
- Evitar el daño, pérdida o robo de activos y la interrupción de las operaciones en la organización.

Cláusula 12: Seguridad operacional

Objetivos:

- Asegurar el buen funcionamiento de las instalaciones de procesamiento de la información.
- Garantizar que las instalaciones de procesamiento de información se encuentren protegidas contra el malware.
- Proteger contra la pérdida de datos.
- Garantizar la integridad de los sistemas operativos.
- Evitar la explotación de vulnerabilidades técnicas.
- Reducir al máximo el impacto de las actividades de auditoria en los sistemas operacionales.

Cláusula 13: Seguridad de la comunicación

Objetivos:

- Garantizar la protección de la información en las redes y en las instalaciones de procesamiento de la información.
- Mantener la seguridad de la información que es transferida dentro de la organización o que se transfiere a una entidad externa.

Cláusula 14: Adquisición, desarrollo y mantenimiento del sistema

Objetivos:

- Garantizar que la seguridad de la información es una parte integral a lo largo de todo el ciclo de vida de los sistemas de información.
- Garantizar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida del desarrollo de los sistemas de información.
- Garantizar la protección de los datos que son utilizados en las pruebas.

Cláusula 15: Relaciones con Proveedores

Objetivos:

- Garantizar la protección de activos a los que pueden acceder los proveedores.
- Conservar un nivel de seguridad acordado para la información y prestación de servicios de acuerdo con los acuerdos de proveedores.

Cláusula 16: Gestión de Incidentes de Seguridad de la Información

Objetivos:

- Asegurar un enfoque eficaz y coherente de la gestión de incidentes de seguridad de la información, incluida las debilidades de seguridad.

Cláusula 17: Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio.

Objetivos:

- La continuidad de la seguridad de la información debe ser incorporada en los sistemas de gestión de continuidad del negocio.
- Garantizar la disponibilidad de instalaciones de procesamiento de información.

Cláusula 18: Cumplimiento

Objetivos:

- Garantizar que la seguridad de la información sea implementada y operada de acuerdo a las políticas y procedimientos de la organización.
- Evitar infracciones legales o reglamentarias relacionadas con la seguridad de la información y de cualquier requisito de seguridad.

PECB (2016) indica también que los beneficios de la ISO/IEC 27002 son aplicables a cualquier organización y a cualquier nivel de madurez de seguridad, ofreciendo un conjunto flexible de controles para que una organización se proteja y reflejando nuevas amenazas a las que la organización se enfrenta.

Así pues, los empleados pueden disfrutar de un entorno de acceso a datos más confiable con menos interrupciones de trabajo.

1.5.3 ISO 27005.

Al ser una norma de la familia o serie ISO/IEC 27000 se encuentra alineada con la ISO 27001, por lo que propone también el ciclo (PHVA) aplicado a la gestión de riesgos. (Pallas, 2009)

Tabla 7:
PHVA aplicado a la norma ISO/IEC 27.005

Ciclo PHVA (PDCA)	Procesos de gestión de riesgos
Planificar - Plan	Establecer el contexto Identificación y evaluación de riesgos Plan de tratamiento de riesgos Aceptación de riesgos
Hacer – Do	Implementación de los controles y del Plan de tratamiento de riesgos.
Verificar – Check	Monitoreo y revisión continua de riesgos y del plan. (métricas, análisis, etc.)
Actuar - Act	Mantener y mejorar el proceso de gestión de riesgos

Fuente: (Pallas, 2009)

1.5.4 ISO 31000: 2009.

Es una norma internacional que ofrece marcos y procesos, principios y directrices para gestionar el riesgo de las organizaciones y que puede ser implementado en cualquier organización.

La Organización Internacional de Normalización por sus siglas en ingles ISO, en participación con IEC, publicaron en noviembre de 2009 la norma ISO 31000. Esta norma tiene como objetivo

gestionar los riesgos de forma efectiva en organizaciones sin importar el tipo o tamaño de las mismas. (ISOTools, s.f.)

Para una efectiva gestión de riesgos ISOTools indica que la norma ISO 31000:2009 está estructurado en tres elementos claves:

- El proceso de gestión de riesgos que consta de tres etapas: establecer del contexto, valorar los riesgos y el tratamiento de los riesgos.
- La estructura de soporte cuyo objetivo es integrar el proceso de gestión de riesgos con la dirección.
- Los principios para la gestión de riesgos para una mayor eficacia.

Para Crespo (2016), se debe considerar los siguientes principios para una adecuada gestión de riesgos:

a) Crea y proteger el valor.
b) Estar integrada a los procesos de la organización.
c) Formar parte de la toma de decisiones.
d) Tratar explícitamente la incertidumbre.
e) Ser sistemática, estructurada y adecuada.
f) Estar hecha a la medida.
g) Tomar en cuenta los factores humanos y culturales.
h) Basarse en la mejor información disponible.
i) Ser transparente e inclusiva.
j) Ser dinámica, iterativa y sensible al cambio.
k) Facilitar la mejora continua de la organización.

1.6 Marcos de referencia

1.6.1 COBIT 5.

Usado actualmente como la quinta revisión y conocido antiguamente como Objetivos de Control para Tecnologías de Información o Relacionadas (COBIT). Es un marco completo que ha sido aceptado internacionalmente, para el gobierno y la gestión de la información en una organización y la tecnología de la información (TI) que mantiene a los ejecutivos de la organización en la consecución de las metas del negocio y las metas de TI relacionadas.

Crespo (2016) explica los cinco principios de COBIT 5 que son:

- Satisfacer las necesidades de las partes interesadas
- Cubrir la empresa de punta a punta
- Aplicar un único marco de referencia integrado
- Hacer posible un enfoque holístico
- Separar el gobierno de la gestión

COBIT está conformado por 7 habilitadores de gestión o catalizadores corporativos:

- Separar el gobierno de la gestión
- Procesos
- Estructuras organizacionales
- Cultura, ética y comportamiento
- Información
- Servicios, infraestructura y aplicaciones
- Gente, habilidades y competencias. (Crespo P. , 2016)

COBIT es la única metodología que se preocupa en tomar los controles técnicos y acoplarlos a los requerimientos del negocio.

Minchala (2016) explica que existe diferencia entre el gobierno y la gestión. Indica que el gobierno asegura que los objetivos empresariales se cumplen, establece la dirección a través de la toma de decisiones, monitorea el rendimiento, la ejecución y el avance con respecto a la dirección y metas acordadas.

También explica que la gestión se encarga de planificar, construir, ejecutar y controlar (PBRM) por sus siglas en inglés, las actividades que el cuerpo de gobierno ha establecido y ha alineado con la dirección con el fin de alcanzar los objetivos empresariales.

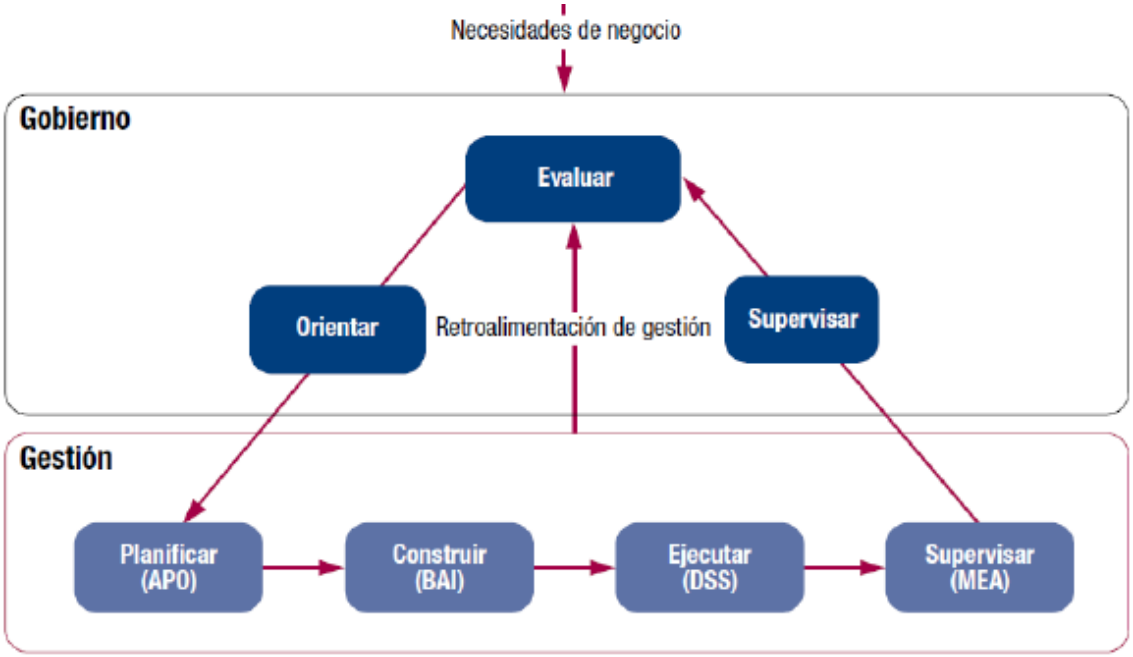

Ilustración 20. Gobierno y Gestión en COBIT 5.
Fuente: Minchala, 2016

1.6.2 COSO III:2013.

El Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) es un modelo de origen estadounidense que mayor difusión ha adquirido, ha sido diseñado con el fin de mejorar el desempeño de las organizaciones y de alguna manera reducir el alcance del fraude en las empresas. (Galaz, 2015)

El modelo incrementa las probabilidades de que una empresa sea gestionada de manera eficiente, suministrando un enfoque integral y herramientas institucionales que sirven de apoyo para encarar medidas de mejora continua. Además, proporciona liderazgo en temas como la gestión del riesgo, disuasión del fraude y control interno. (Galaz, 2015)

La Comisión *Treadway* estaba integrada por cinco organizaciones muy representativas en Estados Unidos en referencia a contabilidad-finanzas-auditoría interna:

- *American Accounting Association* (AAA)
- *American Institute of Certified Public Accountants* (AICPA)
- *Financial Executive Institute* (FEI)
- *Institute of Internal Auditors* (IIA)
- *Institute of Management Accountants* (IMA)

COSO propone un Marco integrado de control interno que provee herramientas y un enfoque integral con el fin de implementar un sistema de control interno efectivo. Un sistema de control interno efectivo hace más eficiente la posibilidad de que un objetivo de la organización se cumpla, es decir; el riesgo se reduce a un nivel aceptable, con la finalidad de que esto no afecte la posibilidad de alcanzar un objetivo en la organización. (AUDITOOL, 2016)

La implementación de un sistema de control interno eficiente les permitirá a las organizaciones combatir los rápidos cambios de la actualidad. La alta gerencia y la administración tienen la responsabilidad de crear un sistema que asegure que los objetivos organizacionales se cumplan y hacer que este sistema se convierta en una pieza primordial en la cultura empresarial. (AUDITOOL, 2016)

El Informe expuesto por COSO divide el control interno en cinco componentes que están relacionados con los objetivos institucionales:

- Entorno de control
- Evaluación de los riesgos
- Actividades de control
- Información y comunicación
- Monitoreo

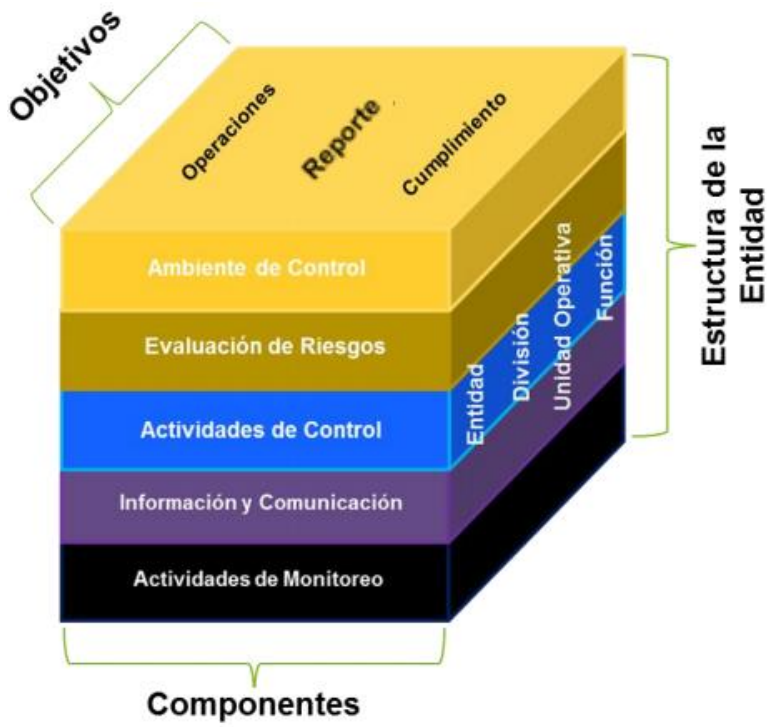

Ilustración 21. Relación entre componentes y objetivos en COSO.
Fuente: Galaz, 2015

Galaz (2015) indica que "De los cinco componentes de Control Interno que establece COSO, se deberán considerar los 17 principios que representan los conceptos fundamentales relacionados con los componentes para el establecimiento de un efectivo Sistema de Control Interno".

Para Crespo P. (2016), los componentes de control interno y los principios están organizados de la siguiente manera:

Ambiente de Control.

Principio 1: La organización demuestra compromiso por la integridad y valores éticos.

Principio 2: El Consejo de Administración demuestra independencia de la administración y ejerce la supervisión del desarrollo y el rendimiento de los controles internos.

Principio 3: La Administración establece, las estructuras, las autoridades y responsabilidades apropiadas en la búsqueda de objetivos.

Principio 4: La organización demuestra un compromiso para la competencia.

Principio 5: La organización retiene individuos comprometidos con sus responsabilidades de control interno. (Crespo P. , 2016)

Evaluación de Riesgos

Principio 6: La organización especifica objetivos con suficiente claridad o relevantes para identificar y valorar los riesgos relacionados a los objetivos.

Principio 7: La organización identifica y analiza los riesgos para determinar cómo esos riesgos deben de administrarse.

Principio 8: La organización considera la posibilidad de fraude en la evaluación de riesgos para el cumplimiento de los objetivos.

Principio 9: La organización identifica y evalúa cambios significantes. (Crespo P. , 2016)

Actividades de Control

Principio 10: La organización selecciona y desarrolla actividades de control que contribuyen a la mitigación de riesgos.

Principio 11: La organización selecciona y desarrolla actividades de control generales sobre la tecnología.

Principio 12: La organización despliega actividades de control a través de políticas y procedimientos que ponen dichas políticas en acción. (Crespo P. , 2016)

Información y Comunicación

Principio 13: La organización obtiene o genera y usa información relevante y de calidad.

Principio 14: La organización comunica información internamente, incluyendo objetivos y responsabilidades sobre el control interno.

Principio 15: La organización se comunica con grupos externos con respecto a situaciones que afectan el funcionamiento del control interno. (Crespo P. , 2016)

Actividades de Monitoreo

Principio 16: La organización selecciona, desarrolla, y realiza evaluaciones continuas y/o independientes.

Principio 17: La organización evalúa y comunica deficiencias de control interno. (Crespo P. , 2016)

CAPÍTULO 2 – El sistema de Gestión Anti Soborno ISO 37001

2.1 Introducción a las organizaciones y sociedades

Las organizaciones públicas y privadas presentan diferencias que tendrán implicaciones sobre sus procesos de dirección estratégicas. Citando a Rainey, Backoff, & Levine (1976) se explica que se han encontrado diferencias significativas en relaciones como medioambiente-organización, estructuras internas y procesos. (Pedraja & Rodríguez, 2008)

Pedraja & Rodríguez (2008) explican también que existe un conjunto de factores que diferencian a las organizaciones públicas sin fines de lucro de las organizaciones privadas con fines de lucro. Estos factores incluyen la complejidad y ambigüedad de objetivos, la estructura organizacional y el grado de formalización. Citando a estudios previos, explican que los directivos de las organizaciones públicas consideran sus objetivos claros y, por lo tanto, no ambiguos. Por esta razón, en las organizaciones públicas no es necesario maximizar el capital.

Las organizaciones públicas no tienen un fin único que sea medible y generalmente aceptado, las influencias externas son varias y difíciles de priorizar, las influencias internas son varias y su impacto es significativo sobre la dirección y la gestión, las limitaciones legales forman parte de la naturaleza de las instituciones públicas. En las empresas privadas estos aspectos son diferentes, donde el objetivo principal es crear valor económico para los accionistas; es decir, maximizar el valor del patrimonio de los accionistas de la institución. Existen las influencias internas y externas, pero la alta dirección elige las mejores respuestas estratégicas.

El éxito de la toma de decisiones en las empresas privadas está asociado al acceso a la información y a los medios necesarios para la implementación de la decisión. En cambio, en las organizaciones sin fines de lucro la participación de los individuos es un aspecto esencial para que un proceso de toma de decisiones sea exitoso.

Se puede afirmar que los procesos estratégicos tienen diferencias entre organizaciones privadas y organizaciones públicas.

Para Salas (2007) estas organizaciones se dividen en tres sectores:

Primer sector: lo estatal. - Lo público al que se puede acceder de forma libre y gratuita. El estado tiene como función la administración de lo público estatal. Los fines más destacados del estado son, incrementar el capital físico, humano y social; así como posibilitar el desarrollo integral de las personas, familias y comunidades. Todo esto lo hará el estado para mejorar la calidad de vida de la ciudadanía.

Segundo sector: lo empresarial. - La empresa es la expresión material y social de la relación entre capital y trabajo asalariado, y la propiedad privada reconocida y garantizada por el Estado, que asegura el acceso y disfrute particular de las ganancias. Para las empresas la responsabilidad social implica generar empleo, acatar la legislación laboral y pagarle impuestos al gobierno.

Tercer sector: lo social. – Conformado por organizaciones civiles sin ánimo de lucro, de iniciativa privada, que prefieren el desarrollo social y humano de grupos, personas, familias y comunidades. Estas organizaciones pueden ser: fundaciones, corporaciones, gremios, asociaciones, partidos políticos, ONG, entidades eclesiásticas, cooperativas, cajas de compensación familiar, sindicatos y juntas de acción comunal. Se diferencia del estado por su origen no oficial y de las organizaciones privadas en la no obtención de lucro. (Salas, 2007)

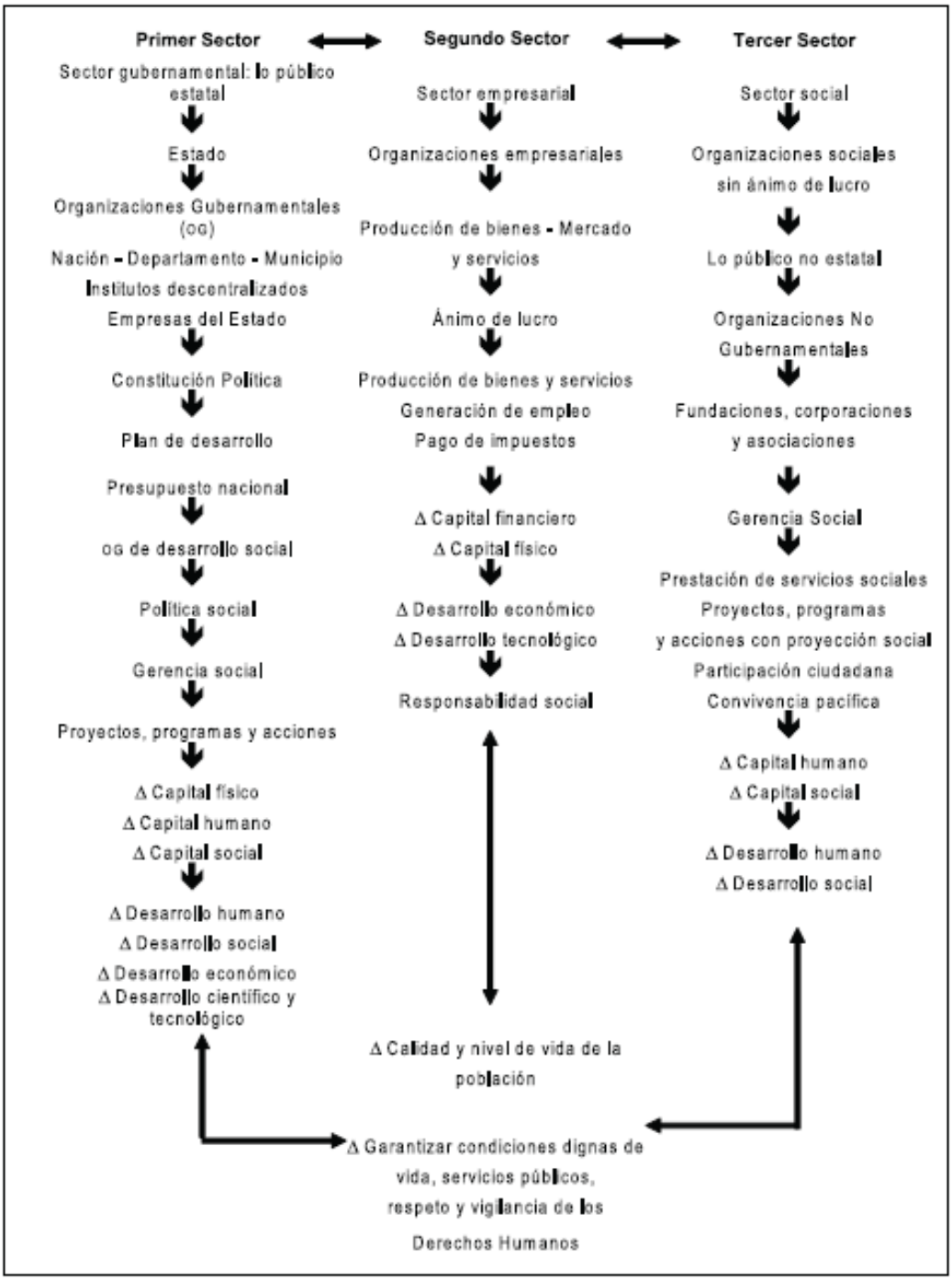

Ilustración 22. Relación entre sectores.
Fuente: Salas, 2007

Sociedad Anónima

Para Buri & Matute (2012), "La compañía anónima es una sociedad cuyo capital, dividido en acciones negociables, está formado por la aportación de los accionistas que responden únicamente

por el monto de sus acciones". Dichas sociedades están sujetas a las reglas de las sociedades anónimas.

Buri y Matute citando a Gorges Ripert expresa también que una sociedad anónima es una sociedad comercial en la que sus accionistas poseen un derecho representado por un título negociable y solo responden con su aporte. Se enfoca en el capital debido a que se caracteriza por ser una sociedad comercial.

Compañía Limitada

Una compañía de responsabilidad limitada se describe como,

> Una sociedad compuesta de socios obligados sólo hasta la concurrencia de sus aportaciones, en la cual las participaciones sociales no pueden estar representadas por títulos negociables y no son cesibles sino en ciertas condiciones, imperativamente determinadas por la Ley y puede existir bajo una razón social. (Buri & Matute, 2012)

También se puede decir que es una sociedad en la cual cada uno de sus socios no está obligado más allá de su aportación. Que se constituye para el desarrollo de actividades económicas y operaciones mercantiles.

Principales características de las compañías de responsabilidad limitada:

- Es de naturaleza mercantil
- Tiene característica de una sociedad de capital
- Es una organización económico jurídica
- Razón Social o denominación objetiva. (Buri & Matute, 2012)

Sociedad de Hecho

Una sociedad de hecho se da cuando dos o más personas llegan a un acuerdo, aportan dinero u otros bienes con el fin de emplear una actividad comercial, y así repartirse entre sí los beneficios.

Tiene capacidad limitada; es decir, no pueden registrar bienes muebles e inmuebles a su nombre y existencia precaria lo que significa que cualquiera de los socios puede pedir la disolución en cualquier momento. (Martinez, 2010)

Características de la formación de una sociedad de hecho:

- No constituye una persona jurídica
- Las obligaciones y derechos que se contraen, se constituyen en cargo y a favor de todos
- No puede tener un nombre comercial
- No se matricula (Martinez, 2010)

Sociedad Civil

Se da por la colaboración de dos o más personas que desean realizar conjuntamente alguna actividad con ánimo de lucro, esto mediante un contrato privado. Se constituye para una actividad mercantil con el fin de obtener beneficios, en la cual cada uno de los socios aporta dinero, trabajo u otros bienes necesarios.

Características de una sociedad civil:

- Existencia de un contrato privado
- Mínimo de 2 socios
- Carece de personalidad jurídica propia
- Se rige por el código del comercio y el código civil
- Cada socio deudor responde por daños o perjuicios que pudieran causar
- Los socios deben darse de alta en autónomos
- La sociedad civil se extingue cuando cumple la duración estipulada en contrato (Infoautónomos, 2017)

2.2 La lucha contra la corrupción y el soborno

Según Transparency International (2009), la corrupción se define como el abuso de poder atribuido para la obtención de un beneficio propio.

Para Frías, Rodríguez, & Isabel (2014) la corrupcion puede definirse como "el abuso de una posición de confianza para la obtención de un beneficio deshonesto".

En la actualidad la corrupción no conoce fronteras, afecta a todos, desde los negocios en países poco desarrollados hasta las compañías multinacionales de países industrializados, así como a ciudadanos comunidades y naciones, afecta a todas la sociedades y economías.

La corrupción en transacciones internacionales se ve favorecida por el desarrollo que han tenido las organizaciones en los últimos tiempos, que disponen de importantes recursos económicos para generar la tentación por parte de personas involucradas con el fin de obtener beneficios propios. (Bedoya, 2016)

El rápido desarrollo del comercio internacional, debido a la globalización económica y a los avances tecnológicos ha favorecido nuevos eventos delictivos, uno de los cuales es conocido como el soborno. El pago de sobornos fomenta una cultura de impunidad y corrupción persistente, y alimenta la percepción pública de que los gobiernos se venden al mejor postor.

El alcance y la magnitud del soborno en las empresas es alarmante. Casi dos de cada cinco ejecutivos de organizaciones encuestados afirmaron que se les había solicitado pagar sobornos al realizar gestiones con instituciones públicas y uno de cada cinco señaló haber perdido oportunidades debido a que un competidor realizo pagos de soborno.

Se estima que tan sólo en los países en desarrollo, los políticos y funcionarios gubernamentales corruptos reciben sobornos por un total de entre 20.000 y 40.000 millones de dólares anuales, esto

significa que equivalen aproximadamente entre el 20% y el 40% de la ayuda oficial para el desarrollo. (Transparency International, 2009)

Bedoya (2016) citando a Fabián Caparrós explica que la corrupción internacional perjudica el desarrollo del comercio e incrementa los costes de las transacciones entre países, restringe la transparencia de los mercados, quebranta la confianza entre naciones y dificulta la correcta asignación de recursos, todo esto, especialmente en los países en vías de desarrollo.

2.2.1 Los beneficios de la lucha contra la corrupción.

Las razones para combatir la corrupción son claras. El 50% de los gerentes en empresas internacionales están de acuerdo en que la corrupción incrementa al menos en un 10% el costo de los proyectos y en determinados casos incrementa hasta el 25%. Además de la pérdida de oportunidades comerciales, perjudicar a la marca, la moral de los empleados y las relaciones externas de las empresas. (Transparency International, 2009)

La aplicación, el cumplimiento más riguroso de las normas anticorrupción y el civismo responsable reporta beneficios directos. Está comprobado que las organizaciones con programas anticorrupción y normas éticas están propensas hasta un 50% menos de sufrir incidentes de corrupción y tienen menor probabilidad de perder negocios en comparación con aquellas empresas que no han desarrollado algún tipo de programa anticorrupción.

Sin embargo, el desafío no se limita a contrarrestar el soborno. Abarca retos más amplios en un entorno global donde existen continuamente nuevas formas de corrupción y surgen nuevas amenazas en la sostenibilidad y competitividad del mercado.

Otras razones que tienen las empresas para rechazar la corrupción suponen asumir altos costes directos, tales como multas y penas de prisión. Asimismo, puede suponer un daño en la reputación de la empresa, en la capacidad de supervivencia y en su rentabilidad.

Muchas empresas utilizan diversos mecanismos de control en su lucha contra el soborno, cuyos resultados pueden ser tan positivos como los procesos normativos. A través de estos mecanismos se pretende concientizar a los empleados y captar su apoyo en la lucha contra el soborno. Por lo tanto, la existencia de políticas puede suponer un impacto positivo en la reputación de las empresas y sobre la confianza de inversionistas. (Frías, Rodríguez, & Isabel, 2014)

Cabe recalcar que el fracaso no solo se da por los altos ejecutivos que han cometido actos de corrupción, sino también por parte de los consejos responsables de su supervisión por haber fallado en sus responsabilidades.

2.2.2 Riesgos de Corrupción.

Los riesgos de corrupción dentro de la empresa incluyen, al fraude corporativo, el soborno, la manipulación de las cuentas, el abuso de información privilegiada, el uso indebido de influencias, la extorsión, algunas formas de comisiones, regalos y favores, el abuso de poder, la financiación ilegal de partidos políticos. Se aplica también a conductas delictivas que pueden ser consecuencia de la corrupción, como el blanqueo de dinero, el chantaje y algunas formas de crimen organizado y mafias.

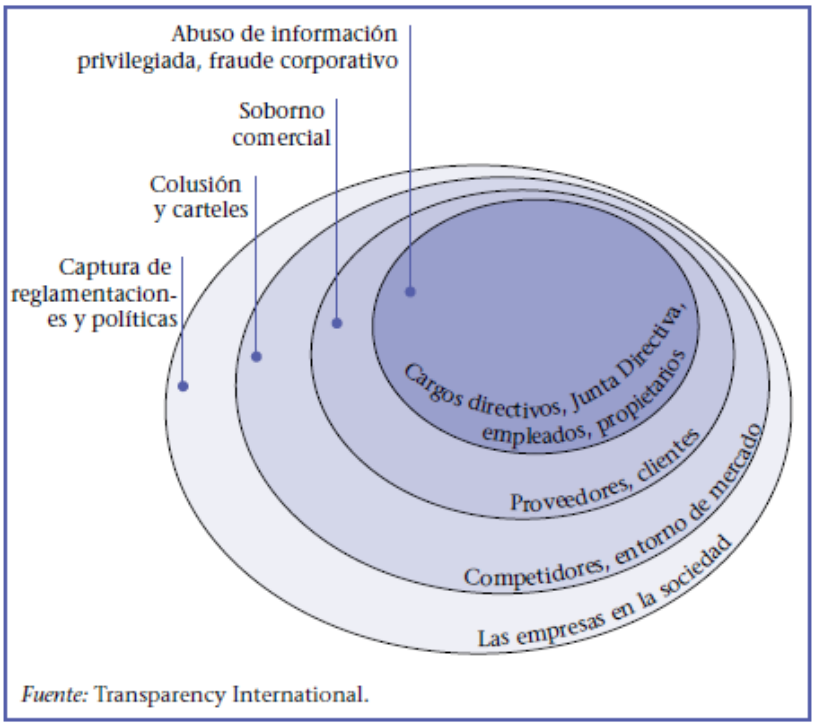

Ilustración 23. Riesgos de corrupción en las distintas esferas de la actividad corporativa.
Fuente: Transparency International, 2009

2.2.3 Lucha contra la corrupción de las PYMES.

Según el informe global de la corrupción 2009, las pequeñas y medianas empresas (PYMES) tienen una gran importancia para la economía global, debido a que representan más del 95% de las empresas del mundo. Debido a que muchas operan en mercados de desarrollo difícil son muy vulnerables a la corrupción. Citando al Banco Europeo de Reconstrucción y Desarrollo (BERD), explica que más del 70% de las PYMES indican que la corrupción es un obstáculo para su empresa, mientras que el 60% lo indican las grandes empresas.

Las PYMES pueden estar constituidas en empresas unipersonales, empresas familiares de 20 integrantes o incluso llegar a alcanzar el tamaño de compañías con cientos de empleados. Independientemente de su tamaño o estructura, las PYMES se enfrentan a cuatro desafíos principales.

- Existe la posibilidad que la cultura del soborno este tan establecido en el entorno empresarial que las PYMES no tengan otra opción más que ceder antes de fracasar.
- A menudo, las PYMES no comprenden ni reconocen las complejidades de la corrupción; es decir, pueden no estar seguras de cuando un obsequio se ofrece como un incentivo, en qué casos una donación a un partido político puede ser utilizada como soborno.
- Los recursos limitados, debido a que muchas de las PYMES se encuentran en la situación de luchar para generar ganancias y así subsistir.
- Las PYMES no reciben gran ayuda para resistir a la extorsión y, por consiguiente, no siempre pueden enfrentarse a ella. (Transparency International, 2009)

Para enfrentar los desafíos mencionados, las pequeñas y medianas empresas deben conocer más a fondo los límites de la corrupción y contar con la información y ayuda adecuada sobre como resistir a propuestas corruptas. Por esto, las empresas deben conocer que el soborno implica la pérdida de control y prestigio, así como posibles sanciones o condenas. También reconocer que los fondos utilizados para pagar sobornos tienen un impacto directo en la viabilidad económica de la organización.

Es fundamental que las PYMES aborden el tema de la corrupción de manera conjunta y coordinada, contar con el apoyo de los gobiernos, principalmente aplicando leyes contra el soborno.

2.2.4 Denunciar la corrupción.

El informe global de la corrupción 2009, indica que los empleados son los actores más importantes capaces de detectar el fraude corporativo.

El informe explica que mediante una encuesta sobre empresas y la forma en que se detectan los fraudes corporativos internos confirma la importancia que tienen los empleados.

Debido a que las empresas reconocen la importancia del rol de los empleados, las compañías integran cada vez más servicios de atención telefónica y sistemas de protección de denunciantes, por lo que consideran que tales medidas son efectivas como se muestra en el siguiente gráfico.

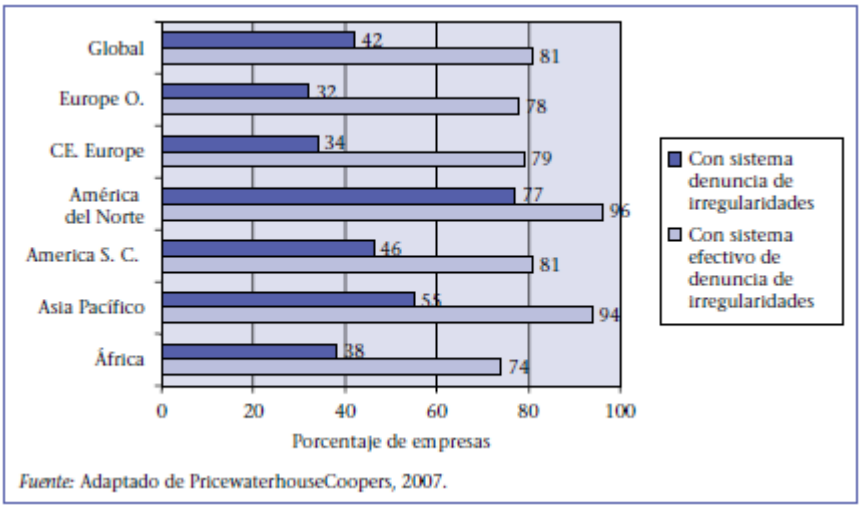

Ilustración 24. Efectividad y porcentaje de compañías con sistemas de denuncia de irregularidades.
Fuente: Transparency International, 2009

En cuanto a la protección legal de los denunciantes en los sectores público y privado, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) explica que es esencial para fomentar la transparencia, promover la integridad y detectar la mala conducta.

La OCDE cuenta con alrededor de dos décadas de experiencia para revisar las medidas de protección de denunciantes, sensibilizar y desarrollar políticas basadas en buenas prácticas nacionales. Fue pionera en la protección del denunciante en el sector público, con la Recomendación de 1998 sobre la mejora de la conducta ética en el Servicio Público.

La OCDE explica que la protección contra el denunciante se refiere a la protección jurídica contra la discriminación para los empleados que divulguen a las autoridades, de buena fe y por motivos razonables de cualquier tipo en el contexto de su lugar de trabajo. Además, promueve una cultura de rendición de cuentas e integridad tanto en el ámbito de instituciones públicas como privadas, y alienta la denuncia de mala conducta, fraude y corrupción. (OECD, 2016)

Más países de la OCDE han establecido leyes de protección de denunciantes en los últimos cinco años. Entre los encuestados de la encuesta de la OCDE, el 84% ha promulgado una ley de protección a los denunciantes en el sector público específicamente para la prevención de represalias.

De los 32 países de la OCDE que respondieron a la encuesta de 2014 sobre la protección de denunciantes del sector público, 27 indicaron una ley específica de protección de denunciantes o disposiciones legales y 13 han aprobado una ley específica que protege a los denunciantes del sector público.

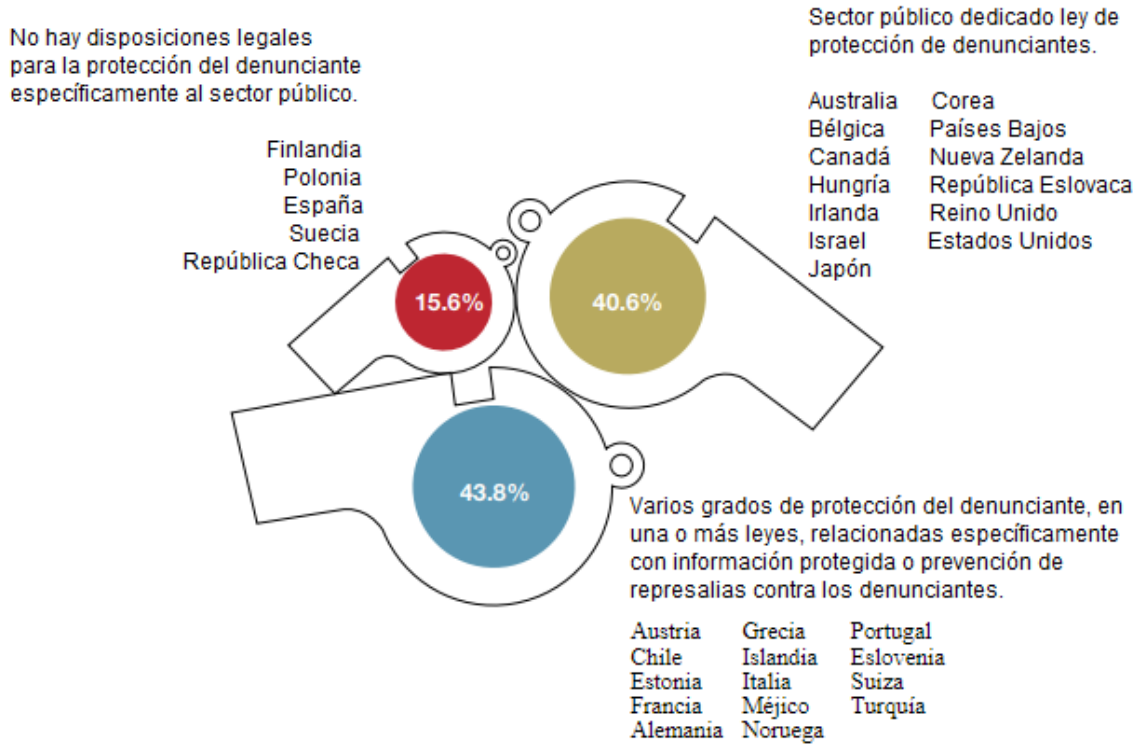

Ilustración 25. Provisión de protección jurídica a los denunciantes en el sector público.
Fuente: OECD, 2016

En los 13 Países de la OCDE que hasta la fecha han promulgado dichas leyes. Más de la mitad de estos países: Hungría, Irlanda, Israel, Japón, Corea, Nueva Zelanda, República Eslovaca y el Reino Unido, optaron por una ley dedicada a la protección de denunciantes que se aplica tanto a los empleados del sector público como privado.

Desde los años 80 hasta principios de los años 2000, sólo cuatro países de la OCDE tuvieron leyes de protección de denunciantes. Desde 2006, se han aprobado leyes de protección de denunciantes en otros nueve países. Con una serie de escándalos evitables que se extendieron por muchos países de la OCDE desde 2000.

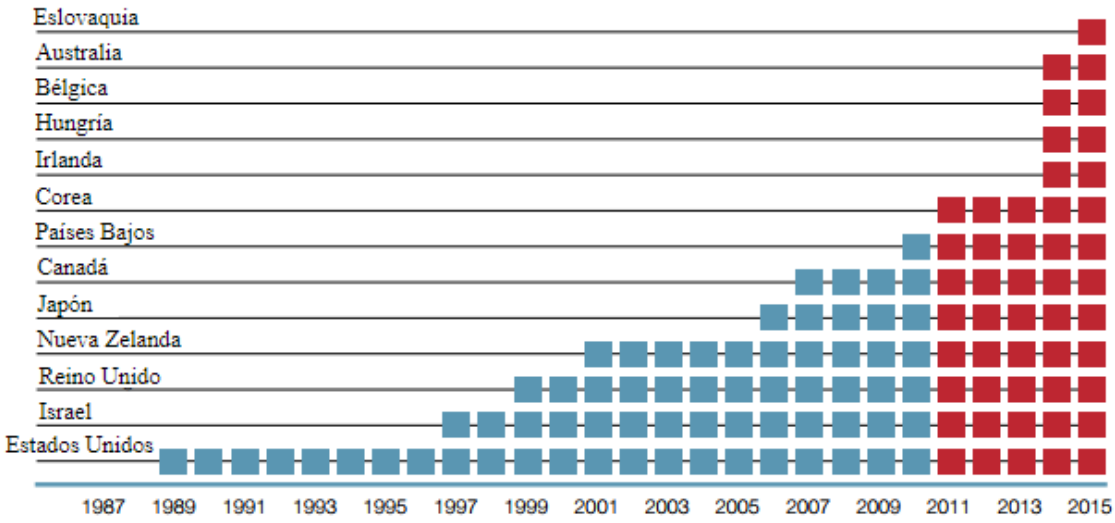

Ilustración 26. Cronograma de entrada en vigor de las leyes de protección de denunciantes.
Fuente: OECD, 2016

Las revelaciones anónimas muestran una falta de confianza en el sistema de protección del denunciante y la integridad de una organización.

En ciertos países, el término denunciante es a menudo asociado a ser un informante, un traidor, un espía o incluso un soplón (Transparency International, 2009)

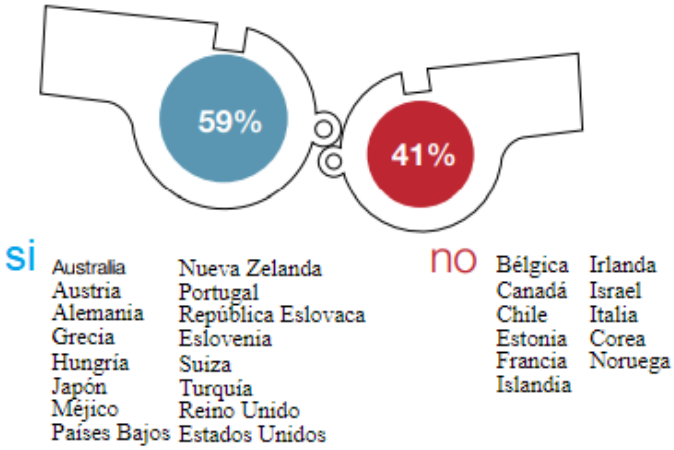

Ilustración 27. Países de la OCDE que garantizan el anonimato del sector público.
Fuente: OECD, 2016

Con el fin de animar a los individuos a reportar la detección de actos ilícitos, los países proporcionan diversos incentivos, tales como fichas de reconocimiento o recompensas financieras. Aunque a menudo se consideran incentivos, los pagos financieros también pueden proporcionar apoyo como consecuencia de represalias.

Las medidas de incentivo existen en ocho países de la OCDE.

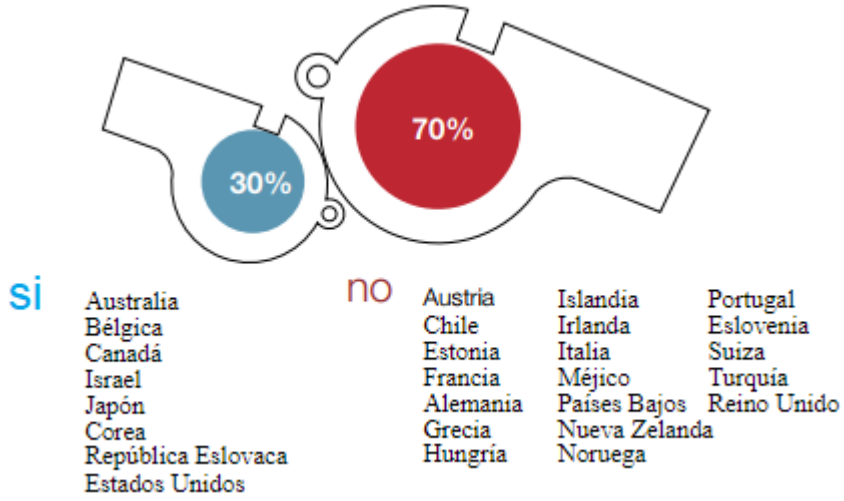

Ilustración 28. Incentivos para que los denunciantes denuncien hechos ilícitos.
Fuente: OECD, 2016

Uno de los primeros pasos que las empresas deben tomar para poner en marcha la protección de denunciantes es establecer un mecanismo de presentación de informes, aunque esto por sí solo no equivale a la protección del denunciante.

De 69 encuestados a la Encuesta de la OCDE sobre Integridad Empresarial y Gobierno Corporativo 59, indicó que sus empresas habían establecido un mecanismo para que los empleados puedan denunciar casos sospechosos de mala conducta corporativa grave.

De los encuestados el 61% de las Empresas cuentan con una política escrita de protección de denunciantes de represalias el 18 % no conoce si tal política existe y el 21 % no dispone de dicha política.

2.2.5 Normas contra la corrupción.

Convención interamericana contra la corrupción (CICC) – suscrita el 29 de marzo de 1996 en el marco de la Organización de Estados Americanos en la ciudad de Caracas. Fue el instrumento fuente que a nivel regional y que significó un verdadero modelo en la lucha contra la corrupción a nivel mundial. (Bedoya, 2016)

Convención de la Organización para la Cooperación y el Desarrollo Económico (OCDE) - La Conferencia Negociadora de la OCDE, adoptó en noviembre de 1997 la convención para combatir el cohecho de servidores públicos extranjeros en transacciones comerciales internacionales. Entró en vigor el 15 de febrero de 1999. (Bedoya, 2016)

Convención Naciones Unidas contra delincuencia organizada transnacional 2003 - suscrita en la ciudad de Palermo (Italia) en diciembre de 2000, en aquel entonces el Secretario General de la ONU se proponía: Si la delincuencia atraviesa las fronteras, lo mismo ha de hacer la acción de la ley. (Bedoya, 2016)

Convención de Naciones Unidas contra la Corrupción (CNUCC) – suscrita en el año 2003, se establecieron una serie de conductas punibles constitutivas de corrupción, entre otras, el soborno de funcionarios públicos extranjeros y de funcionarios de organizaciones internacionales públicas. (Bedoya, 2016)

Otros dos instrumentos jurídicos, relacionados con el soborno transnacional son: la Convención de la Unión Africana para prevenir y combatir la corrupción (2003), la Ley Anti-Corrupción del Reino Unido (2010) y el Plan Andino de Lucha contra la Corrupción (Decisión 668 del Consejo Andino de ministros de relaciones exteriores de la Comunidad Andina 2007).

Organizaciones como ONU, la OEA y la OCDE dejan traslucir la preocupación por la prevención y represión de la corrupción. Se han ocupado del problema y han expedido ciertas convenciones orientadas al control de diversas prácticas consideradas corruptas.

Una ley bastante citada es la ley usada por el Departamento de Justicia de los Estados Unidos (DOJ) y la Comisión de Mercado de Valores de los Estados Unidos (SEC) para sancionar a las personas y entidades (tanto civilmente como criminalmente) por sobornos a funcionarios extranjeros.

La ley FCPA - *Foreign Corrupt Practices Act* - (Ley de prácticas corruptas en el extranjero), promulgada en el año 1977 en los Estados Unidos es la ley de prácticas corruptas en el extranjero que sanciona la entrega de dádivas o el ejercicio de influencias de particulares sobre funcionarios públicos, partidos políticos o entidades públicas extranjeras. (Bedoya, 2016)

La ley FCPA se puede dividir en dos partes:

1) las disposiciones anti-soborno, que generalmente prohíben el pago de "cualquier cosa de valor" a funcionarios extranjeros para obtener o retener negocios.
2) las disposiciones contables, que requieren que los emisores preparen y mantengan libros, registros y cuentas y desarrollen y mantengan sistemas de controles de contabilidad interna suficientes para prevenir o detectar pagos indebidos. (Epstein, 2016)

La ley FCPA es aplicable a la siguiente categoría de personas y entidades:

1) individuos que sean ciudadanos norteamericanos o residentes, y entidades de los Estados Unidos.
2) todos los emisores de valores en los Estados Unidos y los funcionarios, directores, empleados, agentes y accionistas que actúen a nombre del emisor.

3) cualquier extranjero cuyas conductas en el territorio de los Estados Unidos encaucen un pago indebido. (Epstein, 2016)

Según el Informe de cumplimiento de la FCPA para el tercer trimestre de 2017 publicado el 2 de octubre de 2017 por Cassin (2017). Telia Company AB acordó con el DOJ y la SEC pagar $ 965 millones para resolver violaciones de la FCPA en Uzbekistán aterrizando en la cima de la lista del top ten:

1. Telia Company AB (Suecia): 965 millones de dólares en 2017.
2. Siemens (Alemania): 800 millones de dólares en 2008.
3. VimpelCom (Holanda): $ 795 millones en 2016.
4. Alstom (Francia): 772 millones de dólares en 2014.
5. KBR / Halliburton (Estados Unidos): $ 579 millones en 2009.
6. Teva Pharmaceutical (Israel): 519 millones de dólares en 2016.
7. Och-Ziff (Estados Unidos): 412 millones de dólares en 2016.
8. BAE (Reino Unido): $ 400 millones en 2010.
9. Total SA (Francia): $ 398 millones en 2013.
10. Alcoa (Estados Unidos): $ 384 millones en 2014. (Cassin, El Blog de la FCPA, 2017)

Epstein (2016), presenta una lista de las diez Multas Más Altas a Empresas por FCPA (Global):

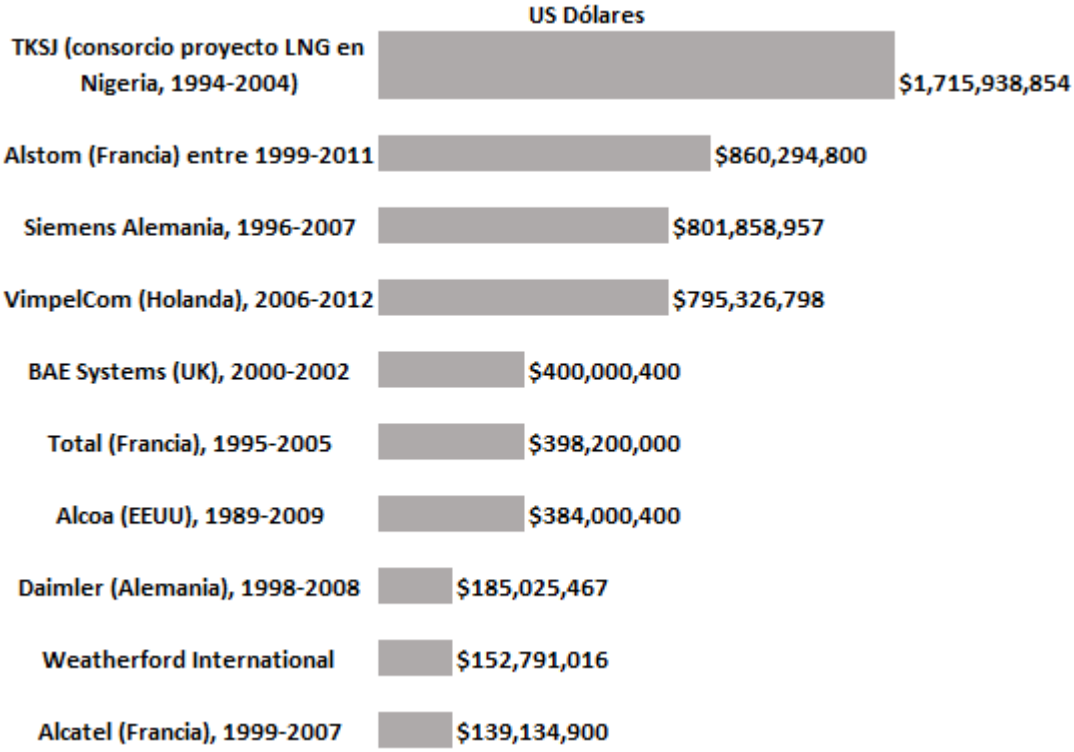

Ilustración 29. Las Diez Multas Más Altas a Empresas por FCPA (Global).
Fuente: Epstein, 2016

El índice de cumplimiento de la FCPA para el año 2016 queda de la siguiente manera:

- En 2015, 11 compañías pagaron $ 133 millones para resolver casos de FCPA.
- En 2014, 10 compañías pagaron 1.560 millones de dólares.
- En 2013, 12 compañías pagaron $ 731.1 millones.
- En 2012, 12 compañías pagaron $ 259.4 millones.
- En 2011, 15 compañías pagaron $ 508.6 millones.
- En 2010, 23 compañías pagaron $ 1.8 mil millones.
- En 2009, 11 compañías pagaron $ 644 millones, y
- En 2008, 11 compañías pagaron $ 890 millones. (Cassin, El Blog de la FCPA, 2017)

La Universidad de Stanford, a través de su *Rock Center for Corporate Governance*, con el apoyo de la firma Sullivan & Cromwell, han inaugurado una base de datos llamada *Foreign*

Corrupt Practices Act Clearinghouse (FCPAC). Esta base de datos contiene los casos de FCPA que el DOJ y la SEC han perseguido en contra de empresas e individuos desde 1977.

La FCPAC presenta un gráfico que indica los países donde se ofrecieron o pagaron sobornos entre el 2008 y 2017, para todos los grupos de la FCPA. ubicación de presuntos pagos indebidos.

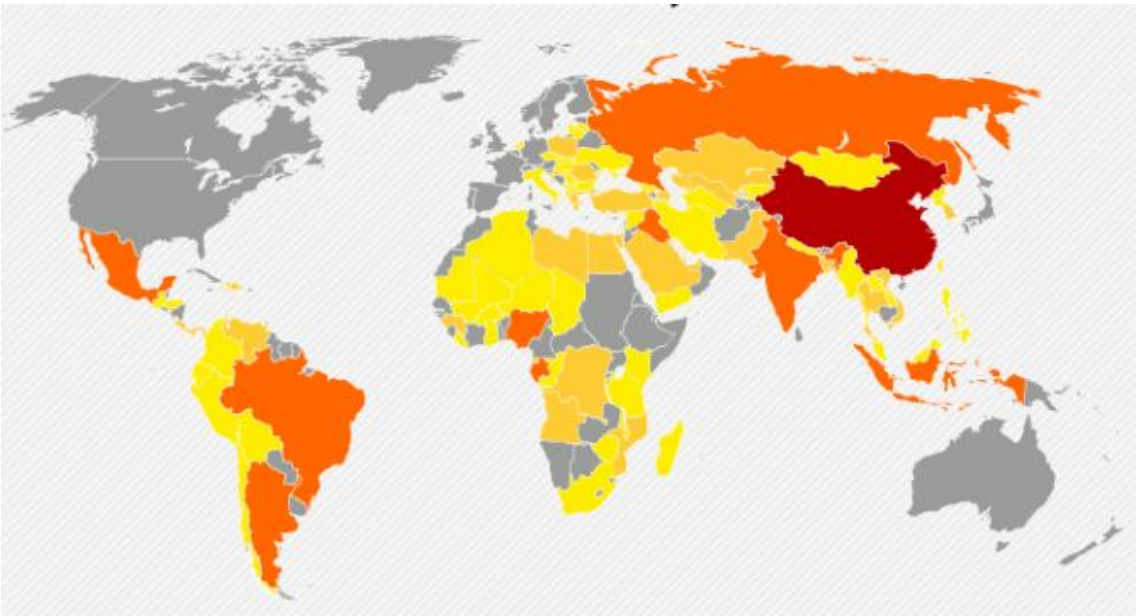

Ilustración 30. Ubicación de pagos indebidos 2008 - 2017.
Fuente: Stanford University, 2017

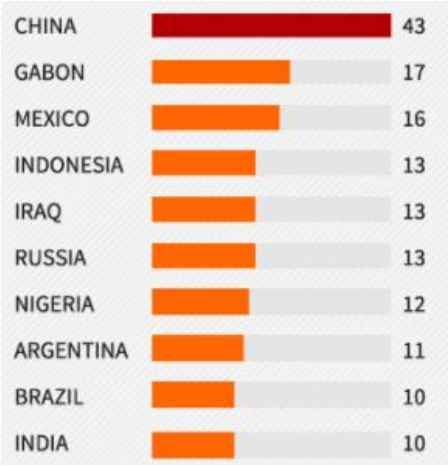

Ilustración 31. Top ten de pagos indebidos 2008 - 2017.
Fuente: Stanford University, 2017

Sanciones por año: Este gráfico identifica el total, el promedio y la mediana de sanciones impuestas en acciones relacionadas con FCPA presentadas entre el 2008 Y 2017.

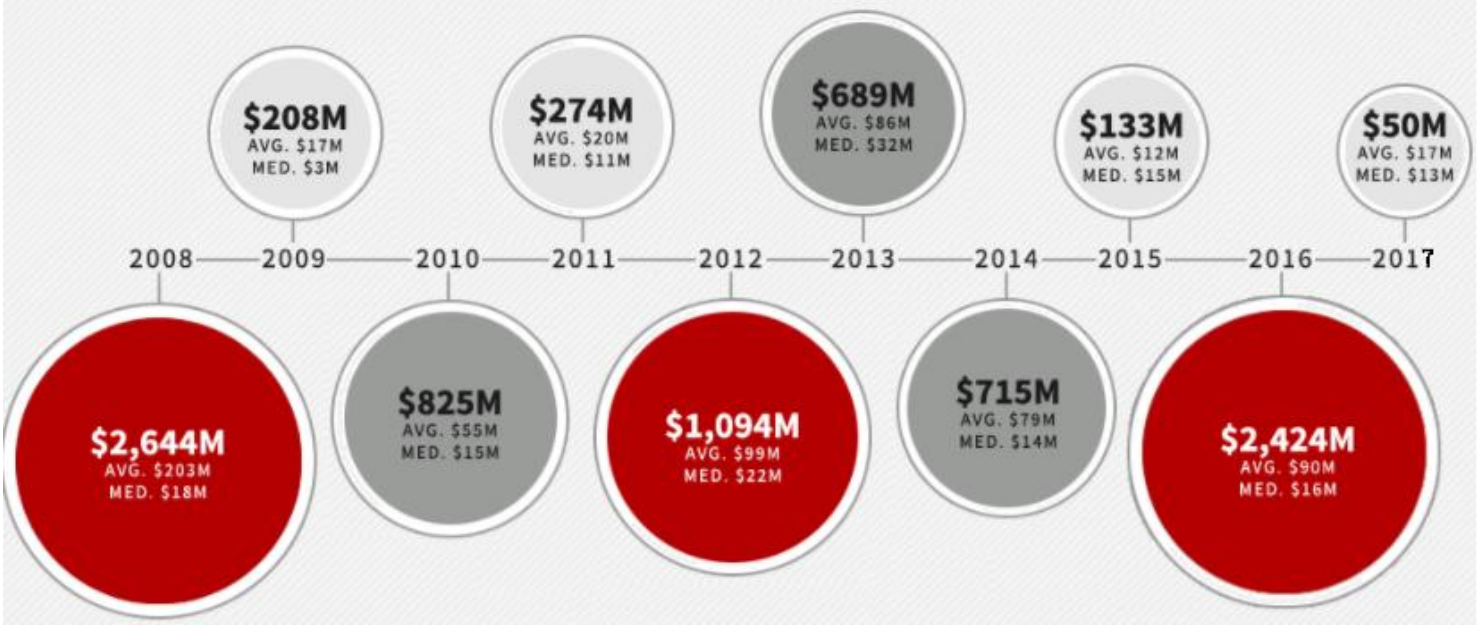

Ilustración 32. Sanciones por año entre 2008 - 2017.
Fuente: Stanford University, 2017

Casos procesados por año donde la SEC y el DOJ han interpuesto acciones legales en contra de empresas o individuos por infracciones de FCPA en la región:

Ilustración 33. Casos procesados por año 2008-2017.
Fuente: Stanford University, 2017

Si bien la ley de FCPA está vigente desde 1977, las demandas por infracciones a esta norma aumentaron de manera considerable sólo a partir de la década pasada, como indica el siguiente gráfico:

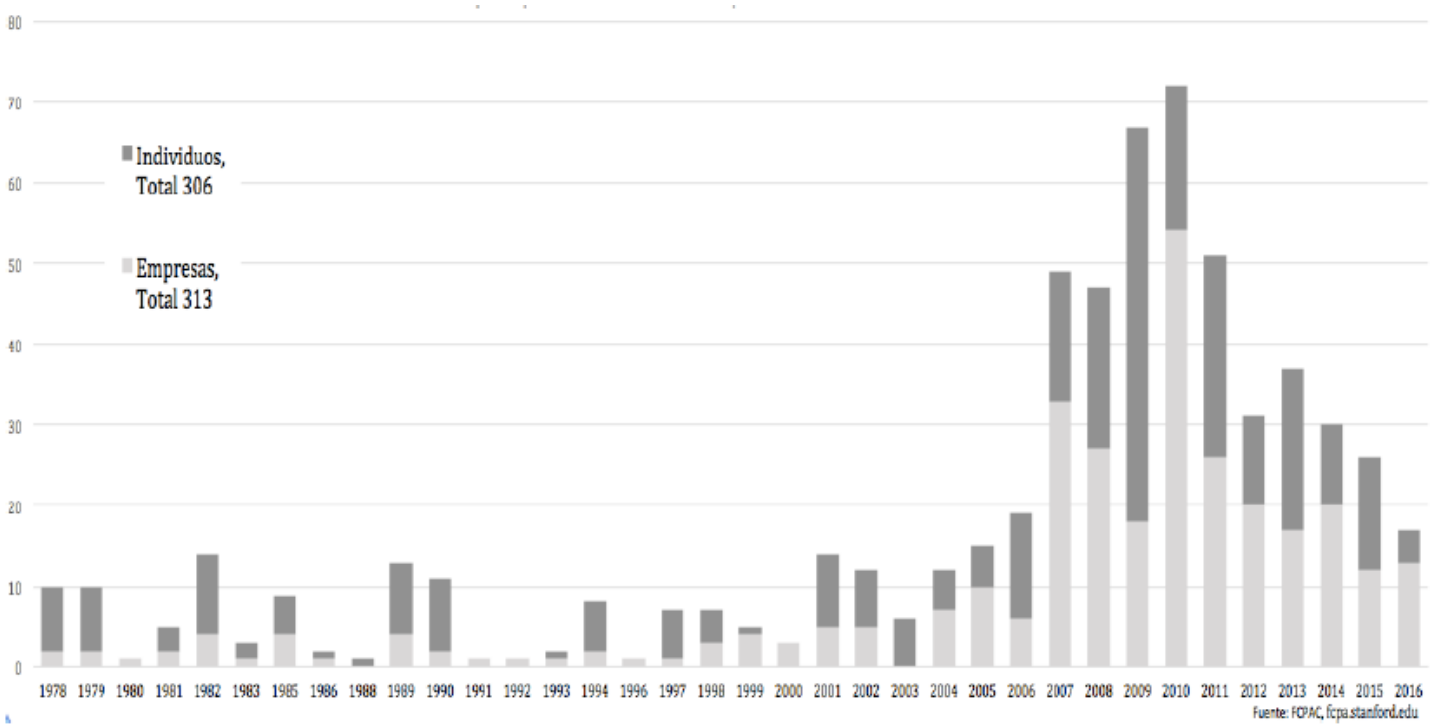

Ilustración 34. Individuos y Empresas Demandadas, 1977-2016.
Fuente: Epstein, 2016

Para información más detallada sobre el reporte 2008 – 2017 de *Foreign corrupt practices Act Clearinghouse,* visitar http://fcpa.stanford.edu/.

2.2.6 Ley FCPA en América Latina.

Muchas empresas de América Latina transan en EEUU, por lo que están sujetas a la normativa FCPA. Por ejemplo, Brasil (81), México (36), Argentina (17), Chile (12), Venezuela (8), Perú (5), Colombia (4), Panamá (3), y Ecuador (1).

Entre 2006 y 2016, se cuentan 54 casos donde la SEC y el DOJ han interpuesto acciones legales en contra de empresas o individuos en América Latina por infracciones de FCPA. Las infracciones han tomado lugar en México (12), Argentina (10), Brasil (8) y Venezuela (8). En total, los casos se reparten en 12 países. (Epstein, 2016)

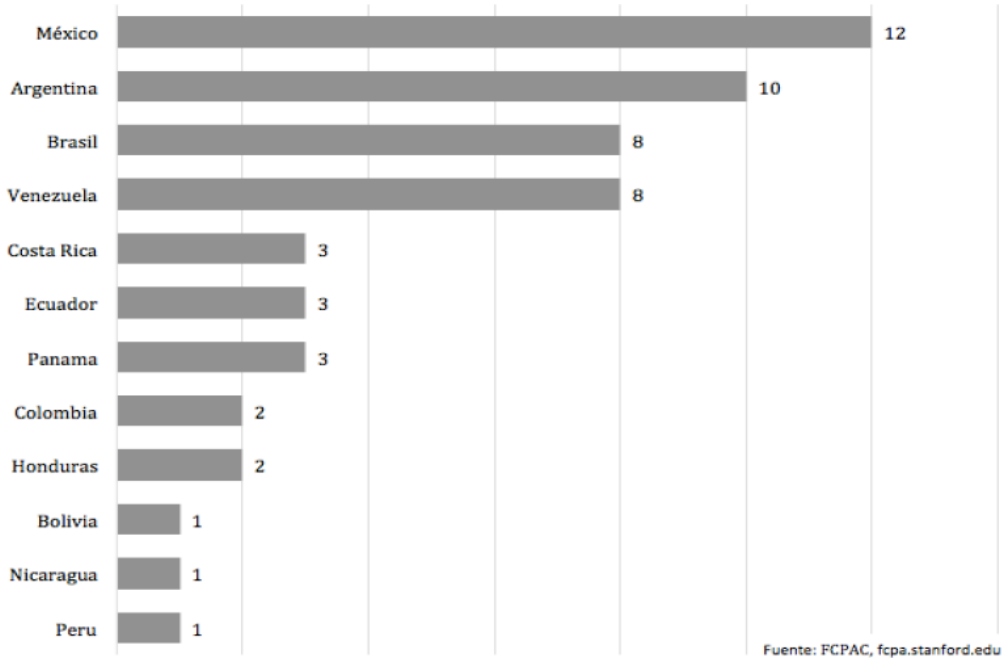

Ilustración 35. Casos de FCPA en América Latina, 2006-2016.
Fuente: Epstein, 2016

Las condenas por infringir las normas FCPA son muy severas. En el siguiente grafico se encuentran las 10 condenas privativas de libertad más largas a individuos en América Latina.

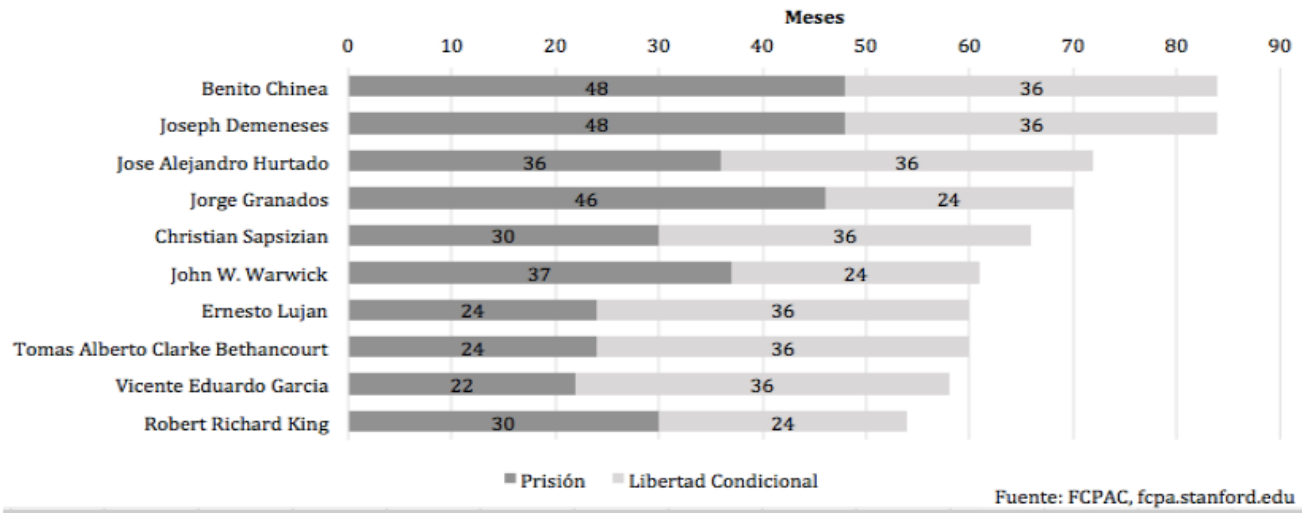

Ilustración 36. 10 condenas Privativas de Libertad Más Altas por FCPA (América Latina).
Fuente: Epstein, 2016

Además, las diez multas más altas a empresas e individuos, por infracciones de FCPA.

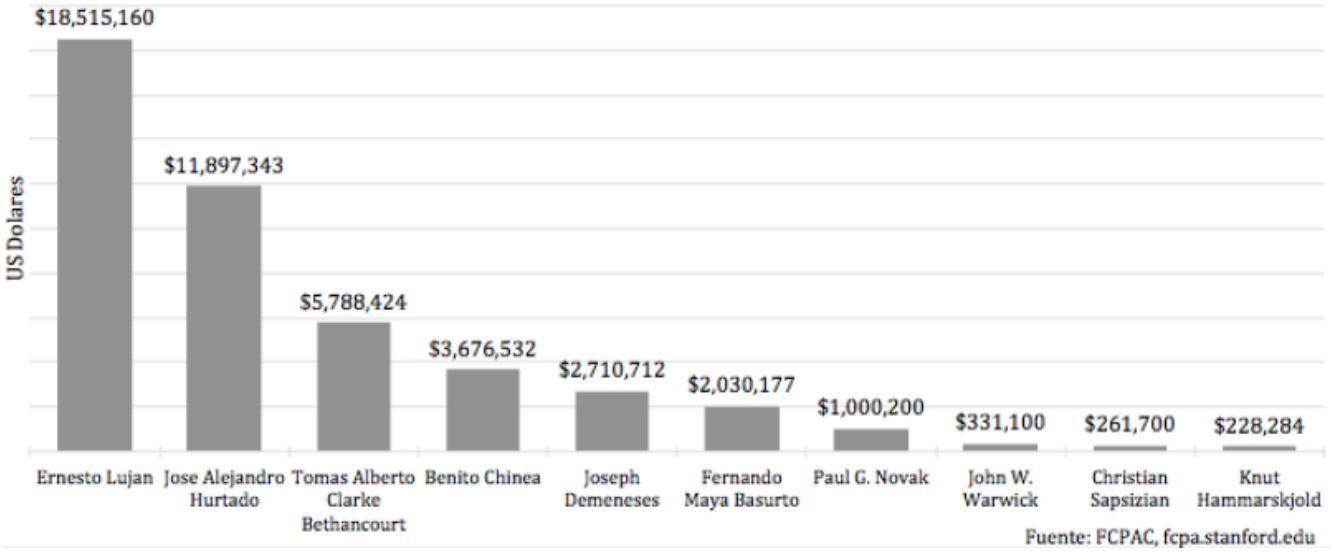

Ilustración 37. Las 10 Multas Más Altas a Individuos por FCPA (América Latina).
Fuente: Epstein, 2016

Y como a nivel global, existen las multas a empresas por FCPA en América Latina son:

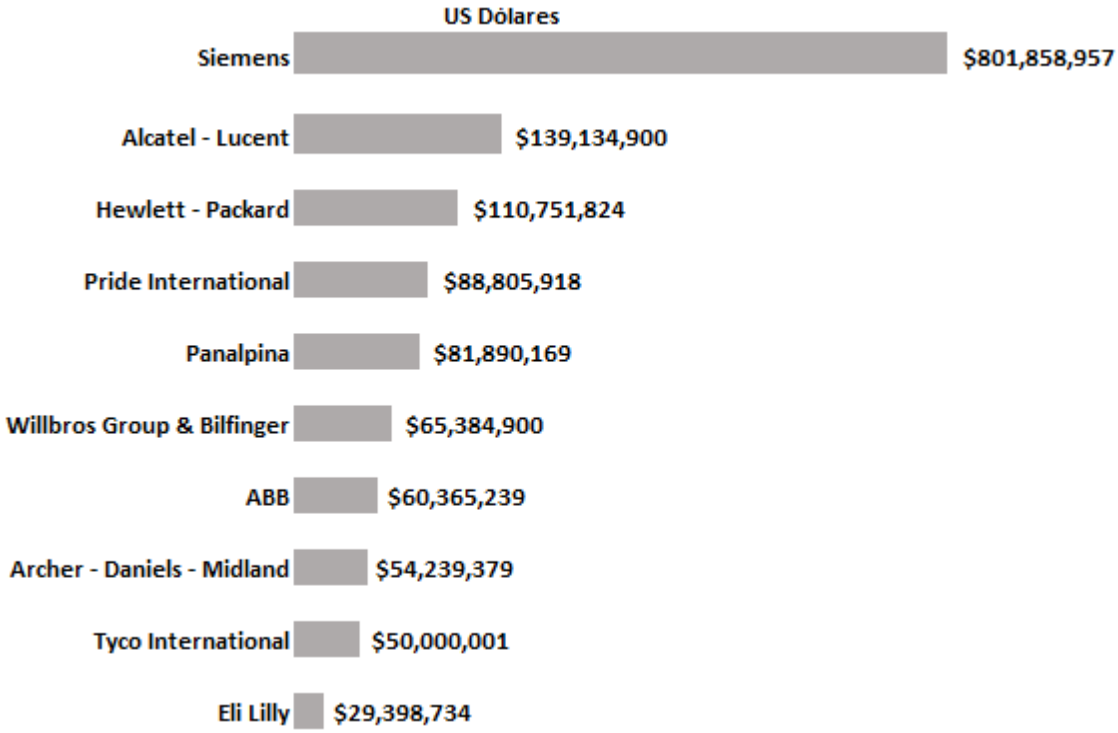

Ilustración 38. Las 10 Multas Más Altas a Empresas por FCPA (América Latina).
Fuente: Epstein, 2016

La ley FCPA establece multas tanto penales como civiles a individuos y empresas. Las autoridades ya han recaudado más de $8.000 millones de dólares en multas por infracciones FCPA En América Latina. En los casos se involucran en gran parte empresas multinacionales que han cometido infracciones de FCPA en la región.

2.2.7 Índice de Percepción de la Corrupción.

El Índice de Percepción de la Corrupción (IPC), o en inglés *Corruption Perceptions Index*, se publica desde 1995. Clasifica a 176 países, en función de cómo empresarios y analistas de país perciben la corrupción de los funcionarios públicos y políticos.

Las fuentes de las que provienen los datos son:

- Banco Asiático de Desarrollo
- Banco Africano de Desarrollo
- Índice de Transformación Bertelsmann
- Evaluaciones de las Políticas e Instituciones Nacionales del Banco Mundial
- Economist Intelligence Unit, Nations in
- Transit de Freedom House
- Global Insight
- IMD International World Competitiveness Center
- Merchant International Group
- Political and Economic Risk Consultancy
- Foro Económico Mundial. (Transparency International, 2009)

Más de dos tercios de los 176 países y territorios en el 2016 caen por debajo del punto medio de la escala de 0 (muy corrupto) a 100 (muy limpio). Los países que obtuvieron mayor puntuación,

es decir, más limpios (amarillo) están superados en número por países naranjos y rojos donde los ciudadanos se enfrentan diariamente a los efectos tangibles de la corrupción. (Transparencia Internacional, 2017)

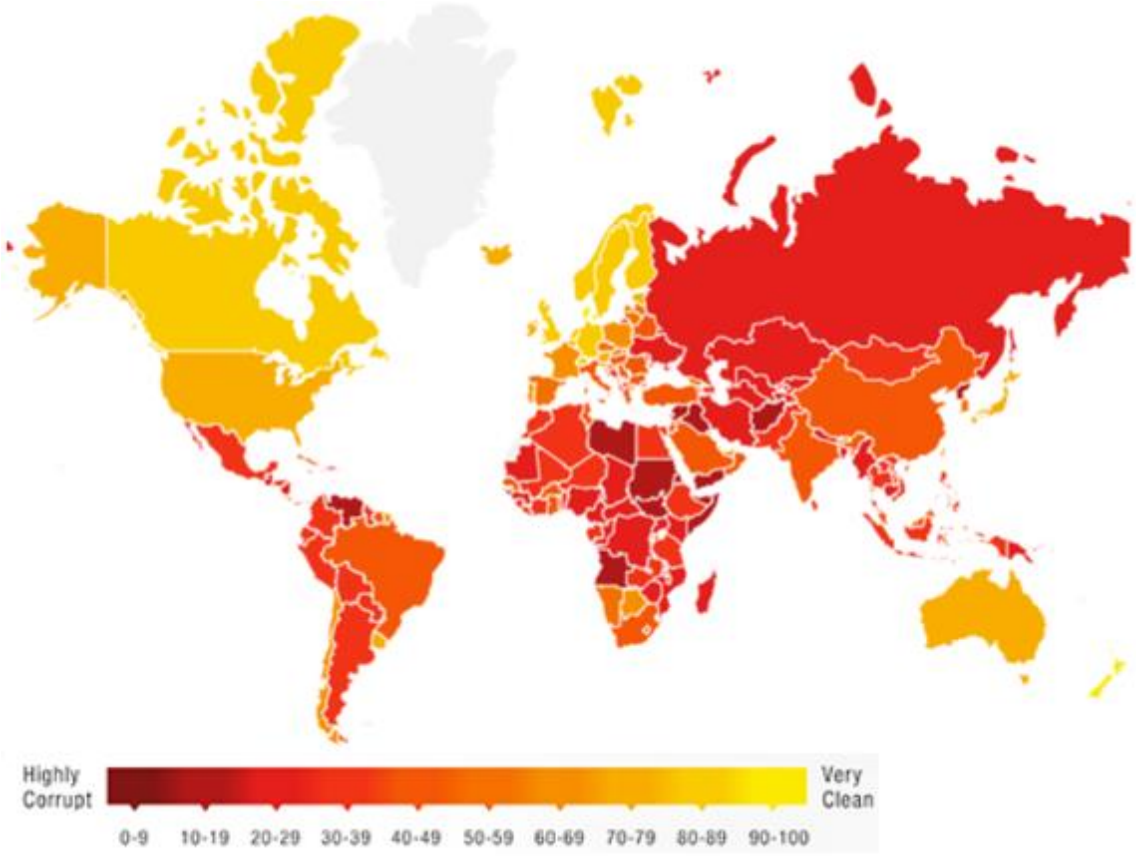

Ilustración 39. Índice de percepción de la corrupción 2016.
Fuente: Transparencia Internacional, 2017

Transparencia Internacional o *Transparency International* (TI) presentó la última versión de su Índice de Percepción de la Corrupción (IPC) 2016. En el que indica que Nueva Zelanda y Dinamarca son los países menos corruptos del mundo. Obtuvieron 90/100 puntos que, según los índices, es el nivel mínimo de corrupción que un país ha alcanzado. Otras naciones que conforman las primeras posiciones del ranking son: Finlandia (89), Suecia (88), Suiza (86), Noruega (85), Singapur (84), Holanda (83), Canadá (82), y Alemania, Luxemburgo y el Reino Unido (81). (Mizrahi, 2017)

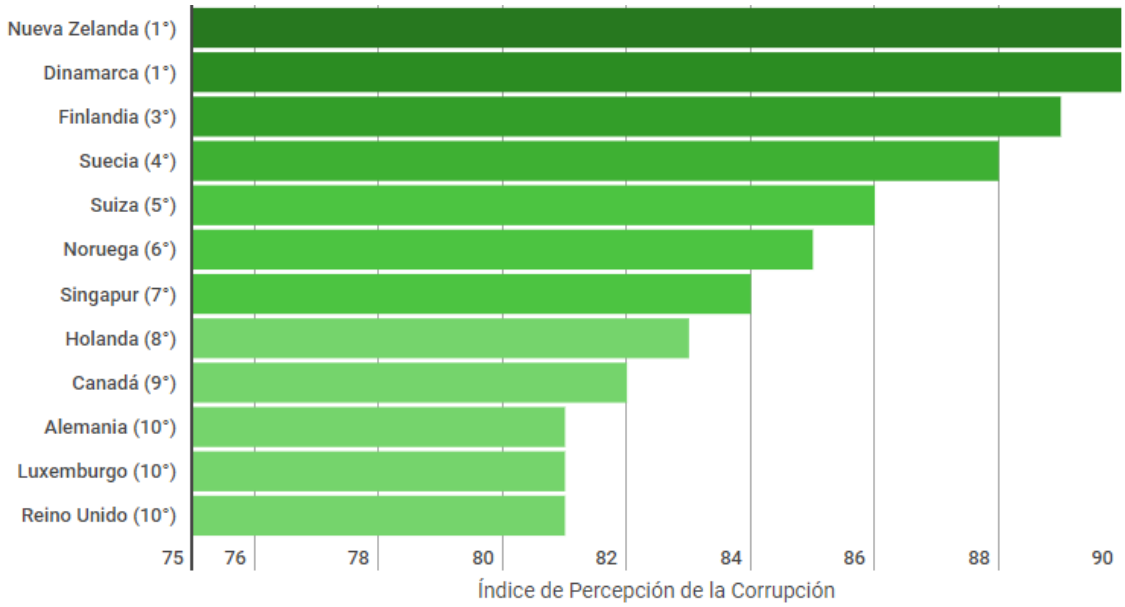

Ilustración 40. Los países menos corruptos del mundo según TI 2016.
Fuente: Mizrahi, 2017

Mizrahi (2017) explica en su reportaje que Somalia es considerado el país más corrupto del mundo durante los últimos 10 años consecutivos, esto de entre los 176 países incluidos. Explica también que de muy cerca lo siguen Sudán del Sur (11), Corea del Norte (12), Siria (13), Libia (14), Yemen (14), Sudán (14), Afganistán (15), Guinea-Bisáu (16), Venezuela (17) e Irak (17).

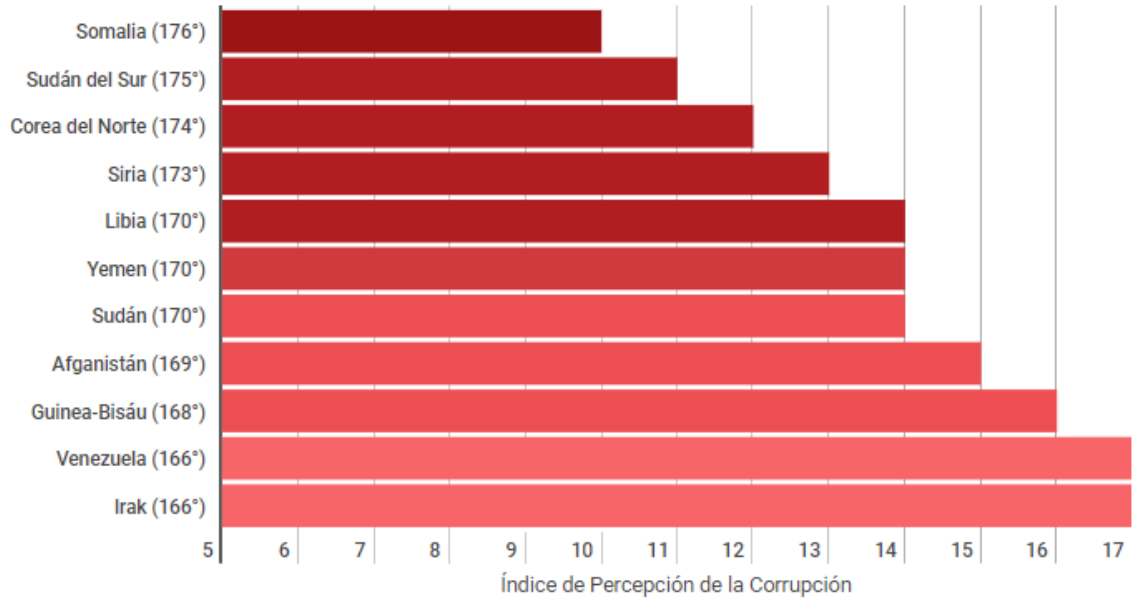

Ilustración 41. Los países más corruptos del mundo según TI 2016.
Fuente: Mizrahi, 2017

Los resultados de este año resaltan la relación entre la corrupción y la desigualdad , que se alimentan mutuamente para crear un círculo vicioso entre la corrupción, la distribución de desigual del poder en la sociedad y la distribución de desigual de la riqueza. (Transparencia Internacional, 2017)

José Ugaz, presidente de Transparency International señala que, “En demasiados países, las personas se ven privadas de sus necesidades más básicas y se acuestan con hambre todas las noches debido a la corrupción, mientras que los poderosos y corruptos disfrutan de estilos de vida con impunidad.”

Transparency International en su informe 2016 también muestra los cambios en puntajes que han tenido los países desde el año 2012:

2016 Rank	Country	2016 Score	2015 Score	2014 Score	2013 Score	2012 Score	Region
1	Denmark	90	91	92	91	90	Europe and Central Asia
1	New Zealand	90	91	91	91	90	Asia Pacific
3	Finland	89	90	89	89	90	Europe and Central Asia
4	Sweden	88	89	87	89	88	Europe and Central Asia
5	Switzerland	86	86	86	85	86	Europe and Central Asia
6	Norway	85	88	86	86	85	Europe and Central Asia
7	Singapore	84	85	84	86	87	Asia Pacific
8	Netherlands	83	84	83	83	84	Europe and Central Asia
9	Canada	82	83	81	81	84	Americas
10	Germany	81	81	79	78	79	Europe and Central Asia
10	Luxembourg	81	85	82	80	80	Europe and Central Asia
10	United Kingdom	81	81	78	76	74	Europe and Central Asia
13	Australia	79	79	80	81	85	Asia Pacific
14	Iceland	78	79	79	78	82	Europe and Central Asia
15	Belgium	77	77	76	75	75	Europe and Central Asia
15	Hong Kong	77	75	74	75	77	Asia Pacific

Ilustración 42. Los países menos corruptos del mundo 2012-2016.
Fuente: Transparencia Internacional, 2017

2016 Rank	Country	2016 Score	2015 Score	2014 Score	2013 Score	2012 Score	Region
159	Republic of Congo	20	23	23	22	26	Sub Saharan Africa
164	Angola	18	15	19	23	22	Sub Saharan Africa
164	Eritrea	18	18	18	20	25	Sub Saharan Africa
166	Iraq	17	16	16	16	18	Middle East and North Africa
166	Venezuela	17	17	19	20	19	Americas
168	Guinea-Bissau	16	17	19	19	25	Sub Saharan Africa
169	Afghanistan	15	11	12	8	8	Asia Pacific
170	Libya	14	16	18	15	21	Middle East and North Africa
170	Sudan	14	12	11	11	13	Middle East and North Africa
170	Yemen	14	18	19	18	23	Middle East and North Africa
173	Syria	13	18	20	17	26	Middle East and North Africa
174	Korea (North)	12	8	8	8	8	Asia Pacific
175	South Sudan	11	15	15	14	N/A	Sub Saharan Africa
176	Somalia	10	8	8	8	8	Sub Saharan Africa

Ilustración 43. Los países más corruptos del mundo 2012-2016.
Fuente: Transparencia Internacional, 2017

Los países de mayor puntaje o rango en la lista, tienden a tener mayores grados de libertad de prensa, permiten el acceso a la información sobre los gastos públicos, normas estrictas para funcionarios públicos y sistemas judiciales independientes. Esto no quiere decir que dichos países sean inmunes a acuerdos a puerta cerrada, conflictos de interés , finanzas ilícitas y aplicación de leyes irregulares. (Transparencia Internacional, 2017)

Los países de menor puntaje o rango en la lista, a menudo están plagados de instituciones públicas poco fiables y mal funcionadas, como la policía y el poder judicial. Incluso cuando existen leyes anti-corrupción y están escritas en los libros, en la práctica son a menudo ignoradas. Las personas se enfrentan a menudo con situaciones de soborno y extorsión.

2.2.8 Índice de corrupción en América.

Desde los ya conocidos *Panamá Papers* o Papeles de Panamá en abril hasta el récord de 3.500 millones de dólares del caso Odebrecht en Brasil en diciembre de 2016, se ha observado que fue un buen año en la lucha contra la corrupción en las América. (Ebrard, 2017)

Los *Panamá Papers* han revelado que un bufete de abogados panameño colaboro para establecer a miles de compañías secretas, muchas de estas compañías han sido usadas por políticos corruptos, criminales y evasores de impuestos alrededor del mundo. El acuerdo de la empresa Odebrecht con el Departamento de Justicia de Estados Unidos (DOJ) exhibe a una empresa que gasta millones de dólares en sobornar a políticos y partidos políticos de América Latina, de igual manera en dos países africanos para ganar contratos comerciales.

En casos como Odebrecht, Petrobras y la FIFA, vemos el incremento de la cooperación y la comunicación entre los reguladores y la aplicación de la ley en toda la región y también con sus semejantes en Europa y los Estados Unidos. (Ebrard, 2017)

Odebrecht SA y la petroquímica Braskem SA han acordado pagar por lo menos 3.500 millones de dólares (2.600 millones de dólares de Odebrecht y 957 millones de dólares de Braskem), el mayor castigo en un caso de soborno extranjero, por cargos internacionales. Esta enorme penalidad fue negociada en un amplio acuerdo con las autoridades estadounidenses, brasileñas y suizas.

La empresa Odebrecht es la mayor empresa de ingeniería de Latinoamérica y la empresa Braskem, el mayor productor petroquímico de la región, es propiedad conjunta de Odebrecht y Petrobras.

De 2001 a 2016, la empresa Odebrecht pagó aproximadamente $ 788 millones en sobornos en asociación con 100 proyectos en 12 países, entre los cuales se encuentran Brasil, Argentina, Colombia, México, Venezuela entre otros, de acuerdo con los documentos de cobro estadounidenses. (Rosenberg & Raymond, 2016)

Aunque 2016 marque el comienzo de un cambio todavía queda mucho camino por recorrer debido a que, en muchas partes de la región, la impunidad sigue siendo un problema importante.

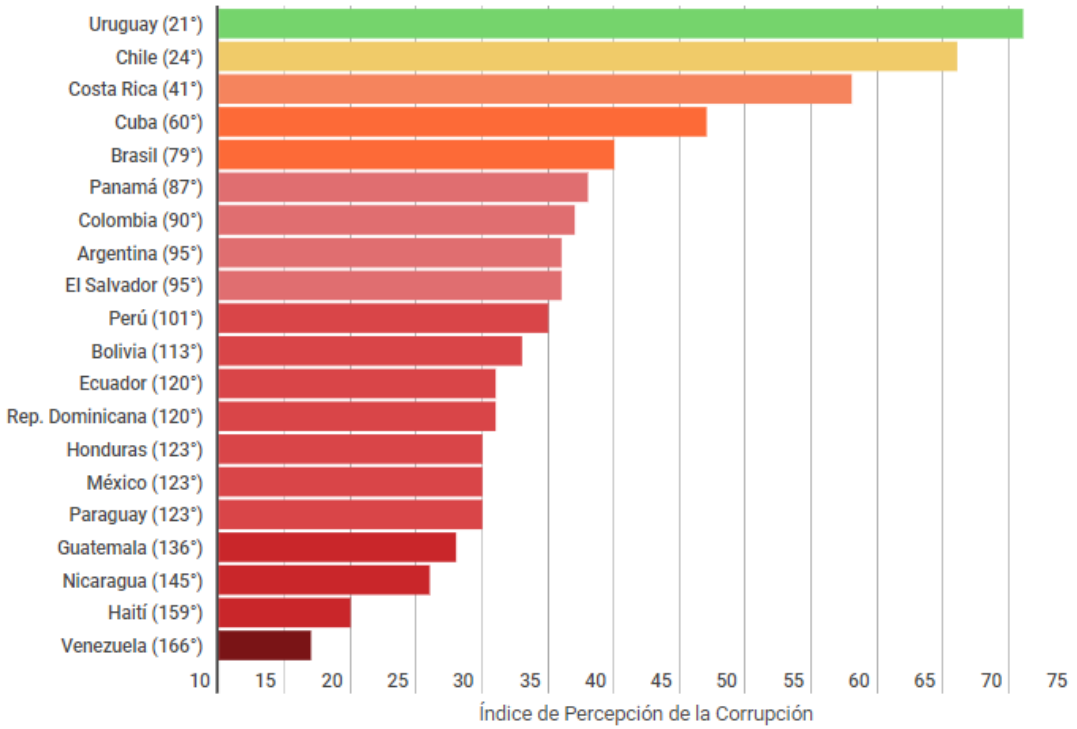

Ilustración 44. Ranking de corrupción en América Latina.
Fuente: Mizrahi, 2017

Venezuela, con una puntuación de 17 se ubica 166 sobre 176 a nivel mundial, Apenas mejor están Haití (159°), Nicaragua (145°), Guatemala (136°), Honduras (123°), México (123°) y Paraguay (123°). (Mizrahi, 2017)

En México es un caso preocupante, porque bajo 5 puntos, mientras el gobierno intenta limpiar la imagen del país a través de una serie de reformas, los escándalos de corrupción siguen aumentando y la imagen del presidente está en un nivel muy bajo. (Ebrard, 2017)

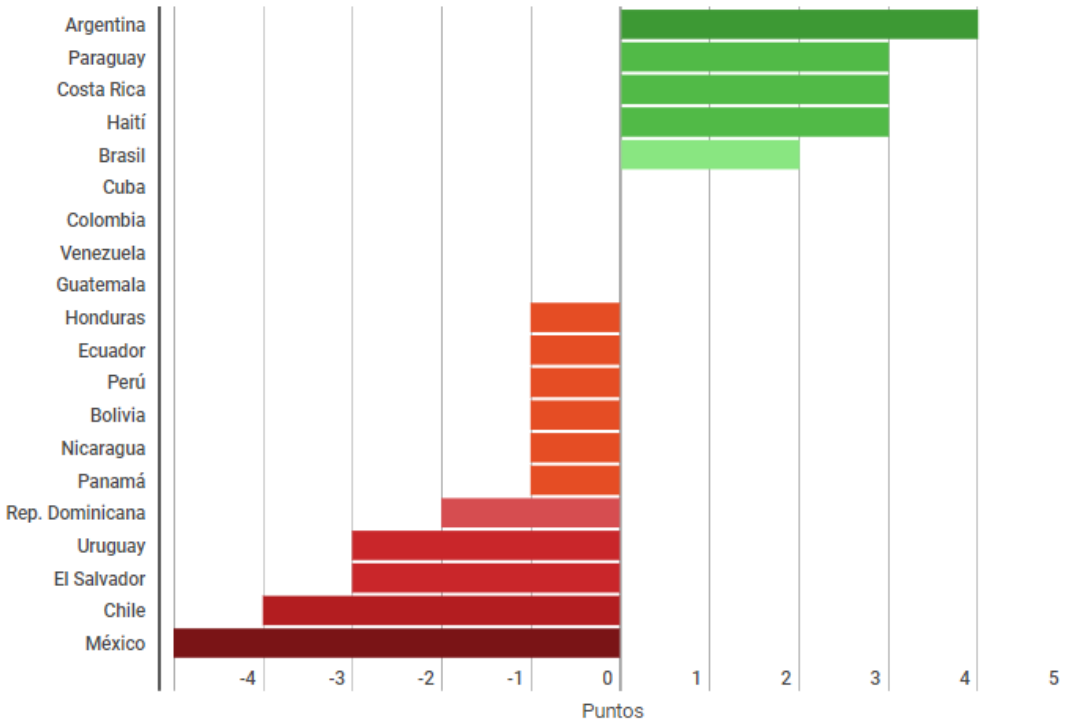

Ilustración 45. Índice de corrupción en América Latina. Diferencias de puntaje con 2015.
Fuente Mizrahi, 2017

Para información más detallada puede visitar la página https://www.transparency.org/

2.2.9 Índice de Fuentes de Soborno.

El Índice de Fuentes de Soborno de Transparency International en su última versión año 2011, clasifica a 28 principales países exportadores a nivel internacional y regional en función de que exista una posibilidad de que sus compañías paguen sobornos en el extranjero.

Las empresas de China y Rusia, se perciben como las más propensas a participar en sobornos en el extranjero, ya que durante el 2010 invirtieron US$ 120.000 millones en el exterior. Por su parte, las empresas de los Países Bajos y Suiza se consideran las menos propensas a pagar sobornos.

El informe presentado en Londres/Berlín con fecha, 2 de noviembre de 2011 – Señala que el soborno de funcionarios públicos en el transcurso de actividades comerciales en el extranjero sería

una práctica cotidiana, así lo señala una encuesta efectuada a 3.000 ejecutivos de empresas de países desarrollados y en desarrollo. (TRANSPARENCY INTERNATIONAL ESPAÑA, 2011)

En la encuesta, diversos líderes de empresas internacionales indicaron que existe el soborno a funcionarios públicos con el fin de, agilizar procesos gubernamentales, conseguir la adjudicación de licitaciones públicas, influir en la determinación de políticas o evitar el cumplimiento de reglamentaciones.

Posición	País/territorio	Puntuación del Índice de Fuentes de Soborno 2011
1	Países Bajos	8,8
1	Suiza	8,8
3	Bélgica	8,7
4	Alemania	8,6
4	Japón	8,6
6	Australia	8,5
6	Canadá	8,5
8	Singapur	8,3
8	Reino Unido	8,3
10	EE. UU.	8,1
11	Francia	8,0
11	España	8,0
13	Corea del Sur	7,9
14	Brasil	7,7
15	Hong Kong	7,6
15	Italia	7,6
15	Malasia	7,6
15	Sudáfrica	7,6
19	Taiwán	7,5
19	India	7,5
19	Turquía	7,5
22	Arabia Saudita	7,4
23	Argentina	7,3
23	Emiratos Árabes Unidos	7,3
25	Indonesia	7,1
26	México	7,0
27	China	6,5
28	Rusia	6,1
	Promedio	7,8

Ilustración 46. Índice de Fuentes de Soborno 2011 por PAÍSES.
Fuente: TRANSPARENCY INTERNATIONAL ESPAÑA, 2011

Las puntuaciones se obtienen a partir de las respuestas ofrecidas por ejecutivos de empresas a la pregunta de con qué frecuencia las compañías de un determinado país, con las cuales mantienen una relación comercial, participan en sobornos (0=siempre, 10=nunca). (TRANSPARENCY INTERNATIONAL ESPAÑA, 2011)

Posición	Sector	Puntuación del sector
1	Agricultura	7,1
1	Industria ligera	7,1
3	Sector aeroespacial civil	7,0
3	Tecnología de la información	7,0
5	Sector bancario y de finanzas	6,9
5	Silvicultura	6,9
7	Servicios para el consumidor	6,8
8	Telecomunicaciones	6,7
8	Transporte y almacenamiento	6,7
10	Sector de armamento, defensa y militar	6,6
10	Pesca	6,6
12	Industria pesada	6,5
13	Sector farmacéutico y de atención de la salud	6,4
13	Generación y transmisión de energía	6,4
15	Minería	6,3
16	Petróleo y gas	6,2
17	Sector inmobiliario, de propiedades y servicios empresariales y jurídicos	6,1
17	Servicios públicos	6,1
19	Contratos de obras públicas y construcción	5,3
	Promedio	6,6

Ilustración 47. Índice de Fuentes de Soborno 2011 por SECTORES.
Fuente: TRANSPARENCY INTERNATIONAL ESPAÑA, 2011

Y se hace un análisis de los cambios en las puntuaciones del Índice de Fuentes de Soborno entre 2008–2011. Un valor positivo significa que ha existido una mejora en la puntuación del país, en tanto una puntuación negativa significa que ha existido un aumento en la percepción sobre la probabilidad de que las empresas de esos países ofrezcan sobornos en el extranjero durante los tres años. (TRANSPARENCY INTERNATIONAL ESPAÑA, 2011)

País/territorio				de Soborno		
	2011	2008	Cambio	2011	2008	Cambio
Países Bajos	8,8	8,7	0,1	1	3	2
Suiza	8,8	8,7	0,1	1	3	2
Bélgica	8,7	8,8	-0,1	3	1	-2
Alemania	8,6	8,6	0,0	4	5	1
Japón	8,6	8,6	0,0	4	5	1
Australia	8,5	8,5	0,0	6	8	2
Canadá	8,5	8,8	-0,3	6	1	-5
Singapur	8,3	8,1	0,2	8	9	1
Reino Unido	8,3	8,6	-0,3	8	5	-3
EE. UU.	8,1	8,1	0,0	10	9	-1
Francia	8,0	8,1	-0,1	11	9	-2
España	8,0	7,9	0,1	11	12	1
Corea del Sur	7,9	7,5	0,4	13	14	1
Brasil	7,7	7,4	0,3	14	17	3
Hong Kong	7,6	7,6	0,0	15	13	-2
Italia	7,6	7,4	0,2	15	17	2
Sudáfrica	7,6	7,5	0,1	15	14	-1
Taiwán	7,5	7,5	0,0	18	14	-4
India	7,5	6,8	0,7	18	19	1
México	7,0	6,6	0,4	20	20	0
China	6,5	6,5	0,0	21	21	0
Rusia	6,1	5,9	0,2	22	22	0
Promedio	7,9	7,8				

Ilustración 48. Cambios en las puntuaciones del Índice de Fuentes de Soborno 2008–2011.
Fuente: TRANSPARENCY INTERNATIONAL ESPAÑA, 2011

2.3 Introducción a la ISO 37001

Un Sistema de Gestión Anti-soborno o *Anti-bribery Management System* (ABMS) significa un compromiso para promover una cultura empresarial ética que ayuda a una organización para aumentar la reputación, actuar bien y evitar posibles riesgos de soborno. La participación en la corrupción puede conducir a daños de reputación y pérdida de credenciales.

La norma ISO 37001:2016 Sistemas de gestión anti-soborno, publicada el 14 de octubre de 2016 y desarrollada por la Organización Internacional de Normalización (ISO). Esta norma determina los requisitos que debe cumplir un sistema de gestión anti-soborno, con los cuales ayuda a las organizaciones a establecer, implementar, mantener y mejorar un sistema de gestión de la lucha contra el soborno. (Quaragroup, 2016)

Incluye controles y medidas que representan buenas prácticas de lucha contra el soborno, las que benefician enormemente a las organizaciones debido a que garantizan a los inversores, directivos, partes interesadas, que la organización está tomando medidas en contra del soborno. Además, la norma es certificable e incluye un anexo que sirve de guía para aplicar la norma en una organización. (Quaragroup, 2016)

Según PECB (2016),

> el término "soborno" se refiere a cualquier oferta, donación, aceptación o ventajas prometedoras con cualquier valor con el fin de influir en la acción, decisión o juicio de las personas encargadas de un deber. Sin embargo, La norma Internacional no aborda específicamente el fraude ("dar sobornos") o cualquier otra actividad relacionada con corrupción; sino que establece requisitos y proporciona orientación para la creación de un sistema de gestión que ayuda a prevenir, detectar y responder al soborno en cumplimiento con las leyes anti-soborno.

La norma aborda los objetivos de gestión para la prevención del soborno en estos contextos:

a. Soborno en los sectores público, privado y sin fines de lucro
b. Soborno por parte de la organización
c. Soborno por parte del personal de la organización que actúe en nombre de la organización o para beneficio propio
d. Soborno por los socios comerciales de la organización que actúan en nombre de la organización o para beneficio propio
e. Soborno del personal de la organización en relación con las actividades de la organización

f. Soborno de los asociados de la organización en relación con las actividades de la organización

g. Pago directo e indirecto (PECB, 2016)

2.3.1 Cláusulas clave de ISO 37001: 2016.

- Cláusula1: Alcance
- Cláusula2: Referencias normativas
- Cláusula3: Términos y definiciones
- Cláusula4: Contexto de la organización
- Cláusula5: Liderazgo
- Cláusula6: Planificación del Sistema de Gestión Anti-soborno
- Cláusula7: Apoyo
- Cláusula8: Operación
- Cláusula9: Evaluación del desempeño
- Cláusula10: Mejora

Cláusula 4: Contexto de la organización

Para una correcta implementación de un Sistema de Gestión Anti-soborno, se debe entender la organización y su contexto, comprender las necesidades y expectativas de la parte interesada, el Sistema de Gestión Anti-soborno y la evaluación del riesgo de soborno.

La cláusula 4 se divide en cinco partes y describe lo que es importante saber acerca de la organización y la implementación del Sistema de Gestión Anti-soborno.

4.1 Entender la organización y su contexto

Para lograr los objetivos de un Sistema de Gestión Anti-soborno, una organización debe determinar los factores externos e internos que son relevantes para su propósito.

Algunos de estos factores incluyen:

- Tamaño y estructura de la organización
- Lugares y sectores en los que la organización opera o anticipa operaciones
- Naturaleza, escala y complejidad de las actividades y operaciones de la organización
- Entidades sobre las cuales la organización tiene control o cualquier empresa conjunta
- Asociaciones de negocios de la organización
- La naturaleza y el alcance de las interacciones con los funcionarios públicos
- Obligaciones legales, reglamentarias, contractuales y profesionales aplicables, y deberes. (PECB, 2016)

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización determinará las partes interesadas que sean relevantes para el Sistema de Gestión Anti-Soborno y determinará los requerimientos oportunos de dichas partes.

4.3 Determinación del alcance del Sistema de Gestión Anti-soborno

La organización decidirá los límites y la aplicabilidad del Sistema de Gestión Anti-Soborno. El alcance se encontrará disponible como información documentada.

Al determinar el alcance, la organización debe considerar:

- Factores externos e internos mencionados en 4.1
- Requisitos a que se refiere el punto 4.2
- Los resultados de la evaluación del riesgo de soborno a la que se hace referencia en el párrafo 4.5 (PECB, 2016)

4.4 Sistema de gestión contra el soborno

La organización establecerá, aplicará, mantendrá, revisará continuamente y, si es necesario, mejorará el sistema de gestión del soborno, incluidos los procesos necesarios y sus interacciones.

El Sistema de Gestión Anti-soborno contendrá medidas diseñadas para identificar, evaluar, tratar y prevenir el soborno. (PECB, 2016)

4.5 Evaluación del riesgo de soborno

La organización llevará a cabo evaluaciones del riesgo de soborno que:

- Identificar los riesgos de soborno que la organización podría razonablemente prever, dados los factores externos e internos determinados
- Evaluar y priorizar los riesgos de soborno identificados
- Evaluar la capacidad y eficacia de los controles existentes de la organización para mitigar los riesgos de soborno evaluados.

La evaluación del riesgo de soborno se revisará periódicamente para evaluar debidamente los cambios y la nueva información; y en el caso de un cambio significativo en la estructura o actividades de la organización. (PECB, 2016)

Cláusula 5: Liderazgo

5.1.1: Un órgano rector o la alta dirección de una organización deberá demostrar liderazgo y compromiso con respecto al Sistema de Gestión Anti-soborno:

- Aprobación de las políticas anti-soborno de la organización
- Asegurar que la estrategia de la organización y la política anti-soborno estén alineadas
- Recibir y revisar la información relacionada con el contenido y el funcionamiento del Sistema de Gestión Anti-soborno de la organización a intervalos planificados

- Asegurar que se asignen los recursos adecuados y apropiados para el funcionamiento eficaz del Sistema de Gestión contra el Soborno
- Garantizar que las medidas apropiadas de investigación y remediación se tomaron en acción y se documentaron eficazmente
- Ejercer una supervisión razonable sobre la implementación de la ABMS de la organización por la alta dirección y su eficacia. (PECB, 2016)

5.1.2 La alta dirección deberá demostrar su liderazgo y compromiso con la ABMS mediante:

- Asegurar que el Sistema de Gestión Anti-soborno, incluyendo sus políticas y objetivos, sea establecido, implementado, mantenido y revisado para hacer frente adecuadamente a los riesgos de soborno en la organización
- Garantizar la integración de los requisitos del ABMS en los procesos de la organización
- El despliegue de recursos adecuados para el funcionamiento eficaz de la ABMS
- Comunicación interna y externa sobre la política anti-soborno
- Comunicación interna de la importancia de una gestión eficaz contra el soborno y de la conformidad con los requisitos ABMS
- Garantizar que el ABMS se diseñe adecuadamente para alcanzar sus objetivos
- Promoción de una cultura anti-soborno adecuada dentro de la organización y mejora continua
- Apoyar otros roles de gestión relevantes para demostrar su liderazgo en la prevención y detección de sobornos
- Fomentar el uso de procedimientos de notificación de sobornos sospechosos y reales
- Garantizar que ningún personal sufrirá represalias o medidas discriminatorias o disciplinarias por los informes hechos de buena fe

- A intervalos planificados, informando al órgano rector, sobre el contenido y el funcionamiento de la ABMS y sobre las denuncias de sobornos graves. (PECB, 2016)

5.2 Una política contra el soborno establecida, mantenida y revisada por la alta dirección deberá:

- Prohibir el soborno
- Estar disponible a las partes interesadas relevante
- Ser comunicado dentro de la organización
- Estar disponible como información documentada
- Comprometerse a la mejora continua del ABMS
- Comprometerse a satisfacer los requisitos del ABMS
- Proporcionar un marco para configuración, revisión y lograr objetivos
- Cumplir con leyes de soborno (PECB, 2016)

La política será apropiada para el propósito de la organización y fomentará el aumento de las preocupaciones en confianza sin temor a represalias.

5.3 Funciones, responsabilidades y autoridades de la organización

La alta dirección asignará a una función, responsabilidad y supervisión del diseño y la aplicación del sistema de lucha contra el soborno, proporcionando asesoramiento y orientación, vigilando que el sistema cumpla con los requisitos de la norma e informar su desempeño. El sistema anti-soborno deberá contar con los recursos adecuados y asignarse a una persona o personas con las competencias, estatus, autoridad e independencia.

5.3.1 Funciones y responsabilidades

- La alta gerencia mantiene la responsabilidad general de la implementación y el cumplimiento de una ABMS.

- Las responsabilidades y las autoridades de las funciones pertinentes se asignan y se comunican a través de la organización. Los gerentes de cada nivel siguen siendo responsables de la aplicación de ABMS y cumplimiento en su departamento o función.
- El órgano rector, la alta dirección y todo el resto del personal son responsables de comprender y aplicar los requisitos de ABMS relacionados con sus funciones. (PECB, 2016)

5.3.2 Función de cumplimiento contra el soborno

La alta dirección asignará a una función de cumplimiento contra el soborno, responsabilidad y autoridad para:

- Supervisar el diseño e implementación de ABMS por la organización.
- Proporcionar asesoramiento y orientación al personal de cajeros automáticos y las cuestiones relacionadas con el soborno.
- Asegurar la conformidad con los requisitos de la norma ISO 37001.
- Informar sobre el desempeño de la ABMS al órgano de gobierno y alta dirección.

La función contará con los recursos adecuados, incluida la persona competente con independencia. La función tendrá acceso directo y rápido al órgano rector y a la alta dirección. (PECB, 2016)

5.3.3 Para el soborno de bajo riesgo, la alta dirección debe establecer y mantener un proceso de toma de decisiones. Los procesos y cumplimientos serán revisados periódicamente por la alta dirección. (PECB, 2016)

El Comité de Riesgo de Tecnología de Información (CRTI) tiene la responsabilidad de evaluar la planificación de riesgo tecnológico y de información, y monitorear la gestión del rendimiento, también los componentes de seguridad de la información. Las decisiones tomadas en esta área se deben basar en un adecuado programa de gestión de riesgo.

Cláusula 6: Planificación

Al planificar un sistema de gestión de la lucha contra el soborno, la organización se referirá a:

- Factores externos e internos determinados en contexto
- Requisitos de las partes interesadas como determinados
- Evaluación de riesgos de soborno y su control efectivo
- Oportunidades de mejora

Los objetivos mensurables y alcanzables de lucha contra el soborno deben ser coherentes con la política, actualizado según convenga. Se mantendrá la información documentada sobre los objetivos anti-soborno.

Al planificar cómo lograr objetivos anti-soborno, la organización debe determinar los recursos necesarios, quién será el responsable, cuándo se alcanzarán los objetivos y cómo los resultados serán evaluados y reportados. (PECB, 2016)

Cláusula 7: Apoyo

La organización proporcionará los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del Sistema de Gestión Anti-soborno. Además, seleccionará a personas competentes para llevar a cabo un marco de Sistema de Gestión de Lucha contra el Soborno junto con sus políticas dentro de la organización.

También proporcionará formación y concienciación adecuada al personal, incluidos los asociados comerciales y personas interesadas para que no actúen en su nombre o para beneficio propio y que no puedan generar un riesgo de soborno en la organización.

La organización deberá implementar procedimientos relacionados con el empleo con controles sobre:

- Condiciones de empleo para cumplir con ABMS y el derecho a disciplina
- Acceso a políticas y formación sobre el mismo

- Acciones que deben tomarse para violar la política anti-soborno y ABMS
- El personal no es penalizado por negarse a participar en alguna actividad con respecto a la cual haya juzgado que existe un riesgo de soborno o por plantear preocupaciones, reportes sobre sobornos reales o sospechosos o el incumplimiento de la política ABMS. (PECB, 2016)

Cláusula 8: Operación

Se aplicarán procedimientos que impidan la oferta, la prestación o la aceptación de donaciones y beneficios similares, ya que podrían percibirse como soborno.

Este estándar internacional ha proporcionado varios controles en las secciones de la debida diligencia (8.2), controles financieros y no financieros. Los controles se realizan principalmente en transacciones, proyectos o actividades y relaciones. (8,3 y 8,4)

La organización deberá implementar procedimientos que exijan que todas las demás organizaciones sobre las que tiene control implementen el sistema de gestión anti-soborno de la organización o implementen sus propios controles anti-soborno (8.5).

Cuando los socios de negocios tienen un riesgo más que aceptable de soborno, se requieren controles y decisiones efectivos. La evaluación del riesgo de soborno para la organización es necesaria. (8.6)

La organización deberá tener un procedimiento para regular las cuestiones relativas a regalos, hospitalidad, donaciones y beneficios similares. (8,7)

Donde la organización no puede manejar el riesgo de soborno, la relación, proyecto o contrato debe ser revisado en las etapas apropiadas y retirarse o declinar, como sea posible. (8,8)

El procedimiento también mantendrá la confidencialidad, permitirá la notificación anónima y protegerá al personal contra represalias. La organización debe asegurarse de que las personas son conscientes del procedimiento de presentación de informes, sus derechos y protecciones. (8,9)

La organización deberá implementar procedimientos para la investigación y el tratamiento del soborno que asegure una investigación efectiva. Las investigaciones deben ser llevadas a cabo por un personal independiente y que reporta los resultados al personal que no es parte de la función investigada. (8.10) (PECB, 2016)

Cláusula 9: Evaluación del desempeño

La organización supervisará, medirá, analizará y evaluará las políticas contra el soborno. Sin embargo, antes de completarlo, la organización determinará:

- Lo que necesita ser monitoreado
- Qué métodos se utilizarán para garantizar resultados válidos
- Cuando se realizarán el control y la medición
- Cómo es documentado

Correspondientemente, se llevará a cabo una auditoría interna con el fin de proporcionar información sobre si el Sistema Anti-soborno se ajusta a los requisitos de la organización y a los requisitos de las Normas Internacionales.

El órgano rector llevará a cabo revisiones periódicas de la ABMS sobre la base de la información proporcionada por la alta dirección. (PECB, 2016)

Cláusula 10: Mejora

La organización reaccionará ante cualquier falta de conformidad que se produzca tomando medidas para controlar, corregir y tratar las consecuencias.

La organización deberá mejorar continuamente la adecuación, eficacia y eficiencia del Sistema de Gestión Anticorrupción que se ha implementado. Además, con la mejora continua, la organización logra sus objetivos de manera más fácil. (PECB, 2016)

2.3.2 Integración de ISO 37001 con otros sistemas de gestión.

La organización puede elegir si desea implementar el Sistema de Gestión Anti-soborno como un sistema separado, o como parte integrada de un sistema de gestión de cumplimiento global.

Tabla 8:
Integración de la ISO 37001 con otros sistemas de Gestión.

Requisitos	ISO 37001: 2016	ISO 9001: 2015	ISO 14001: 2015	ISO 27001: 2013	ISO 22301:2012
Sistema de gestión Objetivos	6.2	6.2	6.2	6.2	6.2
Política del sistema de gestión	5.2	5.2	5.2	5.2	5.3
Liderazgo y Compromiso	5.1	5.1	5.1	5.1	5.2
Información documentada	7.5	7.5	7.5	7.5	7.5
Auditoría interna	9.2	9.2	9.2	9.2	9.2
Mejora continua	10.2	10.3	10.2	10.2	10
Revisión de gestión	9.3	9.3	9.3	9.3	9.3

Fuente: (PECB,2016)

2.3.3 Sistema de gestión contra el soborno - los beneficios del negocio.

La norma ISO 37001 no puede proporcionar garantías de que no se ha producido u ocurrirá ningún riesgo de soborno en la organización, pero puede ayudar a la organización a implementar las medidas necesarias para prevenir, detectar y abordar el soborno.

Las organizaciones que están certificadas y cumplen con un Sistema de Gestión Anti-soborno son más confiables y reconocidas por practicar la cultura de Lucha contra el soborno.

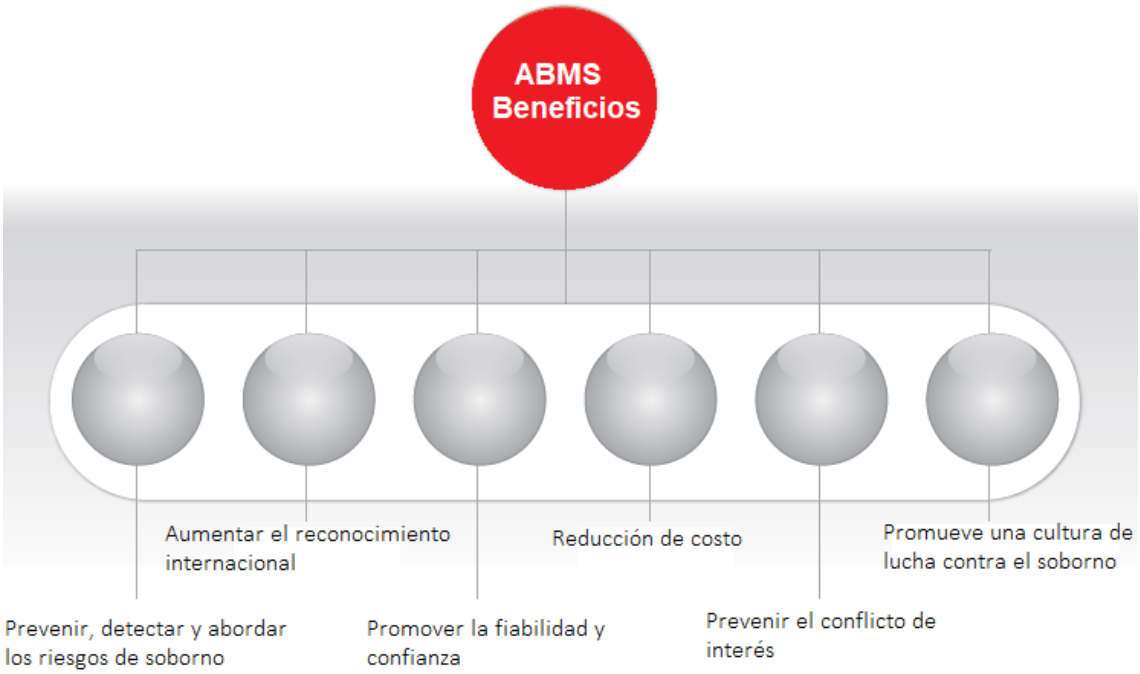

Ilustración 49. Beneficios del ABMS.
Fuente: PECB, 2016

2.3.4 Requisitos que establece la norma.

Según Quaragroup (2016), existen diversos requisitos que la norma determina deben cumplirse. Deberán ser revisados para que ninguno de estos esté en contra de la ley del país en el que se desee implementar.

Entre los requisitos más destacados encontramos:

- Implementar una política y programa de anti soborno.
- Comunicar la política y programa de anti soborno a todo el personal y asociados
- Nombrar a un responsable para supervisar el programa
- Proporcionar al personal la formación anti soborno apropiada.
- Evaluar los riesgos de soborno, incluyendo la apropiada due diligence.

- Asegurar que organizaciones relacionadas y los socios han implementado controles apropiados en temas de anti soborno.
- Verificar dentro de lo razonable, que el personal cumplirá con la política de anti soborno.
- Controlar los regalos, la hospitalidad, donaciones y beneficios similares para asegurar que los mismos no tienen un propósito de soborno.
- Implementar controles apropiados en cuanto a la financiación, adquisiciones y otros aspectos comerciales con el fin de ayudar a prevenir el riesgo de soborno.
- Implementar procedimientos de reporte para las denuncias informales. (Quaragroup, 2016)

2.3.5 Metodología para la implementación de un Sistema de Gestión Anticorrupción.

Cuando se implementa un Sistema de Gestión Anticorrupción basado en ISO 37001, es importante seguir una metodología bien estructurada y efectiva para cubrir todos los requisitos mínimos de la norma. La norma ISO 37001 también utilizará la metodología PDCA

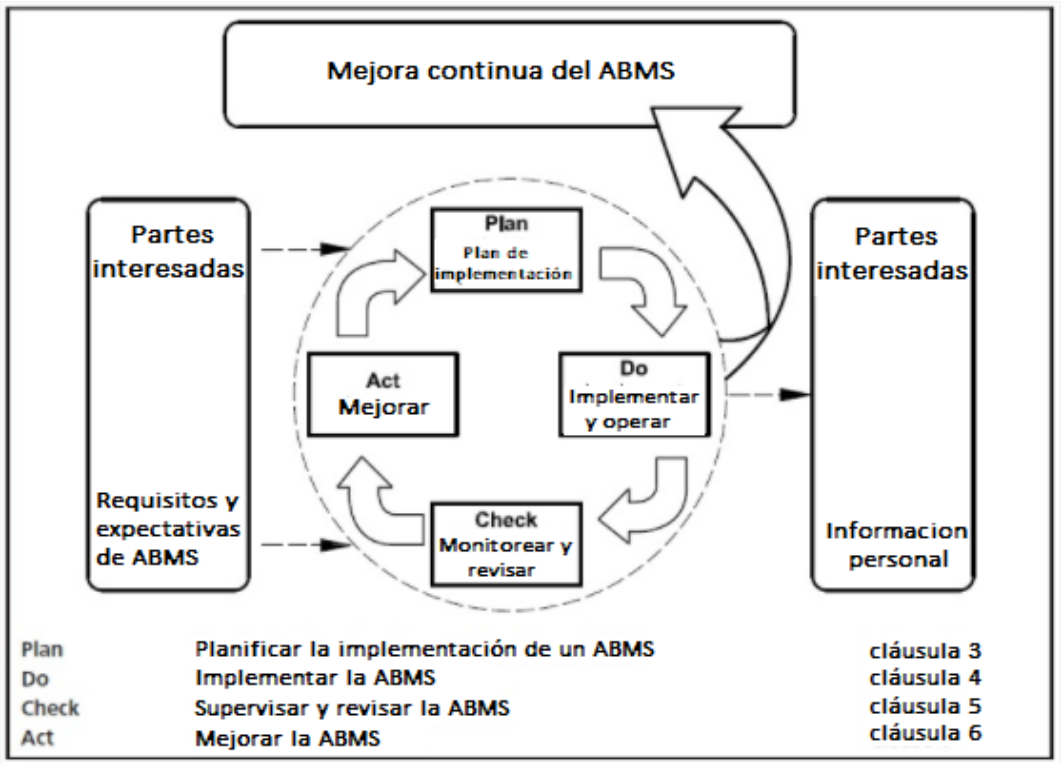

Ilustración 50. PDCA en la ISO 37001.
Fuente: http://www.uniprofessioni.it/sito/index.php/news/75-aggiornamenti-iso-37001

2.4 Conclusiones del capítulo 2

Al revisar la teoría referente a las organizaciones y sociedades, con o sin fines de lucro, se llega a la conclusión, que la mayoría o todas tienen fines en el mercado nacional o internacional; es decir, se constituyen para el desarrollo de actividades económicas y operaciones mercantiles, ya sea, con o sin fines de lucro, pero sí con el fin de desarrollar la organización.

En cuanto a la lucha contra la corrupción y el soborno se concluye que, la corrupción no conoce fronteras debido a que afecta a todos, desde pequeños negocios en países en calidad de desarrollo, hasta compañías multinacionales en países muy desarrollados. Afectando así, el desarrollo del comercio, costes de transacciones, la transparencia de los mercados y quebrantando la confianza

Es por esto que los beneficios de la lucha contra la corrupción son claros, un 50% menos de probabilidad de sufrir actos de corrupción, por lo tanto, menor probabilidad de perder negocios en comparación con otras organizaciones que no han desarrollado algún método o programa anticorrupción. Otras razones suponen asumir altos costes directos como, multas y penas de prisión; daño en la reputación empresarial, en la capacidad de supervivencia y rentabilidad.

Se ha determinado que los empleados son los actores más importantes al momento de detectar el fraude corporativo. Es por esto que la OCDE encuentra muy importante la protección legal de los denunciantes y por lo que cuenta con alrededor de dos décadas de experiencia para revisar las medidas de protección de denunciantes.

Existe una serie de normas contra la corrupción entre las cuales se encuentran, la Convención Interamericana Contra la Corrupción (CICC), la Convención de la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Convención Naciones Unidas contra delincuencia organizada transnacional 2003, la Convención de Naciones Unidas contra la Corrupción (CNUCC), entre otras. Una ley muy conocida, la ley FCPA, se ha encargado de cobrar

millonarias multas por resolver casos de violaciones contra dicha ley a importantes empresas multinacionales. Al igual que ha pasado en diferentes partes del mundo, en América Latina se encuentran casos en donde la SEC y el DOJ han impuesto acciones legales en contra de empresas o individuos.

El Índice de Percepción de la de la Corrupción ha identificado a Nueva Zelanda y Dinamarca como los países menos corruptos del mundo, al mismo tiempo indica que Somalia seguido de Sudán del Sur, Corea del norte, entre otros son los países con más índice de corrupción en el mundo. En América Latina, Venezuela se ubica en el puesto número 166 sobre 176 a nivel mundial.

En cuanto al Índice de Fuentes de Soborno, indica que empresas de China y Rusia son las más propensas a participar en sobornos en el extranjero y esto se debe a que invierten millones de dólares en el exterior. Por otra parte, empresas de los Países bajos y Suiza se consideran las menos propensas a pagar sobornos.

Se concluye también que el estándar ISO 37001 es muy flexible ya que se puede adaptar a una amplia gama de organizaciones en las que se encuentran, Grandes organizaciones, Pequeñas y medianas empresas (PYMES), organizaciones públicas y privadas, Organizaciones no gubernamentales (ONG). La norma puede ser utilizada por organizaciones de cualquier país.

CAPÍTULO 3 – Alineación de ISO 37001 con las normas ISO utilizadas en la Gestión de Riesgos de la Información.

La norma ISO 37001 incluye 10 cláusulas, de las cuales, las tres primeras son introductorias; es decir, no es necesario buscar una alineación con otras normas en dichas cláusulas. A partir de la cláusula 4 se estudiará la existencia de algún tipo de alineación.

3.1 Alineación con ISO 27001

Los cambios entre la ISO 27001:2005 y la ISO 27001:2013 han sido cambios sustanciales para lograr una alineación de esta norma con otros estándares de sistemas de gestión que cubren la garantía de calidad, la protección ambiental, etc.

La ISO / IEC 27001: 2013 tiene las siguientes secciones:

- 0. Introducción
- 1. Alcance
- 2. Referencias normativas
- 3. Términos y definiciones
- 4. Contexto de la organización
- 5. Liderazgo
- 6. Planificación
- 7. Apoyo
- 8. Operación
- 9. Evaluación del desempeño
- 10. Mejora
- Anexo A Objetivos y controles de control de referencia
- Bibliografía (INEN, 2013)

La ISO 37001 tiene alineación con la ISO 27001 desde la cláusula 4 debido a que en ambas normas se trata de comprender el contexto de la organización, se identifican las necesidades y expectativas de las partes interesadas. Todo esto determinará las políticas y los objetivos en el proceso de gestión de riesgos; el alcance del SGSI y el alcance del sistema anti soborno. Se identifican los problemas externos e internos que afectan a la empresa sin importar el tipo de empresa que sea. (ISOTools Excellence, 2015)

En la cláusula 5 debido a que ambas normas se enfocan en el compromiso por parte de la alta gerencia de la organización con los Sistemas de Gestión, tanto el SGSI y el Sistema Anti Soborno. La alta dirección debe demostrar liderazgo y responsabilidad con los sistemas, establecer políticas y asignar funciones, responsabilidades ante las autoridades.

En la cláusula 6 se enfocan en describir el proceso para identificar, analizar y planificar el tratamiento de los riesgos de soborno y riesgos de la información y aclarar los objetivos Anti-Soborno y objetivos de la seguridad de la información.

En la cláusula 7 las normas se enfocan en los requisitos que servirán de apoyo para el establecimiento de la implementación y mejora de los sistemas de gestión, entre los cuales se encuentran, los recursos, el personal competente y la comunicación de todas las partes interesadas. Las normas también establecen procesos para controlar y conservar la documentación que corresponde a los sistemas. En conclusión, en esta cláusula, las normas se enfocan en asignar recursos adecuados y competentes, en concienciar y en preparar y controlar la documentación.

En la cláusula 8 las normas se enfocan en establecer los requisitos para medir el funcionamiento de los sistemas, además del cumplimiento de las normas. Se trabaja más a detalle sobre la evaluación y el tratamiento de los riesgos, la gestión de los controles y la documentación.

En la cláusula 9 las normas se enfocan en monitorear, medir, analizar, evaluar, revisar los controles, los procesos y los sistemas de gestión para realizar mejoras según corresponda. Para la medición de eficacia y desempeño de los sistemas se realizan auditorías internas y revisión de los sistemas.

En la cláusula 10 las normas se enfocan en plantear los hallazgos encontrados en las auditorías y revisiones, como por ejemplo las no conformidades y acciones correctivas, también en hacer ajustes continuos a los sistemas. En esta cláusula los principales elementos para el proceso de mejora son las no conformidades identificadas y las acciones correctivas. (ISOTools Excellence, 2015)

3.2 Alineación con ISO 27002

La norma ISO / IEC 27002 es fundamental para todo tipo de organizaciones, de todos los tamaños como, cualquier organización que maneja y depende de la información.

La norma se refiere explícitamente a la seguridad de la información y no solo la seguridad de los sistemas TI como es la moda del día.

La relación que tiene la norma ISO/IEC 27001 con la norma ISO/IEC 27002 se debe a que la norma ISO/IEC 27001 define formalmente los requisitos obligatorios para un SGSI mientras que utiliza la ISO / IEC 27002 para indicar controles adecuados de seguridad de la información dentro del SGSI. Debido a que la ISO / IEC 27002 es simplemente un código de prácticas o guía en lugar de un estándar de certificación, las organizaciones tienen la libertad de seleccionar e implementar otros controles o adoptar alternativas como mejor le parezca. (IsecT, 2017)

La ISO / IEC 27002:2013 contiene las siguientes secciones:

- Prefacio
- Sección 0: Introducción

- Sección 1: Alcance
- Sección 2: referencias normativas
- Sección 3: Términos y definiciones
- Sección 4: Estructura de esta norma
- Sección 5: Políticas de seguridad de la información
- Sección 6: Organización de la seguridad de la información
- Sección 7: Seguridad de los recursos humanos
- Sección 8: Gestión de activos
- Sección 9: Control de acceso
- Sección 10: Criptografía
- Sección 11: Seguridad física y ambiental
- Sección 12: Seguridad de las operaciones
- Sección 13: Seguridad de las comunicaciones
- Sección 14: Adquisición, desarrollo y mantenimiento del sistema
- Sección 15: relaciones con proveedores
- Sección 16: gestión de incidentes de seguridad de la información
- Sección 17: Aspectos de seguridad de la información de la gestión de la continuidad del negocio
- Sección 18: Cumplimiento
- Bibliografía (IsecT, 2017)

La norma ISO 37001 tiene alineación con la ISO 27002 desde la sección 5 debido a que se enfocan en que la gerencia defina un conjunto de políticas para aclarar su dirección y apoyo para

la seguridad de la información. En la alta dirección debe existir políticas de seguridad de la información como se especifica en ISO / IEC 27001 sección 5.2.

La sección 6 de la ISO 27002 se puede alinear con la cláusula 5.3 de la ISO 37001, ya que se enfocan en la definición de roles y responsabilidades que tendrán los integrantes de la organización para la seguridad de la información. Cuando sea relevante, los deberes deben ser separados entre roles e individuos para evitar conflictos de interés y prevenir actividades inapropiadas. Estos roles y responsabilidades serán definidos por la alta dirección en conjunto con los líderes de la organización.

La sección 7.1, 7.2 y 7.3 de la ISO 27002 se puede alinear con la cláusula 7.2.2 de la ISO 37001, ya que se enfoca en observar las capacidades de las personas, sus competencias para emplearlos adecuadamente en una función para la cual están preparado. La alta dirección de la organización verificará si las personas, antes de ser contratadas y cuando han sido contratadas, cumplen con sus obligaciones de seguridad de la información.

En la sección 8.2 de la ISO 27002 referente a la clasificación de la información, se la puede alinear con la cláusula 7.5 de la ISO 37001 para que la información documentada que se ha obtenido a lo largo del desarrollo y funcionamiento del sistema de gestión anti-soborno, pueda ser debe ser clasificada y etiquetada por sus propietarios de acuerdo con la protección de seguridad necesaria, y pueda manejarse adecuadamente.

La sección 17 de la ISO 27002 referente a la continuidad de seguridad de la información, se la puede integrar con la cláusula 10 de la ISO 37001, para asegurar la continuidad del negocio en aspectos de seguridad de la información, debido a que la norma ISO 37001 establece que la alta dirección asigne una función de cumplimiento que se dedicara a verificar el buen funcionamiento del sistema de gestión con el fin de asegurar la continuidad del negocio. En cuanto a la mejora

continua, la norma exige que el sistema se vaya fortaleciendo a partir de los fallos encontrados en dicho sistema.

La sección 18 de la ISO 27002, se puede alinear con la cláusula 9 de la ISO 37001, debido a que, mediante las auditorías internas, las revisiones de la alta dirección, las revisiones por la función de cumplimiento que exige la norma ISO 37001, se puede identificar y documentar las obligaciones con las autoridades externas y otros terceros en relación con la seguridad de la información. También se pueden auditar los arreglos de seguridad de la información en la organización e informar a la gerencia. La alta dirección junto al órgano rector y la función de cumplimiento deben revisar rutinariamente el cumplimiento de los empleados y sistemas con las políticas de seguridad, procedimientos, etc. e iniciar acciones correctivas cuando sea necesario.

3.3 Alineación con ISO 27005

La Gestión de riesgos de seguridad de la información o *Information Security Risk Management* forma parte de la familia de estándares de la serie ISO / IEC 27000 en el área de sistemas de gestión de seguridad de la información. Es un estándar de apoyo que proporciona pautas a las empresas para adoptar un enfoque estructurado de gestión de riesgos de seguridad de la información.

La norma ISO/IEC 27005:2011 está organizada en las siguientes cláusulas principales:

- Cláusula 5: Antecedentes
- Cláusula 6: Descripción general del proceso de gestión del riesgo de seguridad de la información
- Cláusula 7: Establecimiento de contexto
- Cláusula 8: Evaluación de riesgos de seguridad de la información
- Cláusula 9: Tratamiento de riesgos de seguridad de la información
- Cláusula 10: Aceptación de riesgos de seguridad de la información

- Cláusula 11: Comunicación y consulta de riesgos de seguridad de la información
- Cláusula 12: Control y revisión de riesgos de seguridad de la información. (PECB, 2015)

La cláusula 7 de la ISO 27005 se puede alinear con la cláusula 4 de la ISO 37001 referente a proporcionar una orientación con respecto a información relevante sobre la organización para el establecimiento de contexto de gestión de riesgos de seguridad de la información; es decir, comprender la organización y su contexto para poder establecer una gestión de riesgos. También se puede alinear con la cláusula 7.1 de la norma ISO 37001 referente a que la organización debe evaluar la disponibilidad de los recursos necesarios para:

- Realizar la evaluación de riesgos y establecer un plan de tratamiento de riesgos
- Definir e implementar políticas y procedimientos
- Controles del monitor
- Supervise el proceso de gestión de riesgos de seguridad de la información. (PECB, 2015)

Ya que la norma ISO 37001 establece que la organización determinará los recursos necesarios para el correcto cumplimiento del sistema de gestión.

La cláusula 8 de la ISO 27005 se puede alinear con la cláusula 4.5 de la ISO 37001, debido a que la evaluación de riesgos ayuda a identificar cuáles son los puntos vulnerables de la organización, cuáles son las partes en donde se pudiera generar un acto de soborno. La norma ISO 27005 establece que la identificación del riesgo determina qué puede suceder para causar un posible riesgo y obtener una idea de cómo, dónde y por qué podría ocurrir el riesgo. También se puede alinear con la cláusula 6.1 de la ISO 37001 debido a que las normas exigen, analizar y evaluar todas las situaciones potenciales de riesgo dentro de la organización, y atacarlas con el objetivo de minimizarlas. (PECB, 2015)

La cláusula 9 de la ISO 27005 se puede alinear con la cláusula 6 de la ISO 37001, en lo referente a la planeación; es decir, en el análisis de riesgos, el riesgo puede tratarse mediante la modificación de riesgos, la retención de riesgos, la prevención de riesgos y la distribución de riesgos, una selección basada en los resultados de la evaluación de riesgos y un análisis de costo-beneficio. (PECB, 2015)

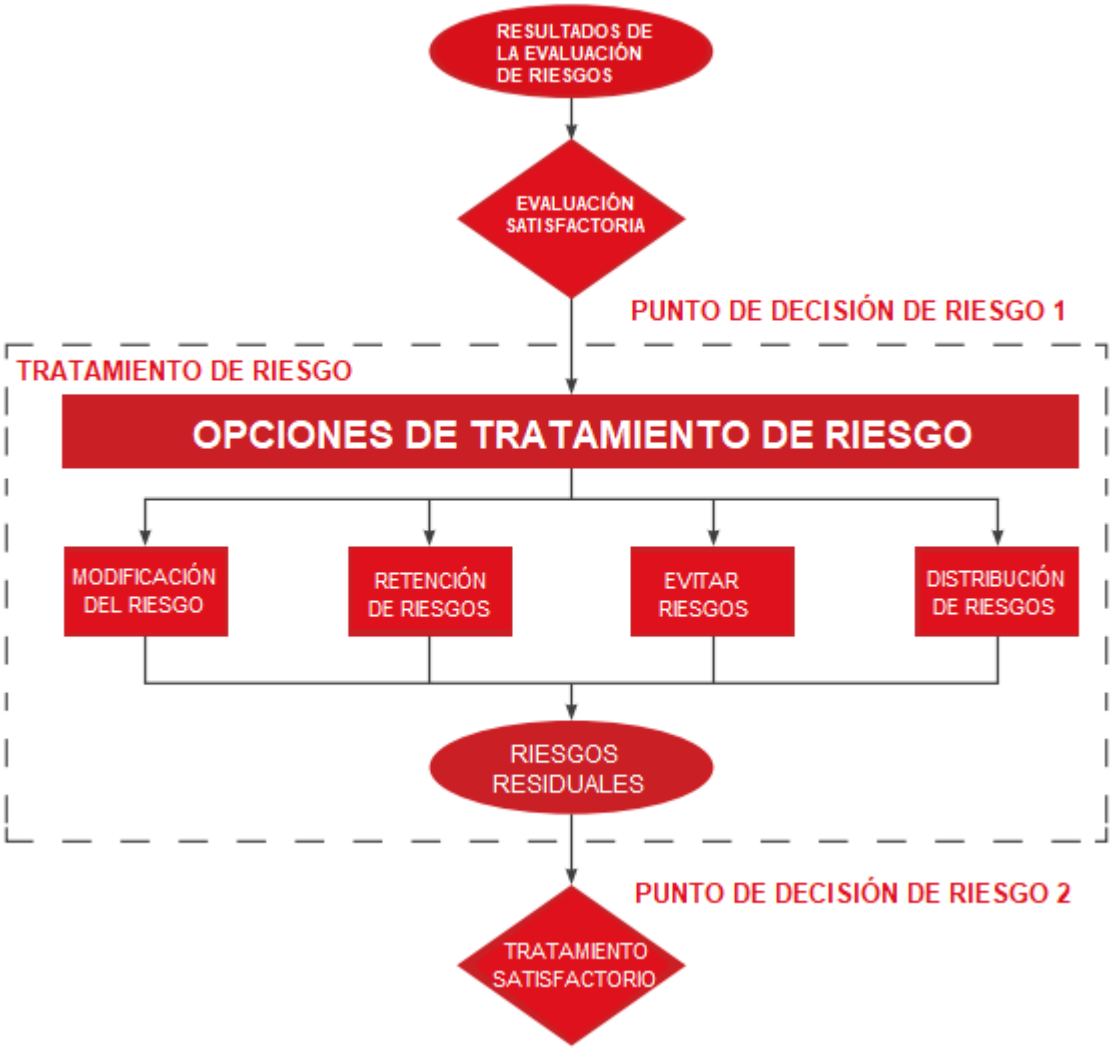

Ilustración 51. Tratamiento de Riesgo ISO 27005.
Fuente: PECB, 2015

La cláusula 10 de la ISO 27005 se puede alinear con la cláusula 9.3 de la ISO 37001, debido a que, en la organización, después del tratamiento de riesgo, la alta dirección necesita tomar

decisiones sobre la aceptación del riesgo residual que ha sido revisado. Como resultado, la organización enumera los riesgos aceptados con justificación.

La cláusula 11 de la ISO 27005 se puede alinear con la cláusula 7.4 de la ISO 37001 ya que las normas piden procesos de comunicación tanto internos como externos. los riesgos de seguridad de la información deben ser comunicados entre las personas responsables y las partes interesadas. La organización debe desarrollar un plan de comunicación de riesgos.

La cláusula 12 de la ISO 27005 se puede alinear con la cláusula 10 de la ISO 37001, debido a que la norma ISO 27005 exige un monitoreo y revisión continua de la gestión de riesgos de seguridad de la información. Además, la norma exige que las mejoras necesarias deben hacerse con el conocimiento de los gerentes apropiados. Por su lado, la cláusula de la norma ISO 37001 exige que la alta dirección debe asignar una función de cumplimiento, esta función de cumplimiento es una parte de la organización que está dedicada a verificar el buen funcionamiento del sistema de gestión y se encarga de encontrar las no conformidades y aplicar las acciones correctivas. En esta cláusula el proceso de mejora continua ayudará a ir mejorando el sistema de gestión. (PECB, 2015)

3.4 Alineación con ISO 31000

La norma ISO 31000 aporta principios y directrices genéricas que ayuda a las organizaciones a establecer, implementar, operar, mantener y mejorar continuamente el marco de gestión de riesgos.

La norma ISO 31000 está organizado en las siguientes cláusulas principales que son los 3 pilares básicos:

- Cláusula 3: Principios
- Cláusula 4: Marco de trabajo
- Cláusula 5: Proceso (PECB, 2015)

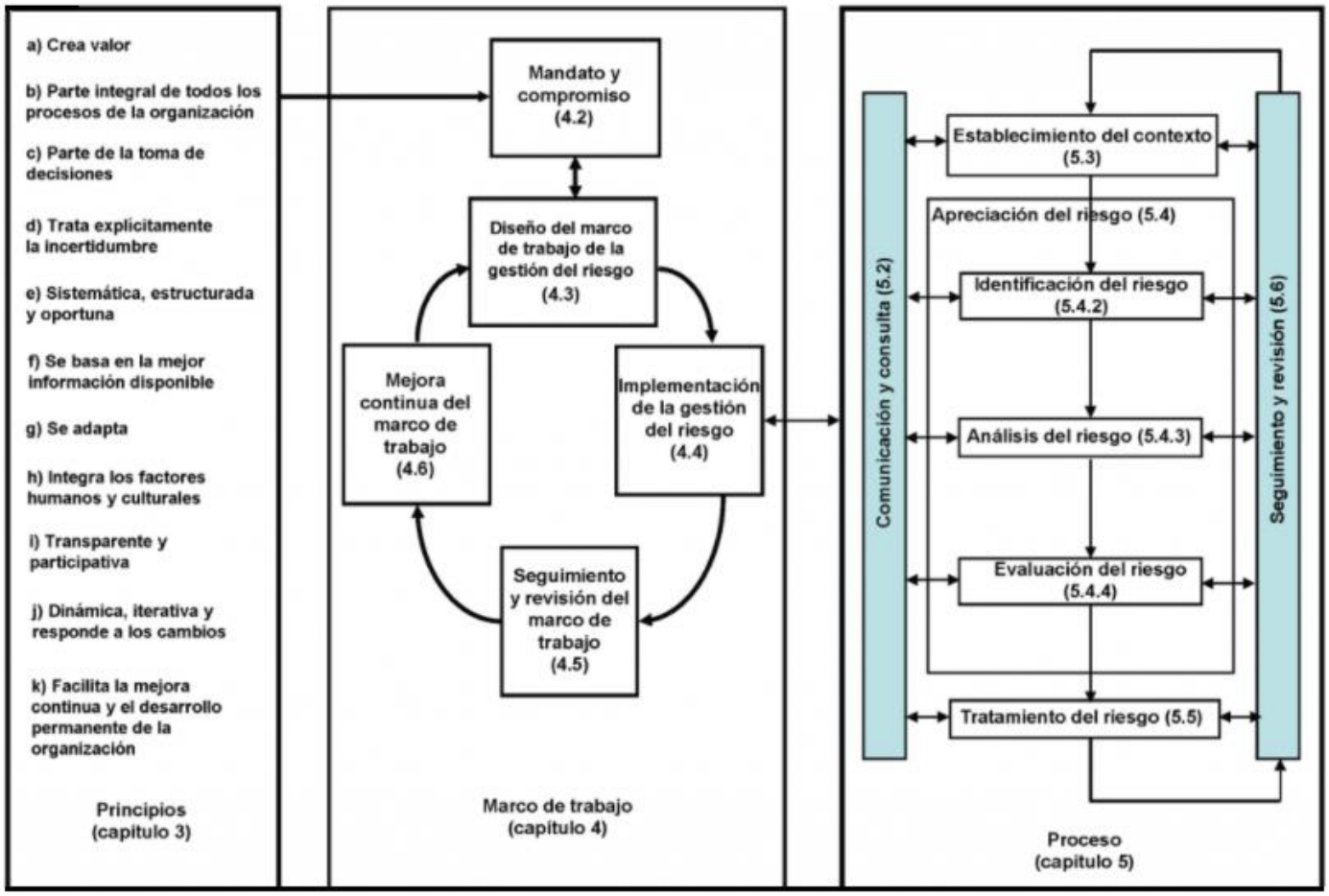

Ilustración 52. Cláusulas ISO 31000.
Fuente: https://www.isotools.org/2015/03/25/iso-31000-norma-gestionar-riesgos-organizacion/

Los principios de: la gestión de riesgos sea parte integral de todos los procesos organizacionales; la gestión del riesgo sea sistemática, estructurada y oportuna; la gestión de riesgos sea diseñada a medida; facilitar la mejora continua de la organización, de la cláusula 3 de la ISO 31000 se puede alinear con la cláusula 4 de la ISO 37001 debido a que la norma exige que se tiene que conocer la estructura de la organización y su contexto, determinar el alcance del sistema de gestión, establecer el sistema de gestión y la evaluación de los riesgos en el sistema.

Los principios de: crear y proteger el valor; la gestión del riesgo sea parte de la toma de decisiones; tratar la incertidumbre; la gestión de riesgos sea transparente e inclusiva, se pueden alinear con la cláusula 5 de la ISO 37001 debido a que la norma exige que los altos órganos de

gobierno de la organización se comprometan y tengan liderazgo para habilitar las vías necesarias con el fin de que el sistema de gestión se incorpore a la organización.

También porque la norma ISO 37001 exige designar las responsabilidades necesarias para poder cumplir con los principios mencionados. Los principios: La gestión de riesgos se basa en la mejor información disponible; La gestión de riesgos tiene en cuenta los factores humanos y culturales, se pueden alinear con la cláusula 7 de la ISO 37001 debido a que la norma exige que la organización determine los recursos necesarios para soportar las operaciones dentro del sistema de gestión. (PECB, 2015)

La cláusula 4: marco de trabajo de la ISO 31000 que exige:

Mandato y compromiso que se puede alinear con la cláusula 5.1 Liderazgo y compromiso de la ISO 37001 ya que la norma exige que la administración de la organización debe demostrar un compromiso sólido y sostenido con el sistema de gestión.

Diseño del marco para la gestión del riesgo que se puede alinear con la cláusula 4. Contexto de la organización de la ISO 37001 ya que la norma exige conocer la estructura de la organización. También con la cláusula 7 de la ISO 37001 ya que la norma exige la asignación de los recursos apropiados y establecer los mecanismos de comunicación tanto internos como externos adecuados para el buen funcionamiento del sistema de gestión.

Implementación de la gestión de riesgos que se puede alinear con la cláusula 8 de la ISO 37001 ya que se habla sobre la implementación del marco para la gestión del riesgo y el proceso de gestión de riesgos en la organización.

Monitoreo y revisión del marco que se puede alinear con la cláusula 9 de la ISO 37001 ya que se habla sobre medir el desempeño y el proceso de la gestión de riesgos, sobre revisar si son

adecuados el marco, la política y el plan de gestión de riesgos, así como la efectividad del marco de gestión de riesgos.

Mejora continua del marco que se puede alinear con la cláusula 10 de la ISO 37001 ya que se habla sobre la resolución de las no conformidades, sobre tomar decisiones para mejorar el marco, la política y el plan de gestión de riesgos. (PECB, 2015)

La cláusula 5: marco de trabajo de la ISO 31000 que habla sobre la comunicación y consulta que se puede alinear con la cláusula 7 de la ISO 37001 ya que las normas exigen la comunicación con las partes interesadas, tanto internas como externas. Este proceso debe darse durante todas las etapas del proceso de la gestión de riesgos.

Establecimiento del contexto que se puede alinear con la cláusula 4 de la ISO 37001 debido a que, al establecer el contexto, la organización reúne sus objetivos, define los parámetros externos e internos, establece el alcance y los criterios de riesgo para el proceso restante.

3.5 Conclusiones del capítulo 3

Al buscar una alineación de la norma ISO 37001 con la norma ISO 27001 no se encontraron mayores inconvenientes debido a los cambios de versión que ha adquirido dicha norma. Como ya se ha explicado, los cambios entre la ISO 27001:2005 y la ISO 27001:2013 han sido sustanciales para lograr una alineación de esta norma con otros estándares de sistemas de gestión, en este caso la alineación con la norma ISO 37001. En conclusión, la norma ISO 27001 es un estándar que más alineación ha presentado y más se apega al estándar ISO 37001.

Debido a que la ISO 27002 es simplemente una guía, un código de buenas prácticas en lugar de un estándar de certificación, ha sido más laborioso poder encontrar la alineación con cada cláusula de la norma ISO 37001, pero debido a que ISO / IEC 27002 es relevante para todo tipo de organizaciones, de todos los tamaños, ha sido necesario buscar un alineamiento con el estándar de

gestión Anti-soborno. La ventaja de que sea simplemente un código de práctica o guía, es que las organizaciones son libres de seleccionar e implementar otros controles o adoptar alternativas como mejor le parezca, por lo que, al momento de ser necesario se puede implementar algún tipo de control o serie de controles que ayuden a que la norma se alinee aún más con la norma ISO 37001.

Los estándares de la familia ISO27000 se encuentran alineados al riesgo, alentando a las organizaciones a evaluar los riesgos de seguridad de su información, es por esto que el estándar ISO 27005 fácilmente se pudo alinear con la norma ISO 37001; esto se debe a que dicho estándar también contempla el análisis de los riesgos de soborno para el correcto desempeño del sistema de gestión anti-soborno.

En conclusión, el estándar ISO 27005, al proporcionar directrices para la gestión de riesgos de seguridad de la información y al respaldar los conceptos generales especificados en ISO / IEC 27001, ayuda a la implementación satisfactoria de un sistema de gestión como es el estándar ISO 37001.

El marco genérico de ISO / IEC 27005 está estrechamente relacionado con el marco genérico sobre la gestión de riesgos de ISO 31000. También está alineado con los requisitos genéricos de gestión de riesgos que se presentan en ISO 31000. Por esto el estándar ISO 31000 con su versión 2009, fácilmente se puede alinear con la norma ISO 37001, debido a que las cláusulas del estándar ISO 37001 se han alineado a los principios, al marco de trabajo y al proceso que exige la norma ISO 31000.

CAPÍTULO 4 – Alineación de ISO 37001 con los marcos de referencia.

4.1 Alineación con COBIT 5

Uno de los principios directrices en COBIT 5 es la distinción entre la gestión y el gobierno. Teniendo en cuenta los procesos para el gobierno y la gestión, la diferencia entre los dos tipos de procesos es:

- Procesos de Gobierno: Se ocupan de optimizar riesgos y recursos, los objetivos de gobierno de las partes interesadas, proporcionar valor, incluir prácticas y actividades enfocadas a evaluar opciones estratégicas, proporcionando dirección a la TI y supervisando sus resultados (Evaluación, Dirección y Supervisión (EDM)).
- Procesos de Gestión: Se alinean con la definición de gestión. Abarcan las áreas de responsabilidad de Planificación, Construcción, Ejecución y Supervisión (PBRM) de las TI de la empresa. (ISACA, 2012)

Para el presente análisis se va a enfocar en los procesos de gobierno ya que el tema de gestión de soborno está enfocado no a la parte de gestión sino a la parte de gobierno que son los procesos de Evaluar, Orientar y Supervisar.

Ilustración 53. Procesos de Gobierno de TI Empresarial.
Fuente: ISACA, 2012

Los procesos tienen partes interesadas internas y externas, con sus propios roles; estas partes y sus niveles de responsabilidad se encuentran detallados en matrices que muestran:

- quién realiza (R);
- quién es responsable (A);

- a quién se consulta (C);
- a quién se informa (I). (ISACA, 2012)

Para el proceso EDM01 - Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno se tiene lo siguiente:

EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	**Área: Gobierno** **Dominio: Evaluar, Orientar y Supervisar**
Descripción del Proceso Analiza y articula los requerimientos para el gobierno de TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	
Declaración del Propósito del Proceso Proporcionar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa. Para garantizar que las decisiones relativas a TI se han adoptado en línea con las estrategias y objetivos de la empresa, garantizando la supervisión de los procesos de manera efectiva y transparentemente, el cumplimiento con los requerimientos regulatorios y legales y que se han alcanzado los requerimientos de gobierno de los miembros del Consejo de Administración.	

Ilustración 54. Proceso EDM01.
Fuente: ISACA, 2012

MATRIZ RACI EDM01

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero(CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Director de Recursos Humanos	Cumplimiento Normativo	Auditoría	Director de Informática (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Director de Privacidad de la Información
EDM01.01 Evaluar el sistema de gobierno.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Orientar el sistema de gobierno	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Supervisar el sistema de gobierno.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

Ilustración 55. Matriz RACI de EDM01.
Fuente: ISACA, 2012

En lo referente a EDM01.01 - Evaluar el sistema de gobierno que trata sobre: Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar el alcance de los requerimientos y realizar una estimación del diseño del gobierno de TI de la empresa actual y

futura; Se puede alinear con la cláusula 4 de la norma ISO 37001 debido a que la norma hace referencia a la Comprensión de la organización y de su contexto, Comprensión de las necesidades y expectativas de las partes interesadas y Determinación del alcance del sistema de gestión anti-soborno. EDM01.02 - Orientar el sistema de gobierno que trata sobre: Informar a los líderes y obtener el apoyo, la aceptación y su compromiso, guiar las estructuras, procesos y prácticas para el gobierno de TI, determinar la información necesaria para una toma de decisiones informadas; Se puede alinear con la cláusula 5 de la ISO 37001 debido a que la norma hace referencia al liderazgo y compromiso de la unidad de gobierno y la alta dirección. La norma también hace referencia a la política anti-soborno, los roles, responsabilidades y autoridades en la organización, la función en el cumplimiento y la delegación de la toma de decisiones. (ISACA, 2012)

EDM01.03 - Supervisar el sistema de gobierno que trata sobre: Analizar si el sistema de gobierno y los mecanismos implementados están operando de forma efectiva y proporcionan una supervisión apropiada de TI, supervisar la ejecución y la efectividad del gobierno de TI de la empresa; Se puede alinear con la cláusula 9 de la ISO 37001 debido a que la norma en esta sección propone controles que permiten evaluar el desempeño en cuanto a la gestión, explica las actividades que realiza la auditoría interna, la revisión por la alta dirección y la revisión por la función de cumplimiento. (ISACA, 2012)

Para el proceso EDM02 - Asegurar la Entrega de Beneficios se tiene lo siguiente:

EDM02 Asegurar la Entrega de Beneficios	**Área: Gobierno** **Dominio: Evaluar, Orientar y Supervisar**
Descripción del Proceso Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.	
Declaración del Propósito del Proceso Asegurar un valor óptimo de las iniciativas de TI, servicios y activos disponibles; una entrega coste eficiente de los servicios y soluciones y una visión confiable y precisa de los costes y de los beneficios probables de manera que las necesidades del negocio sean soportadas efectiva y eficientemente.	

Ilustración 56. Proceso EDM02.
Fuente: ISACA, 2012

MATRIZ RACI EDM02																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
EDM02.01 Evaluar la optimización del valor.	A	R	R	C	R		R			C	C		C	C	C	C	C	R	C	C	C				
EDM02.02 Orientar la optimización del valor.	A	R	R	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I
EDM02.03 Supervisar la optimización del valor.	A	R	R	C	R		R			R	C	C	C	C	C	C	C	R	C	C	C					

Ilustración 57. Matriz RACI de EDM02.
Fuente: ISACA, 2012

En lo referente a EDM02.01 - Evaluar la optimización de valor que trata sobre: Evaluar continuamente los activos del portafolio de TI, servicios y las inversiones para determinar la probabilidad de lograr los objetivos de la empresa y aportar valor a un coste razonable; se puede alinear con la cláusula 9 de la ISO 37001 debido a que la norma pide evaluar todas las medidas que se hayan adoptado para llevar a cabo la implementación del sistema de gestión y así determinar la probabilidad de alcanzar los objetivos de la empresa. EDM02.02 - Orientar la optimización del valor que trata sobre: Orientar las prácticas y los principios de gestión de valor para posibilitar la realización del valor óptimo de las inversiones TI; Se puede alinear con la cláusula 5 de la ISO 37001 debido a que la norma hace referencia al liderazgo y compromiso de la unidad de gobierno y la alta dirección para la correcta orientación del sistema de gestión. (ISACA, 2012)

EDM02.03 - Supervisar la optimización de valor que trata sobre: Identificar los problemas significativos y considerar las acciones correctivas; supervisar los indicadores clave y sus métricas para calcular el valor y los beneficios previstos de los servicios e inversiones TI generados por el

negocio. Se puede alinear con la cláusula 9 de la ISO 37001 debido a que la norma en esta sección propone una supervisión, medición y controles por la alta dirección.

Para el proceso EDM03 - Asegurar la Optimización del Riesgo se tiene lo siguiente:

EDM03 Asegurar la Optimización del Riesgo	**Área: Gobierno** **Dominio: Evaluar, Orientar y Supervisar**
Descripción del Proceso Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	
Declaración del Propósito del Proceso Asegurar que los riesgos relacionados con TI de la empresa no exceden ni el apetito ni la toleración de riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo.	

Ilustración 58. Proceso EDM03.
Fuente: ISACA, 2012

EDM03 RACI Chart

Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la información
EDM03.01 Evaluar la gestión de riesgos.	A	R	C	C	R	C	R			I	R	C		I	C	C	C	R	C							C
EDM03.02 Orientar la gestión de riesgos.	A	R	C	C	R	C	R	I	I	I	R	I	I	I	C	C	C	R	C	I	I	I	I	I	I	I
EDM03.03 Supervisar la gestión de riesgos.	A	R	C	C	R	C	R	I	I	I	R	R	I	I	C	C	C	R	C	I	I	I	I	I	I	C

Ilustración 59. Matriz RACI de EDM03.
Fuente: ISACA, 2012

En lo referente a EDM03.01 - Evaluar la gestión de riesgos que trata sobre: Evaluar continuamente el efecto del riesgo sobre el uso de las TI en la empresa; Se puede alinear con la cláusula 9 de la ISO 37001 debido a que se exige una evaluación continua por parte de los entes respectivos en la organización referente a los riesgos sobre el uso de las TI. EDM03.02 - Orientar la gestión de riesgos que trata sobre: Orientar la implantación de prácticas de gestión de riesgos

para proporcionar una seguridad razonable con el fin de asegurar que el riesgo TI actual no excede el apetito de riesgo del Consejo; Se pueden alinear con la cláusula 5 de la ISO 37001 debido a que la norma hace referencia al liderazgo y compromiso de los entes de gobierno, con el fin de que dichos entes se comprometan y ayuden con el establecimiento de prácticas de gestión de riesgos.

EDM03.03 - Supervisar la gestión de riesgos que trata sobre: Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo los problemas serán identificados, seguidos e informados para su correcta resolución. Se puede alinear con la cláusula 9 de la ISO 37001 debido a que la norma en esta sección propone controles que permiten evaluar el desempeño en cuanto a la gestión, Explica las actividades que realiza la auditoría interna, la revisión por la alta dirección y la revisión por la función de cumplimiento. (ISACA, 2012)

Para el proceso EDM04 - Asegurar la Optimización de Recursos se tiene lo siguiente:

EDM04 Asegurar la Optimización de Recursos	**Área: Gobierno** **Dominio: Evaluar, Orientar y Supervisar**
Descripción del Proceso Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	
Declaración del Propósito del Proceso Asegurar que las necesidades de recursos de la empresa son cubiertas de un modo óptimo, que el coste TI es optimizado y que con ello se incrementa la probabilidad de la obtención de beneficios y la preparación para cambios futuros.	

Ilustración 60. Proceso EDM04.
Fuente: ISACA, 2012

Matriz RACI EDM04																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Jefe de Recursos Humanos	Cumplimiento Normativo (Compliance)	Auditoría	Director de Informática/Sistemas (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio (Service Manager)	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Gestor de Privacidad de la Información
EDM04.01 Evaluar la gestión de recursos.	A	R	C	C	R		R			I	C	C	C	C	C	C	C	R	C	C	C					
EDM04.02 Orientar la gestión de recursos.	A	R	C	C	R	I	R	I	I	I	I	I	I	I	I	I	I	R	C	I	I	I	I	I	I	I
EDM04.03 Supervisar la gestión de recursos.	A	R	C	C	R	I	R	I	I	I	C	C	C	C	C	C	C	R	C	C	C	I	I	I	I	I

Ilustración 61. Matriz RACI de EDM04.
Fuente: ISACA, 2012

En lo referente a EDM04.01 - Evaluar la gestión de recursos que trata sobre: Evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, la asignación de recursos para cumplir de manera óptima con las necesidades de la empresa; Se puede alinear con la cláusula 7 de la ISO 37001 debido a que la norma hace referencia a la asignación de los recursos necesarios para el correcto funcionamiento del sistema de gestión. EDM04.02 Orientar la gestión de recursos que trata sobre: Garantizar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI. Se puede alinear con la cláusula 5 de la ISO 37001 debido a que la norma hace referencia al liderazgo y compromiso de la unidad de gobierno y la alta dirección para adoptar principios de gestión de recursos con el fin de usar óptimamente los recursos TI. (ISACA, 2012)

EDM04.03 - Supervisar la gestión de recursos que trata sobre: Supervisar los objetivos y las métricas clave de los procesos de gestión de recursos y establecer cómo los problemas serán

identificados, seguidos e informados para su correcta resolución. Se puede alinear con la cláusula 9 de la ISO 37001 debido a que la norma en esta sección propone controles que permiten evaluar el desempeño en cuanto a la gestión, Explica las actividades que realiza la auditoría interna, la revisión por la alta dirección y la revisión por la función de cumplimiento. (ISACA, 2012)

Para el proceso EDM05 - Asegurar la Transparencia hacia las Partes Interesadas se tiene lo siguiente:

EDM05 Asegurar la Transparencia hacia las Partes Interesadas	**Área: Gobierno** **Dominio: Evaluar, Orientar y Supervisar**
Descripción del Proceso Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.	
Declaración del Propósito del Proceso Asegurar que la comunicación con las partes interesadas sea efectiva y oportuna y que se ha establecido una base para la elaboración de informes con el fin de aumentar el desempeño, identificar áreas susceptibles de mejora y confirmar que las estrategias y los objetivos relacionados con TI concuerdan con la estrategia corporativa.	

Ilustración 62. Proceso EDM05.
Fuente: ISACA, 2012

Matriz RACI EDM05

Práctica Clave de Gobierno	Consejo de administración	Director General Ejecutivo (CEO)	Director General Financiero (CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Dueños del proceso de negocio	Comité Ejecutivo de estrategia	Comité directivo (de programas/proyectos)	Oficina de Gestión de Proyectos	Oficina de gestión de valor	Director de gestión del riesgo	Director de seguridad de la información	Comité de arquitectura	Comité de riesgo empresarial	Jefe de Recursos Humanos	Conformidad	Auditoría	Director de informática (CIO)	Arquitecto jefe	Jefe de desarrollo	Jefe de operaciones de TI	Jefe de administración de TI	Administrador de servicio	Administrador de seguridad de la información	Administrador de continuidad del negocio	Director de privacidad
EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas.	A	R	C	C	C	I										C	C	R	I			I				
EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.	A	R	C	C	C	I										C	C	R	I			I				
EDM05.03 Supervisar la comunicación con las partes interesadas.	A	R	C	C	C	I										C	C	R	I			I				

Ilustración 63. Matriz RACI de EDM05.
Fuente: ISACA, 2012

En lo referente a EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas que trata sobre: Examinar continuamente los requerimientos actual y futura de comunicación con las partes interesadas y de la elaboración de informes; Se puede alinear con la cláusula 4 de la ISO 37001 debido a que la norma hace referencia a la comprensión de las necesidades y expectativas de las partes interesadas; también con la cláusula 7 para establecer los principios de comunicación. EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes que trata sobre: Garantizar una comunicación y elaboración de informes eficaces, incluyendo mecanismos que aseguren tanto calidad como completitud de la información, crear estrategias de comunicación con las partes interesadas; Se puede alinear con la cláusula 5 de la ISO 37001 debido a que la norma hace referencia al liderazgo y compromiso de la unidad de gobierno y la alta dirección para crear estrategias de comunicación con las partes interesadas y establecer una comunicación e informes eficaces. (ISACA, 2012)

EDM05.03 Supervisar la comunicación con las partes interesadas que trata sobre: Supervisar la eficaz comunicación con las partes interesadas. Evaluar los mecanismos y determinar si se están cumpliendo los requisitos de los diferentes interesados; Se puede alinear con la cláusula 9 de la ISO 37001 debido a que la norma en esta sección propone controles que permiten evaluar el desempeño en cuanto a la gestión, Explica las actividades que realiza la auditoría interna, la revisión por la alta dirección y la revisión por la función de cumplimiento. (ISACA, 2012)

4.2 Alineación entre COBIT 5 y COSO III

Para la presente alineación se han tomado en cuenta únicamente los procesos de gobierno de COBIT 5 que son 5, debido a que el presente trabajo va enfocado al gobierno TI en los marcos de gobierno COBIT 5 y COSO III.

Tabla 9:
Integración de COBIT 5 y COSO III

COSO Principio y descripción		Proceso de COBIT Referencia	Relación con el Principio COSO
Entorno de Control			
1	La organización demuestra compromiso con la integridad y los valores éticos.	EDM01	El proceso EDM01 de COBIT 5 Garantiza la configuración del marco de gobierno y mantenimiento.
2	El consejo administrativo ejerce responsabilidad de supervisión.	EDM01-05	Los cinco procesos de gobierno de COBIT (EDM01 a EDM05) refuerzan esta separación en su guía de gráficos RACI.
3	Establecer la estructura, responsabilidad y autoridad.	EDM01	EDM01 Asegurar la configuración y el mantenimiento del marco de gobierno con respecto a los requisitos de gobierno empresarial.
4	Demostrar compromiso para la competencia profesional.		Se relaciona con los procesos de gestión APO01 y APO07.
5	Reforzar la responsabilidad. (AUDITOOL, 2016)	Todos los procesos de COBIT 5	El habilitador de procesos COBIT 5 y el soporte de gráficos RACI en los 37 procesos son particularmente relevantes para el contexto de la responsabilidad individual.
Evaluación de riesgos			
6	Especificar objetivos relevantes para identificar y evaluar riesgos asociados.	Todos los procesos de COBIT 5	La guía para los 37 procesos de COBIT 5 incluye las metas del proceso (objetivos).
7	Identifica y analiza los riesgos asociados a los objetivos.	EDM03	EDM03 - Garantizar la optimización del riesgo incluye las prácticas y actividades que se requieren para gobernar y administrar el riesgo de manera efectiva, incluida su identificación, análisis y gestión.
8	Considerar el riesgo de fraude.	EDM01	EDM01 apoya los objetivos de cultura, ética y comportamiento, incluido el enfoque de fraude empresarial.
9	Identificar y analizar cambios significativos. (AUDITOOL, 2016)		Se relaciona con los procesos de gestión APO01, BAI02, BAI05, BAI06 y BAI07
Actividades de control			
10	Selecciona y desarrolla actividades de control que ayudan a mitigar los riesgos.	Todos los procesos de COBIT 5	La guía del facilitador de procesos COBIT 5 para los 37 procesos COBIT 5 apoya a las empresas en su selección y desarrollo de actividades de control y otros arreglos, particularmente con las prácticas y actividades a considerar para procesos empresariales relacionados con TI.

11	La organización selecciona y desarrolla actividades de control generales sobre la tecnología para apoyar el logro de los objetivos.	Todos los procesos de COBIT 5	Las actividades de control pueden ser actividades de proceso dentro de los 37 procesos COBIT 5. En particular, el proceso COBIT 5 DSS06 Administrar los controles del proceso empresarial.
12	La organización despliega actividades de control a través de políticas que establecen lo que se espera y procedimientos que ponen las políticas en acción.		Se relaciona con el proceso APO01
Información y comunicación			
13	La organización despliega actividades de control a través de políticas y procedimientos. (AUDITOOL, 2016)	Todos los procesos de COBIT 5	La guía para los 37 procesos de COBIT 5 incluye entradas y salidas que son la comunicación de información entre y desde y hacia la empresa.
14	Comunica internamente información esencial.	Todos los procesos de COBIT 5	Los objetivos se proporcionan para los 37 procesos COBIT 5. La necesidad de comunicar información con las partes interesadas como parte del diseño y ejecución del proceso empresarial, para apoyar el logro del proceso y los objetivos comerciales relacionados, se aborda en los cuadros RACI, con las responsabilidades de "consultar" e "informar", y sugerencias de salida que soportan la guía de proceso para los 37 procesos COBIT 5.
15	Comunica externamente asuntos trascendentes que afecten al control interno. (AUDITOOL, 2016)	EDM05	EDM05 asegura que la comunicación a las partes interesadas es efectiva y oportuna y se establece una base confiable y consistente para informar.
Actividades de monitoreo			
16	Conduce evaluaciones continuas y/o independientes.		Se relaciona con el proceso MEA02
17	Evalúa y comunica oportunamente las deficiencias a los responsables. (AUDITOOL, 2016)	EDM05	EDM05 incluye prácticas y actividades para evaluar, dirigir y monitorear los requisitos de informes y comunicación de los interesados, incluidos los relacionados con las deficiencias de control, a la alta gerencia y al consejo, según corresponda.

Fuente: (ISACA, 2014)

Para analizar la relación que tiene COBIT 5 con COSO III en los procesos de gestión revisar:

ISACA. (2014). *Relating the COSO Internal Control—Integrated Framework and COBIT.*

4.3 Alineación de ISO 37001 con COSO III

Con la ayuda de la alineación entre COBIT 5 y COSO 3 se lograron identificar los principios enfocados al gobierno TI. (ISACA, 2014)

La versión de COSO 2013 está dividido en componentes que ya han sido establecidos en el marco anterior con 17 principios básicos que toda organización debe implementar y 87 puntos de interés. (AUDITOOL, 2016)

Ambiente de control

- Principio 1: La organización demuestra compromiso con la integridad y los valores éticos
- Principio 2: El consejo administrativo ejerce responsabilidad de supervisión
- Principio 3: Establecer estructura, autoridad, y responsabilidad
- Principio 4: Demostrar compromiso para la competencia profesional
- Principio 5: Reforzar la responsabilidad. (AUDITOOL, 2016)

Evaluación de riesgos

- Principio 6: Especificar objetivos relevantes para identificar y evaluar riesgos asociados
- Principio 7: Identifica y analiza los riesgos asociados a los objetivos
- Principio 8: Evalúa el riesgo de fraude
- Principio 9: Identificar y analizar cambios significativos. (AUDITOOL, 2016)

Actividades de control

- Principio 10: Selecciona y desarrolla actividades de control que ayudan a mitigar los riesgos
- Principio 11: La organización selecciona y desarrolla actividades de control generales sobre la tecnología para apoyar el logro de los objetivos.

- Principio 12: La organización despliega actividades de control a través de políticas y procedimientos. (AUDITOOL, 2016)

Información y Comunicación

- Principio 13: Usa información de calidad
- Principio 14: Comunica internamente información esencial
- Principio 15: Comunica externamente asuntos trascendentes que afecten al control interno. (AUDITOOL, 2016)

Actividades de Monitoreo

- Principio 16: Conduce evaluaciones continuas y/o independientes
- Principio 17: Evalúa y comunica oportunamente las deficiencias a los responsables. (AUDITOOL, 2016)

El Principio 1: Demostrar compromiso con la integridad y los valores éticos se lo puede ligar a la cláusula 4 y cláusula 5 de la norma ISO 37001 ya que se habla de demostrar compromiso con la integridad, por lo que se puede hablar también de un compromiso en contra del soborno. Comprender el contexto de la organización y exigir liderazgo y compromiso por parte de la alta administración de la organización.

El Principio 2: Ejercer responsabilidad de supervisión; es decir, quien va a supervisar, en el caso del sistema de gestión serán los entes de control organizacional, en el caso de Tecnologías de la Información será el Comité de Riesgos de Tecnologías de la Información que se encuentra establecido en la cláusula 5 de la ISO 37001.

El Principio 3: Establecer estructura, autoridad, y responsabilidad se la puede alinear a la cláusula 5 de la ISO 37001 debido a que se habla de roles, responsabilidades y autoridades en la organización.

El Principio 4: Demuestra compromiso para la competencia no se alinea con procesos de gobierno sino con procesos de gestión en COBIT 5.

El Principio 5: Hace cumplir con la responsabilidad se alinea con la cláusula 5 de la ISO 37001 debido a que se habla de roles, responsabilidades y la función de cumplimiento, y de la cláusula 9 que habla de evaluación del desempeño para verificar el cumplimiento de las responsabilidades en la organización.

El Principio 6: Especificar objetivos relevantes se puede alinear con la cláusula 5 de la ISO 37001 para establecer la política anti-soborno, la cláusula 6 para establecer los objetivos y la planificación para lograrlos y la cláusula 9 para monitorear, analizar y evaluar los objetivos implantados en la organización.

El Principio 7: Identificar y analizar los riesgos se puede alinear con la cláusula 5 de la ISO 37001 en la que el Comité de Riesgo de Tecnología que identificara los riesgos que afecten el logro de los objetivos, la cláusula 6 que especifica las acciones para tratar riesgos y oportunidades y la cláusula 9 para dar el seguimiento, medición, análisis y evaluación de los mismos.

El Principio 8: Evalúa el riesgo de fraude se puede alinear con la cláusula 5 de la ISO 37001 ya que existe un compromiso por parte de la alta gerencia para combatir el fraude, un compromiso para apoyar los objetivos de cultura, ética y comportamiento. También la cláusula 6 que especifica las acciones para tratar riesgos y oportunidades.

El Principio 9: Identifica y analiza cambios importantes no se alinea con procesos de gobierno sino con procesos de gestión en COBIT 5.

El Principio 10: Selecciona y desarrolla actividades de control se puede alinear con la cláusula 5 de la ISO 37001 ya que debe existir liderazgo y compromiso para dar el visto bueno a las actividades de control, la cláusula 6 que ayuda a identificar las acciones para tratar los riesgos y la

cláusula 9 que exige la revisión por los entes de la organización para la aprobación de las actividades de control.

El Principio 11: Selecciona y desarrolla controles generales sobre tecnología se puede alinear con la cláusula 5 de la ISO 37001 ya que debe existir liderazgo y compromiso para dar el visto bueno a sobre los controles y la cláusula 9 que exige la revisión por los entes de la organización para la aprobación de los controles.

El Principio 12: Se implementa a través de políticas y procedimientos no se alinea con procesos de gobierno sino con procesos de gestión en COBIT 5.

El Principio 13: Usa información Relevante se puede alinear con la cláusula 5 de la ISO 37001 ya que debe existir liderazgo y compromiso para generar y utilizar información de calidad y relevante y la cláusula 9 que exige la revisión por los entes de gobierno para verificar la idoneidad de la información utilizada.

El Principio 14: Comunica internamente se puede alinear con la cláusula 5 de la ISO 37001 ya que debe existir compromiso por la alta gerencia para poder comunicar internamente la información, la cláusula 7 que exige procesos de comunicación internos y la cláusula 9 que exige análisis y evaluación de los procesos de comunicación.

El Principio 15: Comunica externamente se puede alinear con la cláusula 5 de la ISO 37001 ya que debe existir compromiso por la alta gerencia para poder comunicar con partes externas la información, la cláusula 7 que exige procesos de comunicación externos y la cláusula 9 que exige análisis y evaluación de los procesos de comunicación.

El Principio 16: Conduce evaluaciones continuas y/o independientes no se alinea con procesos de gobierno sino con procesos de gestión en COBIT 5.

El Principio 17: Evalúa y comunica deficiencias se puede alinear con la cláusula 7 que exige procesos de comunicación y la cláusula 9 de la ISO 37001 ya que exige evaluación de las deficiencias en el control interno por parte de la alta dirección y el consejo de administración y la comunicación oportuna a las partes responsables para tomar las medidas necesarias.

4.4 Conclusiones del capítulo 4

Debido a que el tema de gestión de soborno está enfocado a la parte de gobierno y no a la parte de gestión, necesaria y únicamente se ha trabajado sobre procesos de Evaluar, Orientar y Supervisar del marco de gobierno COBIT 5. Por esto se determinó que los dominios de Evaluar, Orientar y Supervisar en el área de gobierno se alinean con las cláusulas 5 y 9 del estándar ISO 37001.

En conclusión, los dominios de Evaluar y Orientar se alinean con la cláusula 5 de la norma ISO 37001 debido a que se tratan de temas como el Liderazgo y compromiso de los altos mandos de gobierno en una organización y otros temas como la política, roles y responsabilidades, entre otros. El dominio de Supervisar se alinea con la cláusula 9 de la norma ISO 37001 debido a que se tratan de temas como el seguimiento, medición, análisis y evaluación en el sistema de gestión y otros temas como auditoria interna y la revisión por entes de autoridad dentro la organización.

Para encontrar el alineamiento con el marco de gobierno COSO III, ha sido necesario buscar la relación con el marco de gobierno COBIT 5 debido a que en lo referente a marcos de gobierno se ha visto necesario encontrar un lineamiento solo con procesos de gobierno y no de gestión. Se concluye que el marco de referencia COBIT 5 en los procesos de gobierno, se encuentra alineado con 13 de los 17 principios de COSO III por lo que ha sido de gran ayuda para la evaluación de relación entre COSO III y el estándar ISO 37001.

Se llego a la conclusión de que las cláusulas que mayormente se alinean con COSO III al igual que con el marco de referencia COBIT 5, han sido las de Liderazgo cláusula 5, Apoyo cláusula 7 y Evaluación del desempeño cláusula 9.

CAPÍTULO 5 – Cuadro comparativo entre ISO 37001 y los marcos de referencia

En el capítulo anterior se analizó la alineación entre la ISO 37001 y los marcos de gobierno llegando a la conclusión de que la mayoría de los principios de COSO III se alinean con los procesos de COBIT 5 en el área de gobierno. Esta alineación en el área de procesos de gobierno ayudará para la respectiva alineación con las cláusulas de la ISO 37001 y así entender cómo se puede alinear los Marcos de Gobierno con la norma ISO 37001.

Dicha alineación se colocará en un cuadro para poder entender de mejor manera como se encuentran relacionados los principios de COSO III, los procesos de Gobierno de COBIT 5 y las cláusulas de la norma ISO 37001.

5.1 Cuadro comparativo entre la ISO 37001 y los marcos

Para la realización del cuadro comparativo se utilizarán las siguientes referencias de los procesos de Gobierno en COBIT5:

Tabla 10:
Procesos de Gobierno de TI.

Procesos de Gobierno de TI Empresarial
Evaluar, Orientar y Supervisar
EDM01 - Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.
EDM02 - Asegurar la Entrega de Beneficios.
EDM03 - Asegurar la Optimización del Riesgo.
EDM04 - Asegurar la Optimización de los Recursos.
EDM05 - Asegurar la Transparencia hacia las Partes Interesadas.

Fuente: (ISACA, 2012)

De igual manera se utilizarán las siguientes cláusulas:

Tabla 11:
Cláusulas relacionadas con los Marcos de Referencia.

Cláusulas ISO 37001
Cláusula 4: Contexto de la organización.
Cláusula 5: Liderazgo.
Cláusula 6: Planificación.
Cláusula 7: Apoyo.
Cláusula 9: Evaluación del desempeño.

Fuente: Elaborado por el autor

Quedando la relación entre COSO III, COBIT 5 y el estándar ISO 37001 únicamente en el área de procesos de gobierno de la siguiente manera:

Tabla 12:
Relación entre los Marcos de Referencia e ISO 37001 en los procesos de gobierno.

GOBIERNO			Gestión
COSO III		COBIT 5	ISO 37001
Entorno de Control	**Principio 1**: La organización demuestra compromiso con la integridad y los valores éticos.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 9: Evaluación del desempeño.
	Principio 2: El consejo administrativo ejerce responsabilidad de supervisión.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno. EDM02: Asegurar la Entrega de Beneficios. EDM03: Asegurar la Optimización del Riesgo. EDM04: Asegurar la Optimización de los Recursos. EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.
	Principio 3: Establecer la estructura, responsabilidad y autoridad.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 9: Evaluación del desempeño.

	Principio 5: Reforzar la responsabilidad.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno. EDM02: Asegurar la Entrega de Beneficios. EDM03: Asegurar la Optimización del Riesgo. EDM04: Asegurar la Optimización de los Recursos. EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.
Evaluación de riesgos	**Principio 6**: Especificar objetivos relevantes para identificar y evaluar riesgos asociados.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno. EDM02: Asegurar la Entrega de Beneficios. EDM03: Asegurar la Optimización del Riesgo. EDM04: Asegurar la Optimización de los Recursos. EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.
	Principio 7: Identifica y analiza los riesgos asociados a los objetivos.	EDM03: Asegurar la Optimización del Riesgo.	Cláusula 5: Liderazgo. Cláusula 6: Planificación. Cláusula 9: Evaluación del desempeño.
	Principio 8: Considerar el riesgo de fraude.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 6: Planificación. Cláusula 9: Evaluación del desempeño.
Actividades de control	**Principio 10**: Selecciona y desarrolla actividades de control que ayudan a mitigar los riesgos.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno. EDM02: Asegurar la Entrega de Beneficios. EDM03: Asegurar la Optimización del Riesgo. EDM04: Asegurar la Optimización de los Recursos. EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.

	Principio 11: La organización selecciona y desarrolla actividades de control generales sobre la tecnología para apoyar el logro de los objetivos.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno. EDM02: Asegurar la Entrega de Beneficios. EDM03: Asegurar la Optimización del Riesgo. EDM04: Asegurar la Optimización de los Recursos. EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.
Información y comunicación	**Principio 13**: Usa información de calidad.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno. EDM02: Asegurar la Entrega de Beneficios. EDM03: Asegurar la Optimización del Riesgo. EDM04: Asegurar la Optimización de los Recursos. EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.
	Principio 14: Comunica internamente información esencial.	EDM01: Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno. EDM02: Asegurar la Entrega de Beneficios. EDM03: Asegurar la Optimización del Riesgo. EDM04: Asegurar la Optimización de los Recursos. EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.
	Principio 15: Comunica externamente asuntos trascendentes que afecten al control interno.	EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.
Actividades de monitoreo	**Principio 17**: Evalúa y comunica oportunamente las deficiencias a los responsables. (AUDITOOL, 2016)	EDM05: Asegurar la Transparencia hacia las Partes Interesadas.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 7: Apoyo. Cláusula 9: Evaluación del desempeño.

Fuente: Elaborado por el autor

Los principios restantes se relacionan únicamente con procesos del área de gestión de COBIT 5 y son los siguientes:

Tabla 13:
Relación entre los Marcos de Referencia e ISO 37001 en los procesos de gestión.

Gestión			
COSO III		COBIT 5	ISO 37001
Entorno de Control	**Principio 4**: Demostrar compromiso para la competencia profesional.	APO01: Gestionar el Marco de Gestión de TI. APO07: Gestionar los Recursos Humanos.	Cláusula 5: Liderazgo. Cláusula 7: Apoyo.
Evaluación de riesgos	**Principio 9**: Identificar y analizar cambios significativos.	APO01: Gestionar el Marco de Gestión de TI. BAI02: Gestionar la Definición de Requisitos. BAI05: Gestionar la Introducción de Cambios Organizativos. BAI06: Gestionar los Cambios. BAI07: Gestionar la Aceptación del Cambio y de la Transición.	Cláusula 5: Liderazgo. Cláusula 9: Evaluación del desempeño.
Actividades de control	**Principio 12**: La organización despliega actividades de control a través de políticas y procedimientos.	APO01: Gestionar el Marco de Gestión de TI.	Cláusula 4: Contexto de la organización. Cláusula 5: Liderazgo. Cláusula 8: Operación.
Actividades de monitoreo	**Principio 16**: Conduce evaluaciones continuas y/o independientes. (AUDITOOL, 2016)	MEA02: Supervisar, Evaluar y Valorar el Sistema de Control Interno.	Cláusula 9: Evaluación del desempeño.

Fuente: Elaborado por el autor

5.2 Conclusiones del capítulo 5

El objetivo del cuadro comparativo entre los marcos de gobierno COBIT 5 Y COSO III y el estándar de sistema de gestión anti-soborno ha sido determinar cuáles son las relaciones que se han encontrado a lo largo de todo este trabajo.

La relación entre los marcos de gobierno se ha enfocado en los procesos del área de Gobierno y a breve detalle de los procesos de gestión, con mayor enfoque en el área de Gobierno ya que para el presente trabajo es primordial los procesos relacionados al Gobierno TI. Gracias a la ayuda de ISACA con su informe *Relating the COSO Internal Control - Integrated Framework and COBIT* se ha facilitado encontrar la relación entre los 2 marcos de gestión estudiados en el presente trabajo.

En conclusión, para encontrar la relación entre la norma ISO 37001 y el marco de referencia COSO III, ha sido de gran importancia encontrar antes una relación entre los marcos de referencia COBIT 5 y COSO III debido a que, con esta relación en el área de Gobierno, se ha facilitado encontrar la alineación de los principios de COSO III con las cláusulas expuestas por el estándar ISO 37001.

Conclusiones

Como Areitio (2008) explica, un buen Sistema de Gestión de Seguridad de la Información (SGSI) se lo puede relacionar con una fase, que comienza con la prevención y reducción de las amenazas, la detección y contención de incidentes; es decir, si se ocasionan daños se corrigen y se pasa a la recuperación de los mismos, siguiendo de la evaluación de nuevo y volviendo al principio de la fase que es la prevención de las amenazas.

Para verlo desde otro punto de vista Giraldo (2016) indica que para poner en práctica los objetivos y las políticas en una organización, un SGSI debe contar con, una estructura, recursos, procesos y procedimientos que ayudarán a poner en práctica lo antes mencionado; proporcionando a la alta gerencia una herramienta que le permita obtener visión global acerca de los sistemas informáticos en la organización.

Por consiguiente, se deduce que la implementación de un SGSI ayuda a tratar aspectos de seguridad, con los recursos necesarios y con el respaldo administrativo adecuado garantizando la implantación de los controles necesarios en relación con los objetivos de la organización con el fin de mantener los riesgos en un nivel asumible.

Como ya se ha explicado en reiteradas veces, la información es considerada uno de los activos más valiosos en una organización, es por esto que los controles y contramedidas que sugiere la teoría y práctica de la Seguridad de la Información deben ser consideradas en toda organización con el propósito de proteger la información, cumpliendo con sus tres dimensiones básicas: disponibilidad, confidencialidad e integridad. (Giraldo, 2016)

Otro tema fundamental en la seguridad de la información es el análisis de los riesgos. Este estudio lo deben realizar todas las organizaciones con el fin de determinar las vulnerabilidades que afecten los activos y así detectar las amenazas que se podrían causar a raíz de estas

vulnerabilidades. Por esto se debe identificar los riesgos a los que se encuentra expuesto la organización, para establecer medidas que ayuden a mantener una correcta seguridad de la información. (Giraldo, 2016)

La seguridad de la información en el entorno ecuatoriano, como lo explica Solorzano y compañía (2013), está encabezada por ITIL, ya que es un marco de referencia que detalla buenas prácticas y sugerencias para la administración de servicios de TI seguido de COBIT, que es un marco de gobierno para el control y supervisión de TI.

Las normas tratadas en el presente trabajo han sido consideradas como relevantes para tratar el tema de la gestión en la seguridad de la información. Las normas de la familia ISO 27000 ayudan en la seguridad de la información que se puede aplicar a cualquier tipo de empresa, ya sea grande o PYME, pública o privada.

La principal norma de la serie es la ISO 27001, ya que contiene los requisitos del SGSI y es certificable; seguida de la ISO 27002 que como Giraldo (2016) explica, es una guía de buenas prácticas que recomienda medidas a implementar con el fin de asegurar el sistema de información en la organización; otra es la conocida ISO 27005 que se enfoca en establecer principios, los mismos que contienen directrices y recomendaciones para la gestión de riesgos en lo referente a la seguridad de la información.

Con el fin de protegerse de forma eficaz y hacer crecer al negocio, las organizaciones gestionan los riesgos, aunque sea de una manera AdHoc. Parecida a la norma ISO 27005, la norma ISO 31000 es una guía de principios que ayuda a las organizaciones en el análisis y evaluación de riesgos sin importar el contexto de la organización.

COSO III y COBIT 5 son marcos de gobierno que se pueden aplicar a cualquier tipo de organización, independientemente de la ubicación geográfica, del tamaño o del tipo de industria.

COSO III incrementa la posibilidad de que un objetivo de la organización se cumpla debido a que es un marco integrado con herramientas para la implementación de un sistema de control interno efectivo. Por otro lado, como ISACA (2012) explica, COBIT 5 es un marco para el gobierno y gestión de la información que ayuda a las organizaciones a lograr sus objetivos para el gobierno y la gestión de las TI corporativas.

La lucha contra la corrupción es el tema en el que se fue enfocando el trabajo debido a que la norma ISO 37001 es ha sido el tema principal de este trabajo.

Según la encuesta de Ernst & Young (2016), la corrupción y el soborno representan una amenaza para el crecimiento global; es por esto indica, que organismos nacionales e internacionales se enfocan en investigar practicas no éticas. Explica también que se observa un nivel de apoyo sin precedentes por parte de los gobiernos y organizaciones a nivel mundial en contra de malas prácticas.

Según el Banco Mundial, cada año se paga más de 1 billón de dólares en sobornos lo que ocasiona inestabilidad política, aumento de la pobreza y el incremento del costo de los negocios. A nivel internacional es una barrera importante para el comercio y dentro de una organización puede afectar negativamente la moral de las partes interesadas. (UNIT, 2016)

Hoy en día los comportamientos no éticos no conocen límites, y es debido al rápido desarrollo del comercio internacional que se han propiciado nuevos fenómenos delictivos, uno de los cuales es el delito de soborno. Existen diversas normas en contra de la corrupción, entre ellas la ley FCPA que se ha encargado de cobrar multas millonarias a empresas y personas que han decidido llevar a cabo prácticas o actitudes poco éticas.

Según UNIT (2016), un sistema de gestión anti-soborno está diseñado para inspirar practicas contra la corrupción en una organización y así implementar los controles necesarios para detectar actos corruptos y minimizar su incidencia.

La norma ISO 37001 proporciona una guía para establecer, implementar, mantener y mejorar un sistema de gestión anti-soborno. Dicho sistema, se lo puede integrar con otros sistemas de gestión o puede ser independiente. (ISO, 2015)

La norma aborda los siguientes riesgos:

- Soborno en los sectores público, privado y sin fines de lucro.
- Soborno por la organización, por el personal o socios comerciales que actúan en su nombre o en beneficio propio.
- Soborno de la organización o de su personal o socios comerciales que actúen en su nombre o en su beneficio
- Soborno directo e indirecto (p. ej. un soborno pagado o recibido a través de un tercero) (ISO, 2015)

Esta norma posee 10 cláusulas y se basa en la estructura de alto nivel (HLS). ISO (2015) explica que el texto, los términos comunes y las definiciones básicas del HLS se establecen en las Directivas ISO/IEC del Anexo SL lo que hace que esta norma sea muy fácil de alinear con las normas de la familia ISO 27000 como es la ISO 27001, ISO 27002, ISO 27005.

Por otro lado, al ser una norma que necesita del análisis y evaluación de los riesgos de soborno, es necesario relacionarla con la ISO 31000 para gestionar los riesgos.

Para los marcos de gobierno COSO III y COBIT 5 se vio necesario enfocar la relación en los procesos de gobierno separando así el área de gestión. Los principios de COSO III se alienaron fuertemente a los procesos de gobierno de COBIT 5 y así con esta relación se encontró la

alineación con la norma ISO 37001. La mayor relación que hubo con los marcos de gobierno fueron en las cláusulas 5 y 9.

Concluyendo así que la norma ISO 37001 puede fácilmente alinearse a las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000 y exponiendo en el capítulo 5 un cuadro general donde se explica la relación que se produjo entre los marcos de gobierno COSO III y COBIT 5 con la norma ISO 37001.

Recomendaciones

Para la correcta implementación de un sistema de gestión es necesario conocer el sistema de gestión que se desea implementar, entender que los sistemas que por más que se puedan relacionar, no son los mismos y cada uno necesita de diferentes requerimientos.

A lo largo del presente trabajo se ha recalcado que conocer a la organización, su contexto interno y externo, la estructura, las necesidades de las partes interesadas, el estilo de liderazgo, el compromiso de la alta gerencia, su enfoque hacia los objetivos corporativos, entre otros, es la clave para determinar qué es lo que necesita el sistema de gestión o simplemente para que un sistema de gestión se pueda implementar.

Leer sobre las normas no hacen a una persona experta en el tema de sistemas de gestión. Para ello es necesario certificarse, estudiar a fondo las normas para lograr comprender desde sus conceptos más básicos hasta los más complejos y así poder captar de una forma más objetiva el alcance que puede tener un sistema de gestión, ya que no está limitado a un solo tipo de organización, sino es extensible a varios tipos en los que sus necesidades, sus recursos, sus vulnerabilidades, y su estructura es variable.

Mientras más conocimientos se adquieran sobre sistemas de gestión, mayor será la posibilidad de resguardar uno de los activos más valiosos de una organización, la información.

Bibliografía

Stanford University. (31 de Mayo de 2017). *Foreign Corrupt Practices Act Clearinghouse*. Obtenido de http://fcpa.stanford.edu/

Aguilera, P. (2010). *Seguridad informática.* Madrid, España: Editex.

Alessi, G. (4 de Enero de 2017). *Odebrecht revela la corrupción sistémica en Latinoamérica*. Obtenido de El País: https://elpais.com/internacional/2017/01/04/america/1483488807_369388.html

Areitio, J. (2008). *Seguridad de la información.* Madrid, España: Paraninfo.

AUDITOOL. (1 de Junio de 2016). *17 principios de Control Interno según COSO 2013*. Obtenido de AUDITOOL - Red Global de Conocimientos en Auditoría y Control Interno: https://www.auditool.org/blog/control-interno/2735-17-principios-de-control-interno-segun-coso-iii

Bedoya, J. (2016). *Delito de soborno transnacional. Antecedentes, consideraciones sobre el bien jurídico y estructura típica.* Medellín: Universidad EAFIT.

BSI Group México. (s.f.). *BSI. ...making excellence a habit.* Obtenido de ISO/IEC 27001 – Gestión de Seguridad de la Información – Guía de Transición: https://www.bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20Transici%C3%B3n_ISO27001.pdf

Buri, D., & Matute, J. (2012). *Diferentes modalidades de incremento de capital social en las compañias de responsabilidad limitada y anónimas.* Cuenca: Universidad de Cuenca.

Cassin, R. (2 de Octubre de 2017). *El Blog de la FCPA*. Obtenido de http://www.fcpablog.com/blog/2017/10/2/fcpa-enforcement-report-for-q3-2017.html

Cassin, R. (22 de Septiembre de 2017). *El Blog de la FCPA*. Obtenido de http://www.fcpablog.com/blog/2017/9/22/telia-tops-our-new-top-ten-list-after-we-do-some-math.html

Cassin, R. (3 de Enero de 2017). *El Blog de la FCPA*. Obtenido de http://www.fcpablog.com/blog/2017/1/3/the-2016-fcpa-enforcement-index.html

Cordero, G. (2015). *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información.* Cuenca, Ecuador.

Crespo, E. (2016). Una metodología para la gestión de riesgo aplicada a las MPYMES del Ecuador. *ECU@RISK*.

Crespo, P. (2016). *METODOLOGÍA DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DEL RIESGO INFORMÁTICO APLICABLE A MPYMES.* Cuenca: Universidad de Cuenca.

Ebrard, J. (25 de Enero de 2017). *AMERICAS: A VECES LAS MALAS NOTICIAS SON BUENAS NOTICIAS*. Obtenido de Transparency International: https://www.transparency.org/news/feature/americas_sometimes_bad_news_is_good_news

Epstein, E. (2016). Combate Contra la Corrupción Internacional y Enfoque en América Latina: Ley FCPA y Nuevo Programa del Departamento de Justicia de los Estados Unidos. *Rock Center for Corporate Governance*.

Erb, M. (2008). *WordPress.com*. Obtenido de https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

Ernst & Young. (2016). *14ª Encuesta Global sobre Fraude y Corrupción.* Centro de Estudios EY.

Frías, J., Rodríguez, L., & Isabel, G. (2014). Políticas contra la corrupción y el soborno: ¿se involucran de manera similar los consejeros en diferentes entornos corporativos? *Revista Europea de Dirección y Economía de la Empresa*, 31-42.

Galaz, Y. R. (Junio de 2015). *Deloitte.* Obtenido de https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO-Sesion1.pdf

Giraldo, L. (2016). *Analisis para la implementación de un sistema de gestión de la seguridad de la informacón según la norma ISO 27001 en la empresa Servidoc S.A.* Cali, Valle del Cauca: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA.

Gonzales, J. (2016). *ISO/IEC 27001 y 27002 para la Gestión de Seguridad de la Información.* Andahuaylas: Universidad Nacional José María Arguedas.

González, D. (30 de Agosto de 2013). *Magazcitum* . Obtenido de El magazine para los profesionales de la seguridad de TI: http://www.magazcitum.com.mx/?p=2397#.WcRfxcgjHIU

Gutierrez, C. (18 de Octubre de 2013). *welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2013/10/18/renovados-anexos-iso-iec-27001-2013/

INEN. (2013). *ISO/IEC 27001:2013*. Obtenido de Servicio Ecuatoriano de Normalización: https://inen.isolutions.iso.org/obp/ui#iso:std:iso-iec:27001:ed-2:v1:en

Infoautónomos. (7 de Septiembre de 2017). *Tipos de sociedades*. Obtenido de Infoautónomos: http://infoautonomos.eleconomista.es/tipos-de-sociedades/sociedad-civil-caracteristicas-ventajas/

International Organization for Standardization. (Octubre de 2013). *ISO International Organization for Standardization*. Obtenido de https://www.iso.org/standard/54533.html

ISACA. (2012). *Cobit 5 - Procesos Catalizadores.*

ISACA. (2012). *Cobit 5 - Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.*

ISACA. (2014). *Relating the COSO Internal Control—Integrated Framework and COBIT.*

IsecT. (8 de Octubre de 2017). *ISO/IEC 27002*. Obtenido de ISO / IEC 27002: 2013 Tecnología de la información - Técnicas de seguridad - Código de prácticas para controles de seguridad de la información (segunda edición): http://www.iso27001security.com/html/27002.html

ISO. (2015). *ISO 37001 Anti-bribery management systems.*

ISO 27001 en Español. (3 de 01 de 2016). *¿Qué es un SGSI?* Obtenido de http://www.iso27000.es/sgsi.html

ISOTools Excellence. (18 de Agosto de 2015). *La norma ISO 27001:2013 ¿Cuál es su estructura?* Obtenido de SGSI Blog especializado en Sistemas de Gestión : http://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

ISOTools. (s.f.). *Software ISO Riesgos y Seguridad*. Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000/

López, D., & Vásquez, S. (2016). *Comparación entre metodologías de Gestión de Riesgo Informático.* Cuenca, Ecuador.

Martinez, D. (8 de Septiembre de 2010). *Sociedad de hecho.* Obtenido de SlideShare: https://es.slideshare.net/dmaitam/sociedad-de-hecho

Minchala, P. (2016). *Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI.* Cuenca, Ecuador: Universidad del Azuay.

Mizrahi, D. (25 de Enero de 2017). *El ranking de los países más y menos corruptos del mundo*. Obtenido de infobae: https://www.infobae.com/america/mundo/2017/01/25/el-ranking-de-los-paises-mas-y-menos-corruptos-del-mundo/

OECD. (2016). *Committing to Effective Whistleblower Protection.* Paris: Organisation for Economic Co-operation and Development.

Pallas, G. (2009). *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico.* Montevideo, Uruguay.

PECB. (9 de Enero de 2015). *Whitepapers ISO 31000 Risk Management – Principles and Guidelines*. Obtenido de PECB: https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines

PECB. (27 de Noviembre de 2015). *Whitepapers ISO/IEC 27005 Information Technology – Security Techniques Information Security Risk Management*. Obtenido de PECB: https://pecb.com/whitepaper/isoiec-27005-information-technology--security-techniques-information-security-risk-management

PECB. (23 de Febrero de 2016). *PECB*. Obtenido de Whitepapers ISO/IEC 27002:2013 Information Technology - Security Techniques Code of Practice for Information Security Controls: https://pecb.com/whitepaper/isoiec-270022013-information-technology---security-techniques-code-of-practice-for-information-security-controls

PECB. (12 de Diciembre de 2016). *Whitepapers ISO 37001:2016 - Anti-Bribery Management Systems (Requirements with guidance for use)*. Obtenido de PECB: https://pecb.com/whitepaper/iso-370012016---anti-bribery-management-systems-requirements-with-guidance-for-use

Pedraja, L., & Rodríguez, E. (2008). ESTUDIO COMPARATIVO DE LA INFLUENCIA DEL ESTILO DE LIDERAZGO Y LA CONGRUENCIA DE VALORES EN LA EFICACIA DE EMPRESAS PRIVADAS E INSTITUCIONES PÚBLICAS. *Interciencia*.

Quaragroup. (15 de Noviembre de 2016). *¿Qué es la Norma ISO 37001:2016?* Obtenido de Quara Consulting & Training: http://www.quaragroup.com/es/post/que-es-la-norma-iso-370012016

Rainey, H., Backoff, R., & Levine, C. (1976). Comparing Public and Private Organizations. *Public Administration Review,* 233-244.

Rosenberg, M., & Raymond, N. (21 de Diciembre de 2016). *Firmas brasileñas pagarán recargo de $ 3.500 millones en caso de corrupción*. Obtenido de REUTERS: http://www.reuters.com/article/us-brazil-corruption-usa/brazilian-firms-to-pay-record-3-5-billion-penalty-in-corruption-case-idUSKBN14A1QE

Salas, L. (2007). Estado, empresa privada y sector social: una relación entre sectores que fortalece a la Sociedad Civil. *Trabajo Social*, 107-130.

Solorzano, L., Rezabala , J., & Aranda, A. (23 de Mayo de 2013). *DSpace en ESPOL*. Obtenido de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/24298

Transparencia Internacional. (25 de Enero de 2017). *ÍNDICE DE PERCEPCIÓN DE LA CORRUPCIÓN 2016*. Obtenido de TRANSPARENCY INTERNATIONAL: https://www.transparency.org/news/feature/corruption_perceptions_index_2016

Transparency International. (2009). *Informe Global de la Corrupción 2009 - Corrupción y sector privado.* Nueva York: Cambridge University Press.

TRANSPARENCY INTERNATIONAL ESPAÑA. (2 de Noviembre de 2011). *IFS 2011*. Obtenido de TRANSPARENCY INTERNATIONAL ESPAÑA: http://transparencia.org.es/en/ifs-2011/

UNIT. (2016). *ISO 37001, Sistemas de Gestión Anti-Soborno.* Montevideo.

ANEXOS:

Doctora Jenny Ríos Coello, Secretaria de la Facultad de Ciencias de la Administración de la Universidad del Azuay

C E R T I F I C A:

Que, el Consejo de Facultad en sesión del 29 de mayo de 2017, conoció la petición del estudiante **EDISSON SANTIAGO ARIAS ORTIZ** con código **64282**, que presenta el diseño de su trabajo de titulación denominado: "***ANÁLISIS DE LA NORMA ISO 37001 Y SU RELACIÓN CON LAS ISO UTILIZADAS EN LA GESTIÓN DE RIESGOS***", presentado previa a la obtención del título de Ingeniero de Sistemas y Telemática.- El Consejo de Facultad acogió el informe de la Junta Académica de Ingeniería de Sistemas y Telemática y resolvió aprobar el diseño. Designa como **Director al ingeniero Esteban Crespo Martínez** y como miembros del Tribunal Examinador a los ingenieros Francisco Salgado Arteaga, Ph.D. y Lenin Erazo Garzón.- En esta misma sesión el Consejo de Facultad fija como plazo para la entrega del trabajo de titulación, seis meses contados desde la fecha de su aprobación, esto es hasta el **29 de noviembre de 2017**, debiendo el Director presentar a la Junta Académica, dos informes bimensuales del desarrollo del trabajo de titulación.

Cuenca, mayo 30 de 2017

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION
SECRETARIA

Dra. Jenny Ríos Coello
Secretaria de la Facultad de
Ciencias de la Administración

Oficio Nro. 066-2017-DIST-UDA

Cuenca, 12 de mayo de 2017

Señor Ingeniero
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
Presente.-

De nuestras consideraciones:

La Junta Académica de la Escuela de Ingeniería de Sistemas y Telemática, reunida el día 12 de mayo del 2017, recibió el proyecto de tesis titulado "Análisis de la norma ISO 37001 y su relación con las ISO utilizadas en la gestión de riesgos", presentado por Edison Santiago Arias Ortiz estudiante de la Escuela de Ingeniería de Sistemas y Telemática, y revisado por el Ing. Esteban Crespo, previo a la obtención del título de Ingeniero de Sistemas y Telemática.

Por lo expuesto, y de conformidad con el Reglamento de Graduación de la Facultad, recomendamos como director y responsable de aplicar cualquier modificación al diseño del trabajo de graduación posterior al Ing. Esteban Crespo y como miembros del Tribunal a Francisco Salgado Ph.D. e Ing. Lenin Erazo.

Atentamente,

Ing. Marcos Orellana Cordero
Cordinador Escuela de Ingeniería de Sistemas y Telemática
Universidad del Azuay

UNIVERSIDAD DEL AZUAY

Escuela Sistemas y Telemática

Oficio Estudiante: Solicitud aprobación de Protocolo de Trabajo de Titulación

IST-RE-EST-02
Versión 01
04/04/2017
Página **1** de **1**

Lugar de Almacenamiento	Retención	Disposición Final
F: Archivo Secretaría de la Facultad	5 años	Almacenar en archivo pasivo de la Facultad

Cuenca, 12 de mayo de 2017

Ingeniero,
Oswaldo Merchán Manzano
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN
UNIVERSIDAD DEL AZUAY

De mi consideración,

Estimado Señor Decano, yo **Edisson Santiago Arias Ortiz** con C.I. **0105722052**, código estudiantil 64282 estudiante de la Carrera de Sistemas y Telemática, solicito muy comedidamente a usted y por su intermedio al Consejo de Facultad, la aprobación del protocolo de trabajo de titulación con el tema **"ANÁLISIS DE LA NORMA ISO 37001 Y SU RELACIÓN CON LAS ISO UTILIZADAS EN LA GESTIÓN DE RIESGOS"** previo a la obtención del título de Ingeniero en Sistemas y Telemática para lo cual adjunto la documentación respectiva.

Por la favorable acogida que brinde a la presente, anticipo mi agradecimiento.

Atentamente:

Edisson Arias

Estudiante de la Carrera de Sistemas y Telemática

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500
Nº 0796056

CONVOCATORIA

Por disposición de la Junta Académica de **Ingeniería de Sistemas y Telemática**, se convoca a los Miembros del Tribunal Examinador, a la sustentación del Protocolo del Trabajo de Titulación: **"ANÁLISIS DE LA NORMA ISO 37001 Y SU RELACIÓN CON LAS ISO UTILIZADAS EN LA GESTIÓN DE RIESGOS"**, presentado por el estudiante **Edisson Santiago Arias Ortiz**, previa a la obtención del grado de **Ingeniero en Sistemas y Telemática**, para el día **MARTES 16 DE MAYO DE 2017 A LAS 11h20,** La sustentación se realizará en el **laboratorio del IERSE.**

Cuenca, 11 de mayo de 2017

Dra. Jenny Ríos Coello
Secretaria de la Facultad

Ing. Esteban Crespo Martínez .....

Ing. Lenin Erazo Garzón .....

Dr. Francisco Salgado Arteaga .....

mjmr/

Cuenca, 10 de mayo de 2017

Ingeniero

Oswaldo Merchán

Decano de la Facultad de Ciencias de la Administración

Presente

De mi consideración:

Por la presente, me permito informarle que he revisado el diseño de tesis presentado por el estudiante **Edisson Santiago Arias Ortiz** con código **64282,** cuyo tema es *"Análisis de la norma ISO 37001 y su relación con las ISO utilizadas en la gestión de riesgos"*, como requisito previo para la obtención del título de Ingeniero de Sistemas y Telemática.

Al respecto, el diseño de tesis presenta una estructura teórica, metodológica y técnica coherente, cuyo objetivo es el de analizar el estándar ISO 37001 referente a sistemas de lucha contra el soborno y su relación con las ISO utilizadas en la gestión de riesgos, alineándose al proyecto del libro "Metodología para la gestión de riesgos de información", el mismo que ejecuto actualmente en la Universidad del Azuay.

Por lo expuesto, emito informe favorable y recomiendo su aprobación.

Esteban Crespo Martínez

Docente de la Universidad del Azuay

UNIVERSIDAD DEL AZUAY

DOCTORA JENNY RIOS COELLO, SECRETARIA DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION DE LA UNIVERSIDAD DEL AZUAY

C E R T I F I C A:

Que, el señor **ARIAS ORTIZ EDISSON SANTIAGO,** con código **64282,** alumno de la escuela de **INGENIERIA DE SISTEMAS Y TELEMATICA**, tiene aprobado más del 80% de los créditos de su malla de estudios.

Que, al señor **ARIAS ORTIZ EDISSON SANTIAGO,** le falta aprobar las siguientes asignaturas para finalizar sus estudios:

PRODUCCIÓN II

SISTEMAS DE INFORMACIÓN GERENCIAL

PROYECTOS TELEMÁTICOS

CALIDAD DE SOFTWARE

INGENIERÍA DE SOFTWARE II

METODOLOGIA DE LA INVESTIGACION

Cuenca, 10 de mayo de 2017

Derecho No. **001-001-000156878**

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0792621

UNIVERSIDAD DEL AZUAY

ACTA
SUSTENTACIÓN DE PROTOCOLO/DENUNCIA DEL TRABAJO DE TITULACIÓN

1.1 **Nombre del estudiante:** **Edisson Santiago Arias Ortiz**
1.2 **Director sugerido**: Ing. Esteban Crespo Martínez
1.3 **Codirector (opcional)**:
1.4 **Tribunal:** Ing. Lenin Erazo Garzón/ Dr. Francisco Salgado Arteaga
1.5 **Título propuesto: "ANÁLISIS DE LA NORMA ISO 37001 Y SU RELACIÓN CON LAS ISO UTILIZADAS EN LA GESTIÓN DE RIESGOS"**
1.6 **Resolución**:

1.6.1 Aceptado sin modificaciones ✓

1.6.2 Aceptado con las siguientes modificaciones:

_____

_____

_____

1.6.3 Responsable de dar seguimiento a las modificaciones: Ing. Esteban Crespo

1.6.4 No aceptado
- Justificación:

_____
_____
_____

Tribunal

.....	.....	.....
Ing. Esteban Crespo Martínez	Ing. Lenin Erazo Garzón	Dr. Francisco Salgado Arteaga

.....
Sr. Edisson Santiago Arias Ortiz

Dra. Jenny Ríos Coello
Secretario de Facultad

Fecha de sustentación: día **MARTES 16 DE MAYO DE 2017 A LAS 11h20**

UNIVERSIDAD DEL AZUAY

RÚBRICA PARA LA EVALUACIÓN DEL PROTOCOLO DE TRABAJO DE TITULACIÓN

1.1 Nombre del estudiante: Edisson Santiago Arias Ortiz
1.2 Director sugerido: Ing. Esteban Crespo Martínez
1.3 Codirector (opcional):
1.4 Título propuesto: **"ANÁLISIS DE LA NORMA ISO 37001 Y SU RELACIÓN CON LAS ISO UTILIZADAS EN LA GESTIÓN DE RIESGOS"**
1.5 Revisores (tribunal): Ing. Lenin Erazo Garzón/ Dr. Francisco Salgado Arteaga
1.6 Recomendaciones generales de la revisión:

	Cumple totalmente	Cumple parcialmente	No cumple	Observaciones (*)
Línea de investigación				
1. ¿El contenido se enmarca en la línea de investigación seleccionada?	/			
Título Propuesto				
2. ¿Es informativo?				
3. ¿Es conciso?	/			
Estado del arte				
4. ¿Identifica claramente el contexto histórico, científico, global y regional del tema del trabajo?	/			
5. ¿Describe la teoría en la que se enmarca el trabajo	/			
6. ¿Describe los trabajos relacionados más relevantes?	/			
7. ¿Utiliza citas bibliográficas?	/			
Problemática y/o pregunta de investigación				
8. ¿Presenta una descripción precisa y clara?	/			
9. ¿Tiene relevancia profesional y social?	/			
Hipótesis (opcional)				
10.¿Se expresa de forma clara?				
11.¿Es factible de verificación?				
Objetivo general				
12.¿Concuerda con el problema formulado?	/			
13.¿Se encuentra redactado en tiempo verbal infinitivo?	/			
Objetivos específicos				
14.¿Concuerdan con el objetivo	/			

14.¿Concuerdan con el objetivo general?				
15.¿Son comprobables cualitativa o cuantitativamente?				
Metodología				
16.¿Se encuentran disponibles los datos y materiales mencionados?				
17.¿Las actividades se presentan siguiendo una secuencia lógica?				
18.¿Las actividades permitirán la consecución de los objetivos específicos planteados?				
19.¿Los datos, materiales y actividades mencionadas son adecuados para resolver el problema formulado?				
Resultados esperados				
20.¿Son relevantes para resolver o contribuir con el problema formulado?				
21.¿Concuerdan con los objetivos específicos?				
22.¿Se detalla la forma de presentación de los resultados?				
23.¿Los resultados esperados son consecuencia, en todos los casos, de las actividades mencionadas?				
Supuestos y riesgos				
24.¿Se mencionan los supuestos y riesgos más relevantes?				
25.¿Es conveniente llevar a cabo el trabajo dado los supuestos y riesgos mencionados?				
Presupuesto				
26.¿El presupuesto es razonable?				
27.¿Se consideran los rubros más relevantes?				
Cronograma				
28.¿Los plazos para las actividades son realistas?				
Referencias				
29.¿Se siguen las recomendaciones de normas internacionales para citar?				
Expresión escrita				
30.¿La redacción es clara y fácilmente comprensible?				
31.¿El texto se encuentra libre de faltas ortográficas?				

(*) Breve justificación, explicación o recomendación.

- Opcional cuando cumple totalmente,
- Obligatorio cuando cumple parcialmente y NO cumple.

.....

.....

.....

Ing. Esteban Crespo Martínez

Ing. Lenin Erazo Garzón

Dr. Francisco Salgado Arteaga

UNIVERSIDAD DEL AZUAY

UNIVERSIDAD DEL AZUAY
INGENIERÍA DE SISTEMAS Y TELEMÁTICA
METODOLOGÍA DE LA INVESTIGACIÓN

1. DATOS GENERALES

1. 1 Nombre del estudiante: Arias Ortiz Edisson Santiago.

1. 1. 1 Código: 64282

1. 1. 2 Contacto: 074191454, 0987742579

1. 1. 3 Correo Electrónico: solspp_027@hotmail.com

1. 2 Director Sugerido: Crespo Martínez Paul Esteban, Ing.

1. 2. 1 Contacto: 4091000, 0996804562

1. 2. 2 Correo Electrónico: ecrespo@uazuay.edu.ec

1. 3 Co-director Sugerido: Ninguno.

1. 4 Asesor Metodológico: Salgado Arteaga Francisco, PhD.

1. 4. 1 Correo Electrónico: fsalgado@uazuay.edu.ec

1. 5 Tribunal Designado:

1. 6 Aprobación:

1. 7 Línea de Investigación de la carrera:
Informática de computadores
Sistema de Gestión de Seguridad de la Información

1. 7. 1 Código UNESCO: 1203 Informática de computadoras
1203.99 Sistemas de Seguridad de la Información

1. 7. 2 Tipo de Trabajo: Investigación formativa relacionada con la Gestión de la Seguridad de la Información

1. 8 Área de Estudio: Seguridad de la Información.

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0797209

1. 9 Titulo Propuesto: "Análisis de la norma ISO 37001 y su relación con las ISO utilizadas en la gestión de riesgos".

1. 10 Subtitulo: (opcional)

1. 11 Estado del proyecto: Trabajo de investigación.

2. CONTENIDO

2. 1 Motivación de la Investigación:

Muchos temas de la actualidad están relacionados con los sobornos y los actos de corrupción. Este tipo de actos conllevan sin duda al riesgo, que finalmente termina como un elemento habilitante para la interrupción o negación de los procesos de negocio, afectando a cualquier tipo de organización o empresa.

La ISO 37001, publicada en enero de este año, hace referencia a este tipo de amenazas, por cuanto es importante conocer, a nivel del riesgo operativo y de la seguridad de la información, como esta norma se relaciona con la norma ISO 31000 utilizada en la gestión de riesgos y la ISO 27005, utilizada en la gestión de riesgos de información.

2. 2 Problemática:

La problemática se presenta en relación de como los sobornos pueden generar escenarios de riesgo a los activos de información que forman parte de los procesos de negocio, elementos que deben ser contemplados por las normas de gestión de riesgo, las metodologías y los marcos de gestión. Debido a estos antecedentes se plantea el análisis de la norma anti soborno ISO 37001 y su relación con la gestión de riesgos.

2. 3 Resumen:

En este trabajo se pretende indagar sobre aspectos de gestión de riesgo que mantiene la recién norma publicada en enero de 2017, ISO 37001, y determinar su relación con los capítulos de gestión de riesgo que contemplan las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000.

Además, se estudiará la relación que mantiene esta norma con los marcos de gobierno COBIT 5 y COSO III, utilizados en el aseguramiento y gestión de riesgos de activos de la información.

2. 4 Indagación exploratoria y base conceptual:

En la actualidad, para una organización o para una persona, la información es el elemento más valioso, incluso se puede tomar como un arma para crear ventaja competitiva. Sin embargo, debido a la complejidad de las normas internacionales que brindan procesos de cómo proteger la información, o a la falta de conocimiento de cómo gestionarla adecuadamente, muchas organizaciones o personas en particular, no alcanzan a protegerla. (Crespo, 2017)

COBIT 5 es la nueva versión de ISACA, pensado para empresas de todo tipo y tamaño. Es un marco evolutivo de TI internacional, empresariales, de consultoría, de seguridad de riesgo y de aseguramiento, en lo que un marco de gobierno y gestión debe proporcionar. Se basa en COBIT 4.1, y se desarrolló teniendo en cuenta estándares y marcos de referencia como ITIL, Serie ISO/IEC 27000, Serie ISO/IEC 31000, PMBOK y otros marcos de referencia y normas. (ISACA, 2012)

El marco de referencia COSO:2013 pone un mayor énfasis en los riesgos de fraude y será la nueva norma que evalúa la efectividad de los controles internos. Los riesgos de fraude son considerados cuando un individuo o entidad actúa fuera de los limites esperados de la organización. (Ernst & Young, 2014)

Como explica (Ernst & Young, 2014) "un programa antifraude no proporcionará garantías contra el fraude, pero puede ayudar a mitigar el riesgo de fraude al permitir a la administración identificar y priorizar los riesgos de fraude y asignar recursos para hacerles frente."

Las normas ISO surgen como una necesidad para mejorar la calidad y seguridad de la información, para promover el uso de las buenas prácticas, garantizando la disponibilidad, integridad y confidencialidad debido a que la información siempre está expuesta a amenazas y delitos informáticos, y por esto puede verse afectada o estar en riesgo, la buena imagen, economía y estabilidad operacional de una organización. (Velásquez Pérez, Castro Silva, & Pérez, 2015)

La seguridad de la información es fundamental para el cumplimiento de los objetivos. Como explican Pérez y Silva "La gestión de riesgo de TI tiene relación directa con el concepto de Sistemas de Gestión de la Seguridad de la Información (SGSI), esto involucra el estudio de la familia de normas ISO 27000". (Velásquez Pérez, Castro Silva, & Pérez, 2015)

Hoy en día, las organizaciones gastan mucho dinero en dispositivos de seguridad para la protección de la información, por esto la norma ISO 27001 se convierte en una herramienta importante para gestionar la seguridad de la información en una empresa.

Actualmente existe la norma ISO 27002 que es una versión más detallada y precisa que la ya mencionada ISO 27001, lo que conlleva a la pregunta, ¿Qué objetivo tiene la ISO 27001?

Cabe recalcar que la ISO 27002 no es una norma de gestión; es decir, esta norma define como poner en marcha un sistema; la norma ISO 27001 define el sistema de gestión de seguridad de la información (SGSI). Según (Kosutic, s.f.) "este sistema de gestión significa que la seguridad de la información debe ser planificada, implementada, supervisada, revisada y mejorada." Lo que significa que la gestión tiene responsabilidades y la necesidad de la mejora continua, que se deben revisar objetivos, realizar auditorías, etc. Todo esto está especificado en la norma ISO 27001 y no en la ISO 27002. (Kosutic, s.f.)

Estas normas no han sido integradas debido a que, si fuera una única norma, sería muy extensa y compleja como para ser práctica, cada norma está diseñada con un enfoque especifico. (Kosutic, s.f.)

En el campo de la seguridad cibernética, medir la seguridad es una clara necesidad, es parte de la gestión de riesgo estandarizado, ISO 27001. En el entorno de seguridad

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0797213

física, son pocas las organizaciones que utilizan sistemas de gestión de riesgos, orientado a la mejora continua, ISO 31000. (Bilbao & Bilbao, 2013)

Debido a la gran popularidad del Sistema de Gestión de Calidad – ISO 9001, se han desarrollado otras normas para el Sistema de Gestión, las cuales se han identificado como: ISO 14001, ISO 22000, ISO 27001. En el año 2013 la ISO comenzó el desarrollo de la Gestión Anti-Soborno, estándar del Sistema ISO 37001. El objetivo del sistema es ayudar a promover un negocio ético en pequeñas y medianas empresas, públicas o privadas y de cualquier país. Los Requisitos y definiciones de la norma ISO 37001 son similares con otras normas ISO del sistema de gestión. La estructura común de las normas del Sistema de Gestión ISO, HLS (High Level Structure) ayuda a las organizaciones a implementar más de un Sistema de gestión e integrarlos, por lo que, la reciente norma ISO 37001 puede integrarse con otras normas relacionadas al Sistema de Gestión. (Kafel, 2016)

Los estándares, sistemas y estrategias contra el soborno son la menor manera de lidiar contra la corrupción en un entorno institucional o de negocios. Las organizaciones de hoy en día, están empezando a buscar que sus socios, clientes, proveedores, etc., tengan el objetivo de implementar sistemas anti corrupción o que la hayan implementado con el fin de mejorar las relaciones.

La corrupción es uno de los más grandes obstáculos para el desarrollo de una organización, donde los sobornos dirigidos a funcionarios corruptos, contratistas, proveedores, financiadores, etc., hacen que la pérdida total y el impacto de corrupción sea difícil de cuantificar. (Manuhwa & Stansbury)

El soborno es un problema muy complejo y destructivo con el que tienen que lidiar las organizaciones hoy en día, y a pesar de los esfuerzos para combatirlo, a veces parece inútil. Según el (Instituto Uruguayo de normas técnicas , 2016)"el Banco Mundial estima que cada año se paga más de 1 billón de dólares en sobornos, con efectos desastrosos como la erosión de la estabilidad política, el aumento del costo de los negocios" y esto contribuye al aumento de la pobreza.

La norma ISO 37001 está diseñada con el fin de inculcar una cultura contra la corrupción dentro de una empresa u organización e implementar controles que aumenten la probabilidad de detectar actos de corrupción y poder reducir su incidencia.

Como explica (Instituto Uruguayo de normas técnicas , 2016) la norma ISO 37001 "da los requisitos y orientaciones para establecer, implementar, mantener y mejorar un sistema de gestión anti-soborno."

Según Ernst & Young (EY) en una encuesta mundial sobre el fraude realizada en el año 2016 mostro que el 39% de los encuestados consideran que el soborno y la corrupción tienen un lugar muy amplio en su país. (Ernst & Young, 2016)

La ISO 37001 es un desarrollo significativo para aquellas organizaciones que buscan lidiar con riesgos de soborno y corrupción. La norma proporciona especificaciones para empresas u organizaciones, para establecer, implementar, mantener y mejorar continuamente su sistema de gestión para detectar y prevenir el soborno. Esta norma tiene la ventaja de ser adaptable a cualquier tipo de organización, independientemente de su exposición al riesgo de soborno, de su tamaño, o geografía. La norma exige que las organizaciones implementen medidas suficientes para prevenir y detectar el riesgo de soborno. (Ernst & Young, 2016)

Justificación

En la actualidad, el soborno es un gran obstáculo para el desarrollo, que genera corrupción y falta de confianza.

Se pretende analizar las amenazas por soborno a los activos de información que forman parte de los procesos de negocio. Es por esto que se analizará la norma anti-soborno ISO 37001 para compararla con otras normas relacionadas con la Gestión de riesgo de información.

2. 5 Objetivo General:

Analizar el estándar ISO 37001 referente a sistemas de lucha contra el soborno y su relación con las ISO utilizadas en la gestión de riesgos.

2. 6 Objetivos Específicos:

- Evaluar el estado del arte de la gestión de riesgo en las MPYMES
- Estudiar la norma ISO 37001 y resumir su alineación con las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000 en un cuadro comparativo.
- Identificar la aplicabilidad de la norma ISO 37001 en los marcos de referencia COBIT 5 y COSO III utilizados como marcos de gobierno.

2. 7 Metodología:

Para el desarrollo del proyecto mencionado se realizará una revisión de las normativas ISO 27001, ISO 27002, ISO 27005, ISO 31000 e ISO 37001, además de los marcos de referencia COBIT 5 y COSO III. También se procederá a realizar un análisis sobre estudios referentes a los temas mencionados realizados por terceros con el fin de indagar y recopilar la información necesaria para tener un conocimiento mucho más amplio sobre las normativas de la gestión de la seguridad.

Al final se realizará una comparativa entre dichas normas para encontrar la alineación entre las mismas.

2. 8 Alcances y resultados esperados:

El proyecto pretende generar un documento de análisis entre la norma ISO 37001 y su relación con las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000, lo que permitirá evaluar el aporte de esta nueva norma a la gestión de riesgos de información.

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500 Nº 0797212

2. 9 Supuestos y riesgos:

Falta de información. - En caso de no contar con acceso a la documentación de las ISO referentes a la gestión de riesgos y las metodologías COBIT 5 y COSO III debido al elevado precio de las mismas.

A la falta de acceso a la información sobre la ISO 37001, debido a que es una norma recientemente publicada.

2. 10 Presupuesto:

Rubro-Denominación	**Costo USD (detalle)**	**Justificación ¿para qué?**
Internet	$100	El internet será el medio principal por el cual se puede acceder a la mayor parte de la información referente al proyecto. Por esto es primordial disponer de él.
Impresiones	$100	Se usarán para entregar los documentos físicos del proyecto a realizarse.
Equipos y Suministros	$0	Debido a que los equipos y demás elementos utilizados en el proyecto son propiedad del único integrante del proyecto (Arias Ortiz Edisson Santiago).
Gastos Varios	$50	Gastos referentes a transporte de ser necesario o algún imprevisto que se presente dentro del proyecto.

2. 11 Financiamiento:

Será cubierto en su totalidad por el autor.

2. 12 Esquema Tentativo

PORTADA

ABSTRACT

INTRODUCCIÓN

CAPÍTULO 1 - Fundamentos

Sistemas de Gestión de la Seguridad de Información (SGSI)

La seguridad de la información y el riesgo informático

Los marcos de referencia internacionales utilizados en la gestión de riesgo

ISO 27001

ISO 27002

ISO 27005

UNIVERSIDAD DEL AZUAY

ISO 31000

Marcos de referencia

COBIT 5

COSO III

CAPÍTULO 2 – El sistema de Gestión Anti Soborno ISO 37001

- Describir los procesos que incluyen esta ISO

Conclusiones del capítulo 2

CAPITULO 3 – Alineación de ISO 37001 con las normas ISO utilizadas en la Gestión de Riesgos de la Información.

Alineación con ISO 27001

Alineación con ISO 27002

Alineación con ISO 27005

Alineación con ISO 31000

Conclusiones del capítulo 3

CAPITULO 4 – Alineación de ISO 37001 con los marcos de referencia.

Alineación con COBIT 5

Alineación con COSO 3

Conclusiones del capítulo 4

CAPITULO 5 – Cuadro comparativo entre ISO 37001, las normas y los marcos de referencia

- Cuadro comparativo entre las normas ISO utilizadas en la Gestión de Riesgos de la Información con la ISO 37001
- Conclusiones del capítulo 5

CONCLUSIONES

RECOMENDACIONES

BIBLIOGRAFÍA

ANEXOS

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500
Nº 0797211

2. 13 Cronograma:

Cronograma																								
Objetivo Específico	Actividad	Semanas																						
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Evaluar el estado del arte de la gestión de riesgo en las MPYMES	Evaluación de conceptos e información del estado del arte de la gestión de riesgo en las MPYMES.																							
Estudiar la norma ISO 37001 y resumir su alineación con las normas ISO 27001, ISO 27002, ISO 27005 e ISO 31000 en un cuadro comparativo.	Alineación entre ISO 37001 y demas normas de la Gestión de Riesgos.																							
Identificar la aplicabilidad de la norma ISO 37001 en los marcos de referencia COBIT 5 y COSO III utilizados como marcos de gobierno.	Aplicabilidad de la norma ISO 37001 en los marcos de referencia COBIT 5 y COSO III.																							

2. 14 Referencias.

Bilbao , A., & Bilbao, E. (2013). Measuring security. *2013 47th International Carnahan Conference on Security Technology (ICCST)*, (pág. 1). Medellin.

Crespo, E. (2017). Una metodología para la gestión de riesgo aplicada a las MPYMES del Ecuador. *ECU@Risk*.

Ernst & Young. (2014). *Updated 2013 COSO Framework - fraud risk assessments.*

Ernst & Young. (2016). *ISO 37001 The first international standard on anti-bribery management systems.*

Instituto Uruguayo de normas técnicas . (2016). *ISO 37001 Sistemas de gestión Anti - Soborno.* Montevideo – URUGUAY.

ISACA. (2012). *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Illinois 60008 EE.UU.

Kafel, P. (2016). ANTI-BRIBERY MANAGEMENT SYSTEM AS A TOOL TO INCREASE QUALITY OF LIVE. *1s tInternational conference on Quality of Life*, (págs. 221-222). Kragujevac.

Kosutic, D. (s.f.). *27001 Academy*. Obtenido de https://advisera.com/27001academy/es/knowledgebase/diferencias-y-similitudes-entre-iso-27001-e-iso-27002/

Manuhwa, M., & Stansbury, N. (s.f.). Anti-Bribery Standards, Systems and Strategies for Optimising Engineering Projects Delivery.

Velásquez Pérez, T., Castro Silva, H., & Pérez, Y. (2015). MODELO DE GESTIÓN DE RIESGOS EN PROYECTOS. APROXIMACIÓN CONCEPTUAL PARA PROYECTOS DE TI. *UFPSO*, 93-100.

UNIVERSIDAD DEL AZUAY

2.15 Anexos:

2.16 Firma de responsabilidad (estudiante)

Edisson Santiago Arias Ortiz

2.17 Firma de responsabilidad (director sugerido)

Ing. Paul Esteban Crespo Martínez

2.18 Firma de responsabilidad (asesor metodológico)

PhD. Francisco Salgado Arteaga

2.19 Fecha de entrega

16 de mayo del 2017

Edición autorizada de 10.000 ejemplares
Del 788.501 al 798.500
Nº 0797210