# Ciberseguridad y gestión del riesgo tecnológico en el marco de la NIIF

## Cybersecurity and technology risk management under the NIIF

Mg. Cristian Vaca
Universidad Tecnológica Israel
patos_nice@hotmail.com

Fecha de recepción:11/05/2016
Fecha de aceptación: 04/06/2016

***Resumen***

Con el avance de la tecnología y el bajo costo para el acceso ilimitado a medios informáticos de procesamiento de información que van desde hojas electrónicas, software de gestión administrativa y financiera, hasta los más avanzados ERP (Enterprise Resource Planning) hace de las tecnologías de la información – TI uno de los recursos más importantes dentro de las empresas; y por lo tanto, estas aplicaciones deben cumplir con normas de control interno que aseguren y garanticen a las partes interesadas los principios de la seguridad de la información.

Este artículo expone los riesgos de tecnología a los que está expuesta la información y un detalle de buenas prácticas para su gestión, se realiza también una breve reseña sobre la regulación local para la aplicación de las Normas Internacionales de Información Financiera NIIF, la cantidad de empresas existentes en el Ecuador y cuántas de estas usan aplicaciones informáticas para el procesamiento de información con la finalidad de

establecer un contexto claro sobre la importancia de gestionar el riesgo de seguridad de la información, utilizando para ello varias buenas prácticas como COBIT, ISO 31000, ISO27005, MAGERIT u OCTAVE según las necesidades de las compañías.

Palabras clave: Tecnologías de Información, NIIF, COSO, Control Interno.

### *Abstract:*

With the notorious improvement of technology, low cost for unlimited access to information, electronic processing like media sheets, administrative and financial management software, and the most advanced tool ERP (Enterprise Resource Planning), makes technology information one of the most important resource by the Company. Therefore, this applications must comply with internal control standards that ensure and guarantee to the stakeholders the principles of information security.

This article exposes the technology risks to which the information is exposed and a detail of good management practices. It also gives a brief overview of the local regulation for the application of International Financial Reporting Standards (IFRS), the number of companies are in Ecuador and how many of them use computer applications for information processing in order to establish a clear context about the importance of managing the risk of information security, using several good practices such as COBIT, ISO 31000, ISO27005, MAGERIT or OCTAVE according to the needs of the companies.

Keywords: Information Technology, IFRS, COSO, Internal Control.

## Introducción

La información permite a las empresas establecer estrategias financieras, Comerciales u operativas independiente de su tamaño, giro de negocio o lugar en el que se encuentren domiciliadas, uno de los estándares que permite que esta información sea comparable y legible en cualquier parte del mundo son las normas internacionales de información financiera NIIF.

En Ecuador la superintendencia de compañías según resolución 08-G-DSC-010 del 20 de noviembre del 2008 estableció bajo 3 grupos la fecha límite para que las compañías adopten este estándar Tabla 1.

Tabla 1: Transición a NIIF por Tipo de Compañías

| Grupo | Fecha de aplicación | Tipo de compañías | Periodo de transición |
|---|---|---|---|
| 1 | 01/01/2010 | • Compañías y entes regulados por la Ley de Mercado de Valores.<br>• Compañías que ejercen actividades de auditoría externa. | 2009 |
| 2 | 01/01/2011 | • Compañías con activos totales iguales o superiores a 4'000.000 USD al 31 de diciembre de 2007.<br>• Las compañías Holding o tenedoras de acciones que voluntariamente hayan conformado grupos empresariales.<br>• Compañías de economía mixta.<br>• Entidades del sector público.<br>• Sucursales de compañías extranjeras u otras empresas extranjeras estatales, para estatales, privadas o mixtas, organizadas como personas jurídicas y las asociaciones que éstas formen y que ejerzan sus actividades en Ecuador. | 2010 |
| 3 | 01/01/2012 | • Compañías no consideradas en el grupo 1 y 2 | 2011 |

Fuente: Superintendencia de Compañías. Resolución 08-G-DSC-010
Elaborado por: el autor.

La conversión a NIIF es más que cambios contables y financieros. La adopción de esta norma tiene como efecto: cambio a los procesos operativos y políticas contables, modificación a las aplicaciones de tecnología de la información - TI, mayor inversión en la capacitación de recurso humano, cambio en los flujos de información y un nuevo enfoque para el análisis de la información generada debido a que se necesita de un mayor nivel de detalle para la información a revelar en los estados financieros.

El objetivo de este documento es analizar los tipos de riesgo relacionados desde el punto de vista de la tecnología de la información, así como las diferentes metodologías que existen para la evaluación de la efectividad del control interno que aseguren el correcto desempeño de sus componentes.

## Riesgos asociados a las Tecnologías de la Información

Según publicación del Diario El Hoy (2008):

> *"La aplicación de tecnología o informática en las tareas administrativas de las pequeñas y medianas empresas todavía no es suficiente en Ecuador. De las 300 mil que existen en el país, solo el 40% cuenta con un programa tecnológico. Según un estudio de Memory Computación, el miedo al uso de la tecnología y, sobre todo, la creencia de que es un producto caro son las razones fundamentales que alejan a los dueños de las empresas de las soluciones informáticas: desde el manejo de caja y facturación a un sofisticado sistema para banco. El acceso a programas básicos puede costar entre $600 y $3.000, aunque también hay soluciones informáticas más integrales cuyos costos llegan hasta los $100 mil".*

Para el año 2014 la superintendencia de compañías informa en su anuario estadístico societario la existencia de 55.619 empresas (Tabla 2), donde el mayor porcentaje se encuentra concentrado entre las pequeñas y microempresas con el 81%.

El Banco Interamericano de Desarrollo – BID, indica que en el Ecuador para el año 2006 el 80% de las empresas son de carácter familiar, y tan solo el 4% se mantiene bajo el principio de negocio en marcha hasta la cuarta generación, situación que evidencia un ciclo de vida empresarial cortó. (Jara Soliz et al., 2013).

La importancia de conocer estos datos y su relación con el uso de tecnologías de la información y la implementación de NIIF radica en el comportamiento proporcional que existe entre el tamaño de la empresa y las operaciones (transacciones productivas, comerciales y administrativas) que van a procesar en sus aplicaciones y los riesgos inherentes a los que está expuesta esta información de tener un sistema de control interno deficiente o peor aún carecer de uno.

Debido a la alta complejidad del reporte financiero bajo NIIF, el control interno para procesos financieros y administrativos debe ser reforzado o implementado en las empresas por medio de la gerencia financiera, mientras que en los procesos de tecnología y seguridad de la información por el responsable del área de sistemas de

información y comunicación. De acuerdo al tamaño de la compañía o de sus operaciones es necesario contar con un área de auditoría interna que apoye en el aseguramiento a las políticas y procedimientos que fortalezcan el ambiente de control, el gobierno corporativo, el gobierno de TI y la seguridad de la información.

Tabla 2: Tipo de Compañías – Movimientos Financieros 2014

| Tipo de compañía[1] | Cantidad | | Activo | | Pasivo | | Patrimonio | | Ingresos | |
|---|---|---|---|---|---|---|---|---|---|---|
| | No. | % | USD | % | USD | % | USD | % | USD | % |
| Grande | 3.038 | 5 | 65.707.432.198 | 72 | 39.618.076.678 | 73 | 26.089.355.526 | 71 | 86.145.654.312 | 81 |
| Mediana | 7.332 | 13 | 12.741.031.540 | 14 | 7.683.614.890 | 14 | 5.057.416.649 | 14 | 14.033.813.953 | 13 |
| Pequeña | 17.919 | 32 | 8.009.712.785 | 9 | 4.532.057.915 | 8 | 3.477.630.655 | 9 | 5.816.881.330 | 5 |
| Micro | 27.312 | 49 | 5.052.740.337 | 6 | 2.687.441.788 | 5 | 2.365.034.912 | 6 | 673.229.850 | 1 |
| No definido | 18 | 0 | 14.460 | 0 | 1.256 | 0 | 13.204 | 0 | 0 | 0 |
| **Total** | **55.619** | **100** | **91.510.931.319** | **100** | **54.521.192.528** | **100** | **36.989.450.947** | **100** | **106.669.579.445** | **100** |

Fuente: Anuario estadístico - Superintendencia de Compañías, por tamaño de compañías.
Elaborado por: el autor.

Para hablar de controles a nivel de TI en un proceso de adopción y reporte bajo NIIF primero debemos entender los riesgos tecnológicos a los que están expuestas las empresas. Kincaid James (2008), en la guía de estudio para el examen de certificación en autoevaluación de control – CCSA, define al riesgo como: "la probabilidad de que ocurra un evento que pueda tener un impacto en el alcance de los objetivos. El riesgo se mide en términos de consecuencias y probabilidad de que este ocurra.". Por otro lado, ISACA (2013) define al riesgo tecnológico en su guía COBIT 5 para riesgos como "…el riesgo de negocio asociado con el uso, propiedad,

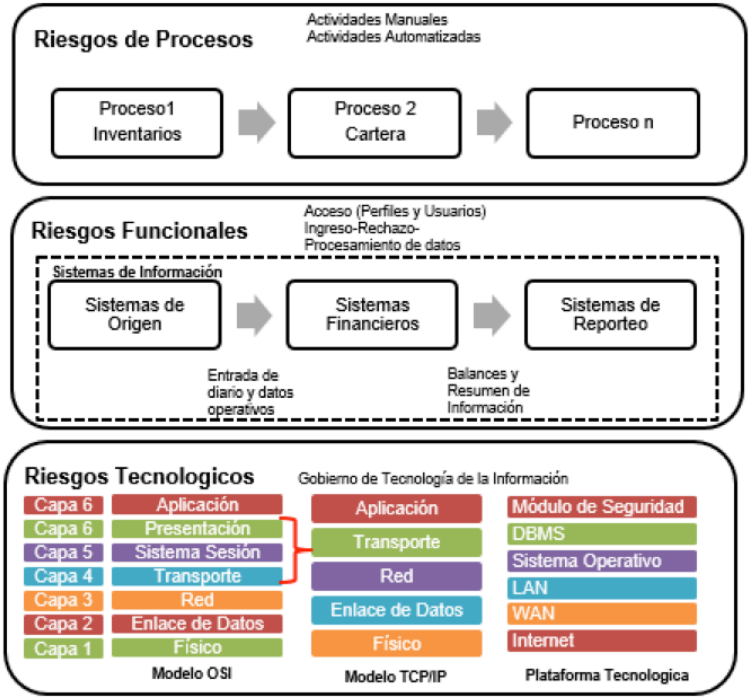
1 Tipo de compañíasdefinido de acuerdo al Código Orgánico de la Producción, Comercio e Inversiones donde:
Microempresas: entre 1 a 9 trabajadores o ingresos menores a 100.000
Pequeña empresa: entre 10 a 49 trabajadores o ingresos entre 100.001 y 1'000.000
Mediana empresa: entre 50 y 199 trabajadores o ingresos entre 1'000.001 y 5'000.000
Empresa grande: más de 200 trabajadores o ingresos superiores a 5'000.001

operación, participación, influencia y adopción de TI dentro de un empresa…". Bajo este nuevo enfoque de ISACA el riesgo de tecnología es parte integral del modelo de negocio sin importar su tamaño o giro y se alinea con los 7 facilitadores que plantea COBIT 5.

Por lo tanto, los riesgos analizados desde el punto de vista del negocio o de tecnología afectan al cumplimiento de los objetivos de las organizaciones, siendo lo más recomendable la implementación de modelos de gestión de riesgos que permitan su categorización (riesgos estratégicos, operacionales, de reportes y de cumplimiento) identificación, y gestión.

La firma de consultoría PriceWaterHouse (2010) establece 3 tipos de riesgos (Figura 1) a los que se exponen las empresas que hacen uso de sistemas informáticos para soportar sus procesos de negocio, estos son: riesgos de procesos de negocio, riesgos funcionales y riesgos de la función de tecnología de información.

Gráfico 1. Tipo de Riesgos Inherentes




Fuente: PriceWaterHouseCoopers, Boletin de Asesoria Gerencial No.5, 2010
Elaborado por: El autor

### *Riesgos de procesos*

Incrementan su probabilidad e impacto de acuerdo al nivel de automatización que tengan y el macroproceso que afecten, por ello es importante que la gerencia general apoye iniciativas para la elaboración y socialización de un código de ética y conducta, reglamento interno, políticas y procedimientos que ayuden a controlar y mitigar estos riesgos.

### *Riesgos funcionales*

Los riesgos funcionales están a nivel de los sistemas de información y la arquitectura de sistemas y pueden ser en la autenticación, ingreso y procesamiento de la Información.

a. Durante la autenticación la correcta definición de perfiles de usuario permite controlar:

· Acceso no autorizado a transacciones o información sensibles, por ejemplo: personal del área comercial que pueda modificar o visualizar información relacionada a clientes.

· Falta de segregación de funciones, a fin de mitigar riesgos de fraude, por ejemplo: personal del área de comercial que pueda ingresar pedidos, facturar y despachar, modificar precios y descuentos sin un nivel de autorización, modificar las características de crédito de un cliente, son eventos que podrían desencadenar un posible fraude.

· Falta administración de usuarios y claves de acceso a fin de mitigar acceso a información y ambientes restringidos, por ejemplo: instalación de programas sin licencia o peor aún que tengan algún virus.

b. En el ingreso de información uno de los mayores inconvenientes es el ingreso de información incorrecta, incompleta, o duplicada que a largo plazo puede ocasionar errores durante el procesamiento de la información, por ejemplo: códigos duplicados de productos podrían ocasionar que durante una toma física se ingrese el conteo por duplicado generando a largo plazo inventarios sobrevalorados y existencias ficticias de productos.

c. Actualmente los sistemas cuentan o permiten validar campos requeridos como RUC o cédula. Así también existen controles a nivel de aplicación (logs de auditoría) para que el sistema reporte cambios o modificaciones atípicas para que según el nivel de automatización de estos controles sean monitoreados mitigando así riesgos de rechazo y procesamiento.

Es muy importante el análisis de los controles a implementar a nivel de procesamiento ya que un exceso de control podría restar funcionalidad por bajo rendimiento de procesamiento a la aplicación y generar cuellos de botella.

### *Riesgos de la función de Tecnología de la Información - TI*

La estructura del área de TI debe estar correctamente definida a fin de mantener un gobierno de TI que ayude a la empresa al logro de objetivos. La falta de una correcta administración de TI puede ocasionar que existan eventos de riesgo (Tabla 3) que impactan directamente en el nivel de confianza al reporte y por lo tanto en NIIF. Si bien, en la actualidad TI es considerado como un proceso de soporte, es de vital importancia su adecuada gestión ya que esta aporta al desarrollo normal de otros procesos dentro de las empresas.

Tabla 3: Factores de Riesgo Tecnológicos

| **Factor de riesgo** | **ISO 27001: Principios** | | |
|---|---|---|---|
| | **Integridad** | **Confidencialidad** | **Disponibilidad** |
| Nivel de servicio bajo | | | X |
| Fuga de datos | X | X | |
| Soporte inadecuado | | | X |
| Falta de aseguramiento | X | | |
| Excedentes presupuestales | N/A | N/A | N/A |
| Retrasos importantes | | | X |
| Baja calidad de los entregables | X | | X |
| Control de cambios ineficaz | X | | |
| Intrusión de software malicioso | X | X | X |
| Ataques de virus | X | X | X |
| Ataques a sitios web | X | X | X |
| Mala administración de parches | X | | X |
| Fallas en los servicios públicos | | | X |
| Desastres naturales | | | X |
| Huelgas | | | X |
| Sanciones ambientales | | | X |
| Pérdida de recursos clave de TI | | X | |
| Incapacidad para reclutar personal de TI | | | X |
| Habilidades inadecuadas | X | | X |
| Falta de conocimiento del negocio | X | | X |

| | | | |
|---|---|---|---|
| Errores del operador durante el respaldo o mantenimiento | X | | X |
| Fallas en los procesos operativos | X | | X |
| Revelación de datos sensibles | | X | |
| Corrupción de datos | | X | |
| Acceso no autorizado | | X | |
| Falla en minar la información | X | | X |
| Daño a los servidores | X | | X |
| Arquitectura de TI inflexible | | | X |
| Robo | | X | |
| Tecnología obsoleta | | | X |
| Aplicaciones no soportadas | X | | X |
| Fallas críticas del sistema | X | | X |
| Incapacidad para manejar la carga | X | | X |
| Asuntos de configuración | X | | X |
| Incumplimiento con reglamentos | | | X |
| Incumplimiento con contratos de licencias de software | | | X |

Fuente: Perspectivas sobre los riesgos de TI, en el panorama de los riesgos de TI, Integrante de Erns & Young Global, 2012 Mancera S.C
Elaborado por: El autor

La evolución de la tecnología y la masificación en el acceso a internet, en la última década, ha ocasionado el uso en casi todas las actividades humanas de dispositivos tecnológicos; que van desde el uso de una computadora de escritorio hasta la gestión de otros dispositivos de nuestros hogares u oficinas a través de un Smartphone, situación que ya hace varios años se conoce como el Internet de las Cosas o IoT. Esta situación genera riesgos contra los principios de la seguridad de la información tanto para las empresas como para las personas, pues con esto el crimen tradicional ha migrado a la web como "Cibercrimen" donde los ataques van el acceso no autorizado a la red, suplantación de identidad hasta el secuestro de la información "ransomware", eventos que con una adecuada capacitación y gestión puede ser en cierta forma mitigada o eliminada.

## Normas de Gestión de Riesgos y Control Interno

Las Normas de Auditoría Generalmente Aceptadas (NAGAS) son principios de general aplicación que permiten al Auditor garantizar calidad en su trabajo profesional. Adicional a la aplicación de las NAGAS, se deben cumplir con las disposiciones de las Normas Internacionales de Auditoría y Aseguramiento (NIAS) y para el caso de Auditoría Interna lo establecido en el Marco Internacional para la Práctica Profesional de la Auditoría

Interna (IPPF). En el caso de Ecuador para el caso de las Instituciones del Sector Público el área de Auditoría debe cumplir con las Normas de la Contraloría General del Estado.

El alto flujo de información que manejan las aplicaciones informáticas asociadas a procesos de negocio requieren un tratamiento especial que permita precautelar la integridad, confidencialidad y disponibilidad, y a la vez permita mejorar significativamente la gestión de la información, ha generado preocupaciones ante su vulnerabilidad, es por ello que se han establecido marcos referenciales de control.

Las metodologías de mayor difusión y uso para gestión gobierno de TI y de riesgos son COBIT y COSO ERM respectivamente, sin embargo, para gestión de riesgos de TI existen otras metodologías como MAGERIT, OCTAVE, NIST 800-30, que se aplican de acuerdo al criterio del consultor o personal de riesgos de la entidad, a continuación, un análisis:

Tabla 4: Metodologías de Gestión de Riesgos de Tecnología

| No. | Modelo | Creador | Objetivo | Estructura | Elementos |
|---|---|---|---|---|---|
| 1 | ISO 31000: 2009 - Gerencia de Riesgos | International Organization for Standardization - ISO | Integrar el proceso de gestión de riesgo en el gobierno corporativo de la organización, planificación y estrategia, gestión, procesos de información, políticas, valores y cultura. | 1. Principios.<br>2. Marco de trabajo.<br>3. Proceso de gestión del riesgo | 1. Establecer contexto<br>2. Evaluación de Riesgos<br>3. Identificación de los Riesgos.<br>4. Análisis de los Riesgos<br>5. Evaluación de los Riesgos.<br>6. Tratamiento de los Riesgos.<br>7. Monitoreo y Revisión.<br>8. Comunicación y Consulta. |
| 2 | ISO 27005: 2008 Técnicas de Seguridad - Administración de Riesgos de Seguridad | International Organization for Standardization - ISO | Proporcionar lineamientos para la administración de riesgos de seguridad de la información de una organización y brindar soporte a los requerimientos de la ISO 27001, sin embargo, no provee una metodología específica para la gestión de riesgos de seguridad de la información. | 1. Principios.<br>2. Marco de trabajo.<br>3. Proceso de gestión del riesgo | 1. Establecer contexto<br>2. Evaluación de Riesgos<br>3. Identificación de los Riesgos.<br>4. Análisis de los Riesgos<br>5. Evaluación de los Riesgos.<br>6. Tratamiento de los Riesgos.<br>7. Monitoreo y Revisión.<br>8. Comunicación y Consulta. |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT | Consejo Superior de Administración Electrónica - CSAE | 1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.<br><br>2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).<br><br>3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control. | 1. Libro I - Método<br><br>2. Libro II - Catálogo de elementos.<br><br>3. Guía de técnicas. | 1. Activos.<br>2. Amenazas.<br>3. Salvaguardas.<br>4. Impacto Residual.<br>5. Riesgo Residual. |
| 4 | Operationally Critical Threats Assets and Vulnerability Evaluation - OCTAVE | Instituto de Ingeniería de Software | 1. Desmitificar la creencia de que la Seguridad Informática es un asunto meramente técnico.<br><br>2. Presentar los principios básicos y la estructura de las mejores prácticas internacionales que guían los asuntos no técnicos. | 1. Método OCTAVE.<br><br>2. Método OCTAVE - S.<br><br>3. Método OCTAVE - ALLEGRO. | 1. Identificación de la información a nivel gerencial.<br>2. Identificación de la información a nivel operacional.<br>3. Identificación de la información a nivel de usuario final.<br>4. Consolidación de la información y creación de perfiles de amenazas.<br>5. Identificación de componentes claves.<br>6. Evaluación de componentes seleccionados.<br>7. Análisis de riesgos de los recursos críticos.<br>8. Desarrollo de estrategias de protección. |

| | | | | | |
|---|---|---|---|---|---|
| 5 | National Institute of Standars and Technology - NITS | Instituto Nacional de Estándares y Tecnología | Desarrollar un documento de interés general sobre la Seguridad de la Información, que permitan asegurar el progreso e innovación tecnológica de cuatro áreas en particular: biotecnología, nanotecnología, tecnologías de la Información, y fabricación avanzada. | 1. Categorizar - Sistemas de Información.<br>2. Seleccionar - Controles de Seguridad.<br>3. Implementar - Controles de Seguridad.<br>4. Evaluar - Controles de Seguridad.<br>5. Autorizar - Sistemas de Información.<br>6. Monitorear - Controles de Seguridad. | 1. Caracterización del sistema.<br>2. Identificación de amenaza.<br>3. Identificación de vulnerabilidades.<br>4. Control de análisis.<br>5. Determinación del riesgo.<br>6. Análisis de impacto.<br>7. Determinación del riesgo.<br>8. Recomendaciones de control.<br>9. Resultado de la implementación o documentación. |
| 6 | Risk IT de ISACA | Asociación de Auditoría y Control de Sistemas de Información - ISACA | Aplicar los conceptos generalmente aceptados de los principales estándares y marcos, así como los principales conceptos de la gestión de otros riesgos de TI, relacionados con las normas. | 1. Marco completo para gestión de riesgos de TI. | 1. Gobierno del riesgos (GR)<br>1.1 RG1 Establecer y mantener una vista de riesgo común.<br>1.2 RG2 Integrar con ERM.<br>1.3 RG3 Tomar decisiones conscientes de los riesgos del negocio.<br>2. Evaluación de riesgos (RE)<br>2.1 RE1 Recoger datos.<br>2.2 RE2 Analizar los riesgos.<br>2.3 RE3 Mantener perfil de riesgo.<br>3. Respuesta de riesgos<br>3.1 RR1 Riesgo articulado<br>3.2 RR2 Manejar riesgos<br>3.3 RR3 Reaccionar a acontecimientos |

Elaborado por: El autor

## Conclusiones

Considerando que hoy en día la tecnología de la información es usada en todas las organizaciones, independientemente de su tamaño o giro de negocio para el procesamiento de sus operaciones y la generación de información para la toma de decisiones, es importante conocer los riesgos a los que dicha información está expuesta a fin de diseñar, implementar y monitorear controles.

Una vez implementado NIIF, es importante que las compañías mantengan una relación costo-beneficio al implementar controles, ya que el costo de un control no debe exceder los beneficios a recibir de la mitigación de un riesgo.

El desarrollo de cada una de las metodologías expuestas a nivel general en el presente documento es necesario para entender el alcance de cada uno, y poder adaptarlo a la realidad de cada empresa logrando así aportar al logro de los objetivos.

# Bibliografía

Diario El Hoy. (18 de Febrero de 2008). Explored, Archivo Digital de Noticias desde 1994. Obtenido de Explored, Archivo Digital de Noticias desde 1994: http://www.explored.com.ec/noticias-ecuador/la-oferta-de-profesionales-supera-la-demanda-289263.html

INSTITUTO DE AUDITORES INTERNOS DEL ECUADOR. (2013). Taller de Mapas de Riesgos Corporativos. Quito.

ISACA. (2013). Cobit for Risk. Rolling Meadows, IL 60008 USA: ISACA.

ISACA. (s.f.). Marco de Riesgos de TI. ISACA.

IT GOBERNANCE INSTITUTE. (2007). COBIT 4.1. Estados Unidos.

JAMES, K. (2008). CCSA - Certificación en Autoevaluación de Control - Guía de Estudio Para el Examen. Florida: IIARF.

Coopers, P. (Mayo de 2010). Boletin de Asesoría Gerencial. Obtenido de https://www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/edicion-05-2010.pdf

Ernst and Young, Mancera S.C. (2012). Cambios en el panorama de los riesgos de TI, El porqué y el cómo de la actual Administración de TI. Perspectivas sobre los riesgos de TI, 5.

Garriga, D. C. (2016). Softonic. Obtenido de https://articulos.softonic.com/virus-ransomware-2016-secret-level

Maldonado, P. (2016). Revista Lideres. Obtenido de http://www.revistalideres.ec/lideres/empresarios-valoran-magnitud-riesgo-informatico.html