GOBIERNO Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y ASPECTOS DIFERENCIADORES CON EL RIESGO ORGANIZACIONAL

GOVERNMENT AND IT RISK MANAGEMENT AND ASPECTS DIFFERENTIATORS WITH THE ORGANIZATIONAL RISK

AUTOR
FRANCISCO JAVIER VALENCIA D.
PhD en Ingeniería, Industria y Organizaciones
*Universidad Nacional de Colombia
Profesor Asociado
Departamento de Informática y Computación
fjvalenciad@unal.edu.co
COLOMBIA

AUTOR
CARLOS EDUARDO MARULANDA
PhD(c) en Ingeniería, Industria y Organizaciones
*Universidad Nacional de Colombia
Profesor Asociado
Departamento de Administración
cemarulandae@unal.edu.co
COLOMBIA

AUTOR
MARCELO LÓPEZ TRUJILLO
PhD en Ingeniería Informática, Sociedad de la Información y del Conocimiento
**Universidad de Caldas
Profesor titular
Departamento de Sistemas e informática
mlopez@ucaldas.edu.co
COLOMBIA

***INSTITUCIÓN**
Universidad Nacional de Colombia
Sede Manizales
UNAL
Universidad Pública
Kra 27 Nro 64-60
Manizales (Caldas)
dima_man@unal.edu.co
COLOMBIA

****INSTITUCIÓN**
Universidad de Caldas
Unicaldas
Universidad Pública
Calle 65 Nro 26 – 10
Manizales (Caldas)
ucaldas@ucaldas.edu.co
COLOMBIA

INFORMACIÓN DE LA INVESTIGACIÓN O DEL PROYECTO: Este artículo es parte de los resultados del proyecto de investigación titulado "Diseño de un modelo integrado de aseguramiento de tecnologías de información y comunicaciones, basado en estándares internacionales" con código Hermes 32050 correspondiente a la convocatoria interna de investigación de la Facultad de Administración 2015 de la Universidad Nacional de Colombia sede Manizales. El objetivo del proyecto es el diseño de un modelo integrado de aseguramiento de tecnologías de información y comunicaciones, aplicables a cualquier tipo de organización.

RECEPCIÓN: 24 de Enero de 2016 **ACEPTACIÓN:** 14 de Marzo de 2016

TEMÁTICA: gestión tecnológica

TIPO DE ARTÍCULO: artículo de investigación científica e innovación

Forma de citar: Valencia, F. J. (2015). Gobierno y gestión de riesgos de tecnologías de información y aspectos de información y aspectos diferenciadores con el riesgo organizacional. En R, Llamosa Villalba (Ed.). Revista Gerencia Tecnológica Informática, 14(40), 65-77. ISSN 1657-8236.

RESUMEN ANALÍTICO

Las tecnologías de información y comunicaciones como parte inherente del negocio, son consideradas un factor clave en la productividad y competitividad de una organización, de allí que los riesgos derivados de su operación se convierten en aspectos críticos que requieren ser tratados a través de un adecuado gobierno y gestión. Es por ello que normas internacionales como la ISO 38500:2008 y marcos de referencia como COBIT establecen lineamientos en materia de riesgos como parte del gobierno y gestión de riesgos de tecnologías de información, que son complementados con las diversas metodologías de riesgos de tecnologías de información que han promulgado diferentes organizaciones a nivel internacional y que a partir de diversos trabajos académicos y profesionales han realizado propuestas de similitudes entre sus estructuras, incluso con las metodologías de riesgo organizacional, lo que nos lleva a determinar dos aspectos críticos que las diferencian: los activos objeto de análisis y los factores de impacto a evaluar, los cuales requieren especial atención al momento de desarrollar un proceso de gestión de riesgos. En este sentido se realiza una propuesta que aporte a la comunidad académica y profesional al desarrollo de un proceso de gestión de riesgos en el contexto de las tecnologías de información y en particular a la clasificación de los activos tecnológicos en doce (12) capas y a la evaluación de su impacto en función de la triada Confidencialidad, Integridad y Disponibilidad.

PALABRAS CLAVES: riesgos de TI, gobierno y gestión de riesgos de TI, metodologías de riesgos de TI, activos tecnológicos.

ANALYTICAL SUMMARY

The information technology and communications as an inherent part of the business, are considered a key factor in the productivity and competitiveness of an organization, hence the risks arising from their operations become critical issues that need to be addressed through appropriate government and management. That is why international standards such as ISO 38500:2008 and frameworks like COBIT establish guidelines on risk as the government and risk management information technology, which are complemented with diverse methodologies risks of information technologies that have enacted different organizations worldwide and from various academic and professional work has made proposals similarities between their structures, even with the methodologies of organizational risk, which leads us to determine two critical aspects that differentiate them, the assets of analysis and impact factors to evaluate, which require special attention when developing a risk management process. In this sense a proposal that contributes to the academic and professional development of a risk management process in the context of information technology and in particular the classification of the technology assets in twelve (12) layers is carried out and impact assessment based on the triad Confidentiality, Integrity and Availability.

KEYWORDS: IT risk, governance and management of IT risk, IT risk methodologies, technology assets.

INTRODUCCIÓN

Las Tecnologías de Información y Comunicaciones han dejado de ser tan solo herramientas de apoyo para convertirse en parte del negocio, y como tal ejercen una influencia directa en la productividad y competitividad organizacional. De allí que sean consideradas recursos estratégicos vitales, para el desarrollo de cualquier organización. Sin embargo, como cualquier recurso, es vulnerable a múltiples amenazas que se pueden materializar en riesgos, con diversos impactos en términos de pérdida de datos, interrupción de servicios, pérdidas financieras, daños a la reputación e incluso pérdidas humanas.

Amenazas tan comunes como los virus, los fallos de software, las caídas de red, los programas espía, troyanos, los robos de equipos, el spam, hasta amenazas tan sofisticadas como las denominadas amenazas persistentes avanzadas (APT, por sus siglas en inglés Advanced Persistent Threat), o los ataques día cero (en inglés, zero-day attack) a las cuales está

expuesta cualquier organización, lleva a la necesidad de valorarlos y a partir de allí tomar acciones que permitan implementar adecuados controles para tratar de garantizar niveles aceptables de riesgo.

Todas las actividades orientadas a mantener niveles aceptables de riesgo en una organización, está en el marco de lo que se denomina gobierno y gestión del riesgo, en este caso en particular, y como parte del universo de riesgos organizacionales, todos aquellos procesos relacionados con los riesgos de Tecnologías de Información y Comunicaciones (en adelante TIC o TI), están en el marco del gobierno y gestión de riesgos de TIC.

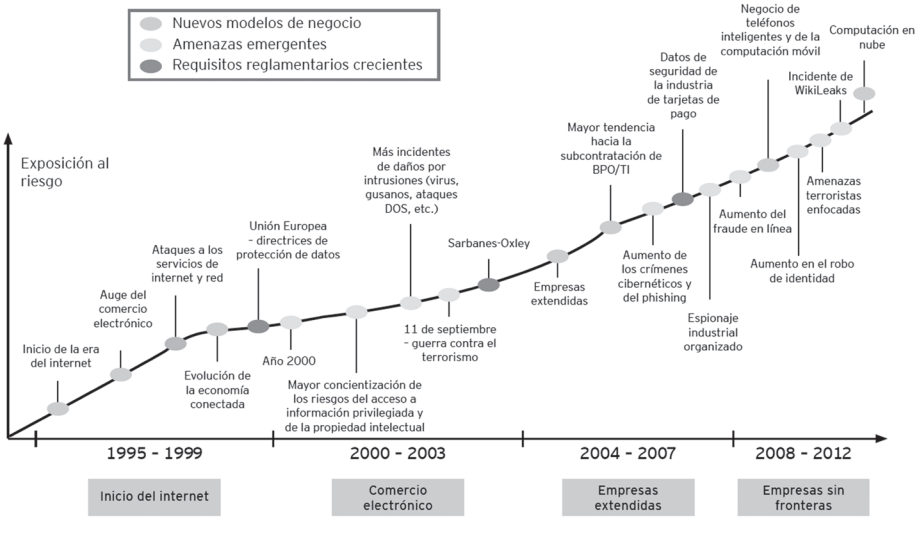
Este articulo pretende poner en contexto el gobierno y gestión de riesgos de tecnologías de información (en adelante GgRTIC), como parte integral del gobierno y gestión de tecnologías de información, para lo cual se analizarán los principales marcos de referencia existentes, los modelos de riesgos de TIC propuestos por diferentes organizaciones a nivel internacional y plantear en detalle los principales componentes que diferencia un modelo de riesgos organizacional, de un modelo de riesgos de TIC, para lo cual se plantea como principal aporte y diferenciador de la gestión de riesgos organizacional, un modelo de clasificación de los activos tecnológicos en doce (12) capas y una propuesta de parámetros de impacto basados en la triada Confidencialidad, Integridad y Disponibilidad.

1. GOBIERNO Y GESTIÒN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Los riesgos de TIC han estado presentes en la evolución de los diferentes modelos de negocio y reglamentaciones que han surgido a través del tiempo, tal como se puede observar en la figura 1, lo que pone de manifiesto que cualquier riesgo tecnológico no puede ser analizado al margen del contexto organizacional dado su efecto dominó sobre sus procesos, metas y objetivos. Ello conlleva un proceso de articulación entre las actividades de riesgo organizacional y riesgo de TIC, y en particular desarrollar iniciativas de GgRTIC.

El concepto de gobierno y gestión de riesgos de TIC surge a partir de la noción de gobierno y gestión de TIC. Entendido el gobierno de TI, tal como lo establece el estándar internacional ISO/IEC 38500:2008 como un sistema por el que se dirige y controla la utilización actual y futura de las TIC [1]. Por su parte la gestión de TI, se centra en administrar e implementar la estrategia tecnológica del día a día, y su enfoque está más orientado al suministro interno de TI, definido de igual forma por la norma internacional como el sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización, y está sujeta a la guía y monitoreo del gobierno de TI.

FIGURA 1. Evolución de las amenazas con los modelos de negocios y las reglamentaciones.



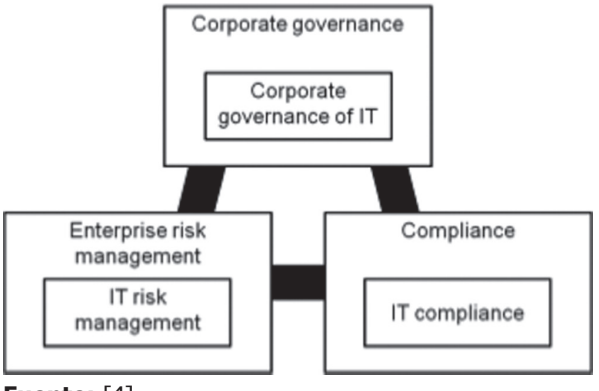
Fuente: [2]

En coherencia con lo expuesto, el gobierno de riesgos de TIC, es el sistema por el cual se dirigen y controlan las incertidumbres presentes y futuras que generan las tecnologías de información en la organización, mientras que la gestión de riesgos de TIC se centra en los procesos requeridos para garantizar niveles aceptables de riesgo de la información y de la infraestructura tecnológica incorporada en el día a día del negocio.

Los riesgos de tecnologías de información, son una disciplina asociada en el ámbito académico y profesional a siglas como ITRM (por sus siglas en ingles de Information Technology Risk Management), o ISRM (Information Security Risk Management), considerada según [3] una de las funciones esenciales del gobierno de Tecnología de Información, aunque desde una perspectiva mucho más amplia, está asociada a lo que se denomina IT GRC (Information Technology Governance Risk and Compliance).

El IT GRC, tal como se puede apreciar en la figura 2, es un subconjunto del GRC compuesto por tres cuerpos de conocimiento, el Gobierno de TI (IT governance), los riesgos de TI (IT Risk) y el cumplimiento regulatorio y normativo de TI (IT compliance) que actúan de forma integrada.

FIGURA 2. IT GRC como parte del GRC



Fuente: [4]

1.1 LOS RIESGOS DE TECNOLOGÌA DE INFORMACIÒN EN LOS PRINCIPALES MARCOS DE REFERENCIA DE GOBIERNO Y GESTIÒN DE TIC

"La gestión de riesgos es un método sistemático que permite planear, identificar, analizar, evaluar, tratar y monitorear los riesgos asociados con una actividad, función o proceso, para que la organización pueda reducir pérdidas y aumentar sus oportunidades"[5], en este caso las actividades, funciones, procesos y recursos que hacen parte de las Tecnologías de Información y Comunicaciones.

La norma ISO/IEC 38500:2008 contempla tanto en la definición de gobierno de TI, como en su estructura, los riesgos de TI, si bien no de manera explícita, si en su contexto al establecer el control como parte de la definición, lo que, en la lógica de las metodologías de gestión de riesgos, conlleva a la existencia de riesgos para poder definir controles.

Por su parte the IT Governance Institute (ITGI) e ISACA son mucho más explícitos, al establecer en COBIT 4.1 cinco (5) áreas de enfoque para establecer el gobierno de TI: alineamiento estratégico, entrega de valor, administración de riesgos, administración de recursos y medición del desempeño. Entendida la administración de riesgos como un área en donde los altos ejecutivos requieren concientizarse acerca de la evolución de las amenazas con los modelos de negocios y las reglamentaciones de los riesgos, a través de un claro entendimiento del apetito del riesgo, de la comprensión de los requerimientos de cumplimiento, la transparencia de los riesgos significativos y la inclusión de las responsabilidades de administración de riesgos dentro de la organización [6].

COBIT 5.0 (como evolución de COBIT 4.1.) es considerado actualmente uno de los principales referentes en materia de gobierno y gestión de tecnologías de información, de allí que contemple desde la perspectiva tanto de gobierno como de gestión de TI, el componente de riesgos.

Desde la perspectiva de gobierno de TI, COBIT 5.0 establece bajo el dominio evaluar, dirigir y supervisar (EDM por sus siglas en inglés Evaluate, Direct and Monitor), el proceso **EDM03 Asegurar la optimización del riesgo** y desde la perspectiva de gestión, el proceso **APO12 Gestionar el riesgo,** en el dominio alinear, planificar y organizar (APO).

El proceso de gobierno de TI, *EDM03 Asegurar la optimización del riesgo*, es descrito por [7] como un proceso requerido para asegurar que el apetito y la tolerancia al riesgo de una organización es entendido, articulado y comunicado y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado. Para lograrlo, ISACA a través de la guía de procesos catalizadores de COBIT 5.0. plantea tres áreas clave: **EDM03.01 Evaluar la gestión de riesgos**. Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado. **EDM03.02 Orientar la gestión de riesgos**. Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo. **EDM03.03 Supervisar la gestión de riesgos**. Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución.

El proceso de gestión de TI, *APO12 Gestionar el riesgo* permite identificar, evaluar y reducir los riesgos de TI de forma continua, dentro de los niveles de tolerancia establecidos por la dirección de la empresa. Para ello se contemplan 6 prácticas:

APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI. **APO12.02 Analizar el riesgo**. Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo. **APO12.03 Mantener un perfil de riesgo**. Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados. **APO12.04 Expresar el riesgo**. Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada. **APO12.05 Definir un portafolio de acciones para la gestión de riesgos**. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio. **APO12.06 Responder al riesgo**. Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

De manera complementaria, ISACA como parte de la familia de productos de COBIT 5.0, dentro de sus guías profesionales ha desarrollado *COBIT 5 para riesgos*, liberada en 2013 y dirigida específicamente a profesionales de riesgos, donde presenta dos perspectivas de riesgos: la perspectiva de la función de riesgos, centrándose en lo requerido para construir y mantener la función de riesgos en una organización; y la perspectiva de la gestión de riesgos, cuyo foco son los procesos orientados a identificar, analizar, responder y reportar los riesgos diariamente [8].

Finalmente, es necesario destacar que la esencia del proceso de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 es la gestión de riesgos.

1.2. CRISC UNA DE LAS PRINCIPALES CERTIFICACIONES EN RIESGOS DE TECNOLOGIAS DE INFORMACIÒN, PARA IMPULSAR EL GOBIERNO Y GESTIÒN DE RIESGOS DE TIC

Para llevar a cabo procesos de gobierno y gestión de riesgos de tecnologías de información, es necesario adquirir competencias que permitan garantizar un proceso ajustado no solo a las necesidades específicas de la organización, sino a las mejores prácticas existentes hasta el momento.

Una de las principales certificaciones que a nivel internacional existen en materia de gestión de riesgos de tecnologías de información es CRISC (Certified in Risk and Information Systems Control), catalogada por la encuesta IT skills and salary survey 2015 desarrollada por Global Knowledge y Windows IT Pro durante el tercer trimestre del 2014, como la certificación mejor valorada dentro de las certificaciones de tecnologías de información[9].

Esta certificación establecida en 2009 por ISACA, representa para aquellos profesionales de tecnologías de información que la obtienen, el respaldo de contar con conocimientos y experiencia práctica para integrar la gestión del riesgo organizacional con habilidades de control de sistemas de información. Ello se adquiere a partir de la aprobación del examen CRISC y demostrar experiencia como mínimo de tres (3) años consecutivos en al menos tres (3) de los cuerpos de conocimiento que contempla la certificación, además de adherirse al código de ética profesional de ISACA y aceptar cumplir con la política de educación continua de CRISC[10].

Dentro de los cuerpos de conocimiento que hacen parte de esta certificación y que le permiten a un profesional dar cobertura a los diferentes aspectos que contempla un adecuado proceso de gobierno y gestión de riesgos, se han establecido cinco (5) dominios de conocimiento: identificación, evaluación y estimación de riesgos; respuesta ante riesgos; monitoreo de riesgos; diseño e implementación de controles de sistemas de información; monitoreo y mantenimiento de controles de sistemas de información.

2. MARCOS DE REFERENCIA Y METODOLOGIAS DE GOBIERNO Y GESTIÒN DE RIESGOS DE TECNOLOGIAS DE INFORMACIÒN

En los últimos años han surgido una serie de marcos de referencia y metodologías que permiten materializar el proceso de gobierno y gestión de riesgos de TIC. Entre los que plantean marcos integrados de gobierno y gestión se destacan RISK IT y RISK FOR COBIT 5.0, mientras que las que establecen tan solo esquemas de gestión del riesgo son principalmente: MAGERIT, ISO/IEC 27005, NIST 800-30, OCTAVE, MEHARI, CRAMM, las cuales se caracterizaran de forma general a continuación.

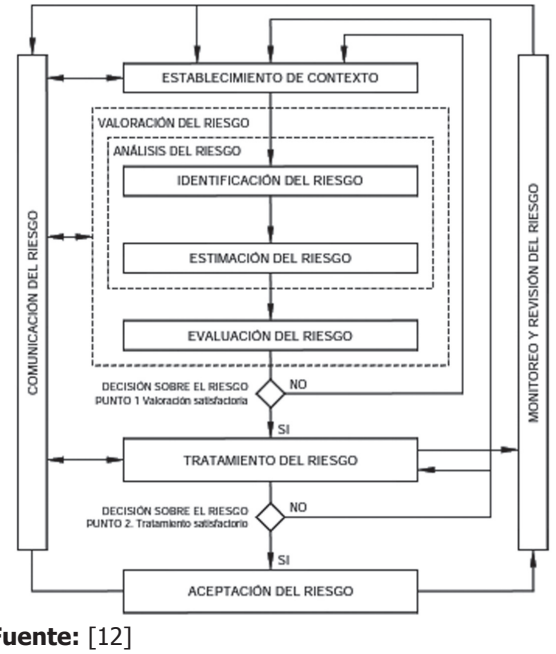
RISK IT: Esta iniciativa de ISACA, fue desarrollada como un complemento de COBIT, teniendo en cuenta el marco de controles que allí se plantean. RISK IT es un marco de riesgos de TI basado en un conjunto de principios, guías, procesos de negocio y directrices, conformado por tres ámbitos y nueve procesos interrelacionados, tal como se puede observar en la figura 3.

FIGURA 3. Marco de gestión de riesgos de RISK IT

Fuente: [11]

ISO/IEC 27005: Esta norma forma parte de la familia ISO 27000, publicada en 2008 y adoptada de forma idéntica en Colombia por ICONTEC en el año 2009, como NTC-ISO/IEC 27005**,** es la norma que proporciona directrices para la gestión de riesgos de Tecnologías de Información, dando soporte de manera particular a la norma ISO/IEC 27001:2013 del sistema de gestión de seguridad de la información. Su estructura es muy similar a la ISO 31000, tal como se puede observar en la figura 4.

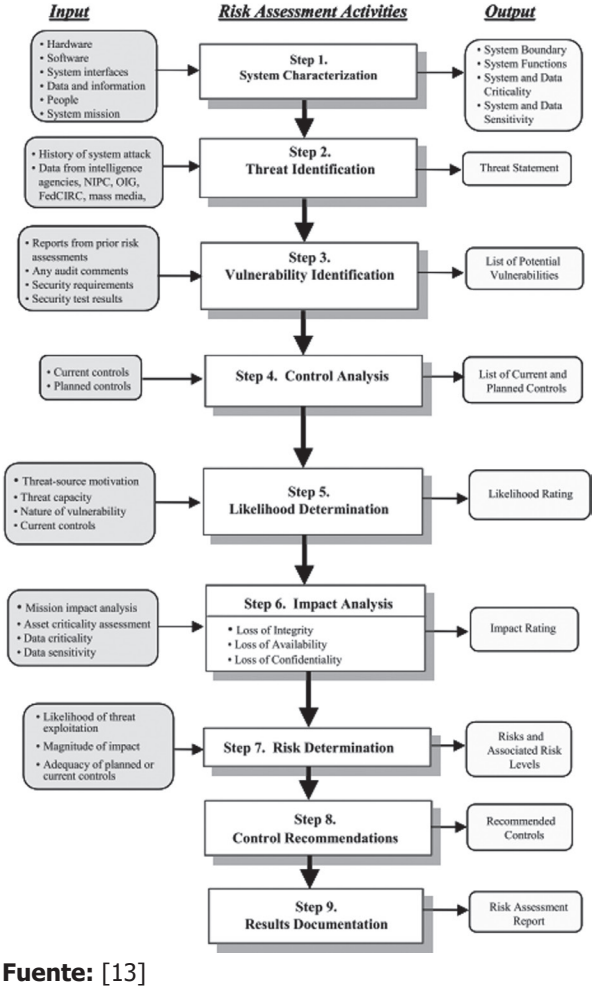
FIGURA 4. Proceso de gestión de riesgos de seguridad de la información de acuerdo a la ISO/IEC 27005:2009



Fuente: [12]

NIST 800-30: Es la guía para la administración de riesgos de Tecnologías de Información del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, aplicable a todas las Instituciones gubernamentales de este país y ampliamente referenciada. Plantea una estructura metodológica basada en 9 fases, tal como se puede apreciar en la figura 5.

FIGURA 5. Actividades de gestión de riesgos de la NIST 800-30.



Fuente: [13]

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation): es una colección de herramientas, técnicas y métodos para evaluar los riesgos de seguridad de la información, desarrollada por el Software Engineering Institute (SEI) de Carnegie Mellon [14], y cuenta con tres versiones: OCTAVE, OCTAVE-S y OCTAVE ALLEGRO. Cada una de estas versiones presenta algunas variaciones en relación a su concepción y a las actividades que se deben realizar en cada una de las fases.[15].

RISK FOR COBIT 5.0: es la visión más reciente de ISACA acerca de cómo se pueden gestionar los riesgos de TIC en el marco de COBIT 5.0, presentando dos perspectivas de cómo usar COBIT en un contexto de riesgos: la función de riesgos y la administración de riesgos. La perspectiva de función de riesgos se focaliza en lo que es necesario para construir una función de riesgos en una organización y la perspectiva de administración de riesgos se focaliza en los procesos de gobierno y gestión de riesgos[8].

MAGERIT: es la metodología de análisis y gestión de riesgos de los sistemas de información, utilizada en la Administración Pública Española, actualmente en su versión 3.0, consta de tres libros: El primero orientado a explicar el método, el segundo explicativo del catálogo de elementos y el tercero es una guía de las técnicas utilizadas en la metodología.

Como parte de la metodología se tiene un software que da soporte a todo el proceso denominada PILAR.

MEHARI: (Method for Harmonized Analysis of Risk) Método Armonizado de Gestión de Riesgos, fue desarrollado por el CLUSIF (Club de la Seguridad de la Información de Francia), desde 1996, con el fin de asistir a diferentes ejecutivos de la organización (Administradores operativos, Jefes de Sistemas, Administradores de riesgos, auditores) en su esfuerzo para gestionar la seguridad de la información y recursos asociados para reducir los riesgos asociados[16].

CRAMM: (CCTA Risk Analysis and Management Method) es una metodología desarrollada por el gobierno del Reino Unido, a través de la CCTA (Central Computer and Telecommunications Agency), su versión inicial surgió en 1987.

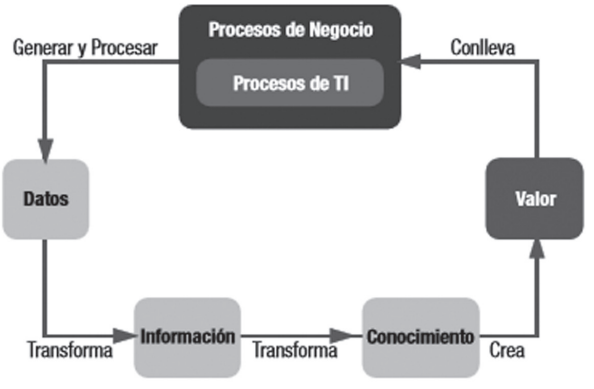
3. ASPECTOS DIFERENCIADORES DE UN PROCESO DE ITRM FRENTE A UNA GESTIÒN DE RIESGOS ORGANIZACIONAL

En la literatura académica y profesional se encuentran diversos trabajos orientados a realizar comparaciones entre las metodologías de gestión de riesgo organizacional y tecnológica y entre las mismas metodologías de ITRM. Trabajos como los desarrollados en [17], [18] que realizan comparaciones entre lo organizacional y lo tecnológico y análisis de relaciones entre las metodologías de riesgos de TIC, como las propuestas por [19],[20],[21] nos llevan a concluir desde el punto de vista metodológico, la existencia de fases comunes de cualquier proceso de riesgos, los cuales se resumen en: establecimiento de contexto, identificación de riesgos, análisis de riesgos, valoración de riesgos, plan de tratamiento de riesgos, comunicación y consulta y monitoreo, siendo dos de los aspectos diferenciadores entre un proceso de gestión de riesgos organizacional y un proceso de gestión de riesgos de tecnologías de información, los activos objeto de análisis y los parámetros con los cuales se mide su impacto, los cuales serán descritos en detalle a continuación.

3.1 LA INFORMACIÒN, LOS SERVICIOS E INFRAESTRUCTURA TIC COMO ACTIVOS OBJETO DE PROTECCIÒN DEL ITRM

El ciclo de información de una empresa, tal como se puede observar en la figura 6, nace a partir de la generación y procesamiento de los datos, los cuales son transformados en información y conocimiento, creando valor para la empresa, a través de la cual se toman decisiones que permiten el funcionamiento de la organización en sus diferentes niveles: operativo, táctico y estratégico.

FIGURA 6. Ciclo de la información.



Fuente: [22]

El proceso de gestión de la información puede ser llevado a cabo de forma manual o con el uso de TIC, siendo esta última la forma más generalizada actualmente para su tratamiento, lo que nos lleva a utilizar los diferentes activos tecnológicos para garantizar eficacia y eficiencia en el tratamiento de la información.

A partir de lo expuesto previamente, los riesgos de TIC cubren por lo general dos tipos de recursos, la información y los activos tecnológicos, sin embargo, frente a la evolución de la función de Tecnologías de Información, ha surgido un tercero, denominado servicios de TIC, como concepto integrador de recursos y cuyo origen se da al pasar de un una gestión de recursos tecnológicos a una gestión de servicios de Tecnologías de Información (ITSM por sus siglas en inglés Information Technology Service Management).

En este sentido, las organizaciones cuentan con una gran cantidad y variedad de activos tecnológicos, lo cual requiere de esquemas conceptuales que permitan tener una visión holística de ellos para su adecuada

protección. Dentro de las propuestas existentes a este requerimiento, se encuentran tres modelos, el propuesto por la Unión Internacional de Telecomunicaciones (ITU siglas en inglés de International Telecomunication Union), el de Microsoft y el de MAGERIT.

La ITU ha planteado un modelo denominado arquitectura de seguridad para sistemas de comunicaciones extremo a extremo, como se puede observar en la figura 7, desarrollado a través de la recomendación UIT-T X.805, donde se definen los elementos de seguridad generales de la arquitectura que son necesarios para garantizar la seguridad extremo a extremo.

FIGURA 7. Arquitectura de seguridad extremo a extremo.

Fuente: Adaptado de [23]

El modelo propuesto por Microsoft, denominado modelo de seguridad en profundidad o defensa en profundidad, cuyo principio está basado en una estrategia militar que tiene como objetivo demorar el avance del oponente al mantener múltiples capas de defensa y no solo una fuerte línea defensiva, tal como se puede observar en la figura 8.

FIGURA 8. Modelo de seguridad en profundidad.

Fuente: [24]

Por último, MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), uno de los principales referentes a nivel internacional para la gestión de riesgos de Tecnologías de Información, desarrollado por el Ministerio de Hacienda y Administraciones Públicas de España, contempla la clasificación propuesta en la tabla 1.

TABLA 1. Capas tecnológicas de MAGERIT versión 3.0.

ACTIVOS ESENCIALES	
INFORMACIÓN	SERVICIOS
ACTIVOS SUBORDINADOS A LOS ACTIVOS ESENCIALES	
DATOS	
SERVICIOS AUXILIARES	
APLICACIONES INFORMÁTICAS	
EQUIPOS INFORMÁTICOS	
SOPORTES DE INFORMACIÓN	
EQUIPAMIENTO AUXILIAR	
REDES DE COMUNICACIONES	
INSTALACIONES	
PERSONAS	

Fuente: Construido a partir de [25]

Es importante tener en cuenta que el recurso más valioso para las organizaciones es la información, y las TIC son el medio para su adecuado procesamiento, de allí la necesidad de diferenciar ambos tipos de activos que son objeto de análisis en los procesos de gestión de riesgos.

A partir de estos modelos y siendo coherentes con el planteamiento inicial de los tres tipos de activos tecnológicos, se propone un modelo compuesto por 12 capas tecnológicas interdependientes y organizadas de forma tal que, en caso de falla de alguna de ellas, puede generar un efecto dominó sobre las demás, lo que lleva a contemplar una gestión de riesgos integral, tal como se puede observar en la figura 9.

FIGURA 9. Capas de tecnologías de información y comunicaciones.

1	PROCESOS DE NEGOCIO
2	SERVICIOS DE TI
3	DATOS/INFORMACIÓN/CONOCIMIENTO
4	SISTEMAS DE INFORMACIÓN TRANSACCIONALES
5	SISTEMAS DE INFORMACIÓN SOPORTE
6	MOTORES DE BASES DE DATOS
7	SISTEMAS OPERATIVOS
8	PC's DE ESCRITORIO E IMPRESORAS
9	SERVIDORES (Físicos, virtuales y en la nube)
10	CENTROS DE REDES Y CABLEADO
11	CENTROS DE COMPUTO
12	ENERGIA

Una descripción general de cada una de estas capas, se presenta a continuación:

Procesos de negocio: los procesos de negocio son todas aquellas actividades desarrolladas por la organización para cumplir con sus objetivos. Tradicionalmente estas se encuentran asociadas en diferentes categorías tales como: procedimientos, los cuales en su conjunto conforman un proceso, y a su vez en su conjunto, se denominan macro procesos.

Todas las organizaciones cuentan por lo general con un mapa de procesos, agrupados en estratégicos, misionales y de apoyo (o términos similares) los cuales reflejan la forma como opera la organización y el nivel de interrelación existente entre cada uno de ellos.

Servicios de TI: de acuerdo a la definición planteada por ITIL, un servicio de TI es un medio por el cual se entregar valor a los clientes (usuarios) facilitándoles un resultado deseado sin la necesidad de que estos asuman los costos y riesgos específicos [26]. Los servicios se construyen a partir de la combinación de la infraestructura tecnológica y los procesos de gestión y operación de TI.

Algunos ejemplos de servicios son: correo electrónico, servicio de backups, servicio de procesamiento de nómina, servicio de soporte y mantenimiento, servicio de capacitación.

Datos, información, conocimiento: son los recursos más valiosos para la organización y los que en definitiva requieren mayor nivel de protección.

Sistemas de información transaccionales: son todos aquellos sistemas de información que utiliza la organización para automatizar sus procesos de negocio. Algunos ejemplos son: ERP (Enterprise Resource Planning), CRM (Customer Relation Management), sistemas de información de nómina, sistemas de información de ventas.

Sistemas de información de soporte: son todas aquellas herramientas de software que apoyan el negocio y la función de tecnologías de información para cumplir diferentes funciones operacionales, y se diferencian de los sistemas de información transaccionales, en que estas herramientas no soportan un proceso de negocio en especial. Dentro de esta categoría podemos encontrar: herramientas ofimáticas, software antivirus, compiladores para desarrollo de software, herramientas RAD (Rapid Application Developer), software utilitario para apoyar diferentes funciones de tecnologías de información.

Motores de bases de datos: equivale a lo que en el mercado se conoce como sistemas gestores de bases de datos (SGBD), los cuales permiten añadir, borrar, modificar, almacenar y analizar los datos que tiene una organización y que son gestionados tradicionalmente a través de sistemas de información. Dentro de los principales motores de bases de datos se encuentran: Oracle, SQL Server, Postgresql, Mysql.

Sistemas Operativos: es el programa que se encarga de administrar los servicios de hardware de un computador personal, de un servidor o de cualquier dispositivo que requiere de un interfaz entre los recursos de hardware y las diferentes funcionalidades de uno o varios sistemas de información. Dentro de esta categoría existen diferentes tipologías de sistemas operativos, desde sistemas operativos para computadores o dispositivos personales de un solo usuario y monotarea, hasta sistemas operativos para servidores, que atienden diferentes tareas y diferentes usuarios. Algunos ejemplos de sistemas operativos: Sistemas operativos Windows (en sus diferentes versiones), Android, OS2 de IBM, Unix, Linux.

PC's de escritorio e impresoras: en el caso de los computadores personales (PC's) son los dispositivos que tradicionalmente tiene cualquier usuario en su escritorio y a través de los cuales pueden acceder a los diferentes sistemas de información de la organización; en el caso de las impresoras, son todos aquellos dispositivos a través de los cuales se puede llevar a papel la información contenida en medios virtuales.

Servidores: los servidores son computadores dotados de ciertas características especiales (mayor capacidad de procesamiento, multitarea, mayores capacidades de almacenamiento, mayor capacidad en memoria) que se encuentran al servicio de otros dispositivos, y tradicionalmente son dedicados a tareas especializadas, para lo cual toman nombres de acuerdo a la tarea especializada asignada: Servidor de aplicaciones, servidor de archivos, servidor de correo, servidor de impresoras, servidor de base de datos.

Dentro de esta categoría podemos encontrar tres tipos genéricos de servidores: servidores físicos, servidores virtuales (una o varias particiones en un servidor para dedicarlo a prestar varios servicios) y servidores en la nube.

Centros de redes y cableado: comprende toda la infraestructura de red con que cuenta una organización y que se encuentra distribuida en sus diferentes dependencias. Dentro de esta categoría encontramos centros de cableado, equipos de red activos y pasivos y todo el tendido de red que interconectan los diferentes dispositivos que tiene la organización.

Centros de cómputo: también llamado centro de procesamiento de datos, centro de datos o data center, es aquel sitio o sitios donde tradicionalmente las organizaciones concentran los dispositivos de computo más críticos a través de los cuales se centraliza el procesamiento y almacenamiento de la información considerada más crítica para el negocio.

Sistemas de Energía: son todos aquellos servicios y dispositivos que permiten que un dispositivo físico de procesamiento de información pueda operar, si se tiene en cuenta que casi en su totalidad hoy dependen de la energía eléctrica. Dentro de esta categoría también se encuentran los dispositivos que permiten generar energía alterna, y que permiten su adecuado resguardo, tal es el caso de los bancos de baterías y las UPS.

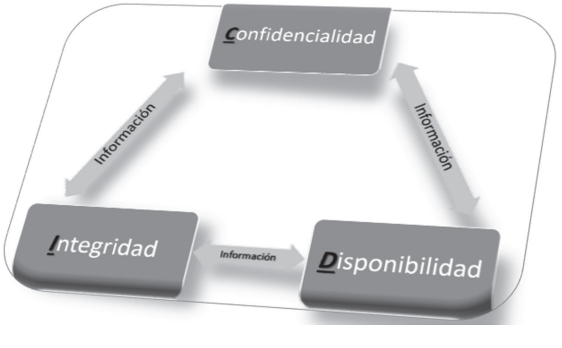
Esta capa tecnológica es una de las capas más importantes, por no decir la más importante de la infraestructura tecnológica de una organización, debido a que es la que permite que las demás capas puedan cumplir su función.

3.2 LA TRIADA DE SEGURIDAD COMO PARÀMETROS DE MEDICIÒN DE IMPACTO DEL ITRM

Si bien el impacto de cualquier riesgo en la organización afecta sus objetivos, el impacto directo de los riesgos de tecnologías de información, tal como se puede observar en la figura 10, son medidos por lo general a través de la triada Confidencialidad, Integridad y Disponibilidad (en adelante CIA, sigla en inglés correspondiente a los términos Confidentiality, Integrity, Availability).

De acuerdo al análisis comparativo de 10 metodologías de riesgos de TIC realizado en [27], los criterios para medir el impacto del riesgo, en el 100% de ellas contemplan la triada CIA, sin embargo existen otros atributos que son considerados elementos que complementan la seguridad de la información, como son la autenticidad, responsabilidad, no repudio y la confiabilidad [28].

FIGURA 10. Triada de seguridad de la información.



3.2.1 Confidencialidad

La confidencialidad es un término asociado con el acceso y uso de la información solo por parte de quienes se encuentran autorizados y tienen la necesidad de conocerla. En términos formales, y de acuerdo a lo establecido en la norma ISO/IEC 27000, la confidencialidad es la propiedad que tiene la información de no estar disponible o revelada a individuos, entidades o procesos no autorizados.

El concepto de confidencialidad es más cercano a la información que a los activos tecnológicos y persigue fundamentalmente que esta sea accesible únicamente por las personas, entidades o mecanismos autorizados.

La confidencialidad está asociada con secretos de diversa índole (personales, empresariales, militares), algunos de ellos son técnicos, como la descripción de un método de fabricación (ejemplo, la fórmula de la Coca-Cola), otros son de índole comercial como una lista de nombres y direcciones de clientes que podría interesar a un competidor, e incluso militares, como planes de guerra, o planes de incursión.

Dentro de los casos más sonados a nivel internacional que se encuentran relacionados con la Confidencialidad está el caso de Wikileaks, una plataforma digital para compartir documentos, que se hizo famosa desde julio de 2010 debido a los miles de documentos de carácter reservado que ha difundido por la web, ganándose la antipatía del gobierno de los Estados Unidos, al divulgar más de 251 mil cables diplomáticos de sus embajadas en 274 países.

Entre los casos más cercanos a nuestro país, tenemos el caso de las chuzadas del DAS, donde se accede a información reservada de forma fraudulenta a través de interceptaciones ilegales ò el caso Andrómeda (hacker Sepúlveda), quien compraba y vendía información confidencial, interceptando comunicaciones a diferentes agentes del gobierno.

3.2.2 Integridad

La integridad es un concepto que presenta diversas interpretaciones, en general podría definirse como la propiedad de salvaguardar la exactitud e integridad de la información y de los activos tecnológicos, ante su modificación o destrucción no autorizada.

De acuerdo con COBIT, la integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a las expectativas y valores del negocio.

La ISO/IEC 27000: 2014 define la integridad de la información como la propiedad de exactitud y completitud. Si la información está completa y libre de errores, es integra [22].

Uno de los ataques recientes contra la integridad de la información es el caso del gusano stuxnet, descubierto en el año 2010, y diseñado con la finalidad de dañar sistemas de control industriales y modificar su código para permitir que los atacantes tomen el control.

3.2.3 Disponibilidad

Referido a que los usuarios autorizados tienen acceso a la información y a los activos tecnológicos, cuando lo requieran. Para COBIT la disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento.

La ISO/IEC 27000:2014 define la disponibilidad como la propiedad de ser accesible y utilizable a petición de una entidad autorizada.

Dentro de las amenazas más cotidianas que afectan la disponibilidad de la información y/o de los activos tecnológicos se encuentra la denegación de servicio.

La disponibilidad de la información y/o de los activos tecnológicos asociados se puede presentar de forma cotidiana en diversas formas, algunos ejemplos de ellas son: La salida de un sistema de información bancario de atención al cliente, ante problemas de bases de datos; un servidor crítico fuera de línea ante un corte de energía; imposibilidad de acceder a la información de un computador personal por problemas de hardware o por una falla del sistema operativo o por caídas de red.

3.2.4 Parámetros CIA propuestos

La mayoría de las metodologías de riesgo de tecnologías de información no establecen parámetros específicos para determinar el nivel de impacto de los riesgos en la confidencialidad, integridad y disponibilidad de la información.

Sin embargo, organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés National Institute of Standards and Technology) ha establecido a través del documento FIPS PUB 199 -estándares para la categorización de seguridad de la información federal y los sistemas de información-, parámetros para evaluar el impacto en la confidencialidad, integridad y disponibilidad de la información, tal como se puede observar en la tabla 2.

TABLA 2. Parámetros de impacto para medir la triada CIA.

BAJO	MODERADO	ALTO
CONFIDENCIALIDAD		
La divulgación no autorizada de información podría tener un efecto adverso **limitado** sobre las operaciones de la organización, los activos relacionados o sus individuos	La divulgación no autorizada de información podría tener un efecto adverso **serio** sobre las operaciones de la organización, los activos relacionados o sus individuos	La divulgación no autorizada de información podría tener un efecto adverso **severo o catastrófico** sobre las operaciones de la organización, los activos relacionados o sus individuos
INTEGRIDAD		
La modificación o destrucción no autorizada de información podrían tener un efecto adverso **limitado** sobre las operaciones de la organización, los activos relacionados o sus individuos	La modificación o destrucción no autorizada de información podrían tener un efecto adverso **serio** sobre las operaciones de la organización, los activos relacionados o sus individuos	La modificación o destrucción no autorizada de información podrían tener un efecto adverso **severo o catastrófico** sobre las operaciones de la organización, los activos relacionados o sus individuos
DISPONIBILIDAD		
La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **limitado** sobre las operaciones de la organización, los activos relacionados , o sus individuos.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **serio** sobre las operaciones de la organización, los activos relacionados , o sus individuos.	La interrupción del acceso o uso de información o a un sistema de información podría tener un efecto adverso **severo o catastrófico** sobre las operaciones de la organización, los activos relacionados , o sus individuos.

Fuente: [29]

De igual forma metodologías como MAGERIT y la ISO/IEC 27005 establece escalas de valoración de los parámetros de impacto basados en la triada CIA.

Al respecto es importante que la organización determine sus propios parámetros y escalas de valoración del impacto de los riesgos tecnológicos en función del CIA, de acuerdo a su cultura de riesgo, dado que, si esta es baja, se convertirá en un factor que determinará la baja calidad de los resultados. De igual forma y ante la necesidad de cuantificar el valor del riesgo es importante definir escalas numéricas y parámetros que estén directamente relacionados con el alcance del proceso de gestión de riesgos, sea este con una cobertura organizacional, de procesos o de un activo específico.

4. CONCLUSIONES

Las Tecnologías de Información y Comunicaciones son activos estratégicos que han generado altos niveles de dependencia en el funcionamiento de las organizaciones, lo que las hace imprescindibles para la buena marcha de sus procesos estratégicos, tácticos y operativos. Frente a este nivel de dependencia un adecuado gobierno y gestión de riesgos tecnológicos se vuelve imprescindible para disminuir la incertidumbre que generan los diferentes eventos adversos a los que está expuesta una organización para salvaguardar su información y los activos de tecnologías de información que de ella dependen.

Es por ello necesario acudir a los referentes internacionales de gobierno y gestión de tecnologías de información y a las metodologías de gestión de riesgos de TIC como referentes para incorporar una metodología que se ajuste a las necesidades de la organización y que diferencie dos de los aspectos específicos propios de un contexto tecnológico como son los activos objeto de análisis y los criterios de impacto.

Los activos objetos de análisis deben ser identificados, teniendo en cuenta las diferentes capas tecnológicas que hacen parte de las TIC, y que a su vez se vuelven interdependientes para dar una cobertura total, no solo de la información, sino de los activos que le dan soporte.

Los criterios de impacto, a su vez, son los que le dan la connotación propia del contexto tecnológico para ser pertinentes y disminuir, al menos en cierta medida, la subjetividad al momento de su evaluación.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] ICONTEC, "Norma Técnica Colombiana NTC-ISO / IEC 38500," Bogotá (Colombia), 2009.
[2] Ernst & Young, "Cambios en el panorama de los riesgos de TI," 2012.
[3] M. S. Saleh and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," *Appl. Comput. Informatics*, vol. 9, no. 2, pp. 107–118, 2011.
[4] N. Racz, E. Weippl, and A. Seufert, "A process model for integrated IT governance , risk , and compliance management," in *The Ninth Baltic Conference on Databases and Information Systems*, 2010, pp. 155–170.
[5] A. Vanegas and C. J. Pardo, "Hacia un modelo para la gestión de riesgos de TI en MiPyMEs : MOGRIT," *Rev. S&T*, vol. 12, no. 30, pp. 35–48, 2014.
[6] IT Governance Institute, "COBIT 4.1.," 2007.
[7] ISACA, *COBIT 5. Procesos Catalizadores*. Rolling Meadows, Illinois, 2012.
[8] ISACA, *COBIT 5 for Risk*. 2013.
[9] Global Knowledge, "Las 15 certificaciones mejor pagadas en 2015," 2016. [Online]. Available: http://www.globalknowledge.es/noticias-y-eventos/noticias/las-15-certificaciones-mejor-pagadas-2015/. [Accessed: 30-Apr-2016].
[10] ISACA, *Manual de Preparaciòn al examen CRISC 2014*. 2013.
[11] ISACA, *The Risk IT Framework*. 2009.
[12] ICONTEC, "Norma Técnica Colombiana. NTC-ISO/IEC 27005. Tecnología de Información. Técnicas de Seguridad. Gestión del riesgo en la seguridad de la información.," Bogotá, 2009.
[13] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology," 2001.
[14] M. Talabis and J. Martin, *Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis*. 2012.
[15] A. Abril, J. Pulido, and J. A. Bohada, "Anàlisis de riesgos en seguridad de la informaciòn.," *Rev. Ciencia, Innovaciòn y Tecnol.*, vol. 1, pp. 39–53, 2013.
[16] CLUSIF, "Club de la Sécurité de l'Information Français," 2015. [Online]. Available: https://www.clusif.asso.fr/en/production/mehari/. [Accessed: 27-Apr-2015].
[17] A. Ramírez and Z. Ortiz, "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios," *Ingeniería*, vol. 16, no. 2, pp. 56–66, 2011.
[18] M. Firoiu, "General Considerations on Risk Management and Information System Security Assessment According to ISO/IEC 27005:2011 and ISO 31000:2009 Standards," *Calitatea*, vol. 16, no. 149, pp. 93–97, 2015.
[19] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of Information Security Risk Assessment (ISRA)," *Comput. Secur.*, vol. 57, pp.

14–30, 2016.

[20] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," in *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 2009, pp. 726–731.

[21] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," *J. Inf. Secur. Appl.*, vol. 18, no. 1, pp. 45–52, 2013.

[22] ISACA, *COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Rolling Meadows, Illinois, 2012.

[23] Union Internacional de Telecomunicaciones, "Arquitectura de Seguridad para sistemas de comunicaciones extremo a extremo.," 2003.

[24] L. Montenegro, "Seguridad de la Información: Más que una actitud, un estilo de vida.," *Microsoft Technet*, 2015. [Online]. Available: http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/. [Accessed: 15-Apr-2015].

[25] Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración Electrónica., "MAGERIT - versiòn 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Mètodo," Madrid, 2012.

[26] ITSMF International, *IT Service Management Based on ITIL V3. A pocket guide*, First Edit. 2007.

[27] A. S. Parra and E. Fernández-medina, "Desarrollando una metodologìa para gestionar los riesgos de seguridad asociativos y jerárquicos y tasar de forma objetiva los Sistemas de Información," in *n.d.*, 2013.

[28] ISO/IEC, "INTERNATIONAL STANDARD ISO / IEC 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary," 2014.

[29] NIST, "FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems," 2004.