Manejo de la capacidad de recuperación en el modelo RMM del CERT

Ricardo Peláez Negro
Universidad Abierta de Cataluña
rpelaezn@uoc.edu

Resumen

Este artículo compara diferentes marcos de trabajo y estándares del manejo de riesgo o relacionados, estableciendo ventajas y desventajas de su implementación; entre ellos, BS 25999, BS 25777, ISO/IEC 27000, COSO-ERM, ISO/IEC 20000, ITIL, Cobit 5, CERT-RMM, NIST SP-37. Describe cuales de los marcos comparados soporta procesos de negocio, procesos de TI, medición de la madurez e integración con otros marcos.

1. Introducción

La recuperación frente a incidentes es uno de los temas que más ha tomado importancia al interior de las empresas. Esta preocupación de las empresas por anticipar los incidentes está motivada por muchos ejemplos nefastos en los cuales empresas han desaparecido o han quedado altamente golpeadas por no prever incidentes tanto externos como internos. Starr en [4] plantea como dos empresas Nórdicas de telecomunicaciones enfrentan la misma crisis, la pérdida de su proveedor principal de microchips, los resultados son diferentes para las dos compañías, al punto que las acciones de una de ellas se incrementan en 3% mientras la otra decrece el mismo 3%.

Variados términos en relación con el manejo de incidentes han salido a la luz gracias a la investigación, tanto de la industria como de académicos que proponen la aplicación de metodologías, estándares y marcos de trabajo que puedan mitigar de manera efectiva los riesgos a los que está sometida cualquier empresa. Es el interés del presente artículo mostrar un panorama de los enfoques desde los cuales se está abordando el manejo de los riesgos y finalmente hacer hincapié en los problemas aun no resueltos y que requieren de mayor investigación.

1.1. Definiciones

Manejo del Riesgo: De acuerdo con [5] el manejo del riesgo o la administración del riesgo parte de una política que ofrece un marco para la toma de acciones en pro de minimizar el impacto de los peligros, además permite definir cuál es el riesgo aceptable para cada empresa o negocio. Las estrategias de la política de riesgo ofrecen diferentes opciones como pueden ser la reducción, eliminación o redistribución del riesgo. Otra definición de manejo del riesgo la proporciona Bs 25999 [12], uno de los estándares más conocidos para la gestión del riesgo, como aplicación estructurada de políticas, procedimientos y prácticas a las tareas de análisis, evaluación y control del riesgo.

A pesar de que el término Manejo del Riesgo (Risk Management) puede ser utilizado en muchos contextos [2], para el presente trabajo el término describe los riesgos relacionados con el cumplimiento de los objetivos misionales de una empresa o aquellos que los soportan como son la información, tecnología, personas o edificaciones, entre los más relevantes.

Resiliencia: Se define como la propiedad física de un material para deformarse y regresar a su posición original siempre y cuando la deformación no exceda su límite elástico. A pesar que esta definición tiene más relación con las características de un elemento físico, puede considerarse que la resiliencia es una propiedad emergente de las organizaciones, que tienen la capacidad de resistir a adversidades o nuevos ambientes de riesgo sin dejar de cumplir con sus objetivos misionales [3] [4]. Al menos tres condiciones debe cumplir una organización para ser resiliente. En primer lugar debe tolerar el impacto del riesgo por algún periodo de tiempo. Segundo, debe cumplir su misión durante el tiempo de impacto. Por último, en un tiempo razonable debe regresar a su normal operación [3]. NIST, uno de los referentes en manejo de riesgo, define resiliencia como la habilidad para recuperarse frente a cambios conocidos o desconocidos del ambiente a través de una implementación holística del manejo del riesgo, contingencia y planificación de la continuidad [9].

Riesgo operacional: Los negocios hoy más que nunca dependen de los servicios de terceros. Un ejemplo de ello es el incremento en el uso de tecnologías orientadas a la nube como IaaS (Infraestructure as a Service), SaaS (Software as a Service), PaaS (Platform as a Service). Estas tecnologías sugieren un incremento en el riesgo operacional. El riesgo operacional se define como el impacto potencial sobre activos o servicios, derivados de fallos en los procesos internos, fallos tecnológicos, acciones deliberadas de empleados o eventos externos [3]. Se hace especial énfasis en

servicios de terceros porque una empresa no puede intervenir directamente sobre estas infraestructuras. Por el contrario la empresa afectada, tendrá que esperar a que el tercero solucione su inconveniente. Es posible que las fallas de terceros puedan generar algún reclamo de tipo contractual, que en definitiva no reparará los daños morales y de imagen que se puedan causar sobre los usuarios finales. Es allí donde resulta benéfico controlar el riesgo operacional.

2. *Marcos de trabajo y estándares para el manejo del riesgo*

Aunque existen renombrados estándares y marcos de trabajo para el manejo del riesgo, su implementación y posterior mantenimiento es un tema que resulta confuso de entender para los empresarios (CEOs) y directivos. Según Gartner en [7], desde el 2007 se han incrementado el número de clientes que solicitan una guía de como direccionar situaciones de riesgo o problemas de seguridad frente a los comités directivos. Si bien los estándares proveen una forma organizada de afrontar el riesgo, existe un riesgo residual que requiere de una estrecha comunicación entre quienes dirigen las empresas y quienes soportan su operación en términos de gestión del riesgo. Vale aclarar que los estándares y marcos de trabajo pueden tener un mayor énfasis en aspectos de riesgo relacionados con el objeto del negocio, otros más orientados a satisfacer los crecientes riesgos derivados del uso de las tecnologías de la información y las comunicaciones, y por último aquellos que relacionan la gestión del riesgo del negocio y las tecnologías. A continuación se describen los estándares y marcos de trabajo que serán objeto de análisis en el desarrollo del presente artículo:

BS-25999 Gestión de la continuidad del negocio - BCM: Proporciona las bases para la comprensión, desarrollo e implementación de un sistema de gestión de la continuidad del negocio, ofreciendo confianza a los acuerdos empresariales (business-to-business) y relación con clientes (business-to-customers). Permite medir de manera confiable la capacidad del sistema de continuidad de negocio (BCM) [12].

BS 25777:2008 Gestión de la continuidad de TI: Es un estándar liberado por BSi (British Standards), se encarga de ofrecer una referencia para la recuperación del negocio frente a problemas de TI [13]. BS-25777 complementa a BS-25999 y otros estándares de BSi.

ISO/IEC 27000 Sistema de gestión de la seguridad de la información: la serie de normas asociadas establece políticas, procedimientos y guías para proteger la información de una organización [15]. Puesto que la información se considera como un activo a proteger, es un componente en la gestión de riesgos.

ISO/IEC 20000 Sistema de gestión de servicios de IT: es la serie de estándares donde se especifican los requerimientos de un proveedor de servicios de TI. Está pensado para asegurar que los usuarios (clientes, proveedores, inversionistas) de un servicio tecnológico reciban niveles de servicio satisfactorios. Se podría considerar como un remplazo a la BS-15000 desarrollada por Bsi.

Cobit 5: Es un marco de trabajo para el gobierno y gestión de TI. Liberado recientemente por ISACA como una revisión a Cobit 4.1 [8]. Entre sus objetivos principales se encuentra el crear valor de IT, guardando un balance entre beneficios, niveles de riesgo y utilización de recurso [22]. Está basado en cinco principios, satisfaciendo las necesidades de los inversionistas, cubriendo la empresa de extremo a extremo, aplicando un único e integrado marco de trabajo, facilitando una aproximación holística y separando el gobierno de la gestión de TI.

ITIL Biblioteca de infraestructura de tecnologías de la información: es una guía de buenas prácticas en la gestión de servicios de TI. Su estructura nuclear de funcionamiento está representada por diferentes ciclos de vida iterativos y multidimensionales. Estos ciclos de vida se describen en cinco publicaciones, proporcionando el conocimiento útil para alcanzar el estándar ISO/IEC 20000. Hacen parte de la biblioteca, estrategia de servicio, diseño del servicio, transición del servicio, operación del servicio y mejoramiento continuo de los servicios [14].

NIST (National Institute of Standards and Technology): es parte del departamento de comercio de los Estados Unidos. Es uno de los más antiguos laboratorios de ciencia. Hacen parte de las publicaciones de NIST, la serie 800 y son de interés general en el campo de la seguridad de computadores. Para el presente artículo se destacan SP NIST 800-34 (Contingency Planning Guide for Information Technology Systems) [16], SP NIST 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems) [11], SP NIST 800-39 (Managing Information Security Risk) [17].

COSO-ERM (Enterprise Risk Management): es desarrollado por empresas voluntarias del sector privado de Estados Unidos y se enfoca en aspectos del negocio. Su marco para la gestión de riesgo abarca los siguientes aspectos, alineando el riesgo y la estrategia, decisiones que mejoren la respuesta a los riesgos, reduciendo sorpresas operacionales y perdidas, identificando y manejando múltiples riesgos transversales a la organización, aprovechando las oportunidades y mejorando la utilización del capital [18].

CERT-RMM (Modelo para el manejo de la resiliencia): es un modelo de gestión de riesgos propuesto por el CERT (Computer Emergency Response Team) de la Universidad Carnigie Mellon en Estados Unidos [1]. Evalúa la resiliencia de una empresa y propone desde su modelo la convergencia del manejo de la seguridad, la continuidad del negocio y las operaciones de TI. No pretende cambiar las prácticas ya establecidas por la empresa, sino evaluar las existentes y determinar los vacíos para su posterior mejoramiento. Su desarrollo está influenciado por el conocido CMMI, creado por la misma Universidad y otros marcos de trabajo como ITIL, COBIT, ISO-2700, BS-25999, NFPA-1600, PCI DSS y NIST.

Otros estándares y marcos de trabajo no menos importantes son, Basel II:2005, PMBOK 4th Edition:2008, NS 5814:2008, JIS Q 2001:2001:2007, FSA CP142, CAN/CSA-Q850-97 (R2009):1997, AENOR UNE 71504:2008, ISACA Risk IT:2009, ARMS:2002, M_o_R:2007, Microsoft SRMG:2006, AS/NZS 4360:2004. Para efectos del presente trabajo no se abordarán en profundidad. Existen muchos otros estándares que apenas salen a la luz pública o que son desarrollados para uso exclusivo de algunas organizaciones. Respecto de ellos pueden ser objeto de futuras investigaciones en el área del manejo del riesgo.

No solo la industria ha desarrollado estándares, marcos de trabajo o códigos de buenas prácticas. Las universidades a través de sus investigadores han propuesto nuevos marcos para el manejo de riesgos [2], esquemas para medir el riesgo [6], o propuestas de cómo mejorar y ajustar los marcos existentes a las necesidades emergentes de un medio ambiente del riesgo cambiante [2]. Algunas de estas propuestas tienen tanta aceptación, que se incorporan en nuevas versiones de los estándares luego de las revisiones por parte de los comités especializados e interdisciplinarios designados por el organismo creador del estándar. Continua siendo difícil medir el impacto de las aportaciones hechas desde la academia a los estándares y marcos de trabajo de la industria, pues la literatura existente sobre estos no se encuentra en formato de publicación científica, ni se cita en la versión final del documento.

2.1. *Metodologías al interior de los estándares y marcos de trabajo*

Cada estándar o marco de trabajo aborda una metodología para asegurar su propósito en la gestión de riesgo. Si bien existen etapas y actividades en común, no necesariamente se ejecutan en el mismo orden. En la línea de estándares publicados por ISO [10], [19], [20] se encuentra el ciclo de vida Planear-Hacer-Verificar-Actuar que se ajusta a las siguientes etapas dentro de la gestión de riesgos:

- Identificar el riesgo
- Medir el riesgo
- Tratar el riesgo
- Monitorear y reportar el riesgo

Diferentes sub-actividades se desarrollan en cada uno de estas etapas generales, convirtiéndose en un aspecto diferenciador en cada uno de los estándares que abordan el mismo ciclo de vida planteado por ISO. Algunos ejemplos de estándares o marcos de trabajo que siguen este ciclo de vida o uno similar son [12], [2], [13], [8], [9], [14] y [3].

El resultado de las actividades y los productos generados en términos de la gestión del riesgo (Identificación de riesgo, Medición del impacto de los riesgos, Planes de continuidad y recuperación ante desastres, Controles, Resiliencia operacional, Gobernanza de TI, Recuperación frente a incidentes y problemas, Madurez e institucionalización de los procesos, Estrategias, Sostenibilidad), finalmente determinan la efectividad del estándar o marco de trabajo y su metodología asociada.

2.2. *Problemas asociados a la gestión del riesgo*

Los estándares y marcos de trabajo son uno de los posibles puntos de partida para la gestión de riesgos, sin embargo a la hora de implementar uno u otro, se requiere determinar con claridad cuál de ellos cubre mejor las expectativas de la alta dirección en cada empresa. Como lo afirma Garnert, en su informe [7], la preocupación de los CEOs es creciente en términos de alinear sus procesos de negocio con un manejo adecuado del riesgo operacional derivado del uso de tecnología.

Algunas propuestas de solución son la utilización de múltiples estándares como es el caso de ISO, que para completar su marco de gestión de riesgo integra las series 27000, 20000 y la serie 31000 que generaliza el marco de la gestión de riesgo. En contraposición, ISACA ha publicado una nueva versión del marco de trabajo Cobit, donde ha decidido unificar tres de sus antiguos marcos, gobierno y control de TI (Cobit 4.1), manejo del riesgo de TI en los negocios (Risk IT) y manejo del negocio soportado por TI (Val IT). De esta manera Cobit 5, le apunta a una solución de mayor cubrimiento, integrando varios marcos que antes se aplicaban de manera independiente y poco articulada.

En la tendencia de ISACA en su marco de trabajo Cobit 5, el CERT a través de su modelo para el manejo de la resiliencia [3], propone la convergencia de tres disciplinas en un solo modelo, continuidad del negocio, operaciones de TI y seguridad de la

información; los cuales son transversales a cualquier organización, y desde estas áreas aplicar una metodología de medición y cuantificación del riesgo operacional.

En el presente artículo se desarrolla una comparación de los marcos de trabajo desarrollados para el manejo del riesgo, en busca de ventajas y desventajas de marcos de trabajo unificados y transversales a los procesos de negocio y de tecnología, frente a los ya bien utilizados marcos complementarios y de aplicación independiente como ISO e ITIL.

3. *Justificación de los parámetros de comparación*

Desde cada marco y estándar se aborda la gestión de riesgo de una manera distinta, que agrega valor a la empresa u organización que los implementa. Para evidenciar las ventajas y desventajas de los marcos y estándares mencionados hasta el momento es importante ver su aplicación desde distintos parámetros como son su capacidad de soporte a los procesos de negocio y TI, modelos utilizados para asegurar su madurez, su integración con otros marcos de trabajo o estándares y finalmente si es posible certificar la empresa bajo el marco o estándar.

Cabe anotar que existen otros parámetros y enfoques que pudieran tenerse en cuenta para comparar los marcos y estándares, sin embargo para el alcance del presente trabajo los parámetros escogidos se consideran como factores diferenciadores y de alto impacto en cualquier organización.

3.1. *Capacidad de soporte a los procesos de negocio*

La necesidad de blindar los procesos de negocio a través de la gestión de riesgos ha sido recurrente en empresas del sector financiero por el valor de sus activos y la importancia de los mismos para la estabilidad de un país. Los cambios de un mercado globalizado impactan a todos los actores involucrados directa o indirectamente. En este sentido el manejo del riesgo en los procesos de negocio es una necesidad que no da espera. Aunque se ha tenido éxito en muchas de las practicas implementadas para minimizar el riesgo, siguen existiendo brechas que deben ser cubiertas de modo que se pueda hacer más efectiva la gestión del riesgo y la resiliencia de las empresas [4]. Como se menciono anteriormente, algunos de los marcos de la gestión del riesgo están definitivamente ligados al análisis de los procesos de negocio. Es por esto que la siguiente parte aborda la capacidad de algunos marcos de trabajo para soportar los procesos de negocio.

En primer lugar COSO [18], lista entre sus principios del manejo del riesgo que una entidad (unidad de negocio), puede crear valor, ser preservada o gradualmente destruida por las decisiones administrativas. De esta manera el marco de gestión de riesgos sugerido por [18], intenta tratar los eventos futuros y evitar la probabilidad de una reducción de ingresos en la entidad. Los objetivos de cada entidad se visualizan por [18] en cuatro categorías, estrategias, operaciones, reportes y cumplimiento de las normas. También considera las actividades a todos los niveles de la organización. Finalmente considera afectar positivamente tanto los objetivos como las actividades a través de los ocho componentes del principales del marco de trabajo [18]: ambiente interno, ajuste de objetivos, identificación de eventos, evaluación del riesgo, respuesta al riesgo, actividades de control, información y comunicación y por último monitoreo. Gráficamente el modelo se representa por un cubo que alinea objetivos y actividades frente a cada etapa del modelo.

Por su parte BS-25999 [12], es otro de los estándares altamente enfocados a proteger los procesos de negocio. Su principal objetivo es consolidar en la empresa u organización el manejo de continuidad del negocio. De acuerdo con el estándar [12] BCM (Bussiness Continuity Management) se define como, el manejo holístico de los procesos para identificar amenazas internas o externas y el manejo del impacto del negocio frente a estas amenazas. En el contexto de la estrategia de la organización, el manejo de la continuidad del negocio debe asegurar la consecución de los objetivos misionales de corto mediano y largo plazo. Para alcanzar su objetivo [12] debe:

- Proactivamente identificar riesgos operacionales y tener la capacidad de mitigar y manejar estos riesgos.
- Manejar los riesgos no asegurables como la reputación.
- Responder efectivamente a rupturas graves de servicio.
- Mantener el servicio al cliente, la rentabilidad y el empleo de su personal.

Los anteriores ítems no pretenden ser una lista exhaustiva de los resultados de [12], sin embargo permiten inferir que su mayor enfoque y aplicación está dirigida a los aspectos inherentes a los procesos de negocio. El estándar no excluye los riesgos asociados a la tecnología y la seguridad de la información, en lugar de ello, sugiere la articulación con otros estándares como BS-25777 [13], ISO/IEC 27000 [10].

En el CERT-RMM [3] existen 26 procesos fundamentales divididos en cuatro categorías. Una de estas categorías está dedicada al soporte de los procesos de negocio. En el acervo del modelo esta categoría se denomina como "Gestión Empresarial". En su interior se encuentran los siguientes procesos:

- Comunicaciones: Este proceso enfoca su atención en desarrollar, implementar y administrar comunicaciones internas y externas que apoyen los demás procesos y actividades del modelo en tiempos de estrés o interrupción, de manera confidencial [3].
- Gestión del cumplimento: asegura el cumplimento de todas las regulaciones, estándares y legislación vigente aplicable a la organización tanto interna como externa. De esta manera la organización reconoce que el resultado de sus procesos no pueden ser contrarios a las directivas de la empresa ni el marco legal del país donde se desarrolle la actividad económica [3].
- Enfoque empresarial: Focaliza la atención de los planes de manejo del riesgo sobre los objetivos misionales. De esta manera se pretende que la alta dirección ejerza liderazgo y gobierno sobre los planes de gestión del riesgo de la organización. Asimismo cataloga los procesos de misión crítica para que la gestión de riesgo este alineada con los propósitos institucionales [3].
- Gestión de los recursos financieros: El costo de proteger y sostener en funcionamiento los servicios de una organización, requiere que exista una vigilancia sobre el manejo de los recursos financieros. Es por esto que dentro del modelo la gestión de recursos financieros se propende por balancear los costos asociados a la gestión del riesgo, sin olvidar la mejora continua de los servicios y procesos de la organización, es decir calcular riesgo vs retorno de inversión [3].
- Gestión del talento humano: la forma como una empresa contrata y administra su personal tiene un impacto significativo sobre la gestión del riesgo. Es por esto que el efecto de una mala contratación puede significar un fallo en los servicios de la empresa. La aplicación de este proceso pretende que la descripción de roles y la distribución de la responsabilidad sea la adecuada. Igualmente fomenta la conservación de su personal, minimizando así el impacto de las renuncias, sobre la capacidad productiva de la organización [3].
- Capacitación y toma de conciencia: promueve el aprendizaje de nuevas habilidades en el personal de una organización, mejora la comprensión del manejo del riesgo y el papel que cada miembro de la organización desempeña. La toma de conciencia hace referencia a los comportamientos esperados para soportar los procesos de mayor riesgo generando una cultura organizacional [3].
- Gestión del riesgo: Establece las directrices para identificar, analizar y mitigar el riesgo que se produce sobre los activos (Personas, Edificaciones, Información y Tecnología), que pueden ser adversos a los servicios de la empresa. También debe identificar el riesgo tolerable, previniendo interrupciones potenciales en los servicios que impidan cumplir los objetivos misionales. Se consideran fuentes de riesgo, los fallos en los procesos internos, acciones deliberadas o inadvertidas por el personal, problemas asociados a la tecnología y eventos externos [3].

Los procesos mencionados anteriormente están conformados por prácticas y sub-practicas que se pueden alinear con los procesos propios de la empresa, códigos de buenas prácticas y otros estándares tanto comerciales como gubernamentales. Se convierte en un modelo flexible que mejora la compresión general de la gestión de riesgo en los procesos inherentes al negocio.

Finalmente aparece Cobit 5 [22] como un marco para el gobierno y manejo empresarial de TI. El estudio de los procesos de negocio hace parte de los 37 procesos que conforman la totalidad del modelo planteado por [22]. Se clasifican en dos grandes categorías, lo dirigidos al gobierno de TI y los de gestión de TI. Dentro de los cinco principios de [22] hay una separación conceptual de gobierno y gestión. El gobierno debe satisfacer las necesidades de los clientes o usuarios del servicio prestado por la empresa, asegurando que sus necesidades estén alineadas con los objetivos misionales. De su

ejercicio se deriva la evaluación, el direccionamiento estratégico y el monitoreo. La gestión entre tanto, debe planear, construir, desarrollar y monitorear las actividades establecidas por el gobierno, a fin que se cumplan los objetivos generales de la empresa.

A continuación se destacan los procesos del modelo que atienden los aspectos relacionados con el negocio:

- Asegurar la gobernanza del marco de trabajo y su mantenimiento: Las directivas de la empresa analizan y articulan los requerimientos del gobierno de TI, habilitando estructuras, principios, procesos y prácticas, asociadas. Una vez que hay un conocimiento de los lineamientos establecidos se asignan las responsabilidades y autoridad a quien corresponda, de modo que sea posible alcanzar la misión, metas y objetivos de la empresa [22].
- Asegurar la entrega de beneficios: Optimizar la contribución de valor a la empresa de los procesos de negocio, servicios de TI y los activos de TI como resultado de las inversiones realizadas por ella en costos aceptables [22].
- Asegurar la optimización de los riesgos: este proceso define el riesgo tolerable para la empresa y lo da a conocer, de modo que dentro de la articulación con los procesos de negocio es identificable y gestionado [22].
- Asegurar la optimización de recursos: asegura que las capacidades TI (Personas, Tecnología) sean suficientes, de tal manera que soporten los objetivos empresariales a un costo óptimo [22].
- Asegurar la transparencia a los usuarios o clientes: Este proceso monitorea las metas y métricas establecidas al interior de la empresa y las reporta a sus usuarios o clientes de manera transparente. Si es necesario ejecuta acciones correctivas [22].

Las entradas y salidas de los procesos mencionados anteriormente tienen una relación directa con los demás procesos del modelo. Por ejemplo el análisis de riesgos es un sub-producto del proceso encargado de la gestión del riesgo, sin embargo parte del análisis será reportado como una estrategia de comunicación y transparencia hacia los usuarios o clientes.

Otros marcos de trabajo y estándares como ITIL e ISO 27000, mencionan superficialmente los procesos de negocios, por esta razón no se tendrán en cuenta en este apartado.

3.2. *Capacidad de soporte a los procesos de TI*

La gestión de TI ha pasado de ser un simple departamento al interior de la empresa, para convertirse en un aliado estratégico de cualquier iniciativa de nuevos servicios o productos. La razón fundamental es que las TI soportan los nuevos servicios o propuestas de valor, convirtiéndose en foco de atención no solo para el oficial encargado de tecnología sino también para la alta dirección. Es allí donde entran en el plano los estándares, marcos de trabajo y códigos de buenas prácticas, que de manera estructurada apoyan el buen funcionamiento de la infraestructura tecnológica, seguridad de la información y la continuidad de los servicios en el tiempo.

Luego de ver que estándares y marcos de trabajo ofrecen soporte a los procesos de negocio, es importante conocer aquellos que ofrecen soporte a los procesos de TI. BS 25777:2008 [13] es el código de prácticas publicado por BSi (British Standars) para el manejo de la continuidad de las tecnologías de la información y la comunicación. Este código es un complemento para las empresas que ya utilizan [12] en la gestión de la continuidad del negocio, sin embargo como se menciono en el apartado anterior, [12] tiene un mayor enfoque a los procesos de negocio.

Al ser [13] un código complementario uno de sus mayores objetivos es alinearse con el programa de continuidad del negocio establecido por [12]. A continuación se destacan los procesos de TI soportados por el código:

- Entender las vulnerabilidades y las amenazas a los servicios de TI
- Identificar el impacto potencial de una ruptura de los servicios de TI
- Mejorar la comunicación entre administradores de TI y los proveedores de servicios de TI
- Desarrollar competencias en los administradores de TI, para responder a los planes de continuidad desarrollados
- Demostrar la habilidad para mantener en funcionamiento los servicios en tiempos de ruptura o afectación de la infraestructura tecnológica.
- Ofrecer información oportuna a los usuarios o clientes, cumpliendo con sus expectativas en el uso de los servicios soportados por IT en la empresa.

[13] hace referencia a otros estándares como ISO/IEC 27001:2005 [10] para asegurar la protección a los datos y los aspectos relacionados a la seguridad de la información. En resumen, [13] aporta un marco lógico para construir los planes de continuidad de las TI. Algunos de los sub-productos

del la implantación de la continuidad de TI se mencionarán en apartados siguientes.

La serie ISO/IEC 27000, también conocida como la familia de estándares del sistema de gestión de la seguridad de la información, tiene como función asistir organizaciones de todo tipo en la implementación y operación del SGSI[1]. Desde esta perspectiva, soporta los procesos de manejo de riesgo asociados a la seguridad de la información. A continuación una breve descripción del alcance de algunos de los estándares de la familia ISO 27000:

- ISO/IEC 27000:2009, Sistemas de gestión de Seguridad de la información - Información general y vocabulario
- ISO/IEC 27001:2005 [10], Sistemas de gestión de Seguridad de la información – Requerimientos del SGSI para obtener la certificación.
- ISO/IEC 27002:2005, Código de prácticas para la gestión de la seguridad de la información.
- ISO/IEC 27003, Guía de implementación del SGSI
- ISO/IEC 27004, Medición del SGSI
- ISO/IEC 27005:2008, Manejo del riesgo de la seguridad de la información
- ISO/IEC 27006:2007, Requisitos para organismos que presten servicios de auditoría y certificación de seguridad de la información
- ISO/IEC 27007, Guía para la auditoría del SGSI

Estos estándares son aplicables en la medida de las necesidades de la organización y generalmente se empieza por [10] pues en él se encuentran los requerimientos formales para una posterior certificación. El estándar propone 11 clausulas de seguridad, y a su vez contiene 39 categorías principales de seguridad. Las clausulas de seguridad son la generalidad de los procesos de TI abordados por la norma. A continuación se describen las clausulas que soportan los procesos de TI:

- Política de seguridad: Documento que define el alcance del SGSI y los controles aplicables a la organización en concordancia con la regulación vigente.
- Aspectos organizativos de la seguridad de la información: Cubre los aspectos relacionados con el manejo de la seguridad a nivel interno y regula el flujo de información a terceros.
- Gestión de Activos: Identifica y protege los activos (Información, Infraestructura). Puesto que no todos los activos tienen la misma importancia, establece niveles de protección.
- Seguridad ligada a los recursos humanos: Define las responsabilidades para empleados, contratistas y terceros frente a la seguridad de la información. Considera tres estados relación laboral, antes del empleo, durante el empleo y una vez finalice su contrato.
- Seguridad física y del entorno: Establece los permisos de acceso a los lugares que concentran activos. De igual manera los protege los activos frente a daños o robo.
- Gestión de comunicaciones y operaciones: Recoge todos los aspectos técnicos y de carácter administrativo que permitan la operación y funcionamiento de los activos.
- Control de acceso: Maneja los niveles de acceso lógico a la información, aplicaciones y estaciones de trabajo desde dentro o fuera de la organización.
- Adquisición, desarrollo y mantenimiento de sistemas de Información: Asegura la existencia de políticas de seguridad en los sistemas de información que se van a adquirir, están en desarrollo o requieren de un fortalecimiento de la seguridad existente.
- Gestión de incidentes en la seguridad de la información: Aplica las acciones preventivas o correctivas que puedan presentar en los activos.
- Cumplimiento: Asegura el cumplimiento de los estándares técnicos y las regulaciones vigentes que puedan incidir directa o indirectamente sobre el tratamiento de la información.

ISO/IEC 20000 [20] es el estándar para el manejo de los servicios de TI. No se dedica a los aspectos de manejo del riesgo, pero bien vale la pena mencionar que al ser parte de las normas ISO, soporta algunos procesos de seguridad de la información de ISO 27000; gestión de la continuidad y disponibilidad de los servicios de TI.

- Seguridad de la información: hace parte del código de prácticas del estándar, sin embargo redirige al lector a ISO 27000 para obtener un mayor detalle de como desarrollar el SGSI y así mantener coherencia entre los estándares ISO.
- Gestión de la continuidad y disponibilidad de los servicios: Debe asegurar que los acuerdos de nivel de servicio establecido con los usuarios o clientes de un servicio de TI, se mantengan incluso al enfrentar fallas mayores o desastres naturales. Para esto propone planes de continuidad similares a los expuestos por [12].

ITIL es la librería de infraestructura tecnológica para el manejo de servicios de TI, desarrollada por la oficina de comercio del gobierno Británico. A pesar de que no es un marco de trabajo asociado directamente al manejo del riesgo, su contenido soporta procesos de TI importantes dentro del

1 Sistema de Gestión de la Seguridad de la Información

manejo del riesgo. A nivel general este marco está conformado por cinco publicaciones, que resultan ser el núcleo de su propuesta metodológica. A continuación se listan las publicaciones:

- Estrategia del servicio: su objetivo principal es decidir sobre las estrategias de servicio a usuarios o clientes, empezando por medir las necesidades de los clientes y los diferentes mercados. El estudio determina cuales servicios de TI debe ofrecer la organización y definir las capacidades requeridas para soportarlos.
- Diseño del servicio: su objetivo es diseñar nuevos servicios de TI y mejorar los ya existentes.
- Transición del servicio: desarrollar e implementar los servicios de TI, asegurando que los cambios estén coordinados con la gestión de servicios.
- Operación del servicio: Asegura que los servicios de TI se ofrezcan de manera efectiva y eficiente. En el están contenidos los procesos relacionados con al manejo de riesgos.
- Mejoramiento continúo del servicio: su función principal es monitorear los servicios existentes y propender por su mejoramiento.

A continuación se listan los procesos de TI que hacen parte del manejo de riesgos:

- Gestión de problemas: es responsable de mitigar los problemas en los servicios de TI. ITIL se define problema, como la causa de incidentes o rupturas en los servicios de TI provocados por factores externos o internos a la organización. Su objetivo es reducir el impacto de las interrupciones sobre los servicios [24].
- Gestión del cambio: los cambios pueden venir por diferentes razones, en ITIL se identifican cambios proactivos y reactivos. Aquellos que se efectúan buscando reducción de costo o mejora de servicios, son proactivos. Los reactivos como respuesta a la solución de errores, adaptación o cambio de circunstancias. Su objetivo final es reducir el potencial impacto negativo y las consecuencias de cambios inesperados [25].
- Gestión de la disponibilidad: asegura que los niveles de disponibilidad de cada uno de los servicios de TI sean iguales o superiores a los acuerdos establecidos con usuarios o clientes de manera rentable. Para lograr su objetivo ITIL propone un plan de disponibilidad que debe ser medido y monitoreado de manera similar a los análisis de riesgos [23].
- Continuidad de servicios de TI: garantizar que las instalaciones técnicas y de servicio (incluyendo computadores, redes, aplicaciones, repositorios de datos, telecomunicaciones, medio ambiente, soporte técnico y mesa de ayuda) se puedan reanudar dentro del tiempo requerido y acordado con los usuarios o clientes en los contratos de negocio [23].

Como se menciono en el apartado anterior Cobit 5 [22] divide los procesos en categorías de gobernabilidad y gestión. A continuación se listan los procesos de gestión y que a su vez representan los procesos de TI en temas de riesgos:

- Gestión de operaciones: Coordinar y ejecutar las actividades requeridas para entregar a los usuarios o clientes los servicios de TI contratados. Hacen parte de la gestión de operaciones el monitoreo constante para alcanzar niveles óptimos del servicio [22].
- Gestión de las solicitudes de servicio e incidentes: Proveer una respuesta efectiva a las solicitudes de los usuarios y la solución de todo tipo de incidentes. Restaurar los servicios cuando estos se vean afectados. Como parte del proceso de la gestión de incidentes, se debe registrar, investigar, diagnosticar, escalar y resolver minimizando el riesgo de futuros incidentes con similares características [22].
- Gestión de problemas: Identificar y clasificar problemas, tratando de encontrar su causa, previniendo así incidentes recurrentes. De igual forma proporcionar recomendaciones para eliminar la causa de los problemas encontrados. Finalmente la gestión de problemas, según [22] se traduce en disponibilidad, mejora de los niveles de servicio, reducción de costos y satisfacción del usuario final del servicio [22].
- Gestión de la continuidad: establecer y mantener un plan de respuesta a incidentes e interrupciones de los servicios de TI, manteniendo así la operación tanto de los de los procesos de negocio como los de TI. En ninguna manera como resultado de las interrupciones se debe superar el nivel de tolerancia acordado por la alta dirección, de lo contrario es necesario replantear los componentes del plan [22].
- Gestión de servicios de seguridad: proteger la información de la organización y mantener los niveles de riesgo aceptables de acuerdo con la política de seguridad. Establecer y mantener los roles asociados a la seguridad de la información, los privilegios de acceso y el monitoreo constante. En resumen minimiza el impacto operacional sobre la información de vulnerabilidades e incidentes [22].

NIST-37 [11] establece los lineamientos para establecer el marco de la gestión de riesgo. En este estándar se presenta un enfoque similar al de [10], donde su principal objetivo es proteger la

información. Los procesos de TI soportados por NIST se estructuran en 18 familias y dentro del modelo se denominan como controles de seguridad. A continuación se listan los procesos de TI relevantes en la gestión del riesgo:

- Gestión de la configuración
- Planes de contingencia
- Respuesta a incidentes
- Evaluación de riesgos

CERT-RMM soporta muchos de los procesos de TI ya mencionados por otros marcos de trabajo, sin embargo en cada uno de ellos se puede encontrar un grado diferente de profundización y detalle. A continuación se listas los procesos de TI soportados por el modelo de resiliencia del CERT:

- Control y gestión de incidentes: establecer procesos para análisis y detección de eventos e incidentes, y así determinar la mejor respuesta posible para la organización [3].
- Análisis de vulnerabilidades y resolución: identificar, analizar y gestionar las vulnerabilidades en todos los lugares de operación de la empresa u organización [3].
- Gestión de controles: establecer, monitorear, analizar y gestionar los sistemas de control interno que aseguran la eficiencia y efectividad de las operaciones de la organización. Los controles protegen los servicios de misión crítica y los activos que los soportan [3].
- Requisitos de resiliencia para el desarrollo: identificar, documentar y analizar los requerimientos para alcanzar la resiliencia operacional. Los requerimientos son estudiados a partir de los servicios ofrecidos y los activos que los soportan [3].
- Soluciones de ingeniería resilientes: asegurar que el software y los sistemas desarrollados, cumplan con los requerimientos de resiliencia establecidos [3].
- Continuidad del servicio: asegurar la continuidad de las operaciones vitales que soportan el buen funcionamiento de los servicios, aún en momentos de ruptura. Son fuentes de interrupciones, incidentes, desastres naturales u otros eventos de impacto negativo [3].

3.3. Modelos de madurez

El termino madurez, dentro del contexto de la gestión del riesgo, hace referencia al grado de institucionalización de uno o más procesos implementados al interior de una empresa [3]. Entre mayor grado de madurez o capacidad el proceso está mejor articulado con otros procesos y existe un compromiso continuo por parte de las personas involucradas para su desarrollo. La madurez es evaluada de manera individual en cada proceso, entendiendo que no todos los procesos de la empresa requieren el mismo grado de madurez.

En muchos aspectos la madurez o capacidad de un proceso puede confundirse con el mejoramiento continuo. Sin embargo, mejoramiento continuo hace referencia al ciclo de vida del modelo aplicado por el marco de trabajo o estándar. Ejemplo de ello son las normas ISO, que al aplicar su ciclo planear-hacer-verificar-actuar, procuran en cada iteración obtener mejoras sustanciales en la totalidad de los procesos participantes del ciclo, sin que esto implique la existencia de un indicador de mejoramiento alcanzado por cada iteración. [22] y [3] desarrollan el concepto de madurez como se ve a continuación.

Cobit 5 [22] plantea 6 niveles de madurez posibles, para cada uno de los 37 procesos que componen su modelo:

- Nivel 0 – Proceso incompleto: El proceso no ha sido implementado. En este nivel, la evidencia de logro del proceso es poca o no existe [22].
- Nivel 1 – Proceso realizado: El proceso descrito anteriormente logra sus objetivos iniciales [22].
- Nivel 2 – Proceso gestionado: (dos atributos): El proceso en estado realizado, ahora es gestionado (planeado, monitoreado y ajustado), sus productos son controlados y mantenidos [22].
- Nivel 3 – Proceso establecido: El proceso en estado gestionado, ahora es implementado usando definiciones específicas y es capaz de alcanzar resultados.
- Nivel 4 – Proceso predecible: El proceso en estado establecido, ahora opera dentro de los límites definidos y alcanza nuevos resultados.
- Nivel 5 – Proceso optimizado: El proceso en estado predecible, ahora es mejorado para alcanzar las metas de negocio, actuales y futuras.

En el modelo propuesto por CERT-RMM, cada uno de los 26 procesos tienen asociadas metas específicas y genéricas; prácticas específicas y genéricas; productos resultados y sub-prácticas. El grado de capacidad de cada proceso depende del número de metas y prácticas genéricas alcanzadas.

- Capacidad nivel 0 – Incompleto: Proceso no desarrollado o parcialmente desarrollado. Una o más metas específicas sugeridas por el modelo no son cumplidas. No existen metas genéricas para este nivel pues es posible que este proceso no requiera institucionalización en la organización [3].
- Capacidad nivel 1 – Realizado: El proceso cumple todas las metas específicas sugeridas por el modelo. El proceso soporta las prácticas que conducen a la resiliencia operacional definidas en las metas específicas. Los logros alcanzados se pueden perder en el tiempo, por tanto requiere continuar mejorando su grado de institucionalidad [3].
- Capacidad nivel 2 – Gestionado: El proceso es planeado y ejecutado de acuerdo con la política; emplea personas capacitadas para generar resultados controlados; involucra a los beneficiarios del proceso; adicionalmente es monitoreado, controlado y revisado. En este nivel las prácticas definidas se mantienen durante los tiempos de estrés o interrupción [3].
- Capacidad nivel 3 – Definido: Es el máximo grado de institucionalización alcanzado por un proceso. Algunas características de un proceso definido son; está ajustado a la medida de la organización, tiene propósitos establecidos, criterios de entrada, actividades, roles asociados, evaluación, pasos de verificación y criterios de salida [3].

3.4. *Integración con otros marcos de trabajo o estándares*

Al interior de los marcos y estándares estudiados por el presente articulo, se encuentran constantes referencias a prácticas complementarias ubicadas en otros marcos, códigos o estándares. En el caso del estándar Británico para la gestión de riesgos [12] se referencia a [13] y [10] como estándares complementarios. De manera similar ocurre con ITIL [14], el cual propone incluir sus prácticas dentro del estándar ISO 20000 [20] en calidad de complemento a lo establecido por el estándar. Desde ITIL también se referencia a [22] como una propuesta de integración de buenas practicas de TI (ITIL) más un marco de control y gobernanza de TI. En esta tendencia de integrar marcos de trabajo, códigos de buenas prácticas y estándares, se destacan [22] y [3] por incluir dentro de sus modelos una propuesta viable y coherente de integración con otros marcos de trabajo.

En Cobit 5 [22] en cada uno de los 37 procesos del modelo incluye un sección denominada *guía relacionada* [22], donde se referencia una o más prácticas complementarias al proceso, más el detalle de la práctica de acuerdo con la numeración propia de la práctica referenciada en otros marcos de trabajos o estándares.

En CERT-RMM existe un documento complementario al modelo [28], donde se mapean cada uno de los 26 procesos incluyendo prácticas, metas, sub-practicas frente a [12], CMMI, [8], [20], [10], [19], NFPA-1600, PCI-2009. Adicionalmente debido al fuerte vinculo entre el CERT y NIST (Instituto Nacional de Estándares y Tecnología), se desarrollo otro documento dedicado a mapear RMM [27] frente a las diferentes publicaciones de NIST relacionadas con la gestión del riesgo [17], [16], [11], [9].

A marcos como [22] y [3] les podríamos llamar meta-marcos o marco de marcos, pues funcionan como estructuras más grandes, articuladoras de las mejores prácticas extraídas del conjunto de lineamientos aplicables a la gestión de riesgo. Adicionalmente, estos meta-marcos pueden ser utilizados cuando se requiere la implementación de múltiples estándares, exigidos en las regulaciones legales establecidas para un sector o empresa.

3.5. *Certificación*

Aunque la implementación de todos los marcos de trabajo o estándares recibe una validación o certificación por parte de la empresa u organización creadora, no en todos los casos se convierte en un reconocimiento internacional y válido para cumplir con las regulaciones legales de cada país o los estándares de calidad esperados en algunos sectores empresariales. A continuación se describen las generalidades de las certificaciones alcanzadas por los marcos de trabajo y estándares estudiados.

COSO-ERM [18], es una iniciativa de algunas empresas del sector privado Estadounidense. Por tanto es recomendable su implementación para cumplir con las regulaciones establecidas en la ley Sarbanes–Oxley [21]. Es posible que la certificación bajo [18] no tenga el mismo impacto y validez requerida, en comparación con estándares publicados por ISO o BSi.

De otro lado tenemos a [12] y [13] hacen parte de los estándares publicados por el Instituto de Estándares Británicos (BSi). Los estándares de Bsi, son aplicados en más de 150 países, la implementación de sus estándares por ente tiene un

reconocimiento internacional o fácilmente homologable.

En la línea de BSi se encuentran los estándares publicados por la Organización Internacional de Normalización (ISO), reconocida como la más grande organización no gubernamental desarrolladora de estándares en el mundo. Hacen parte de los estándares publicados por ISO, las series ISO/IEC 270000 y ISO/IEC 200000 entre muchas otras relacionadas con la gestión de riesgo en los procesos de TI.

A diferencia de los estándares ya mencionados, ITIL es desarrollado por la Oficina de Comercio del Gobierno Británico. Su amplia aplicabilidad y efectividad le hacen el código de buenas prácticas de TI con mayor reconocimiento. Como se presenta en este trabajo, no está directamente relacionado a la gestión del riesgo, sin embargo puede ser aplicado como una estrategia válida para minimizar el riesgo en los procesos de TI ante amenazas internas o externas.

El Instituto Nacional de Estándares y Tecnología es una agencia federal del Departamento de Comercio Estadounidense, encargada del desarrollo de estándares aplicables, a los sistemas de información gubernamentales. Las publicaciones especiales de la serie 800 hacen parte de los muchos estándares desarrollados por NIST. Debido al reconocimiento del instituto y el avance de la industria Estadounidense, sus estándares son bien valorados a nivel internacional.

ISACA es la organización encargada del desarrollo de [22]. Su antigüedad la posiciona como uno de los referentes internacionales en estándares relacionados a tecnología. No solo certifica la aplicación de [22] a nivel empresarial, sino que también califica la fuerza laboral de una empresa mediante la certificación de competencias. Al igual que ITIL sirve de código de buenas prácticas a otros estándares entre ellos ISO y Bsi.

Finalmente CERT-RMM fue desarrollado por la Universidad Carnegie Mellon. Hace parte de muchos otros modelos propuestos entre ellos el conocido CMMI. No existe una certificación similar a las que entregan ISO o Bsi para [3], como resultado de finalizar la implementación del estándar. Esto se explica debido a que es una organización sin ánimo de lucro; sin embargo provee certificaciones individuales para quienes desean validar sus conocimientos alrededor de la aplicación y soporte del modelo.

De los marcos de trabajo y estándares mencionados anteriormente, solo los documentos publicados por NIST y CERT no tienen un costo asociado. Por los demás se debe pagar una cantidad de dinero, que garantiza el acceso al documento en formato digital o impreso. Posterior a la implementación del estándar, se debe pagar para que una empresa, autorizada por el desarrollador del estándar, para que efectúe la evaluación con fines a obtener la certificación.

4. *Conclusiones*

Las organizaciones requieren de marcos de trabajo, códigos de buenas prácticas y estándares que les permita articular el manejo del riesgo de sus procesos de negocio con los procesos de TI. Al no ser una tarea trivial, en muchos casos es recomendable aplicar procesos y estrategias provenientes de diferentes marcos de trabajo y estándares que finalmente contribuyan a fortalecer el manejo del riesgo.

De igual forma se requiere medir el grado de institucionalización de los procesos de misión crítica para determinar con claridad su nivel de resiliencia y su capacidad de recuperación frente a interrupciones o rupturas provocadas por fuentes internas o externas a la organización.

Algunos marcos de trabajos o estándares no tienen la suficiente documentación para integrarlos de manera sistemática con otros códigos de buenas prácticas o estándares relacionados; en esta situación resulta de gran utilidad la aplicación de meta-marcos como los propuestos por Cobit o RMM. Finalmente, si se requiere la certificación posterior a la aplicación de un estándar, se debe observar su validez nacional e internacional y su cumplimiento frente a las regulaciones legales del país donde se localice la organización.

Referencias

[1] R.A. Caralli, J.H. Allen, P.D. Curtis, D.W. White, L.R. Young, "Improving Operational Resilience Processes: The CERT Resilience Management Model," Social Computing (SocialCom), 2010 IEEE Second International Conference on, vol., no., pp.1165-1170, 20-22 Aug. 2010 doi: 10.1109/SocialCom.2010.173

[2] A. Jones, “A framework for the management of information security risks,” BT Technology Journal, Vol. 25, No. 1, January 2007

[3] R.A. Caralli, J.H. Allen, D.W. White, “CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience”. Addison-Wesley, 2011

[4] R. Starr, J. Newfrock and M. Delurey, “Enterprise Resilience: Managing Risk in the Networked Economy,” strategy+business 30, 2003

[5] K. J. Soo Hoo, “How Much Is Enough? A Risk-Management Approach To Computer Security”. PhD thesis, Stanford University, CA, 2000. http://cisac.stanford.edu/publications/11900/.

[6] W. Boehmer, “Survivability and business continuity management system according to bs 25999. In: Proc. Int. Conf. on Emerging Security Information, Systems and Technologies (SECURWARE 2009), Athens/Vouliagmeni, Greece, IEEE Computer Society (June 2009)

[7] P. E. Proctor, “EightPractical Tips to Link Risk and Security to Corporate Performance”, Gartner ID Number: G00173779, January 2010

[8] ITGI. “Cobit, control objective in information and related technology”, 4th. ed. IT Governance Institute, ISBN 1-933284-37-4, 2006.

[9] NIST SP 800-30, “Risk Management Guide for Information Technology Systems”, National Institute of Standards and Technology (Special publication 800-30)

[10] International Organization for Standardization and International Electrotechnical Commission. “ISO/IEC 27001:2005, information technology - security techniques - information security management systems- requirements”, 2005.

[11] NIST SP 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems”, National Institute of Standards and Technology (Special publication 800-37)

[12] British Standards Institution. “Business Continuity Management – Part 1: Code of Practice”. British Standard BS 25999–1:2006, BSI Group, 2006.

[13] British Standards Institution. “Information and communications technology continuity management – Code of practice”, British Standard BS 25777: 2008”, BSI Group, 2008.

[14] Office of Government Commerce, “ITIL Service Strategy”, TSO, London, 2011

[15] International Organization for Standardization, “ISO/IEC 27001 for Small Businesses Practical advice”, 2010. http://www.iso.org/iso/specific-applications_it-security

[16] NIST SP 800-34, “Contingency Planning Guide for Federal Information Systems”, National Institute of Standards and Technology (Special publication 800-34)

[17] NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View”, National Institute of Standards and Technology (Special publication 800-39)

[18] COSO, “Enterprise Risk Management - Integrated Framework. Executive Summary”. Committee of Sponsoring Organizations of the Threadway Commission, (2004)

[19] International Organization for Standardization and International Electrotechnical Commission. “ISO/IEC 31000:2009, Risk management – Principles and guidelines”, 2009.

[20] International Organization for Standardization and International Electrotechnical Commission. “ISO/IEC 20000-1:2011, Information technology -- Service management -- Part 1: system requirements”, 2009.

[21] PUBLIC LAW 107- 204 - SARBANES-OXLEY ACT OF 2002, Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html, 2002.

[22] ITGI. “Cobit 5, A business framework for the governance and management of enterprise IT”, IT Governance Institute, ISBN 978-1-60420-237-3 , 2012.

[23] Office of Government Commerce, “ITIL Service Design”, TSO, London, 2011

[24] Office of Government Commerce, “ITIL Service Operation”, TSO, London, 2011

[25] Office of Government Commerce, “ITIL Service Transition”, TSO, London, 2011

[26] Office of Government Commerce, “ITIL Continual Service Improvement”, TSO, London, 2011

[27] K. G. Partridge, L. R. Young, “CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1 ”. Carnegie Mellon, 2011

[28] K. G. Partridge, L. R. Young, “CERT® Resilience Management Model (RMM) v1.1: Code of Practice Crosswalk Commercial Version 1.1 ”. Carnegie Mellon, 2011