Guía para la Implementación de Resiliencia en el Software de un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores Prácticas

José Domingo Carrillo Verdún, Kevin Edgardo Ducón Pardey
Facultad Informática
Universidad Politécnica de Madrid
Madrid - España
jcarrillo@fi.upm.es, usokkev@gmail.com

Resumen: *El papel de la tecnología, y específicamente del software, en las organizaciones es mucho más relevante, lo que en su momento era innovación, hoy por hoy es un soporte a varias funciones del negocio y la automatización de procedimientos vitales para el alcance de la misión de la organización. Dada la complejidad de los procesos en los que interviene, es cada vez más crítico y los defectos en su fabricación son el objetivo fundamental de delincuentes y uno de los mayores riesgos para las organizaciones. Las organizaciones pueden construir, adquirir o contratar software, y debe saber si en dichos procesos se ha tenido en cuenta las amenazas y nuevos ambientes de riesgos, la relación entre el software y los servicios de alto valor, y si existen planes de seguridad y continuidad sobre los servicios. Para esto se propone establecer estrategias de Protección y Sostenimiento que garanticen que el software tendrá la máxima disponibilidad posible para funcionar posteriormente a un evento de interrupción o estrés –así sea en condiciones degradadas– evitando paradas en los servicios, lo que llamamos resiliencia operacional. Esto será una estrategia desde la dirección hasta la operación, asegurando que durante todo el ciclo de vida del software y durante su administración se sigan los procedimientos, planes, metodologías y técnicas necesarias que aseguren que el software es resiliente y que cumple con los requisitos de resiliencia a nivel operacional. Esta guía busca orientar a la organización en las prácticas que implican asegurar la resiliencia operacional del software y la resiliencia del software como tal, basándose en modelos, estándares y mejores prácticas, tanto para la construcción, adquisición o contrato de software, que aporten a la implementación de la resiliencia operacional, enmarcada por un modelo de gestión de TI y bajo los principios de gestión de la seguridad, gestión de servicios de TI y continuidad del negocio.*

Abstract: *The role of technology, specifically software, in organizations is much more relevant, what at some time was innovation, now is support of multiple business functions and automation of vital procedures in order to reach organization's mission. Given the complexity of the processes which is involved, Software is becoming more critical and its defects are the main objective of attackers and one of the greatest risks for organizations. Organizations can build, purchase or contract software, so they must know if has they taken into account new threats and risk environments, the relationship between software and high-value services, and if there are security and continuity plans on services. For that reason we propose to develop protect and sustain strategies to ensure that software will have the highest availability to work after a disruption or stress event –whether in degraded conditions– avoiding service stops, what we call operational resilience. This will be a strategy from management to operation, ensuring that throughout the software life cycle and during administration, procedures, plans, methodologies and techniques are followed, to ensure that the software is resilient and met operational-level resilience requirements. This guide seeks to lead the organization in practices involving ensure software operational resilience and software resilience as such, and it's based on standards, models and best practices both for software build, acquisition or contract, that contribute to the implementation of operational resilience, framed by an IT management model and the principles of security management, IT service management and business continuity.*

Keywords: *Resilience Management, Operational Resilience, Resilient Software, IT Governance, IT Management, IT Service Management, Business Continuity, Security Management.*

1. Introducción

Actualmente las organizaciones invierten en seguridad TI no solo por las amenazas de diferente índole que surgen a lo largo del tiempo, sino también porque TI ha transformado el negocio al punto que parte de sus servicios operacionales dependen de la infraestructura tecnológica de la organización.

Gartner afirma que en seguridad de TI sólo se gasta entre el 2% y el 7% del presupuesto total de IT, del cual la mayoría se gasta en la seguridad de las perimetral [1], en contraste, indica que el 75% de las amenazas de seguridad pertenecen a la capa de aplicación y si se redujeran el 50% de vulnerabilidades en el software antes que saliera a producción, los costes que estas generan se reducirían al 75% [2].

El software suele soportar servicios de alto valor para la organización, y por esto se le valorará en cuanto al riesgo que representa su interrupción para el alcance de la misión de los servicios. La organización en su haber puede construir, adquirir o contratar software. El producto puede ser el mismo y suplir la misma funcionalidad, pero las responsabilidades, los procesos, las vulnerabilidades, el soporte y en general la gestión sobre el software cambia.

Los defectos en el software se deben en gran parte a fallos en el proceso, en el ciclo de vida y en algunos casos, importa más el precio o el tiempo de la entrega que la calidad, todo lo cual influye en que no se tengan en cuenta los requisitos de seguridad desde el principio del proyecto. Las amenazas que tiene el software no solo son a nivel técnico, el auge de los atacantes, los excesivos privilegios internos, acceso de terceras partes, ingeniería social y negligencia interna e inclusive el riesgo que el proyecto no se lleve a cabo son otras causas igual de comprometedoras. Del mismo modo situaciones impensables e improbables (*Black Swan*) que se materializan, ataques terroristas, fuerzas de la naturaleza, en fin. Actualmente esta tarea la tiene que llevar la gestión de riesgos.

Debido al entorno complejo de las organizaciones en la actualidad, los directivos se fijan en tres cambios en los ambientes de control de riesgos [3]: Sienten que los marcos y proceso de riesgos que siguen actualmente en la organización no les dan el nivel de protección que necesitan; ven como se incrementa tanto la velocidad en la que los eventos de riesgo se producen, como la extensión en la cual su impacto en el negocio es "contagioso", lo que quiere decir que se extiende por las diferentes categorías de riesgo, con una preocupación mayor sobre la velocidad y contagio de los riesgos catastróficos, que pueden amenazar la existencia de la organización e inclusive la industria entera; sienten que se gasta mucho tiempo y dinero en los actuales procesos de gestión de riesgos, en vez de considerar los ambientes cambiantes para actuar de manera rápida y flexible en la identificación y ataque de nuevos riesgos, e inclusive algunas directivas consideran que no se justifica el gasto frente al retorno de nivel de protección.

Por esto PriceWaterhouseCoopers propone tres pasos para ir más allá del ERM: Desarrollar una cultura de conciencia de riesgos, un enfoque explícito sobre el apetito de riesgos y un alineamiento entre riesgo y estrategia [3]. La resiliencia operacional forma parte del primer paso, pues va más allá de identificar, medir y priorizar los riesgos, e intenta proteger y sostener los activos que le dan mayor valor a la organización debido al servicio que prestan y adicionalmente desarrolla la cultura de conciencia de riesgos en la organización.

Tendremos que establecer estrategias de Protección y Sostenimiento que garanticen que el software tendrá la máxima disponibilidad posible para funcionar posteriormente a un evento de interrupción o estrés –así sea en condiciones degradadas– evitando paradas de servicio, lo que llamamos resiliencia operacional. Esto será una estrategia desde la dirección hasta la operación, asegurando que durante todo el ciclo de vida del software y durante su administración se sigan los procedimientos, planes, metodologías y técnicas necesarias que aseguren que el software es resiliente y que cumple con los requisitos de resiliencia a nivel operacional.

Algunos proyectos de software ya implican el concepto de Software seguro, que es aplicar mejores prácticas de seguridad para el diseño, construcción y pruebas. Este software está "blindado" a vulnerabilidades conocidas y probadas, y es una práctica que requiere de un alto conocimiento. Sin embargo un software seguro no necesariamente ofrecerá resiliencia operacional, pues las relaciones que tenga el software con otros activos como tal y los servicios que llegue a soportar, implican que los requisitos de resiliencia del software, enmarcados dentro de la resiliencia operacional, nos haga plantear nuevas medidas –aparte de las técnicas– e implantar una cultura para la resiliencia del software y de su implicación con los servicios.

Este artículo explica el proceso de desarrollo de la Guía, que tiene como objetivo orientar a la organización para tener en cuentas esas medidas a través de prácticas basadas en un modelo de resiliencia operacional para asegurar la resiliencia operacional del software y la resiliencia del software como tal, basándose en

modelos, estándares y mejores prácticas, tanto para la construcción, adquisición o contrato de software, enmarcada por un modelo de gestión de TI y bajo los principios de gestión de la seguridad, gestión de servicios de TI y continuidad del negocio.

2. Estado del arte

2.1. Estándares y mejores prácticas para el entorno de Implantación en la organización

Se propone un entorno de implantación (Figura 1) de la guía de modo que la organización la adapte de acuerdo a los procesos que tenga establecidos.

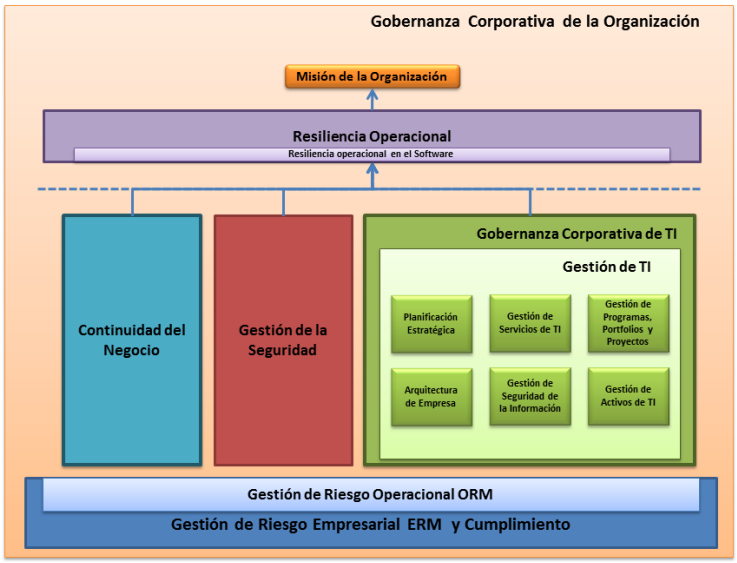


Figura 1. Entorno de implantación de la Guía [4]

La organización debe establecer un marco para la Gobernanza Corporativa, que es la forma en que se organizará, se dirigirá y controlará. Esta gobernanza buscará establecer estrategias que le ayuden a conseguir los objetivos y la misión de la organización. La organización, con el fin de alcanzar sus objetivos y frente a las amenazas existentes establece un marco de gestión de Riesgos ERM para o que se sugiere utilizar los alineamientos propuestos en la familia ISO/IEC 31000:2009.

En cuanto a TI, debe estar establecida una Gobernanza Corporativa de TI, (sistema mediante el cual la TI es dirigida y controlada) que será no solo factor de éxito para la organización, sino que hará de TI un factor de supervivencia, prosperidad y competitividad. En este se sugiere seguir el modelo del estándar ISO/IEC 38500:2008.

Del mismo modo debe estar establecida una Gestión de la Seguridad, es decir que se aseguren los activos críticos de la organización, garantizando la triada CIA (*Confidentiality*, *Integrity*, *Availability*). Para implantar un sistema de gestión de la seguridad, es muy ajustable la norma ISO/IEC 27001:2005.

Paralela a la Seguridad, se debe instituir la Gestión de la Continuidad del negocio, de modo que la organización sea capaz de continuar entregando productos o servicios a unos niveles predefinidos aceptables después de un incidente de interrupción. Para este se sugiere la norma ISO/IEC 22301:2012.

Como se puede ver en la figura 1, la gestión de riesgos suministra o mantiene parte de las actividades de la cada una, sin embargo en la actualidad trabajan por separado, lo que se propone es establecer esfuerzos

coordinados de modo que se trabaje de manera óptima, reduciendo posibles sobrecostos y cambiando el entorno actual de riesgos, situaciones reactivas a proactivas.

La Gobernanza corporativa de TI y la Gestión de TI son conceptos distintos, pero están estrechamente relacionadas pues la norma ISO/IEC 38500:2008 define el concepto de Gestión como: "El sistema de controles y procesos requeridos para la consecución los objetivos estratégicos establecidos por el cuerpo de gobierno. La gestión está sujeta a la guía de las políticas y monitorización establecidas por la gobernanza corporativa." [5] La gestión de TI decide como la TI debe utilizarse para conseguir un uso eficaz y eficiente de los recursos y ayudar a alcanzar los objetivos del negocio. Un marco de Gestión de TI agrupa la mayoría de actividades de la gestión requeridas es COBIT (*Control Objectives for Information and related Technology*), que es una guía de mejores prácticas enfocada a la Gestión de TI, que permite establecer un marco de referencia a través de los recursos que ofrece para su implementación. Es una iniciativa mantenida por ISACA (*Information Systems Audit and Control Association*) y el IT *Governance Institute*. A su vez, la gestión de TI tiene unas disciplinas identificadas por John Thorp (2005): Planificación estratégica, Arquitectura de empresa, Gestión del portafolio, programas y proyectos, Gestión de activos de TI (se puede usar marcos de referencia de *Software Asset Management*), gestión de servicios de TI (ITIL e ISO/IEC 20000), Seguridad de la Información

Una categoría de la Gestión de Riesgo Empresarial ERM es la Gestión de Riesgo Operacional ORM, considerando este riesgo uno de los cuatro tipos de riesgos en la organización junto a los naturales, estratégicos y financieros.

Finalmente tenemos la resiliencia operacional, que considerará estas actividades en un esfuerzo coordinado propuesto por el *Computer Emergency Response Team* del *Software Engineering Institute* de *Carnegie Mellon* en el modelo CERT-RMM (CERT *Resilience Management Model* v 1.0) [6] que será nuestro marco de referencia para la resiliencia operacional. El CERT-RMM tiene 26 áreas de proceso que están organizadas dentro de cuatro categorías de resiliencia operacional de alto nivel: Ingeniería, Gestión Empresarial, Operaciones y Gestión de Proceso. Por área de proceso hay 3 metas genéricas y 13 prácticas genéricas, además de 94 metas específicas y 251 prácticas específicas.

La resiliencia operacional será apoyada por el entorno planteado y otros que influyan en la actividad del negocio como procesos como gestión financiera o recursos humanos. Adicionalmente tenemos la resiliencia en el software que hace parte de los activos de tecnología considerados en el modelo y es donde se pretende ayudar a la organización a través de la guía propuesta.

2.2. Resiliencia operacional y modelo CERT-RMM

Es un hecho que las organizaciones cada vez tienen mayor complejidad, y se desarrollan en ambientes complejos tanto a nivel de negocio como operativo. Dicha complejidad ha hecho que se enfrenten a situaciones de estrés e incertidumbre que provocan interrupciones en la operación efectiva de la organización. Este estrés puede ser producido por la masificación de los avances tecnológicos y la tecno-dependencia de la compañía para hacer eficaces los procesos de negocio y por tanto la complejidad que añade la tecnología a nivel de vulnerabilidades y riesgos; también lo produce la evolución de las organizaciones a nivel de proveedores, asociaciones, outsourcing, etc., crean nuevos ambientes de riesgo; así como la globalización y expansión geográfica de las organizaciones que les obliga a considerar nuevos riesgos y amenazas [6].

La resiliencia operacional “es la propiedad emergente de una organización que puede continuar llevando a cabo su misión después de una interrupción que no excede su límite operacional” [6] Se puede considerar la resiliencia operacional un aporte significativo a la Gobernanza Corporativa, pues será una medida para garantizar que se consiga la misión de la organización, manteniendo operativos los servicios.

La gestión de la resiliencia operacional deberá considerar la complejidad de los entornos de riesgos y como base tendrá que pensar en los riesgos que implica cada actividad. El modelo CERT-RMM considera el concepto de “convergencia” como la armonización de las actividades de gestión de riesgo operacional que tienen objetivos y resultados similares, como fundamental para la gestión de la resiliencia operacional. Esta convergencia involucra la Gestión de TI, Gestión de servicios de TI, Gestión de Seguridad y Continuidad del Negocio. El resultado es el establecimiento de un soporte a los riesgos comunes y una alineación de las prácticas de cada área con el fin de obtener el mayor beneficio para el alcance de la misión de la organización ofreciendo los servicios no solo con las mejores prácticas sino en cualquier situación, de manera óptima en funcionamiento normal y de manera productiva en condiciones de estrés o interrupción.

En resumen, la gestión de la resiliencia operacional tiene cuatro objetivos [6]:

1. Prevenir la el impacto de un riesgo operacional en un servicio de alto valor (instancia de estrategia de protección),

2. Mantener el servicio de alto valor si la amenaza del riesgo se lleva a cabo (instancia de estrategia de sostenibilidad),

3. Tratar de manera efectiva las consecuencias que tiene en la organización que el riesgo se ejecute,

4. Devolver a la organización a un estado de operación “normal” y por último optimizar el logro de estos objetivos para maximizar la eficacia al menor costo.

Poniéndolo en contexto, esto es lo que sucede en la organización: Existen unos activos que soportan uno o varios procesos de negocio que a su vez soportan uno o más servicios que ayudan a conseguir un objetivo que establece la misión de la organización (Figura 2), consideremos que sea un software el activo que soporta un servicio de alto valor para el negocio. Si el software falla, fallará un proceso de negocio y las relaciones con otros activos y servicios. Esto hará que el servicio falle y no cumpla su misión y que tampoco cumpla la de la organización. Lo que propone el modelo CERT-RMM, es establecer la estrategia de resiliencia sobre lo básico, el activo, y sobre este establecer procesos de resiliencia, para el caso del software, buscar la manera que se maneje procesos resilientes en el ciclo de vida del software y software resiliente.

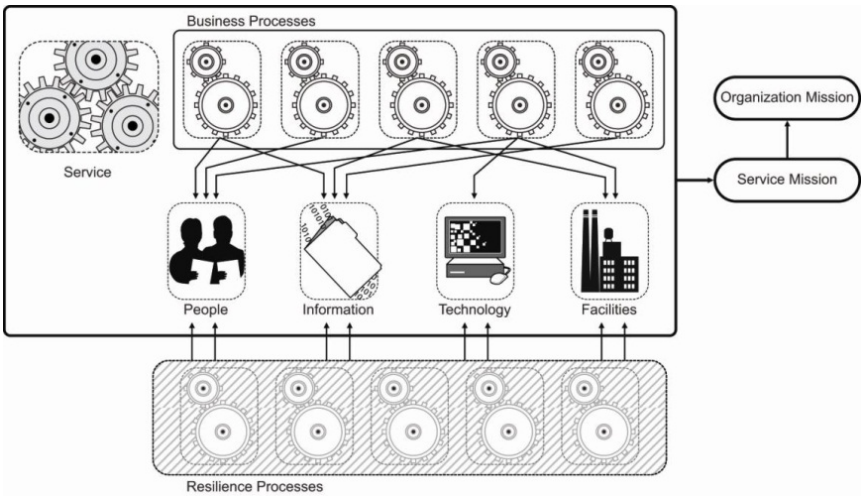


Figura 2. Relación entre Servicios y Procesos de Gestión de Resiliencia operacional Entorno de implantación de la Guía [6]

2.3. Software Resiliente

La TI es fundamental en las organizaciones, no solo para las que prestan servicios basados en TI, sino para todas las que utilizan Sistemas de Información. El Software y los Sistemas son activos ubicuos en las organizaciones que automatizan servicios y soportan procesos de negocio, que ayudan a la organización a la consecución de la misión. Para organizaciones dónde es vital el uso de software y sistemas en cualquier circunstancia y en las cuales se debe mantener el servicio así sea en condiciones degradadas, es necesario considerar la resiliencia como una opción.

Teniendo una idea general sobre Resiliencia operacional, haremos énfasis en lo que concierne a la Resiliencia Software. Teniendo en cuenta la definición de Resiliencia operacional en el CERT-RMM, se puede decir que la Resiliencia del Software es la habilidad de un software para recuperarse y ajustarse a sí mismo en situaciones de interrupción o estrés logrando ejecutar la tarea para la cuál ha sido diseñado, apoyando los servicios de la organización.

No todas las organizaciones están expuestas a las mismas amenazas, ni deben garantizar resiliencia en los mismos servicios, para cada organización la planeación de la resiliencia software es distinta, los requisitos de resiliencia de la organización son diferentes. Los esfuerzos serán a ofrecer software resiliente, es decir un software que sobreviva y sea resistente a amenazas. Esto se logrará a través de un compromiso organizacional que dirija la resiliencia a través de su ciclo de vida, la consideración de amenazas, las condiciones de funcionamiento y el ambiente cambiante de riesgos en los cuales va a operar, así como las prioridades y necesidades de sostenimiento de los servicios que soportan y tener claro que es casi imposible que un software sea resiliente en todos los escenarios, por lo tanto debe asegurar planes de contingencia y continuidad. La idea es hacer de la resiliencia una característica de calidad de software, como lo intenta realizar a nivel de seguridad las iniciativas de Software Assurance. Es casi imposible que un software sea resiliente en todos los escenarios.

Para una organización que enmarcada en la Gobernanza de TI tenga una gestión de la resiliencia organizacional sobre sus activos de software, debe cerciorarse que de acuerdo a sus necesidades, no sólo el software desarrolle sus requisitos funcionales, sino que se realice bajo unos parámetros de calidad y cumpliendo unos parámetros de seguridad, disponibilidad, rendimiento, confiabilidad y sostenibilidad.

Utilizar software resiliente en las organizaciones, tiene sus ventajas y también desventajas que tendrán que ser consideradas de acuerdo a los intereses de la organización (Tabla 1).

Ventajas	Desventajas
Ideal para organizaciones que requieren que sus sistemas trabajen por largos periodos de tiempo. Blindar la operación frente a “fuerzas externas”. Reducir pérdidas a la organización, pues garantiza la misión del servicio y por ende la de la organización. Visión del activo software en función de Protección y Sostenibilidad.	Aumenta la complejidad al sistema. Puede incrementar tiempo y costo de desarrollo y mantenimiento. Mayor formación de las personas que lo han de desarrollar No está al alcance de todas las organizaciones.

Tabla 1. Ventajas y desventajas del Software Resiliente [4]

3. Desarrollo de la Guía

3.1. Consideraciones en la Gestión de Riesgos

El marco de gestión de riesgos que se debe establecer a la hora de pensar en la implantación de un proyecto de resiliencia operacional, y específicamente de resiliencia operacional en el software, debe considerar:

- Que el establecimiento de una buena práctica para la organización de la gestión de riesgos empresariales ERM es un buen inicio para una buena gestión de riesgo operacional ORM.
- La visión de software como inversión, pues la organización espera que se gestione el riesgo de las estimaciones de tiempos y de retornos que se establecen en su inversión y que el enfoque no se haga sólo sobre el producto –como se suele hacer– sino también sobre el proceso, sobre el ciclo de vida.
- Los diferentes tipos de software en la organización, pues su gestión de riesgos para cada caso es distinta.
- Identificar, analizar y mitigar los riesgos enmarcado en las definiciones de tolerancia y apetencia que defina la organización.
- Se debe considerar la teoría del cisne negro o *Black Swan* de Nassim Taleb, que es un riesgo que cumple el triplete: rareza, impacto extremo y retrospectiva (aunque no prospectiva) previsibilidad (p.ej. ataque 11S, ciberguerra). En [3], PriceWaterhouseCoopers justifica la resiliencia como la implementación de una nueva cultura de riesgos que es consciente de los ambientes cambiantes de riesgos, el mayor costo de la gestión de riegos y la necesidad de ejecución de actividades coordinadas.

Para la guía como tal, se consideró el área de proceso RISK de CERT-RMM que establece la responsabilidad de la organización para desarrollar e implementar un plan y un programa para ORM, con base en el ERM, que cubra de manera comprensiva y cooperativa los servicios y activos de alto valor de la organización. Este suministrará información para establecer los requisitos de resiliencia que defina la organización.

3.2. Tipos de Software en la organización

Hay varias tipologías de software, por funcionalidad, por área de conocimiento, por prácticas implementadas, por sectores de la industria, etc. Sin embargo la visión que se considerará en este estudio, es tipo de software por la responsabilidad que tiene la organización sobre él y por el proceso que requiere,

es decir, si la compañía hace el software, contrata a un tercero para su construcción, lo adquiere a una tercera parte, o lo contrata como un servicio. De este modo tenemos cuatro tipos de software:

- **Software construido *in-house*:** La organización tiene un área de desarrollo encargada de construir y mantener el software a nivel interno.
- **Software construido por externos:** La organización contrata a un externo para desarrollar una aplicación a medida. (*Outsourced Development*).
- **Software adquirido:** Es cuando la compañía adquiere un software a una tercera parte. (*Packaged Software*).
- **Software como servicio contratado:** Con la importancia actual de las aplicaciones en *Cloud*, es necesario considerar cuando la compañía contrata el acceso a un servicio que se ajusta a sus requisitos, que corresponde a un software que ya está desarrollado. ITIL v3 introduce el concepto de servicios como activos. Considera que un servicio es un activo para su consumidor.

Sin embargo, aunque tenemos estos tipos, tenemos un denominador común para cualquier tipo de software o sistema, ya sea desarrollando, adquiriendo o contratando la solución, todas requieren un proceso específico, y ahí es donde se tendrá en cuenta la resiliencia, sobre el proceso que requiere el activo software, para ser desarrollado o adquirido.

3.3. Áreas de Proceso CERT-RMM y Tipos de Software

En la figura 3 se pueden ver las relaciones que abordan la resiliencia que refieren a tecnología según el modelo CERT-RMM en ellas se resaltaron las que involucran la construcción, adquisición o contrato de software, algunas áreas involucran directamente con las operaciones y gestión empresarial, que involucran directamente a la consideración general que haga la organización. Casi todas están relacionadas directamente con la Gestión de la Tecnología, por lo tanto consideraremos el marco de aplicación el cual justificará la importancia y el campo de aplicación de la resiliencia en el software para la organización

La mayoría de las áreas de proceso implicadas pertenecen a la categoría de *Ingeniería*, es decir, corresponden a los que se enfocan en establecer e implementar la resiliencia para los activos, procesos de negocio y servicios de la organización, a través de procesos guiados por requisitos. Esta será la base y lo básico para proteger y sostener los activos, procesos de negocio y servicios.

Dentro de esta categoría hay tres subcategorías [6],

1. Gestión de Requisitos –Aborda el desarrollo y gestión de los objetivos de seguridad (proteger) y resiliencia (sostener) de los activos y servicios– (*Desarrollo de Requisitos de Resiliencia* RRD *y Gestión de Requisitos de Resiliencia* RRM),
2. Gestión de Activos –Establece los activos más importantes para la organización– (*Definición y Gestión de Activos* ADM) y
3. Establecimiento y gestión de la resiliencia – Aborda la gestión de controles preventivos, el desarrollo e implementación de la continuidad del servicio y gestión de impacto, y consideración del ciclo de vida de los atributos de calidad de la resiliencia para software y sistemas– Se deberá

considerar conceptos de esquema de exigencia y cierres estructurados. (Gestión de Controles CTRL, *Ingeniería de Soluciones Técnicas Resilientes* RTSE y *Continuidad del Servicio* SC).

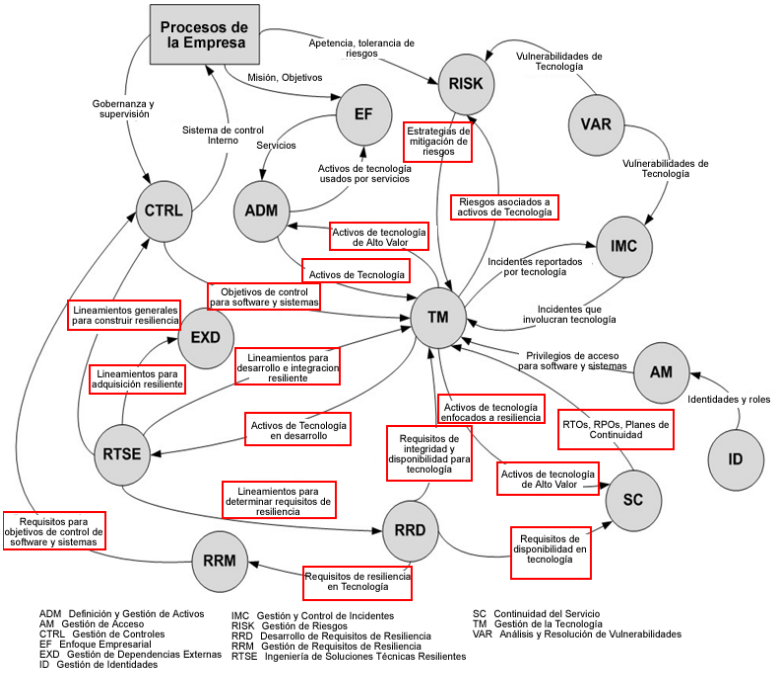


Figura 3. Relaciones que abordan la resiliencia de tecnología [6] resaltado en [4]

Adicionalmente se consideró la *Gestión de Dependencias Externas* EXD. Esta pertenece a la categoría *Operaciones*, y a la subcategoría *Gestión de Proveedores*, y a pesar de no entrar en *Ingeniería* aborda la gestión de dependencias externas y su impacto en la resiliencia operacional de la organización. En esta parte podemos aplicar metas que definan lineamientos para terceros.

Luego de identificar los tipos de software y áreas de proceso de CERT-RMM, estos se relacionaron para el establecimiento de las prácticas aplicable para cada tipo de software (Tabla 2).

Tipo de Software	Área de Proceso CERT-RMM asociada								
	RISK	ADM	RRD	RRM	CTRL	EXD	SC	TM	RTSE
Software construido *in-house*	X	X	X	X	X		X	X	X
Software construido por externos	X	X	X	X	X	X	X	X	X
Software adquirido	X	X	X	X	X	X	X	X	
Software como servicio contratado	X	X	X	X	X	X	X	X	

Tabla 2. Tipos de Software y Áreas de proceso involucradas [4]

Como se indicaba en el apartado 3.1, para todos los tipos de software tendremos un marco de Gestión de Riesgo RISK.

- **Definición y Gestión de Activos ADM:** Su labor es identificar, evaluar la criticidad y valor de los activos por su relación con los servicios, asignar propietarios y vigilantes, entre otras tareas. Aplica para todos los casos.

- **Desarrollo de Requisitos de Resiliencia RRD:** Identificación, documentación y análisis de requisitos de resiliencia con base a los Intereses y consideraciones sobre activos y servicios de alto valor de la organización. Basada en RISK tanto a nivel de empresa, servicio y activo. Aplica para todos los casos.

- **Gestión de Requisitos de Resiliencia RRM**: Gestión de los requisitos durante su ciclo de vida. Los requisitos cambian por intereses, nuevos servicios, nuevos riesgos, etc. Aplica para todos los casos.

- **Gestión de Controles CTRL**: Establecimiento, monitorización, análisis y gestión del sistema de control interno con sus respectivos objetivos de control y controles. Una gestión efectiva considerará estrategias para balancear relación costo beneficio. Aplica para todos los casos.

- **Gestión de Dependencias Externas EXD:** Consideración de la importancia de las entidades externas dentro de la resiliencia operacional de la organización, posibles riesgos que implican y tomar medidas para la protección los activos. Aplica para los tipos que involucren a terceros.

- **Continuidad del Servicio SC:** Es muy difícil que ninguna amenaza se materialice. Esta área se considera como una preparación para afrontar las consecuencias de interrupciones a nivel operativo que se le presentan y aseguramiento de continuidad de operaciones esenciales de servicios y activos relacionados. Aplica para todos los casos.

- **Gestión de la Tecnología TM:** La tecnología inmersa en las operaciones de la organización, hace un aporte significativo a nivel competitivo y estratégico. Como se vio anteriormente, la gestión de la tecnología será la base que relacionará las prácticas y las implementará, será el justificante y del cual se podrán establecer las mejores prácticas para cada una de las áreas. Busca establecer y gestionar un nivel apropiado de controles relacionados a la integridad y disponibilidad de los activos de tecnología para soportar las operaciones resilientes de servicios organizacionales. Aplica para todos los casos.

- **Ingeniería de Soluciones Técnicas Resilientes RTSE:** Busca que la organización establezca para el software construido *in-house*, compromiso para que se desarrolle software que cumpla las necesidades de protección y sostenimiento para así alcanzar la misión del servicio y por tanto la de la organización, y para las organizaciones contratadas para la construcción definir unos lineamientos para que las soluciones que construyen cumplen con los requisitos de resiliencia planteados. La idea es que en el ciclo de vida del diseño y desarrollo de software no solo se contemple cumplimiento de los requisitos funcionales, sino que también contemple requisitos de calidad como seguridad, rendimiento, confiabilidad y sostenimiento. Esto puede implicar un mayor esfuerzo y costo, y aumento de complejidad en los sistemas, por lo tanto se debe estudiar los beneficios a obtener. En algunos casos no considerar estos requisitos, es mucho más costoso cuando se pone en producción [2]. El propósito es asegurarse que el software y los sistemas están desarrollados para satisfacer los requisitos de resiliencia. Se recomendaron algunas prácticas y marcos de referencia como OWASP [7]. Solo aplica a Software construido in-house y el Software construido por externos.

3.4. COBIT y Resiliencia en el Software

Para justificar la aplicación de la guía alineándola a la estrategia que siga la gestión de TI, se utilizó CoBIT 5 [8]. Siguiendo el proceso propuesto, la organización primero debe plantearse qué le motiva a establecer resiliencia operacional y específicamente resiliencia en el software de la organización.

Por ejemplo preguntas: ¿He contemplado todos los riesgos relacionados con TI? ¿Estoy ejecutando una operación de TI eficiente y robusta? ¿Cómo es de crítica la TI para para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible?

Estas preguntas nos relacionarían con al menos tres de las metas corporativas establecidas por COBIT, pero nos centraremos en una que es común y que es un objetivo de la resiliencia operacional y específicamente relacionada con la tecnología, "Continuidad y disponibilidad del servicio de negocio", esto justificado que se busca garantizar la operación del servicio en condiciones de estrés o interrupción.

Las metas de TI relacionadas a la continuidad y disponibilidad son:

- ***Meta 1. Alineamiento de TI y la estrategia de negocio (Secundario).*** Como se pudo ver, concuerda con el CERT-RMM específicamente en el planteamiento de las metas generales. Es necesaria la alineación de TI y negocio como punto de partida para el establecimiento de la resiliencia operacional.

- ***Meta 4. Riesgos de negocio relacionados con las TI gestionados (Primario).*** Es fundamental tener en cuenta un marco de gestión de riesgos. También concuerda con CERT-RMM.

- ***Meta 7. Entrega de servicios de TI de acuerdo a los requisitos del negocio (Secundario).*** La gestión de servicios se debe tener en cuenta para lograr esta meta corporativa, y también concuerda con CERT-RMM.

- ***Meta 8. Uso adecuado de aplicaciones, información y soluciones tecnológicas (Secundario)*** Esta corresponde directamente a la gestión de TI, es decir que también tiene concordancia con CERT-RMM.

- ***Meta 10. Seguridad de la información, infraestructuras de procesamiento y aplicaciones (Primario)*** La gestión de la seguridad es uno de los pilares del planteamiento de la resiliencia operacional para CERT-RMM

- ***Meta 14. Disponibilidad de información útil y relevante para la toma de decisiones (Primario).*** Esta meta considera la importancia del gobierno sobre esta meta relacionada a TI, pues le dará las herramientas (métricas, seguimiento, informes) de la eficacia de las medidas sobre la continuidad y disponibilidad, y en contexto las medidas en resiliencia operacional.

Algunos procesos COBIT relacionados con esas metas de TI fueron seleccionados y se realizó una breve justificación de su relación con la resiliencia software en la tabla 3. Los procesos EDM se relacionan con el Gobierno de TI, el resto con la Gestión de TI.

Proceso COBIT	Justificación
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Es la primera estancia para el establecimiento de la gestión de la resiliencia operacional, por lo tanto aplica para la gestión de la resiliencia software. Se relaciona con metas 1 y 7.
EDM02 Asegurar la Entrega de Beneficios	Asegurar que se obtendrán beneficios de la inversión en resiliencia software. Se relaciona con metas 1 y 7.
EDM03 Asegurar la Optimización del Riesgo	El entendimiento de la tolerancia, apetito de riesgo que acepta la organización en cuanto a servicios basados en software y en la gestión de los riesgos operacionales. Se relaciona con metas 4 y 10.
EDM05 Asegurar la Transparencia hacia las Partes Interesadas	Las métricas que se presenten para informar la eficacia de la implantación de la resiliencia deben contar con la transparencia y conformidad. Se relaciona con meta 7.
AP009 Gestionar los acuerdos de servicio	Es necesaria la identificación de los servicios de TI, y hacer la valoración de los mismos, para identificar los de alto valor y que estén relacionados con el software. Del mismo modo será necesario evaluar los niveles de servicio con las necesidades y expectativas de la empresa. Se relaciona con metas 7 y 14.
APO10 Gestionar los Proveedores	Es necesario que se administren los servicios de TI prestados por todo tipo de proveedores para soportar las necesidades del negocio. Por lo tanto se debe tener en cuenta la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados. Se relaciona con metas 4 y 7.
APO12 Gestionar el Riesgo	Como se indicaba anteriormente, es vital para la resiliencia identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Se relaciona con metas 4 y 10.
BAI03 Gestionar la Identificación y Construcción de Soluciones	Este proceso es el que se ve relacionado de manera directa con la gestión de la resiliencia software, pues la descripción define "Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios." Se relaciona con meta 7. En este apartado hay prácticas específicas relacionadas con la construcción, verificación, calidad, requisitos, que pueden aportar a los tipos de software desarrollados *in-house*.
BAI04 Gestionar la Disponibilidad y la Capacidad	La importancia de este proceso es que establece la evaluación de la disponibilidad actual, y el impacto sobre el negocio. Se relaciona con metas 7 y 14.
BAI09 Gestionar los Activos	A pesar que no está relacionado dentro de las metas, en nuestro caso la resiliencia debe considerar el activo software para clasificarlo, no todo el software es de alto valor para la organización y no todo software de alto valor para la organización está estrechamente relacionado a un servicio de alto valor.
DSS01 Gestionar Operaciones	La gestión de las operaciones se puede relacionar con los procedimientos tanto internos como externos para entrega de los servicios de TI. Se relaciona con metas 4 y 7.
DSS04 Gestionar la Continuidad	La gestión de la continuidad es vital, pues no podemos hacer resiliente al software de cualquier amenaza, por lo tanto hay que tener en cuenta la continuidad en caso que se presente una interrupción.

Tabla 3. Procesos de COBIT 5 [8] relacionados con Resiliencia en el Software [4]

Basado en estos procesos se podrían gestionar las prácticas relacionadas y se podrá establecer la gestión de la resiliencia del software que aporte a las metas de TI y a la vez a la meta de la gestión corporativa. Del mismo modo basado en COBIT podemos asignar responsabilidades sobre cada uno de los procesos que soporta la implantación de la resiliencia del software en la organización.

4. Guía propuesta

4.1. ¿A quién va dirigida la Guía?

La guía va dirigida a todos aquellos interesados en el activo software durante su ciclo de vida, y a aquellos con responsabilidad en la seguridad y continuidad de los servicios en la organización.

Esta guía será utilizada por la dirección para saber cómo el software se mantendrá disponible e íntegro para la operación de los servicios. También será suministro de información de rendimiento para los ejecutivos en el proceso de aseguramiento de la consecución de la misión de la organización frente a amenazas, a través de las TI y específicamente de aquellos servicios que sean basados en software. La cartera proyectos de tecnología lo tendrá como referencia para saber cómo relacionar el proyecto de TI con la estrategia de la organización y qué prácticas seguir para implantar la resiliencia en los proyectos. Los equipos de construcción, personal de seguridad y continuidad, así como los de gestión de riesgos tendrán la tarea de coordinar sus actividades de acuerdo a la guía con el fin de ofrecer servicios resilientes. El equipo de adquisición o contrato, tendrá que tener en cuenta las condiciones que debe cumplir el proveedor de servicios de modo que se mantengan las estrategias de resiliencia operacional con base en el software adquirido o contratado. Los terceros deberán ser conscientes de la estrategia que establezca la organización para mantener operativos sus servicios y comprometerse a través de los contratos o SLA.

4.2. Propósito de la Guía

La guía será una ayuda para implementar la resiliencia en el software, como para los procesos que implica la construcción, adquisición o contrato del mismo, en un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores prácticas, de modo que se asegure la resiliencia operacional de los servicios que soporte el software, a través de estrategias de seguridad y continuidad.

Esta guía de mejores prácticas tiene como referencia el modelo CERT-RMM (CERT Resilience Management Model) que establece una gestión de resiliencia operacional en ambientes complejos y con riesgo de evolución. Traza con los procesos COBIT para establecerlo en un marco de Gestión de TI que apoye la Gobernanza de TI, e incluye estándares que soportan tanto la gestión de los servicios de TI, como la gestión de la seguridad informática y de la continuidad del negocio.

4.3. Beneficios implantar la guía en la Organización

- La guía aporta resiliencia en el software y los servicios que el software soporta. Garantía en las soluciones software en cuanto a disponibilidad e integridad.
- Consideración durante todo el ciclo de vida del software de mejores prácticas en seguridad y continuidad.
- Motiva a la organización a establecer un esfuerzo coordinado en las prácticas para el control y sostenimiento del activo, con el fin de garantizar el éxito en el proceso de negocio, en el servicio, y por ende en la misión de la organización.
- Incentiva el análisis costo beneficio en la implantación de soluciones y puede reducir los costos de la gestión de riesgos.
- Propone prácticas de monitorización y seguimiento durante la implantación.

4.4. Aplicaciones de la Guía

La creciente tecno-dependencia en las organizaciones, y los servicios que soporta el software –siendo actualmente el software uno de los eslabones más vulnerables a amenazas en la organización– la guía es un aporte para garantizar que se realizan las mejores prácticas de resiliencia que le garantiza a la organización la protección y sostenibilidad del software y los servicios que este soporte.

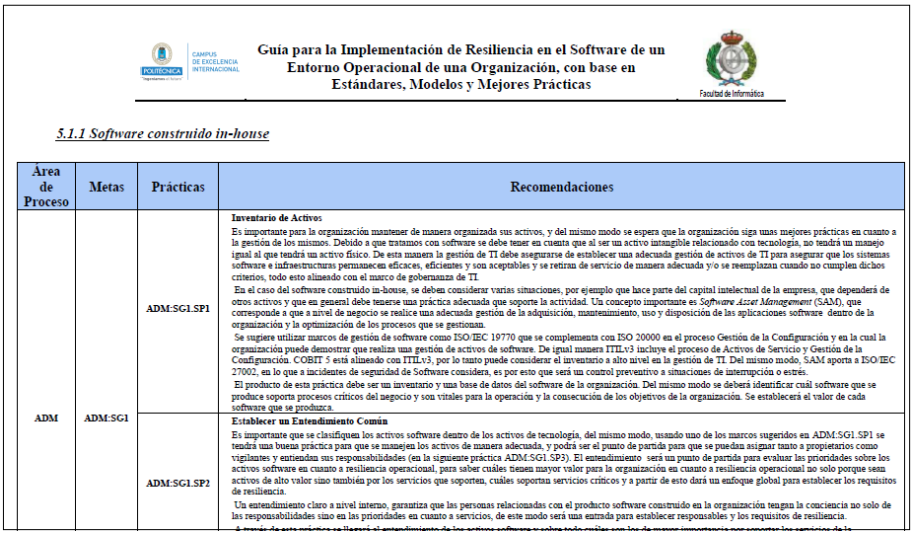
Es aplicable si se necesita establecer mejores prácticas en ciberseguridad, si se tiene por objeto garantizar mejores prácticas de seguridad durante el ciclo de vida del software y a la vez establecer un "blindaje" a los servicios que soporte y una capacidad no solo reactiva sino proactiva a amenazas de seguridad.

Contribuye de manera significativa en un entorno empresarial el cual se base en estructuras complejas debido al trabajo con terceros, tanto para la construcción, adquisición y contrato de software, pues su base es el modelo CERT-RMM que considera estas relaciones y entornos cambiantes de riesgos.

4.5. Guía de Implantación de Resiliencia en el Software de un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores prácticas

Teniendo en cuenta un marco de Gestión de TI como COBIT, que nos da una idea del aporte de la resiliencia software en los procesos de gestión de TI, y del mismo modo conocer el aporte de la resiliencia operacional a los nuevos ambientes más complejos de riesgos, y entrando a fondo en un modelo que nos traza un camino sobre la consideración de la resiliencia operacional en las organizaciones, el resultado de este trabajo es una guía que pretende establecer unas recomendaciones basadas en las prácticas que establece el CERT–RMM para considerar la resiliencia del software en la organización.

La guía consiste en una matriz por cada tipo de software que contiene las áreas de procesos relacionadas con la resiliencia operacional, y estas a su vez con las metas y prácticas asociadas basadas en el modelo CERT-RMM. Sobre estas prácticas se realizaron una serie de recomendaciones que le permitirá al gestor de la resiliencia seguir cada una de las prácticas con las recomendaciones indicadas. Estas recomendaciones se basarán tanto en el análisis del CERT-RMM y se complementará con diferentes marcos de referencia, estándares y mejores prácticas, haciendo énfasis en la importancia y producto de la aplicación de la práctica.



Guía para la Implementación de Resiliencia en el Software de un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores Prácticas

5.1.1 Software construido in-house

Área de Proceso	Metas	Prácticas	Recomendaciones
ADM	ADM:SG1	ADM:SG1.SP1	**Inventario de Activos** Es importante para la organización mantener de manera organizada sus activos, y del mismo modo se espera que la organización siga unas mejores prácticas en cuanto a la gestión de los mismos. Debido a que tratamos con software se debe tener en cuenta que al ser un activo intangible relacionado con tecnología, no tendrá un manejo igual al que tendrá un activo físico. De esta manera la gestión de TI debe asegurarse de establecer una adecuada gestión de activos de TI para asegurar que los sistemas software e infraestructuras permanecen eficaces, eficientes y son aceptables y se retiran de servicio de manera adecuada y/o se reemplazan cuando no cumplen dichos criterios, todo esto alineado con el marco de gobernanza de TI. En el caso del software construido in-house, se deben considerar varias situaciones, por ejemplo que hace parte del capital intelectual de la empresa, que dependerá de otros activos y que en general debe tenerse una práctica adecuada que soporte la actividad. Un concepto importante es *Software Asset Management* (SAM), que corresponde a que a nivel de negocio se realice una adecuada gestión de la adquisición, mantenimiento, uso y disposición de las aplicaciones software dentro de la organización y la optimización de los procesos que se gestionan. Se sugiere utilizar marcos de gestión de software como ISO/IEC 19770 que se complementa con ISO 20000 en el proceso Gestión de la Configuración y en la cual la organización puede demostrar que realiza una gestión de activos de software. De igual manera ITILv3 incluye el proceso de Activos de Servicio y Gestión de la Configuración. COBIT 5 está alineado con ITILv3, por lo tanto puede considerar el inventario a alto nivel en la gestión de TI. Del mismo modo, SAM aporta a ISO/IEC 27002, en lo que a incidentes de seguridad de Software considera, es por esto que será un control preventivo a situaciones de interrupción o estrés. El producto de esta práctica debe ser un inventario y una base de datos del software de la organización. Del mismo modo se deberá identificar cuál software que se produce soporta procesos críticos del negocio y son vitales para la operación y la consecución de los objetivos de la organización. Se establecerá el valor de cada software que se produzca.
		ADM:SG1.SP2	**Establecer un Entendimiento Común** Es importante que se clasifiquen los activos software dentro de los activos de tecnología, del mismo modo, usando uno de los marcos sugeridos en ADM:SG1.SP1 se tendrá una buena práctica para que se manejen los activos de manera adecuada, y podrá ser el punto de partida para que se puedan asignar tanto a propietarios como vigilantes y entiendan sus responsabilidades (en la siguiente práctica ADM:SG1.SP3). El entendimiento será un punto de partida para evaluar las prioridades sobre los activos software en cuanto a resiliencia operacional, para saber cuáles tienen mayor valor para la organización en cuanto a resiliencia operacional no solo porque sean activos de alto valor sino también por los servicios que soporten, cuáles soportan servicios críticos y a partir de esto dará un enfoque global para establecer los requisitos de resiliencia. Un entendimiento claro a nivel interno, garantiza que las personas relacionadas con el producto software construido en la organización tengan la conciencia no solo de las responsabilidades sino en las prioridades en cuanto a servicios, de este modo será una entrada para establecer responsables y los requisitos de resiliencia. A través de esta práctica se llegará al entendimiento de los activos software y sobre todo cuáles son los de mayor importancia para soportar los servicios de la

Figura 4. Vista de la guía en [4]

RPM 10 (1) (2013) ISSN 1698-2029

5. Conclusiones

- El modelo CERT-RMM, en el cual baso la guía, es un aporte significativo para considerar la resiliencia operacional en la organización, y traza perfectamente con mejores prácticas. Del mismo modo, permite que la implementación de la guía se haga en un entorno sin tener que ajustar las condiciones de la organización, si esta tiene un modelo adecuado de gobierno corporativo. Resalto así la importancia de los estándares debido a que sugieren prácticas con las cuáles las organizaciones, a través de las TI, no solo generan valor sino a su vez confianza cara al mercado.

- Una organización que establece una gobernanza de TI que está alineada con la gobernanza corporativa de la organización, tiene más probabilidades de aprovechar las ventajas que ofrece la tecnología para alcanzar los objetivos y la misión de la organización. La parte de gestión de TI debe estar integrada con la gobernanza corporativa de TI para que de la función de TI se obtengan beneficios a nivel operacional. Con esto la implantación de la resiliencia operacional sobre los activos de tecnología será mucho más fácil.

- Los marcos para la Gestión de Servicios de TI, y gestión de la seguridad de la información (que incluye la seguridad informática) y gestión de la continuidad del negocio (que incluye la continuidad del servicio), apoyan una estrategia de gestión efectiva de resiliencia en la organización, y con esto se puede realizar esfuerzos conjuntos y coordinados, y con esto una reducción de costos.

- La gestión de riesgos es una práctica de gran importancia en las organizaciones, sin embargo en algunos casos se queda corta al no considerar los *Black Swan*, y puede ser muy costosa debido a la complejidad de las relaciones internas y externas de las organizaciones y los nuevos entornos de riesgos. Implantar resiliencia puede hacer menos costosa la gestión de riesgos y ambas estrategias pueden apoyarse mutuamente.

- La resiliencia operacional es una la solución para mantener los servicios operativos en caso de estrés o interrupción. Puesto que los servicios operativos de la organización dependen en gran parte de la tecnología, y muchos directamente del software, es necesario establecer mejores prácticas que ayuden a preservar y proteger al software y los servicios que soporte, frente a las amenazas cambiantes actuales de modo que el servicio siga operativo así sea de manera degradada. La experiencia en la aplicación de los principios de resiliencia operacional podrá definir cuáles serán las mejores prácticas para obtener un software resiliente.

- La visión operacional de la resiliencia en el software hace que no solo que el producto cumpla con los requisitos de resiliencia establecidos, sino que lo que implique el proceso dentro de la organización, y las relaciones que tenga con otros servicios y activos, también cumplan con la estrategia de resiliencia de la organización.

- Aplicar metodologías de desarrollo seguro es una buena práctica para hacer software resiliente, pero se deben considerar estrategias de continuidad del servicio en caso que un riesgo se materialice creando situaciones de interrupción o estrés. Un “Software seguro” no necesariamente es un software resiliente, pero todo software resiliente debe ser un “software seguro”.

Referencias

[1] Gartner. Is Your IT Security Budget Immature? Disponible en http://www.gartner.com/technology/metrics/

[2] Morana M. (2009) How to Create a Business Case for Software Security Initiatives. Pág 8. The OWASP Foundation. Disponible en: <https://www.owasp.org/images/7/7b/OWASP-Italy_Day_IV_Morana.pdf>

[3] PriceWaterhouseCoopers. Black swans turn grey. Tranformation of Risk. Visto en: http://www.pwc.com/im/en/publications/assets/Black_swans_turn_grey.pdf

[4] Ducón, K. (2013). Guía para la Implementación de Resiliencia en el Software de un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores Prácticas. Trabajo fin de Máster. Máster Universitario en Ingeniería Informática, Universidad Politécnica de Madrid, España.

[5] ISO/IEC. (2008). ISO/IEC 38500. Corporate governance of information technology.

[6] Caralli, R. A. Allen, J.H. Curtis, P.D. White, D.W. Young L.R. (2010). CERT® Resilience Management Model, Version 1.0. Software Engineering Institute, CERT® Program. Carnergie Mellon University.

[7] The Open Web Application Security Project OWASP (2011). Software Assurance Maturity Model. A guide to building security into software development. Version - 1.0. The Open Web Application Security Project (OWASP).

[8] ISACA. (2012). COBIT® 5 an ISACA® Framework (Serie de tres documentos: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa, Implementación, Procesos Catalizadores).