Recomendaciones para la Gestión de la Continuidad de los Servicios de Tecnologías de Información.

José Solano, Esteban Soto, Julio Córdoba

Escuela de Ingeniería,
Universidad Latinoamericana de Ciencia y Tecnología,
ULACIT, Urbanización Tournón, 10235-1000
San José, Costa Rica
[jsolanoh486,esotos711,jcordobar022]@ulacit.ed.cr
http://www.ulacit.ac.cr

Keywords: Gestión de la Continuidad, ITIL, Plan de Recuperación de Desastres, ISO / IEC 20000

1 Introducción

En Costa Rica, las organizaciones son vulnerables a diferentes tipos de desastres naturales, como terremotos o erupciones volcánicas, y adicionalmente están expuestas a otros tipos de riesgos que podrían afectar las operaciones normales de estas, como por ejemplo, un fallo en un dispositivo de red, ataques informáticos, eventos sociales, como una huelga generalizada del sector público, o acontecimientos de seguridad organizacional, como un conflicto militar, los cuales podrían impedir que una organización brinde sus servicios por varias horas o días (Rushton, 2007). Por lo anterior, es importante para las organizaciones, contar con una adecuada gestión de la continuidad del negocio.

Se entiende como BC[1], la capacidad de la organización para continuar la entrega de productos o servicios en los niveles mínimos aceptables después de un incidente que haya provocado la interrupción de éste (ISO 22301, 2012). En cuanto al BCM[2], se puede definir como un proceso de gestión completo que localiza las amenazas potenciales de una organización y el impacto que podrían causar estas amenazas, mediante un marco para la construcción organizacional con la capacidad de un programa respuesta que salvaguarde los intereses de sus grupos de interés clave, la reputación, la marca y las actividades de creación de valor (ISO 22301, 2012). Es fundamental entender la importancia de prever los eventos antes mencionados, que pueden llegar a afectar las operaciones normales de los servicios de la organización, provocando daños en la infraestructura o cortes de fluido eléctrico, entre algunos de los problemas que se pueden mencionar, materializando así riesgos que se desconocen o que presentan pocas probabilidades de

[1] *Business Continuity* o en español Continuidad del Negocio.
[2] *Business Continuity Management* o en español Gestión de la Continuidad del Negocio.

que ocurran, y que, sin embargo, podrían impactar fuertemente sus negocios, por lo que es significativo, que en caso de ocurrir un evento de esta índole, que las organizaciones continúen brindando servicios de la forma más completa posible. Las organizaciones que no cuenten con una adecuada gestión de la continuidad, quedan expuestas a interrumpir sus servicios durante tiempos indefinidos, lo cual podría tener consecuencias de alto impacto, ocasionando el disgusto sus clientes, llevando en algunos casos a sanciones disciplinarias y regulatorias, así como la pérdida de imagen de la empresa, y dependiendo de la gravedad, hasta la destitución de sus representantes, con las respectivas acciones judiciales por daños y perjuicios (Bautista, 2014).

El objetivo de este trabajo es desarrollar un documento con recomendaciones y mejores prácticas en el tema de la gestión de la continuidad de los servicios de TI, que sirva de guía general para cualquier organización que necesite cumplir con un plan de continuidad del negocio, minimizando el impacto de los eventos en sus operaciones principales y que pueda implementarse en un tiempo menor a 1 año.

Este objetivo se planea realizar mediante una metodología de investigación y análisis de marcos de trabajo, normas y estándares, como ITIL v3 2011 y ISO/IEC 20000, sobre el tema de la Gestión de Continuidad, donde se determine cuáles recomendaciones se pueden extraer de éstos.

Con base en ese análisis, elaborar una guía basada en los marcos de trabajo, normas y estándares mencionados anteriormente, con las mejores prácticas de negocios para la gestión de la continuidad de los servicios, que pueda aplicarse en cualquier organización.

La problemática reside en el hecho de que un gran número de empresas a nivel mundial, no le brindan la importancia necesaria a la gestión de la continuidad de sus servicios, por lo que no implementan acciones preventivas y correctivas que ayuden a las organizaciones a mantenerse funcionando en caso de un evento que atente contra la continuidad de sus servicios.

También muchas organizaciones desconocen la existencia de los instrumentos que ofrece el mercado para gestionar la continuidad del servicio, como son las normas, estándares y marcos de referencia, los cuales abarcan este tema a profundidad, brindando recomendaciones y buenas prácticas a la hora de implementar un sistema de gestión de la continuidad en la organización, con el fin de obtener un mayor panorama del compromiso presente de la organización en el tema de gestión de la continuidad.

2 Marco Teórico

Es de suma importancia la gestión eficaz y eficiente de las operaciones y mantenimiento de los servicios de TI[3], debido a que estos se refieren a mecanismos tecnológicos (*hardware y software*) que logran editar, producir, almacenar, intercambiar y transmitir datos entre varios sistemas de información diferentes que poseen reglas comunes y que son los responsables de la generación, intercambio,

[3] Tecnologías de Información.

difusión, gestión y acceso al conocimiento, tanto a nivel organizacional como personal (Romaní, 2009).

Los servicios de TI constituyen gran parte de los costos de una organización, debido a que estos son fundamentales en la operativa de esta; sin embargo, la gestión de la continuidad es un proceso de negocio que no tiene un beneficio tangible para las organizaciones y que carece de una rentabilidad directa. Pero si bien es cierto, brinda grandes beneficios a las organizaciones al momento de enfrentarse a un incidente que interrumpa sus servicios u operaciones, logrando impedir o minimizar los efectos o consecuencias de una ruptura de servicios que imposibilite a una organización continuar operando de manera normal, tales como defectos en equipos informáticos, tanto de *software* como de *hardware*, desastres naturales, problemas con la infraestructura, errores humanos o actos de terrorismo (Forrester, Buteau, & Shrum, 2011).

Para una correcta gestión de la continuidad de servicios, se deben poner en práctica actividades proactivas y reactivas en las organizaciones. Por medio de las proactivas se busca impedir o minimizar los efectos de una interrupción del servicio; mientras que con las reactivas se intenta reanudar el servicio lo más pronto posible después del evento o desastre. Con esto se busca que la gestión de la continuidad del servicio pueda anticipar, impedir o minimizar la interrupción de servicios de las TI por las situaciones antes descritas, que podrían tener consecuencias catastróficas para las organizaciones (ITILv3, 2011).

Para esto se debe garantizar la continuidad de los servicios por medio del desarrollo, prueba y activación de uno o más planes de continuidad. Con el fin de desarrollar un proceso de continuidad del servicio, es necesario que se conozcan los servicios y recursos críticos de la organización, para identificar cuáles pueden interrumpirse por un periodo de tiempo y cuáles no. Para los servicios críticos que pueden ser interrumpidos por un evento, se debe identificar cuáles son las posibles amenazas, susceptibilidades y su posible impacto en caso de materializarse (Forrester et al., 2011).

Para cumplir con lo antes mencionado, la gestión de la continuidad del servicio debe tener insumos que alimenten el proceso, como lo es el BIA[4], que es una herramienta de gran valor para el proceso de continuidad en las organizaciones, ya que cuantifica el impacto que podría tener la pérdida temporal de un servicio en la organización. Es una herramienta que sirve para identificar los servicios más importantes, para así poder definir una estrategia de recuperación. El propósito principal de un BIA es mostrar cuáles son las partes del negocio más afectadas por un incidente y qué efecto podrían tener en la organización como un todo. La forma de cuantificar los daños o pérdidas puede ser: pérdida de ingresos, costos adicionales, reputación perdida, pérdida de beneficios, pérdida de ventajas competitivas, incumplimiento de leyes, pérdida de cuota de mercado, pérdida de capacidad organizacional, etc. (Wise, 2011).

[4] *Business Impact Analysis* o en español Análisis de Impacto de Negocio.

Actualmente se utilizan los términos BCP[5] y el término DRP[6] como si fueran lo mismo, cuando en realidad no lo son, debido a que el BCP se refiere a cómo las organizaciones deben planear qué hacer en caso de un desastre, mientras que el DRP se refiere específicamente a cómo TI debe recuperarse en caso de un desastre (Bautista, 2014).

Al día de hoy, en la industria, existen organizaciones dedicadas a la creación de marcos de trabajo, estándares o normas que gestionan la continuidad de los servicios. A continuación se mencionan ITIL v3 2011 e ISO/IEC 20000, con el fin de brindar recomendaciones para la debida gestión de la continuidad y disponibilidad del servicio, ya que estas se encuentran alineadas. Otros marcos de referencia, como COBIT 5 y CMMi para servicios, no serán abarcados en este artículo por motivos de alcance y limitaciones de tiempo del proyecto y quedan a futuro.

El marco de referencia ITIL v3 2011 trata de forma muy completa el tema de la continuidad de negocio, dice que hay que establecer las políticas y alcance, evaluar el impacto de la interrupción, analizar y prever los riesgos, establecer estrategias de continuidad, adoptar medidas de prevención, desarrollar planes de contingencia y ponerlos a prueba, además revisarlos periódicamente (ITILv3, 2011).

El ITSCM[7] es el proceso de ITIL v3 2011 que se encarga de los desastres que impactan los servicios de TI y permite que el negocio continúe operando en caso de un evento o desastre. El proceso ITSCM consta de 4 etapas, las cuales se procede a describir (ITILv3, 2011).

Iniciación: sus actividades principales serían definir políticas y alcance los cuales se deben establecer claramente por medio de un política empresarial, los objetivos, el alcance y compromiso de la organización de TI con la gestión de la continuidad del negocio. El alcance debe quedar establecido en función de los planes generales de continuidad de negocio, los servicios estratégicos de TI, los estándares de calidad adoptados, el histórico de eventos de interrupciones y las expectativas de negocio. También se debe asignar recursos, por lo que se debe conocer la disponibilidad de los recursos de la organización. Todo el personal de la organización debe conocer su papel y sus tareas en momentos de crisis. Iniciar los proyectos: la iniciación de la administración de los servicios de continuidad es mucho mejor manejada cuando se hace como si fuera un proyecto, ya que ayuda en la asignación de recursos y las estructuras de control de la organización (ITILv3, 2011).

Requerimientos y estrategia: sus actividades principales serían realizar un BIA, el cual debe ser analizado en función de las consecuencias en la interrupción del servicio, el tiempo máximo que se puede esperar para restaurar un servicio y los compromisos de los SLA[8]. También se deben analizar los servicios

[5] *Backup Continuity Plan* o en español Plan de Continuidad del Negocio.
[6] *Disaster Recovery Plan* o en español Plan de Recuperación de Desastres.
[7] *IT Service Continuity Management* o en español Gestión de la Continuidad del Servicio de TI.
[8] *Service Level Agreement* o en español Acuerdo de Nivel de Servicio.

y sus dependencias debido a que en la actualidad, la mayoría de los servicios de las organizaciones dependen de servicios informáticos. Adicionalmente, se deben definir los servicios estratégicos de la organización, aquellos que son claves para la supervivencia del negocio y poder así apuntar a la continuidad de estos. Para los demás servicios se puede optar por planes de recuperación.
Analizar los riesgos que puedan afectar el negocio: sin conocer los riesgos a los que se enfrenta, es imposible realizar políticas de prevención y recuperación. Se deben enumerar y evaluar los riesgos de acuerdo con la probabilidad e impacto de cada uno, para lo que es necesario conocer profundamente la infraestructura de TI y los elementos involucrados en cada servicio, para así analizar las posibles amenazas con el fin de estimar su probabilidad. Este estudio le será de gran utilidad a la organización para conocer cuáles son los puntos más débiles en su infraestructura. Para la estrategia de ITSCM se deben diseñar estrategias preventivas y de recuperación que ofrezcan garantías suficientes a la organización y que tengan costos razonables. Las preventivas implican análisis de riesgos y vulnerabilidades, por lo que requieren de la colaboración de los altos mandos en la organización, debido a que pueden conllevar cambios a la infraestructura física de la organización. Las actividades de recuperación van a depender en gran parte de los recursos tecnológicos de los que se disponga, ya que podría contarse con tecnología para una recuperación inmediata, recuperación gradual o que requiera movilización completa de toda la organización hacia un sitio alterno.

La Implementación: sus actividades principales serían la de desarrollar, probar e implementar planes, para asignar y organizar los recursos necesarios, por medio planes de prevención de riesgos, gestión de emergencias y recuperación. El plan de ITSCM debe contener toda la información necesaria para recuperar los sistemas de información, redes o servicios de comunicación en caso de darse un evento. El planeamiento organizacional, que se refiere a que la estructura organizacional durante un evento, tiene que ser diferente a la de la operación normal, es por esto que se deben definir equipos de trabajo de varios niveles: ejecutivos, con autoridad y control dentro de la organización para el manejo de crisis; coordinadores, que organicen los esfuerzos de recuperación, que representan las funciones del negocio y servicios vitales de la organización. Otro punto sería la reducción de riesgos, la cual debe ejecutar las acciones necesarias que permitan la puesta en marcha de la estrategia de recuperación, por lo que muchas veces se necesita negociar para tener recursos de recuperación en un sitio alterno, se necesita preparar y equipar ese sitio, además de comprar e instalar todos los equipos necesarios para que estén disponibles en caso de un evento. La última actividad es la implementación de la recuperación, que nos dice que antes de poder utilizar un plan, esté debe probarse, ya que de otra forma podría tener graves consecuencias para la organización, por lo que las pruebas de los planes son una parte crítica dentro del proceso de ITSCM, son la única forma para que la organización se asegure de que la estrategia, logística, procedimientos y planes de recuperación servirán cuando sean necesarios. Se pueden hacer pruebas parciales con solo cierto personal, pruebas de escenarios, si se quiere

probar un determinado escenario o una prueba completa que involucre a toda la organización, siempre tratando que las pruebas sean los más realistas posibles.

La cuarta y última etapa es la operación en uso, cuyas actividades principales son entrenar al personal de la organización, ya que de nada sirve tener completos los planes de prevención y recuperación, si las personas que podrían llegar a usarlos no están familiarizados con ellos. Los planes deben darse a conocer en toda la organización de TI, y deben ofrecer formación sobre los diferentes procedimientos de prevención y recuperación. Adicionalmente, se deben realizar simulacros periódicos para diferentes tipos de desastres como parte de la capacitación, y la información de los planes debe ser accesible para el personal. Como última actividad, se deben revisar periódicamente los planes y hacer los cambios pertinentes, por lo que las políticas, estrategias y planes deben ser revisados y actualizados periódicamente para asegurar que están vigentes para la organización. Cualquier cambio en los planes de negocio o infraestructura puede requerir modificaciones en los planes para adecuarlos a los nuevos entornos.

En la figura 1 se observan las diferentes etapas y actividades del proceso ITSCM de ITIL v3 2011.

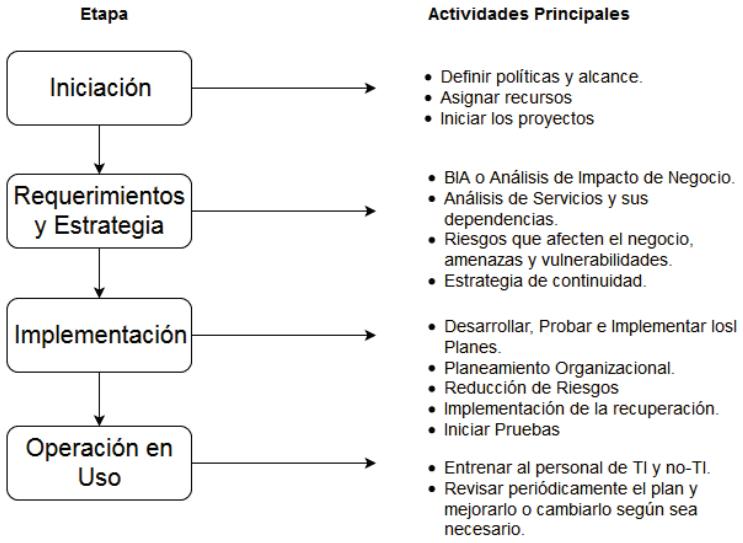

Figura 1. Etapas del ciclo de vida de ITSCM y sus principales actividades.

La ISO/IEC 20000 es una norma internacional de gestión de servicios de TI para organizaciones en las que la tecnología juega un papel primordial para sus operaciones, en donde también se puede emplear para asegurar que sus servicios se encuentran alineados con las necesidades del negocio y que se pueden proveer con un costo moderado. En otras palabras, es un estándar que aplica no

solo a organizaciones de TI que dan servicio a clientes externos, sino también a departamentos de informática cuyo fin son los usuarios internos. Esta norma precisa los requisitos y las características que debe tener un sistema de gestión de servicios de TI y los procesos que éste debe dominar, además requiere de un acercamiento integral que incluya las relaciones con clientes y proveedores.

La norma ISO/IEC 20000 sigue el modelo para la mejora continua de PDCA[9], también conocido como ciclo de Deming, el cual mejora la calidad y la efectividad de los procesos por medio de 4 etapas, que se explican a continuación.

Planear: en esta etapa se definen los objetivos y procesos que se desea mejorar, recolectando datos y atacando las causas de los problemas. Hacer: es en donde se desarrolla e implementa una solución, validando su efectividad por medio de los resultados. Verificar: aquí se confirman los resultados comparando los datos antes y después de la implementación de la mejora. Actuar: esta última etapa es mediante la cual se documentan los resultados, se informa a las partes interesadas sobre los cambios en el proceso y se sugieren recomendaciones para tomar en cuenta en el próximo ciclo (TechTarget, 2015).

La Norma ISO/IEC 20000 no es una competencia directa de ITIL v3 2011, sino que lo complementa, ya que como ITIL v3 2011 no es un estándar, no es posible certificar a las organizaciones en su utilización. La certificación de ISO/IEC 20000 es importante para las organizaciones de TI, ya que es una forma de mostrar a sus clientes o a otras partes de la organización, que se están entregando servicios y procesos de TI de calidad y de forma efectiva (Bauset Carbonell, 2012).

La Norma ISO/IEC 20000 se encuentra constituida en dos documentos que son: ISO/IEC20000-1, el cual contiene los requisitos de acatamiento obligatorio que debe cumplir la organización con el fin de poder gestionar la continuidad del servicio.Y el otro es ISO/IEC20000-2, en el que se trata cada uno de los elementos mencionados en la ISO/IEC20000-1, analizando y explicando su contenido con el fin de ayudar a formar los procesos para que cumplan los objetivos del primer documento(Bauset-Carbonell & Rodenes-Adam, 2012).

Para el tema de continuidad de negocio, en ISO/IEC 20000 se encuentra el proceso de administración de la continuidad y disponibilidad del negocio, el cual contiene 3 subprocesos que se describen a continuación.

Identificar y acordar con los clientes y partes interesadas, los requisitos de continuidad del servicio, dentro de los que al menos se debe incluir: derechos de acceso, tiempos de respuesta y disponibilidad para cada uno de los servicios. Se debe crear, implementar y mantener un plan de continuidad y disponibilidad, el cual debe incluir al menos: procedimientos a utilizar en caso de un evento, objetivos de disponibilidad, requisitos de recuperación, enfoque para el retorno a la normalidad, además de requisitos y objetivos de disponibilidad. Por otra parte, se deben probar periódicamente los planes de continuidad y disponibilidad contra los requerimientos establecidos, especialmente cuando hay un cambio en los servicios. Los resultados de las pruebas deben quedar registrados y deben usarse para tomar las acciones necesarias, incluyendo informar a las partes interesadas.

[9] *Plan-Do-Check-Act* o en español Planear-Hacer-Chequear-Actuar.

En la figura 2 se observan las etapas y actividades del proceso de administración de la continuidad y disponibilidad del negocio de ISO/IEC 20000:

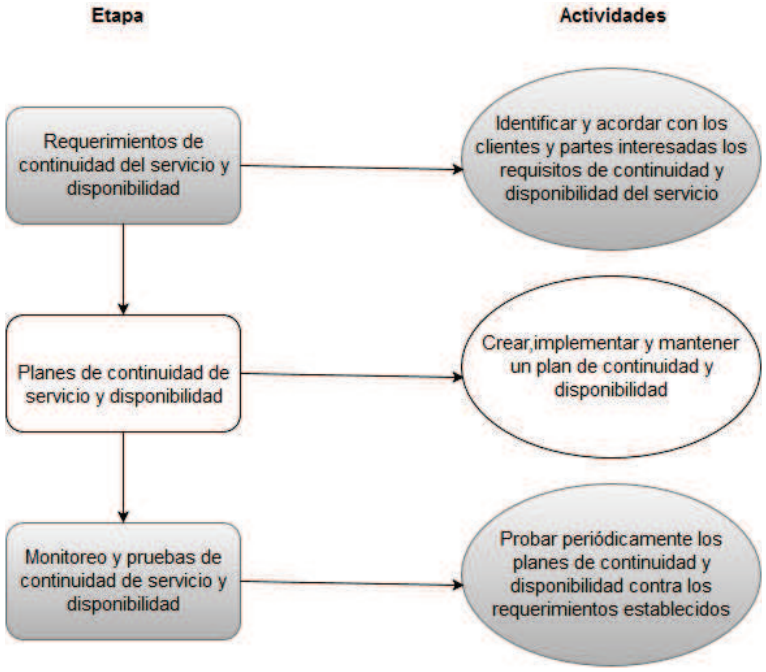

Figura 2. Etapas del proceso de ISO/IEC 20000 administración de la continuidad y disponibilidad del negocio.

3 Comparación de Marcos de Referencia

Al comparar los procesos sobre gestión de la continuidad de ISO/IEC 20000 e ITIL v3 2011, se puede mapear el proceso de administración de la continuidad y disponibilidad de negocio de ITIL v3 2011 con el proceso de administración de continuidad y disponibilidad de servicio de ISO/IEC 20000.

El proceso de administración de la continuidad de ITIL v3 2011 posee 4 etapas, cada una con un conjunto de actividades bien definidas y documentadas, mientras que el proceso de administración de la continuidad y disponibilidad de servicio de ISO-IEC 20000 consta de solo 3 subprocesos, donde las actividades se presentan muy generales. En la tabla 1 se puede observar cómo quedan mapeadas las etapas de ITIL v3 2011 con los subprocesos de ISO/IEC 2000.

Comparación de Procesos		
Marco de Trabajo	**ITIL v3 2011**	**ISO/IEC 20000**
Proceso	Administración de la Continuidad del Servicio de TI	Administración de la Continuidad y Disponibilidad del Servicio de TI
Actividad	Iniciación	No existe
	Requerimientos y Estrategia	Requerimientos de Continuidad de Servicio y Disponibilidad
	Implementación	Planes de Continuidad de Servicio y Disponibilidad
	Operación en Curso	Monitoreo y Pruebas de Continuidad de Servicio y Disponibilidad

Tabla 1. Comparación de los procesos sobre Gestión de la Continuidad de ISO/IEC 20000 e ITIL v3 2011.

La primera etapa del proceso de ITIL v3 2011 es la de iniciación, donde se establecen políticas, se define el alcance y se inicia el proyecto (ITILv3, 2011). En el ISO/IEC 20000 no se especifica una etapa de iniciación y en los siguientes subprocesos no se hace mención de las actividades que indica ITIL v3 2011 (ISO 20000-1, 2011).

Las principales actividades de la etapa 2 de requerimientos y estrategia de ITIL v3 2011 corresponden a realizar el análisis de impacto o BIA, hacer un diagnóstico de los riesgos y definir la estrategia de continuidad de TI (ITILv3, 2011). Este proceso tiene algunas semejanzas con el proceso de requerimientos de continuidad de servicio y disponibilidad de ISO/IEC 20000, cuya actividad principal es identificar y acordar con todas las partes interesadas, los requisitos de continuidad del servicio (ISO 20000-2, 2011).

La tercera etapa, llamada implementación de ITIL v3 2011, es la que tiene más actividades, dentro de las que se puede citar: desarrollar planes de continuidad del servicio de TI, desarrollar planes y procedimientos de recuperación de TI, planeamiento organizacional, reducción de riesgo e implementación de la recuperación y las pruebas iniciales (ITILv3, 2011). En cuanto a ISO/IEC 20000, el proceso de planes de continuidad de servicio y disponibilidad muestra algunas similitudes, siento sus tares principales: crear procedimientos a implementar en caso de pérdida del servicio, establecer objetivos de disponibilidad cuando se invoque el plan, definir requisitos de recuperación, definir el enfoque para el retorno a las condiciones normales de trabajo y definir los requisitos de disponibilidad y objetivos (ISO 20000-2, 2011).

La última etapa en ITIL v3 2011, etapa 4 operación en curso, tiene como actividades principales promover la educación, conciencia y entrenamiento al personal de la organización, revisar los resultados de la aplicación de los planes y auditarlos, pruebas a los planes, y manejo de cambios a los planes, para mantenerlos válidos y actualizados (ITILv3, 2011). En ISO/IEC 20000, el último proceso que tiene que ver con continuidad de negocio se refiere al monitoreo y pruebas de continuidad de servicio y disponibilidad, cuya actividad principal es probar periódicamente los planes de continuidad contra los requerimientos es-

tablecidos, registrando los resultados de las pruebas, modificando los planes de ser necesario y informando a todos los interesados (ISO 20000-2, 2011).

Al momento de hacer esta comparación se puede observar que las etapas de ITIL v3 2011 son mucho más específicas que los subprocesos de ISO/IEC 20000, por lo que se considera una mejor opción comparar las actividades de ITIL v3 2011 contra los subprocesos de ISO/IEC 20000, para determinar de mejor forma las diferencias entre ellos, como se ve en la tabla 2.

Comparación de Procesos y actividades	
ITIL v3 2011	**ISO/IEC 20000**
Administración de Continuidad del Servicio de TI.	Administración de Continuidad y Disponibilidad del Servicio de TI.
Definir políticas y alcance	Identificar los requisitos de continuidad
Asignar recursos	No existe
Iniciar los proyectos	No existe
Realizar el BIA	No existe
Analizar los servicios y sus dependencias	No existe
Analizar los riesgos	No existe
Definir estrategias de ITSCM	No existe
Desarrollar, probar e implementar planes	Crear, implementar y mantener un plan de continuidad.
Planeamiento organizacional	No existe
Reducción de riesgos	No existe
Implementación de la recuperación	Probar los planes de continuidad
Entrenar al personal	No existe
Revisar periódicamente los planes	Los resultados deben usarse para tomar las acciones necesarias

Tabla 2. Comparación de las actividades del proceso de administración de la continuidad del negocio de ITIL v3 2011, contra los subprocesos de la administración de la continuidad y disponibilidad de servicios de ISO/IEC 20000.

En la tabla 2 se observan claramente las diferencias y semejanzas entre el proceso de ITIL v3 2011 y el proceso ISO/IEC 20000, referentes a la gestión de la continuidad. Los tareas de ISO/IEC 20000 se toman de los 3 subprocesos que lo componen y se comparan directamente contra las 13 actividades de ITIL v3 2011, quedando 9 actividades de ITIL v3 2011 sin relacionar, ya que ISO/IEC 20000 no menciona nada similar a esas 9 actividades.

4 Análisis de Resultados

Después del análisis y comparación de los procesos de continuidad de negocios de ITIL v3 2011 e ISO/IEC 20000, se puede concluir que ambos marcos de referencia tienen similitudes y diferencias sobre cómo administrar la continuidad del negocio, ya que ITIL v3 2011 es muy específico sobre las cosas que deben hacerse, mientras que si bien es cierto ISO/IEC 20000 es más general, ayuda

mucho a las organizaciones a orientarse con respecto a cómo deben hacerse las cosas. Es por esto que se puede concluir que ambos marcos tienen aportes muy positivos sobre el tema y que esta propuesta debe incluir lo mejor de ambos.

En la tabla 3 se define la utilización total o parcial de las actividades de ITIL v3 2011, como base para la propuesta del proceso de gestión de la continuidad de este artículo.

Actividad	**Utilización en la propuesta**
Definir políticas y alcance	Total
Asignar recursos	Total
Iniciar los proyectos	Nula
Realizar el BIA	Total
Analizar los servicios y sus dependencias	Total
Analizar los riesgos	Total
Definir estrategias de ITSCM	Total
Desarrollar, probar e implementar planes	Parcial
Planeamiento organizacional	Total
Reducción de riesgos	Total
Implementación de la recuperación	Parcial
Entrenar al personal	Total
Revisar periódicamente los planes	Total

Tabla 3. Actividades del proceso de administración de la continuidad del negocio de ITIL v3 2011 a utilizar como mejores prácticas para la propuesta del proceso de gestión de la continuidad.

En la tabla 4 se encuentran los subprocesos de ISO/IEC 20000 que se utilizarán de forma total o parcial como base del proceso de gestión de la continuidad de este artículo.

Actividad	**Utilización en la propuesta**
Identificar los requisitos de continuidad	Parcial
Crear, implementar y mantener un plan de continuidad.	Total
Probar los planes de continuidad	Total
Los resultados deben usarse para tomar las acciones necesarias	Parcial

Tabla 4. Subprocesos de administración de la continuidad y disponibilidad del servicio de ISO/IEC 20000 a utilizar como mejores prácticas para la propuesta del proceso de gestión de la continuidad.

La propuesta de este artículo toma lo más relevante de las actividades de ITIL v3 2011 e ISO/IEC 20000, agrupadas en los siguientes tres ámbitos.

Requisitos y análisis empresarial

Políticas, objetivos y alcance, para esta tarea se combinan las actividades de ITIL v3 2011 e ISO/IEC 20000, tomando como base ITIL v3 2011 y agregando la parte de ISO/IEC 20000 que dice que se deben acordar con los clientes y las partes interesadas los requisitos de continuidad, quedando de la siguiente manera: definir de forma clara la política empresarial, objetivos y alcance de la organización de TI con respecto a la gestión de la continuidad de negocio, tomando en cuenta los servicios estratégicos de TI, estándares de calidad que se hayan adoptado, interrupciones ocurridas en los últimos 5 años, así como los compromisos con entidades supervisoras, clientes estratégicos, acuerdos con proveedores y otras partes interesadas. Los objetivos y el alcance deben ser realistas y alcanzables con los recursos de tecnológicos y de infraestructura de la organización. Análisis de impacto, al no existir esta tarea en ISO/IEC 20000, se toma como base ITIL v3 2011, en este punto se debe determinar el impacto de los eventos en función de las consecuencias de una interrupción del servicio, que indique tanto el tiempo máximo que la organización puede esperar a que se restaure y los compromisos que tengan con terceros. Análisis de servicios, para esta tarea se toma como base ITIL v3 2011, ya que esta no existe en ISO/IEC 20000, aquí se debe identificar cuáles son los servicios estratégicos a los cuáles se debe dar prioridad en un evento y cuales pueden quedar en un segundo plano. Análisis y reducción de riesgos, al no existir esta tarea en ISO/IEC 20000, se toma como base ITIL v3 2011, enumerar y evaluar los riesgos a los que la organización está expuesta, de acuerdo con la probabilidad y el impacto de cada uno. Se debe trabajar de forma preventiva con aquellos riesgos que podrían impedir la puesta en marcha de una estrategia de continuidad. También se deben tomar las medidas necesarias para que se pueda realizar la recuperación de los servicios de acuerdo con los requerimientos y alcance de la organización. Y el último punto en este ámbito, habla acerca de estrategias de continuidad, para esta tarea, se toma como base ITIL v3 2011, ya que esta no existe en ISO/IEC 20000, se debe diseñar estrategias preventivas y de recuperación de acuerdo con los resultados del análisis de los riesgos. Las preventivas deben buscar solventar los puntos más débiles o vulnerables en la organización, y las de recuperación deben buscar la vuelta a la normalidad de los servicios de la forma más rápida posible, de acuerdo con los recursos con que se cuente.

Planes de acción

En este ámbito se encuentran los planes de continuidad, para esta tarea se combina las actividades de ITIL v3 2011 e ISO/IEC 20000, tomando como base ISO/IEC 20000, complementándolo con información de ITIL v3 2011, quedando de la siguiente manera: se crean, implementan y prueban planes que indiquen por medio de procedimientos, toda la información necesaria a utilizar en caso de una interrupción de servicio, y que además tomen en cuenta los objetivos y requisitos de recuperación definidos por la organización. Otro punto es definir equipos de trabajo, tarea que no menciona ISO/IEC 20000, por lo cual fue tomada de ITIL v3 2011, y en donde se definen, por medio de equipos de trabajo, de diferentes niveles, los responsables de las distintas tareas a realizar

durante una recuperación. El equipo de continuidad de negocio será el responsable de tomar las decisiones ejecutivas. El equipo administrador, responsable de la gestión general del incidente, como asignación de recursos, planificación y coordinación de las tareas. Mientras que los equipos de recuperación que operan en el sitio del incidente, evalúan la extensión de problema y responden en concordancia con el incidente. Las pruebas de recuperación, donde se combinan actividades de ITIL v3 2011 e ISO/IEC 20000, tomando como base ISO/IEC 20000, complementándolo con información de ITIL v3 2011, aquí se prueban los planes de continuidad contra los requisitos establecidos al menos una vez al año o cuando se dé un cambio en los servicios o la infraestructura física o tecnológica. Los resultados de las pruebas deben ser comunicados a todas las partes interesadas y deben utilizarse para tomar las acciones necesarias, como mejoras a los planes o adaptación de éstos. Las pruebas pueden ser totales o de algún escenario específico, y deben ser lo más realistas posible.

Actividades permanentes

Este ámbito se refiere a actividades recurrentes, como la capacitación al personal sobre cuál es su rol en caso de una interrupción, tarea que no existe en ISO/IEC 20000 y que fue tomada de ITIL v3 2011, esta labor puede incluirse en los manuales de inducción a cada puesto y debe estar disponible en todo momento para todos los colaboradores que podrían formar parte de alguno de los equipos de trabajo durante un evento, ya sea por medio de material escrito, correos electrónicos o por medio de la intranet de la organización. El último punto es la revisión continua de las políticas, objetivos, estrategias, alcance, análisis de riesgos, servicios e impacto, así como los planes de continuidad, tomando en cuenta los resultados de las pruebas de continuidad, deben ser revisados y actualizados de forma periódica o en caso de un cambio en el negocio o en la infraestructura de la organización, para asegurar que aún están vigentes, para esta tarea se combinan las actividades de ITIL v3 2011 e ISO/IEC 20000, tomando como base ITIL v3 2011 y agregando la parte de ISO/IEC 20000 que dice los resultados deben usarse para tomar las acciones necesarias.

5 Modelado del proceso

A continuación se muestra el modelo BPMN[10] para la propuesta del artículo por medio de la figura 3.

[10] *Business Process Model and Notation* o en español Modelo y Notación de Procesos de Negocio.

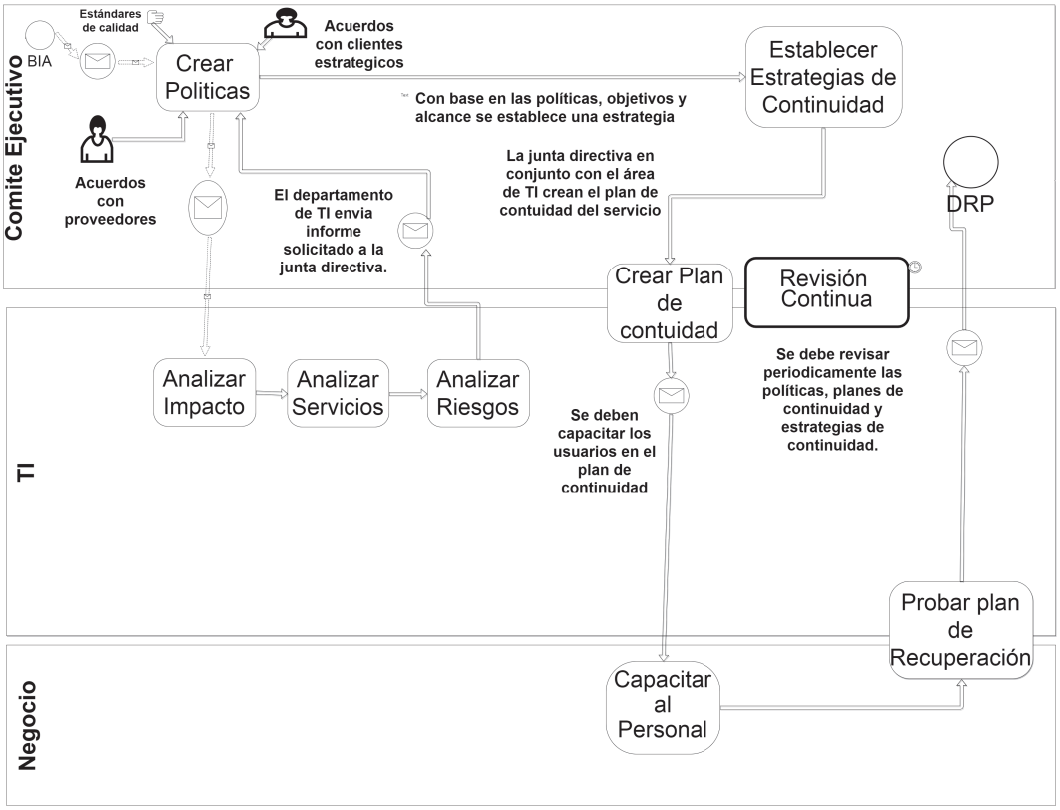

Figura 3. Modelado del proceso de gestión de la continuidad.

6 Casos de Éxito

El primer caso de éxito revisado es el caso del sistema PACS[11] de hospitales universitarios, un complejo de centros médicos sin fines de lucro en Cleveland, Ohio, Estados Unidos. Este sistema es de gran importancia en los tiempos de radiología digital, ya que busca y almacena todas las imágenes de los exámenes médicos, y está integrado con los otros sistemas de información de hospitales universitarios, por lo que cualquier fallo o interrupción podría representar un impacto severo en la atención a los pacientes, por lo que es indispensable asegurar por medio de planes de recuperación de desastres la continuidad del sistema PACS. La solución de DR implementada en hospitales universitarios, es una configuración que provee un acceso ininterrumpido a las imágenes desde varios frentes, por medio de múltiples copias sincronizadas de los datos en al menos dos instalaciones físicas, tomando en cuenta la plataforma de *hardware*, sistemas

[11] *Picture Archiving and Comunication System* o en español Sistema de Archivo de Imágenes y Comunicación.

operativos, conectividad de la red, versión de la base de datos y recuperación fuera del sitio primario por medio de un respaldo completo. Según en el análisis de la solución implementada, se puede inducir que en el caso de hospitales universitarios se utilizaron al menos los siguientes puntos de la propuesta que se plantea en este documento, como se aprecia en la tabla 5 (Mansoori, Rosipko, Erhard, & Sunshine, 2014).

Ámbito	**Utilizado**
Requisitos y análisis	Sí
Planes de acción	Sin información
Acciones permanentes	Sin información

Tabla 5. Ámbitos utilizados de la propuesta, en el sistema de archivo de imágenes y comunicación de hospitales universitarios en Cleveland, Ohio, Estados Unidos.

El segundo caso de éxito que se investigó es el de la AWWA[12],la cual es una asociación internacional sin fines de lucro, científica y educacional, con el fin de mejorar los suministros y la calidad del agua, la cual cuenta con cerca de 50.000 miembros alrededor del mundo. La AWWA desarrolló un recurso de BCP para sus organizaciones que incluye un documento guía, una plantilla y herramientas en línea para que las organizaciones relacionadas con el suministro y tratamiento del agua desarrollen su propio BCP. En esta guía se mencionan varias de las tareas o actividades que se plantean en la propuesta de este documento, como se ve en la tabla 6 (Moyer & Novick, 2012).

Ámbito	**Utilizado**
Requisitos y análisis	Sí
Planes de acción	Sí
Acciones permanentes	Sin información

Tabla 6. Ámbitos utilizados de la propuesta, en el BCP de la asociación americana de abastecimiento del agua.

7 Conclusiones y Recomendaciones

En conclusión, el marco de referencia ITIL v3 2011 brinda una información más detallada sobre actividades para el análisis del impacto, análisis de servicios, análisis de riesgos y definición de estrategias de continuidad. Todas estas labores sirven como insumo para una buena gestión de la continuidad; sin embargo, estas

[12] *American Water Works Association* o en español Asociación Americana de Abastecimiento del Agua

no se mencionan en la norma ISO/IEC 20000. No obstante, esta norma aporta una idea clave que complementa las tareas descritas por ITIL v3 2011, la cual es, que se deben acordar con los clientes y las partes interesadas los requisitos de continuidad, lo cuál se considera primordial para poder cumplir compromisos con los clientes, patrocinadores y entidades supervisoras.

También se concluye que un análisis previo de la organización es vital, con el fin de sentar las bases para un planteamiento que salvaguarde los intereses de la organización, su reputación, su marca y las actividades que le aportan valor, con el fin de reducir la incertidumbre de la puesta en marcha de las estrategias de continuidad del negocio, aumentando así las posibilidades de éxito de los planes de continuidad propuestos.

Los ámbitos propuestos en esta investigación se complementan entre ellos, de forma que el cumplimiento de las actividades propuestas protegerá a las organizaciones frente a un evento que afecte la continuidad de sus servicios de TI. Entre más tareas se logren implementar en las organizaciones, mayores posibilidades de éxito se tendrá en caso de ocurrir un evento en donde se vea comprometida la continuidad de los servicios.

Se recomienda que, como mínimo, las organizaciones apliquen las actividades del ámbito de requisitos y análisis empresarial, ya que estas proporcionan un panorama detallado del entorno de la organización y brindan conocimiento sobre cuáles son los activos y servicios tecnológicos estratégicos, los riesgos que podrían llegar a afectarlos y la selección de la estrategia a utilizar para recuperarse. Lo anterior se fortalece con las tareas detalladas en los ámbitos de planes de acción y medidas permanentes, los cuales detallan a la organización, la forma más eficiente y eficaz de recuperar sus servicios de una manera segura.

También se hace la observación de que la administración de la disponibilidad de ITIL v3 2011 se encuentra fuera del alcance de este artículo por razones de tiempo, por lo que se recomienda abarcar este tema en investigaciones futuras, debido a que la gestión de la disponibilidad y la gestión de la continuidad son procesos de negocio que están altamente relacionados. Igualmente, solo se analizó ITIL v3 2011 como marco de referencia para este artículo, por lo que se recomienda complementar esta investigación agregando otros marcos como COBIT 5 y CMMi para Servicios, con el fin de complementar las buenas prácticas de nuestra propuesta con otros marcos de referencia que aporten más conocimiento a la gestión de la continuidad de los servicios.

Referencias

Bauset-Carbonell, M. C., & Rodenes-Adam, M. (2012). La gestiÓn de servicios de ti: Itil e iso/iec 20000. *DYNA - Ingeniería e Industria*, *87*(5), 492 - 495. Retrieved from `http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=80241268&lang=es&site=ehost-live` pages 7

Bauset Carbonell, M. d. C. (2012). *Modelo de aporte de valor de la implantación de un sistema de gestión de servicios de ti (sgsit), basado en los requisitos de la norma iso/iec 20000* (Unpublished doctoral dissertation). pages 7

Bautista, M. (2014). Marco de referencia para la formulación de un plan de continuidad de negocio para ti, un caso de estudio. *Revista Técnica Energía*, 200 - 207. Retrieved from `http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=95648743&lang=es&site=ehost-live` pages 2, 4

Forrester, E., Buteau, B., & Shrum, S. (2011). *Cmmi for services: Guidelines for superior service*. Pearson Education. Retrieved from `https://books.google.co.cr/books?id=ywvSVLmQmjoC` pages 3

ISO/IEC 20000-1 (Norm No. ISO 20000). (2011). ISO, Geneva, Switzerland. pages 9

ISO/IEC 20000-2 (Norm No. ISO 20000). (2011). ISO, Geneva, Switzerland. pages 9, 10

ISO/IEC 22301 (Norm No. ISO 22301). (2012). ISO, Geneva, Switzerland. pages 1

ITILv3, F. (2011, Jul). *Itil v3 2011.* Retrieved from `http://itilv3.osiatis.es/` pages 3, 4, 9

Mansoori, B., Rosipko, B., Erhard, K., & Sunshine, J., Jeffrey3. (2014). Design and implementation of disaster recovery and business continuity solution for radiology pacs. *Journal of Digital Imaging*, *27*(1), 19 - 25. Retrieved from `http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=94061929&lang=es&site=ehost-live` pages 15

Moyer, J., Jack1, & Novick, k., Kate. (2012). Introducing a new resource for water and wastewater system business continuity planning. *Journal: American Water Works Association*, *104*(3), 37 - 39. Retrieved from `http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=88856484&lang=es&site=ehost-live` pages 15

Romaní, J. (2009). El concepto de tecnologías de la información. benchmarking sobre las definiciones de las tic en la sociedad del conocimiento. *ecompetencies.org*, 295-318. Retrieved from `http://www.ehu.eus/zer/hemeroteca/pdfs/zer27-14-cobo.pdf` pages 3

Rushton, J. (2007). Leveraging itil to improve business continuity and availability. *SDA Asia Magazine*, *21*, 25 - 28. Retrieved from `http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=34013185&lang=es&site=ehost-live` pages 1

TechTarget. (2015, Abril). *Pdca (plan-do-check-act).* Retrieved from `http://whatis.techtarget.com/definition/PDCA-plan-do-check-act` pages 7

Wise, P. R. S. (2011). *The purpose and value of business impact analysis.* itsmprofessor.net/. pages 3