

 INSTITUCIÓN UNIVERSITARIA DE ENVIGADO	ARTICULO DE TRABAJO DE GRADO	Código: F-PI-028
		Versión: 01
		Página 1 de 8

ITIL Y SU PROCESO GESTION DE CONTINUIDAD DEL SERVICIO

MARTHA ISABEL ESTRADA VÉLEZ

Gobernación de Antioquia

Isaestrada50@hotmail.com

Resumen: Las organizaciones requieren modelos de gestión e implantación de mejores prácticas, metodologías y estándares para que los servicios ofrecidos por estas, logren satisfacer las necesidades para el cual fueron creados; por esta razón las empresas buscan alinear sus servicios con ITIL v3-Biblioteca de Infraestructura de Tecnologías de Información, que dividiéndose en procesos provee un guía de implantación en cada uno de ellos. Dentro de estos procesos, existe la ITSCM –Gestión de Continuidad de los servicios de Tecnología de Información-, ayudando a las entidades en definir estrategias de continuidad a los servicios informáticos para que estos cumplan su objetivo final y es el de dar continuidad en la prestación de estos sin interrupción alguna a los usuarios. Para lograr esta continuidad, la ITSCM ofrece una metodología a utilizar basada en cuatro fases: Iniciación, Requisitos y Estrategias, Implementación y Gestión Operacional.

Palabras claves: *ITIL, Tecnología de Información, plan de continuidad, servicios, Gestión operacional.*

Abstract: The Organizations require models of management and implementation of best practices, methodologies and standards for services offered by them, can satisfy the needs for which they were created, for this reason, the companies seek to align its services with ITIL v3-Information Technology Infrastructure Library, wich divided in processes provides a guide to implementing each of them. One of these processes is the ITSCM- Information Technology Services Continuity Management, helping organizations to define continuity strategies to the technological services facilities that they accomplish their final goal, wich is to provide continuity in the provision of these without any interruption to users. The ITSCM provides a methodology to use based on four phases: Initiation, Requirements and Strategies, Implementation and Operational Management.

Key words: *ITIL - Information Technology, Continuity Plan, Services, Operational Management.*

1. INTRODUCCIÓN

Ante el incremento de la cultura informática derivada del creciente empleo de la Tecnología de la Información, surge la necesidad y responsabilidad de proteger los medios de almacenamiento y su ambiente de operación. La cantidad de datos guardados en los medios y equipos de almacenamiento se acrecienta día tras día, es por ello, que los usuarios o personal directamente relacionado con el uso y operación de bienes informáticos de las entidades deben propiciar la adopción de medidas de seguridad para proteger su información. La integridad, confidencialidad y disponibilidad son principios o criterios de la información que se maneja en las organizaciones, permitiendo asegurar que ésta este protegida ante cualquier situación en la que pueda verse en riesgo de sufrir algún daño.

Por lo anterior, las organizaciones adoptan modelos de gestión e implementación de mejores prácticas que trabajen paralelamente con normas internacionales que permitan que la información requerida por los servicios ofrecidos por las tecnologías, habiliten adecuadamente los procesos de negocio y puedan entregar el valor que la organización espera brindar; por esto, las organizaciones buscan alinear sus servicios y procesos con ITIL - Biblioteca de Infraestructura de Tecnologías de Información (*Information Technology Infrastructure Library*)-, ya que es consistente con la norma ISO /IEC 27001, donde esta especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información, y que conjuntamente pueden facilitar la gestión de los servicios de Tecnologías de la Información de las entidades.

Dentro de los Proceso manejados en ITIL, existe el proceso Gestión de la continuidad de

 INSTITUCIÓN UNIVERSITARIA DE ENVIGADO	ARTICULO DE TRABAJO DE GRADO	Código: F-PI-028
		Versión: 01
		Página 2 de 8

los servicios de Tecnología de Información (*Information Technology Services Continuity Management, ITSCM*) - que basado en un riguroso análisis de impacto sobre el negocio y evaluación de riesgos, permite a las entidades la ejecución de un Plan de continuidad para actuar durante y después de un evento desastre que afecte la operación normal de los servicios.

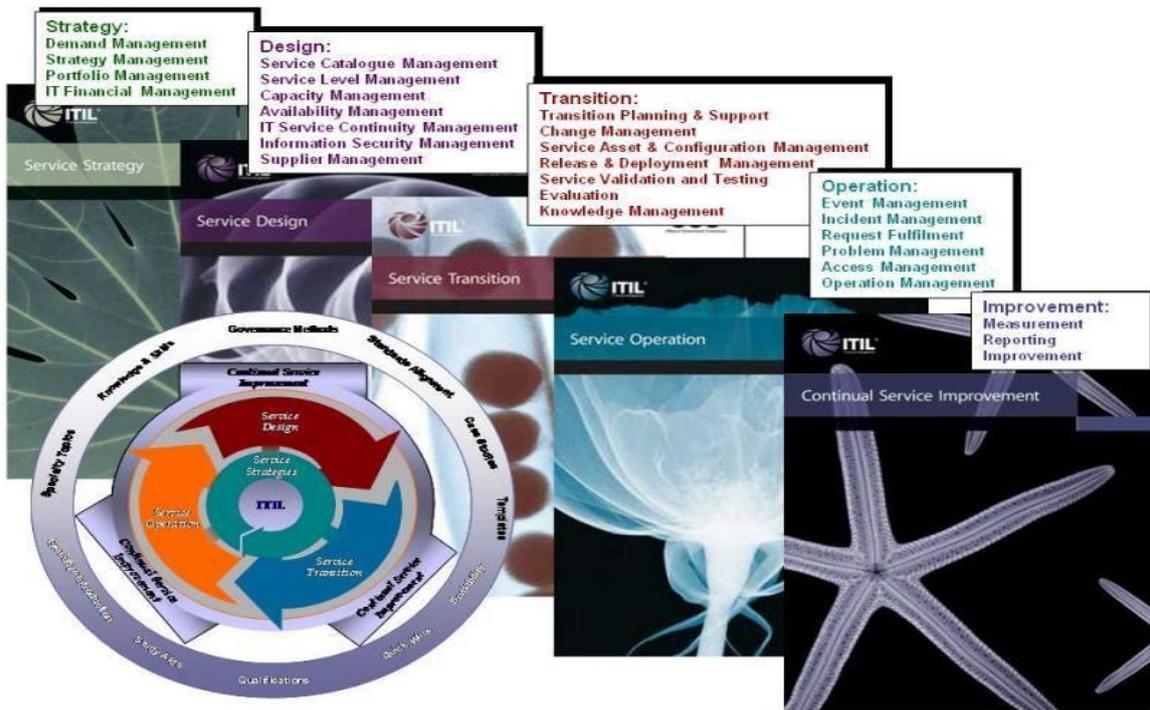
La ejecución de un Plan de Continuidad debe ser preparado teniendo en cuenta las diferentes actividades que comprende el proyecto en las siguientes fases: Iniciación, Requisitos y Estrategias, Implementación y Gestión Operacional, el cual deberá ser actualizado a medida que se presenten cambiantes a nivel de los servicios para así asegurar que dicho plan si este a la altura de estar cumpliendo su objetivo final.

2. BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGIA DE INFORMACIÓN

La Biblioteca de Infraestructura de Tecnología de Información - ITIL – ITIL es el método más ampliamente aceptado para la gestión de servicios. ITIL es un marco de mejores prácticas coherentes, procedentes de los sectores público y privado a nivel internacional.

ITIL actualmente se encuentra en la versión tres, donde maneja cinco publicaciones basándose en el ciclo de vida del servicio como: Estrategia, Diseño, Operación, Transición y Mejora Continua del Servicio, como se muestra en la figura 1.

Figura 1. ITIL v3- Ciclo de vida del servicio



Tomado de (Compuredes ,2009: p: 67)

La Gestión de Servicios TI (*IT Services Management, ITSM*) deriva enormes beneficios de un enfoque de mejores prácticas, donde es impulsada por la tecnología y la amplia gama de entornos organizativos en los que opera, que debe encontrarse en un estado de constante

evolución, para ello, las mejores prácticas¹, se basan en el asesoramiento de expertos y

¹ Office of government commerce ITILv3. (2007). *Best Management Practice*, desde <http://www.best-management-practice.com/Knowledge-Centre/Best-Practice-Guidance/ITIL/>

 INSTITUCIÓN UNIVERSITARIA DE ENVIGADO	ARTICULO DE TRABAJO DE GRADO	Código: F-PI-028
		Versión: 01
		Página 3 de 8

aportaciones de los usuarios de ITIL para así estar actualizado en su contenido ofreciendo guías de implementación para todas aquellas empresas que quieran adoptarla.

3. GESTION DE LA CONTINUIDAD

El propósito de la Gestión de Continuidad - ITSCM es apoyar el proceso global de Continuidad de Negocio de Gestión para garantizar que la Tecnología de la Información requiere instalaciones técnicas y de servicio (incluyendo sistemas informáticos, redes, aplicaciones, repositorios de datos, telecomunicaciones, medio ambiente, apoyo técnico y Mesa de ayuda) se puedan reanudar en tiempos requeridos y en los plazos de negocios establecidos²

Se ocupa de tener la infraestructura y los servicios de TI funcionando dentro de los tiempos límites especificados para que los servicios a nivel de negocio sigan operando en su normalidad.

La Gestión de la Continuidad se ocupa de impedir que una imprevista y grave interrupción de los servicios TI, debido a desastres naturales u otras fuerzas de causa mayor, tenga consecuencias catastróficas para el negocio.

La ITSCM debe combinar equilibradamente estrategias como:

- **Proactivos:** que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio,
- **Reactivos:** cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

3.1 Objetivos de la Gestión de Continuidad:

- Garantizar la pronta recuperación de los servicios (críticos) TI tras un desastre.

- Establecer políticas y procedimientos que eviten, en la medida de lo posible, las perniciosas consecuencias de un desastre o causa de fuerza mayor.

4. METODOLOGIA GESTION DE LA CONTINUIDAD

El proceso de Gestión de la Continuidad de los servicios, define una metodología a utilizar para la implementación de este en una organización esta metodología consta de 4 fases: Iniciación, Requisitos y Estrategias y Gestión operacional³.

A continuación se dará una breve descripción de las fases que componen la Metodología:

4.1 Iniciación:

El primer paso necesario para desarrollar una Gestión de la Continuidad del Servicio coherente es establecer claramente sus objetivos generales, su alcance y el compromiso de la organización TI: su política.

Su dimensión depende de su alcance y sería absurdo y contraproducente instaurar una política demasiado ambiciosa que no dispusiera de los recursos correspondientes.

4.2 Requisitos y Estrategias:

Esta fase se subdivide en dos etapas, la primera es Requisitos y la segunda son las Estrategias.

4.2.1 Requisitos: El propósito de esta primera etapa se centra en el análisis del Impacto del negocio o los servicios (*Business Impact Analysis, BIA*), esto es cuantificar que tanto sería la pérdida por el impacto de un riesgo a los servicios del negocio,

Una correcta Gestión de la Continuidad del Servicio requiere en primer lugar determinar el impacto que una interrupción de los servicios TI pueden tener en el negocio. Cuanto mayor sea el impacto asociado a la interrupción de un determinado servicio mayor habrá de ser el esfuerzo realizado en actividades de prevención.

² Osiatis (2007), *Gestión de Servicios TI*, desde http://itilv3.osiatis.es/disen_servicios_TI/gestion_continuidad_servicios_ti.php

³ Taylor S, Lloyd V & Rudd C. (2007). *ITIL v3 Service Design*. London: TSO, P.216.

 INSTITUCIÓN UNIVERSITARIA DE ENVIGADO	ARTICULO DE TRABAJO DE GRADO	Código: F-PI-028
		Versión: 01
		Página 4 de 8

determinado servicio mayor habrá de ser el esfuerzo realizado en actividades de prevención.

La Gestión de la Continuidad del Servicio debe enumerar y evaluar, dependiendo de su probabilidad e impacto, los diferentes factores de riesgo. Para ello la ITSCM debe:

- Conocer en profundidad la infraestructura TI y cuáles son los elementos de configuración (CIs) involucrados en la prestación de cada servicio, especialmente los servicios TI críticos y estratégicos.
- Analizar las posibles amenazas y estimar su probabilidad.
- Detectar los puntos más vulnerables de la infraestructura TI.

4.2.2 Estrategias: La continuidad de los servicios TI puede conseguirse bien mediante medidas preventivas, que eviten la interrupción de los servicios, o medidas reactivas, que recuperen unos niveles aceptables de servicio en el menor tiempo posible. Es responsabilidad de la Gestión de la Continuidad del Servicio diseñar actividades de prevención y recuperación que ofrezcan las garantías necesarias a unos costes razonables.

4.3 Implementación:

Esta fase se enfoca en el desarrollo del Plan de Continuidad del Negocio basándose en la disponibilidad de los servicios, instalaciones y recursos.

También, en esta fase se lleva a cabo las pruebas (rendimiento, funcionales, operativos y de las pruebas de aceptación) necesarias antes de la entrega del plan, y la validación de la integridad de los datos y la coherencia.

La distribución del plan es importante, ya que debe asegurarse de que las copias están disponibles para el personal clave y previamente autorizado de tenerlo en el momento que se requiera.

4.4 Gestión Operacional:

Formación: Es inútil disponer de unos completos planes de prevención y recuperación si las personas que eventualmente deben llevarlos a cabo no están familiarizadas con los mismos.

Es indispensable que la Gestión de la Continuidad:

- Dé a conocer al conjunto de la organización TI los planes de prevención y recuperación.
- Ofrezca formación específica sobre los diferentes procedimientos de prevención y recuperación.
- Realice periódicamente simulacros para diferentes tipos de desastres con el fin de asegurar la capacitación del personal involucrado.
- Facilite el acceso permanente a toda la información necesaria, por ejemplo, a través de la Intranet o portal B2E de la empresa.

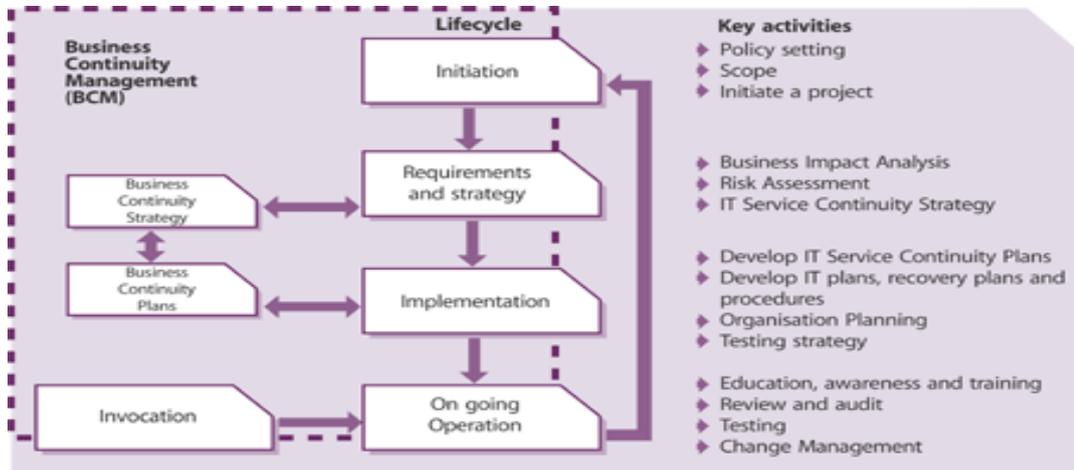
Actualización y Auditoria: Tanto las políticas, estrategias y planes han de ser actualizados periódicamente para asegurar que responden a los requisitos de la organización en su conjunto. Cualquier cambio en la infraestructura TI o en los planes de negocio puede requerir de una profunda revisión de los planes en vigor y una consecuente auditoría que evalúe su adecuación a la nueva situación.

En ocasiones en que el dinamismo del negocio y los servicios TI lo haga recomendable, estos procesos de actualización y auditoría pueden establecerse de forma periódica.

A continuación se muestra en la figura 1, la metodología de la Gestión de Continuidad indicando las principales actividades en cada una de sus fases.

	ARTICULO DE TRABAJO DE GRADO	Código: F-PI-028
		Versión: 01
		Página 5 de 8

Figura 1. Metodología Gestión de la Continuidad



Tomado de (Taylor, 2007, p: 218)

5. PROYECTO PLAN DE CONTINGENCIA INFORMÁTICO PARA EL SERVICIO IMPUESTO DE REGISTRO DE RENTAS DEPARTAMENTALES DE LA GOBERNACION DE ANTIOQUIA.

La Gobernación de Antioquia, en el segundo semestre de 2010 tuvo como prioridad elaborar un proyecto de plan de contingencia informático para uno de sus servicios ofrecidos a la comunidad antioqueña que estuviera alineado al proceso ITSCM de ITIL. El servicio seleccionado fue Impuesto de Registro de Rentas departamentales, éste proyecto fue elaborado por la practicante de Ingeniería de sistemas Martha Isabel estrada Vélez de la Institución Universitaria de Envigado,⁴ Para llevar a cabo la realización de éste, tuvo en cuenta la metodología anteriormente mencionada en la figura 2. A continuación se mostraran detalles de la elaboración del proyecto:

5.1. Objetivos del proyecto:

5.1.1 Objetivo general del proyecto:
Elaborar un plan de contingencia informático como propuesta para la solución y restablecimiento del servicio Impuesto de Registro como procedimiento crítico de la Gobernación de Antioquia mediante el estudio de las buenas prácticas ITIL.

5.1.2 objetivos específicos:

- Identificar los riesgos relacionados con el servicio Impuesto de Registro, determinando la probabilidad y el impacto de una variedad de amenazas que pueden ocasionar interrupciones al servicio.
- Elaborar el procedimiento a seguir para la recuperación del servicio Impuesto de Registro de Rentas Departamentales posterior a un evento de contingencia que interrumpa la continuidad del servicio a nivel de negocio

⁴ Estrada, M. (2011). *Plan de contingencia informático para el servicio Impuesto de registro de rentas Departamentales de la Gobernación de Antioquia*. Informe de Práctica Profesional para optar al título de Ingeniera de Sistemas, Facultad de Ingeniería, Institución Universitaria de Envigado, Envigado, Colombia.

5.2. Desarrollo de los objetivos:

5.2.1 Inicio del proyecto: como primera fase se tuvo el inicio del proyecto, se realizó entrevistas a los funcionarios encargados directamente del servicio Impuesto de Registro, con el fin de tener conocimiento previo sobre este y así poder pasar a la siguiente fase de identificación de riesgos.

5.2.2 Requisitos y Estrategias: como requisitos en este proyecto se realizó la debida identificación y análisis de los riesgos asociados al servicio, para esta actividad, se contó con las

sugerencias del equipo de informática de la Gobernación de Antioquia, donde cada riesgo fue evaluado con su nivel de Probabilidad e Impacto y de acuerdo a esto se realizó la debida calificación del riesgo, es decir, se cuantifico que tan grave podría ser el caso de materializarse determinado riesgo relacionado al servicio.

A continuación se muestra en la tabla 1. Los riesgos que fueron identificados para el servicio Impuesto de Registro de Rentas Departamentales.

Tabla 1. Riesgos identificados al servicio.

RIESGO	PROBABILIDAD		IMPACTO		CALIFICACION DEL RIESGO	
	(P)		(I)		(C)	
	VALOR	NIVEL	VALOR	NIVEL	VALOR	ZONA
falla en el fluido eléctrico	2	Media	20	Catastrófico	40	Importante
acceso no autorizado a la información	1	Bajo	20	Catastrófico	20	Moderado
fallas en hardware y software	3	Alta	10	Moderado	30	Importante
colapso de telecomunicaciones	2	Media	20	Catastrófico	40	Importante
virus informático	2	Media	10	Moderado	20	Moderado
suministro para la normal operación	1	Bajo	10	Moderado	10	Tolerable
ausencia del líder	2	Medio	5	Leve	10	Tolerable
recurso humano no idóneo para llevar a cabo sus funciones	3	Alto	10	Moderado	30	Importante
carga de trabajo al personal	2	Medio	5	Leve	10	Tolerable

La identificación de los riesgos se realizó con la metodología de calificación que provee la guía de Administración del riesgo de la función Pública⁵, ya que con esta la entidad siempre ha utilizado para certificaciones de normas de calidad como NTCGP 1000 Y el modelo de control interno – MECI.

Luego de realizar la identificación de los riesgos se analizaron estrategias que podrían ser convenientes para minimizar el impacto que los

riesgos pudieran ocasionar al momento de materialización de alguno de estos. Algunas de las estrategias son:

- Realizar mantenimiento continuo al cableado de red de los equipos del Centro de Cómputo, de éste modo, se podrá minimizar posibles fallas a estos permitiendo un mejor funcionamiento de los equipos.

⁵ Departamento administrativo de la función pública, (2009). *Guía de Administración del Riesgo*, República de Colombia. P.29

- En la segunda fase- Requisitos y Estrategias de la Metodología utilizada en la elaboración del proyecto Plan de Contingencia, se identificaron nueve riesgos, de los cuales, el que más frecuentemente se materializaba era Falla del Fluído Eléctrico, para esto, se diseñó dos formatos de Contingencia: el primero es para los funcionarios de Rentas Departamentales y el segundo para el cliente-Beneficiario del servicio, quién tendrá en su poder la constancia y la satisfacción de haber sido atendido por la entidad; con ellos se logra minimizar el impacto del riesgo y continuar con la prestación del servicio sin interrupciones.
- De las estrategias proactivas propuestas para los riesgos, se determinó que el mantenimiento continuo al cableado de red de los equipos del Centro de Cómputo es importante realizarlo, de éste modo, se podrá minimizar posibles fallas a estos permitiendo un mejor funcionamiento de los equipos.

REFERENCIAS

Departamento administrativo de la función pública, (2009). *Guía de Administración del Riesgo*, República de Colombia. P.29.

Office of government commerce ITILv3. (2007). *Best Management Practice*, Obtenido el 15 de Septiembre de 2010, desde <http://www.best-management-practice.com/Knowledge-Centre/Best-Practice-Guidance/ITIL/>

Osiatis (2007), *Gestión de Servicios TI*. Obtenido el 12 de Agosto de 2010, desde http://itilv3.osiatis.es/disenos_servicios_TI/gestion_continuidad_servicios_ti.php

Taylor S, Lloyd V & Rudd C. (2007). *ITIL v3 Service Design*. London: TSO, P.216.

Estrada, M. (2011). *Plan de contingencia informático para el servicio Impuesto de registro de rentas Departamentales de la Gobernación de Antioquia*. Informe de Práctica Profesional para optar al título de Ingeniera de Sistemas, Facultad de Ingeniería, Institución Universitaria de Envigado, Envigado, Colombia

C.V.: Martha Isabel Estrada Vélez: Aspirante al título de Ingeniera de Sistemas. Actualmente Coordinadora Proyecto ISA–Renovación Tecnológica en la empresa Interconexión Eléctrica S.A.