Segunda Conferencia de Directores de Tecnología, TICAL 2012
Gestión de las TICs para la Investigación y la Colaboración, Perú 2 y 3 de Julio de 2012

Metodología para la formulación del plan de contingencia de TI para Instituciones de Educación Superior.

Gina Paola Maestre Góngora[a,b] Mariutsi alexandra Osorio Sananbria [a,c], Andrea Trillos[a,d], Edlin Palencia[a,e]

[a] Universidad Cooperativa de Colombia, Sede Bucaramanga
[b] Docente Ingeniería de Sistemas, gina.maestre@campusucc.edu.co,
[c] Docente Ingeniería de Sistemas, mariutsi.osorio@ucc.edu.co,
[d] Estudiante de Ingeniería de Sistmas, andrea.trillos@ campusucc.edu.co
[e] Estudiante de Ingeniería de Sistmas, edlin.palencia@campusucc.edu.co

Resumen.

En la actualidad las Instituciones de Educación Superior (IES) cuentan y soportan sus actividades y procesos con servicios de Tecnologías de las Información (TI) y donde los planes de contingencia se han convertido en parte esencial de la gestión de tecnologías de la información, ya que las amenazas y riesgos pueden aparecer en cualquier momento y con origen en muchas fuentes. Las situaciones de catástrofe para una organización de educación superior, pueden ser de origen natural (sismos, terremotos, tormentas, etc.), origen humano (hurtos, errores, huelgas, etc.) o de origen técnico (daños software y hardware, falla energía eléctrica, etc.) y la materialización de estos eventos no previstos pueden provocar crisis y consecuencias reflejadas en la continuidad de los procesos y actividades que son soportadas en las TI en las IES. Este articulo presenta una propuesta metodológica para formular un plan de contingencias que proporcione una guía en la prevención, atención y recuperación de desastres, para que de esta manera se protejan las tecnologías de la información de las diversas amenazas a las que están expuestas, evitando pérdidas que causen parálisis en el servicio de una IES. Para la metodología propuesta se han consultado diversas fuentes con el fin de proponer la metodología más adecuada y un esquema de procedimientos, acordes con la naturaleza de las IES. Adicionalmente se ha tomado como caso del estudio la Universidad Cooperativa de Colombia sede Bucaramanga con el fin seguir esta metodología y proponer al Departamento de TI de plan de contingencia que satisfaga las necesidades de esta IES en particular. Se espera que esta metodología y el plan formulado puedan ser replicados como un modelo y un apoyo los departamentos de TI de las 18 sedes de UCC o para cualquier institución de educación superior.

Palabras Clave: Plan de Contingencia, Tecnología de la Información, Desastre, Recuperación, Riesgo

1 Introducción

Las TI se han asentado plenamente como parte integral de las IES a lo largo de la última década, apoyando cada una de las actividades académicas, administrativas y de gestión de tal manera que se han convertido junto con la información en un activo de

alto valor para las mismas. Para llegar a la incorporación y uso habitual de las TI en la universidad los departamentos, direcciones de TI y la administración han tomado, a lo largo de los últimos años, decisiones estratégicas que han condicionado y determinado la situación actual[1]

Actualmente las IES se enfrentan al desafío de manejar y soportar sus actividades en TI: gestión académica, administrativa, financiera, de apoyo a la docencia y la comunicación, encontrándonos con sistemas de información e infraestructura tecnológica que dan soporte y atienden las necesidades de las distintas dependencias y departamentos así como de la comunidad universitaria y por lo anterior radica la importancia de cuidar, salvaguardar y asegurar la continuidad del negocio en el momento de que ocurra un evento, ya sea natural, humano o físico; ayudando así a causar el menor impacto en el servicio ya que es indiscutible que son vitales para el mejoramiento de los procesos y eficiencia de la organización.

Al interior de las IES es frecuente encontrar problemas relacionados con la carencia de una estrategia de continuidad del negocio, apoyo de la alta dirección, falta de análisis de riesgos e impacto al negocio, planes de contingencia y recuperación, procedimientos no actualizados, falta de pruebas de continuidad, inexistencia de responsabilidades de continuidad, entre otros. Los desafíos actuales relacionados con la continuidad del negocio envuelven adicionalmente a los desastres naturales, conflictos de tipo ambiental, político y financiero, fallas técnicas, errores humanos, ciber-guerra-crimen-terrorismo, etc. Por tal motivo es fundamental contar con una estrategia que permita a las IES resistir ante este tipo de hechos y mantener la continuidad del negocio, suministrando y recuperando los servicios adecuadamente.

El presente artículo tiene como fin proponer una metodología para la formulación de un plan de contingencia de tecnologías de información, de una manera estructurada y modular (por fases o etapas) para que sirva como herramienta de apoyo a las direcciones o departamentos de las Instituciones de Educación Superior (IES) en la revisión, actualización o formulación del mismo.

2 Plan de Contingencia de TI

Las Tecnologías de la Información constituyen el 70% del capital [2] por lo tanto una organización debe saber cuándo y cómo invertir en TI, así mismo la forma de protegerlas, pues estos aspectos son indiscutiblemente importantes para la prosperidad y eficiencia de una entidad, ya que existen diversos incidentes cuya ocurrencia pueden afectar las tecnologías de la información, incluso paralizando total o parcialmente el normal funcionamiento de las organizaciones y aumentando los niveles de costo.

Las IES están expuestas a variadas amenazas de diferente origen natural, humano y técnico que pueden afectar la continuidad de los procesos soportados por las TI, causando daños en materiales, equipos (hardware) y sistemas de información (software), pérdida de recursos físicos, perjuicios a usuarios y personal de la Universidad. En resumen, para una institución educativa proteger las TI, significa

velar por el normal funcionamiento de los procesos y actividades, para esto existe un elemento clave, es el Plan de Contingencia.

El plan de contingencias de TI, es una herramienta elaborada de forma planificada, que contiene las acciones, decisiones y eventos que ayudará a recuperar, a pesar de la ocurrencia de una falla, aunque sea en parte los procesos críticos de una organización, manteniendo la capacidad funcional del sistema afectado, entendiendo por recuperación, tanto la capacidad de seguir trabajando en un plazo mínimo después de que se presenta un problema, como la posibilidad de volver a la situación inmediatamente anterior al mismo, habiendo remplazo o recuperando el máximo posible de recursos informáticos, permitiendo que la organización continúe operando.

En la literatura podemos encontrar otros conceptos de plan de contingencia como se muestra en la Tabla 1.

Tabla 1. Conceptos Plan de Contingencias

Fuente	Descripción
MARIO G. PIATTINI Auditoria informática un enfoque practico.	El plan de contingencias es una estrategia planificada constituida por: un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por la paralización total o parcial de la capacidad operativa de le empres. Esta estrategia materializa da en un manual, es el resultado de todo un proceso de análisis y definiciones, las cuales dan lugar a las metodología.[6]
IAN. A. GILHOOLEY INFORMATION System Management, Control and Audit	El termino plan de contingencia se usa comúnmente para referir a los planes y procedimientos establecidos en el caso de la ocurrencia de una paralización. Por lo general los problemas en el centro de procesamiento de datos de naturaleza temporal no son cubiertos en el plan de contingencias.[4]
NATIONAL INSTITUTE OF STANDARS AN TECNOLOGY – NIST Contingency planning guide for information technology systems.	El plan de contingencias se refiere a las medidas temporales de recuperación de TI a una emergencia o interrupción de la TI. Las medidas temporales pueden incluir reubicación de los sistemas TI y de las operaciones de una sitio alterno, funcionando con equipo alterno o el funcionamiento de métodos manuales [5].

Fuente: [3]

3 Metodología propuesta para la formulación de un plan de contingencia de TI

A continuación en la Figura 1 se presenta una metodología propuesta para la formulación de planes de contingencia, resultado de la investigación de algunas metodologías ya establecidas como: administración de la continuidad del negocio (BCM), plan de continuidad del negocio (BCP), plan de recuperación de desastres (PRD). [7]

Figura 1. Metodología para la formulación del plan de Contingencia

Tabla 2. Fases y descripción de la Metodología

Fase	Descripción
1.Estudio Preliminar	En esta fase se determinan los actores, funciones de la organización y del departamento de TI y se realiza un inventario de los recursos de TI que soportan las actividades y procesos de la organización.
2. Análisis de impacto	Se hace un análisis de los recursos críticos y prioridades de recuperación de las TI que orientarán la formulación de los diferentes planes.
3. Plan de respaldo	Después de conocer los recursos críticos, se identifican los principales riesgos a mitigar, prioridades y controles de prevención

4. Plan de Emergencias	En esta etapa se coordinan los controles y funciones del plan en caso de eventualidades.
5. Plan de recuperación	Detallar estrategias después de una eventualidad para la pronta de recuperación de servicios de TI.
6. Socialización	Difundir el plan de contingencias por medio de pruebas, capacitación al personal, simulacros, etc.

Para cada una de las fases anteriores se establecieron los siguientes procesos y actividades siguiendo la notación plateada por BPMN (Notación para el Modelado de Procesos de Negocio)), para una mejor comprensión de la metodología:

Figura 2. Metodología Propuesta

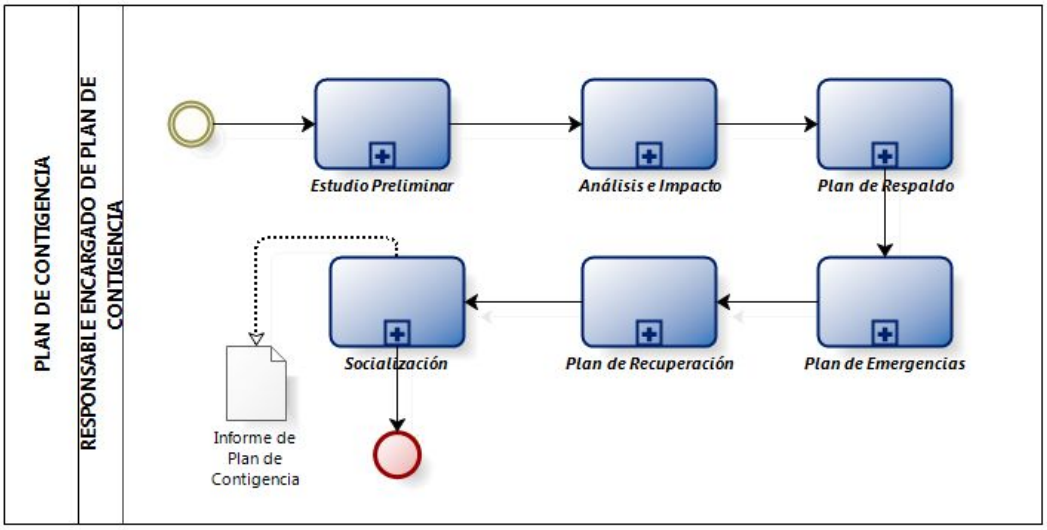


Figura 3. Actividades de la fase Estudio Preliminar

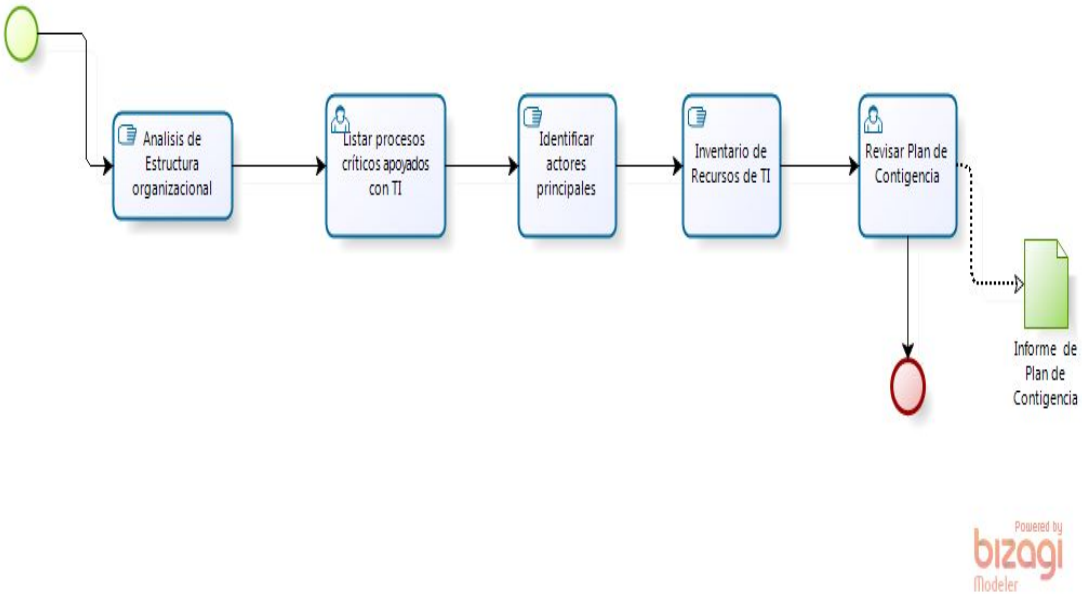


Figura 4.Actividades Fase Análisis de Impacto

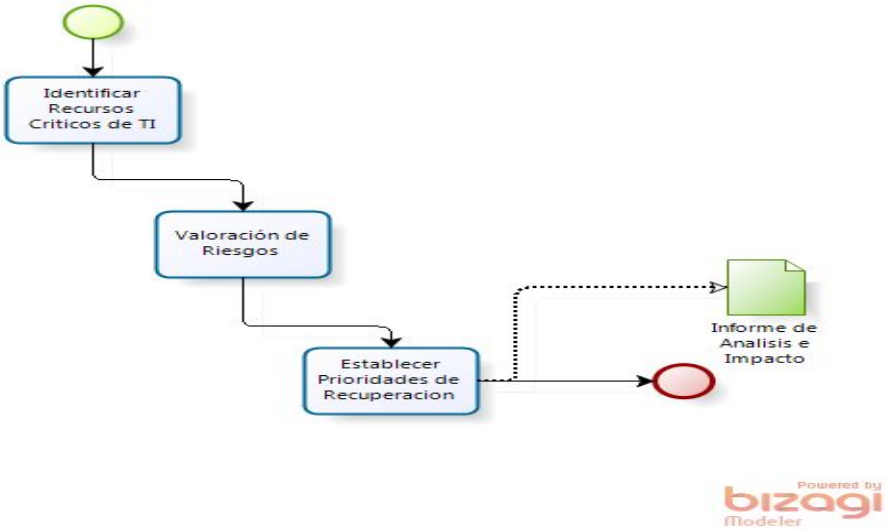


Figura 5. Actividades plan de respaldo

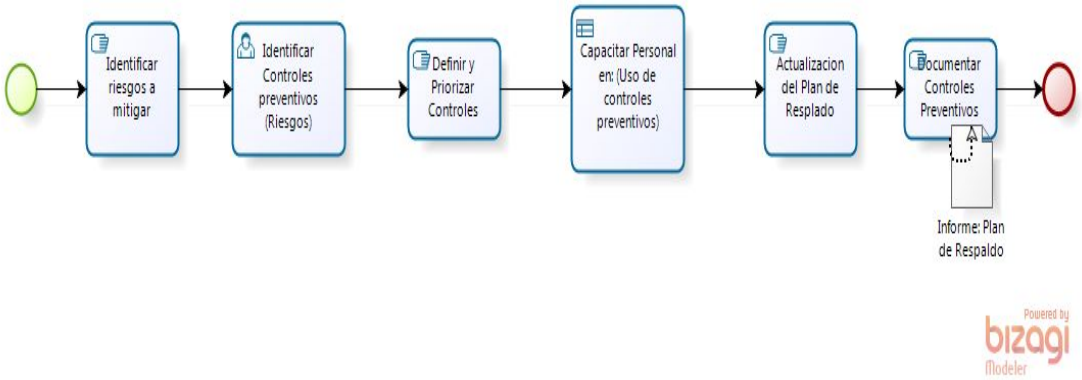


Figura 6. Actividades Plan de Emergencias

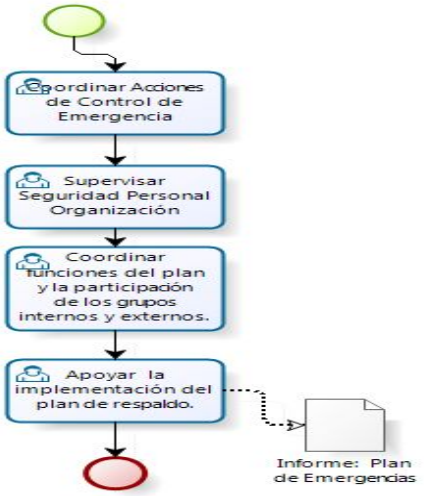


Figura 7. Actividades Plan de Recuperación

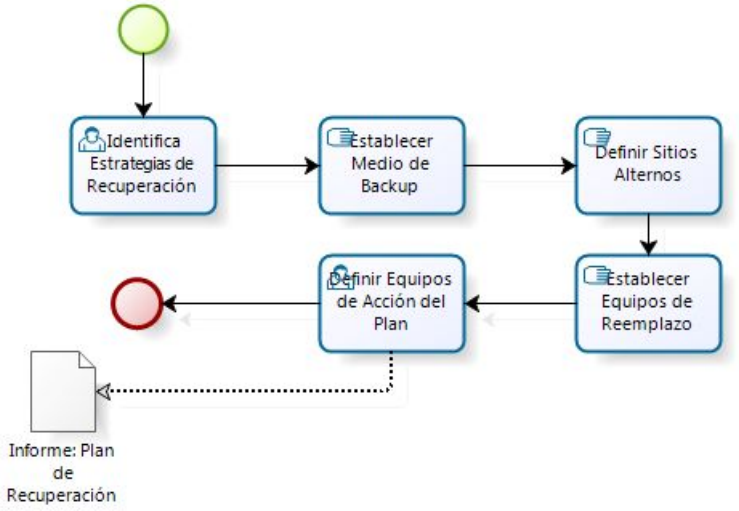
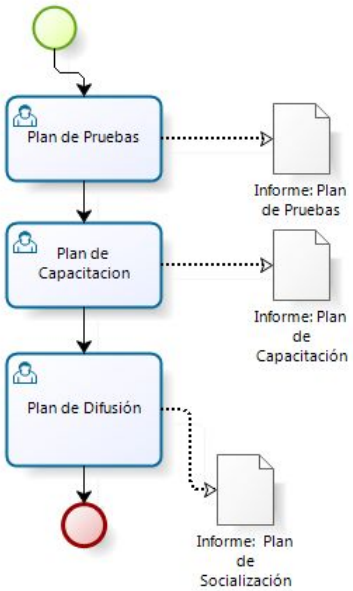


Figura 8. Actividades Socialización



3 Caso de aplicación de la metodología: Universidad Cooperativa de Colombia Sede Bucaramanga. Algunos avances.

La metodología descrita anteriormente para la formulación del plan de contingencia de TI en IES, se ha venido aplicando en la Universidad Cooperativa de Colombia Sede Bucaramanga, donde actualmente se desarrolla como proyecto de grado del programa de ingeniería de sistemas. A continuación se muestran algunos avances y resultados en la aplicación de la metodología particularmente en las fases de estudio preliminar y análisis de riesgos, acordes con la naturaleza de una IES y la particularidad de la UCC sede Bucaramanga.

3.1 Estudio Preliminar

1. **Análisis de estructura organizacional**: En esta actividad se busca obtener la información necesaria de la organización y el sistema de información en explotación para adquirir el suficiente conocimiento y tomar la decisión de la formulación del plan de Contingencia. Se analiza la Misión, Visión, estructura organizacional de la IES (organigrama), la estructura organizacional de la dirección de TI (misión, visión, propósitos, funciones, etc.)

Tabla 3. Estudio preliminar Universidad Cooperativa de Colombia Sede Bucaramanga.

Tabla 3. Estudio preliminar UCC

UNIVERSIDAD COOPERATIVA DE COLOMBIA
MISIÓN: Son sus propósitos fundamentales: LA FORMACIÓN de profesionales con criterios políticos, creativos y solidarios que contribuyan al desarrollo armónico de la sociedad, LA INVESTIGACIÓN, vinculada a la enseñanza y el aprendizaje, como aporte a la solución de problemas científicos y sociales. LA EXTENSIÓN Y PROYECCIÓN SOCIAL orientada al servicio público y al vínculo efectivo con el sector productivo, y LA INTERNACIONALIZACIÓN orientada a la interacción de conocimientos teóricos y prácticos entre las comunidades académicas mundiales, a la movilidad de profesores, investigadores, currículo y estudiantes, y a la cooperación entre las culturas.
ESTRUCTURA ORGANIZACIONAL: La UCC cuenta con 18 sedes a nivel nacional distribuidas en todo el territorio colombiano, donde desde la sede principal se cuenta con las direcciones nacionales de las diversas dependencias que soportan los procesos misionales de la universidad.
DIRECCIÓN NACIONAL DE TI – UCC: La universidad, por producto de la dirección nacional de tecnología de la información, tienen por reto la construcción, operación y desarrollo de un modelo integrado de tecnologías de información y comunicación (TI), para apoyar estratégicamente la gestión académica y administrativa, y soportar el modelo de operación unificado que busca la universidad, con la centralización,

estandarización e integración de los procesos, la tecnología y los datos, tiene tres grandes ramas que conforman su razón de ser: Sistemas de Información institucionales, Software (Académico y de docencia) y administrativo (Financiero y de oficina), Hardware (PCs y Servidores) y sistemas de conectividad.
ESTRUCTURA ORGANIZACIÓNAL Es de resaltar que se cuenta con la dirección nacional de TI (Sede Medellín) quien coordina y lidera a los 18 departamentos de TI que se encuentran en cada una de las sedes.

2. **Identificación de los proceso críticos soportados en TI:** En esta actividad se identifican los procesos de la organización que son fundamentales para el desarrollo de las actividades propias de la IES. De manera general se identifican 3 procesos críticos: Academico, administrativo e Investigación.

Tabla 4.Procesos Críticos soportados en TI en IES, Caso UCC Sede Bucaramanga

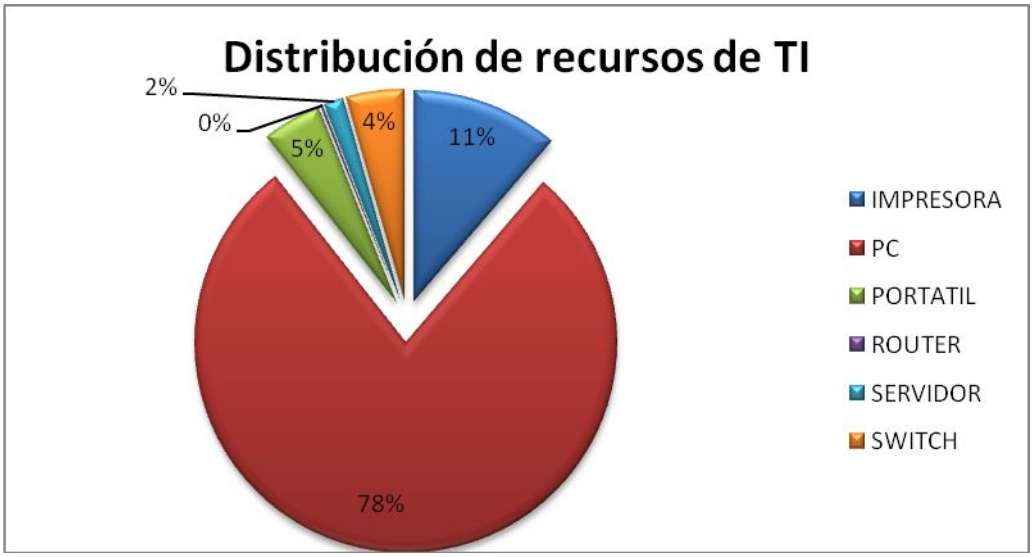
Proceso	Actividades	Recursos de TI
Acádemico	Matricula Acádemica, Gestion de Notas, Gestión de Hoja de vida estudiante y profesor Mensajería Digital, Gestión Academica, Sistemas de gestion de aprendizaje LMS	PCs,Redes,.Sofware Oracle People Soft; Moodle, Blackboard, AVES,Tell me more,laboratorios y salas de informática , mensajería digtal
Administrativo	Gestion Administrativa	PCs,Redes,Software Oracle People Soft;Mensajería digital
Investigación	Gestón de Convocatorias, Proyectos de Investigación, eventos academicos	PCs, Redes,Sofware Ofimática, Sitio Web , Mensajería Digital

3. **Identificación de actores principales:** Los anteriores procesos son desarrollados por actores que deben ser claramente identificados y que pueden intervernir en uno o varios procesos anteriores, en diversos niveles de complejidad. Por ejemplo los estudiantes realizan actividades en los 3 procesos , los profesores son actores clave en los procesos acádemicos y de investigación y los directivos pueden estar relacionados en los 3 procesos críticos.

4. **Inventario de recursos de TI**: Se listan los recursos de TI entendidos estos como hardware, software y telecomunicaciones que soportan los procesos críticos y apoyan las actividades de los actores principales de las IES. Se pueden analizar cual es el porcentaje de recursos hardware, software y

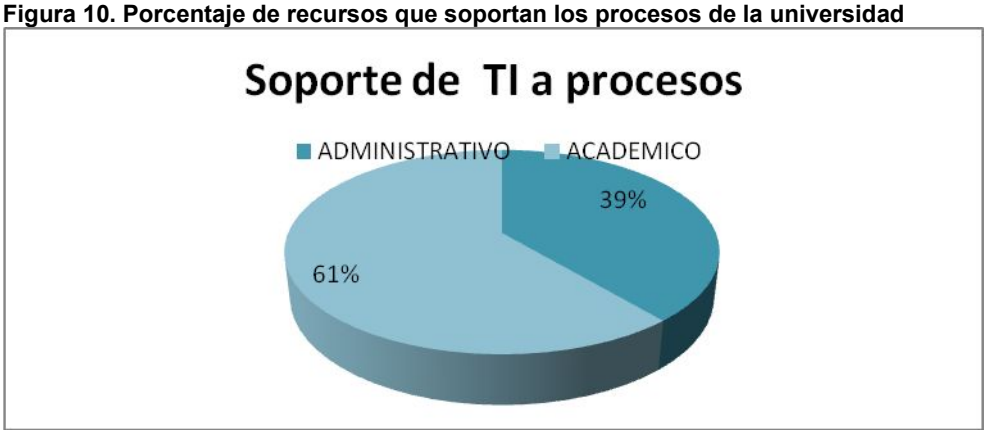
telecomunicaciones, ubicación, responsables, entre otros. A continuación se presentan algunos análisis del inventario de TI.

Figura 9. Tipos de Recursos de TI_ UCC Sede Bucaramanga



Fuente: Departamento de TI- UCC sede Bucaramanga

Figura 10. Porcentaje de recursos que soportan los procesos de la universidad

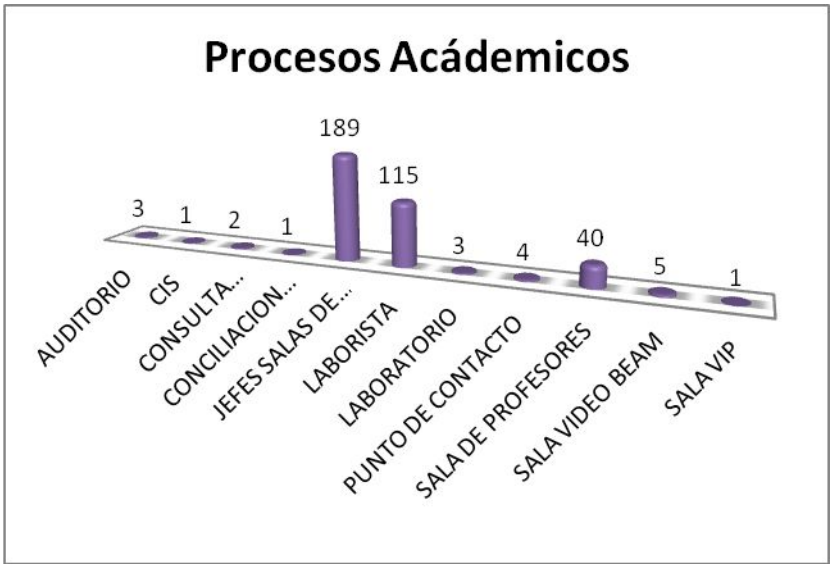


Fuente: Departamento de TI- UCC sede Bucaramanga

Figura 11. Número de recursos de TI que soportan procesos administrativos por dependencias

Fuente: Departamento de TI- UCC sede Bucaramanga

Figura 12. Número de recursos de TI que soportan procesos académicos e investigación por dependencias



Fuente: Departamento de TI- UCC sede Bucaramanga

5. **Revisar plan de contingencia:** se evalúa la existencia del plan de contingencia. De existir se hace un análisis de la pertinencia o no del mismo, si se aprueba de acuerdo a la información recolectada previamente, si se actualiza o si se procede a formular uno nuevo.

En la universidad cooperativa de colombia sede bucaramanga, actualmente no existe un plan de contigencias de TI, por lo que se aprecia la necesidad de la formulación del mismo.

3.2 Análisis de Impacto

1. Identificar los recursos críticos de TI: Una vez se lista el inventario de TI del que dispone la IES, es necesario analizar cuales esos recursos los cuales son indispensables para garantizar el desarrollo de las actividades de la IES. Si bien se han considerado dentro de los recursos de TI el hardware, el software y las telecomunicaciones es de resaltar que para la elaboración del plan de contingencias de la UCC Bucaramanga se consideran recursos críticos particularmente el hardware y algunos elementos de las telecomunicaciones. El software principalmente el que gestiona las actividades académicas y administrativas centrales no depende del departamento de TI de la sede, sino de la dirección nacional de TI, por ello y por no ser de competencia directa del departamento no se ha incluido como un recurso crítico para la sede en particular.

2. Valoración de riesgos: permite conocer los peligros que tiene el Departamento de TI y el tiempo de descenso de funciones de la Institución y operaciones. El análisis de estos riesgos es fundamental en el desarrollo del plan de respaldo y para la pronta recuperación después de alguna eventualidad. Por tal motivo, se debe entender la vulnerabilidad de que ocurra un desastre y establecer medidas preventivas para eliminar o minimizar la ocurrencia del desastre.

En la siguiente tabla se presenta la guía para el análisis de probabilidad y vulnerabilidad con los riesgos detectados para cada caso.

Tabla 5. Matriz para la valoración de riesgos

Impacto	**Riesgo**			
Muy alto	Alto	Muy alto	Muy alto	Muy alto
Alto	Medio	Alto	Muy alto	Muy alto
Medio	Bajo	Medio	Alto	Muy alto
Bajo	Muy bajo	Bajo	Medio	Alto
Muy bajo	Muy bajo	Muy bajo	Bajo	Medio
	Poco frecuente	Normal	Frecuente	Muy frecuente
		Vulnerabilidad		

Fuente: MAGERIT

Tabla 6.Matriz evaluación de riesgo

Posibles Amenazas	Valoración Impacto	Valoración Vulnerabilidad	Valoración del riesgo
NATURALES			
Incendio			
Terremoto			
Rayos			
Inundación			
TECNICAS			
Fallo energía eléctrica			
Fallos aire acondicionado			
Fallos CPU y hardware			
Falla en los enlaces de telecomunicaciones locales.			
Falla del servidor de aplicaciones.			
HUMANAS			
Errores humanos			
Vandalismo			
Robo			

3 Conclusiones

Apoyar al Departamento de TI de las Universidades, brindando un plan de contingencia que proporcione a las tecnologías de información, seguridad y continuidad a los procesos que soportan para dar continuidad al negocio en el momento de presentarse cualquier eventualidad, es un elemento importante dentro de la gestión de TI, impidiendo pérdidas que ocasionen parálisis en el servicio de las Universidades.

La metodología presentada es flexible y se puede contextualizar y aplicar al ámbito organizacional de las IES, en donde los departamentos de TI deben buscar las condiciones tanto para la formulación y la aplicación de planes de contingencia.

Se propone elaborar un software que soporte la formulación, actualización y evaluación del plan de contingencia según la metodología planteada, para que esta sea aplicable de una manera más fácil en otras instituciones de educación superior.

Agradecimientos

Este trabajo ha sido desarrollado en marco del por el Proyecto de Investigación propuesta de modelo de gestión de servicios de ti, basado en ITIL v.3, para instituciones de educación superior colombianas, caso de estudio Universidad Cooperativa de Colombia, sede Bucaramanga y forma parte del trabajo de grado Plan de Contingencias de TI para Instituciones de Educación Superior- UCC Bucaramanga.

Los autores desean expresar su agradecimiento a la Universidad Cooperativa de Colombia.

Referencias

[1] Fernández Martínez, Antonio; Llorens Largo, Faraón. (2009) Gobierno de las TI para universidades Editorial Conferencia de Rectores de las Universidades Españolas (CRUE).

[2] Laudon, Kenneth C., Laudon, Jane P. Sistemas de Información Gerencial. 2002.

[3] Prada O., Lyda Zugelly. Propuesta de un sistema para el desarrollo del plan de contingencias de tecnología de información en las organizaciones. Trabajo de Grado. Universidad Industrial de Santander. 2005.

[4] Ian A. Gilhooley. Information Systems Management – Control and Audit. 1991 Editorial Inst of Internal Auditors.

[5] National Institute of Standars and Technology – NIST. http://www.nist.gov/index.html

[6] Piattini, Mario y Del Peso, Emilio. Auditoría Informática – Un enfoque Práctico. 2001.

[7] Cerezo, Alejandro. Recuperación Y Continuidad Del Negocio. Semana de seguridad Informática UNAM ENEP ARAGON. 2005.