Continuidad de Servicio de TI en el Ministerio de Trabajo y Seguridad Social de Costa Rica.

Juan Carlos Mora Abarca y Jorge Isaac Vargas Télles

Escuela de Ingeniería,
Universidad Latinoamericana de Ciencia y Tecnología,
ULACIT, Urbanización Tournón, 10235-1000
San José, Costa Rica
[jmoraa831,jvargast932]@ulacit.ac.cr
http://www.ulacit.ac.cr

Resumen En la actualidad las instituciones del gobierno deben administrar gran cantidad de información para brindar una variedad de servicios a los ciudadanos, los cuales requieren el uso de tecnologías de información para gestionar y procesar un alto volumen datos. Para una adecuada gestión de los recursos tecnológicos existen marcos de trabajo y estándares que describen recomendaciones y lineamientos a seguir, así muchas organizaciones se implementan en sus departamentos de tecnología. El Ministerio de Trabajo costarricense debe seguir un marco de trabajo establecido por la Contraloría General de la República, el cual tiene en sus bases, el marco de referencia COBIT4.1. El MTSS presenta problemas con la gestión de los recursos de TI, por lo que se han encontrado oportunidades de mejora a los procesos del DS4 relacionados a la continuidad del negocio y TI, por lo que se realizó un análisis de brechas y un listado de recomendaciones para mejorar los servicios y procesos de TI que brinda la institución.

Keywords: Continuidad de TI, COBIT, Instituciones Publicas, Análisis de Brechas

1. Introducción

El Ministerio de Trabajo y Seguridad Social de Costa Rica (MTSS) es la institución pública responsable de realizar el seguimiento y la aplicación de las leyes, decretos y acuerdos laborales, así como de los temas relacionados con la seguridad social (Ministerio de Trabajo y Seguridad Social, 2010).

Para cumplir con las obligaciones que las leyes prescriben, es importante que cada departamento cumpla con sus objetivos específicos para contribuir con el desempeño general del MTSS. Sin embargo, el ministerio sufre de limitaciones presupuestarias, falta de personal, insuficiencia de equipos informáticos y problemas de obsolencia con muchos de sus equipos y software. Lo anterior es extensivo al Departamento de Tecnologías de Información y Comunicación del Ministerio de Trabajo (DTIC), el cual enfrenta problemas de infraestructura, seguridad y la

ausencia o inadecuada definición de los procesos relacionados con las tecnologías de la información.

Es importante tener en cuenta que el DTIC gestiona y brinda mantenimiento a los equipos y sistemas que se encargar de administrar y almacenar la información de la mayoría de los trabajadores costarricenses. Por lo que es necesario llevar a cabo la implementación de mejoras y controles adecuados para que pueda ofrecer servicios adecuados para procesar y proteger dicha información (Ministerio de Trabajo y Seguridad Social, s.f.).

De acuerdo con lo anterior, este proyecto tiene por objetivo llevar a cabo el análisis de las brechas que existen entre el estado deseado de la continuidad de los servicios de TI de acuerdo con Cobit 4.1, y el estado actual. El fin de dicho análisis es apoyar el mejoramiento de la continuidad de los servicios de TI el DTIC brinda al MTSS. En consecuencia con este dato,se establece los siguiente objetivos específicos:

1. Realizar un estudio sobre el conocimiento e implementación de continuidad de TI dentro del DTIC.
2. Elaborar un listado de recomendaciones y posibles mejoras de continuidad de TI para el DTIC con el análisis de la información brindada por la institución.
3. Visualizar el nivel actual de madurez en la institución, a partir del DS4 de COBIT 4.1.

Hace varios años el DTIC elaboró un documento para llevar a cabo el mantenimiento de los recursos y servicios de TI de la institución, pero fue descartado con el tiempo. con base en lo anterior,se genera el siguiente cuestionamiento para investigar:

¿Cómo contribuir con el mejoramiento del proceso de continuidad de los servicios de TI del MTSS mediante el análisis de brechas entre la situación actual y la situación deseada?

Este trabajo lleva a cabo la revisión de una serie de documentos que fueron facilitados por el MTSS, así como una encuesta entre el personal del DTIC, el cual determina el estado actual de la situación con respecto a la continuidad de los servicios de TI.

2. Marco Teórico

La continuidad del negocio es un concepto que parte de los procesos, servicios o actividades necesarios, y tiene una organización que debe mantenerse funcional, a pesar del fallo u interrupción que se presente. Además, es importante destacar que el objetivo principal de la continuidad es prevenir un desastre o que este impacte de alguna manera. (S. Institute, 2002).

Para mantener la continuidad del negocio, es necesario tener un listado de procesos y normas bien definidas, el cual se conoce como un plan de continuidad. Los planes de continuidad son elaborados por un experto o un equipo de expertos que conocen muy bien los procesos del negocio, los riesgos y desastres que pueden materializarse y la forma de resolverlo (Government of Canada, 2014).

Hoy los servicios de los negocios operan por medio de TI, ya sea con datos, aplicaciones, bases de datos, entre otros, por lo que tener una infraestructura que soporte estas necesidades, es una de las prioridades de las empresas en el mercado actual. Pero aún con todo lo anterior, no es suficiente, si existe la posibilidad de fallos,y no se tiene algún plan de contingencia o recuperación de desastres, el cual los respalde. Muchos proveedores de infraestructura de TI, a través de la nube, ofrecen este tipo de planes en caso de que el servicio llegase a fallar; sin embargo, esto no es suficiente, ya que un proceso u servicio que se interrumpa, sin importar por cuánto tiempo, puede significar una gran pérdida de dinero, clientes, datos, entre otros; lo cual es vital para cualquier empresa. Por ello, un plan de continuidad se considera de alta prioridad, ya que va enfocado a la prevención de accidentes y brinda un servicio sin ningún contratiempo. (I. Institute, 2012).

Existen estándares y marcos de referencia para la implementación y mantenimiento de infraestructuras de TI, que incluyen planes de continuidad. En Costa Rica,por ejemplo se exige el cumplimiento de las normas técnicas para la gestión y el control de las tecnologías de información de la Contraloría General de la República(Contraloria General de la Republica, 2007). Ésta es basada en los marcos de referencia como PMBOK, ITIL y Cobit,los cuales son estándares como ISO 27001, ValIT, ISO 9001, ISO 30000, entre otros. Con base en esta información se obtiene el análisis de los datos Cobit 4.1 . A partir de estos resultados y las recomendaciones, los cuales podrán ser utilizados en la norma de la Contraloría General de la Republica. (IT Governance Institute, 2007b).

Cobit es un marco de referencia que es utilizado en muchas áreas de tecnologías de información y se enfoca en la evaluación de los niveles de madurez de las organizaciones, de acuerdo al grado de cumplimiento de las políticas. Mientras que los objetivos de ITIL están orientados a la ejecución y el cumplimiento de los aspectos relacionados con la continuidad (IT Governance Institute, 2007a).

ITIL tiene un componente específico para la continuidad denominado como Administración de la Continuidad de los Servicios de TI[1] el cual define el proceso de gestión de continuidad del negocio y el aseguramiento de los servicios. Es importante destacar que el objetivo principal de ITIL es apoyar la gestión de la continuidad y asegurar la recuperación de los servicios ante una interrupción . (CNTEC, 2011).

En la Tabla A se comparan los objetivos de control de Cobit4 e ITIL3, así como los componentes incluidos en un plan de continuidad. (TechTarget, 2009).

En resumen ambos marcos de referencia se enfocan en ayudar al negocio a entender la importancia y necesidad de un plan de continuidad en sus procesos, existen similitudes entre ambas y en muchas organizaciones se implementan ambos marcos, complementándose uno al otro como en el caso de la norma de

[1] conocido como IT Service Continuity Management (ITSCM) por su acepción en inglés

Tabla A – Comparativa de actividades de ITIL V3 y Cobit 4.1				
Actividades	COBIT		ITIL	
	Objetivo	Denominación	Objetivo	Denominación
· Enfoque consistente y global de la administración de la continuidad de TI	DS4.1	Marco de trabajo de continuidad de TI	SD 4.5	· Administración de la continuidad del servicio TI
				· Etapa 1: Inicio
			SD 4.5.5.1	· Administración de la continuidad del servicio TI
			CSI 5.6.3	
· Planes individuales de continuidad basados en el marco de trabajo	DS4.2	Planes de continuidad de TI	SD 4.5.5.2	· Etapa 2: Requerimientos y estrategia
· Análisis de la incidencia en el negocio				· Etapa 3: Implementación
· Resistencia, procesamiento alternativo y recuperación			SD 4.5.5.3	
· Enfoque sobre la infraestructura crítica, resistencia y priorización	DS4.3	Recursos críticos de TI	SD 4.4.5.2	· Actividades de administración de la disponibilidad
· Respuesta para diferentes periodos de tiempo				· Etapa 4: Operación en curso
			SD 4.5.5.4	
· Control de cambios que refleje los requerimientos actuales del negocio	DS4.4	Mantenimiento del plan de continuidad de TI	SD 4.5.5.4	· Etapa 4: Operación en curso
· Realización de pruebas con regularidad	DS4.5	Pruebas del Plan de continuidad de TI	SD 4.5.5.3	· Etapa 3: Implementación
· Implementación de un plan de acción			SD 4.5.5.4	· Etapa 4: Operación en curso
· Capacitación regular de todas las partes interesadas	DS4.6	Ensayo del plan de continuidad de TI	SD 4.5.5.3	· Etapa 3: Implementación
			SD 4.5.5.4	· Etapa 4: Operación en curso
· Distribución adecuada y segura del plan a todas las partes autorizadas	DS4.7	Distribución del plan de continuidad de TI	SD 4.5.5.3	· Etapa 3: Implementación
			SD 4.5.5.4	· Etapa 4: Operación en curso
· Plan de acción en períodos de recuperación y reanudación de los servicios TI	DS4.8	Recuperación y reanudación de los servicios TI	SD 4.4.5.2	· Actividades de administración de la disponibilidad
· Comprender el negocio y apoyar las inversiones				· Etapa 4: Operación en curso
			SD 4.5.5.4	
· Almacenamiento fuera de las instalaciones de todos los recursos críticos	DS4.9	Copias de seguridad fuera de las instalaciones	SD 4.5.5.2	· Etapa 2: Requerimientos y estrategia
			SO 5.2.3	· Copia de seguridad y restauración
· Evaluación regular de los planes	DS4.10	Revisión Post-reanudación	SD 4.5.5.3	· Etapa 3: Implementación
			SD 4.5.5.4	Etapa 4: Operación en curso

la Contraloría General de la Republica. (Contraloria General de la Republica, 2007).

3. Metodología

Es el método a utilizar para realizar la investigación sobre el Plan de Continuidad de TI del departamento de TI del Ministerio de Trabajo y Seguridad Social, para determinar un problema, objetivo o proyecto necesario, para que cumplan con sus requerimientos y metas del departamento por medio de su Plan de continuidad; se utilizará la investigación con aptitudes de conocedor, seguro, analítico y comunicativo; actitudes de respetuoso, trato ameno, oyente, observador y discreto. El instrumento a utilizar para obtener la información es la encuesta con preguntas puntuales sobre el plan de continuidad de TI, el cual está formado por 22 ítem y cada uno hace referencia a los objetivos de control del proceso del DS4 del COBIT, luego es analizado para obtener los resultados de lo que se está realizando; luego un capítulo donde se realiza un análisis por apartado del DS4 con el resultado de las preguntas del cuestionario que lo relacionan, con su análisis de brechas y recomendación, por último se realiza una propuesta para el mejoramiento del proceso del Plan de Continuidad de TI del Ministerio de Trabajo y Seguridad Social.

La encuesta fue preparada haciendo uso de Google Forms y distribuida por correo electrónico. Dicha encuesta estaba dirigida al personal del DTIC y se dividió en 10 grupos, que se corresponden con los objetivos de CobiT 4.1 (DS4.1, DS4.2, DS4.3, DS4.4, DS4.5, DS4.6, DS4.7, DS4.8, DS4.9, DS4.10). Los objetivos de las preguntas de acuerdo con cada uno de los objetivos de Cobit 4.1 se muestran en la tabla B.

Se consultó al personal de TI del Ministerio de Trabajo y Seguridad Social, sobre el plan de continuidad de TI, donde participaron sus 13 integrantes, de los cuales 5 ocupan el cargo de coordinador o Jefe y 8 de profesionales o técnicos, todos de la rama de ciencias informáticas; con el fin de determinar si se alinean al DS4 Cobit.

Para el análisis que se va a presentar en el proyecto se pretende hacer un estudio de madurez que utiza como base los estándares y métricas presentadas por

Tabla B – Asociación y descripción de los objetivos de control con las preguntas		
Objetivo de control	Preguntas asociadas	¿Qué buscan evaluar las preguntas?
DS4.1 Marco de Trabajo de Continuidad de TI	Q7, Q16	Corroborar la existencia de un marco de gestión de continuidad.
		Identificar los recursos utilizados en la continuidad de TI.
		Identificar todos los elementos requeridos por
DS4.2 Planes de Continuidad de TI	Q1, Q20, Q21	Estudiar la existencia de un servicio continuo en la estructura de TI, como los requisitos para recursos críticos de TI.
		Corroborar que existan guías definidas y documentadas con los roles de los involucrados en la continuidad de TI.
DS4.3 Recursos Críticos de TI	Q3, Q5, Q17	Corroborar que existe una efectiva gestión de los recursos críticos de TI.
		Verificar la existencia de una gestión de recuperación con prioridades claramente definidas.
DS4.4 Mantenimiento del Plan de Continuidad de TI	Q2, Q14	Definir si los planes de continuidad de TI se basan en los objetivos de la organización.
		Analizar si existe familiaridad con los planes de continuidad de TI para los individuos involucrados.
DS4.5 Pruebas del Plan de Continuidad de TI	Q4, Q15, Q18, Q19	Corroborar la experiencia de los integrantes del DTIC en la recuperación de procesos de sistemas de TI.
		Definir la capacidad de una recuperación efectiva de los sistemas de TI.
DS4.6 Entrenamiento del Plan de Continuidad de TI	Q6, Q20	Corroborar que el DTIC cuenta con el personal con experiencia para la recuperación de desastres de sistemas de TI.
		Definir si existe un programa de capacitaciones para el personal responsable.
DS4.7 Distribución del Plan de Continuidad de TI	Q8	Corroborar que el personal está capacitado para los procesos de recuperación.
		Verificar que los planes son disponibles y accesibles para todas las partes involucradas.
DS4.8 Recuperación y Reanudación de los Servicios de TI	Q9, Q11, Q21	Definir la capacidad de minimizar el tiempo de recuperación.
		Definir la capacidad de Minimizar el costo de recuperación.
		Corroborar la priorización de la recuperación de tareas críticas del negocio.
DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones	Q10, Q12	Verificar la capacidad de respaldar datos en caso de daño físico al hardware
		Asegurar que los datos externos son constantemente gestionados por el DTIC.
DS4.10 Revisión Post Reanudación	Q13	Corroborar que se actualiza los planes de recuperación.
		Comprobar que los planes de reanudación están de acuerdo con las necesidades del negocio.

Cobit 4.1; específicamente en su apartado DS4, llamado 'Garantizar la Continuidad del Servicio'. El cual se va a enfocar únicamente en el área de Tecnologías de Información, para presentar un plan de continuidad que promueva la continuidad de los servicios de TI que actualmente brinda el Ministerio de Trabajo y Seguridad Social.

Entre los procesos que se recomiendan en el DS4 se puede destacar la utilización de respaldos que almacenan la información, en un lugar fuera de donde los equipos actuales de TI se encuentran, además revisar de manera continua que los planes de continuidad sean ejecutados apropiadamente y asegurarse que el personal esté capacitado para tal tarea; todo esto asegura que los servicios y procesos clave que brinda la institución tengan la mayor disponibilidad y continuidad posible,y disminuya la posibilidad de interrupciones o posibles fallos que se puedan presentar. El proceso DS4 cuenta con diez objetivos de control orientados a asegurar la continuidad y el mínimo impacto al negocio en caso de una interrupción de servicios de TI.(IT Governance Institute, 2007a).

4. Discusión

Las discusiones de la información obtenida a partir de la cada una de las preguntas incluidas en el instrumento se encuentran en los Anexos del documento actual.

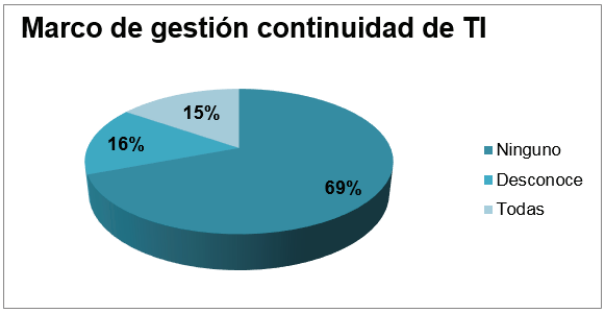
5. Resultados

Se realizó una encuesta para conocer sobre el plan de continuidad del departamento de TI en el MTSS, con el fin de conocer las políticas y procedimientos para soportar la continuidad de TI en sus servicios brindados a la institución y si utilizan el COBIT como requisito que tiene por parte del gobierno el MTSS; el estudio en el departamento de TI del MTSS, donde su mayoría es integrada por personal con un grado profesional técnico.

5.1. DS4.1 Marco de Trabajo de continuidad de TI

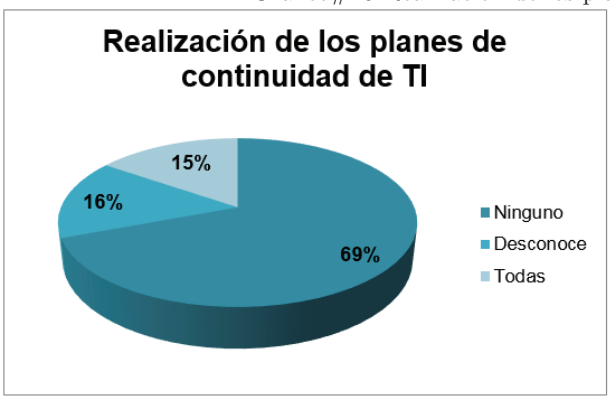
Ver Gráfico#7 y Gráfico#16 a continuación.

Gráfico#7 Marco de gestión continuidad de TI.



N	Válido	13
	Perdidos	0
Media		1.28
DE		0.45
Mínimo		1
Máximo		4

Gráfico#16 Realización de los planes de continuidad de TI.



N	Válido	13
	Perdidos	0
Media		1.62
DE		1.08
Mínimo		1
Máximo		4

Discusión y Resultados La mayoría de los colaboradores encuestados indica que no existen pruebas para el plan de continuidad de TI, ni se está realizando

el plan establecido, por esta razón no se cumple con lo requerido en un marco de trabajo de continuidad de TI.

Análisis de Brechas De acuerdo con los resultados obtenidos la mayoría de los colaboradores no reconoce la existencia de un marco de gestión de continuidad de TI, comparado con lo estipulado por los objetivos de control de COBIT tendríamos inconsistencias por la falta de elementos que sustente la continuidad de los servicios de TI, esto incrementa las vulnerabilidades ante una falla en los recursos críticos que soportan las operaciones de la institución.

Existen una carencia importante en la administración de los servicios de TI, debido al desconocimiento reflejado actualmente por el personal sobre la utilización de mecanismos que aumenten el nivel de tolerancia ante un evento critico que pueda comprometer la plataforma tecnológica de la institución, según COBIT es requerido un proceso de comunicación fluido entre todos los colaboradores del área de TI y del negocio, para reconocer las necesidades de continuidad de sus servicios y generar planes contingentes y de recuperación de desastres.

La gobernabilidad de TI tiene que garantizar una adecuada gestión de su arquitectura de TI, para facilitar el alineamiento de los servicios ofrecidos con los objetivos de la organización, esto porque dentro de la visión está contemplado ofrecer servicios tecnológicos de avanzada y con cobertura nacional y lo cual no es posible sin tener bien definidos los planes de los servicios de TI.

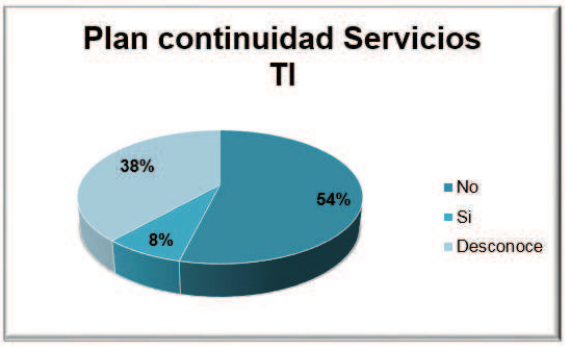
Recomendaciones Se recomienda la propuesta de elaborar un marco de gestión de continuidad de los servicios críticos de TI, el mismo debe contener los elementos básicos que establece el control de COBIT, en el apartado DS4.1 Marco de Trabajo de Continuidad de TI,lo cual proporciona a la institución los mecanismos para documentar planes de continuidad, contigencia y recuperación,que minimiza el impacto ante un desastre,y disminuye la dependencia del personal, que fomenta las practicas de administracion de la continuidad de estas operaciones.

Se debe gestionar la creación de un comité de continuidad integrado por miembros de la área de TI, directores de área, junta directiva y altos mandos políticos; esto porque la administración de un marco de gestión de continuidad requiere involucrar a toda la institución y asi, garantizar los recursos necesarios para su operación.

5.2. DS4.2 Planes de continuidad de TI

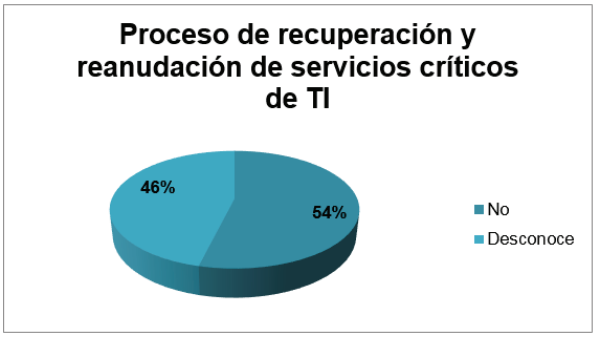
Ver Gráfico#1, Gráfico #9, Gráfico#20 y Gráfico#21 a continuación.

Gráfico# 1 Plan continuidad Servicios TI.



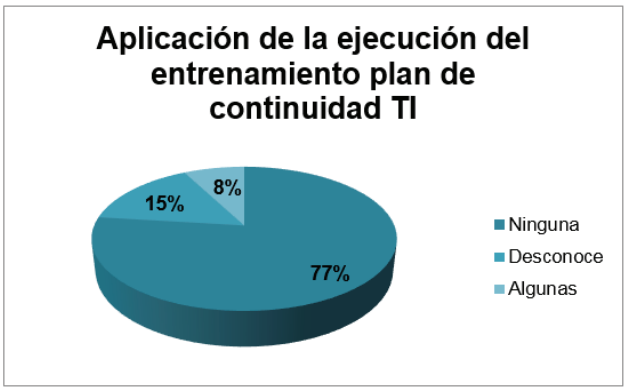
N	Válido	13
	Perdidos	0
Media		1.62
DE		0.84
Mínimo		1.00
Máximo		4.00

Gráfico #9 Proceso de recuperación y reanudación de servicios críticos de TI.



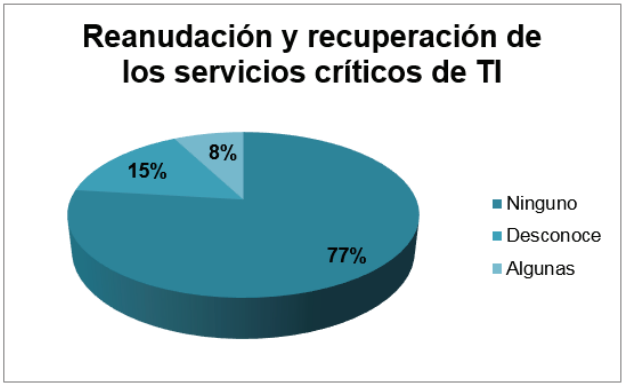
N	Válido	13
	Perdidos	0
Media		1.46
DE		0.5
Mínimo		1
Máximo		4

Gráfico# 20 Aplicación de la ejecución del entrenamiento plan de continuidad TI.



N	Válido	13
	Perdidos	0
Media		1.31
DE		0.61
Mínimo		1
Máximo		4

Gráfico #21 Reanudación y recuperacion de los servicios críticos de TI



N	Válido	13
	Perdidos	0
Media		1.31
DE		0.61
Mínimo		1
Máximo		4

Discusión y Resultados Como se puede observar en el resultado de los gráficos anteriores; tres cuartas partes del departamento, afirman carecer de un plan de continuidad bien definido, por procesos de aplicación, recuperación y reanudación en el departamento de TI.

Análisis de Brechas Según los requerimientos estipulados por COBIT para implementar un plan de continuidad se debe abarcar toda el área de TI, se puede afirmar que la institución carece de un plan de continuidad de los servicios críticos de TI; por esta razón, está vulnerable a riesgos como la imposibilidad de responder a una falla de equipos de almacenamiento y de mitigar un impacto, en el momento de la ejecucion de los procesos.

La separación entre las necesidades del negocio y la gestión de servicios de TI es inviable, según los generadores de valor dicha ruptura interpone un aspecto negativo para enumerar los servicios críticos,y así, cumplir con los objetivos de

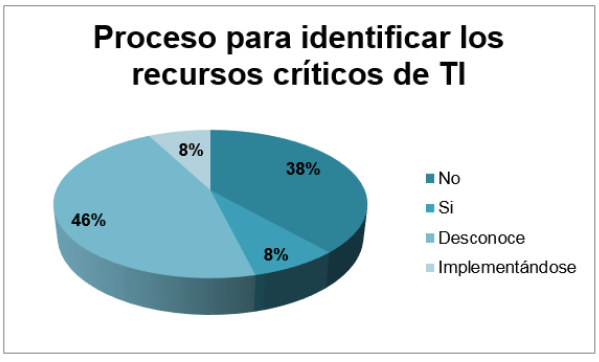
la institución y proponer la mejora continua de los servicios ofrecidos a fuerza laboral del país.

Recomendaciones El departamento de TI debe desarrollar un plan de continuidad que pueda reducir el impacto de la pérdida de servicios críticos ofrecidos por la institución; dicho programa debe centrarse en aquellos procesos que por su complejidad representan un mayor el riesgo, por lo tanto, tiene que operar en soluciones basadas en redundancia en sitio e inclusive utilizar mecanismos de replicación, en tiempo real y alta disponibilidad en sitio alterno. Dentro del plan de continuidad se debe establecer como mínimo los siguientes elementos: los objetivos, alcance, contexto de la arquitectura critica de los servicios de TI,roles y responsables de ejecución del plan tanto internos como externos. En este matco de procesamiento alterno;y con estos insumos, se puede establecer los pasos iniciales para mitigar los efectos de un evento crítico.

5.3. DS4.3 Recursos críticos de TI

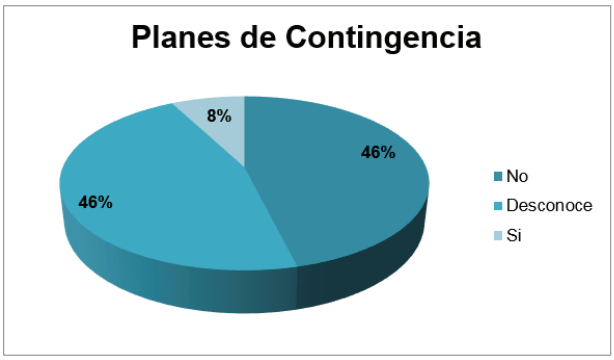
Ver Gráfico#3, Gráfico #5, Gráfico#17 a continuación.

Gráfico# 3 Proceso para identificar los recursos críticos de TI.



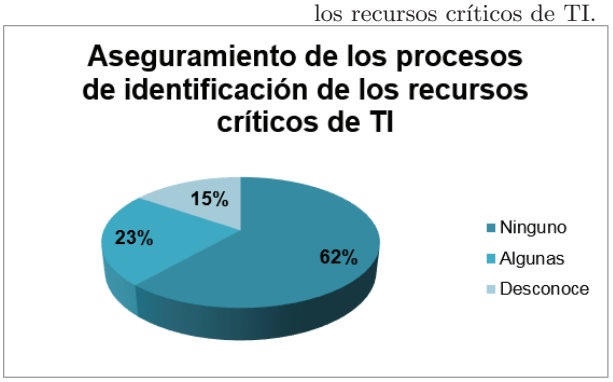
N	Válido	70
	Perdidos	0
Media		1.85
DE		0.86
Mínimo		1
Máximo		4

Gráfico #5 Planes de Contingencia.



N	Válido	13
	Perdidos	0
Media		1.69
DE		0.82
Mínimo		1
Máximo		4

Gráfico# 17 Aseguramiento de los procesos de identificación de los recursos críticos de TI.



N	Válido	13
	Perdidos	0
Media		1.62
DE		0.84
Mínimo		1
Máximo		4

Discusión y Resultados La mayoría indica desconocerla existencia de procesos o planes de contingencia para el aseguramiento de recursos críticos de TI; por consiguiente, que no se cumple con la norma de Recursos críticos de TI.

Análisis de Brechas Dentro de los elementos primordiales para establecer un marco de gestión de continuidad está la identificación de los recursos críticos que forman parte de los servicios prioritarios del negocio; no obstante. los resultados nos indican un inadecuado control por des- conocimiento de esta actividad fundamental. Según los documentos entregados se está elaborando un inventario de los equipos que utiliza la institución; aunque este paso es importante, marca solo el inicio del proceso de análisis de recursos críticos.

Según COBIT la identificación de recursos críticos es parcial, si no está alineado a los servicios ofrecidos por TI, los cuales son funciones primordiales de la organización; por esta razón aunque esté en proceso el mapeo de los recursos críticos aún es insuficiente,ya que no cuenta con un plan de contingencia que estipule cuál es la prioridad de las funciones requeridas, según la necesidad del negocio.

La división entre las necesidades del negocio y la gestión de servicios de TI es inviable, según los generadores de valor esta bifurcación interpone un aspecto negativo para enumerar los sectores críticos, cumplir con los objetivos de la institución y proponer la mejora continua de los servicios ofrecidos a la fuerza laboral del país.

Recomendaciones Se sugiere realizar reuniones de entendimiento con las áreas operativas de la institución, para identificar y documentar los procesos críticos del negocio, y establece la prioridad del levantado de los servicios en caso de un evento contingente.

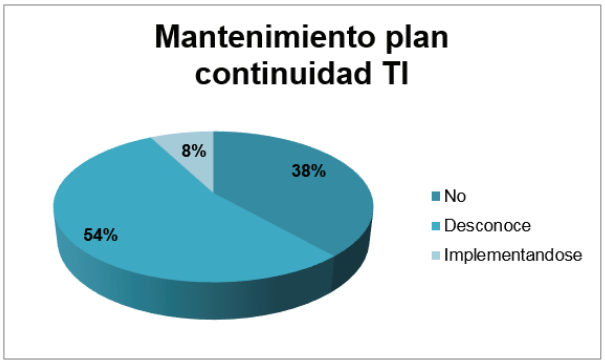
El departamento de TI debe de realizar un plan contingente donde se especifiqué los servicios utilizados en las operaciones del negocio,y así estructurar un apartado que haga referencia a los protocolos necesarios para restablecer los servicios de TI. Dicho plan debe de garantizar los objetivos legales y requerimientos regulatorios.

Realizar un mapeo o inventario de los recursos de TI (servidores, dispositivos de almacenamiento o gestores, equipos de comunicación, cableado estructurado y configuraciones) y determinar cuáles son utilizados por los servicios críticos de la institución; además definirles un protocolo de restauración para cada uno de ellos. Esto colabora a disminuir los costos para la continuidad del negocio y permite enfocarse en la recuperación de los servicios críticos, según las necesidades plasmadas por la institución.

5.4. DS4.4 Mantenimiento del plan de continuidad de TI

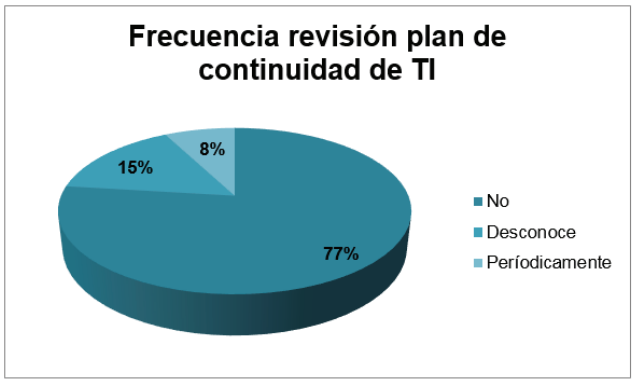
Ver Gráfico#2, Gráfico #14 a continuación.

Gráfico# 2 Mantenimiento plan continuidad TI.



N	Válido	70
	Perdidos	0
Media		1.69
DE		0.61
Mínimo		1
Máximo		4

Gráfico #14 Frecuencia revisión plan de continuidad de TI.



N	Válido	13
	Perdidos	0
Media		1.38
DE		0.84
Mínimo		1
Máximo		4

Discusión y Resultados Desconocen que exista mantenimiento del plan de continuidad y la mayoría afirma que no hay revisión del plan de continuidad de TI; de esta manera podemos decir que no cumplen con el mantenimiento del plan de continuidad de TI.

Análisis de Brechas Debido a que la institución no cuenta con un plan de continuidad de servicios, no existen argumentos para identificar las brechas en el mantenimiento de plan de continuidad.

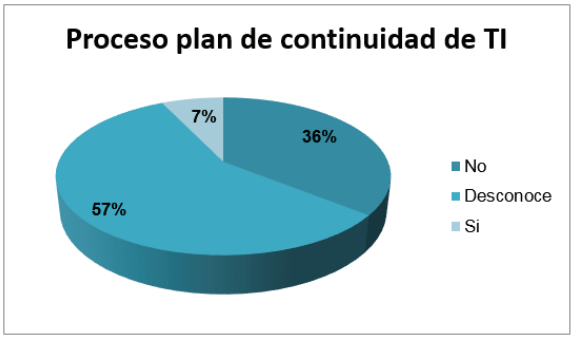
Recomendaciones Después de realizar el plan de continuidad, se debe definir y documentar una política para dar mantenimiento al mismo, dicha política tiene que prever un procedimiento para administrar el control de cambios y asegurar que estén acorde con los objetivos de continuidad actuales de la organización.

Se debe calendarizar revisiones trimestrales; si ocurre algún cambio en los elementos relacionados con los servicios críticos de TI,estos se tienen que guardar en todas las copias existentes del plan de continuidad,ya que con ello, se mantendrá actualizado el plan de continuidad conforme a las necesidades del negocio, y así se evitará la obsolescencia y el incremento de costos, en caso de ejecutarse el plan ante un desastre.

5.5. DS4.5 Pruebas del plan de continuidad de TI

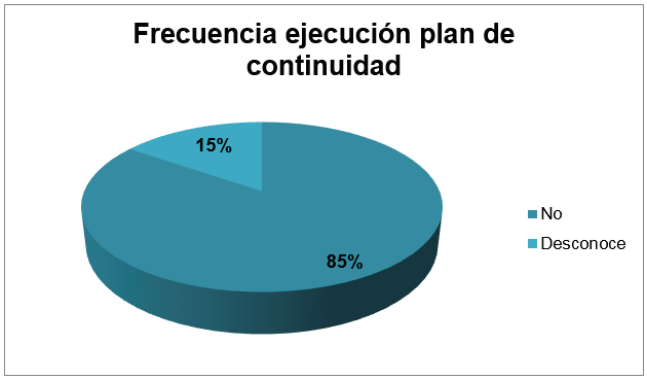
Ver Gráfico#4, Gráfico #15, Gráfico#18 y Gráfico#19 a continuación.

Gráfico# 4 Proceso plan de continuidad de TI.



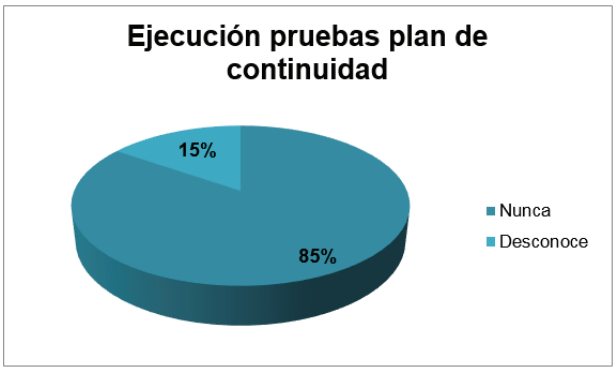
N	Válido	13
	Perdidos	0
Media		1.77
DE		0.8
Mínimo		1
Máximo		4

Gráfico #15 Frecuencia ejecución plan de continuidad.



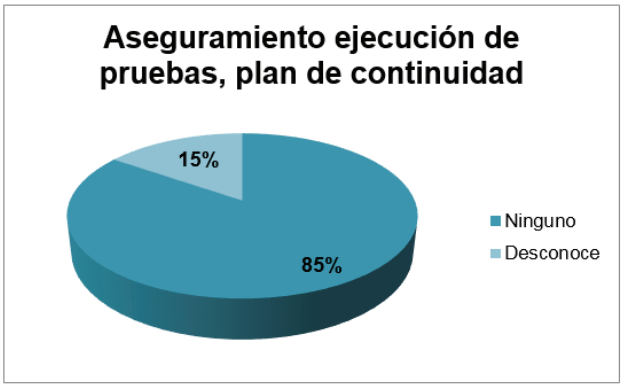
N	Válido	13
	Perdidos	0
Media		1.15
DE		0.36
Mínimo		1
Máximo		4

Gráfico# 18 Ejecución pruebas plan de continuidad.



N	Válido	13
	Perdidos	0
Media		1.15
DE		0.36
Mínimo		1
Máximo		4

Gráfico #19 Aseguramiento ejecución de pruebas, plan de continuidad.



N	Válido	13
	Perdidos	0
Media		1.15
DE		0.36
Mínimo		1
Máximo		4

Discusión y Resultados Según el estudio realizado y cómo podemos observar en los gráficos anteriores, la mayoría afirma que no existe pruebas para el plan de continuidad de TI y desconocen si existe un proceso definido.

Análisis de Brechas Según los objetivos de control de DS4, para el buen funcionamiento de plan de continuidad tienen que estarse realizando pruebas que sustenten la efectividad del plan, no obstante estos exámenes no se están realizando ante la carencia de procedimientos de continuidad del negocio.

Recomendaciones Se debe elaborar un plan de pruebas que tome en cuenta todos los elementos de la arquitectura tecnológica involucrados en los servicios críticos de TI, este plan debe contar al menos con una plantilla para la preparación de la muestra que incluya un plan de roolback y los responsables de dicha ejecución.

Una plantilla donde se documente la duración de las actividades de la prueba y los resultados obtenidos. Otra para reflejar los planes de acción y de mejora

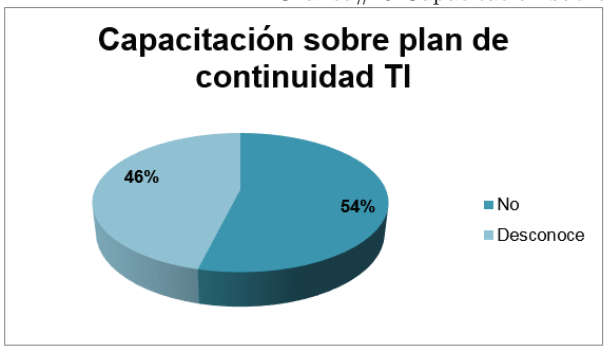
detectados durante las actividades de ejecución de la prueba y en caso de requerir cambios en la estructura del plan de continuidad los mismos tienen que ser comunicados y gestionados al comité de continuidad del negocio. Dicha ejecución de pruebas permite fortalecer la experiencia de los colaboradores involucrados en los procesos de recuperación de los servicios críticos de TI y aumentar la efectividad de la ejecución del plan de continuidad, en caso de la ocurrencia de un desastre real.

. Dicha ejecución de pruebas permite fortalecer la experiencia de los colaboradores involucrados en los procesos de recuperación de los servicios críticos de TI y aumentar la efectividad de la ejecución del plan de continuidad, en caso de la ocurrencia de un desastre real.

5.6. DS4.6 Entrenamiento del plan de continuidad de TI

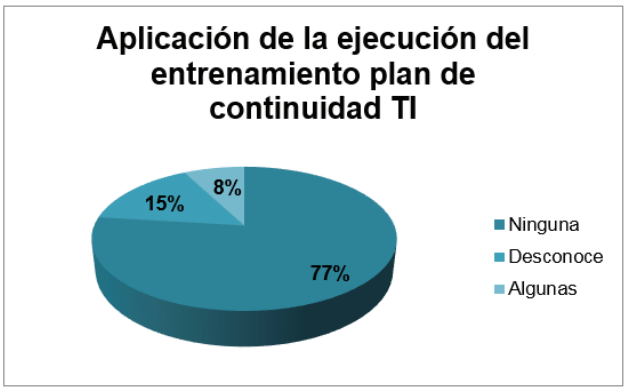
Ver Gráfico#6 y Gráfico#20 a continuación.

Gráfico# 6 Capacitación sobre plan de continuidad TI.



N	Válido	13
	Perdidos	0
Media		1.46
DE		0.5
Mínimo		1
Máximo		4

Gráfico #20 Aplicación de la ejecución del entrenamiento plan de continuidad TI.



N	Válido	13
	Perdidos	0
Media		1.31
DE		0.61
Mínimo		1
Máximo		4

Discusión y Resultados La mayoría expresa la no existencia de una capacitación o entrenamiento para el plan de continuidad, por lo cual no se realiza o aún no se ha implementado y es esencial antes de comenzar a trabajar el plan de continuidad de TI.

Análisis de Brechas El personal de TI no se encuentra capacitado para atender los procesos de desarrollo de un plan de continuidad.

Recomendaciones Capacitar al personal de TI en el marco de referencia COBIT e ITIL, esto permitirá una orientación sobre los elementos relacionados con la continuidad de las operaciones y servicios de TI, dichas capacitaciones son fundamentales para concientizar al personal sobre los riesgos existentes en la ejecución de sus funciones en caso de tener una emergencia operativa.

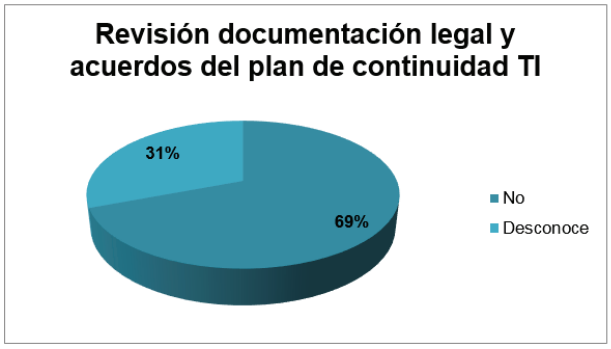
El plan de entrenamiento debe evidenciar claramente, cuales son los roles y responsabilidades de los involucrados en la gestión de continuidad de TI.

Se debe calendarizar sesiones de entrenamiento al menos trimestralmente o cuando existan cambios en el plan de continuidad.

5.7. DS4.7 Distribución del plan de continuidad de TI

Ver Gráfico#8 a continuación.

Gráfico# 8 Revisión documentación legal y acuerdos del plan de continuidad TI.



N	Válido	13
	Perdidos	0
Media		1.31
DE		0.46
Mínimo		1
Máximo		4

Discusión y Resultados Es evidente que no existe una revisión de la documentación legal y acuerdos del plan de continuidad TI por parte del personal del departamento, donde los colaboradores afirman el que no lo hacen o desconocen si es realizada.

Análisis de Brechas De acuerdo con los resultados obtenidos la institución carece de planes de continuidad, por esta razón hay un desconocimiento completo sobre la gestión de distribución de los elementos del plan de continuidad conforme a los roles y responsabilidades establecidas por COBIT, esta situación disminuirá la efectividad de la administración de la continuidad de los servicios de la institución.

Recomendaciones Posteriormente a la creación del plan de continuidad se deben establecer un procedimiento para definir los roles y las responsabilidades de los encargados de gestionar las distintas actividades del plan de continuidad, para logralo tienen que implementar una matriz RACI, en conformidad con la recomendada por COBIT en el apartado "DS4 Garantizar la Continuidad del Servicio"; asimismo la distribución de roles debe contemplar los criterios de clasificación de la información para evitar comprometer información sensible; el aplicar dicho procedimiento garantiza una apropiada distribución y accesibilidad de todas los colaboradores internos y externos involucrados en la prestación de servicios de TI.

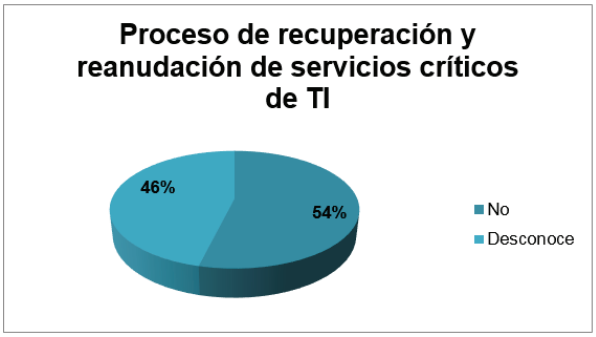
Establecer una política y procedimiento para la revisión de los OLA, UC, SLA's utilizados por el departamento de TI en la prestación de los servicios críticos para la institución. La presente exploración debe prevenir modificaciones

que pueda tener el plan de continuidad por vencimiento de contratos, cambio de garantías de cumplimiento, variacion e incorporación de nuevos elemento de la arquitectura tecnológica

5.8. DS4.8 Recuperación y reanudación de los servicios de TI

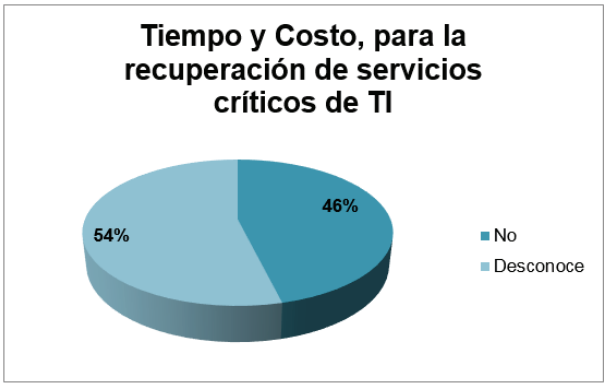
Ver Gráfico#9, Gráfico #11 y Gráfico#21 a continuación.

Gráfico# 9 Proceso de recuperación y reanudación de los servicios de TI.



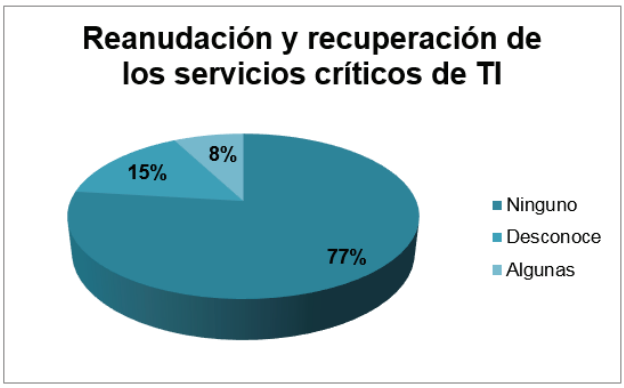
N	Válido	13
	Perdidos	0
Media		1.46
DE		0.5
Mínimo		1
Máximo		4

Gráfico# 11 Tiempo y Costo, para la recuperación de servicios críticos de TI.



N	Válido	13
	Perdidos	0
Media		1.54
DE		0.5
Mínimo		1
Máximo		4

Gráfico# 21 Reanudación y Recuperación de los servicios críticos de TI.



N	Válido	13
	Perdidos	0
Media		1.31
DE		0.61
Mínimo		1
Máximo		4

Discusión y Resultados Según el resultado de la mayoría no hay procesos de recuperación y aplicación de servicios críticos de TI y tampoco un tiempo y costo establecido para dicho cambio; por lo cual podemos afirmar que no cumplen con un proceso de recuperación y reanudación de servicios críticos de TI.

Análisis de Brechas Dentro las principales tareas para ejecutar una buena administración de la continuidad de servicios, está la definición de tiempos de respuesta esperados por la institución, dicho insumo es fundamental para planear las acciones de recuperación de los servicios de TI; no obstante, no se toman las medidas apropiadas a pesar de estar conscientes del riesgo que tiene la institución sin un mecanismo de recuperación ante desastres.

Según se puede constatar la institución no tiene un centro de procesamientos de datos alternativo, ni cuenta con un plan de comunicación a sus clientes e interesados, asimismo hay una limitación en los recursos económicos, para sufragar los gastos relacionados con la continuidad de las operaciones; según el objetivo de control de COBIT estos elementos son esenciales para establecer una política de continuidad de las funciones operativas de la empresa.

Recomendaciones El departamento de TI debe solicitar la elaboración de una política o priorización de recuperación de servicios críticos, detalle del impacto financiero, análisis de riesgos, roles y responsables del negocio encargados de activar los protocolos de contingencia y comunicación ante un evento que dificulte la operación normal de las actividades operativas de la organización.

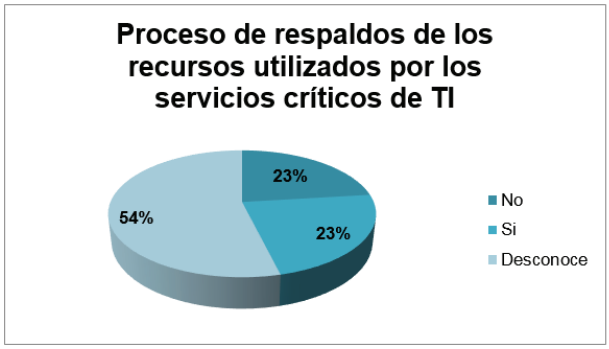
El departamento de TI debe implementar un sitio alterno de procesamiento alternativo, que permita la continuidad de las operaciones, según los tiempos de respuesta previamente establecidos, no obstante el acondicionamiento del sitio tiene que contar con procesos de replicación de datos en tiempo real (alta disponibilidad), equipos de procesamiento, red y líneas de comunicación que permitan conectar los usuarios y clientes en caso de un estado contingente; la implantación

de esta funcionalidad ayudara a minimizar tiempos y costos en la normalización de los servicios críticos de la organización.

5.9. DS4.9 Almacenamiento de respaldos fuera de las instalaciones

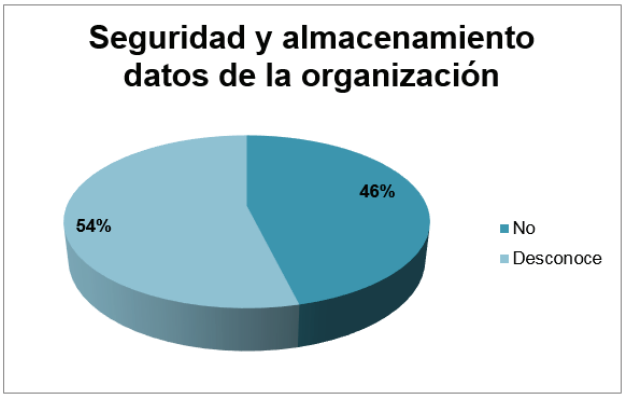
Ver Gráfico#10 y Gráfico #12 a continuación.

Gráfico# 10 Proceso de respaldos de los recursos utilizados por los servicios críticos de TI.



N	Válido	13
	Perdidos	0
Media		1.7
DE		0.46
Mínimo		1
Máximo		4

Gráfico# 12 Seguridad y almacenamiento datos de la organización.



N	Válido	13
	Perdidos	0
Media		1.54
DE		0.5
Mínimo		1
Máximo		4

Discusión y Resultados Desconocen el proceso para respaldos de los recursos utilizados por los servicios críticos de TI y no existe seguridad y almacenamiento de datos; se comprueba que no hay una asistencia que cubra los recursos fuera de las instalaciones.

Análisis de Brechas De conformidad con los datos suministrados existe una carencia en conocimiento de la seguridad de la información y los procesos de respaldo de los datos y otros elementos críticos de la arquitectura tecnológica.

Según la entrevista realizada al director de TI, se cuenta con un proceso de respaldo de bases de datos en la nube, a pesar de tener esta práctica elemental para salvaguardar la información, no se puede tomar como un proceso maduro, ya que, los objetivos de control de COBIT se especifica la necesidad de un proceso evaluador, para garantizar la disponibilidad, seguridad e integridad de los respaldos almacenados en sitios alternos.

Recomendaciones El departamento de TI, en conjunto con los responsables de los procesos del negocio, deben determinar el contenido de los respaldos almacenados; para formalizar esta actividad se debe hacer un acuerdo de necesidades de la información donde se indica el nombre del sistema, origen de los datos, localización, tipos de datos (base datos), de almacenamiento, tiempo de almacenamiento, medio de almacenamiento y frecuencia de actualización, con dicho acuerdo se establece los mecanismos de respaldos según la necesidades del negocio.

Se debe establecer los mecanismos de seguridad y acceso a los medios de respaldo conforme a la política de clasificación de los datos de la organización, en caso de no existir dicha clasificación se debe agregar los responsables en el documento de acuerdos de necesidades de la información. Definir un procedimiento de validación de los respaldos para determinar si efectivamente ejecutaron de manera correcta, por medio de bitácoras de revisión de respaldos, que genera la herramienta de administración de respaldos o el responsable en caso de hacerse manual.

Definir un protocolo o guía de restauración de bases de datos donde se pueda evidenciar el paso a paso para montar nuevamente una bases de datos online, dicho protocolo tiene que contemplar tanto la restauración en sitio como en sitio alterno.

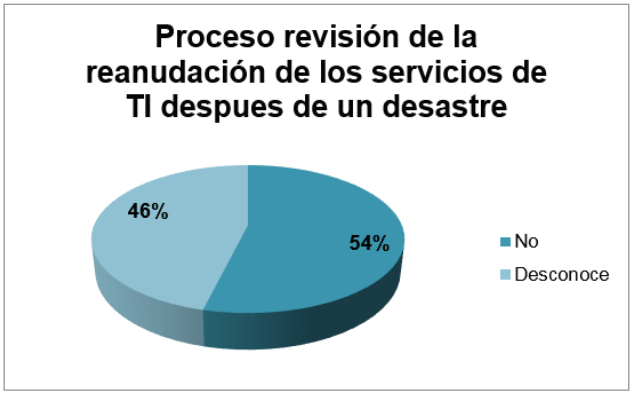
Definir un procedimiento de pruebas de los respaldos en custodio en sitio alterno para evaluar periódicamente la integridad de los datos almacenados, asimismo debe agregarse un apartado donde indique los resultados de las pruebas; esta actividad se debe realizar al menos una vez a la semana para minimizar la materialización de perdida de información y una gestión apropiada de la administración de respaldos.

Definir un protocolo o guía de restauración de los sistemas de información donde se especifique el paso para conectarse con los orígenes de datos y los métodos de publicación, dicho protocolo tiene que contemplar tanto la restauración en sitio como en sitio alterno. Establecer una política de revisión de los contratos establecidos con los proveedores de sitios de almacenamiento alterno; esta actividad se debe calendarizar al menos dos veces al año.

5.10. DS4.10 Revisión post reanudación

Discusión y Resultados Ver Gráfico#13 a continuación.

Gráfico# 13



N	Válido	13
	Perdidos	0
Media		1.46
DE		0.5
Mínimo		1
Máximo		4

No existen o desconocen el proceso de revisión de la reanudación de los servicios de TI, después de un accidente o desastre; por lo cual no cumplen con la revisión de post reanudación.

Análisis de Brechas De acuerdo con los lineamientos establecidos por COBIT después de ocurrir un evento adverso a la continuidad de las operaciones los directores de TI deben valorar lo adecuado de la ejecución del plan, conforme a las respuestas obtenidas no hay un plan de continuidad por tanto es una brecha contra el objetivo de control.

Recomendaciones Realizar un procedimiento de valoración post reanudación de los servicios críticos de TI donde se pueda medir la efectividad del plan, el insumo para hacerlo es un checklist que contenga la lista de actividades del diseño de continuidad y sus relaciones con otros elementos como protocolos de restauración, asimismo debe contener un apartado donde indique si es requerido la actualización del proyecto de continuidad.

6. Propuesta

De conformidad con los requerimientos establecidos por COBIT en el proceso DS4.Garantizar la continuidad del servicio, además de tomar en cuenta las mejores prácticas recomendadas por ITL v3; se propone utilizar el siguiente esquema de marco de gestión de continuidad para el MTSS:

6.1. Marco de Gestión de Continuidad de TI: Disposiciones Generales

Introducción: Describir los aspectos básicos de la necesidad de implementar el marco de gestión

Objetivo General: Describir los objetivos buscados con la implementación del marco de gestión

Objetivos Específicos: Describir los objetivos específicos

Alcance: Indicar cuales son los servicios críticos estará cubiertos por el marco de gestión de continuidad

6.2. Directrices

Legislación Aplicable: Indicar cuales normas regulatorias son aplicadas al área de tecnologías de información del MTSS

Plan de Continuidad: En este apartado se debe hacer las referencias al plan de continuidad, con una descripción de los elementos principales, hacer referencia al objetivo de control DS4.2 Planes de continuidad de TI de COBIT y al Service Desing (4.5 Gestión de continuidad de servicios de TI, 4.5.5.1 Etapa 1 – Inicio) de ITIL V3

Plan de Contingencia: En este apartado se enumerar los mecanismos contingentes que utilizará la organización ante el colapso de sus operaciones, esta actividad debe ser definida en conjunto con las demás áreas de la institución

Identificación de Recursos Críticos: Establecer los lineamientos que se deben utilizar para la gestión de identificación los recursos críticos de TI, hacer referencia al objetivo de control DS4.3 Recurso Críticos de TI de COBIT y Service Desing (4.4.5.2 Actividades proactivas de la gestión de la disponibilidad) de ITIL v3

Riesgos y Controles: En este apartado se define el proceso de gestión de riesgos y los planes de acción involucrados en el proceso de gestión de continuidad de las operaciones, hacer referencia al proceso Evaluar y Administrar los Riesgos de TI de COBIT.

Indicadores de desempeño: En este apartado se deben realizar los indicadores de desempeño que permitan medir la capacidad del marco de gestión de continuidad de TI, hacer referencia al objetivo de control DS4 y Garantizar la Continuidad del Servicio en el apartado Metas y Métricas de COBIT

6.3. Roles y Responsabilidades

En este apartado se establecen los roles del marco de gestión y se indica los colaboradores responsables del mantenimiento y ejecució, hacer referencia al objetivo de control DS4 Garantizar la Continuidad del Servicio en el apartado Matriz RACI de COBIT, adaptar la matriz acorde a las áreas de la institución.

6.4. Mejora Continua

En este apartado se definen los procesos administrativos para la gestión y administración del marco de gestión de continuidad, hacer referencia a DS4.4 Mantenimiento del plan de continuidad de TI de COBIT y Service Desing (4.5.5.4 Etapa 4 – Operación continua) de ITIL v3 .

7. Conclusiones

El personal del departamento de tecnologías de información del MTSS desconoce la existencia de un marco de gestión de continuidad de los servicios considerados críticos por la institución; según los lineamientos establecidos por COBIT 4.1 es indispensable fomentar la implantación de la recuperación de los servicios de TI, a través de un plan documentado que pueda evidenciar las políticas y procedimientos destinados a salvaguardar la disponibilidad de los servicios de la institución.

De acuerdo al análisis de resultados de la investigación existe una falencia en la comunicación de temas trascendentales como el alineamiento del negocio con TI,esta a través de la experiencia se retoma uno de los elementos fundamentales para la implementación de un marco de gestión de continuidad, como es la comunicación, por esta razón debe existir un órgano interno (comité de continuidad) que pueda tomar decisiones e informarle a todos los interesados sobre la continuidad de servicios de la institución.

Es importante tomar en cuenta los resultados donde nos indican la carencia de un plan de continuidad de los servicios críticos de TI; esto aumenta las vulnerabilidades para responder en un momento oportuno ante fallas en la plataforma tecnológica que soporta la operación critica de la institución; dicha falencia impide cumplir con las regulaciones de la CCntraloría General de la Republica ,aplicadas a la gestión de tecnología de las instituciones públicas del país.

Según las mejores prácticas de control de COBIT, una las causas que afectan considerablemente la continuidad de las operaciones del negocio está la falta de un proceso que permita la identificación de recursos críticos que conforman la arquitectura tecnológica, por esta razón es necesario su implementación para construir resistencia y definir las prioridades ante la materialización de un evento no deseado.

Para el buen funcionamiento del plan de continuidad es trascendental contar con un proceso de pruebas. Estas se verifican mediante situaciones inesperadas.

Las cuales se constantan que no se están realizando ante la carencia de procedimientos de continuidad de la empresa; en vista de lo anterior después proporcionar un plan de continuidad a la institución se debe elaborar una política para la ejecución de pruebas de continuidad de las operaciones.

Un aspecto positivo la institución es contar con un proceso de respaldo de bases de datos en la nube, a pesar de tener esta práctica elemental para salvaguardar la información, no se puede tomar como un proceso maduro, ya que los objetivos de control de COBIT se deben implementar, en un un sitio de procesamiento alternativo que permita la continuidad de las operaciones, según los tiempos de respuesta previamente establecidos por la institución.

Los colaboradores indican que no han recibido entrenamiento para estructurar un plan de continuidad de TI y la distribución del mismo; esto disminuye la efectividad de la administración de la continuidad de los servicios de la institución, es importante la incursión en capacitaciones al personal clave, sobre el marco de referencia COBIT e ITIL, esto permitirá una orientación sobre los elementos relacionados con la continuidad de las operaciones de la institución. Al concluir la investigación sobre la continuidad de los servicios críticos de TI del MTSS,se toma en cuenta el resultado de la encuesta aplicada a sus colaboradores del área de tecnologías de información y el análisis de brechas, con lo que se afirma que la institución esta consiente de los riesgos , vulnerabilidades, amenazas y el impacto, que se pudiera presentar por la pérdida de la continuidad de los servicios críticos, por lo tanto, se sugiere trabajar en la implementación de un marco de gestión de continuidad que pueda colaborar en el reforzamiento de la continuidad de las operaciones críticas de la institución.

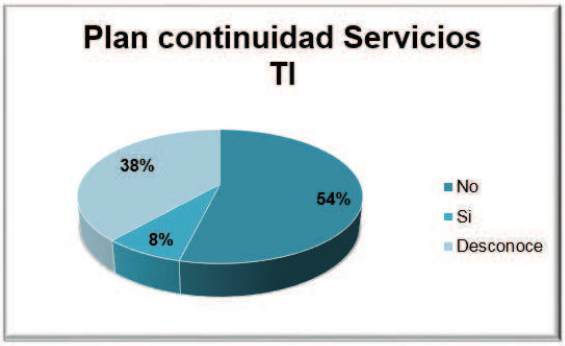
8. Anexos

8.1. Anexo 1

¿La organización cuenta con un plan de continuidad de los servicios de TI que ayuden a soportar la continuidad del negocio? Ver Tabla#1 y Gráfico# 1 a continuación.

Tabla #1 – Discusión de los datos obtenidos de la pregunta #1.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	7	53.85	53.85	53.85
Desconoce	2,00	5	38.46	38.46	92.31
Implementándose	3,00	0	0	0	92.31
Sí	4,00	1	7.69	7.69	100
	Total	13	100	100	

Gráfico#1 - Discusión de los datos obtenidos de la pregunta#1.



N	Válido	13
	Perdidos	0
Media		1.62
DE		0.84
Mínimo		1.00
Máximo		4.00

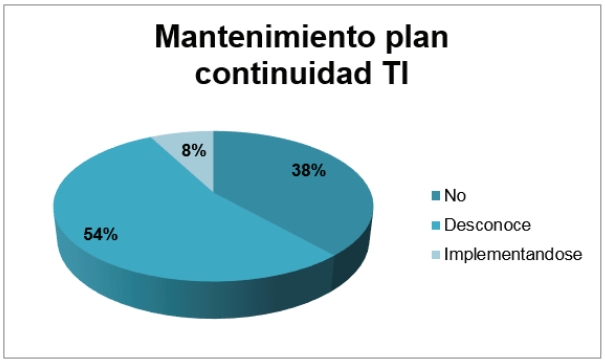
Cada día se crean en las instituciones y empresas más aplicaciones de servicio, que se basan en tecnología de información, y se hace más dependiente de TI, cualquier falla puede afectar severamente. Para ello se formula la pregunta (ver tabla 1 / gráfico 1) como soporte continuo del negocio; tal cuestionamiento da como resultado un 54 % del personal que indica no haber un plan de continuidad que sirva como soporte para la ejecución de funciones, el 38 % desconoce si existe y un 8 % indica que sí existe, para lo cual este único % afirmativo, no es relevante, ya que corresponde a un único colaborador. (Ver DS4.2 Planes de Continuidad de TI)

8.2. Anexo 2

¿Existe un procedimiento para el mantenimiento del plan de continuidad TI que permita asegurar su actualización conforme a las necesidades actuales del negocio? Ver Tabla #2 y Gráfico #2 a continuación.

Tabla #2 – Discusión de los datos obtenidos de la pregunta #2.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	5	38.46	38.46	38.46
Desconoce	2,00	7	53.85	53.85	92.31
Implementándose	3,00	1	7.69	7.69	100
Sí	4,00	0	0	0	100
	Total	13	100	100,00	

Gráfico#2 - Discusión de los datos obtenidos de la pregunta#2.



N	Válido	70
	Perdidos	0
Media		1.69
DE		0.61
Mínimo		1
Máximo		4

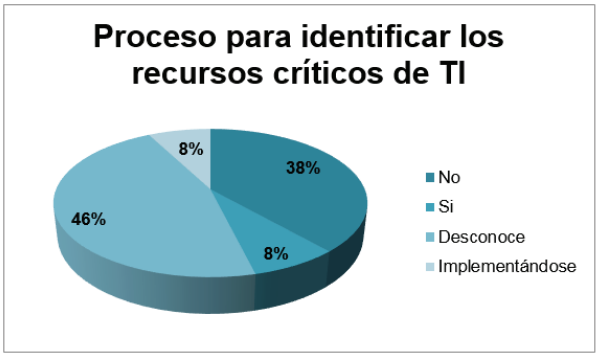
Todos los colaboradores a cargo de un proceso del negocio debe adueñarse y conocer al 100 % del mismo, es por ello que se realiza el mantenimiento de los planes de continuidad, pero al consultar a los colaboradores de TI del MTSS el 54 % desconoce la existencia de procedimientos para el mantenimiento de plan de continuidad, el 38 % indica que no existe y el 8 % dice que se encuentran implementándolo. (Ver DS4.4 Mantenimiento del Plan de Continuidad de TI)

8.3. Anexo 3

¿El departamento de Tecnologías de información cuenta con un proceso definido y documentado para identificar los recursos críticos de TI? Ver Tabla #3 y Gráfico #3 a continuación.

Tabla #3 – Discusión de los datos obtenidos de la pregunta #3.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	5	38.46	38.46	38.46
Desconoce	2,00	6	46.15	46.15	84.62
Implementándose	3,00	1	7.69	7.69	92.31
Sí	4,00	1	7.69	7.69	100
	Total	13	100	100,00	

Gráfico#3 - Discusión de los datos obtenidos de la pregunta#3.



N	Válido	70
	Perdidos	0
Media		1.85
DE		0.86
Mínimo		1
Máximo		4

Para poder identificar los recursos críticos existentes en el MTSS,se consultó si cuentan con un proceso definido y documentado, para que sean identificados en su plan de continuidad, de lo cual se encontró que el 46 % desconoce si existe o no un proceso definido y documentado, para identificar los recursos críticos de TI, un 38 % indican que no lo hay, un 8 % indica que se encuentra en implementación y 8 % afirma su existencia, estos dos últimos resultados no son relevantes para este estudio ya que representa solo dos colaboradores. (Ver DS4.3 Recursos críticos de TI)

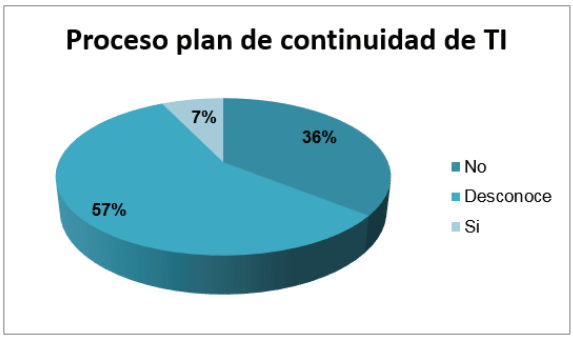
8.4. Anexo 4

¿El departamento de Tecnologías de información cuenta con un proceso definido y documentado para realizar las pruebas sobre el plan de continuidad de TI? Ver Tabla #4 y Gráfico #4 a continuación.

Tabla #4 – Discusión de los datos obtenidos de la pregunta #4.

Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	5	38.46	38.46	38.46
Desconoce	2,00	7	53.85	53.85	92.31
Implementándose	3,00	0	0	0	92.31
Sí	4,00	1	7.69	7.69	100
	Total	13	100,00	100,00	

Gráfico#4 - Discusión de los datos obtenidos de la pregunta#4.



N	Válido	13
	Perdidos	0
Media		1.77
DE		0.8
Mínimo		1
Máximo		4

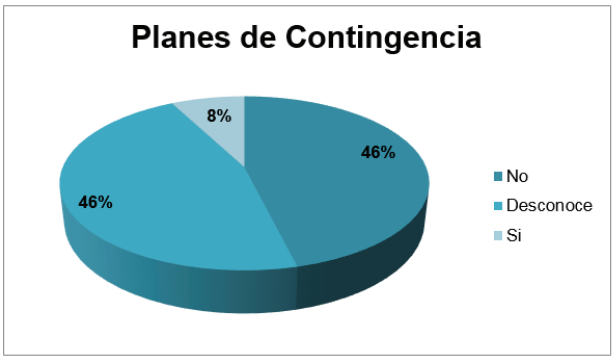
Un plan de continuidad de TI, debe ser exitoso si tiene un proceso bien definido, revisado por medio de pruebas antes de aplicar cualquier nuevo proceso, de lo que se encontró que el 57 % desconoce si hay proceso definido y documentado, para el plan de continuidad de TI, un 36 %indica que no existe y un 7 % afirma que si lo hay. (Ver el DS4.5 Pruebas del plan de continuidad de TI)

8.5. Anexo 5

¿El departamento de Tecnologías de información tiene planes de contingencia para el procesamiento alternativo, principios de respaldo y recuperación? Ver Tabla #5 y Gráfico #5 a continuación.

Tabla #5 – Discusión de los datos obtenidos de la pregunta #5.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	6	46.15	46.15	46.15
Desconoce	2,00	6	46.15	46.15	92.31
Implementándose	3,00	0	0	0	92.31
Sí	4,00	1	7.69	7.69	100
	Total	13	100,00	100,00	

Gráfico#5 - Discusión de los datos obtenidos de la pregunta#5.



N	Válido	13
	Perdidos	0
Media		1.69
DE		0.82
Mínimo		1
Máximo		4

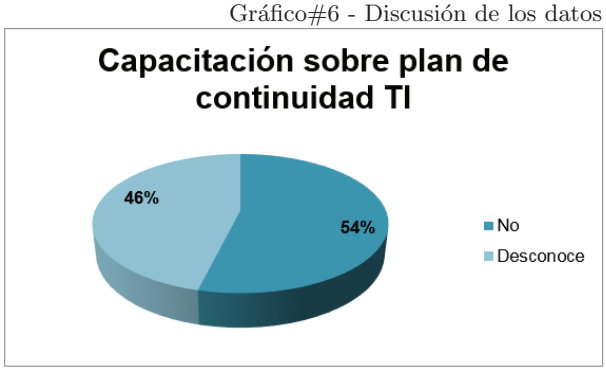
En las áreas de TI siempre debe de haber un plan de contingencia, que sirva como instrumento de gestión, para el buen gobierno de las Tecnologías, pero para implementarlo es necesario identificar los procesos críticos de la operación, que puedan ser eventuales interrupciones al plan y buscar una forma de amortiguarlo; al tratar de conocer cuál es el procesamiento alternativo del MTSS y cuáles son los principios de respaldo y recuperación; no hubo una respueta clara, ya que el 46 % indica que no existen planes de contingencia para el procesamiento alternativo, para el respaldo y recuperación, un 46 % desconoce si existe algún plan y un 8 % afirma que sí hay un plan de contingencia, lo cual no es significativo, ya que corresponde a una persona.(Ver el DS4.3 Recursos críticos de TI)

8.6. Anexo 6

¿El departamento de Tecnologías de información cuenta con un proceso definido y documentado para realizar el entrenamiento sobre el plan de continuidad de TI? Ver Tabla #6 y Gráfico #6 a continuación.

Tabla #6 – Discusión de los datos obtenidos de la pregunta #6.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	7	53.85	53.85	53.85
Desconoce	2,00	6	46.15	46.15	100
Implementándose	3,00	0	0	0	100
Sí	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#6 - Discusión de los datos obtenidos de la pregunta#6.



N	Válido	13
	Perdidos	0
Media		1.46
DE		0.5
Mínimo		1
Máximo		4

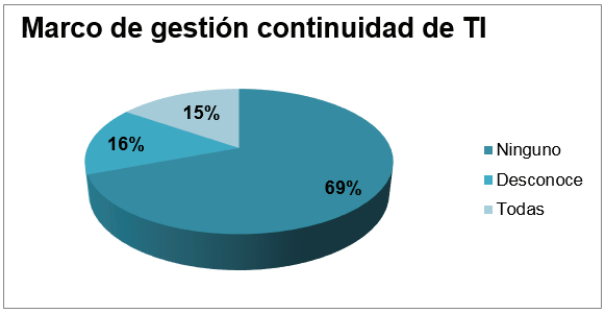
En un plan de continuidad se realiza el entrenamiento sobre los procedimientos y roles que participan cada uno de los colaboradores, por lo que se consultó, si existe un proceso definido y documentado que responsabilice a alguien, en caso de un desastre. Donde 54 % indica que no existen procesos definidos y documentados, para capacitar al personal sobre un plan de continuidad para TI y el 46 % expresa desconocer sobre si existe un plan de entrenamiento. (Ver el DS4.6 Entrenamiento del plan de continuidad de TI)

8.7. Anexo 7

¿El departamento de Tecnologías de información cuenta con un proceso definido y documentado para realizar la administración del plan de continuidad de TI? Ver Tabla #7 y Gráfico #7 a continuación.

Tabla #7 – Discusión de los datos obtenidos de la pregunta #7.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	8	61.54	61.54	61.54
Desconoce	2,00	5	38.46	38.46	100
Implementándose	3,00	0	0	0	100
Sí	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#7 - Discusión de los datos obtenidos de la pregunta#7.



N	Válido	13
	Perdidos	0
Media		1.28
DE		0.45
Mínimo		1
Máximo		4

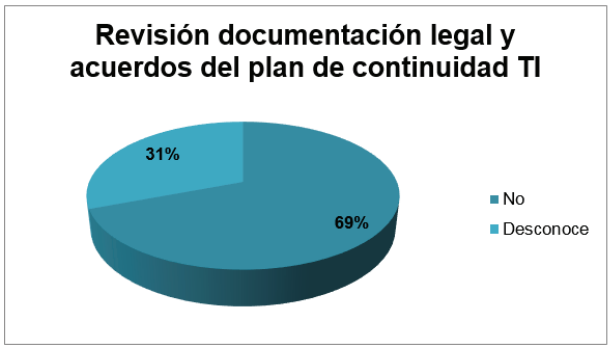
Conocer el negocio es primordial a la hora de realizar y ejecutar un marco de continuidad, es por ello que por medio de esta pregunta se quiso conocer el marco de gestión de continuidad de TI del MTSS y si el mismo cuenta con un proceso definido y documentado para su administración, se encontró que el 62 % manifiesta que no existe en el departamento de TI, pruebas para los procesos de plan de continuidad de TI y un 38 % indica desconocer del tema. (Ver el DS4.1 Marco de Trabajo de Continuidad de TI)

8.8. Anexo 8

¿El departamento de Tecnologías de información realiza revisiones periódicas sobre los contratos y acuerdos de nivel de servicio involucrados dentro del plan de continuidad de TI? Ver Tabla #8 y Gráfico #8 a continuación.

Tabla #8 – Discusión de los datos obtenidos de la pregunta #8.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	9	69.23	69.23	69.23
Desconoce	2,00	4	30.77	30.77	100.00
Implementándose	3,00		0.00	0.00	100.00
Sí	4,00		0.00	0.00	100.00
	Total	13	100,00	100,00	

Gráfico#8 - Discusión de los datos obtenidos de la pregunta#8.



N	Válido	13
	Perdidos	0
Media		1.31
DE		0.46
Mínimo		1
Máximo		4

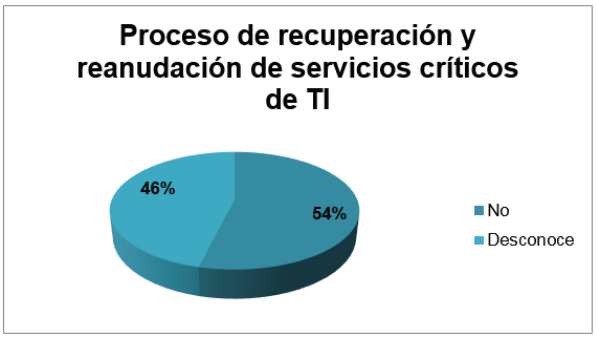
En todo plan de una empresa, ya sea de continuidad u otro tema, se debe de revisar que la documentación legal no solo se alinee a la legislación del país, si no que se adapte a los requerimientos de la empresa en sus contratos y acuerdos del mismo. Para conocer si tal efecto se lleva a cabo, se consultó a los empleados de TI del MTSS. Cuyo resultado fue: el 69 % dice que no existe y un 31 % indica que lo desconoce . (Ver el DS4.7 Distribución del plan de continuidad de TI)

8.9. Anexo 9

¿El departamento de Tecnologías de información cuenta con un proceso definido y documentado para realizar la recuperación y reanudación de los servicios críticos de TI? Ver Tabla #9 y Grafico #9 a continuación.

Tabla 9 – Discusión de los datos obtenidos de la pregunta #9.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	7	53.85	53.85	53.85
Desconoce	2,00	6	46.15	46.15	100
Implementándose	3,00	0	0	0	100
Sí	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#9 - Discusión de los datos obtenidos de la pregunta#9.



N	Válido	13
	Perdidos	0
Media		1.46
DE		0.5
Mínimo		1
Máximo		4

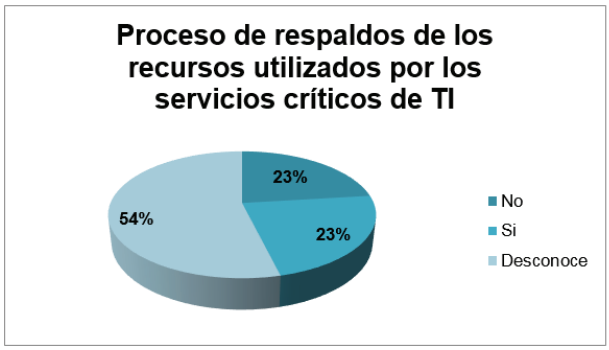
Es importante siempre tener un plan de trabajo que permita continuar con la operación, después de un desastre, que no traiga consecuencias a futuro o en el momento. Para esto se investiga cómo lo hace el MTSS en su departamento de TI, cuál es su proceso y si el mismo se encuentra definido y documentado, habrá que averiguar dónde se detectó. El resultado de los encuestados son: 54 % indica que no existe un proceso de recuperación y reanudación de servicios críticos de TI y el 46 % tiene desconocimiento de si existe un proceso definido. (Ver el DS4.2 Planes de Continuidad de TI y DS4.8 Recuperación y reanudación de los servicios de TI)

8.10. Anexo 10

¿El Departamento de Tecnologías de Información contará con un proceso definido y documentado para realizar respaldos de fuera de sitio de los recursos utilizados por los servicios críticos de TI? Ver Tabla #10 y Gráfico#10 a continuación.

Tabla #10 – Discusión de los datos obtenidos de la pregunta #10.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	3	23.08	23.08	23.08
Desconoce	2,00	7	53.85	53.85	76.92
Implementándose	3,00	0	0	0	76.92
Sí	4,00	3	23.08	23.08	100
	Total	70	100,00	100,00	

Gráfico#10 - Discusión de los datos obtenidos de la pregunta#10.



N	Válido	13
	Perdidos	0
Media		1.7
DE		0.46
Mínimo		1
Máximo		4

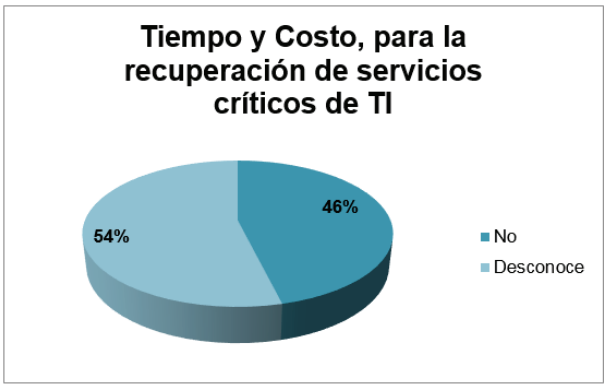
Todo proceso debe existir la seguridad de la información y esto implica la existencia de respaldos físicos y electrónicos. Para ello, se debe conocer qué tipo de apoyo se utilizan para los servicios críticos de TI y si este se encuentra como proceso (definido y documentado). Asimismo,¿ dónde se encontró? Con base en lo expresado por los trabajadores de TI del MTSS, el 54 % desconoce si existe un proceso definido y documentado para realizar respaldos de fuera de sitio de los recursos utilizados, un 23 % indica que no los hay y un 23 % afirman su existencia. El mismo es utilizado para analizar el DS4.9 Almacenamiento de respaldos fuera de las instalaciones.

8.11. Anexo 11

¿La organización establece los tiempos y costos aceptables para la recuperación y normalización de los servicios críticos de TI? Ver Tabla #11 y Gráfico #11 a continuación.

Tabla #11 – Discusión de los datos obtenidos de la pregunta #11.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	6	46.15	46.15	46.15
Desconoce	2,00	7	53.85	53.85	100
Implementándose	3,00	0	0	0	100
Sí	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#11 - Discusión de los datos obtenidos de la pregunta#11.



N	Válido	13
	Perdidos	0
Media		1.54
DE		0.5
Mínimo		1
Máximo		4

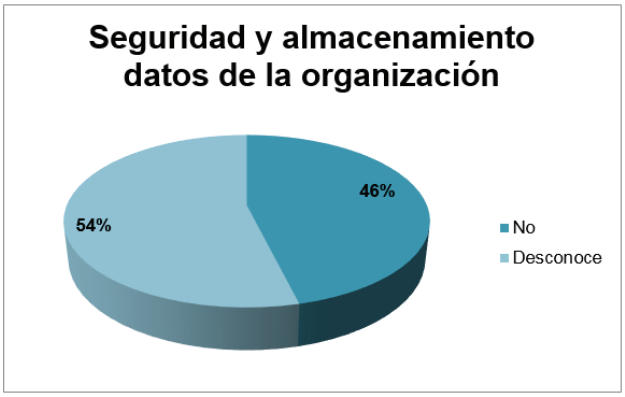
Todo proyecto requiere de un proceso, el cual está acompañado de un cronograma para asegurar que se cumpla con los requerimientos y un presupuesto adeecuado a la empresa, po lo que en esta apartado se pretende averiguar cómo se da el proceso de recuperación y normalización de los servicios críticos de TI y de qué forma los respaldan; para lo cual se consultó a los colaboradores de TI y se encontró que el 54 % indica desconocer de si existe un tiempo y costo establecido, para la recuperación de servicios críticos de TI y el 46 % dice no existir. (Ver el DS4.8 Recuperación y reanudación de los servicios de TI y DS4.9 Almacenamiento de respaldos fuera de las instalaciones)

8.12. Anexo 12

¿El departamento de Tecnologías de información cuenta con un proceso definido y documentado para la clasificación, aseguramiento y almacenamiento de los datos de la organización? Ver Tabla #12 y Gráfico #12 a continuación.

Tabla #12 – Discusión de los datos obtenidos de la pregunta #12.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	6	46.15	46.15	46.15
Desconoce	2,00	7	53.85	53.85	100
Implementándose	3,00	0	0	0	100
Sí	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#12 - Discusión de los datos obtenidos de la pregunta#12.



N	Válido	13
	Perdidos	0
Media		1.54
DE		0.5
Mínimo		1
Máximo		4

Cuando se inicia un proyecto se debe tener en cuenta que pueden existir acontecimientos o desastres durante su ejecución, es por ello, que la seguridad y almacenamiento datos de la organización son esenciales para conocer el manejo de sus respaldos o seguridad electrónica. En el análisis realizado se encontró en el departamento de TI del MTSS que: el 54 % desconoce si hay un proceso documentado y definido para su clasificación y un 46 % indican la no existencia.(Ver el DS4.9 Almacenamiento de respaldos fuera de las instalaciones)

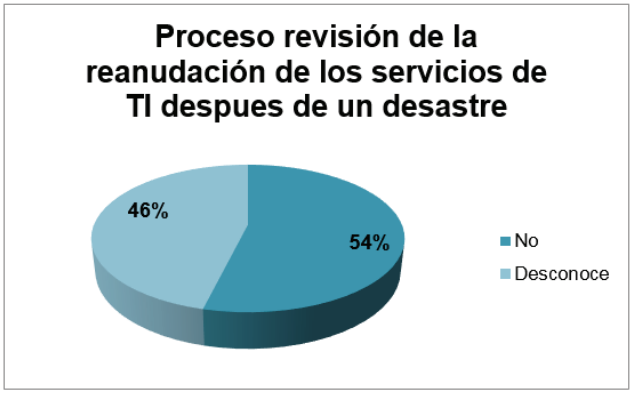
8.13. Anexo 13

¿En el departamento de Tecnologías de la información se contará con un proceso definido y documentado para la revisión de la reanudación de los servicios críticos de TI, después de ocurrir un desastre? Ver Tabla #13 y Gráfico #13 a continuación.

Tabla #13 – Discusión de los datos obtenidos de la pregunta #13.

Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	7	53.85	53.85	53.85
Desconoce	2,00	6	46.15	46.15	100
Implementándose	3,00	0	0	0	100
Sí	4,00	0	0	0	100
	Total	70	100,00	100,00	

Gráfico#13 - Discusión de los datos obtenidos de la pregunta#13.



N	Válido	13
	Perdidos	0
Media		1.46
DE		0.5
Mínimo		1
Máximo		4

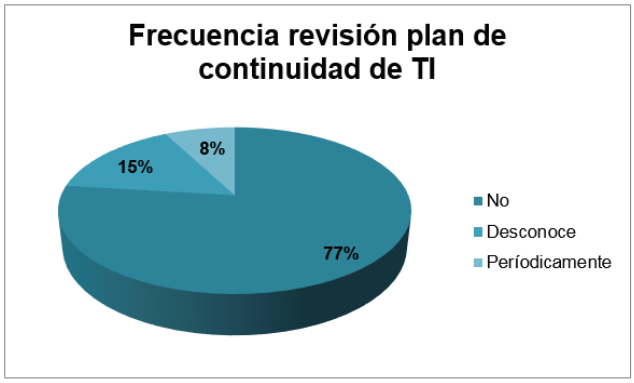
La revisión de los procesos es siempre esencial, para identificar si se cumple con los requerimientos del proyecto o proceso; en este caso la reanudación de los servicios de TI después de un desastre es fundamental para garantizar que el proceso no tuvo ningún inconveniente o pérdida importante de datos que se deba subsanar; para ello, se consultó sobre la existencia de un proceso ya definido y documentado en TI del MTSS y se obtuvo que el 54 % de los colaboradores de TI indican que no existe un proceso definido y documentado, para la revisión de la reanudación de los servicios de TI después de un desastre y el 46 % desconocen del tema.(Ver el DS4.10 Revisión post reanudación)

8.14. Anexo 14

¿Cuál es la frecuencia de revisión del plan de continuidad de TI? Ver Tabla #14 y Gráfico #14 a continuación.

Tabla #14 – Discusión de los datos obtenidos de la pregunta #14.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	10	76.92	76.92	76.92
Desconoce	2,00	2	15.38	15.38	92.31
Mensual	3,00	0	0	0	92.31
Periódicamente	4,00	1	7.69	7.69	100
	Total	13	100,00	100,00	

Gráfico#14 - Discusión de los datos obtenidos de la pregunta#14.



N	Válido	13
	Perdidos	0
Media		1.38
DE		0.84
Mínimo		1
Máximo		4

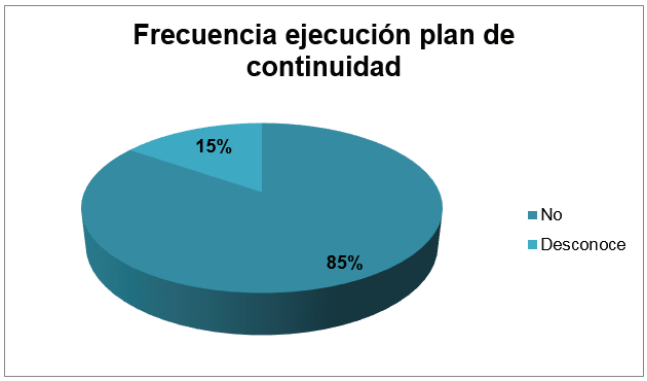
Se debe determinar según el proceso o proyecto que se esté realizando, cuál es el tiempo adecuado entre una revisión y otra que permita controlar la ejecución del mismo, en este caso la frecuencia de revisión del plan de continuidad de TI, así analizar si es el más adecuado. Lo anterior no fue posible, ya que sus colaboradores de TI expresaron: el 77 % que no se realiza revisiones al plan de continuidad de TI, un 15 % dice no saber y el 8 % afirma que se realizan de forma periódica; lo cual indica que no existe control ni un proceso de mantenimiento al plan de continuidad de TI del MTSS (Ver DS4.4 Mantenimiento del Plan de Continuidad de TI)

8.15. Anexo 15

¿Cuál es la frecuencia de la ejecución de las pruebas del plan de continuidad de TI? Ver Tabla #15 y Gráfico #15 a continuación.

Tabla #15 – Discusión de los datos obtenidos de la pregunta #15.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
No	1,00	11	84.62	84.62	84.62
Desconoce	2,00	2	15.38	15.38	100
Mensual	3,00	0	0	0	100
Periódicamente	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#15 - Discusión de los datos obtenidos de la pregunta#15.



N	Válido	13
	Perdidos	0
Media		1.15
DE		0.36
Mínimo		1
Máximo		4

Las pruebas del plan de continuidad de TI son fundamentales para todo proceso a implementar o como revisión de los mismos, por lo que siempre debe estar definido por un cronograma cuando se van a realizar y documentado el proceso, en este caso al revisar con el personal de TI del MTSS, se encontró que, según el 85 % de los colaboradores, no se realiza y el 15 % indica desconocer si se realiza. (Ver el DS4.5 Pruebas del plan de continuidad de TI)

8.16. Anexo 16

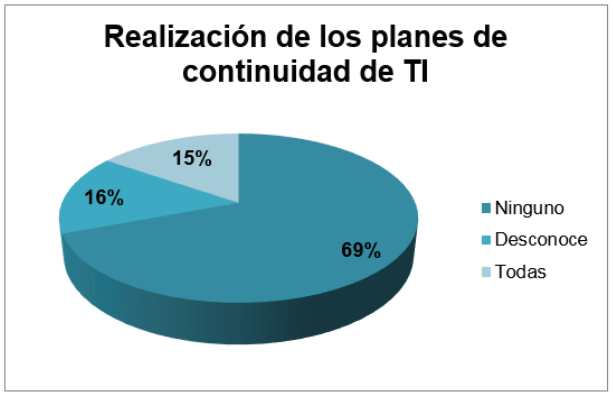
¿Los siguientes procedimientos y planes son contempladas por el plan de continuidad de TI? Establece la resistencia de la infraestructura tecnológica

a) Establece planes de recuperación de desastres
b) Establece planes de contingencia
c) Establece la estructura de administración de la continuidad de los servicios.
d) Establece los procesos de comunicación y distribución de funciones y responsabilidades.
e) Establece los roles y responsabilidades de los proveedores de servicios internos y externos de TI.

Ver Tabla #16 y Gráfico #16 a continuación.

Tabla #16 – Discusión de los datos obtenidos de la pregunta #16.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
Ninguno	1,00	9	69.23	69.23	69.23
Desconoce	2,00	2	15.38	15.38	84.62
Algunas	3,00	0	0	0	84.62
Todas	4,00	2	15.38	15.38	100
	Total	13	100,00	100,00	

Gráfico#16 - Discusión de los datos obtenidos de la pregunta#16.



N	Válido	13
	Perdidos	0
Media		1.62
DE		1.08
Mínimo		1
Máximo		4

Los procedimientos para la realización de los planes de continuidad, deben de encontrarse definidos y administrados por sus colaboradores según sus roles y responsabilidades; por lo cual se les dio una lista con el fin de identificar si tienen definido un marco de trabajo, para el plan de continuidad de TI, y se obtuvo que el 69 % indica que no existen, el 16 % no saben si los hay y un 15 %

afirma que todos se realizan. (Ver el DS4.1 Marco de Trabajo de Continuidad de TI))

8.17. Anexo 17

¿Cuáles de los siguientes puntos son asegurados en los procesos de identificación de recursos críticos de TI?

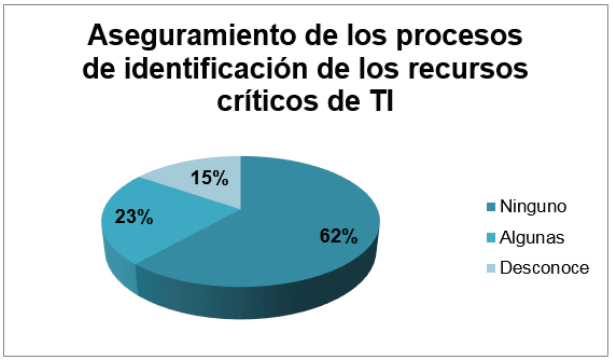
a) Establece la priorización de los recursos críticos.
b) La identificación de recursos está conforme a las necesidades prioritarias del negocio.
c) Mantiene los costos de recuperación en niveles aceptables para el negocio.
d) Cumple con los requisitos regulatorios y contractuales del negocio.
e) Considera los requerimientos de resistencia, respuesta y recuperación conforme a los niveles de priorización.

Ver Tabla #17 y Gráfico #17 a continuación.

Tabla #17 – Discusión de los datos obtenidos de la pregunta #17.

Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
Ninguno	1,00	8	61.54	61.54	61.54
Desconoce	2,00	2	15.38	15.38	76.92
Algunas	3,00	3	23.08	23.08	100
Todas	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#17 - Discusión de los datos obtenidos de la pregunta#17.



N	Válido	13
	Perdidos	0
Media		1.62
DE		0.84
Mínimo		1
Máximo		4

Asegurar la información de los datos con los que se trabajan, en cada proceso, son fundamentales ante un desastre; por lo que se les dio una lista de algunos

que son esenciales en un plan de continuidad, para conocer si el personal de TI del MTSS, tienen asegurados e identificados los recursos críticos de TI; donde el 62 % indica que no existe aseguramiento de los procesos de identificación de los recursos críticos de TI, el 23 % señala que algunas si se cumplen por prioridad y un 15 % dice que ninguno se realiza. (Ver el DS4.3 Recursos críticos de TI)

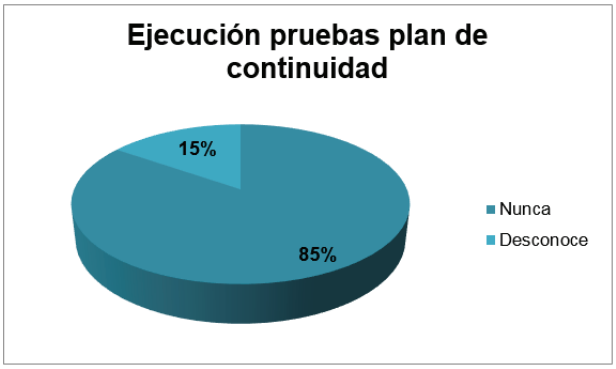
8.18. Anexo 18

¿La ejecución de las pruebas del plan de continuidad de TI se maneja adecuadamente? Ver Tabla #18 y Gráfico #18 a continuación.

Tabla #18 – Discusión de los datos obtenidos de la pregunta #18.					
Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
Nunca	1,00	11	84.62	84.62	84.62
Desconoce	2,00	2	15.38	15.38	100
A veces	3,00	0	0	0	100
Siempre	4,00	0	0	0	100
	Total	13	100,00	100,00	

Cuadro 1. My caption

Gráfico#18 - Discusión de los datos obtenidos de la pregunta#18.



N	Válido	13
	Perdidos	0
Media		1.15
DE		0.36
Mínimo		1
Máximo		4

Se debe conocer en todo plan de continuidad cómo se ejecutan las pruebas del plan de continuidad, al consultar al personal de TI como se lleva a cabo dicho examen, el 85 % de los colaboradores no existe ningún procedimiento, como tal, para el plan de continuidad de TI, el 15 % manifiesta desconocer de si existe o se realizan adecuadamente. (Ver el DS4.5 Pruebas del plan de continuidad de TI)

8.19. Anexo 19

¿Los siguientes puntos son asegurados durante la ejecución de las pruebas del plan de continuidad de TI?

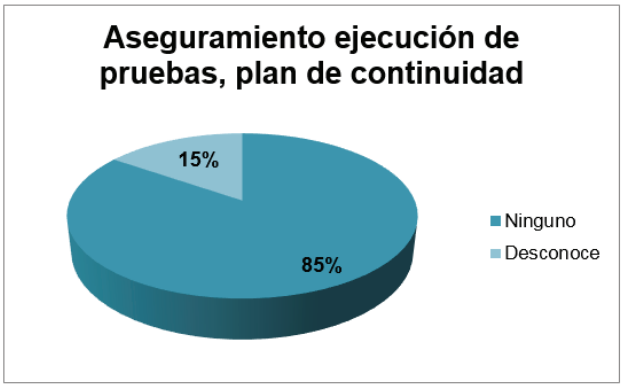
a) Se utiliza un plan de pruebas documentado y reportes de resultados
b) Los sistemas de información pueden ejecutarse de forma satisfactoria.
c) Se atienden los hallazgos acontecidos durante las pruebas
d) Se implementan planes de acción acorde a los resultados.

Ver Tabla #19 y Gráfico #19 a continuación.

Tabla #19 – Discusión de los datos obtenidos de la pregunta #19.

Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
Ninguno	1,00	11	84.62	84.62	84.62
Desconoce	2,00	2	15.38	15.38	100
Algunas	3,00	0	0	0	100
Todas	4,00	0	0	0	100
	Total	70	100,00	100,00	

Gráfico#19 - Discusión de los datos obtenidos de la pregunta#19.



N	Válido	13
	Perdidos	0
Media		1.15
DE		0.36
Mínimo		1
Máximo		4

Es responsabilidad del personal de TI velar por el aseguramiento de la ejecución de pruebas del plan de continuidad, donde existen puntos fundamentales a la hora de analizar si se realiza adecuadamente y de la forma más segura, se les preguntó a los colaboradores cuáles de ellos cumplían y se obtuvo que para el 85 % no hay aseguramiento de los procesos a la hora de ejecutar pruebas al plan de continuidad de TI y un 15 % dice no saber. (Ver el DS4.5 Pruebas del plan de continuidad de TI)

8.20. Anexo 20

¿Cuáles de los siguientes puntos son aplicables durante la ejecución del entrenamiento del plan de continuidad de TI?

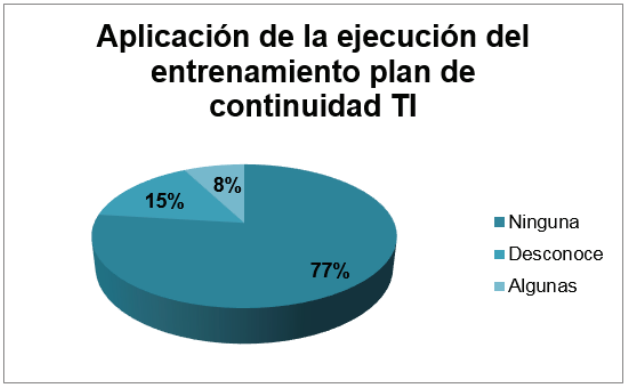
a) Identificación y comunicación de las responsabilidades de los involucrados en la continuidad de los servicios críticos de TI
b) Identificación y comunicación de las funciones dentro del plan de continuidad de TI
c) Identificación de mejoras para el entrenamiento y ejecución del plan de continuidad de TI.

Ver Tabla #20 y Gráfico #20 a continuación.

Tabla #20 – Discusión de los datos obtenidos de la pregunta #20.

Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
Ninguna	1,00	10	76.92	76.92	76.92
Desconoce	2,00	2	15.38	15.38	92.31
Algunas	3,00	1	7.69	7.69	100
Todas	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#20 - Discusión de los datos obtenidos de la pregunta#20.



N	Válido	13
	Perdidos	0
Media		1.31
DE		0.61
Mínimo		1
Máximo		4

Un entrenamiento debe ser planificado, para asegurar que el personal es capacitado en la totalidad de los procesos que va a ejecutar; por lo que se quiso conocer la aplicación de la ejecución del entrenamiento del plan de continuidad de TI, donde se les dio a los colaboradores consultados tres puntos esenciales durante la ejecución del entrenamiento, para conocer si se está realizando de la forma más adecuada en las capacitaciones realizadas al departamento de TI del

MTSS, donde se obtuvo que el 77 % indica que no se utiliza ninguno de los procesos durante la aplicación de la ejecución del entrenamiento plan de continuidad TI, el 15 % desconoce si se realizan y el 8 % afirma que algunas se realizan. (Ver el DS4.2 Planes de Continuidad de TI y el DS4.6 Entrenamiento del plan de continuidad de TI)

8.21. Anexo 21

¿Los siguientes puntos son aplicables durante la reanudación y recuperación de los servicios críticos de TI?

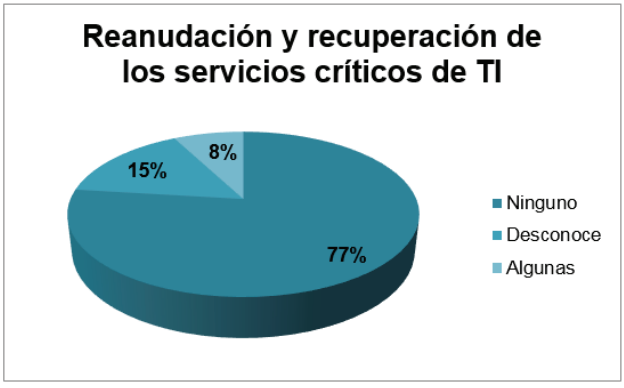
a) Funcionamiento de los sitios de respaldo.
b) Activación de protocolos de reanudación.
c) Procesamiento de los sistemas de información críticos en sitio contingente.
d) Ejecución de protocolos de comunicación asertiva a usuarios y clientes.

Ver Tabla #21 y Gráfico #21 a continuación.

Tabla #21 – Discusión de los datos obtenidos de la pregunta #21.

Etiqueta de Valor	Valor	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
Ninguna	1,00	10	76.92	76.92	76.92
Desconoce	2,00	2	15.38	15.38	92.31
Algunas	3,00	1	7.69	7.69	100
Todas	4,00	0	0	0	100
	Total	13	100,00	100,00	

Gráfico#21 - Discusión de los datos obtenidos de la pregunta#21.



N	Válido	13
	Perdidos	0
Media		1.31
DE		0.61
Mínimo		1
Máximo		4

Se debe tener un proceso definido de reanudación y servicios críticos de TI para todo plan de contingencia, por lo que observó si en el departamento de TI

del MTSS existen y aplican los cuatro puntos esenciales que deben contener, lo que se mostró fue que un 77 % indican que no se realizan los procesos aplicables durante la reanudación y recuperación de los servicios críticos de TI, el 15 % desconoce su existencia y solo una persona indica que se cumplen algunos, el cual representa el 8 % de los resultados. (Ver el DS4.2 Planes de Continuidad de TI y el DS4.8 Recuperación y reanudación de los servicios de TI)

Referencias

CNTEC. (2011, may). *Itil vs cobit.* Descargado de `http://www.cntec.mx/noticias/41/122-itilvscobit.html` pages 3

Contraloria General de la Republica, C. (2007, jun). *Normas técnicas para la gestión y el control de las tecnologías de información.* Descargado de `http://www.ocu.ucr.ac.cr/Leyes/Nuevas%20normas%20de%20TI%20-CGR%20N-2-2007-CO-DFOE.pdf` pages 3, 4

Government of Canada, G. (2014, mar). *A guide to business continuity planning.* Descargado de `http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/bsnss-cntnt-plnnng/index-eng.aspx` pages 2

Institute, I. (2012, dec). *It continuity planning.* Descargado de `http://resources.infosecinstitute.com/it-continuity-planning/` pages 3

Institute, S. (2002). *Introduction to business continuity planning.* Descargado de `https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559` pages 2

IT Governance Institute, I. (2007a). *Cobit 4.1.* Rolling Meadows. pages 3, 5

IT Governance Institute, I. (2007b). *It assurance guide.* Rolling Meadows. pages 3

Ministerio de Trabajo y Seguridad Social, M. (s.f.). *Plan operativo institucional 2015.* Descargado de `https://docs.google.com/viewer?a=v\&pid=sites\&srcid=bXRzcy5nby5jcnxtdHNzfGd4OjZlZTg0MzkwMjhhMTg0NGQ` pages 2

Ministerio de Trabajo y Seguridad Social, M. (2010, nov). *Plan estratégico institucional.* Descargado de `https://docs.google.com/viewer?a=v\&pid=sites\&srcid=bXRzcy5nby5jcnxtdHNzfGd4OjEyZmFjOTFiMzFjYzQwM2E` pages 1

TechTarget. (2009, nov). *Proyectar con cobit e itil el plan de recuperación de desastres.* Descargado de `http://searchdatacenter.techtarget.com/es/consejo/Proyectar-con-COBIT-e-ITIL-el-plan-de-recuperacion-de-desastres` pages 3