ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"DESARROLLO DE UN PLAN DE CONTINUIDAD DE LOS SERVICIOS QUE BRINDA EL CENTRO DE DATOS DE LA UNIVERSIDAD TÉCNICA DE MACHALA, COMBINANDO LAS MEJORES PRÁCTICAS DE ITIL V3, EDICIÓN 2011 Y COBIT V5"

TRABAJO DE TITULACIÓN

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Byron Fabricio Ramírez Carrillo

Freddy Andrés Rojas Vilela

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTO

A Dios, por ser el motor que impulsa mi vida; a mis padres pilar fundamental de mi formación personal y espiritual, a mi esposa por todo su amor, apoyo y tiempo; a mi amigo y compañero en este proyecto por la dosis de calma y conocimientos aplicados durante el desarrollo de este trabajo; a la Universidad Técnica de Machala, por la ayuda brindada desde el inicio hasta el final de este ciclo de estudios, y a todos quienes de una u otra manera, me ayudaron, Gracias Totales.

Byron Ramírez

Primero agradezco a Dios por ser la luz que guía mis pasos. A mi familia por su confianza y apoyo durante el tiempo de estudio. A mi amigo y compañero de tesis por el esfuerzo y dedicación para la culminación del presente trabajo. A la UTMACH por permitirnos realizar el estudio, lo cual devendrá en el mejoramiento de los servicios ofrecidos. A nuestro tutor Jorge Olaya PhD. por brindarnos su oportuna asesoría técnica.

Freddy Rojas

DEDICATORIA

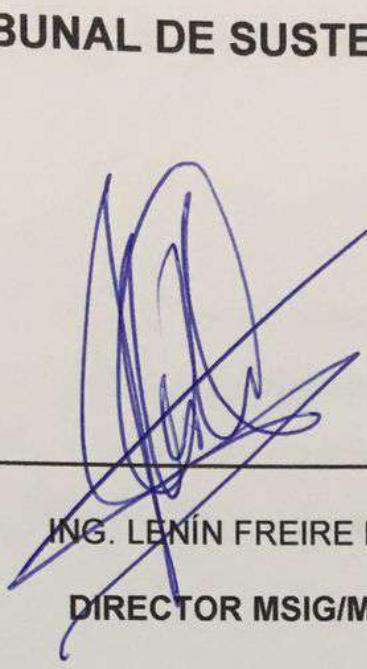
A mi esposa y a mis padres, regalos de mi Dios, por su paciencia y sus consejos llenos de calma y sabiduría, los amo mucho y a ustedes dedico este trabajo.

Byron Ramírez

A Dios por darme la fortaleza y la convicción de continuar siempre el proceso de mejoramiento continuo y a mi familia por estar siempre a mi lado apoyándome y alentándome.

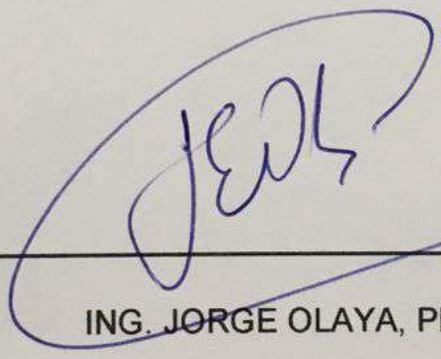
Freddy Rojas

TRIBUNAL DE SUSTENTACIÓN



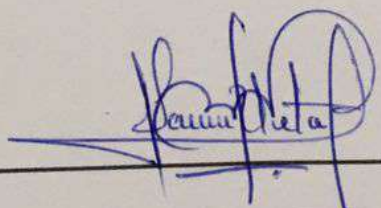
ING. LENÍN FREIRE MGS.

DIRECTOR MSIG/MSIA



ING. JORGE OLAYA, PhD.

DIRECTOR DEL PROYECTO DE GRADUACIÓN

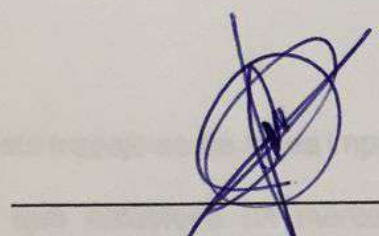


LIC. LAURA URETA, MSIG

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"Declaramos de forma expresa que todo el contenido de esta Tesis de Grado es de nuestra completa autoría y responsabilidad, por lo que damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"



Byron Fabricio Ramírez Carillo

Freddy Andrés Rojas Vilela

RESUMEN

El presente trabajo tuvo como objetivo principal el Diseñar un plan de continuidad de los Servicios que brinda el Centros de Datos de la Universidad Técnica de Machala, combinando las mejores prácticas de ITIL v3, edición 2011 y COBIT v5, además de NIST 800-34 con IT RISK. La utilización de este esquema permitió evaluar de manera adecuada y consistente los eventos de riesgo a los que se encuentran sujetos los servicios que ofrece el Centro de Datos, así como el planteamiento de las medidas necesarias para su mitigación y el levantamiento del plan de continuidad.

Este trabajo es de suma importancia para la Universidad Técnica de Machala, debido a que establece un marco de referencia para garantizar la continuidad de los procesos declarados como críticos, centrándose en la correspondencia de los mismos con los servicios que ofrece el Centros de Datos, lo que contribuye significativamente a generar confianza a todos los que conforman la comunidad universitaria.

En cada uno de los apartados se describe de forma detallada las actividades que conforman el plan de continuidad de los servicios del Centro de Datos de la

Universidad Técnica de Machala, lo que sin duda permite comprender de una mejor manera el presente estudio.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La Universidad Técnica de Machala es una institución de Educación Superior, que se orienta a la docencia, investigación y a la vinculación con la sociedad, formando y perfeccionando profesionales en múltiples áreas de conocimiento, competentes, emprendedores y comprometidos con el desarrollo en sus dimensiones económico, humano, sustentable y científico-tecnológico para mejorar la producción, competitividad y calidad de vida de la población en su área de influencia [1].

En los últimos años uno de los aspectos fundamentales dada la extensión de los procesos que se asientan sobre la plataforma tecnológica, es garantizar la disponibilidad de los mismos, así como proteger la información que se almacena. Entonces se hace indispensable que la Dirección de Tecnologías de la información y comunicación de la Universidad Técnica de Machala cuente con un plan de continuidad de los servicios que ofrece el centro de datos.

Con el plan de continuidad de los servicios, se busca establecer cuáles son los procesos críticos para la institución y su relación con los servicios ofrecidos por el centro de datos, así como su impacto ante una eventual interrupción, además de conocer los eventos de riesgo que posiblemente puedan afectar el normal funcionamiento, identificando amenazas y vulnerabilidades con el fin de detallar las estrategias necesarias que conlleven a cumplir con el objetivo principal del presente estudio.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

La Universidad Técnica de Machala fue creada el 14 de abril de 1969, entre los factores que influyeron se destacan, el auge de la producción bananera en la provincia, situación que influyó en un acelerado crecimiento poblacional el cual vino acompañado de un incremento de la población estudiantil egresada, apta para los estudios universitarios, pero no contaban con las facilidades para acceder a los mismos.

La población universitaria egresada, empezó a integrarse a realizar actividades económicas propias del medio y la comunidad, actividades particulares como el comercio, la producción agrícola, pero en su mayoría primaba la desocupación.

Con los antecedentes mencionados, se promueve la creación de un centro de educación superior, que solucione los problemas técnicos y culturales que existían en aquel entonces.

La conformación de un comité Pro Universidad Técnica, integrado por Rectores y representantes estudiantiles de los Colegios Secundarios existentes en la provincia y los Presidentes de los Municipios Orenses del Consejo Provincial iniciaron la lucha que detonó en enfrentamientos contra la fuerza pública, dirigida por el gobierno de aquel entonces, el cual finalmente dio paso al anhelo de la provincia referente a contar con una institución de educación superior, conformándose así la Universidad Técnica de Machala (UTMACH). [2]

Desde aquel entonces, la UTMACH ha enfrentado dificultades de gestión académica y administrativa, que estancaron su desarrollo, llegando a convertirse en una Universidad con calificación “D”, la cual fue otorgada por el Organismo máximo de evaluación de la educación superior en el año 2012 [3].

A partir de aquel doloroso acontecimiento, que sirvió de impulso para la ejecución de cambios en toda su estructura organizativa, la comunidad universitaria se ha unido en la lucha por demostrar que la provincia puede y debe contar con una institución de educación superior que esté ubicada entre las mejores del país y del mundo.

En el mes de junio del año 2015 la Universidad Técnica de Machala, contrató un acompañamiento para realizar un reajuste en sus procesos, como parte del Plan de Mejora Institucional con la empresa SGS que marcó el inicio del camino hacia la implementación del estándar ISO 9001.

Para el mes de octubre del año 2016, el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES), comunica de manera oficial que tras culminar con el proceso de evaluación del que fue objeto, se ubica en categoría "B", logro que impulsó el proceso de desarrollo de la Alma Mater [4].

1.2 Descripción Del Problema

Actualmente la UTMACH, no dispone de un plan de continuidad de los servicios del Centro de Datos, que permita reaccionar, tomar decisiones y medidas en caso de que determinada amenaza se materialice. De acuerdo a varios estudios realizados en base al tema de continuidad podemos decir que una de cada cinco organizaciones sufrirá un incendio, inundación o tormenta, falla en la energía eléctrica, terrorismo, sin dejar de lado los desastres de equipos de cómputo (hardware y software), y debido a la obligatoriedad de mantener operativo ininterrumpidamente el Centro de Datos ya que es el sitio donde se albergan todos los equipos y componentes que brindan los servicios de la

UTMACH, o cuando menos reducir al mínimo el tiempo de caída ante una catástrofe, surge la necesidad de contar con un marco de referencia para gestionar la continuidad de los servicios en la Institución.

Desde el establecimiento del Centro de Datos de la Universidad Técnica de Machala en el año 2010, se han suscitado los siguientes incidentes:

- Fallas del suministro eléctrico, llegando a estar hasta 2 días fuera de línea.

- Intermitencia con el Servicio de Internet contratado a un proveedor único, ocasionando problemas en el correcto desenvolvimiento de los procesos internos, hasta por 1 día.

- Fallas de Hardware en la parte activa de la red Institucional sin equipos de reposición, causando la no disponibilidad de todos los servicios del Centro de Datos hasta la ejecución de los procesos de garantía.

- Fallas en Servidores y demora en el restablecimiento del servicio, al no contar con una opción de replicación, teniendo que instalarlo desde cero y recurrir a los respaldos.

- Ataques de Denegación de Servicios (DDos), a los Servidores de Aplicaciones, provocando lentitud en el acceso a los servicios, con tiempos hasta de 1 hora de no acceso según la naturaleza del ataque.

- Es evidente entonces la necesidad de poseer un plan de continuidad para los servicios que brinda el centro de datos de la UTMACH, ya que cualquier amenaza que se ha materializado hasta el momento o que pudiera llegar a suceder, repercutirá gravemente en la consecución de los objetivos de la Institución.

1.3 Solución Propuesta

El desarrollo de un plan de continuidad de los servicios ofrecidos por el Centro de Datos basado en la combinación de las mejores prácticas de: ITIL v3, edición 2011 y COBIT v5, permitirá a la UTMACH, identificar la criticidad de sus servicios, establecer planes de acción, planes de gestión de riesgos, definir métricas, capacitar al personal, entre otros, en pro de mitigar los riesgos y reducir el impacto de la no disponibilidad de los servicios que residen en el Centro de Datos.

Para la consecución de la solución propuesta, se involucrará de manera activa a las Autoridades de la Institución en lo referente a la concientización,

participación y mantenimiento del Plan continuidad de Servicios, a través de un enfoque de trabajo participativo y un plan de capacitación; así mismo se seleccionará a las personas adecuadas y se realizarán esfuerzos en identificar los recursos requeridos tales como: Infraestructura, servicios, suministros básicos, recursos tecnológicos y no tecnológicos, para que sean partícipes del desarrollo del Plan de Continuidad de Servicios.

La definición de contingencia y el concepto de escenarios nos permitirán resolver dos problemas fundamentales:

- Lograr una solución de continuidad que garantice un nivel de recuperación determinado, independientemente de los eventos que puedan presentarse.
- Brindar una guía clara y concreta referente a escenarios de prueba y activación del Plan.

.Además, los beneficios que obtendrá la UTMACH al contar con un plan de continuidad de los servicios ofrecidos por el Centro de Datos basado en la combinación de las mejores prácticas de ITIL v3, edición 2011 y COBIT v5, serán:

- Operatividad ininterrumpida de los servicios del Centro de Datos.

- Contar con medidas preventivas, que permitan mitigar situaciones de riesgo, donde se encuentren involucrados los servicios ofrecidos por el Centro de Datos.

- Lograr una detección oportuna de cualquier situación que pueda colocar al Centro de Datos en una situación de contingencia.

- Contar con planes de acción que permitan tomar medidas oportunas al personal técnico que desempeña sus servicios en el Centro de Datos.

- Tener la Capacidad de recuperar el nivel operativo mínimo requerido en un período de tiempo definido en conjunto con las autoridades de la Institución.

- Proyectar una imagen de preparación y seguridad ante situaciones imprevisibles.

- Planificar la interrupción puntual de ciertos servicios de ser necesario, ya con el conocimiento de cómo debe responder la Institución.

1.4 Objetivo General

Diseñar un Plan de Continuidad de los Servicios que brinda el Centro de Datos de la UTMACH, combinando las mejores prácticas de ITIL v3, edición 2011 y Cobit v5.

1.5 Objetivos Específicos

- Establecer la situación Actual del Centro de Datos de la UTMACH.

- Levantar el catálogo de los servicios que brinda el Centro de Datos de la UTMACH, mismo que servirá como insumo para el diseño del Plan de Continuidad de los Servicios.

- Combinar los marcos de referencia ITL V3 y COBIT 5 para diseñar el plan de continuidad de los servicios.

- Definir la hoja de ruta y el portafolio de proyectos de Tecnologías de la Información y Comunicación (TICS), que se deriven del Plan de Continuidad de los Servicios.

- Preparar a largo plazo a la UTMACH en lo referente a las acciones necesarias que le permitan mantener la disponibilidad de sus servicios críticos ante la ocurrencia de interrupciones provocadas por fenómenos naturales, personas o la falla de los equipos del Centro de Datos.

- Minimizar a través de una gestión de riesgos y un análisis de impacto al negocio los efectos de las interrupciones que afecten a los servicios críticos.

- Involucrar en el corto, mediano y largo plazo a las autoridades de la UTMACH en la revisión y mantenimiento, asignación de recursos, personas y la validación de los servicios críticos del Centro de Datos que permitirán el diseño del Plan de Continuidad de servicios.

1.6 Metodología

El tipo de metodología de investigación a utilizarse en el presente estudio corresponde al tipo exploratorio debido a que se busca diseñar un Plan de Continuidad de los Servicios que ofrece el Centro de Datos de la UTMACH, a través de marcos de referencia (Frameworks), de Tecnologías de la Información y Comunicación previamente establecidos.

CAPÍTULO 2

MARCO TEÓRICO

El presente capítulo tiene por objetivo describir cada uno de los estándares y Marcos de Referencia de Tecnologías de la Información y Comunicación, que se orientan hacia las mejores prácticas en cada uno de sus ámbitos y que servirán de insumo para el Desarrollo de un plan de continuidad de los servicios que brinda el Centro de Datos de la Universidad Técnica de Machala.

2.1 Plan De Continuidad De Los Servicios

El Plan de Continuidad de los Servicios de Tecnologías de la Información y Comunicación (TIC), se encarga de prevenir y proteger a la empresa de los efectos y el impacto que se pudieran presentar ante una interrupción de los

servicios de TIC, los cuales pueden ser ocasionados por una falla técnica, por causas naturales o que pueden ser provocados voluntaria o involuntariamente por una persona.

La Gestión de la Continuidad del Servicio (ITSCM) debe considerar y combinar los siguientes procedimientos:

- **Procedimientos proactivos:** Aquellos que buscan impedir o minimizar las consecuencias de una grave interrupción de los servicios.

- **Procedimientos reactivos:** Aquellos cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable), una vez que ocurre un desastre.

La administración de la continuidad de los servicios de TIC requiere de una labor de evangelización en toda la organización [5] y debe formar parte del Plan de Continuidad del negocio, ya que cumple con los parámetros siguientes:

- Difícil de justificar y costosa.

- Beneficios perceptibles a largo plazo.
- Sólo se afectan servicios de TIC que son intangibles pero pueden paralizar a toda la organización.

- No pueden ser aceptados con resignación como en el caso de los desastres naturales.

Con los parámetros mencionados, un Plan de continuidad de los servicios de TIC resulta extremadamente beneficioso al momento de enfrentar escenarios de contingencia.

El ciclo de vida sobre el que se fundamenta la administración del Plan de Continuidad de los servicios de TIC y el plan de continuidad del negocio se resume a continuación.

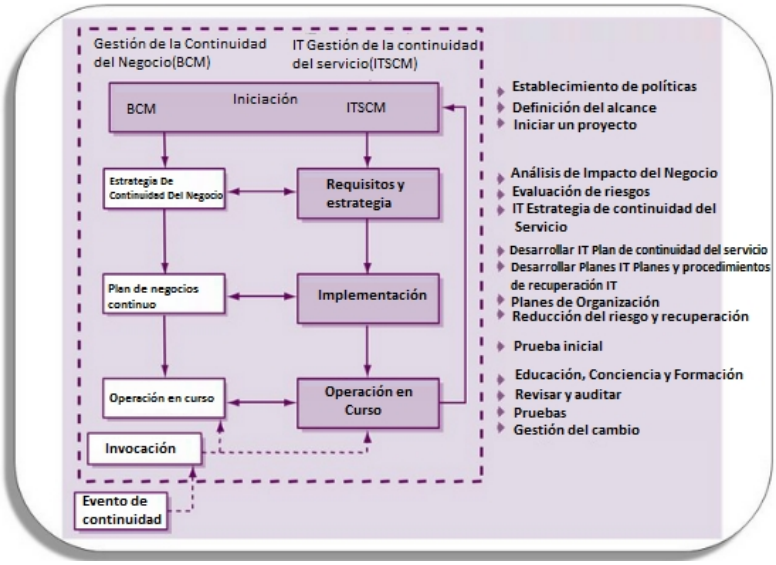


Figura 2.1 Ciclo de Vida de ITSCM (Manejo de la continuidad del servicio de TI). Fuente: ITIL v3, edición 2011

.Para el presente estudio, los insumos para el Diseño del Plan de Continuidad de los servicios de TIC son:

- Definición del proyecto.
- Análisis del impacto en el negocio (BIA)
- Plan de Riesgos.

2.2 Plan De Recuperación De Desastres

Se define a un desastre como un evento que imposibilita la continuación de las funciones normales, por lo que, bajo este contexto, un Plan de Recuperación de Desastres (DRP), describe cómo enfrenta una organización los posibles desastres que puedan presentarse y se compone de todas las precauciones tomadas para que los efectos de un desastre se reduzcan al mínimo y la organización sea capaz de mantener o reanudar rápidamente sus funciones o actividades de misión crítica.

Debido a que los sistemas empresariales actuales tienden a ser grandes y cada vez más complejos, es necesario considerar algunas variables de entre las cuales se pueden mencionar:

- Tipo de negocio.
- Procesos involucrados

- Niveles de seguridad

Ya que la interrupción de los servicios o la pérdida de datos pueden generar consecuencias financieras graves, ya sean de manera directa o a través de la pérdida de confianza y credibilidad por parte del cliente. El proceso para el Plan de Recuperación de Desastres se esquematiza de la siguiente manera:

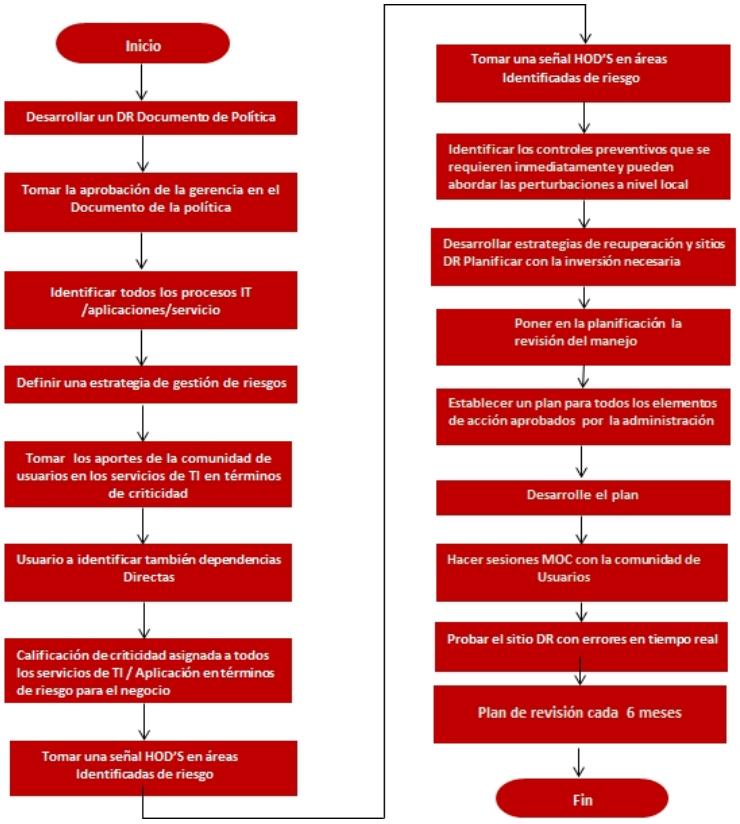


Figura 2.2 Proceso del Plan de Recuperación de desastres. Fuente: SP 800-34 del NIST

Para cumplir con las actividades del esquema del Plan de Recuperación de Desastres, es necesario considerar:

- Apoyo de la Alta Gerencia a fin de lograr alcanzar los objetivos del Plan.

- Organizar y reunir la información clave para diseñar el Plan.
- Contar con Estándares que permitan diseñar el Plan.
- Cotejar los resultados del Plan con los líderes de las unidades de Negocio a fin de alinearlos hacia objetivos comunes.
- Identificar la capacidad de respuesta de los proveedores externos en función de los Acuerdos de Nivel de Servicio establecidos.
- Identificar los tiempos de respuesta del personal del departamento de TIC ante disrupciones de la infraestructura crítica de TI y determinar su nivel de conocimiento y preparación para uso y operación de sistemas críticos en casos de emergencia.

Para el presente estudio, los insumos para el Diseño del Plan de Continuidad de los servicios de TIC en relación al Plan de Recuperación de Desastres son:

- Identificar los procesos y aplicaciones de TI

- Identificar las dependencias de TI de las diferentes unidades de Negocio de la Universidad Técnica de Machala.

- Identificar Riesgos.

- Análisis del Impacto del Negocio (BIA).

2.3 Marcos De Referencia

2.3.1 COBIT V5

COBIT 5 (a Business Framework for the Governance and Management of Enterprise IT), provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos [6].

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas.

Figura 2.3 Principios de COBIT. Fuente: COBIT v5 Framework

Catalizadores COBIT 5 [7]

- **Principios, políticas y marcos de referencia:** Medio por el cual se traduce el comportamiento deseado en guías prácticas para la gestión del día a día.

- **Procesos:** Describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI.

- **Estructuras organizativas:** Entidades de toma de decisiones clave en una organización.

- **Cultura, ética y comportamiento:** Los individuos de una organización son considerados como factor de éxito en las actividades de gobierno y gestión.

- **Información:** Incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.

- **Servicios, infraestructuras y aplicaciones:** Incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.

- **Personas, habilidades y competencias:** Están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas.

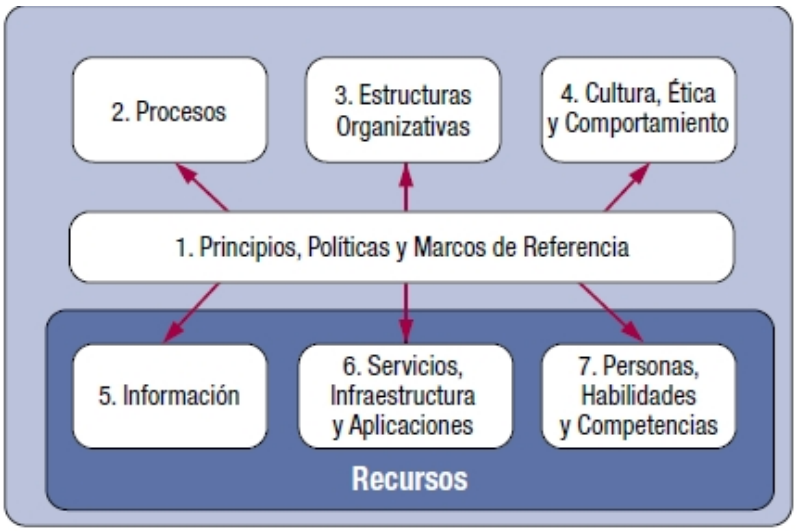


Figura 2.4 Catalizadores Corporativos COBIT 5. Fuente: COBIT v5 Framework

COBIT 5 incluye un modelo de referencia de 37 procesos que define y describe en detalle varios procesos de gobierno y de gestión que representa todos los procesos de la organización relacionados con TIC

El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible, ya que cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

COBIT 5, incorpora de un modelo operacional y un lenguaje común para todas las partes de la organización involucradas en las actividades de

TI, convirtiéndolo en uno de los pasos más importantes y críticos hacia el buen gobierno corporativo.

Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

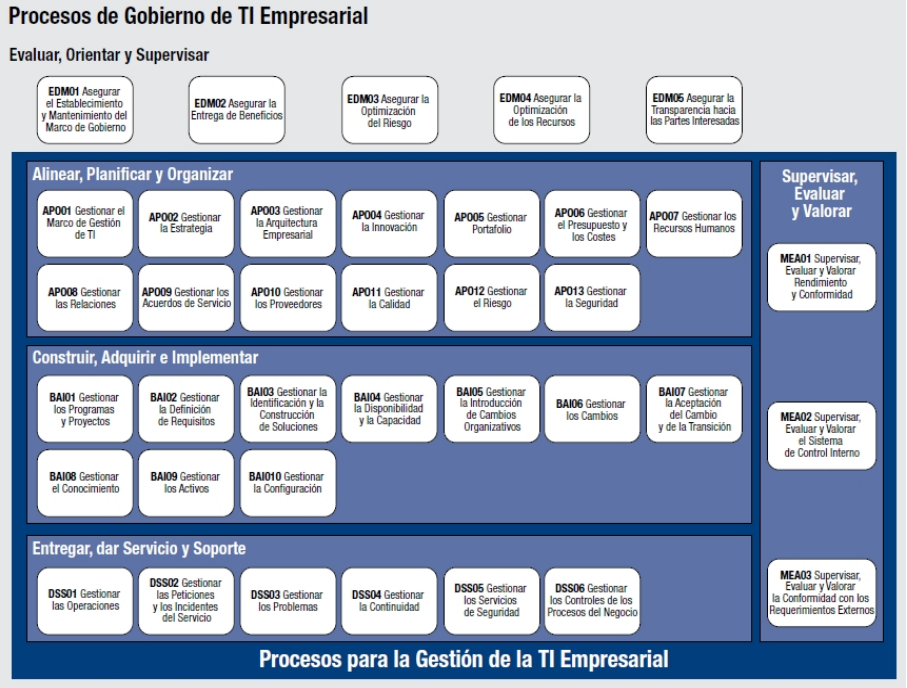


Figura 2.5 Proceso de Gobierno de TI Empresarial. Fuente: COBIT v5 Framework

Matriz RACI

RACI es una herramienta utilizada para la asignación de responsabilidades dentro de un determinado proceso, proyecto, servicio o incluso dentro de un departamento o función.

Significado de la matriz:

- R: Responsable para la realización de la actividad (ejecutor).

- A: Autoridad, es quien debe responder por la actividad. Conforme a lo sugerido por el framework COBIT, una actividad debe contar con una sola autoridad.

- C: Consultado, son quienes participan de una decisión o actividad que se realiza en un determinado momento.

- I: Informado, es quien debe recibir la información de que una actividad se llevó a cabo.

Para el presente estudio, se utilizarán como insumos:

- Matriz RACI
- Gestionar la continuidad (DSS04).

2.3.2 ITIL V3, Edición 2011

ITIL (Information Technology Infraestructure Library), nace en la década de 1980 debido al encargo que recibió la Agencia Central de Telecomunicaciones del Reino Unido, referente a la creación de una metodología estándar que permita garantizar una entrega eficaz y

eficiente de los servicios de TIC, la cual deba ser independiente de los proveedores internos o externos. El resultado del mismo fue la publicación de la Biblioteca de la Infraestructura de Tecnología de Información (ITIL), que está formada por una serie de mejores prácticas provistas por todos los suministradores de servicios de TI.

ITIL especifica un método sistemático que garantiza la calidad de los servicios de TI, ofrece una descripción detallada de los procesos más importantes de TIC dentro de una organización, incluyendo listas de verificación para tareas, procedimientos y responsabilidades que pueden servir como base para adaptarse a las necesidades concretas de cada organización.

ITIL define los siguientes conceptos [8]:

- **Servicio:** Medio por el cual se entrega valor a un cliente, facilitando el resultado que el cliente pretende conseguir sin asumir costos o riesgos específicos.

- **Gestión del servicio:** Conjunto de capacidades organizativas especializadas cuyo fin es generar valor para los clientes en forma de servicios.

- **Valor:** Desde el punto de vista del cliente, el valor consta de dos componentes: Funcionalidad y garantía. La funcionalidad es lo que el cliente recibe, mientras que la calidad reside en cómo se proporciona.

- **Sistema:** Grupo de componentes interrelacionados o interdependientes que forman un conjunto unificado y que funcionan juntos para conseguir un objetivo común.

- **Función:** Subdivisión de una organización que está especializada en realizar un tipo concreto de trabajo y tiene la responsabilidad de obtener resultados concretos.

- **Proceso:** Conjunto estructurado de actividades diseñado para cumplir un objetivo en concreto.

Figura 2.6 Valor del Servicio. Fuente: ITIL v3, edición 2011

Ciclo de vida del servicio

- **Estrategia del servicio**
  - Cubre toda la planificación estratégica de los servicios de TI.
  - Incluye la planificación financiera y la definición de valor para el cliente

- **Diseño del servicio**
  - Cubre el diseño y desarrollo de los servicios, gestión del servicio y los procesos relacionados.
  - Inicia cuando un cliente solicita un nuevo servicio o un cambio a uno ya existente.
  - El diseño del servicio incluye:
    - Escalabilidad
    - Procesos de negocio y unidades de negocio
    - Servicios de TI y funcionalidad del negocio
    - SLR, SLA y OLA
    - Componentes tecnológicos
    - Soporte externo del servicio
    - Métricas
    - Niveles de seguridad

- **Transición del servicio**
  - Utiliza procesos, sistemas y funciones.
  - Construye, prueba y despliega los servicios antes de ponerlos en producción.
  - Cierra las brechas entre el Diseño del Servicio y la Operación del Servicio.
- **Operación del servicio**
  - Lugar donde el servicio se encuentra disponible de primera mano para el cliente.
  - Cuenta con sus propios procesos y funciones para proveer el servicio al nivel acordado.
- **Mejora continua del servicio**
  - Puede ser aplicada en todas las fases del ciclo de vida del servicio.
  - Utiliza métricas para establecer fortalezas y debilidades.
  - Es continuo y concurrente.

- Se encuentra focalizado en proveer mejoras en todas las fases.

Figura 2.7 Esquema del ciclo de vida del Servicio. Fuente: ITIL v3, edición 2011

Figura 2.8 Procesos y funciones de cada una de las etapas del ciclo de vida del servicio. Fuente: ITIL v3, edición 2011

Para el presente estudio se utilizarán como insumos:

- Gestión de la Continuidad

2.3.3 IT RISK [9]

Marco de referencia desarrollado por ISACA y lanzado al mercado el 8/12/2009, que ayuda a la gestión eficaz de los riegos Corporativos asociados a las TICS, basado en un conjunto de principios, guías y directrices corporativas que se ajustan a estos principios.

Fundada en 1969, ISACA es una asociación sin fines de lucro integrada por 86.000 profesionales de TICS, que desarrolló, y actualiza continuamente los marcos de referencia: COBIT, Val IT y Risk IT, que ayudan a los profesionales y a las empresas líderes de TI a satisfacer sus responsabilidades de administración de TICS y generar valor a sus organizaciones.

Tabla 1 Requerimientos funcionales y no funcionales IT RISK. Fuente: RISK IT Framework

Requerimientos funcionales (RISKIT)	Requerimientos no funcionales (RISKIT)
Guía práctica independiente; Extiende COBIT y Val IT	Modelo de proceso continuo, apoyado por modelos de madurez y herramientas prácticas
Enlace con enfoques de gestión del riesgo empresarial	Incluye un marco y guía de buenas prácticas
Utilizar un enfoque de rendimiento de procesos de negocio de extremo a extremo	
Integrar silos de gestión de riesgos tecnológicos	

Objetivos de RISKIT

- Proporciona orientación para ayudar a los ejecutivos y la administración a formular las preguntas clave, tomar decisiones ajustadas al riesgo y guiar a sus organizaciones para que el riesgo se gestione de manera efectiva.

- Ahorrar tiempo, costo y esfuerzo en la implementación de herramientas innecesarias para hacer frente a los riesgos del negocio.

- Integrar la gestión de los riesgos de negocio relacionados con TICS en la gestión global del riesgo corporativo.

- Ayudar a los altos ejecutivos de la organización a comprender el apetito de riesgo y la tolerancia al riesgo.

Principios de RISKIT

- Alinear los riesgos corporativos con los riesgos asociados a las TICS.

- Equilibrar los costos y beneficios de la administración del riesgo.

- Promover una comunicación justa y abierta referente al riesgo de las TICS.

- Entender que el riesgo se trata de un proceso continuo y forma parte importante de las actividades diarias.

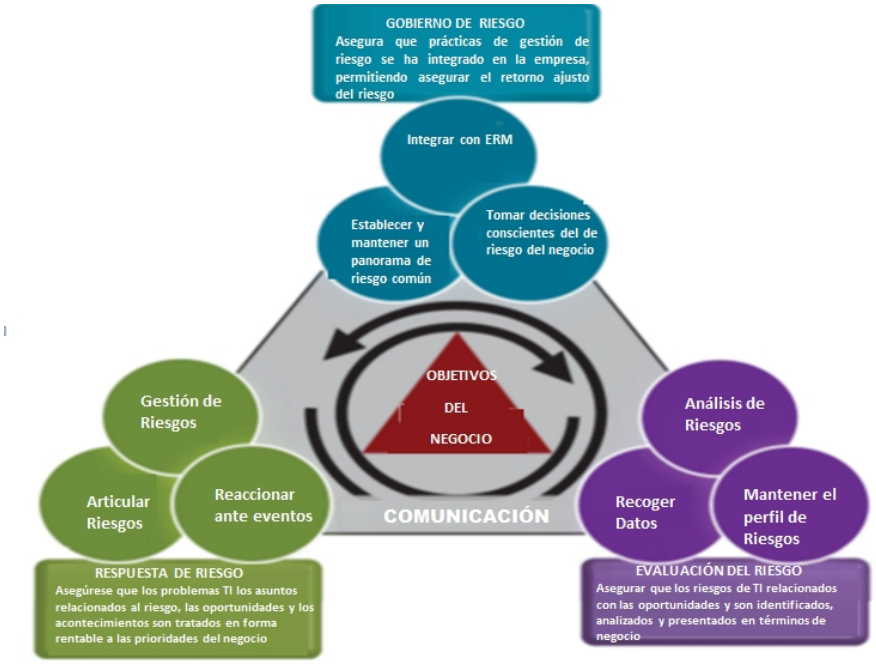


Figura 2.9 Dominios de IT RISK. Fuente: RISK IT Framework

Riesgo de TI

- Es un riesgo de negocio asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de las TICS en la organización.

- Consiste en eventos relacionados con las TICS que potencialmente pueden impactar al negocio.
- Influye en frecuencia y magnitud, crea retos para el cumplimiento de metas y objetivos estratégicos, así como la incertidumbre en la búsqueda de oportunidades.

Figura 2.10 Riesgos Organizacionales relacionados con TI. Fuente: RISK IT Framework

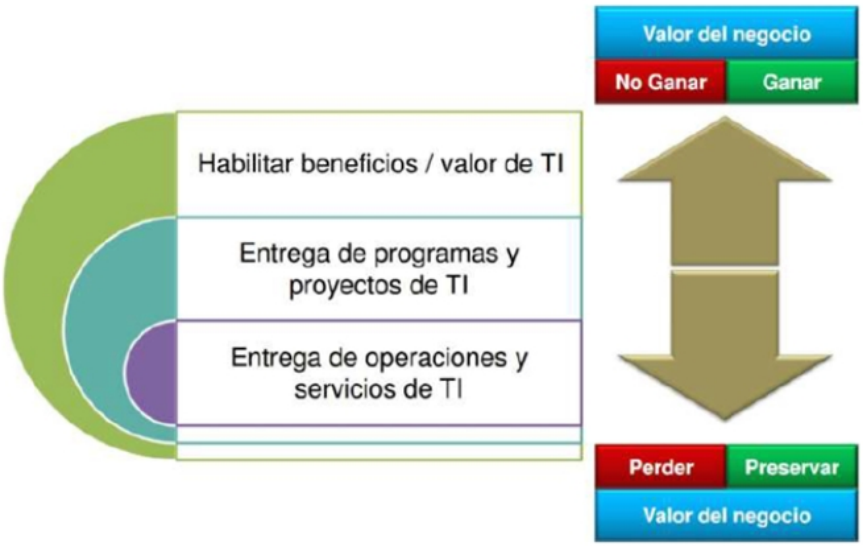


Figura 2.11 Clasificación de los riesgos de TI. Fuente: RISK IT Framework

Gobierno de Riesgos (RISKIT)

Consiste en asegurar que la Organización cuenta con prácticas de Riesgo de las TICS que aseguran un retorno de la administración del Riesgo. Se divide en tres categorías:

RG1: Establecer y mantener una visión común del riesgo.

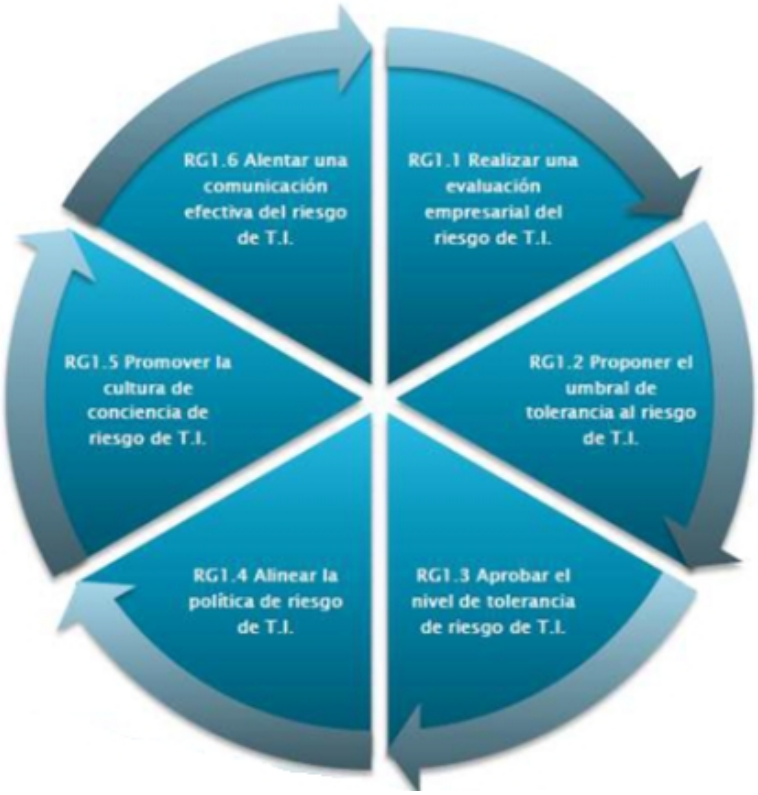


Figura 2.12 RG1. Fuente: RISK IT Framework

RG2: Integrar la gestión de riesgos de las TICS con la gestión de riesgos corporativos.

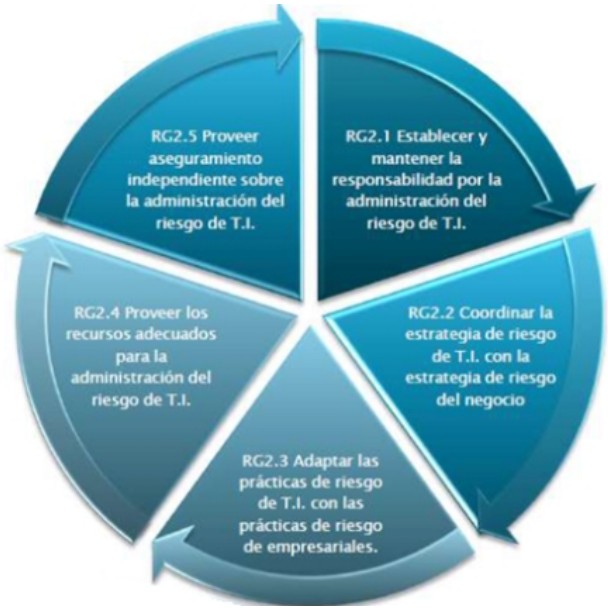


Figura 2.13 RG2. Fuente: RISK IT Framework

RG3: Tomar decisiones conscientes referentes a los riegos de las TICS.

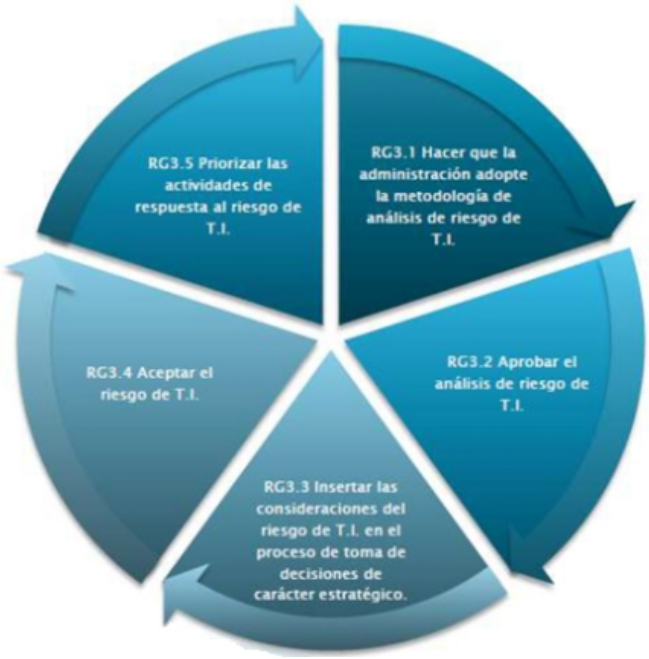


Figura 2.14 RG3. Fuente: RISK IT Framework

Fundamentos de la respuesta de Riesgos (RISKIT)

Consiste en asegurar que las TICS relacionadas con asuntos de riesgos, oportunidades y los eventos se traten de manera rentable y sean alineadas a las prioridades del negocio. Según RISKIT, se divide en tres partes:

RR1: Articular el riesgo

Figura 2.15 RR1. Fuente: RISK IT Framework

RR2: Gestionar el riesgo

Figura 2.16 RR2. Fuente: RISK IT Framework

RR3: Gestionar el riesgo

Figura 2.17 RR3. Fuente: RISK IT Framework

Para el presente estudio se utilizará como insumo:

- Elaboración de la matriz de riegos.
- Planes de acción para mitigar, asumir o transferir los riesgos

2.3.4 NIST 800 – 34 [10]

Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology), proporciona instrucciones, recomendaciones y consideraciones para la planificación de contingencia de sistemas de información. La planificación de contingencia se refiere a medidas provisionales para recuperar los servicios de los sistemas de información después de una interrupción. Las medidas provisionales pueden incluir la reubicación de los sistemas de información y las operaciones del negocio en un sitio alterno, la recuperación de funciones de los sistemas de información utilizando equipos alternativos o el desempeño de funciones de los sistemas de información mediante métodos manuales. Esta guía aborda recomendaciones de planificación de contingencia específicas para tres tipos de plataformas y proporciona estrategias y técnicas comunes a todos los sistemas.

Los sistemas en mención son:

- Sistemas cliente – servidor.

- Sistemas de Telecomunicaciones.
- Sistemas Mainframe.

NIST 800-34, establece el siguiente proceso para el desarrollo del plan de contingencia de los sistemas de información:

1	2	3	4	5	6	7
Desarrollar las Políticas del Plan de Contingencia	**Realizar un Análisis de Impacto de Negocio (BIA)**	**Identificar Controles Preventivos**	**Crear las estrategias de Contingencia**	**Desarrollar el Plan de Contingencia**	**Planificar, ejecutar probar y capacitar**	**Mantenimiento del Plan de Contingencia**
Identificar requerimientos de orden legal y regulatorio	Determinar los procesos críticos de negocio y su estrategia de recuperación	Identificar controles	Respaldo y Recuperación	Documento referente a la estrategia de recuperación	Planificar y probar	Revisar y actualizar el plan
Desarrollar las políticas y estatutos del plan de contingencia de TIC	Identificar los impactos y estimación de tiempos de caída (downtime)	Implementar controles	Considerar Confidencialidad, disponibilidad e integridad (ISO 27002)		Entrenar al personal	Coordinar con organizaciones internas y externas
Considerar Confidencialidad, disponibilidad e integridad (ISO 27002)	Identificar los recursos necesarios	Mantener los controles	Identificar roles y responsabilidades			Documentar cambios
Publicar Políticas	Identificar las prioridades de recuperación para cada sistema		Direccionar al sitio alterno			
			Considerar costos e identificar equipos			
			Integrar la arquitectura de los sistemas			

Figura 2.18 Proceso para desarrollar el plan de contingencia de los sistemas de información establecido por NIST 800-34

Para el desarrollo del plan de contingencia, NIST 800-34 estipula que deberán definirse procedimientos que deberán seguirse ante un evento en el cual el personal no pueda ser contactado. Dichos procedimientos deberán ser claros y específicos dentro del plan de contingencia, y deberán mantener una estructura de árbol, como se muestra en la siguiente gráfica:

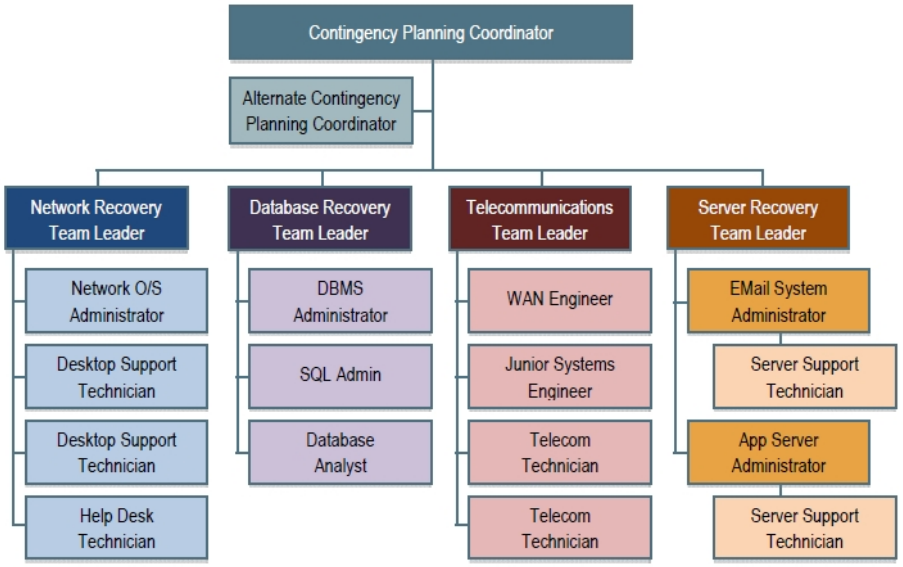


Figura 2.19 Estructura de árbol para la definición del plan de contingencia

Para el presente estudio se utilizarán como insumos:

- BIA.
- Matriz de Roles y responsabilidades.
- Direccionar los servicios críticos al sitio alterno.
- Identificar los recursos necesarios.
- Prioridades de recuperación.
- Estimación de tiempos de recuperación y caída (Down time).

2.4 Seguridad De La Información

Conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que

proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardarla y protegerla buscando mantener sus características principales [11]:

Confidencialidad: Garantizar que la información es accesible únicamente a personas autorizadas.

Integridad: Salvaguardar la exactitud y totalidad de la información, así como también los métodos de procesamiento y transmisión.

Disponibilidad: Garantizar que los usuarios autorizados tienen acceso a la información y a los recursos relacionados toda vez que lo requieran [12].

Figura 2.18 Historia de la ISO/EC 27001. Fuente: ISO/EC 27000

"Cualquiera que sea la forma que tome la información, o el medio por el cual sea compartida o almacenada, ésta siempre debe estar protegida apropiadamente" ISO/IEC 27002:2005

Clasificación del estándar ISO /IEC 27000 [13]

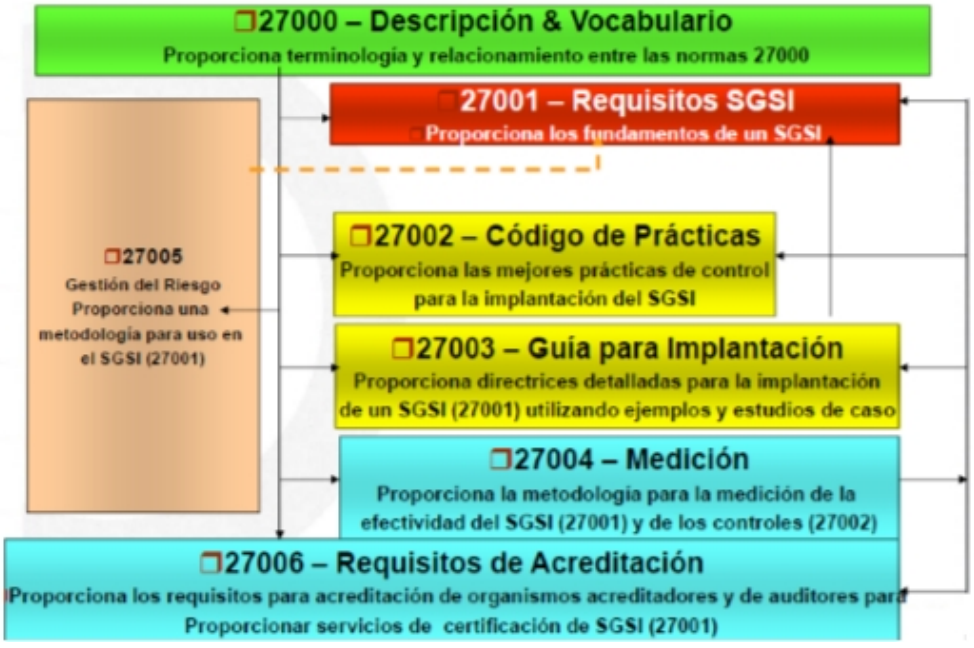


Figura 2.19 Clasificación del estándar ISO /IEC 27000. Fuente: ISO/EC 27000

Para el presente estudio se utilizará como insumo el Código de Prácticas 27002 Versión 2013, dominio: Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio.

2.5 Infraestructura Del Centro De Datos

Un centro de datos o un cuarto de telecomunicaciones deberá contar con una infraestructura adecuada que contemple:

- **Piso Falso:** Formado por capas modulares y removibles que se encuentra sobre el nivel del firme terminado. Su principal función es la de crear un espacio para pasar y ocultar las instalaciones eléctricas, voz, datos y crear una cámara para la distribución eficiente del aire acondicionado.

- **Distribución del cableado:** La normativa TIA-942, recomienda que el diagrama de distribución del cableado en un Centro de Datos tenga al menos las siguientes áreas funcionales:

    - Cuartos de entrada donde se instalen los equipos de Telefonía

    - Área de distribución principal que servirá como punto centralizado de conexión cruzada para el sistema de cableado estructurado

- Áreas de distribución horizontal desde donde se realizará el reparto para el cableado de los equipos.

- Áreas de distribución de zonas para el cableado estructurado de los equipos que se ubicarán a ras de suelo.

- Áreas de distribución de los equipos donde se albergarán los gabinetes y racks

- **Sistema de energía:** Dentro de la infraestructura del Centro de Datos, es necesario contar con un esquema redundante de energía y disponer de al menos dos alimentadores y UPS que alimenten circuitos múltiples para los equipos informáticos

- **Control de acceso:** Sistemas que permitan controlar la asistencia de personal no autorizado al Centro de Datos. Los sistemas de control de acceso deberán contar como mínimo con los siguientes componentes:

- **Software:** Programa para configuración de acceso y preparación de reportes.

- **Controladoras:** Tarjetas electrónicas que manejan el sistema físico y que proporciona la información histórica de los accesos.

- **Lectoras:** Componentes de interfaz con el usuario las cuales pueden ser: PIN, tarjetas de proximidad, códigos de barras, sistemas biométricos, entre otros.

- **Cerraduras:** Accesorios que físicamente controlan los accesos de las puertas, y que pueden ser: Sensores, estaciones manuales de puertas, botones de apertura y alarmas.

- **Seguridad:** Componentes y herramientas que deben contemplar:
    - Cerraduras electromagnéticas.
    - Torniquetes.
    - Cámaras de seguridad.
    - Detectores de movimiento.
    - Tarjetas de identificación.

Figura 2.22 Centro de datos que cumple con la Norma TIA-942. Fuente: TIA-942

De tal manera que garantice que los equipos se encuentran en perfectas condiciones ambientales para su operación y sea posible garantizar su correcto desempeño y funcionamiento.

El presente estudio describe la infraestructura mínima que debe ser considerada para un Centro de Cómputo, actualmente la Universidad Técnica de Machala cuenta con su Centro de Cómputo, por lo que no se enfocará en el diseño del mismo.

2.6 Centro De Datos Alterno

Un centro de procesamiento de datos alterno tiene como objetivo prestar aquellos servicios de tecnología de información que sean críticos para las operaciones del negocio, ante eventos que afecten la disponibilidad del centro de procesamiento de datos principal.

Un centro de procesamiento de datos alterno no necesariamente debe abarcar todos los servicios que presta el centro de procesamiento de datos principal, ni es requerido que cuente con las mismas características del principal, sin embargo, existen unas consideraciones mínimas que deben ser tomadas en cuenta.

Clasificación de los Centros de Datos Alternos

- **Cold Site:** Corresponde al nivel de inversión más baja que puede realizar una organización que requiere la implementación de un centro alterno, sin embargo, los tiempos de recuperación son mucho más lentos, debido a que no se encuentra con la preparación necesaria para dar continuidad inmediata a los servicios.

- **Hot Site:** Corresponde al nivel de inversión más alto, debido a que se cuenta con la plataforma duplicada y con la información casi en tiempo

real, de tal manera que ante la pérdida del centro principal, inmediatamente este pueda entrar en funcionamiento.

- **Warm Site:** Intermedio entre el Cold Site y el Warm Site, contempla los equipos y los medios de respaldo con la información a ser recuperada, sin embargo, de llegar a ocurrir un evento que ocasione la pérdida del centro principal, es altamente probable que se pierda al menos un día de información.

Según la norma TIA 942, los centros de cómputo se clasifican en [14]:

- **Tier I: Centro de Datos básico:** Puede ser susceptible a interrupciones tanto planeadas como no planeadas. Cuenta con sistemas de aire acondicionado y distribución de energía; pero puede o no tener, UPS o generador eléctrico; si los posee pueden no tener redundancia y existir varios puntos únicos de falla. La carga máxima de los sistemas en situaciones críticas es del 100%.Para poder clasificar un centro de datos como Tier I, la tasa de disponibilidad máxima del centro de datos debe ser de 99.671% del tiempo.

- **Tier II: Centro de datos con componentes redundantes:** Pueden ser menos susceptibles a interrupciones, tanto planeadas como las no planeadas.

Estos centros de datos cuentan con piso falso, UPS y generadores eléctricos, pero están conectados a una sola línea de distribución eléctrica. Su diseño es lo necesario más uno(N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura. La carga máxima de los sistemas en situaciones críticas es del 100%. El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura puede causar una interrupción del procesamiento.

Para poder clasificar un centro de datos como Tier II, la tasa de disponibilidad máxima del centro de datos debe ser de 99.749% del tiempo.

- **Tier III: Centro de Datos con mantenimiento concurrente:** Las capacidades de un centro de datos de este tipo permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación ya que incluyen mantenimiento preventivo y programado, reparaciones o reemplazo de componentes, agregar o eliminar elementos y realizar pruebas de componentes o sistemas

- **Tier IV: Centro de Datos tolerante a fallas:** Permite proveer la capacidad para realizar cualquier actividad planeada sin interrupciones

en las cargas críticas, además la funcionalidad tolerante a fallas le permite a la infraestructura continuar operando aun ante un evento crítico no planeado para lo cual se requiere de dos líneas de distribución eléctrica simultáneamente activas, lo que significa al menos dos sistemas de UPS independientes y cada sistema con un nivel de redundancia N+1.

La carga máxima de los sistemas en situaciones críticas es de 90% y persiste un nivel de exposición a fallas, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia.

Para poder clasificar un centro de datos como Tier IV, la tasa de disponibilidad máxima del centro de datos debe ser de 99.995% del tiempo

CAPÍTULO 3

SITUACIÓN ACTUAL

El presente capítulo tiene como objetivo detallar las actividades, procesos y procedimientos actuales con los que cuenta la Dirección de TICS de la UTMACH.

3.1 Introducción

Conforme a lo indicado en la página 23 del Informe de la evaluación del Plan Operativo Anual – POA – del segundo semestre y anual 2015:

Tabla 2 Logros y debilidades evaluación POA 2015. Fuente: POA 2015 Dtics

LOGROS	DIFICULTADES
1) Mantenimiento preventivo y correctivo de equipos informáticos	**1)** Implementar sistemas de seguridad: Adquisición de 600 licencias de antivirus que no fue realizada por falta de presupuesto
2) Elaboración de políticas de Tecnologías de la Información y Comunicaciones	**2)** Mantenimiento a dispositivos de protección eléctrica para equipos de networking: No ejecutado debido a que se remite estudios y presupuesto por un valor de USD 40.700 y solo fueron asignados USD 1,290.90
3) Elaboración de comunicaciones e informes	**3)** Adecuación de los cuartos de comunicaciones de las unidades académicas y ciudadela 10 de Agosto: Proceso no ejecutado
4) Capacitación a los usuarios en el uso de aplicaciones informáticas	**4)** Integración de servicio para videoconferencia
5) Brindar soporte a los usuarios informáticos	**5)** Implementación de equipo mobiliario en las oficinas
6) Desarrollo e Implementación de Sistemas para la UTMACH	**6)** Ajustes y correcciones del POA no alineadas con la realidad de la Dirección de TICS
7) Mantenimiento de los módulos integrados al SIUTMACH	
8) Estudio para la implementación de 5 Utmáticos en las unidades académicas	
9) Mejorar al 100% la cobertura de internet en las edificaciones y espacios del campus de la UTMACH	
10) Mejorar el acceso a las bases de datos especializadas	
11) Mantenimiento de la infraestructura de red de la Universidad	

A excepción del logro 8 que fue solicitado por la máxima autoridad de la UTMACH y delegado a la Dirección de TICS, se evidencia que tanto los logros como las dificultades, no corresponden a necesidades del negocio que dependen o se relacionan directa o indirectamente con TICS.

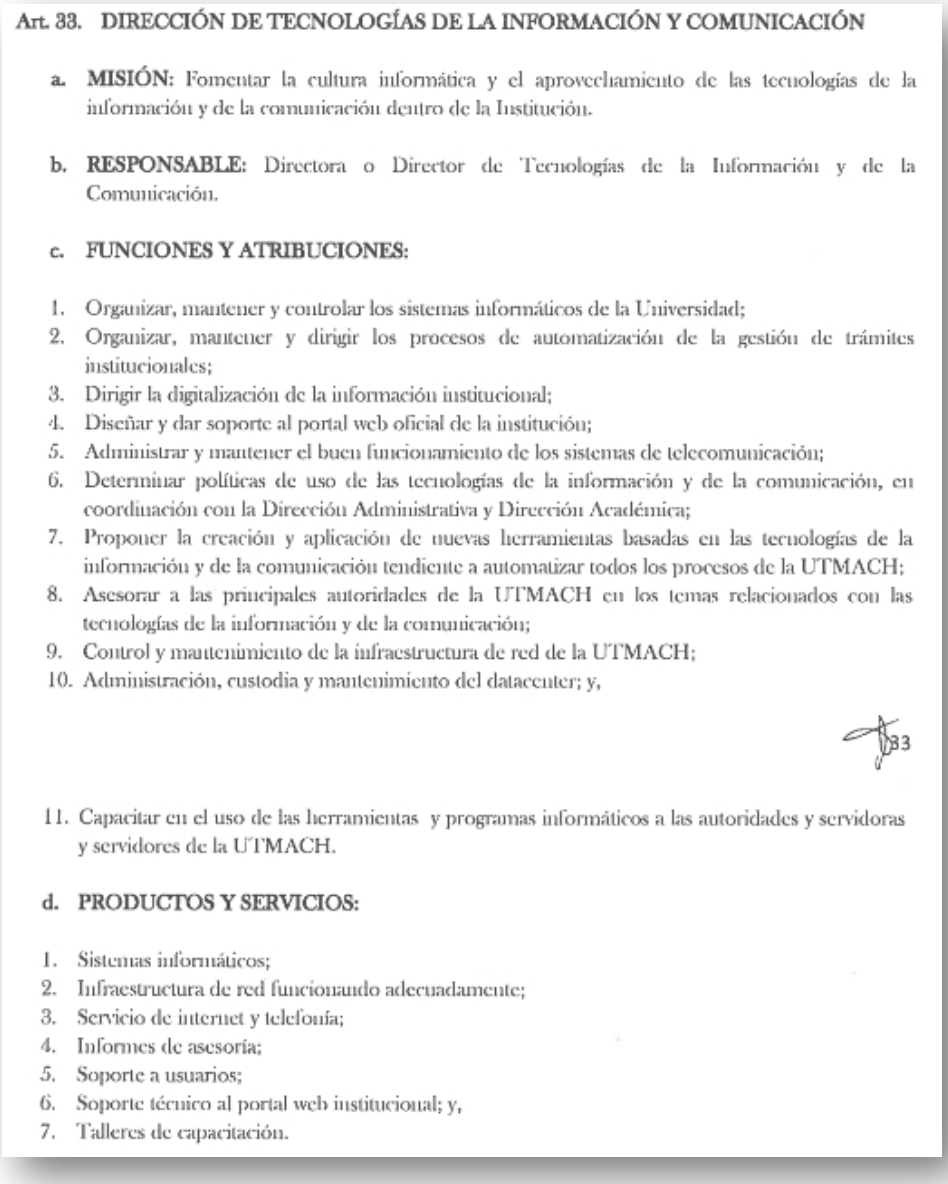
Se evidencia también que en las dificultades los presupuestos proyectados por la Dirección de TICS vs los presupuestos realmente asignados, no guardan ninguna relación, notándose de esta manera la no relación y comunicación entre la Dirección de TICS y la máxima autoridad.

Las actividades descritas en los logros hacen que la Dirección de TICS se ubique dentro de la UTMACH no como unidad estratégica sino como una unidad de apoyo, y no guardan ninguna relación con lo requerido por el Plan de Continuidad de Servicios.

Conforme a lo establecido en la página 7 (mapa de procesos), del Reglamento Orgánico de Gestión Organizacional por Procesos de la UTMACH, se corrobora que la dirección de TICS no es considerada como una unidad estratégica de la institución sino como una unidad de apoyo.

Figura 3.1 Organización por procesos de la UTMACH. Fuente: Reglamento Orgánico de Gestión Organizacional por Procesos de la UTMACH

En la página 33 del mismo reglamento, se definen las funciones, atribuciones, productos y servicios esperados de la Dirección de TICS de la UTMACH:



Art. 33. DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

a. **MISIÓN:** Fomentar la cultura informática y el aprovechamiento de las tecnologías de la información y de la comunicación dentro de la Institución.

b. **RESPONSABLE:** Directora o Director de Tecnologías de la Información y de la Comunicación.

c. **FUNCIONES Y ATRIBUCIONES:**

1. Organizar, mantener y controlar los sistemas informáticos de la Universidad;
2. Organizar, mantener y dirigir los procesos de automatización de la gestión de trámites institucionales;
3. Dirigir la digitalización de la información institucional;
4. Diseñar y dar soporte al portal web oficial de la institución;
5. Administrar y mantener el buen funcionamiento de los sistemas de telecomunicación;
6. Determinar políticas de uso de las tecnologías de la información y de la comunicación, en coordinación con la Dirección Administrativa y Dirección Académica;
7. Proponer la creación y aplicación de nuevas herramientas basadas en las tecnologías de la información y de la comunicación tendiente a automatizar todos los procesos de la UTMACH;
8. Asesorar a las principales autoridades de la UTMACH en los temas relacionados con las tecnologías de la información y de la comunicación;
9. Control y mantenimiento de la infraestructura de red de la UTMACH;
10. Administración, custodia y mantenimiento del datacenter; y,

33

11. Capacitar en el uso de las herramientas y programas informáticos a las autoridades y servidoras y servidores de la UTMACH.

d. **PRODUCTOS Y SERVICIOS:**

1. Sistemas informáticos;
2. Infraestructura de red funcionando adecuadamente;
3. Servicio de internet y telefonía;
4. Informes de asesoría;
5. Soporte a usuarios;
6. Soporte técnico al portal web institucional; y,
7. Talleres de capacitación.

Figura 3.2 funciones, atribuciones, productos y servicios esperados de la Dirección de TICS. Fuente: Reglamento Orgánico de Gestión Organizacional por Procesos de la UTMACH

Dentro de las funciones atribuciones se identifican 4 ítems (numerales 2, 3, 7 y 8), que se encuentran directamente relacionados con las máximas autoridades y en el numeral 6 se indica que las políticas de uso de las TICS deben ser

elaboradas en coordinación con la Dirección Administrativa y Dirección Académica, lo cual deja por fuera o en un segundo plano la revisión y evaluación de las mismas por parte de la máxima autoridad.

Dentro de los productos y servicios esperados, no se especifica el alcance del ítem 2 y se evidencia también que no se mencionan planes de continuidad de los servicios, análisis de impacto de negocio y gestión de riesgos, orientando de esta manera a la dirección de TICS de la UTMACH como responsable del servicio de soporte y desarrollo de sistemas.

Conforme a lo establecido por el POA – PEDI 2013 – 2017, en su página 18:

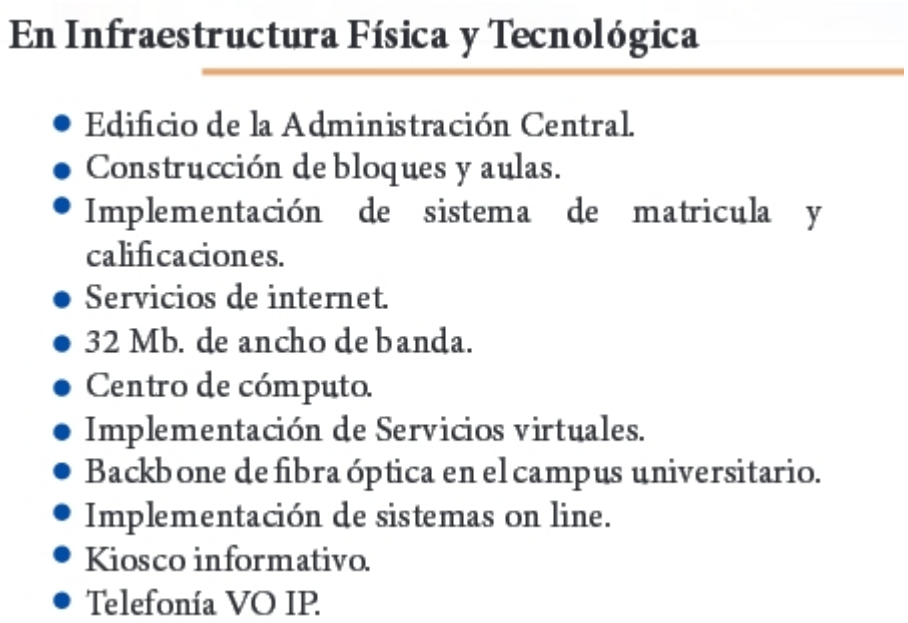


Figura 3.3 Inversión en Infraestructura Física y Tecnológica. Fuente: POA – PEDI 2017 de la UTMACH

- Se menciona al Centro de Datos, servicios de conectividad e internet y el desarrollo e implementación de sistemas.

- En las páginas 33 – 34: Análisis FODA, no se involucra a las TICS en ninguno de los 4 ámbitos.

- En la página 52, objetivo Organizacional, se establece como objetivo estratégico 11: Incorporar las TICS, incluido el Gobierno Electrónico a toda la Gestión Institucional.

- En la página 65, la meta para el objetivo estratégico 11 establece: Mejorar al 100% la cobertura de internet de las edificaciones y espacios de la UTMACH para docentes, estudiantes y usuarios.

Mediante estos insumos puede concluirse que no existe una visibilidad completa en lo referente a los servicios que brinda el Centro de Datos de la UTMACH, y se enfoca únicamente en los frentes de: Desarrollo de sistemas y conectividad de internet, sin considerarse que tanto interna como externamente existen diferentes participantes y diferentes servicios que son expuestos a través de la institución y contribuyen de manera directa a la Planificación Estratégica.

El presente estudio se enfocará en identificar los servicios que ofrece el Centro de Datos de la UTMACH, alinearlos a la planificación estratégica, POA y PAC institucionales, establecer planes de acción que permitan tomar acciones preventivas y correctivas frente a desastres y combinar marcos de referencia (frameworks), de las TICS con el propósito de diseñar un Plan de Continuidad de los servicios del Centro de Cómputo.

3.2 Levantamiento De Requerimientos

El levantamiento de requerimientos actualmente no cuenta con un proceso o metodología determinada, por lo que dependiendo de la naturaleza de los mismos, pueden existir varias formas de receptarlos (ya sea verbalmente o a través de un documento formal), por parte de la Dirección de TICS.

3.2.1 Requerimiento De Acceso A Aplicaciones

- Usuario requirente solicita el acceso a una aplicación de la UTMACH al Director de TICS a través de un oficio o mediante un correo electrónico.

- Director de TICS asigna la solicitud al Analista de Sistemas que se encuentre como responsable o que sea afín a la aplicación a la que se solicita el acceso.

- El Analista de Sistemas analiza el requerimiento, comunica verbalmente al Director de TICS si el acceso solicitado es procedente y finalmente, el Director de TICS comunica al usuario requirente mediante un oficio o a través de un correo electrónico la aprobación o rechazo del acceso.

3.2.2 Requerimiento De Acceso A Internet O Red Interna

- Usuario requirente solicita atención a un requerimiento de conectividad a internet o red interna al Director de TICS a través de un oficio o mediante un correo electrónico.

- Director de TICS asigna la solicitud para su revisión al Analista de TICS 3, a través de un oficio sumillado o la copia de correo del usuario requirente.

- Analista de TICS 3 planifica y solicita por correo o vía telefónica, una visita al área requirente.

- Analista de TICS 3 determina factibilidad técnica e informa sobre situación y posibilidades de acceso al usuario requirente.

3.2.3 Requerimiento De Administración De Acceso Externo A Equipos Fuera Del Centro De Datos

- Usuario requirente solicita el acceso a equipos desde una localidad externa al Centro de Datos de la UTMACH centro de Datos al Director de TICS a través de un oficio o mediante un correo electrónico.

- Director de TICS asigna la solicitud para su revisión al Analista de TICS 3, a través de un oficio sumillado o la copia de correo del usuario requirente.

- El Analista de Sistemas analiza el requerimiento, comunica verbalmente al Director de TICS si el acceso solicitado es procedente y finalmente, el Director de TICS comunica al usuario requirente mediante un oficio o a través de un correo electrónico la aprobación o rechazo del acceso.

3.2.4 Requerimiento De Creación De Máquinas Virtuales

- Usuario requirente solicita la creación de una máquina virtual al Director de TICS a través de un oficio o mediante un correo electrónico.

- Director de TICS asigna la solicitud para su revisión al Analista de TICS 3, a través de un oficio sumillado o la copia de correo del usuario requirente.

- Analista de TIC 3 revisa requerimiento para determinar factibilidad técnica y operativa, e informa sobre la factibilidad técnica al usuario requirente.

3.3 Administración Y Control De Tecnologías De La Información

Actualmente, la administración y control de la Unidad de Tecnologías de la Información y Comunicación de la UTMACH, se encuentra definida por 3 niveles:

- **Director de TICS:** Recibe los requerimientos y asigna las solicitudes hacia la unidad de TICS.

- **Analista de Sistemas 3:** Recepta los requerimientos referentes a: Automatización, desarrollo y mantenimiento de sistemas informáticos que son asignados por el Director de TICS y los analiza con el equipo de Analistas de Sistemas 1.

- **Analista de TICS 3:** Recepta los requerimientos referentes a: Virtualización, seguridad de la infraestructura de red, accesos internos y externos que son asignados por el Director de TICS.

3.4 Organigrama Del Departamento De TIC

Actualmente, la Dirección de TICS de la Universidad Técnica de Machala no cuenta con una estructura orgánico - jerárquica dentro del orgánico funcional institucional. Conforme lo mencionando en el ítem 3.3 del presente estudio, la Dirección de TIC de la Universidad Técnica de Machala, se encuentra concebida de la siguiente manera:

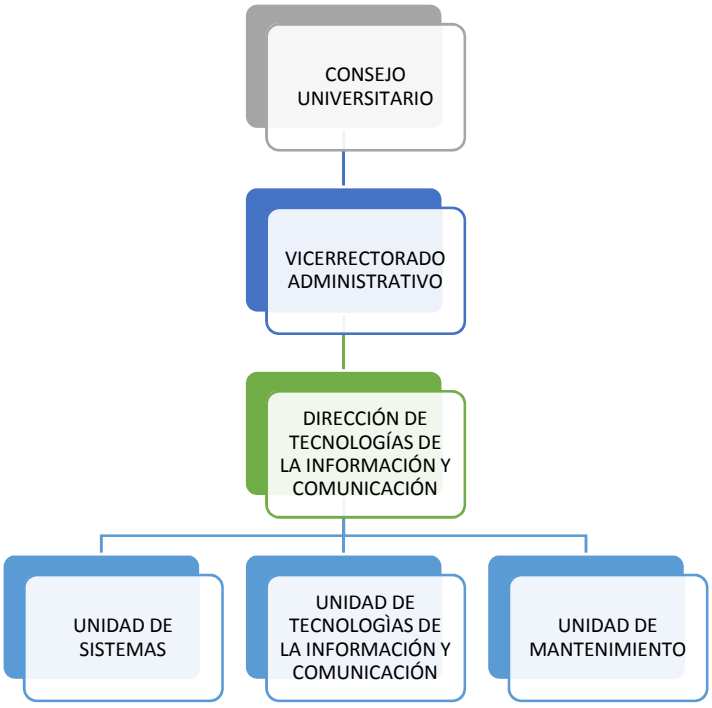


Figura 3.4 Organización Jerárquica DTICS. Fuente: Mapa Organizacional de la UTMACH

3.5 Roles Y Responsabilidades

EDT	SERVICIO	MIEMBROS EQUIPO					
		Analista de TIC 3	Director de TIC	Analistas de Mantenimiento	Dirección de evaluación interna	Usuarios	Analista de sistemas I
1	**SERVICIOS DE CONECTIVIDAD**						
	Acceso a internet	R	A,I		I,C	I	
	Provisión de conectividad interna	R	A,I		I,C	I	
	Provisión de conectividad entre Campus	R,C	A,I				
	Provisión de acceso a las aplicaciones de la institución	R,C	A,I			I	I,C
	Administración de acceso externo a Equipos fuera del Centro de Datos	R,C	A,I			I	
	Administración de usuarios VPN	R,C	A,I			I	
2	**SERVICIO DE ACTUALIZACION**						
	Actualización de bases de firmas de antivirus	R,C	A,I	R			
	Actualización de sistemas operativos Windows y Microsoft Office	R,C	A,I	R			
3	**SERVICIO DE COLABORACION**						
	Telefonía IP		A,I			I	R,C
	Mensajería instantánea	R,C	A,I	R		I	
4	**SERVICIO DE VIRTUALIZACION**						
	Provisión de máquinas virtuales	R,C	A,I			I	I,C
	Respaldo de máquinas virtuales	R,C	A,I			I	I,C
5	**SERVICIOS DE GENERALES**						
	Monitorización de servidores y equipos de red	R,C	A,I	R			I,C
	Suministro eléctrico contingente	R,C	A,I	R			I
	Sistema de Climatización	R,C	A,I	R			I

3.6 Situación Actual Del Centro De Datos De La UTMACH

3.6.1 Condiciones Físicas

El cuarto destinado para el centro de datos cuenta con una longitud de 6,84m x 5,19m, el piso se encuentra revestido completamente por vinil antiestático, posee una ventana que da hacia la oficina de monitoreo permitiendo una visibilidad completa del centro de datos sin necesidad de ingresar al mismo.

Para el ingreso de cables backbone, eléctrico, ductos de aire acondicionado, tiene instaladas rejillas metálicas sostenidas a la loza, estas rejillas están instaladas de tal manera que dividen el cableado eléctrico del cableado de datos.

El ingreso al Centro de Datos cuenta con una puerta de aluminio sin controles de acceso, sensores y sistemas biométricos. Tampoco se cuenta con un sistema contra incendios.

3.6.2 Condiciones Ambientales

El Centro de Datos cuenta con dos aires acondicionados modulares tipo gabinete de 42U con arquitectura InRow escalable, de expansión directa, capacidad de refrigeración de 9,9 KW 33788 BTU/h y fuentes de alimentación interna redundantes.

Para garantizar un adecuado enfriamiento de los racks de servidores y equipos, cada aire acondicionado cuenta con un sensor de temperatura en la línea de ingreso de aire frío de los racks.

3.6.3 Condiciones Eléctricas

El centro de datos cuenta con una red eléctrica con balanceo de cargas, conformada por dos UPS de 15 KVA, cada UPS cuenta con su tablero de bypass y dentro de estos un tablero de distribución de 220V con doce puntos.

Los aires acondicionados poseen acometidas tanto para las manejadoras de los aires (220v) y las condensadoras (220V). Adicionalmente se cuenta con instalaciones eléctricas para lámparas de emergencia, cámaras de seguridad, y sistema biométrico.

3.7 Situación Actual Del Modelo De Red De La UTMACH

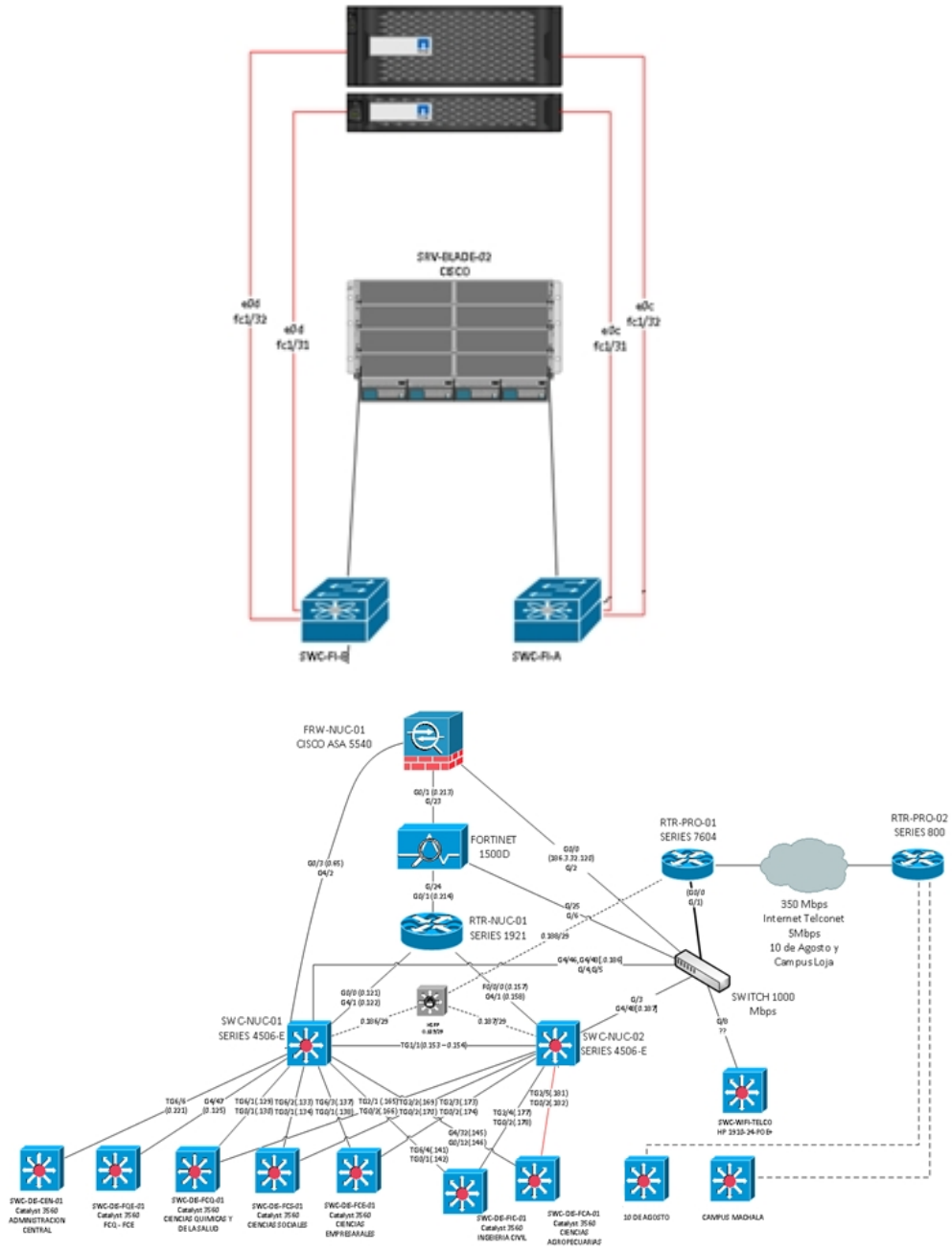


Figura 3.5 Diagrama de Red de la UTMACH. Fuente: Unidad de Tecnologías de la Información y Comunicación

Del modelo de red actual de la UTMACH se puede concluir:

- Los componentes de seguridad perimetral no son redundantes, por lo que una falla en cualquiera de ellos provocaría ataques de Denegación de Servicios.

- El equipo que frontera las conexiones externas: Acceso a internet y conectividad con terceros, no cuenta con un equipo de backup, por lo que una falla del mismo dejaría expuesta y vulnerable a toda la red institucional (incluidos los servidores y los sistemas de almacenamiento). Ante este escenario, todos los servicios expuestos por la UTMACH y de acceso desde terceros no estarán disponibles.

- Se evidencia que existe un modelo de red de tres capas: Core, distribución y acceso.

- Los switches de distribución se encuentran únicamente en las siguientes facultades: Ciencias Químicas y de la Salud, Ciencias Sociales, Ciencias Empresariales, Ingeniería Civil y Ciencias Agropecuarias, los cuales no cuentan con un equipo de backup. Ante la pérdida de uno de los equipos, la facultad afectada no dispondrá de los servicios que requiere.

- Se cuenta con un solo switch que provee el acceso a la red inalámbrica y un equipo de acceso con conectividad redundante hacia cada uno de los switches de core.

3.8 Catálogo De Servicios

Podemos considerar al Catálogo de Servicios como la piedra angular de la prestación de los mismos ya que es la parte visible a los clientes, además de identificar los servicios que proporciona TI. Para el presente estudio nos enfocaremos en los servicios que son ofrecidos por el Centro de Datos de la Universidad Técnica de Machala.[1]

3.8.1 Servicios De Conectividad

Proveen el acceso de los usuarios a los diferentes recursos de red disponibles tales como impresoras, escáneres, archivos compartidos, aplicaciones de la Institución, así como acceso a fuentes externas de información y acceso remoto a la intranet de los 3 campus.

Dentro de esta categoría se han identificado los siguientes servicios:

- Acceso a Internet
- Provisión de conectividad interna
- Provisión de conectividad entre Campus
- Provisión de acceso a las aplicaciones de la Institución

[1] **En el Anexo A se incluye la descripción completa de todos los servicios detallados en esta sección**

- Administración de acceso externo a equipos fuera del Centro de Datos
- Administración de Usuarios VPN
- Administración de Nombres de Dominio

3.8.2 Servicios De Actualización

Garantizan las actualizaciones necesarias para aquellas aplicaciones que lo requieran por liberaciones del Fabricante, tales como bases de datos de virus.

Dentro de esta categoría se ha identificado el siguiente servicio:

- Actualización de Antivirus

3.8.3 Servicios De Colaboración

Permiten el establecer una comunicación entre los usuarios de la Institución, ya sea por medio de mensajes de texto o voz.

Dentro de esta categoría se han identificado los siguientes servicios:

- Telefonía IP
- Mensajería Instantánea

3.8.4 Servicios De Virtualización

Debido a la infraestructura tecnológica con la cuenta el Centro de Datos de la Universidad Técnica de Machala, es posible proveer la virtualización de servidores, por lo tanto dentro de esta categoría podemos identificar los siguientes servicios:

- Provisión de máquinas virtuales
- Respaldo de máquinas virtuales

3.8.5 Servicios Generales

A través de las herramientas proveídas por la plataforma de virtualización de servidores, es posible realizar la monitorización de los mismos, además con otros aplicativos es posible revisar el estado de los equipos de Red. Así mismo, con la finalidad de garantizar el adecuado funcionamiento y estado de los equipos que se encuentran en el Centro de Datos de la Universidad Técnica de Machala se proporciona climatización y suministro eléctrico alterno.

Dentro de esta categoría se han podido identificar los siguientes servicios:

- Monitorización de servidores y equipos de red

- Suministro Eléctrico contingente
- Sistema de Climatización

CAPÍTULO 4

ANÁLISIS Y DISEÑO – DESARROLLO DEL PLAN DE CONTINUIDAD DEL SERVICIO

4.1 Alcance Del Plan De Continuidad Del Servicio

El plan de continuidad de los servicios de TI que se alojan en el Centro de Datos de la Universidad Técnica de Machala tiene por alcance:

- Definir los servicios y procesos críticos de TICS requeridos por las áreas prioritarias del negocio.
- Historia de las interrupciones graves de los servicios de TICS.
- Expectativas del negocio.
- Disponibilidad de los recursos.

El énfasis de los alcances de la administración de la continuidad de los servicios y sus dependencias de TICS, deberán ser considerados dentro de las prioridades del negocio a través de la máxima autoridad o su delegado.

4.2 Administración De Riesgos

El término de Administración de riesgos hace referencia a una metodología lógica y sistemática, con la finalidad de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal manera que permita a la organización minimizar las pérdidas y maximizar las oportunidades.

Para el presente proceso de Administración de Riesgos del Centro de Datos de la Universidad Técnica de Machala se establece la manera en la que se debe llevar a cabo el análisis de los diferentes riesgos que potencialmente podrían afectarlo.

Análisis y Evaluación de Riesgos

El objetivo de realizar el análisis de riesgos es determinar a que se encuentra expuesto del Centro de Datos de la Universidad Técnica de Machala, así como el entorno asociado a este, estimando la probabilidad de ocurrencia y el nivel

de impacto que puede ocasionar, en el caso de que el riesgo se llegara a materializar, y poder sugerir las medidas apropiadas que deberían seguirse para conocer, prevenir, impedir, reducir o controlar el riesgos establecido.

Identificación De Riesgos

En la tabla que se describe a continuación se establecen aquellos riesgos potenciales por los cuales se podría ver afectado el Centro de Datos de la Universidad Técnica de Machala. La presente identificación de riesgos incluye todos aquellos que se encuentran bajo control o no de la Dirección de Tecnologías de la Información y Comunicación y por lo tanto de la Institución.

Tabla 3 Identificación de Riesgos. Fuente: Dtics UTMACH

Id	Categoría	Actividad	Hallazgo/Causa	Evento de Riesgo
1	Servicios de Conectividad	Conectividad Interna/Acceso a Internet: ¿Existen en las Unidades Académicas equipos activos con capacidad de controlar Spanning - Tree?	Usuarios no calificados pueden conectar patchcords en switches pertenecientes a una cascada, causando un lazo en el segmento de red, que puede dejar sin servicio a toda la unidad académica.	Interrupción del Servicio acceso a la red e Internet
2	Servicios de Conectividad	Conectividad Interna/Acceso a internet: ¿Existe algún mecanismo para la detección y mitigación de ataques de denegación de servicio?	No se cuenta con mecanismos de prevención y defensa ante ataques de denegación de servicios	Saturación de los servidores
3	Servicios de Conectividad	Conectividad Interna/Acceso a internet: ¿Existen recorridos diferenciados para la ruta principal y backup del anillo de Fibra Óptica?	Las rutas principal y backup poseen dos puntos de fallo, ya que comparten el mismo poste eléctrico hacia la salida del Centro de Datos y hacia el ingreso de la Unidad Académica de Ciencias Agropecuarias	Corte de la fibra
4	Servicios de Conectividad	Conectividad Interna/Acceso a Internet: ¿Se han realizado capacitaciones acerca de	El plan de capacitación existente no toma en cuenta los temas tecnológicos de la unidad de TIC.	Indisponibilidad parcial o total de los Servicios del Centro de Datos

Id	Categoría	Actividad	Hallazgo/Causa	Evento de Riesgo
		temas tecnológicos para el personal encargado de la Infraestructura de red?		
5	Servicios Generales	Suministro eléctrico contingente: ¿Existe una reserva de combustible suficiente para poder garantizar la el funcionamiento continuo del suministro eléctrico alterno?	Existe una planta de energía que se alimenta por medio de diésel, la misma no cuenta con un procedimiento de custodia o mantenimiento del nivel de diésel en la cámara de combustible de la planta.	Corte de energía eléctrica
6	Servicios Generales	Suministro eléctrico contingente: ¿Con que frecuencia se realizan los trabajos de mantenimiento de los UPS del Centro de Datos?	Existe un plan de mantenimiento, pero depende de disponibilidad presupuestaria	Falla en el sistema de protección eléctrica
7	Servicios Generales	Sistema de climatización: ¿Se realiza un mantenimiento periódico de los aires acondicionados de precisión dispuestos	Existe un plan de mantenimiento, pero depende de disponibilidad presupuestaria	Falla en los equipos de climatización

Id	Categoría	Actividad	Hallazgo/Causa	Evento de Riesgo
		para el Centro de Datos?		
8	Servicios de Virtualización	Provisión de Máquinas Virtuales: ¿Los equipos con los que cuenta actualmente el Centro de Datos son capaces de satisfacer demandas exigentes de recursos?	La Dirección de investigación para el desarrollo de sus proyectos demanda la provisión de máquinas virtuales con grandes capacidades de procesamiento y almacenamiento	Recursos limitados
9	Servicios de Virtualización	Respaldo de Máquinas Virtuales: ¿Se almacenan los respaldos de las máquinas virtuales en un lugar seguro fuera del Centro de Datos?	Los respaldos son almacenados en una bóveda de discos ubicada en el Centro de Datos. Lo que en caso de suscitarse un desastre provocaría pérdida de información	Pérdida de información
10	Servicios Generales	Monitorización de servidores y equipos de red: ¿Existen equipos dedicados al monitoreo de eventos que permitan identificar amenazas y apliquen las restricciones del caso?	Actualmente se cuenta con un proceso de revisión de alertas y logs de los equipos que permiten la detección se lo acontecido	Interrupción de los servicios

Id	Categoría	Actividad	Hallazgo/Causa	Evento de Riesgo
11	Servicio de conectividad	Conectividad entre campus: ¿Existen respaldos de las configuraciones de los equipos de comunicación que establecen los enlaces de datos e internet con los campus Machala y 10 de agosto?	Se cuenta con respaldo de configuraciones de los equipos instalados en el centro de datos, pero no se cuenta con respaldos de las configuraciones de la red MPLS del proveedor	Pérdida de comunicación hacia el campus principal
12	Servicio de conectividad	Conectividad entre campus: ¿Se cuenta con enlaces de respaldo para conexión con los campus que están fuera de los predios de la universidad?	El tendido de fibra del proveedor, cuenta con rutas principal y alterna instaladas en postes de alumbrado público, que siguen rutas diferenciadas	Caída de enlace de respaldo hacia el campus principal
13	Servicio de conectividad	Acceso a aplicaciones de institución: ¿Se posee procedimientos claros para la apertura y cierre de puertos para las aplicaciones de la institución?	Existen controles internos para el registro de reglas de acceso a las aplicaciones, pero no están estandarizados y documentados.	Duplicidad u omisión de reglas de filtrado

Id	Categoría	Actividad	Hallazgo/Causa	Evento de Riesgo
14	Servicio de conectividad	Acceso externo a equipos fuera del centro de datos: ¿Se lleva un control ordenado de registros de acceso a equipos instalados fuera del centro de datos?	El único control al registro de acceso a equipos instalados fuera del centro de datos se realiza al crear las reglas en el firewall	Accesos configurados a equipos que ya no se encuentran activos
15	Servicio de conectividad	Administración de usuarios VPN: ¿Existen controles sobre las sesiones VPN realizadas en la red de la UTMACH?	Existen usuarios registrados con password para acceso al circuito VPN, pero no se realiza monitoreo sobre las sesiones que estos inician.	Consumo excesivo de recursos para el servidor de sesiones VPN
16	Servicios de Actualización	Actualización de bases de firmas de antivirus: ¿Se cuenta con servidores de actualización en clúster, para alta disponibilidad ?	Existe un único servidor de actualizaciones de antivirus	Interrupción del servicio de actualización de base de firmas
17	Servicios de Actualización	Actualización de SO y Office: ¿Se cuenta con servidores de actualización en clúster, para alta	Existe un único servidor de actualizaciones de SO y Office	Interrupción del servicio de actualización de SO y Office

Id	Categoría	Actividad	Hallazgo/Causa	Evento de Riesgo
		disponibilidad ?		
18	Servicios de colaboración	Telefonía IP: ¿Existe un proceso de cifrado en la comunicación punto a punto?	El canal de comunicación punto a punto no se encuentra cifrado	Interceptación de llamadas telefónicas
19	Servicios de colaboración	Mensajería instantánea: ¿Es posible intercambiar archivos a través de la plataforma de IM?	Actualmente es posible el intercambio de cualquier tipo de archivo	Interrupción en la transmisión para archivos mayores a 1 GB

Análisis De Riesgos

Es necesario tener un completo entendimiento y comprensión de los riesgos, para poder determinar cómo deben ser tratados de una manera efectiva, lo cual involucra:

- La probabilidad de ocurrencia.
- La determinación de su impacto potencial.
- Nivel de Exposición, mediante la combinación del impacto con la probabilidad de ocurrencia.

Así mismo, se deben identificar los controles existentes, en los procesos y actividades que contribuyan a minimizar los riesgos negativos o mejorar los riesgos positivos, debiendo evaluar sus fortalezas y debilidades.

El Nivel de exposición del riesgo se determina mediante el producto de la probabilidad de ocurrencia y el impacto.

Exposición = Probabilidad * Impacto

El riesgo se debe medir, en relación al impacto y la probabilidad, ubicándolo en una matriz de priorización.

- **Impacto:** Forma en la cual el riesgo afectaría a los resultados y las repercusiones que puede tener, se ha establecido la siguiente escala:

Tabla 4 Valoración del Impacto. Fuente: Los autores

Impacto	Valor
Alto	100
Medio	50
Bajo	10

- **Probabilidad:** Que tan frecuente puede que se presente el riesgo, se ha establecido la siguiente escala:

Tabla 5 Valoración de la Probabilidad de ocurrencia. Fuente: Los autores

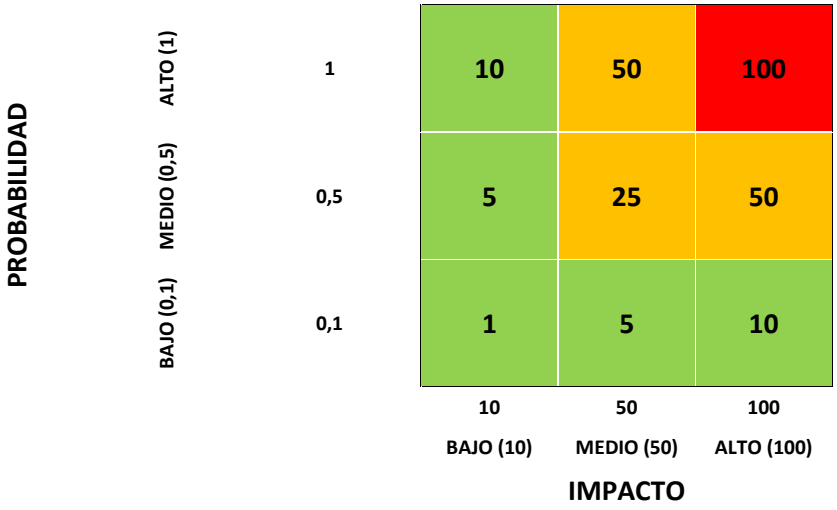
Probabilidad	Valor
Alto	1,0
Medio	0,5
Bajo	0,1

Tomando en consideración la valoración tanto para el impacto como para probabilidad de ocurrencia, nos es posible clasificar los riesgos de acuerdo a su nivel de Exposición, así:

Tabla 6 Nivel de Exposición del Riesgo. Fuente: Los autores

Mínimo	Máximo	Importancia
51	100	**Alto**
11	50	**Medio**
1	10	**Bajo**

Tabla 7 Matriz de Priorización. Fuente: Los autores



A continuación, se despliega en una tabla la valoración del nivel de exposición al Riesgo en base al Impacto y la Probabilidad, la cual será muy importante para evaluación del riesgo:

Tabla 8 Análisis de Riesgos. Fuente: Los autores

Id	Categoría	Evento de Riesgo	Probabilidad	Impacto	Exposición
1	Servicios de Conectividad	Interrupción del Servicio acceso a la red e Internet	Alto	Alto	100
2	Servicios de Conectividad	Saturación de los servidores	Alto	Alto	100
3	Servicios de Conectividad	Corte de la fibra	Medio	Alto	50
4	Servicios de Conectividad	Indisponibilidad parcial o total de los Servicios del Centro de Datos	Alto	Alto	100
5	Servicios Generales	Corte de energía eléctrica	Alto	Alto	100
6	Servicios Generales	Falla en el sistema de protección eléctrica	Alto	Alto	100
7	Servicios Generales	Falla en los equipos de climatización	Medio	Medio	25
8	Servicios de Virtualización	Recursos limitados	Alto	Medio	50
9	Servicios de Virtualización	Pérdida de información	Medio	Alto	50
10	Servicios Generales	Interrupción de los servicios	Alto	Alto	100
11	Servicio de conectividad	Pérdida de comunicación hacia el campus principal	Medio	Alto	50
12	Servicio de conectividad	Caída de enlace de respaldo hacia el campus principal	Medio	Medio	25
13	Servicio de conectividad	Duplicidad u omisión de reglas de filtrado	Medio	Medio	25

Id	Categoría	Evento de Riesgo	Probabilidad	Impacto	Exposición
14	Servicio de conectividad	Accesos configurados a equipos que ya no se encuentran activos	Medio	Medio	25
15	Servicio de conectividad	Consumo excesivo de recursos para el servidor de sesiones VPN	Medio	Alto	50
16	Servicios de Actualización	Interrupción del servicio de actualización de base de firmas	Medio	Medio	25
17	Servicios de Actualización	Interrupción del servicio de actualización de SO y Office	Medio	Medio	25
18	Servicios de colaboración	Interceptación de llamadas telefónicas	Medio	Medio	25
19	Servicios de colaboración	Interrupción en la transmisión para archivos mayores a 1 GB	Bajo	Bajo	1

Evaluación De Riesgos

El propósito de la evaluación de riesgos es el poder tomar decisiones, sustentadas en los resultados del análisis para identificar cuáles deben ser tratados y la prioridad de su tratamiento.

Tabla 9 Evaluación de Riesgos. Fuente: Los autores

Id	Categoría	Evento de Riesgo	Probabilidad	Impacto	Expo.	Eval. del Riesgo
1	Servicios de Conectividad	Interrupción del Servicio acceso a la red e Internet	Alto	Alto	100	(51 - 100) Alto
2	Servicios de Conectividad	Saturación de los servidores	Alto	Alto	100	(51 - 100) Alto
3	Servicios de Conectividad	Corte de la fibra	Medio	Alto	50	(11 - 50) Medio
4	Servicios de Conectividad	Indisponibilidad parcial o total de los Servicios del Centro de Datos	Alto	Alto	100	(51 - 100) Alto
5	Servicios Generales	Corte de energía eléctrica	Alto	Alto	100	(51 - 100) Alto
6	Servicios Generales	Falla en el sistema de protección eléctrica	Alto	Alto	100	(51 - 100) Alto

7	Servicios Generales	Falla en los equipos de climatización	Medio	Medio	**25**	**(11 - 50) Medio**
8	Servicios de Virtualización	Recursos limitados	Alto	Medio	**50**	**(11 - 50) Medio**
9	Servicios de Virtualización	Pérdida de información	Medio	Alto	**50**	**(11 - 50) Medio**
10	Servicios Generales	Interrupción de los servicios	Alto	Alto	**100**	**(51 - 100) Alto**
11	Servicio de conectividad	Pérdida de comunicación hacia el campus principal	Medio	Alto	**50**	**(11 - 50) Medio**
12	Servicio de conectividad	Caída de enlace de respaldo hacia el campus principal	Medio	Medio	**25**	**(11 - 50) Medio**
13	Servicio de conectividad	Duplicidad u omisión de reglas de filtrado	Medio	Medio	**25**	**(11 - 50) Medio**
14	Servicio de conectividad	Accesos configurados a equipos que ya no se encuentran activos	Medio	Medio	**25**	**(11 - 50) Medio**
15	Servicio de conectividad	Consumo excesivo de recursos para el servidor de sesiones VPN	Medio	Alto	**50**	**(11 - 50) Medio**
16	Servicios de Actualización	Interrupción del servicio de actualización de base de firmas	Medio	Medio	**25**	**(11 - 50) Medio**

17	Servicios de Actualización	Interrupción del servicio de actualización de SO y Office	Medio	Medio	**25**	**(11 - 50) Medio**
18	Servicios de colaboración	Interceptación de llamadas telefónicas	Medio	Medio	**25**	**(11 - 50) Medio**
19	Servicios de colaboración	Interrupción en la transmisión para archivos mayores a 1 GB	Bajo	Bajo	**1**	**(1 - 10) Bajo**

Tabla 10 Análisis de los eventos de Riesgos y contramedidas. Fuente: Los autores

Id	Categoría	Evento de Riesgo	Contramedidas		
			Mitigación	Contingencia	Plan de Acción
1	Servicios de Conectividad	Interrupción del Servicio acceso a la red e Internet	Eliminar cascadas de switches, implementando enlaces directos desde el switch de distribución a los switches de acceso de un grupo de oficinas.	N/A debido a que actualmente, en la Unidades Académicas se cuenta únicamente con equipos de switching genéricos	Realizar la adquisición de equipos de switching con capacidad de control de spanning tree
2	Servicios de Conectividad	Saturación de los servidores	Revisar los logs del servidor afectado, determinando el tipo de peticiones de los diferentes clientes y bloqueando a aquellos que se consideren sospechosas dada su estructura	Levantar dos servidores de aplicaciones uno interno y otro externo compartiendo la misma base de datos con la finalidad de garantizar la continuidad de los servicios, dado que la mayoría de ataques provienen del exterior	Implementa soluciones de seguridad de tipo appliance o software que permitan dar visibilidad al tráfico de la red, para el tratamiento del tráfico entrante y saliente
3	Servicios de Conectividad	Corte de la fibra	Implementa un plan de mantenimiento de las rutas de la FO	Levantar de manera automática la segunda ruta del anillo de fibra óptica	Levantar un proyecto que considere la separación física de las rutas principal y backup del anillo de fibra óptica
4	Servicios de Conectividad	No disponibilidad parcial o total de los Servicios del Centro de Datos	Establecer líneas de contacto con proveedores y personal de soporte de infraestructura contratado.	N/A	Identificar las necesidades de capacitación dentro de la dirección de TIC Elaborar el plan de capacitación del personal de TIC e incluirlo

					dentro del plan de capacitación institucional
5	Servicios Generales	Corte de energía eléctrica	Mantener una reserva de combustible para el generador en el Edificio de Rectorado	N/A debido a que actualmente se cuenta con un solo generador en el edificio de Rectorado	1) Levantar el procedimiento de custodia y mantenimiento del nivel de combustible del cuarto de cámaras de combustible 2) Evaluar el costo - beneficio de la adquisición de un generador adicional para la unidad de Rectorado
6	Servicios Generales	Falla en el sistema de protección eléctrica	Contratar el servicio de mantenimiento anual para los UPS del Centro de Datos	Encendido de planta de energía eléctrica alterna	Definir en el POA - PAC un rubro que considere trabajos de mantenimiento para los UPS.
7	Servicios Generales	Falla en los equipos de climatización	Contratar el servicio de mantenimiento anual para los aires acondicionados de precisión	N/A	Definir en el POA - PAC un rubro que considere trabajos de mantenimiento para los aires acondicionados de precisión
8	Servicios de Virtualización	Recursos limitados	N/A	N/A	Realizar un redimensionamiento de los equipos de cómputo y almacenamiento del Centro de Datos
9	Servicios de Virtualización	Pérdida de información	N/A	N/A	Diseñar un procedimiento para la obtención y custodia de los

					respaldos de las máquinas virtuales en un lugar seguro fuera del centro de datos
10	Servicios Generales	Interrupción de los servicios	Bloquear el tráfico no permitido hacia los equipos	N/A	Llevar a cabo un proceso de ethical hacking que permita identificar y mitigar las posibles amenazas
11	Servicio de conectividad	Pérdida de comunicación hacia el campus principal	Mantener actualizadas las configuraciones de los equipos de comunicación que establecen los enlaces.	Establecer una línea de salida directa hacia internet sin pasar por la red de la UTMACH.	Realizar simulacros de salida a internet a través de la red del proveedor.
12	Servicio de conectividad	Caída de enlace de respaldo hacia el campus principal	Solicitar al proveedor informes mensuales de estado y mantenimiento de los enlaces de respaldo.	Solicitar habilitación de enlace de respaldo a empresa proveedora	Mantener contrato de enlace de respaldo con empresa proveedora
13	Servicio de conectividad	Duplicidad u omisión de reglas de filtrado	Implementar procedimientos y bitácora de creación de reglas de acceso a servicios de la institución.	Depuración de reglas de filtrado en equipos de seguridad	Mantener un procedimiento de respaldos semanales de las configuraciones de los equipos de seguridad
14	Servicio de conectividad	Accesos configurados a equipos que ya no se encuentran activos	Implementar procedimientos y bitácora de creación de reglas de acceso a equipos instalados fuera del centro de datos	Depuración de reglas de filtrado en equipos de seguridad	Establecer procedimientos de depuración de reglas de filtrado para los equipos de seguridad
15	Servicio de conectividad	Consumo excesivo de recursos para el servidor de sesiones VPN	Limitar la creación de sesiones VPN, verificando los límites establecidos por el fabricante del	Denegar el uso de sesiones VPN que sobrepasen el límite permitido por el	Realizar un análisis de rendimiento del equipo de seguridad, al momento de

			equipo de seguridad que las soporta.	dispositivo de seguridad.	servir sesiones VPN
16	Servicios de Actualización	Interrupción del servicio de actualización de base de firmas	Instalación y configuración de un clúster de servidores de antivirus	Restaurar la MV del servidor de antivirus, del último respaldo válido disponible	Mantener un procedimiento de respaldos semanales de la MV del servidor de antivirus
17	Servicios de Actualización	Interrupción del servicio de actualización de SO y Office	Instalación y configuración de un clúster de servidores WSUS	Restaurar la MV del servidor de WSUS, del último respaldo válido disponible	Mantener un procedimiento de respaldos semanales de la MV del servidor de WSUS
18	Servicios de colaboración	Interceptación de llamadas telefónicas	Implementar un estándar de cifrado de comunicaciones de voz sobre IP	N/A	Seleccionar el mejor estándar de cifrado para comunicaciones para su posterior implementación
19	Servicios de colaboración	Interrupción en la transmisión para archivos mayores a 1 GB	N/A	N/A	Explorar alternativas de servicios para IM, que permitan superar esa limitación

Mapa de Calor

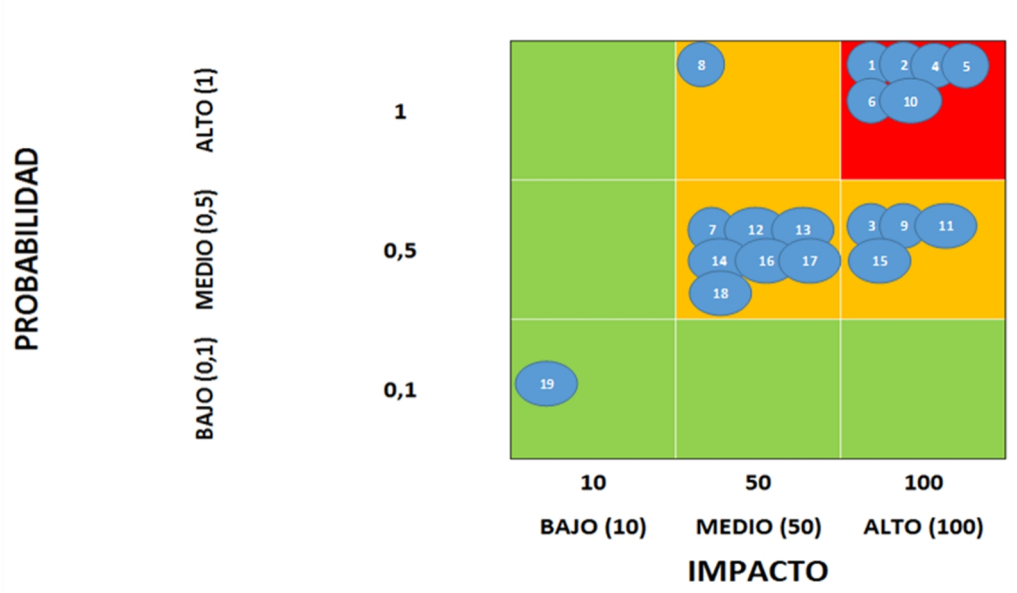


Figura 4.1 Mapa de Calor. Fuente: Los Autores

4.3 Análisis De Impacto Del Negocio

Para efecto de la realización del Análisis de Impacto del Negocio, se trabajó con la Vicerrectora Académica y se establecieron los procesos más importantes como:

Dirección de Talento Humano

- **Selección Docente**: Proceso en el cual los aspirantes a docentes de la Universidad Técnica de Machala, registran su hoja de vida a la aplicación destinada para tal efecto, para el proceso de calificación de méritos.

Dirección Académica

- **Evaluación Docente:** Proceso en el cual los estudiantes y pares académicos evalúan el desempeño Docente.

Personal Administrativo y Docente

- **Registro Académico:** El registro académico consiste en
    - Gestión de Distributivos y Horarios
    - Gestión de Syllabus
    - Gestión de Matrícula
    - Gestión de Calificaciones.

Podemos observar que todos los procesos críticos se asientan sobre la aplicación integrada que tiene la Universidad Técnica de Machala denominada SIUTMACH.

Considerando que en el presente estudio se han declarado los servicios que ofrece el Centro de Datos, y al haber identificado los procesos críticos para la Universidad Técnica de Machala, es necesario establecer una matriz de correspondencia, así:

Tabla 11 Mapeo de Procesos Críticos son servicios del Centro de Datos.
Fuente: Los autores

PROCESO CRÍTICO DEL NEGOCIO	SERVICIO DEL CENTRO DE DATOS
Evaluación Docente	Acceso a internet
	Conectividad Interna
	Conectividad Campus
	Acceso a Aplicaciones
	Provisión de Máquina Virtual
	Respaldo de Máquina Virtual
	Monitoreo Serv-Eq Red
	Suministro eléctrico alterno
Selección Docente	Acceso a internet
	Conectividad Interna
	Conectividad Campus
	Acceso a Aplicaciones
	Provisión de Máquina Virtual
	Respaldo de Máquina Virtual
	Monitoreo Serv-Eq Red
	Suministro eléctrico alterno
Registro Académico	Acceso a internet
	Conectividad Interna
	Conectividad Campus
	Acceso a Aplicaciones
	Provisión de Máquina Virtual
	Respaldo de Máquina Virtual
	Monitoreo Serv-Eq Red
	Suministro eléctrico alterno

Observamos que cada uno de los procesos identificados como críticos por la autoridad, al ser aplicaciones informáticas estos se encuentran asentados sobre la plataforma de servidores, además de los servicios de conectividad.

De acuerdo al mapa de calor, varios de los riesgos que tienen relación con los servicios que soportan los procesos críticos se encuentran en un nivel alto por lo tanto son los que deben ser controlados y minimizados en el menor tiempo posible.

Actualmente la Universidad Técnica de Machala, no cuenta con un procedimiento de registro manual en el caso de que los sistemas dejaran de funcionar, de ahí que los dichos procesos se consideren altamente críticos.

Los criterios que se han considerado para poder realizar la valoración del impacto en el negocio BIA son los siguientes:

Tabla 12 Criterios de Valoración del Impacto del negocio. Fuente: Los autores

Niv.	Criterio	Regulatorio / Legal	Reputacional	Operacional	Servicios a Terceros
3	Alta	Productos cuya paralización tiene implicaciones lega les a nivel de universidad.	Pérdida de imagen a nivel de toda la universidad.	Productos cuya paralización podría generar problemas al sistema educativo de la universidad.	El tiempo máximo en el que el servicio debe ser recuperado es inferior a 4 horas
2	Media	Productos cuya paralización produce una falta leve de orden legal para la universidad.	Pérdida de imagen ante autoridades y consejo universitario.	Productos cuya paralización podría afectar las operaciones internas de la universidad.	El tiempo máximo en el que el servicio debe ser recuperado es igual o superior a 4 horas e inferior a 1 día

1	Baja	Productos cuya paralización podrían o no generar algún problema o responsabilidad de orden legal.	Pérdida de imagen ante usuarios internos.	Productos cuya paralización podría generar o no problemas administrativos para la universidad.	El tiempo máximo en el que el servicio debe ser recuperado es igual o superior a 1 día e inferior a 5 días

Valoración De Los Servicios Del Centro De Datos

Tabla 13 Valoración de los Servicios del Centro de Datos. Fuente: Los autores

Procesos	Productos / servicios	Valoración de Criterios de Impacto				Calificación BIA (promedio de impactos)	Valor del BIA Criticidad (valoración)
		Regulatorio / Legal	Reputacional	Operacional	Servicio a Usuarios		
• **Evaluación Docente** • **Selección Docente** • **Registro Académico**	Acceso a internet	1	3	3	3	3	ALTO
	Conectividad Interna	1	3	3	3	3	ALTO
	Conectividad Campus	1	3	3	3	3	ALTO
	Acceso Aplicaciones	1	2	2	3	2	MEDIO
	Provisión de MV	1	3	2	3	2	MEDIO
	Respaldo de MV	1	3	3	3	3	ALTO
	Monitoreo Serv-Eq Red	1	2	1	1	1	BAJO

Procesos	Productos / servicios	Valoración de Criterios de Impacto				Calificación BIA (promedio de impactos)	Valor del BIA Criticidad (valoración)
		Regulatorio / Legal	Reputacional	Operacional	Servicio a Usuarios		
	Suministro eléctrico alterno	1	3	2	3	2	MEDIO

Tabla 14 Definición de RTO, RPO y MTPD. Fuente: Vicerrectora Académica

Procesos	Productos / servicios	Tiempo de espera antes de iniciar contingencia RTO (min.)	Periodicidad de respaldo – RPO (<= # horas)	Tiempo máximo Tolerable de Interrupción – MTPD
• **Evaluación Docente** • **Selección Docente** • **Registro Académico**	Acceso a internet	30 minutos	<=4horas	40h00
	Conectividad Interna	30 minutos	<=24horas	40h00
	Conectividad Campus	30 minutos	<=24horas	40h00
	Acceso Aplicaciones	30 minutos	<=4horas	40h00
	Provisión de MV	30 minutos	<=48horas	40h00
	Respaldo de MV	30 minutos	<=48horas	40h00
	Monitoreo Serv-Eq Red	30 minutos	<=24horas	40h00
	Suministro eléctrico alterno	30 minutos	<=24horas	40h00

Descripción De La Valoración De Criterios De Impacto

Tabla 15 Descripción de la valoración de criterios de impacto. Fuente: Los autores

Procesos	Productos / servicios	Regulatorio / Legal	Reputacional	Operacional	Servicio a Usuarios
Evaluación Docente	Acceso a internet	La interrupción del servicio no genera inconvenientes de orden legal.	Afectación a la imagen institucional ante la comunidad universitaria como para la población en general.	Generación de incidente al ISP.	Usuarios no pueden acceder desde internet a la aplicación.
Evaluación Docente	Conectividad Interna	La interrupción del servicio no genera inconvenientes de orden legal.	Afectación a la imagen institucional ante la comunidad universitaria.	Generación de incidente al Analista de TIC 3.	Usuarios no pueden acceder a la aplicación, desde la locación afectada en cualquiera de los campus universitarios
Evaluación Docente	Conectividad Campus	La interrupción del servicio no genera inconvenientes de orden legal.	Afectación a la imagen institucional ante la comunidad universitaria.	Generación de incidente al Analista de TIC 3 y al ISP.	Usuarios no pueden acceder a la aplicación, desde el campus universitario afectado.

Evaluación Docente	Acceso Aplicaciones	La interrupción del servicio no genera inconvenientes de orden legal.	Malestar por parte del usuario.	Generación de incidente al Analista de TIC 3.	Usuarios no pueden acceder a la aplicación.
Evaluación Docente	Provisión de MV	La interrupción del servicio no genera inconvenientes de orden legal.	Capacidad limitada para la asignación de recursos tecnológicos.	Ajuste de requerimientos de acuerdo a la disponibilidad de recursos tecnológicos y prioridad operativa.	Dificultad para el usuario de realizar la evaluación docente.
Evaluación Docente	Respaldo de MV	La interrupción del servicio no genera inconvenientes de orden legal.	Afectación a la imagen institucional ante la comunidad universitaria.	Falta de puntos de restauración ante eventualidades que causen daño a la Data.	Pérdida de capacidad para garantizar la recuperación de la información de los usuarios en caso de desastres.
Evaluación Docente	Monitoreo Serv-Eq Red	La interrupción del servicio no genera inconvenientes de orden legal.	La interrupción del servicio no genera inconvenientes en la reputación ante la comunidad universitaria.	Falta de visibilidad para supervisar situa ciones que ocurran en los equipos activos de la UTMACH.	La interrupción del servicio no genera inconvenientes en el servicio a los usuarios.
Evaluación Docente	Suministro eléctrico contingente	La interrupción del servicio no genera inconvenientes de orden legal.	Afectación a la imagen institucional ante la comunidad universitaria.	Incapacidad operativa de los equipos activos	Usuarios no pueden acceder al servicio de evaluación docente.

La Universidad Técnica de Machala requiere de forma urgente poder contar con una réplica en un Centro de Datos alterno, así como una nube de respaldo, para garantizar la operatividad de los procesos que dependen de estos servicios proporcionados por el Centro de Datos principal.

Se debe tomar en cuenta que la activación del Centro de Datos alterno debe ser menor que el MPTD de los procesos.

4.4 Diseño Del Plan De Continuidad Del Servicio

El plan de continuidad del servicio define los pasos para la recuperación de uno o más servicios de TI. El plan identifica los disparadores de la invocación del plan, las personas que han de ser involucradas, las comunicaciones necesarias, etc. El plan de continuidad de los servicios de TI debería ser parte de un plan de continuidad del negocio.

El presente plan de continuidad de los servicios está diseñado para ser aplicado en caso de una amenaza de desastre para el Centro de Datos de la Universidad Técnica de Machala, considerando los riesgos más relevantes detectados dentro del análisis de impacto realizado.

Se ha planteado que la Universidad Técnica de Machala, contrate los servicios de un centro de datos alterno, que albergue tecnología similar a la del centro de datos de la Universidad y que permita mantener la continuidad de sus operaciones, en este contexto se presentaran los pasos necesarios para que la organización ejecute en caso de presentarse un evento que afecta a la operación normal del centro de datos.

4.4.1 Plan De Continuidad Del Servicio

La continuidad del servicio se encarga de prevenir y proteger a la organización de los efectos que pudiera tener una disrupción de los servicios de TI de cualquier índole (técnica, natural, provocada intencionalmente o no por una persona).

El plan de continuidad debe contener procedimientos, preventivos que buscan eliminar o mitigar los riesgos de interrupción y sus posibles efectos, y reactivos que permiten la reanudación inmediata del servicio luego de que se haya sucedido una interrupción.

En resumen, los objetivos principales podrían definirse como:

- Asegurar la pronta recuperación de los servicios críticos de TI después de cualquier desastre.

- Establecer políticas, tomar medidas, y desarrollar procedimientos para mitigar las consecuencias de cualquier evento disruptivo.

Este plan no puede considerarse como exclusivo de TI, debe formar parte de la disciplina de continuidad del negocio de la organización, insumo con el que la UTMACH no cuenta, pero debe ser considerada para implementación futura.

La Universidad Técnica de Machala no cuenta con los siguientes insumos:

- Plan de continuidad del negocio (BCP)
- Gestión del Plan de Continuidad del Negocio (BCM).
- Plan de recuperación de Desastres (DRP).
- Clasificación e identificación de los activos de información conforme lo establecido por la ISO 27001.
- Plan de contingencia de los servicios de TIC.

Actualmente, se llevan procesos de recuperación manuales, ante la eventual falla de un servidor y reponerlo implica instalar desde cero uno nuevo, como puede evidenciarse, este esquema no es suficiente para una restauración efectiva y eficiente cuyo resultado puede incurrir en

omisiones involuntarias deviniendo en complicaciones para el ambiente de producción.

En este sentido, se diseñará el Plan de continuidad de los servicios de TI que se alojan en el Centro de Datos en función de los procesos críticos de la UTMACH y las dependencias de TI de los mismos que apalancan su operatividad y que fueron identificados por la autoridad académica de la Institución.

4.4.2 Infraestructura Del Centro De Datos Alterno

Infraestructura De Red

Las comunicaciones entre el centro de datos principal y alterno, deben ser compatibles a las configuraciones realizadas en el centro de datos principal, esto con el fin de garantizar la conexión directa entre las Unidades Académicas y campus externos por medio de fibra oscura, sea funcional.

Los enlaces hacia cada una de las unidades académicas y el centro de datos alterno se realizarán por medio de enlaces capa 3 hacia la infraestructura alterna, en la siguiente tabla se muestra las configuraciones de IP necesarias para conectar con el sitio alterno.

Tabla 16 Direccionamiento IPv4 para enlaces núcleo-distribución.
Fuente: Los autores

LOCACION	DISTRIBUCIÓN	NÚCLEO - ALTERNO
Medicina	172.30.0.125	172.30.0.126
UACQS	172.30.0.129	172.30.0.130
UACS	172.30.0.133	172.30.0.134
UACE	172.30.0.137	172.30.0.138
UAIC	172.30.0.141	172.30.0.142
UACA	172.30.0.145	172.30.0.146
10 AGOSTO	172.30.0.149	172.30.0.150
CAMPUS MACHALA	172.30.0.209	172.30.0.210

Para la configuración de las rutas hacia las unidades académicas y los servidores desde los equipos de networking en el proveedor alterno, se usará el protocolo RIP el mismo que debe anunciar la red 172.30.0.0/16, aprendiendo las redes declaradas por los switches de distribución de las unidades académicas, y anunciando la red de los servidores.

Los servicios alojados en el centro de datos alterno, deben ser visibles desde el mundo, para esto se deben agregar reglas de NAT que permitan hacer visibles a los servidores de la red interna que publican servicios, en la tabla siguiente se muestra la lista de NAT que debe configurarse en el equipo que haga la traducción de las redes en el proveedor alterno.

1	Exempt	any	172.30.0.112/29 172.30.0.192/28	(outbound)	
2	Static	172.30.0.2		outside	186.3.32.114
3	Static	172.30.0.5		outside	186.3.32.115
4	Static	172.30.0.8		outside	181.198.74.19
5	Static	172.30.0.9		outside	181.198.74.21
6	Static	172.30.0.10		outside	186.3.32.122
7	Static	172.30.0.11		outside	186.3.32.117
8	Static	172.30.0.14		outside	186.3.32.123
9	Static	172.30.0.17		outside	186.3.32.126
10	Static	172.30.0.25		inside	192.168.30.2
11	Static	172.30.0.26		outside	181.198.74.23
12	Static	172.30.0.37		outside	181.198.74.26
13	Static	172.30.0.38		outside	181.198.74.22
14	Static	172.30.0.20		outside	181.198.74.18
15	Static	172.30.0.39		outside	181.198.74.24
16	Static	172.30.0.43		outside	181.198.74.25
17	Static	172.30.0.42		outside	181.39.20.51
18	Static	172.30.0.48		outside	181.39.20.52
19	Dynamic	any		outside	186.3.32.124

Figura 4.1 Captura de Tabla de NAT para los servidores de la DMZ del Firewall. Fuente: Los Autores

Seguridad Perimetral

Parte importante para la seguridad de los servicios, es reducir la superficie de ataque hacia cada uno de los servidores de la infraestructura, esto se logra con la implementación de un firewall de seguridad perimetral, que mediante reglas establecidas permita o no el acceso a puertos específicos para cada uno de los servidores, en la tabla siguiente se presentan las reglas para varios de los servidores alojados en la infraestructura virtual, incluidos aquellos que contienen a los servicios críticos.

Tabla 17 Listas de Control de Acceso para los servidores. Fuente: Los autores

SERVIDOR	ORIGEN	DESTINO	SERVICIO	ACTION
DMZ	Red Admin TIC	172.30.0.0/26	All	ACCEPT
SIUTMACH PORTAL SIUTMACH_PRUEBAS	Red Interna	172.30.0.2/32 172.30.0.41/32 172.30.0.42/32	tcp/80 tcp/443	ACCEPT
BASELOCAL	172.30.0.2/32 172.30.0.41/32 172.30.0.42/32	172.30.0.3/32	tcp/5432	ACCEPT
CHAT INTERNO	Red Interna	172.30.0.6	tcp/161, tcp/5222, tcp/5223, tcp/5229, tcp/5269, tcp/5275, tcp/7070, tcp/7443, tcp/9090, udp/3478, udp/3479, udp/5269, udp/snmp	ACCEPT

Servidores Y Almacenamiento

Para la solución de Centro de Datos alterno, se propone la renta de un espacio en un Centro de Datos privado que aloje los servicios críticos de la UTMACH, y que permita la sincronización de la información de las 43 máquinas virtuales alojadas en el centro de datos principal.

Para esto se debe replicar la infraestructura FLEXPOD en el centro de datos alterno, para que contenga los siguientes equipos:

Tabla 18 Equipos que componen la tecnología de servidores FlexPod. Fuente: Los autores

#	TIPO	MARCA	MODELO
1	SWITCH FABRIC INTERCONNECT	CISCO	UCS-SP7-INFR-FI48
2	SWITCH FABRIC INTERCONNECT	CISCO	UCS-SP7-INFR-FI48
3	ALMACENAMIENTO PRINCIPAL –CTL1	NETAPP	FAS2552
4	ALMACENAMIENTO PRINCIPAL –CTL2	NETAPP	FAS2552
5	ALMACENAMIENTO DE RESPALDOS-CTL1	NETAPP	FAS2554
6	ALMACENAMIENTO DE RESPALDOS-CTL2	NETAPP	FAS2554
7	CHASIS	CISCO	UCS-SA-B-CH-201
8	SERVER BLADE	CISCO	UCS-SP7-SR-B200-V
9	SERVER BLADE	CISCO	UCS-SP7-SR-B200-V
10	SERVER BLADE	CISCO	UCS-SP7-SR-B200-V
11	SERVER BLADE	CISCO	UCS-SP7-SR-B200-V

Para la virtualización de los servicios críticos se debe usar VMWARE mínimo en su versión Academic, cuyas licencias deben estar configuradas de la siguiente manera:

Tabla 19 Licenciamiento VMware. Fuente: Los autores

#	ELEMENTO	MARCA	CANT.	LICENCIA
1	vCENTER	vMWARE	1	Academic vMWARE vCENTER Server 5 Standard for vSphere 5 (Per Instance)
2	vSPHERE	vMWARE	8	Academic vMWARE vSPHERE 5 Standard for 1 processor

Las 8 licencias de vSPHERE, serán instaladas en los 4 servidores CISCO que poseen 2 procesadores cada uno.

Para la realización de la réplica del storage se usará SNAPMIRROR, tecnología de NETAPP que permite realizar respaldos asíncronos, por lo que es necesario contar con mínimo dos controladoras FAS2552, con las mismas capacidades en espacio y volúmenes existentes en el Centro de Datos principal, según el detalle mostrado en la siguiente tabla, cada volumen contiene la data de las MV incluyendo a las de los servicios críticos.

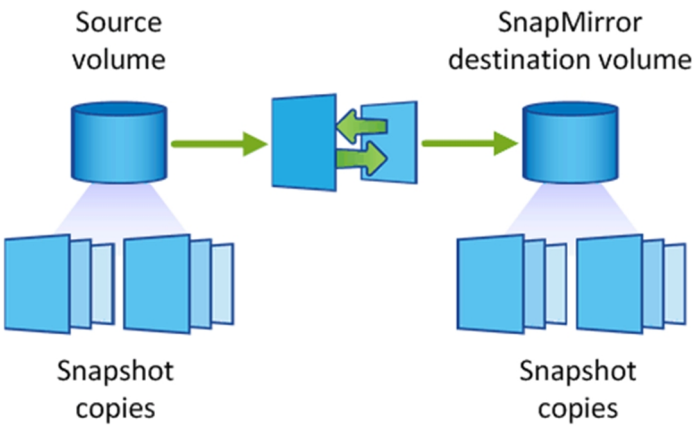


Figura 4.1 Esquematización de Snapmirror NetApp. Fuente: OnCommand Cloud Manager Documentation Center

Tabla 20 Volúmenes con su capacidad por controladora. Fuente: Los autores

Controladora	Volumen	Capacidad
FAS2552 – CTL 1	/vol/vol0	500 GB
	/vol/VOL_VMWARE_1	1.5 TB
	/vol/VOL_VMWARE_2	1.5 TB
	/vol/VOL_VMWARE_3	1 TB
FAS2552 – CTL 1	/vol/vol0	500 GB
	/vol/VOL_VMWARE_4	1.2 TB
	/vol/VOL_VMWARE_1	1.5 TB
	/vol/VOL_VMWARE_3	1.2 TB

Procedimiento para activación de SNAPMIRROR

Por medio de la red MPLS del proveedor del centro de datos alterno, se realiza la conectividad entre las controladoras, estas deben estar configuradas dentro del mismo segmento de red 172.30.1.64/27 al que pertenecen las controladoras del centro de datos principal. En las tablas

siguientes se muestran las VLAN's y el direccionamiento IP propuesto para las controladoras en el centro de datos alterno.

Tabla 21 VLAN'S para el tráfico de los servidores y su administración. Fuente: Los autores

VLAN	DESCRIPCION	RED
99	DMZ	172.30.1.0/26
100	ADMINISTRACION	172.30.1.64/27

Tabla 22 Direccionamiento de las controladoras Fuente: Los autores

Almacenamiento principal en centro de datos Alterno				
DIRECCION IP	**MASCARA DE RED**	**PUERTA DE ENLACE**	**NOMBRE DE EQUIPO**	**DETALLE**
172.30.1.72	255.255.255.224	172.30.1.65	ALT-FAS2552-CTL1	FAS2552 Controlador 1 Alterna
172.30.1.73	255.255.255.224	172.30.1.65	ALT-FAS2552-CTL2	FAS2552 Controlador 1 Alterna

Una vez configurados los datos de red y se haya establecido la comunicación, se puede proceder a activar el snapmirror desde la controladora alterna, para esto se deben ejecutar el siguiente comando ***Snapmirror initialize –S UTM-FAS2552-CTL1: /vol/VOL_VMWARE_1 ALT-FAS2552-CTL1: /vol/VOL_VMWARE_1.***

Una vez activo el snapmirror debe comprobarse que la relación se encuentre establecida, para esto se debe ejecutar el comando ***Snapmirror status***

El status en la salida del comando debe indicar *Snapmirrored* con esto se confirma que el procedimiento se ejecutó correctamente.

Estos pasos se deben seguir para cada uno de los volúmenes existentes en ambas controladoras principales, con esto se garantiza que toda la data se encuentre respaldada en el sitio alterno.

Para establecer un RTO de 5 minutos, se debe configurar un S*chedule* que indicará al sistema de almacenamiento, cada que tiempo debe realizarse la transferencia de los datos entre el cetro de datos principal y el centro de datos alterno, para esto se siguen los siguientes pasos:

- Se edita el archivo */etc/snapmirror.conf,* y
- Se ingresa la siguiente línea *0-59/5 * * **

Con esto el sistema realizará la transferencia de los datos cada 5 minutos.

4.4.3 Comité De Contingencia, Roles Y Responsabilidades

La gestión de la continuidad de los servicios necesita de una estructura organizacional, que se encargue de promover el desarrollo de los lineamientos establecidos para el presente estudio. A continuación se enuncian los integrantes del comité de contingencia y el rol que desempeñan:

Tabla 23 Definición de Roles del Comité de contingencia Fuente: Los autores

COMITE DE CONTINGENCIA	ROLES DE CONTINGENCIA
DIRECTOR DE PLANIFICACION	DIRECTOR DE CONTINUIDAD

COMITE DE CONTINGENCIA	ROLES DE CONTINGENCIA
VICERRECTOR ACADEMICO	DIRECTOR ALTERNO DE CONTINUIDAD
DIRECTOR ADMINISTRATIVO	LIDER DE ADMINISTRACION/RECUPERACION INFRAESTRUCTURA FISICA
DIRECTOR DE TIC	LIDER DE RECUPERACION TECNOLÓGICA
ANALISTA DE TIC 3 **ANALISTA DE SISTEMAS 1**	COORDINADORES DE RECUPERACION
ANALISTA DE MANTENIMIENTO 1 **VIP TELCONET**	TAREAS DE APOYO, CONTROL Y CUMPLIMIENTO
DIRECTOR DE COMUNICACIONES	ASESOR DE COMUNICACIONES

En el caso de que el comité decida activar el plan de continuidad de los servicios, tiene la posibilidad de convocar a otros funcionarios responsables de la ejecución de actividades que impactan las operaciones del Centro de Datos.

En ese sentido, se describen a continuación los roles y responsabilidades de los integrantes del comité en lo referente al plan de continuidad de los servicios; cabe indicar que aquellos nombrados como alternos tienen las mismas responsabilidades de los principales.

Director De Continuidad

El Director de continuidad es el responsable de dirigir y liderar todas las actividades del plan de continuidad de los servicios, así como de declarar

la contingencia ante un escenario de interrupción para el Centro de Datos, en base a decisiones tomadas por el comité o en alguna situación donde amerite realizar la activación inmediata.

Responsabilidades

- Delegar expresamente en el Comité, la responsabilidad de la actualización, mantenimiento y pruebas del plan de continuidad.

- Evaluar y aprobar los recursos que son necesarios para establecer y mantener la estrategia de recuperación.

- Liderar las reuniones del comité

- Monitorear los reportes sobre el estado de la recuperación o evaluación durante la crisis.

- Velar por la realización del análisis causal del evento que originó la activación del plan de continuidad.

Líder De Recuperación Tecnológica

Se encarga de liderar las tareas que impliquen la recuperación tecnológica, apoyándose en las estrategias de continuidad

implementadas. Apoya las Decisiones tomadas por el Director de Continuidad, durante la declaración y activación de la contingencia; además, tiene la responsabilidad de ser el contacto directo entre la Dirección de Tecnologías y el Comité de Contingencia.

Responsabilidades

- Liderar las tareas que impliquen la recuperación tecnológica, apoyándose en las estrategias de continuidad implementadas.

- Realizar un análisis de riesgos de aspectos tecnológicos que afecten la continuidad de la operación normal de la organización y que puedan evidenciar falencias del plan de continuidad.

- Establecer y mantener constante comunicación entre los coordinadores de recuperación del negocio durante el evento de contingencia.

- Mantener la comunicación con los proveedores en los temas o servicios que le competen, sobre el estado de contingencia en el que se encuentra la entidad, siempre y cuando haya sido autorizado por el Director de Continuidad, apoyándose con la Dirección de Comunicación para elaborar los comunicados.

- Elaborar reportes que indiquen el estado de los trabajos de recuperación, al comité de contingencia

Líder De Administración / Recuperación De Infraestructura Física

El Líder administrativo colabora con la coordinación de los aspectos logísticos internos cuando se active el plan de continuidad de los servicios. Es el responsable de gestionar el suministro de los elementos esenciales para garantizar el desarrollo de las operaciones.

Responsabilidades

- Coordinar el suministro de los elementos esenciales como transporte, recursos de infraestructura, entre otros.

- Mantener informado al comité sobre los posibles incidentes por la no disponibilidad de suministros.

Coordinadores De Recuperación

Los Coordinadores de recuperación son aquellos encargados de liderar la recuperación de los procesos críticos, tomando como base las

estrategias de contingencia. Colaboran con al decisiones tomadas por el Director de Continuidad y el comité, durante la activación del plan.

Responsabilidades

- Liderar las reuniones del equipo de recuperación, con la finalidad de realizar el diagnóstico y evaluación de las interrupciones que afectan directamente a la prestación del servicio.

- Ejecutar el plan de continuidad.

- Mantener comunicación constante durante la activación y ejecución del plan de continuidad.

- Colaborar con la comunicación a los usuarios, sobre el estado de los procesos.

- Entregar los reportes correspondientes al comité

Responsable De Tareas De Apoyo Y Control

- Realizar las actividades que le sean asignadas, durante la declaración de emergencia.

Asesor De Comunicaciones

Tiene la responsabilidad de asesorar en la comunicación del evento de interrupción, tanto a nivel interno como externo.

Responsabilidades

- Asesorar al comité y al Director de continuidad para la comunicación durante la crisis.

CAPÍTULO 5

DESARROLLO Y PRUEBAS

5.1 Desarrollo De La Estrategia Para El Plan De Continuidad Del Servicio

El Plan de continuidad de TI debe estar alineado al Plan de Continuidad del negocio, a fin de asegurar su consistencia.

El análisis de las estrategias de continuidad debe realizarse considerando los objetivos estratégicos de la organización, respecto a las 3 dimensiones fundamentales para la disponibilidad: Datos, Infraestructura Tecnológica y Personal (Gente)

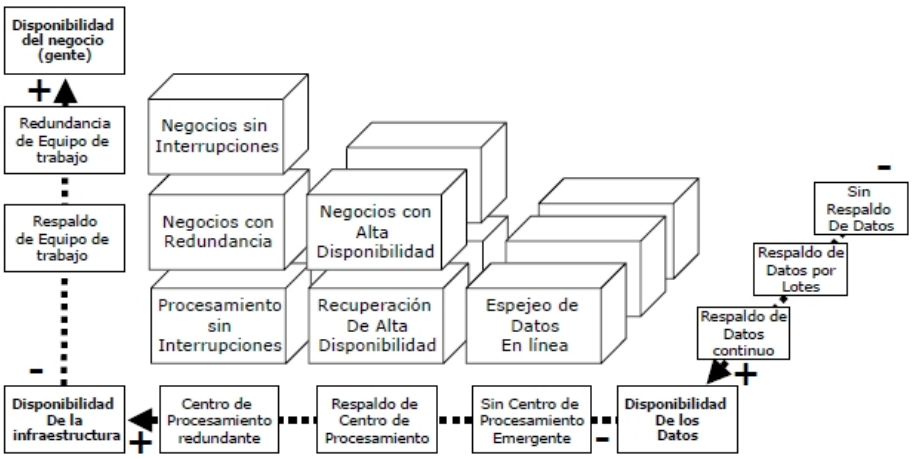


Figura 5.1 Esquema de la estrategia de continuidad de los servicios de TI. Fuente: Itil v3 edición 2011

El desarrollo de la estrategia de continuidad de los servicios de TI que se alojan en el centro de datos de la UTMACH, tuvo como enfoque metodológico:

1. Identificar los procesos críticos del negocio, para lo cual se realizó una entrevista a la autoridad académica (vicerrectora académica).

2. Mapeo de servicios de TI asociado a procesos críticos.

3. Elaboración del Análisis de impacto del negocio (BIA) referente a las dependencias de TI identificadas en el punto 3. El BIA obtenido como resultado se encuentra citado en el punto 4.3 del presente estudio.

4. Elaboración de la matriz de Riesgos para las dependencias de TI identificadas en el punto 3. La matriz de riesgos obtenida como resultado, se encuentra citada en el punto 4.2 del presente estudio.

5.1.1 Centro De Datos Alterno Del Proveedor

Luego de realizado el análisis de impacto (BIA) y el análisis de riesgos se propone la contratación a un tercero de un servicio de centro de datos alterno fuera de la ciudad de Machala en modo activo – pasivo, que permita replicar toda la información del centro de datos primario al sitio alterno, permitiendo recuperar las operaciones en caso de que el centro de datos primario no esté operativo por un periodo prolongado de tiempo.

El centro de datos alterno debe cumplir con las características en lo referente a: Seguridad, condiciones físicas, ambientales, eléctricas, etc. Que permitan garantizar la operación y continuidad del sistema académico SIUTMACH ante la falla o pérdida del centro de datos primario.

El detalle de los servicios que debe cumplir un centro de datos, de lista a continuación:

Centro De Datos

Debe garantizar la disponibilidad y continuidad de los servicios de TI, además de ser tolerante a fallos, permitir escalamiento en número de servidores, debe contar con:

- Centro de operaciones de seguridad, SOC por sus siglas en inglés (Security Operations Center).
- Seguridad física con vigilancia 7x24x35.
- Detección y extinción de incendios.
- Respaldo de energía eléctrica con plantas eléctricas redundantes.
- UPS redundantes.
- Climatización con sistema de aires redundantes.

Hosting Virtual

Se debe soportar el aprovisionamiento de servidores virtuales bajo demanda, gestionados por el proveedor o gestión compartida entre cliente y proveedor.

Para el aprovisionamiento de las máquinas virtuales y el respaldo de la información se debe contar con infraestructura similar a la del centro de datos principal, a continuación, se detalla el equipamiento necesario para cumplir con lo requerido:

Tabla 24 Equipamiento necesario para aprovisionamiento de máquinas virtuales Fuente: Los autores

Cant.	Equipo	Función
2	Switches Fabric Interconnect UCS6248	Permiten la comunicación de los servidores con el almacenamiento
1	Chasis UCS5108	Aloja los servers Blades
4	Servidores tipo Blade UCS B200 M3	Servidores
1	Equipo NetApp FAS2552	Almacenamiento Transaccional
1	Equipo NetApp FAS2554	Almacenamiento de Respaldos
1	Licencia para VMware VCenter	
4	Licencias para VMWare VSphere	

A continuación, se muestra el esquema de conexión actual, instalado en el centro de datos de la UTMACH y propuesto para el centro de datos alterno.

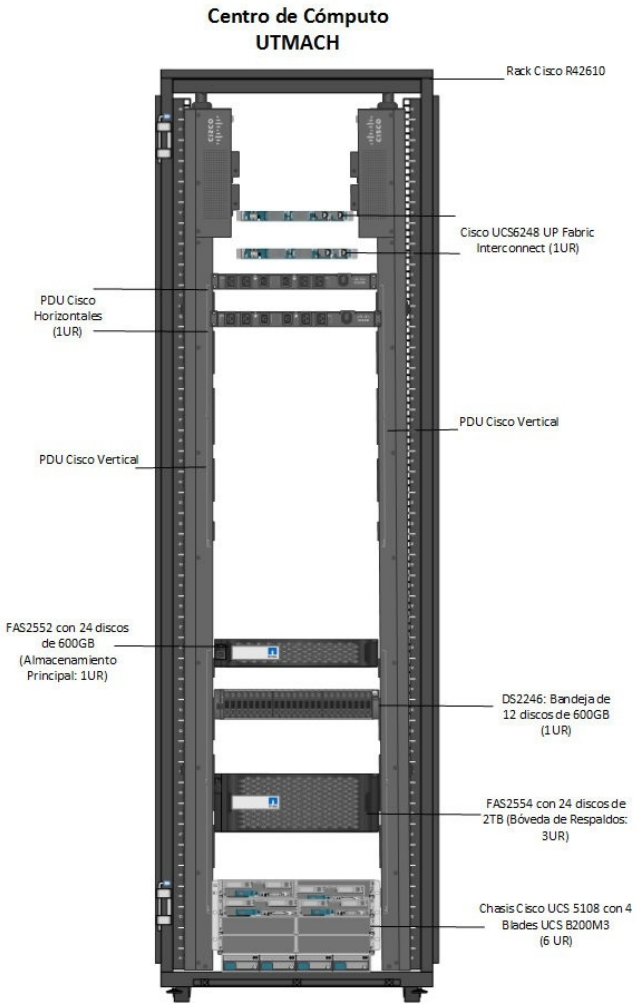


Figura 5.2 Esquema de conexión dual. Fuente: Los autores

Monitoreo

Se debe mantener un servicio de monitorio 7x24x365, de los equipos activos e infraestructura de servidores, emitiendo reportes semanales que permitan conocer su estado, incidentes ocurridos, planes de prevención.

Seguridad

El proveedor debe administrar el servicio de seguridad, que debe estar compuesto por un firewall principal con monitoreo constante, soporte técnico 7x24x365, todo integrado en un Centro de operaciones de seguridad, SOC por sus siglas en inglés (Security Operations Center).

5.1.2 Centro De Respaldos En La Nube

A fin de garantizar las copias de seguridad del sistema académico (SIUTMACH), el cual engloba a todos los procesos críticos identificados por la autoridad académica, será necesario contar en el Centro de Datos Alterno con un esquema de respaldos que permita obtener:

- Garantizar velocidad de acceso y transferencia, disponibilidad y redundancia de la información bajo demanda.

- Respaldo online e incrementales de archivos, carpetas, servidores, aplicaciones y bases de datos que conforman el sistema académico (SIUTMACH).

- Paneles de control que permitan configurar preferencias, programar copias de seguridad, estadísticas de uso, monitoreo, reportes, etc.

- Protección de datos continua, Restaurar la última versión y seguir obteniendo copias de la información, aunque se presente o materialice una amenaza antes de respaldar la información.

- Compresión opcional de las copias de seguridad de la información que permitan aumentar la velocidad y optimizar el consumo del medio.

- Restauración de la última copia realizada o desde hace un año atrás.

- Agentes disponibles que permitan obtener copias de seguridad consistentes para bases de datos tales como: Oracle, SQLSERVER, MySQL, PostgreSql.

- Clientes compatibles con sistemas operativos estándar tales como: Windows y Linux.

5.1.3 Proveedor Alterno De Internet

Para contar con un enlace de Internet y Datos alterno, la UTMACH deberá acogerse al Acuerdo Ministerial 141 publicado en el registro oficial 459

del 31 de mayo del 2011 (ver anexo A1), que en su artículo 1 establece que: “Cuando demanden la contratación de servicios de Telecomunicaciones (telefonía fija, servicio móvil avanzado, enlaces de datos), servicios de valor agregado (servicio de internet), y otros servicios vinculados con este ámbito, lo hagan con una empresa pública de Telecomunicaciones, aplicando lo establecido en la Ley Orgánica del Sistema Nacional de Contratación pública y su reglamento general”

Este enlace deberá tener las siguientes características:

- Ancho de banda simétrico para la red alterna de la UTMACH de 100Mbps que pueden ser aumentados de acuerdo a la necesidad.

- Relación 1-1 entre la capacidad de conectividad de última milla y capacidad de acceso a internet. Se debe garantizar la utilización de los canales de las últimas millas de los enlaces al 100%.

- Servicio de internet sin ningún tipo de restricción ni bloqueo de puertos por parte del proveedor. Todos los servicios asociados al protocolo IP deberán estar sin restricción.

- Redundancia en los enlaces con proveedor local.

- Conmutación automática entre enlaces de última milla, dado el caso de fallas, en un tiempo máximo de 45 segundos.

- Al obtener 100% de paquetes perdidos en un canal no congestionado durante una muestra de 5 minutos continuos, se considerará el enlace como caído, convirtiéndose en una interrupción de servicio para propósitos de aplicación de los acuerdos de nivel de servicio.

- La disponibilidad del servicio, será como mínimo un 99,92% mensual, calculado sobre un mes de 720 horas.

5.1.4 Plan De Comunicaciones

El Plan de continuidad de los servicios de TI que aloja el Centro de Datos de la UTMACH, debe ser concebido como un proyecto, el mismo que sugerimos, deberá ser gestionado mediante las mejores prácticas establecidas por el PMI (Project Management Institute), a través de la guía PMBOK (Project Management Body of Knowledge), que, para el plan de comunicaciones, contempla el formato definido en el anexo: “Plan de comunicaciones”

5.2 Prueba De Conectividad Con El Centro De Datos Alterno Del Proveedor

La conectividad con el centro de datos alterno se realizará, siguiendo el esquema de comunicación mostrado en la Figura <#Figura>, que detalla las líneas de comunicación existentes en el modelo de Centro de datos alterno.

Al mantenerse una réplica asíncrona tanto del storage como de la base de datos, en el centro de datos alterno del proveedor, se asegura el acceso al SIUTMACH a través de internet, luego de realizar cambios a nivel físico y lógico desde la capa de distribución de las Unidades Académicas y edificio de Rectorado de la UTMACH.

Para realizar los cambios físicos y lógicos desde la red interna de la UTMACH, se seguirán los siguientes pasos:

1. Contacto con soporte VIP de proveedor alterno para comunicar inicio de trabajos de cambio de enlaces a centro de datos alterno.

2. Desconexión de ruta principal de fibra (interna) en puerto TenGiga de switch de distribución.

3. Conexión de fibra oscura (Proveedor) en puerto TenGiga de switch de distribución.

4. Pruebas de conexión con punto remoto por medio del protocolo ICMP.

5. Prueba de conexión con internet por medio de protocolos ICMP.
   a. Ping 8.8.8.8
   b. traceroute 8.8.8.8

6. Detención de réplica entre centro principal y alterno.

7. Levantar la base de datos, volúmenes, Luns (Réplica de Storage).

8. Acceso por SSH a máquina virtual que aloja SIUTMACH en proveedor alterno.

9. Acceso por SSH a máquina virtual que aloja BD de SIUTMACH en proveedor alterno

10. Activación de réplica desde sitio alterno hacia sitio principal.

Registro De Conectividad A Centro De Datos Principal

1. Contacto con soporte VIP de proveedor alterno para comunicar inicio de trabajos de cambio de enlaces a centro de datos principal.

2. Detención de todos los servicios en sitio alterno.

3. Desconexión de fibra oscura (Proveedor) de puerto TenGiga de switch de distribución.

4. Conexión de ruta principal de fibra (interna) en puerto TenGiga de switch de distribución.

5. Pruebas de conexión con centro de datos principal por medio del protocolo ICMP.

6. Prueba de conexión con internet por medio de protocolos ICMP.
   a. Ping 8.8.8.8
   b. traceroute 8.8.8.8

7. Detención de réplica desde sitio alterno a sitio principal.

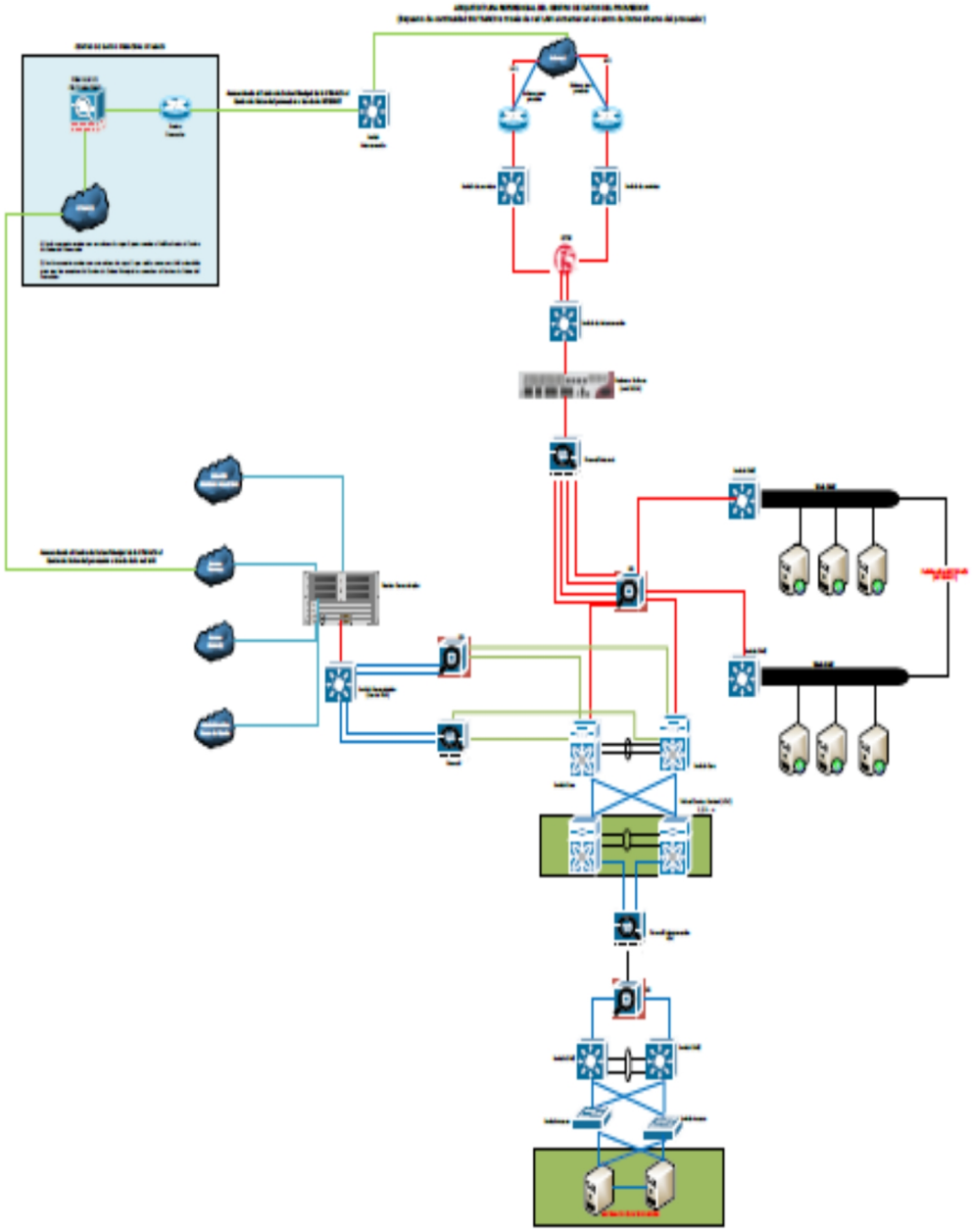
8. Levantar la base de datos, volúmenes, Luns (Réplica de Storage).

9. Acceso por SSH a máquina virtual que aloja SIUTMACH en proveedor principal.

10. Acceso por SSH a máquina virtual que aloja BD de SIUTMACH en proveedor alterno.

11. Activación de réplica entre sitio principal y alterno.

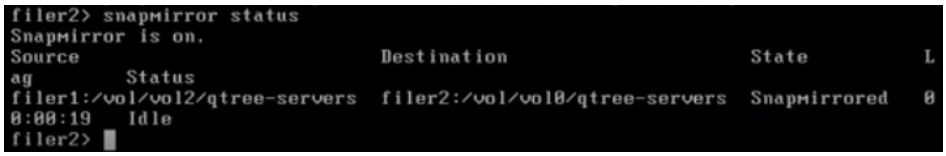
Diagrama Del Centro De Datos Alterno



5.3 Prueba De Actualización De Información De Respaldo En La Nube

Una vez que se hayan concluido las tareas de enlace al centro de datos alterno, se procede a realizar las pruebas de actualización de información de respaldo en la nube, las pruebas se pueden realizar para uno de los volúmenes, para esta prueba se usará el volumen "/vol/VOL_VMWARE_2" para esto se deben seguir los siguientes pasos:

1. Con el comando *snapmirror status*, se verifica que el estado se encuentre "*snapmirrored".*



2. Se ejecuta el comando *snapmirror quiesce* para esperar que procesos snapmirror que se estén ejecutando se completen y luego se interrumpa futuras actualizaciones.

3. Se verifica con *snapmirror status* que el status de todos los snapmirror sea "*Quiesced"*

```
filer2> snapmirror status
Snapmirror is on.
Source                          Destination                   State          L
ag        Status
filer1:/vol/vol2/qtree-servers  filer2:/vol/vol0/qtree-servers  Quiesced       0
0:01:56   Idle
filer2>
```

4. Para romper la relación de snapmirror entre el almacenamiento principal y el alterno utilizamos el comando *snapmirror break /vol/VOL_VMWARE_2*, con esto el sistema nos indicará que el volumen en el sitio alterno es ahora escribible.

```
filer2> snapmirror break /vol/vol0/qtree-servers
snapmirror break: Destination /vol/vol0/qtree-servers is now writable.
filer2>
```

5. Verificar el estado de la relación de snapmirror, este debe estar en Broken-off.

```
filer2> snapmirror status
Snapmirror is on.
Source                          Destination                   State          L
ag        Status
filer1:/vol/vol2/qtree-servers  filer2:/vol/vol0/qtree-servers  Broken-off     0
0:04:31   Idle
filer2>
```

6. Como paso final presentar las LUNS del volumen a probar a los servidores en el centro de datos alterno.

5.4 Prueba De Enlace De Internet Con El Proveedor Alterno

Para la realización de estas pruebas, se debe mantener un monitoreo permanente del estado del enlace con el proveedor de internet alterno; cuando este se encuentre operativo, realizamos lo siguiente:

Perdida de enlace de internet con proveedor principal

1. Levantar en el Firewall de borde la interfaz Giga que tenga conectado el enlace con el CPE del proveedor de internet alterno.

2. Cambiar en el ASA la ruta de salida al mundo hacia la IP asignada por el proveedor alterno, con el comando *route outside <0.0.0.0 0.0.0.0> <ip_CPE_proveedor_alterno>*.

3. Cambiar en el nat de la interfaz inside el pool de direcciones del proveedor principal por el pool de direcciones del proveedor alterno.

4. Prueba de conexión con internet por medio de protocolos ICMP.
   a. Ping 8.8.8.8
   b. traceroute 8.8.8.8

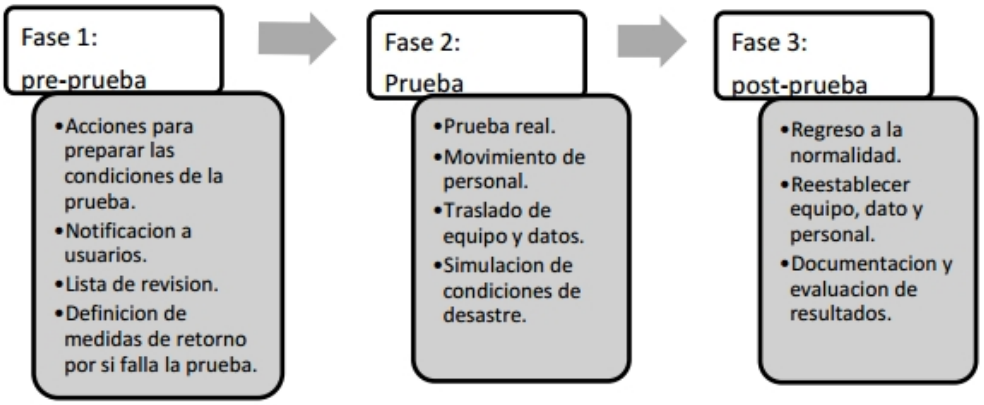
5.5 Prueba Del Plan De Comunicaciones

Para la prueba del plan de comunicaciones definido en el ítem 5.1.4 del presente estudio, se procederá de inicio con la definición de la matriz RACI, con todo el personal involucrado cuando una amenaza o riesgo se materialice, a fin de activar el plan de continuidad propuesto.

Al ser un plan de pruebas propuesto para el plan de continuidad propuesto en el presente estudio, las pruebas del mismo serán medidas conforme a la matriz RACI establecida y de acuerdo al indicador que se definirá en el ítem 6.4 del presente estudio.

5.6 Prueba Integral Del Plan De Continuidad De Los Servicios

Para realizar una prueba integral del plan de continuidad de los servicios de TI que se alojan en el Centro de Datos de la UTMACH, proponemos el siguiente esquema:



CAPÍTULO 6

MODELOS PARA LA EVALUACIÓN DE RESULTADOS

Los datos operacionales son observaciones básicas, pueden ser por ejemplo de eventos operacionales que se extraen de las herramientas del área de TIC, son el punto de arranque del modelo y serán usadas para el cálculo de los indicadores clave de rendimiento (KPI por sus siglas en inglés).

Los KPI son métricas usadas para proveer una información básica para una toma de decisión. Los KPI's son calculados a partir de uno o más datos operacionales. El resultado de ese cálculo se compara con el rango de tolerancia, para identificar si el resultado se encuentra dentro máximo y mínimo. Definir la tolerancia es crítico ya que nos indican cuando hay que entrar en acción y tomar medidas de gestión.

6.1 Conectividad Con El Centro De Datos Del Proveedor

Para la evaluación de esta prueba se considerará indicadores clave de rendimiento (KPI), que permitirán determinar, si las acciones tomadas para mantener la alta disponibilidad de los servicios son suficientes o se debe realizar cambios al contrato del servicio para el centro de datos alterno del proveedor.

A continuación, el detalle de los KPI para esta prueba.

Tabla 25 Detalle del KPI para la prueba de conectividad con el Centro de Datos Alterno. Fuente: Los autores

Indicador	Descripción	Meta KPI	Responsable
Porcentaje de pruebas exitosas de conectividad con el centro de datos alterno.	Porcentaje medido de acuerdo al número de pruebas planificadas durante un periodo de tiempo (anual), sobre el número de pruebas completadas a satisfacción.	100%	Analista de TIC 3
Porcentaje de interrupción debido a incidentes (indisponibilidad no planificada)	Porcentaje de interrupción (indisponibilidad) debido a incidentes en el entorno de TI, en relación con las horas de servicio.	<20%	Analista de TIC3
Número de interrupciones del negocio debido a incidentes TI	Entrega de servicios de TI de acuerdo a requisitos del negocio	0	Analista de TIC 3

6.2 Integridad De Las Actualizaciones En La Nube Del Proveedor

La evaluación de la integridad de las actualizaciones se realizará tanto para la infraestructura virtual almacenada en un storage, como para cada base de datos respaldada. Se tomará en cuenta que la sincronización o replicación deberá ser cumplida según los parámetros (frecuencia) establecidos y apoyada por la creación de respaldos de información para cada una de las bases de datos.

A continuación, el detalle de los KPI para esta prueba:

Tabla 26 Detalle del KPI para la prueba de actualizaciones en la nube.
Fuente: Los autores

Indicador	Descripción	Meta KPI	Responsable
Porcentaje de sincronizaciones exitosas de la información a la nube del proveedor	Porcentaje obtenido del número de sincronizaciones exitosas sobre el número de veces programadas que se realiza la tarea de sincronización de la información del sitio principal al sitio alterno	100%	Analista de TIC 3
Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información.	Número de veces que el negocio ha tenido que interrumpir sus operaciones debido a indisponibilidad de la información	0	Analista de TIC 3 Analista de Sistemas I
Promedio de imágenes virtuales por administrador	Promedio de imágenes virtuales por administrador. Según IDC, el promedio de la VM a la proporción de administrador, o el promedio de imágenes virtuales por administrador, es de 200.	<200	Analista de TIC 3

Número de backups restaurados y sometidos a prueba de legibilidad de la información	*Número de backups restaurados y sometidos a prueba de legibilidad de la información*		Analista de TIC 3

6.3 Conectividad A Internet Con El Proveedor Alterno

Para el caso de la conectividad a internet por medio del proveedor alterno, las pruebas a realizarse se enfocan en determinar:

Tabla 27 Detalle del KPI para la prueba de conectividad con el proveedor alterno de internet. Fuente: Los autores

Indicador	Descripción	Meta KPI	Responsable
Disponibilidad (excluyendo el tiempo de inactividad previsto)	Porcentaje del tiempo de actividad real (en horas) del equipo en relación con el número total de horas de funcionamiento previstas (en horas). Tiempo de funcionamiento previsto = horas de servicio - tiempo de inactividad previsto El tiempo de inactividad previsto es el tiempo de inactividad programado para el mantenimiento. También conocido como: Service Outage Duration	100%	Analista de TIC 3
Porcentaje de solicitudes de servicio debido a pobre rendimiento	Porcentaje de solicitudes de servicio debido al mal desempeño de los servicios		Analista de TIC 3

	prestados a los clientes finales.		
Número de incumplimientos SLA debido al mal desempeño	Número de violaciones del Acuerdo de Nivel de Servicio (SLA) debido al mal desempeño	0	Analista de TIC 3

6.4 Efectividad De Las Comunicaciones

La efectividad de las comunicaciones, determinará el éxito o fracaso de las tareas del plan de continuidad de servicios. A continuación, el detalle de los KPI para esta prueba.

Tabla 28 Detalle del KPI para la efectividad de las comunicaciones. Fuente: Los autores

Indicador	Descripción	Meta KPI	Responsable
***Porcentaje de funciones con descripciones de posición documentadas*:**	Porcentaje de roles con descripciones documentadas de posición y autoridad.	100%	Director de TH
Tiempo promedio de respuesta a incidentes	La cantidad media de tiempo (por ejemplo, en minutos) entre la detección de un incidente y la primera acción tomada para reparar el incidente.		Analista de TIC 3
Tiempo transcurrido entre ocurrencia de deficiencia de control interno y presentación de informes	Tiempo transcurrido entre la ocurrencia de la deficiencia del control interno y la presentación de informes.		Analista de TIC 3

CONCLUSIONES Y RECOMENDACIONES

1. El centro de datos de la Universidad Técnica de Machala, mantiene una infraestructura que le permite cumplir con los requerimientos de operación básicos de la Institución, sin embargo, no cuenta con procedimientos estandarizados de recuperación de los servicios que brinda, es decir, ante un evento de disrupción grave, no podrá mantener la disponibilidad de los mismos.

2. La elaboración del catálogo de servicios permitió identificar los servicios que presta el centro de datos y su alcance, el cual se utilizó como insumo para el diseño del presente plan de continuidad de los servicios.

3. Mediante la combinación de ITIL v3 edición 2011 y COBIT 5, y su enfoque en las actividades que garantizan la continuidad de los servicios de TI y con cada

objetivo de control involucrado se logró diseñar el plan de continuidad de los servicios

4. Como resultado del diseño del plan de continuidad de los servicios, se dejan enunciados varios proyectos para futuras implementaciones, quedando como recomendaciones en el presente trabajo.

5. Con el diseño del plan de continuidad de los servicios, se deja un documento de preparación para la Universidad Técnica de Machala que servirá como estrategia de recuperación de los servicios y por lo tanto de los procesos identificados como críticos.

6. De acuerdo al mapa de calor, varios de los riesgos que tienen relación con los servicios que soportan los procesos críticos se encuentran en un nivel alto por lo tanto son los que deben ser controlados y minimizados en el menor tiempo posible

7. Al ser la academia la principal actividad de la Universidad Técnica de Machala, se involucró principalmente al Vicerrectorado Académico y por su intermedio a las demás autoridades quienes son conscientes de la importancia del presente

plan de continuidad de los servicios, lo que garantiza su implementación en el mediano plazo.

8. Implementar un modelo de red segura, que permita proteger la transmisión de la información además de facilitar la gestión y el monitoreo del tráfico que se produce en la red LAN y WAN de la Universidad Técnica de Machala.

9. Implementar una solución de centro de datos alterno, la misma que para minimizar costos y solventar la falta de personal en la unidad de redes, debe ser en modo servicio con un proveedor de servicios de centro de datos dentro del País.

10. Desarrollar un Plan Estratégico de Tecnologías de la Información y comunicación (PETIC) que permita la optimización de los recursos tecnológicos informáticos, una visión de mediano y largo plazo respecto al uso de la tecnología informática como elemento básico para apoyar las estrategias de la Universidad, y oriente en aspectos de sistemas de información y tecnología con los que la Institución pueda lograr las metas y objetivos.

11. Definir e implementar acuerdos de nivel operacional (OLA) y acuerdos de nivel de servicio (SLA) para los servicios que presta el centro de datos.

BIBLIOGRAFÍA

[1] Universidad Técnica de Machala, Manual Institucional, Editorial Universitaria 3era Edición, 2013

[2] Aguilar F., Historia de la Universidad Técnica de Machala, Editorial Universitaria 2da Edición, 2009

[3] CEAACES, Informe General sobre la Evaluación, Acreditación y Categorización de las Universidades y Escuelas Politécnicas, 2014

[4] CEAACES, Resultados de la acreditación y categorización vigentes, http://www.ceaaces.gob.ec/sitio/acreditacion-y-categorizacion/, fecha de consulta octubre de 2016

[5] Llorens Fabregas J., Tecnología de Información, Gerencia de Servicios (Basado En ITIL), 2009

[6] Information Systems Audit and Control Association, COBIT 5 Framework, 2012, pp. 13, 27, 33

[7] Information Systems Audit and Control Association, COBIT 5 Procesos Catalizadores, 2012

[8] AXELOS, Information Technology Infrastructure Library version 2. 2011 edition. Service Design, TSO, 2011

[9] Information Systems Audit and Control Association, The Risk IT Framework, 2009

[10] NIST, NIST SP 800-34 r1 Contingency Planning Guide for Federal Information Systems, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf, fecha de consulta octubre de 2016

[11] Galindo, C., La firma electrónica avanzada y su certificación, Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica, p. 100, 2014

[12] International Organization for Standardization, ISO 27001, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, fecha de consulta octubre 2016

[13] International Organitzation for Standardization, ISO 27000, http://www.iso27000.es/iso27000.html, fecha de consulta octubre de 2016

[14] Telecomunications Industry Association, Advancing Global Comunications, http://www.tiaonline.org, fecha de consulta noviembre 2016

[15] Information Systems Audit and Control Association, COBIT 5 Implementación, 2012

[16] Sánchez, Ó.; Herrero , R.; Hortigüela, M., Gestión auxiliar de documentación económico-administrativo y comercial, 2013

[17] Pacio, G., Data Centers hoy, 2014

ANEXOS

ANEXO A

Catálogo de Servicios

1 Servicios de Conectividad

Provee el acceso de los usuarios a los diferentes recursos de red disponibles tales como impresoras, escáneres, archivos compartidos, aplicaciones de la Institución, así como acceso a fuentes externas de información y acceso remoto a la intranet de los 3 campus.

- **Acceso a Internet**

  Descripción del Servicio

  Se encarga de suministrar y garantizar el acceso al servicio de Internet a la comunidad universitaria, en relación a la actividad que estos desempeñen.

  Tipo de Servicio.

  Servicio General

  Dueño del Servicio

  Analista de Tecnologías de la Información y Comunicación 3

  Administrador del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Procedimiento de solicitud del Servicio

El jefe inmediato superior debe realizar la solicitud formal al Director de Tecnologías de la Información y Comunicación, a través de un oficio o mediante correo electrónico.

Horario de Servicio

Ininterrumpido

1

Horario de Soporte

De Lunes a Viernes de 07:30 a 16:00

Cobertura del Servicio

Campus Principal

Campus Machala

Campus 10 de Agosto

Condiciones de Entrega del Servicio

Los miembros de la comunidad Universitaria que tengan acceso a Internet, deben utilizarlo con fines estrictamente académicos y/o administrativos.

- **Provisión de conectividad interna**

Descripción del Servicio

Se encarga de proveer y garantizar la conectividad de los diferentes recursos disponibles en la red interna, tales como como servidores, estaciones de

trabajo, impresoras, escáneres, entre otros autorizados por la Dirección de Tecnologías de la Información y Comunicación.

Tipo de Servicio

Servicio General

Dueño del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Administrador del Servicio

Personal de Soporte en el Sitio

Procedimiento de solicitud del Servicio

El jefe inmediato superior debe realizar la solicitud formal al Personal de Soporte en el Sitio, y el caso de no haber personal asignado debe solicitarlo al Director de Tecnologías de la Información y Comunicación, a través de un oficio o correo electrónico.

Matriz de Prioridades

Componente	Requerimiento	Prioridad Alta Dirección	Prioridad Niveles Operativos de Apoyo
Internet	Acceso a Internet		
	Eliminación de acceso a Internet		
	Acceso a sitios Web Especiales		

Horario de Servicio

Ininterrumpido

Horario de Soporte

De Lunes a Viernes de 07:30 a 16:00

Cobertura del Servicio

Campus Principal

Campus Machala

Campus 10 de Agosto

Condiciones de Entrega del Servicio

Los usuarios de la comunidad universitaria a quienes se les provea el acceso a la red de la Institución deben utilizarla para fines administrativos y/o académicos de acuerdo a la labor que estos desarrollaran.

- **Provisión de conectividad entre CAMPUS**

Descripción del Servicio

Provee la comunicación de entre las redes de los diferentes campus de la Universidad Técnica de Machala.

Tipo de Servicio

Servicio General

Dueño del Servicio

Analista de Tecnologías de la Información y Comunicación 3 (

Administrador del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Horario de Servicio

Ininterrumpido

Horario de Soporte

De Lunes a Viernes de 07:30 a 16:00

Cobertura del Servicio

Campus Principal

Campus Machala

Campus 10 de Agosto

Condiciones de Entrega del Servicio

Los campus deben mantener algún tipo de relación o convenio con la Universidad Técnica de Machala y estar dentro de un área en la que es posible instalar una conexión de red.

- **Provisión de acceso a las aplicaciones de la Institución**

Descripción del Servicio

Provee el acceso tanto interno como externo de las aplicaciones de la Institución.

Tipo de Servicio

Servicio General

Dueño del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Administrador del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Matriz de Prioridades

Componente	Requerimiento	Prioridad Alta Dirección	Prioridad Niveles Operativos de Apoyo
Aplicaciones	Acceso a los Sistemas	Crítico	Alto
	Revocación de acceso a los Sistemas	Crítico	Alto

Horario de Servicio

Horario Indefinido

Horario de Soporte

De Lunes a Viernes de 07:30 a 16:00

Área Responsable

Tecnologías de la Información y Comunicación

Cobertura del Servicio

Nacional como Internacionalmente

- **Administración de Acceso Externo a equipos fuera del Centro de Datos**

Descripción del Servicio

Se encarga de proveer y garantizar el acceso externo a los equipos ubicados fuera del Centro de datos, que son utilizados en la diferentes Unidades Académicas.

Tipo de Servicio

Servicio bajo demanda

Dueño del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Administrador del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Procedimiento de solicitud del Servicio

El usuario puede ser un docente o personal administrativo de las Unidades Académica, que mediante oficio formal remitido a la Dirección de Tecnologías

de la Información y Comunicación solicita se le proporcione acceso externo al equipo, se evalúa la factibilidad del mismo y se informa sobre el aceptación o negación de la solicitud.

Matriz de Prioridades

Componente	Requerimiento	Prioridad Alta Dirección	Prioridad Niveles Operativos de Apoyo
Equipos	Acceso Externo a Equipos	NA	Medio
	Revocación de acceso a Equipos	NA	Medio

Horario de Servicio

Ininterrumpido

Horario de Soporte

De Lunes a Viernes de 07:30 a 16:00

Cobertura del Servicio

A nivel nacional e Internacional

Condiciones de Entrega del Servicio

En el caso de reportarse alguna anomalía en el equipo por mala administración del mismo al poseer acceso externo, se notificará al usuario por dos ocasiones y a la tercera se revocará el acceso hasta que solvente adecuadamente la seguridad de los equipos

- **Administración de usuarios VPN**

Descripción del Servicio

Se encarga de proveer y revocar el acceso a los usuarios a la intranet a través de un circuito VPN.

Tipo de Servicio

Servicio bajo demanda

Dueño del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Administrador del Servicio

Analista de Tecnologías de la Información y Comunicación 3

Procedimiento de solicitud del Servicio

El usuario puede ser un docente o personal administrativo de las Unidades Académica, 6que mediante oficio formal remitido a la Dirección de Tecnologías de la Información y Comunicación solicita se le proporcione acceso a la intranet, se evalúa la factibilidad del mismo y se informa sobre la aceptación o negación de la solicitud.

Matriz de Prioridades

Componente	Requerimiento	Prioridad Alta Dirección	Prioridad Niveles

			Operativos de Apoyo
Intranet	Acceso	NA	Bajo
	Revocación	NA	Bajo

Horario de Servicio

Ininterrumpido

Horario de Soporte

De Lunes a Viernes de 07:30 a 16:00

Cobertura del Servicio

A nivel nacional e Internacional

Condiciones de Entrega del Servicio

Las credenciales de acceso que son proporcionadas al usuario son entera responsabilidad del mismo, cualquier acción negativa que pueda devenir en el uso inadecuado deberá ser asumida por este.

Servicio de Actualización

- **Actualización de bases de firmas de antivirus**

  Descripción del Servicio

  Este servicio administra, mantiene y actualiza el sistema de antivirus, lo que permite agregar un nivel de protección a la información de la universidad, mitigando ataques de virus, malware y código malicioso.

  Tipo de Servicio

Servicio General.

Dueño del Servicio

Analista de TIC 3.

Administrador del Servicio

Analista de TIC 3.

Procedimiento de solicitud del Servicio

Actualización automática luego de la instalación y configuración del antivirus en las maquinas cliente.

Matriz de Prioridades

Componente	Requerimiento	Matriz de prioridades Alta Dirección	Matriz de prioridades niveles operativos de apoyo
Antivirus	**Instalación**	**Medio**	**Medio**
	Actualización	**Medio**	**Medio**
	Eliminación	**Medio**	**Medio**
	Configuración	**Medio**	**Medio**

Horario de Servicio

24 x 7.

Horario de Soporte

De lunes a Viernes de 7:30 a 16:00.

Tiempos de respuesta

Una vez al día.

Cobertura del Servicio

Se encuentra disponible tanto en el campus principal, y en los 2 campos ubicados en Machala.

Condiciones de Entrega del Servicio

El equipo cliente debe estar ubicado dentro de los predios de la Universidad.

El equipo cliente debe tener instalada y configurada la versión actualizada del antivirus.

- **Actualización de sistemas operativos Windows y Microsoft Office**

Descripción del Servicio

Este servicio administra, mantiene y actualiza los sistemas operativos Windows y Microsoft Office, lo que permite agregar un nivel de protección a la información de la universidad, mitigando posibles amenazas como backdoors o mal funcionamiento de los sistemas operativos y las herramientas ofimáticas.

Tipo de Servicio

Servicio General.

Dueño del Servicio

Analista de TIC 3.

Administrador del Servicio

Analista de TIC 3.

Procedimiento de solicitud del Servicio

Actualización automática luego de la unión del equipo cliente al dominio de la Universidad Técnica de Machala.

Matriz de Prioridades

Componente	Requerimiento	Matriz de prioridades Alta Dirección	Matriz de prioridades niveles operativos de apoyo
WSUS	**Instalación**	**Medio**	**Medio**
	Actualización	**Medio**	**Medio**
	Eliminación	**Medio**	**Medio**
	Configuración	**Medio**	**Medio**

Horario de Servicio

24 x 7.

Horario de Soporte

De lunes a Viernes de 7:30 a 16:00.

Tiempos de respuesta

Una vez al día.

Cobertura del Servicio

Se encuentra disponible tanto en el campus principal, y en los 2 campos ubicados en Machala.

Condiciones de Entrega del Servicio

El equipo cliente debe estar ubicado dentro de los predios de la Universidad.

Cuando exista una actualización que se necesite implementar en los sistemas operativos Windows o Microsoft Office.

Servicios de Colaboración

- Telefonía IP

Descripción del Servicio

Este servicio es multiplataforma, permite la asignación de una extensión telefónica, sobre un PC, Smartphone o algún otro dispositivo inteligente. Permite la comunicación de voz por medio del protocolo IP, utilizando el mismo medio por el que se envían datos, optimizando el uso de la red LAN y las comunicaciones entre las diferentes dependencias de la Universidad.

Tipo de Servicio

Servicio General.

Dueño del Servicio

Analista de Tecnologías de la información y comunicación 3.

Administrador del Servicio

Analista de Tecnologías de la información y comunicación 3.

Procedimiento de solicitud del Servicio

Se solicita mediante oficio de parte del Director, Jefe de Unidad o Delegado al Director de TIC, la creación de una extensión telefónica, la cual es, posterior a su creación, configurada en el dispositivo deseado, en el oficio se debe indicar los siguientes datos de la persona que será responsable de la extensión:

- Nombres completos.
- Unidad a la que pertenece.

Matriz de Prioridades

Componente	Requerimiento	Matriz de prioridades Alta Dirección	Matriz de prioridades niveles operativos o de apoyo
Extensión telefónica	Creación	Crítica	Crítica

Horario de Servicio

24 x 7.

Horario de Soporte

De lunes a Viernes de 7:30 a 16:00.

Tiempos de respuesta

1 segundo.

Cobertura del Servicio

Se encuentra disponible tanto en el campus principal, y en los 2 campos ubicados en Machala.

Condiciones de Entrega del Servicio

El equipo cliente debe estar ubicado dentro de los predios de la Universidad.

El equipo cliente debe tener instalada y configurada la extensión en el dispositivo telefónico.

- Mensajería instantánea

TAREAS

- Definir un plan de actualización de antivirus para las computadoras de la Universidad Técnica de Machala.
- Planificar la ejecución del plan de actualización de antivirus.
- Mantener actualizado el repositorio del servidor de actualización de antivirus.
- Probar el proceso de actualización de antivirus en las computadoras de la Universidad Técnica de Machala.

Descripción del Servicio

Servicio Multiplataforma que mediante una cuenta de usuario en Spark permite la comunicación entre los miembros del personal administrativo vía chat, este sistema es efectivo para mensajes cortos que requieren de respuestas rápidas.

Tipo de Servicio

Servicio General.

Dueño del Servicio

Analista de TIC 3.

Administrador del Servicio

Analista de TIC 3.

Procedimiento de solicitud del Servicio

Se solicita mediante oficio de parte del Director, Jefe de Unidad o Delegado, al Director de TIC, la creación de una cuenta en IMSpark,

la cual es, posterior a su creación, configurada en el dispositivo deseado, en el oficio se debe indicar los siguientes datos de la persona que será responsable de la extensión:

- Número de DNI.
- Nombres completos.
- Unidad a la que pertenece

Matriz de Prioridades

Componente	Requerimiento	Matriz de prioridades Alta Dirección	Matriz de prioridades niveles operativos o de apoyo
Spark	Creación	Media	Crítica

Horario de Servicio

24 x 7

Horario de Soporte

De lunes a Viernes de 7:30 a 16:00.

Tiempos de respuesta

Tiempo real

Cobertura del Servicio

Se encuentra disponible tanto en el campus principal, y en los 2 campos ubicados en Machala.

Condiciones de Entrega del Servicio

El equipo cliente debe estar ubicado dentro de los predios de la Universidad.

El equipo cliente debe tener instalado y configurado el cliente IMSpark.

Servicios de Virtualización

- Provisión de máquinas virtuales

Descripción del Servicio

Alojamiento y soporte de servidores en máquinas virtuales aportando facilidad de gestión, ahorro energético y espacio.

Tipo de Servicio

Servicio bajo demanda.

Dueño del Servicio

Analista de TIC 3.

Administrador del Servicio

Analista de TIC 3.

Procedimiento de solicitud del Servicio

Se solicita mediante oficio de parte del Director, Jefe de Unidad o Delegado, al Director de TIC para la creación de una máquina virtual, se debe indicar la siguiente información:

- Responsable de la mv.
- Uso de la máquina virtual.
- Servicios que se instalaran.
- Puertos adicionales que necesiten los servicios.
- Espacio de almacenamiento en GB.
- Tamaño de memoria RAM.
- Número de VCPU's y cores.
- Sistema Operativo
- Conectividad a internet o red lan

Matriz de Prioridades

Componente	Requerimiento	Matriz de prioridades Alta Dirección	Matriz de prioridades niveles operativos o de apoyo

Servidores	Creación	Crítica	Alta
	Eliminación	Crítica	Alta

Horario de Servicio

24 x 7.

Horario de Soporte

De lunes a Viernes de 7:30 a 16:00.

Tiempos de respuesta

De 1 a 3 días

Cobertura del Servicio

Se encuentra disponible tanto en el campus principal, y en los 2 campos ubicados en Machala.

Condiciones de Entrega del Servicio

- Respaldo de máquinas virtuales

Descripción del Servicio

Servicio de contingencia ante posibles problemas lógicos en las máquinas virtuales.

Tipo de Servicio

Bajo demanda

Dueño del Servicio

Analista de TIC 3

Administrador del Servicio

Analista de TIC 3

Procedimiento de solicitud del Servicio

Se solicita mediante oficio de parte del Director, Jefe de Unidad o Delegado, al Director de TIC para que cree un respaldo de una

máquina virtual a cargo del solicitante. La solicitud debe indicar lo siguiente:

- Nombre de la MV a respaldar
- Periocidad del respaldo (Mensual, semanal, diaria, x horas)

Matriz de Prioridades

Componente	Requerimiento	Matriz de prioridades Alta Dirección	Matriz de prioridades niveles operativos o de apoyo
Respaldo MV	Creación	Media	Alta
	Eliminación	Baja	Media
	Recuperación	Media	Alta

Horario de Servicio

Depende de la periocidad indicada

Horario de Soporte

De lunes a Viernes de 7:30 a 16:00.

Tiempos de respuesta

Diario

Cobertura del Servicio

Se encuentra disponible tanto en el campus principal, y en los 2 campos ubicados en Machala

Condiciones de Entrega del Servicio

La máquina virtual debe estar alojada en el Centro de Datos de la UTMACH

El almacenamiento estará sujeto a las condiciones de almacenamiento existentes en la infraestructura de la UTMACH

5 Servicios Generales

- Monitorización de servidores y equipos de red

Descripción del Servicio

Servicio que recolecta, analiza y utiliza la información de los dispositivos activos de red y de los servidores instalados en el Data Center, para conocer cómo, cuándo y dónde se suceden las actividades, quien las ejecuta y a quienes beneficia.

Tipo de Servicio

Servicio General

Dueño del Servicio

Analista de TIC 3

Administrador del Servicio

Analista de TIC 3

Procedimiento de solicitud del Servicio

El responsable del servicio, o dispositivo que se desea sea monitorizado, debe solicitar a la Dirección de TIC, que se agregue el dispositivo al sistema de monitoreo, indicado lo siguiente:

- Nombre del elemento
- Tipo de elemento
- Ubicación del elemento
- Servicios que se desea monitorear

Matriz de Prioridades

Componente	Requerimiento	Matriz de prioridades Alta Dirección	Matriz de prioridades niveles operativos o de apoyo
Dispositivos de red	Monitoreo	Media	Alta
Servicios	Monitoreo	Media	Media

Horario de Servicio

24 x 7

Horario de Soporte

Lunes a viernes 7:30 a 16:00

Cobertura del Servicio

El servicio tiene cobertura a nivel de toda la UTMACH

Condiciones de Entrega del Servicio

Los servidores deben estar alojados en el Data Center de la UTMACH.

Deben tener la capacidad de generar Logs.

Deben permitir por lo menos un tipo de servicio de monitoreo.

- Suministro Eléctrico Contingente

Descripción del Servicio

Servicio de emergencia ante la falla del suministro eléctrico público o el sistema Interconectado Central, conformado por dos UPS de 15 Kva, que dan respaldo hasta por una hora y media

Tipo de Servicio

Servicio General

Dueño del Servicio

Analista de TIC 3

Administrador del Servicio

Analista de TIC 3

Procedimiento de solicitud del Servicio

Cuando existe falla en el suministro eléctrico público o el sistema interconectado central, inmediatamente se realiza la conmutación al sistema de protección eléctrico.

Matriz de Prioridades

No aplica

Horario de Servicio

24 x 7

Horario de Soporte

24 x 7

Tiempos de respuesta

0.05 segundos

Cobertura del Servicio

Este servicio cubre a todos los equipos instalados dentro del Centro de Datos conectados a tomas protegidas.

Condiciones de Entrega del Servicio

El servicio cubrirá todos los dispositivos instalados dentro del Centro de Datos y conectados a una de las tomas eléctricas protegidas.

- Sistema de Climatización

Descripción del Servicio

Servicio de control de temperatura mediante un sistema de enfriamiento con sensores que detectan humedad y temperatura de Data Center.

Tipo de Servicio

Servicio General

Dueño del Servicio

Analista de TIC 3

Administrador del Servicio

Analista de TIC 3

Procedimiento de solicitud del Servicio

Cuando la temperatura generada por los equipos instalados dentro del Centro de Datos supera los 30 grados centígrados, el sistema de sensores detecta esta variación y automáticamente se ajusta para generar más frío y bajar la temperatura hasta el límite recomendado de climatización.

Matriz de Prioridades

No aplica

Horario de Servicio

24 x 7

Horario de Soporte

24 x 7

Tiempos de respuesta

0.05 segundos

Cobertura del Servicio

Este servicio cubre a todos los equipos instalados dentro del Centro de Datos.

Condiciones de Entrega del Servicio

El servicio cubrirá todos los dispositivos instalados dentro del Centro de Datos.